

VPN

R75.40

Administration Guide



15 October 2012

© 2012 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (<http://www.checkpoint.com/copyright.html>) for a list of our trademarks.

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation

The latest version of this document is at:

http://supportcontent.checkpoint.com/documentation_download?ID=13961

For additional technical information, visit the Check Point Support Center (<http://supportcenter.checkpoint.com>).

For more about this release, see the R75.40 home page (<http://supportcontent.checkpoint.com/solutions?id=sk67581>).

Revision History

| Date | Description |
|-----------------|---|
| 15 October 2012 | Updated Special Considerations for Wire Mode (on page 91) Added section VPN with One or More LSM Profiles (on page 57) |
| 17 April 2012 | First release of this document |

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments

(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on VPN R75.40 Administration Guide).

Contents

| | |
|---|-----------|
| Important Information | 3 |
| The Check Point VPN Solution | 9 |
| VPN Components | 9 |
| Understanding the Terminology | 9 |
| Site to Site VPN | 10 |
| VPN Communities | 10 |
| Remote Access VPN | 11 |
| IPSEC & IKE | 13 |
| Overview | 13 |
| IKE Phase I | 13 |
| IKE Phase II (Quick mode or IPSec Phase) | 15 |
| IKEv1 and IKEv2 | 16 |
| Methods of Encryption and Integrity | 16 |
| Phase I modes | 17 |
| Renegotiating IKE & IPSec Lifetimes | 17 |
| Perfect Forward Secrecy | 17 |
| IP Compression | 18 |
| Subnets and Security Associations | 18 |
| IKE DoS Protection | 19 |
| Understanding DoS Attacks | 19 |
| IKE DoS Attacks | 20 |
| Defense Against IKE DoS Attacks | 20 |
| SmartDashboard IKE DoS Attack Protection Settings | 21 |
| Advanced IKE Dos Attack Protection Settings | 21 |
| Configuring Advanced IKE Properties | 22 |
| On the VPN Community Network Object | 23 |
| On the Gateway Network Object | 23 |
| Introduction to Site to Site VPN | 24 |
| The Need for Virtual Private Networks | 24 |
| Confidentiality | 24 |
| Authentication | 24 |
| Integrity | 24 |
| How it Works | 25 |
| VPN Communities | 25 |
| Authentication Between Community Members | 26 |
| VPN Topologies | 27 |
| Access Control and VPN Communities | 32 |
| Routing Traffic within a VPN Community | 33 |
| Excluded Services | 33 |
| Special Considerations for Planning a VPN Topology | 33 |
| Configuring Site to Site VPNs | 33 |
| Migrating from Traditional Mode to Simplified Mode | 34 |
| Configuring a Meshed Community Between Internally Managed Gateways | 34 |
| Configuring a Star VPN Community | 35 |
| Confirming a VPN Tunnel Successfully Opens | 35 |
| Configuring a VPN with External Security Gateways Using PKI | 35 |
| Configuring a VPN with External Security Gateways Using a Pre-Shared Secret | 37 |
| How to Authorize Firewall Control Connections in VPN Communities | 38 |
| Why Turning off FireWall Implied Rules Blocks Control Connections | 39 |
| Allowing Firewall Control Connections Inside a VPN | 39 |
| Discovering Which Services are Used for Control Connections | 39 |
| Public Key Infrastructure | 40 |

| | |
|---|-----------|
| Need for Integration with Different PKI Solutions | 40 |
| Supporting a Wide Variety of PKI Solutions | 40 |
| PKI and Remote Access Users | 41 |
| PKI Deployments and VPN | 41 |
| Trusting An External CA | 43 |
| Enrolling a Managed Entity | 43 |
| Validation of a Certificate | 44 |
| Special Considerations for PKI | 47 |
| Using the Internal CA vs. Deploying a Third Party CA..... | 47 |
| Distributed Key Management and Storage..... | 47 |
| Configuration of PKI Operations | 47 |
| Trusting a CA – Step-By-Step | 47 |
| Certificate Revocation (All CA Types) | 49 |
| Certificate Recovery and Renewal | 49 |
| CA Certificate Rollover..... | 49 |
| Adding Matching Criteria to the Validation Process..... | 50 |
| CRL Cache Usage | 51 |
| Modifying the CRL Pre-Fetch Cache..... | 51 |
| Configuring CRL Grace Period | 51 |
| Configuring OCSP | 51 |
| Site-to-Site VPN | 52 |
| Domain Based VPN..... | 53 |
| Overview of Domain-based VPN | 53 |
| VPN Routing and Access Control | 53 |
| Configuring Domain Based VPN | 54 |
| Route Based VPN | 61 |
| Overview of Route-based VPN | 61 |
| VPN Tunnel Interface (VTI)..... | 62 |
| Using Dynamic Routing Protocols..... | 63 |
| Configuring Numbered VTIs..... | 63 |
| VTIs in a Clustered Environment | 65 |
| Configuring VTIs in a Clustered Environment | 65 |
| Enabling Dynamic Routing Protocols on VTIs | 71 |
| Configuring Anti-Spoofing on VTIs..... | 74 |
| Configuring a Loopback Interface | 74 |
| Configuring Unnumbered VTIs..... | 74 |
| Routing Multicast Packets Through VPN Tunnels..... | 75 |
| Tunnel Management..... | 77 |
| Overview of Tunnel Management | 77 |
| Configuring Tunnel Features..... | 79 |
| Route Injection Mechanism | 82 |
| Overview of Route Injection | 82 |
| Automatic RIM | 82 |
| Custom Scripts | 83 |
| Injecting Peer Security Gateway Interfaces..... | 85 |
| Configuring RIM..... | 85 |
| Configuring RIM on Gaia | 87 |
| Wire Mode | 88 |
| Overview of Wire Mode..... | 88 |
| Wire Mode Scenarios..... | 88 |
| Special Considerations for Wire Mode | 91 |
| Configuring Wire Mode | 91 |
| Directional VPN Enforcement | 93 |
| Overview of Directional VPN..... | 93 |
| Directional Enforcement within a Community | 93 |
| Configurable Objects in a Direction..... | 94 |
| Directional Enforcement between Communities..... | 95 |
| Configuring Directional VPN Within a Community..... | 95 |
| Configuring Directional VPN Between Communities | 96 |

| | |
|---|------------|
| Link Selection | 97 |
| Link Selection Overview | 97 |
| Configuring IP Selection by Remote Peer | 97 |
| Configuring Outgoing Route Selection | 99 |
| When Initiating a Tunnel | 99 |
| Configuring Source IP Address Settings | 101 |
| Outgoing Link Tracking | 101 |
| Link Selection Scenarios | 101 |
| Service Based Link Selection | 105 |
| Trusted Links | 109 |
| On Demand Links (ODL) | 112 |
| Link Selection and ISP Redundancy | 113 |
| Link Selection and ISP Redundancy Scenarios | 114 |
| Link Selection with non-Check Point Devices | 115 |
| Multiple Entry Point VPNs | 117 |
| Overview of MEP | 117 |
| Explicit MEP | 118 |
| Implicit MEP | 123 |
| Routing Return Packets | 125 |
| Special Considerations | 126 |
| Configuring MEP | 126 |
| Traditional Mode VPNs | 130 |
| Introduction to Traditional Mode VPNs | 130 |
| VPN Domains and Encryption Rules | 131 |
| Defining VPN Properties | 132 |
| Internally and Externally Managed Security Gateways | 132 |
| Considerations for VPN Creation | 132 |
| Configuring Traditional Mode VPNs | 132 |
| Converting a Traditional Policy to a Community Based Policy | 137 |
| Introduction to Converting to Simplified VPN Mode | 137 |
| How Traditional VPN Mode Differs from a Simplified VPN Mode | 137 |
| How an Encrypt Rule Works in Traditional Mode | 138 |
| Principles of the Conversion to Simplified Mode | 139 |
| Placing the Security Gateways into the Communities | 139 |
| Conversion of Encrypt Rule | 139 |
| Remote Access VPN | 143 |
| Check Point Remote Access Solutions | 144 |
| Providing Secure Remote Access | 144 |
| Types of Solutions | 144 |
| Remote Access Solution Comparison | 145 |
| Summary of Remote Access Options | 146 |
| Remote Access VPN Overview | 149 |
| Remote Access VPN Overview | 149 |
| SecureClient Remote Access Solution | 149 |
| Need for Remote Access VPN | 154 |
| VPN for Remote Access Considerations | 155 |
| Policy Definition for Remote Access | 155 |
| User Certificate Creation Methods when Using the ICA | 155 |
| Multiple Certificates per User | 155 |
| Internal User Database vs. External User Database | 155 |
| NT Group/RADIUS Class Authentication Feature | 156 |
| Configuring Remote Access VPN | 157 |
| Remote Access VPN Workflow | 158 |
| Creating Remote Access VPN Certificates for Users | 158 |
| Creating and Configuring the Security Gateway | 160 |
| Defining User and Authentication Methods in LDAP | 160 |
| Enrolling User Certificates - ICA Management Tool | 160 |
| Configuring Certificates Using Third Party PKI | 160 |
| Enabling Hybrid Mode and Methods of Authentication | 161 |

| | |
|---|-----|
| Configuring Authentication for NT groups and RADIUS Classes..... | 161 |
| Using a Pre-Shared Secret | 162 |
| Defining an LDAP User Group | 162 |
| Defining a User Group | 162 |
| Defining a VPN Community and its Participants..... | 162 |
| Defining Access Control Rules..... | 162 |
| Installing the Policy | 162 |
| User Certificate Management | 163 |
| Modifying Encryption Properties for Remote Access VPN | 163 |
| Working with RSA Hard and Soft Tokens..... | 164 |
| Office Mode | 166 |
| The Need for Remote Clients to be Part of the LAN..... | 166 |
| Office Mode | 166 |
| Enabling IP Address per User | 171 |
| Office Mode Considerations..... | 174 |
| Configuring Office Mode | 174 |
| Packaging SecureClient | 180 |
| Introduction: The Need to Simplify Remote Client Installations | 180 |
| The Check Point Solution - SecureClient Packaging Tool..... | 180 |
| Creating a Preconfigured Package | 181 |
| Configuring MSI Packaging..... | 182 |
| Desktop Security | 185 |
| The Need for Desktop Security | 185 |
| Desktop Security Considerations | 185 |
| Configuring Desktop Security..... | 186 |
| Layer Two Tunneling Protocol (L2TP) Clients..... | 187 |
| The Need for Supporting L2TP Clients | 187 |
| Solution - Working with L2TP Clients | 187 |
| Considerations for Choosing Microsoft IPsec/L2TP Clients | 190 |
| Configuring Remote Access for Microsoft IPsec/L2TP Clients..... | 191 |
| Secure Configuration Verification | 195 |
| The Need to Verify Remote Client's Security Status | 195 |
| The Secure Configuration Verification Solution | 195 |
| Considerations regarding SCV..... | 198 |
| Configuring SCV | 198 |
| VPN Routing - Remote Access..... | 219 |
| The Need for VPN Routing | 219 |
| Check Point Solution for Greater Connectivity and Security..... | 219 |
| Configuring VPN Routing for Remote Access VPN | 222 |
| Link Selection for Remote Access Clients | 224 |
| Overview..... | 224 |
| Configuring Link Selection for Remote Access Only | 224 |
| Using Directional VPN for Remote Access | 225 |
| Directional VPN in RA Communities | 225 |
| Configuring Directional VPN with Remote Access Communities | 226 |
| Remote Access Advanced Configuration..... | 227 |
| Non-Private Client IP Addresses..... | 227 |
| Preventing a Client Inside the Encryption Domain from Encrypting..... | 228 |
| Authentication Timeout and Password Caching | 231 |
| Secure Domain Logon (SDL) | 231 |
| Back Connections (Server to Client) | 232 |
| Auto Topology Update (Connect Mode only) | 233 |
| How to Work with non-Check Point Firewalls | 233 |
| Resolving Internal Names with the SecuRemote DNS Server..... | 233 |
| Multiple Entry Point for Remote Access VPNs..... | 234 |
| The Need for Multiple Entry Point Security Gateways | 234 |
| The Check Point Solution for Multiple Entry Points | 234 |
| Disabling MEP | 236 |
| Configuring MEP..... | 236 |

| | |
|---|------------|
| Configuring Preferred Backup Security Gateway | 237 |
| Disabling MEP | 237 |
| Userc.C and Product.ini Configuration Files | 238 |
| Introduction to Userc.C and Product.ini..... | 238 |
| Userc.C File Parameters..... | 239 |
| Product.ini Parameters | 246 |
| SSL Network Extender | 249 |
| Introduction to the SSL Network Extender | 249 |
| How the SSL Network Extender Works..... | 250 |
| Commonly Used Concepts | 250 |
| Special Considerations for the SSL Network Extender..... | 251 |
| Configuring the SSL Network Extender..... | 253 |
| SSL Network Extender User Experience..... | 259 |
| Troubleshooting SSL Network Extender | 269 |
| Resolving Connectivity Issues | 271 |
| The Need for Connectivity Resolution Features | 271 |
| Check Point Solution for Connectivity Issues | 271 |
| Overcoming NAT Related Issues | 271 |
| Overcoming Restricted Internet Access | 276 |
| Configuring Remote Access Connectivity | 279 |
| Appendices | 284 |
| VPN Command Line Interface | 285 |
| VPN Commands..... | 285 |
| SecureClient Commands..... | 286 |
| Desktop Policy Commands..... | 287 |
| VPN Shell..... | 289 |
| Configuring a Virtual Interface Using the VPN Shell | 289 |
| Index | 291 |

Chapter 1

The Check Point VPN Solution

In This Chapter

| | |
|-------------------------------|----|
| VPN Components | 9 |
| Understanding the Terminology | 9 |
| Site to Site VPN | 10 |
| VPN Communities | 10 |
| Remote Access VPN | 11 |

Virtual Private Networking technology leverages existing infrastructure (the Internet) as a way of building and enhancing existing connectivity in a secure manner. Based on standard Internet secure protocols, VPN implementation enables secure links between special types of network nodes: Check Point Security Gateways. Site to Site VPN ensures secure links between Security Gateways. Remote Access VPN ensures secure links between Security Gateways and remote access clients.

Check Point's Security Gateway is an integrated software solution that provides connectivity to corporate networks, remote and mobile users, branch offices and business partners on a wide range of open platforms and security appliances.

Check Point Security Gateways integrate access control, authentication, and encryption to guarantee the security of network connections over the public Internet.

A typical deployment places a Check Point Security Gateway connecting the corporate network (from the Internet), and remote access software on the laptops of mobile users. Other remote sites are guarded by additional Check Point Security Gateways and communication between all components regulated by a strict security policy.

VPN Components

VPN is composed of:

- *VPN endpoints*, such as Security Gateways, Security Gateways clusters, or remote clients (such as laptop computers or mobile phones) that communicate using a VPN.
- *VPN trust entities*, such as a Check Point Internal Certificate Authority (ICA). The ICA is part of the Check Point suite used for creating SIC trusted connection between Security Gateways, authenticating administrators and third party servers. The ICA provides certificates for internal Security Gateways and remote access clients which negotiate the VPN link.
- *VPN Management tools*. Security Management server and SmartDashboard. SmartDashboard is the SmartConsole used to access the Security Management server. The VPN Manager is part of SmartDashboard. SmartDashboard enables organizations to define and deploy Intranet, and remote Access VPNs.

Understanding the Terminology

A number of terms are used widely in Secure VPN implementation, namely:

- **VPN**. An encrypted, private network that makes secure connections between Security Gateways and VPN endpoints over a public network, such as the Internet.
- **VPN Tunnel Interface**. A Virtual Tunnel Interface (VTI) is a virtual interface on a Security Gateway that is related to an existing, Route Based VPN tunnel. The Route Based VPN tunnel works as a point-to-point connection between two peer Security Gateways in a VPN community.

- **Peer.** A Security Gateway that connects to another Security Gateway using a Virtual Tunnel Interface.
- **VPN Topology.** The basic element of VPN is the link or encrypted tunnel. Links are created between Security Gateways. A collection of links is a *topology*. The topology shows the layout of the VPN. Two basic topologies found in VPN are *Mesh* and *Star*.
- **VPN Security Gateway.** The endpoint for the encrypted connection, which can be any peer that supports the IPSec protocol framework. Security Gateways can be single standalone modules or arranged into clusters for "high availability" and "load sharing".
- **VPN Domain.** A group that specifies the hosts or networks for which encryption of IP datagrams is performed. A VPN Security Gateway provides an entrance point to the VPN Domain.
- **Site to Site VPN.** Refers to a VPN tunnel between two Security Gateways.
- **Remote Access VPN.** Refers to remote users accessing the network with client software such as Check Point Remote Access Clients or third party IPSec clients. The Check Point Security Gateway provides a *Remote Access Service* to the remote clients.
- **Encryption algorithm.** A set of mathematical processes for rendering information into a meaningless form, the mathematical transformations and conversions controlled by a special key. In VPN, various encryption algorithms such as 3DES and AES ensure that only the communicating peers are able to understand the message.
- **Integrity.** Integrity verification (using hash functions) ensures that the traffic has not been intercepted or altered during transmission.
- **Trust.** Public key infrastructure (PKI), certificates and certificate authorities are employed to establish trust between Security Gateways. (In the absence of PKI, Security Gateways employ a pre-shared secret.)
- **IKE & IPSec.** Secure VPN protocols used to manage encryption keys, and exchange encrypted packets. IPSec is an encryption technology framework which supports several standards to provide authentication and encryption services of data on a private or public network. IKE (Internet Key Exchange) is a key management protocol standard. IKE enhances IPSec by providing additional features, flexibility, and ease of configuration.

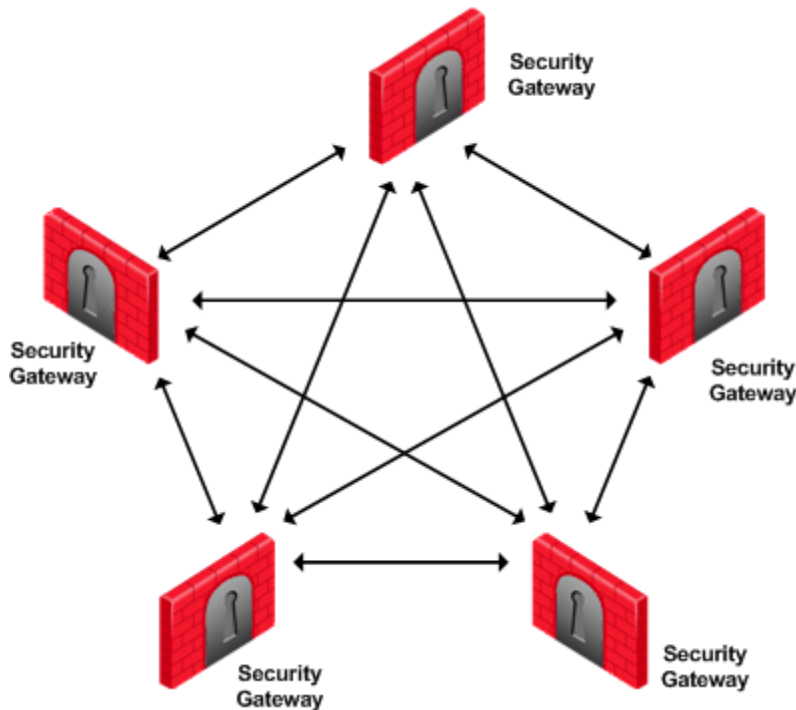
Site to Site VPN

At the center of VPN is the encrypted tunnel (or VPN link) created using the IKE/IPSec protocols. The two parties are either Check Point Security Gateways or remote access clients. The peers negotiating a link first create a trust between them. This trust is established using certificate authorities, PKI or pre-shared secrets. Methods are exchanged and keys created. The encrypted tunnel is established and then maintained for multiple connections, exchanging key material to refresh the keys when needed. A single Security Gateway maintains multiple tunnels simultaneously with its VPN peers. Traffic in each tunnel is encrypted and authenticated between the VPN peers, ensuring integrity and privacy. Data is transferred in bulk via these virtual-physical links.

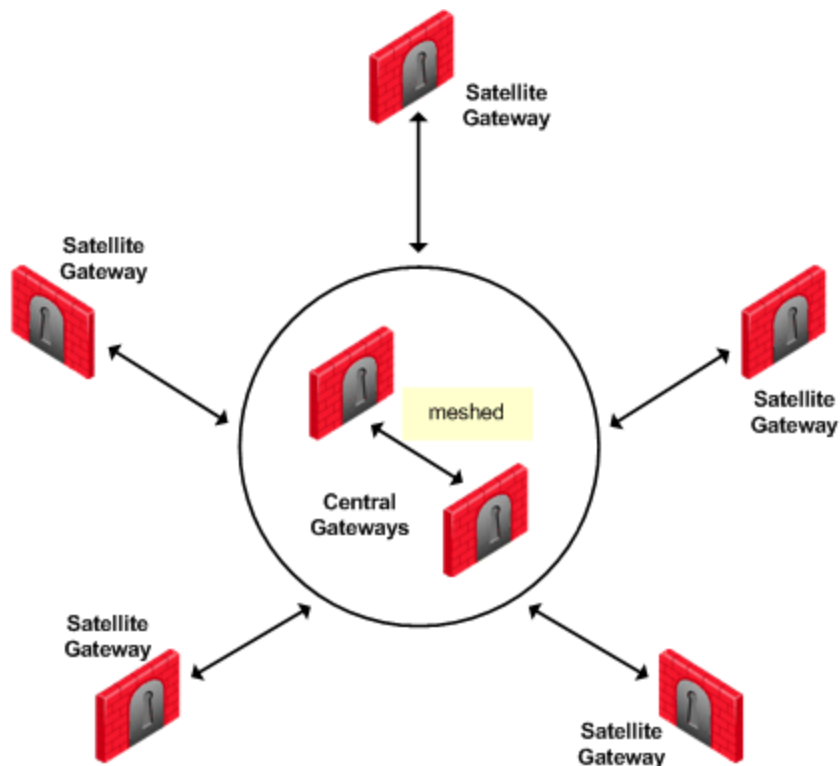
VPN Communities

There are two basic community types - Mesh and Star. A topology is the collection of enabled VPN links in a system of Security Gateways, their VPN domains, hosts located behind each Security Gateway and the remote clients external to them.

In a Mesh community, every Security Gateway has a link to every other Security Gateway:



In a Star community, only Security Gateways defined as Satellites (or "spokes") are allowed to communicate with a central Security Gateway (or "Hub") but not with each other:



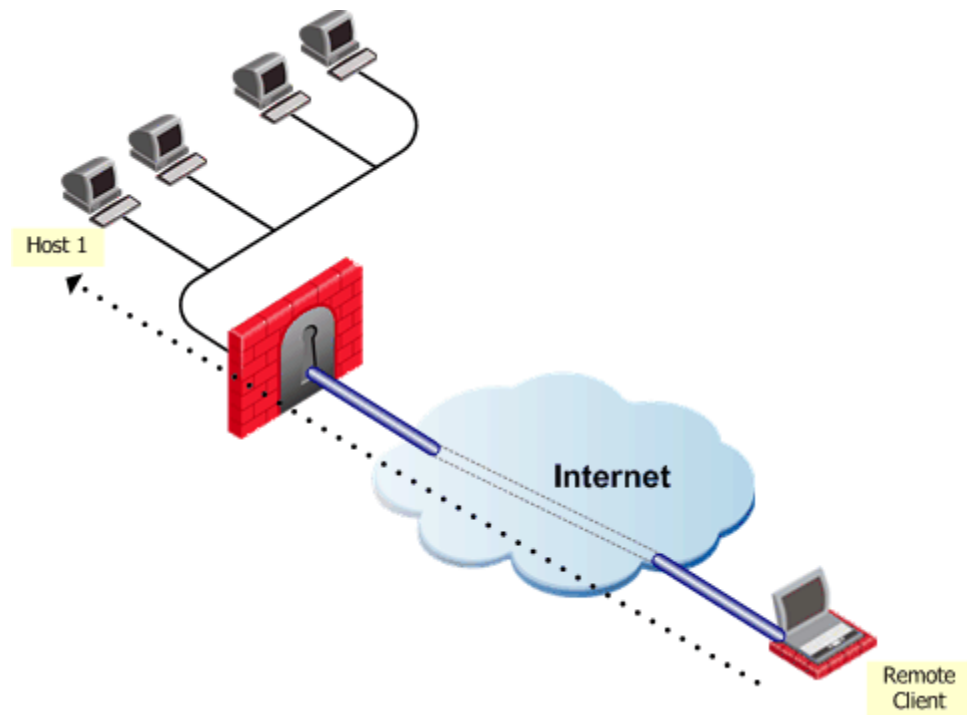
Connectivity can be further enhanced by meshing central Security Gateways. This kind of topology is suitable for deployments involving Extranets that include networks belonging to business partners.

Remote Access VPN

Whenever users access the organization from remote locations, it is essential that the usual requirements of secure connectivity be met but also the special demands of remote clients.

SecuRemote/SecureClient extends VPN functionality to remote users, enabling users to securely communicate sensitive information to networks and servers over the VPN tunnel, using both dial-up

(including broadband connections), and LAN (and wireless LAN) connections. Users are managed either in the internal database of the Check Point Security Gateway or via an external LDAP server.



The remote user initiates a connection to the Security Gateway. Authentication takes place during the IKE negotiation. Once the user's existence is verified, the Security Gateway then authenticates the user, for example by validating the user's certificate. Once IKE is successfully completed, a tunnel is created; the remote client connects to Host 1.

Chapter 2

IPSEC & IKE

In This Chapter

| | |
|-------------------------------------|----|
| Overview | 13 |
| IKE DoS Protection | 19 |
| Configuring Advanced IKE Properties | 22 |

Overview

In symmetric cryptographic systems, both communicating parties use the same key for encryption and decryption. The material used to build these keys must be exchanged in a secure fashion. Information can be securely exchanged only if the key belongs exclusively to the communicating parties.

The goal of the *Internet Key Exchange* (IKE) is for both sides to independently produce the same symmetrical key. This key then encrypts and decrypts the regular IP packets used in the bulk transfer of data between VPN peers. IKE builds the VPN tunnel by authenticating both sides and reaching an agreement on methods of encryption and integrity. The outcome of an IKE negotiation is a *Security Association* (SA).

This agreement upon keys and methods of encryption must also be performed securely. For this reason IKE, is composed of two phases. The first phase lays the foundations for the second. Both IKEv1 and IKEv2 are supported in Security Gateways of version R71 and higher.

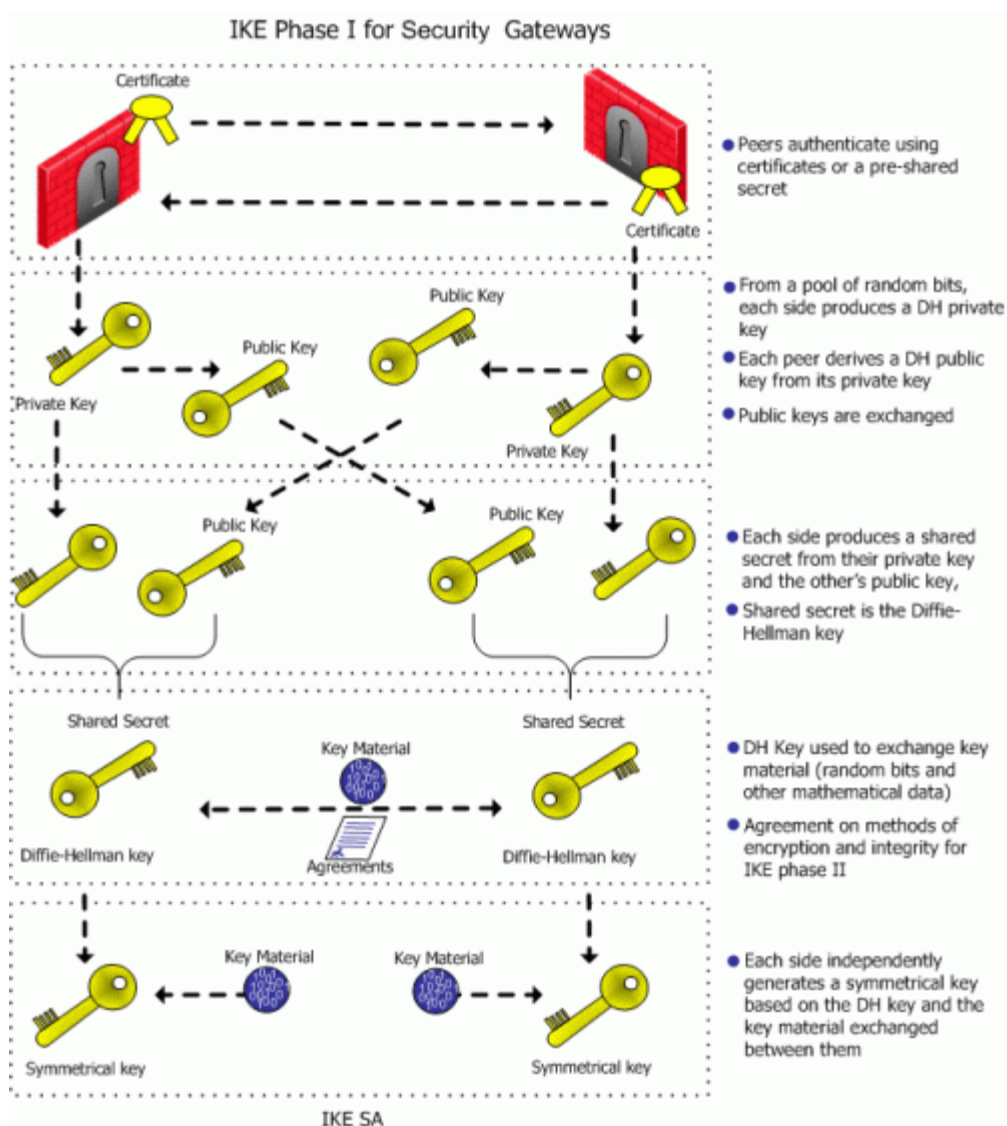
Diffie-Hellman (DH) is that part of the IKE protocol used for exchanging the material from which the symmetrical keys are built. The Diffie-Hellman algorithm builds an encryption key known as a "shared secret" from the private key of one party and the public key of the other. Since the IPSec symmetrical keys are derived from this DH key shared between the peers, at no point are symmetric keys actually exchanged.

IKE Phase I

During IKE Phase I:

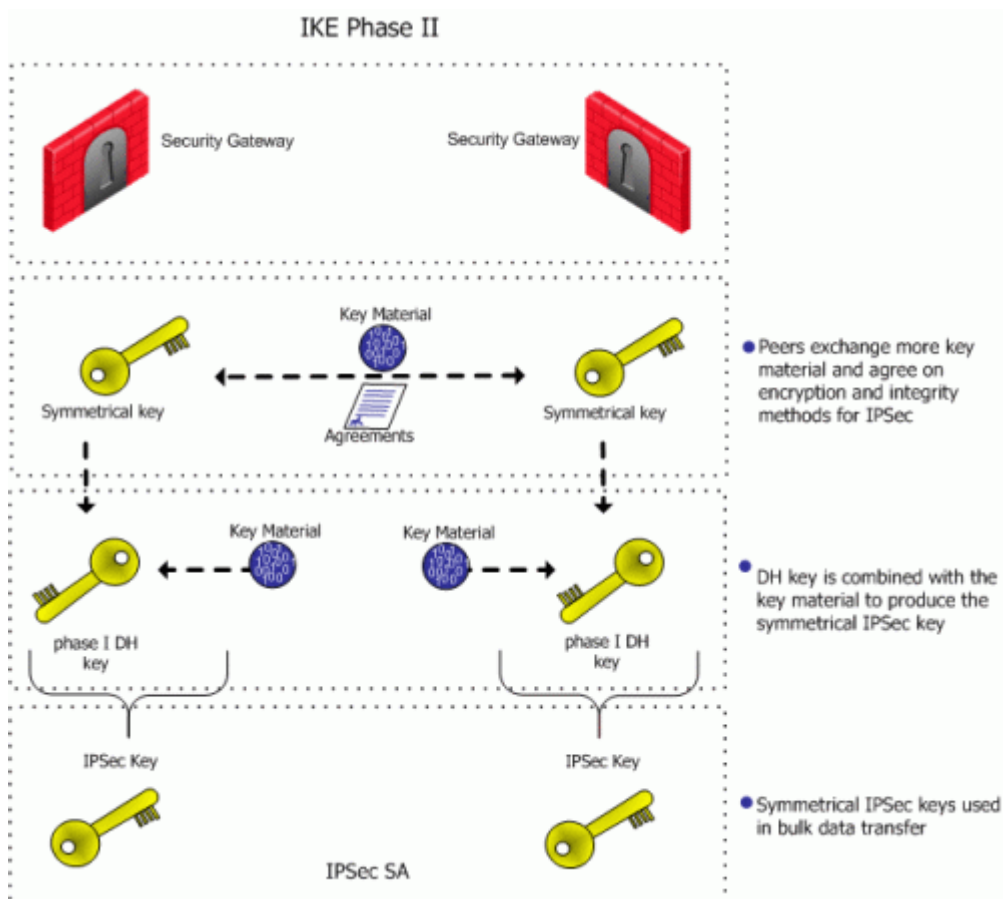
- The peers authenticate, either by certificates or via a pre-shared secret. (More authentication methods are available when one of the peers is a remote access client.)
- A Diffie-Hellman key is created. The nature of the Diffie-Hellman protocol means that both sides can independently create the shared secret, a key which is known only to the peers.
- Key material (random bits and other mathematical data) as well as an agreement on methods for IKE phase II are exchanged between the peers.

In terms of performance, the generation of the Diffie Hellman Key is slow and heavy. The outcome of this phase is the IKE SA, an agreement on keys and methods for IKE phase II. Figure 2-1 illustrates the process that takes place during IKE phase I but does not necessarily reflect the actual order of events.

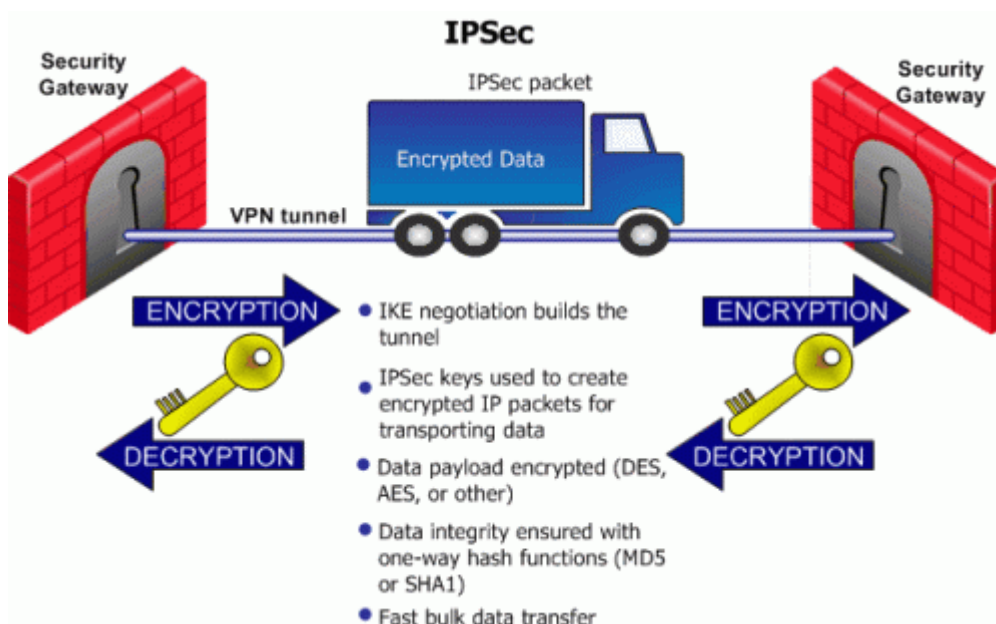


IKE Phase II (Quick mode or IPSec Phase)

IKE phase II is encrypted according to the keys and methods agreed upon in IKE phase I. The key material exchanged during IKE phase II is used for building the IPSec keys. The outcome of phase II is the IPSec Security Association. The IPSec SA is an agreement on keys and methods for IPSec, thus IPSec takes place according to the keys and methods agreed upon in IKE phase II.



Once the IPSec keys are created, bulk data transfer takes place:



IKEv1 and IKEv2

IKEv2 is supported inside VPN communities working in Simplified mode in versions R71 and higher. IKEv2 is a standard that is implemented differently in each vendor's products. When vendors implement IKE v2 the same way, it enables better interoperability and integration. See RFCs 4306 and 4301 for more information.

IKEv2 is configured in the **VPN Community Properties window > Encryption**. The default setting is **IKEv1 only**.

For Remote users, the IKE settings are configured in **Global Properties > Remote Access > VPN Authentication and Encryption**.



Note - IKEv2 is not supported on UTM-1 Edge devices or VSX objects before R75.40VS. If UTM-1 Edge devices or such VSX objects are included in a VPN Community, the Encryption setting should be **Support IKEv1**.

Methods of Encryption and Integrity

Two parameters are decided during the negotiation:

- Encryption algorithm
- Hash algorithm

Methods of Encryption/integrity for IKE

| Parameter | IKE Phase 1 (IKE SA) | IKE PHASE 2 (IPSec SA) |
|------------|---|---|
| Encryption | <ul style="list-style-type: none"> • AES -256(default) • 3DES • DES • CAST | <ul style="list-style-type: none"> • AES -128 (default) • 3DES • AES - 256 • DES • CAST • DES -40CP • CAST -40 • NULL • AES-GCM -128 • AES-GCM -256 |
| Integrity | <ul style="list-style-type: none"> • SHA1 (default) • MD5 • SHA -256 • AES-XCBC • SHA -384 | <ul style="list-style-type: none"> • MD5 (default) • SHA1 • SHA -256 • AES-XCBC • SHA -384 |

NULL means perform an integrity check only; *packets are not encrypted*.

Diffie Hellman Groups

The Diffie-Hellman key computation (also known as exponential key agreement) is based on the Diffie Hellman (DH) mathematical groups. A Security Gateway supports these DH groups during the two phases of IKE.

DH groups

| Parameter | IKE Phase 1 (IKE SA) | IKE Phase 2 (IPSec SA) |
|-----------------------|--|--|
| Diffie Hellman Groups | <ul style="list-style-type: none"> • Group2 (1024 bits) (default) • Group1 (768 bits) • Group5 (1536 bits) • Group14 (2048 bits) • Group19 (256-bit ECP) • Group20 (384-bit ECP) | <ul style="list-style-type: none"> • Group2 (1024 bits) (default) • Group1 (768 bits) • Group5 (1536 bits) • Group14 (2048 bits) • Group19 (256-bit ECP) • Group20 (384-bit ECP) |

A group with more bits ensures a key that is harder to break, but carries a heavy cost in terms of performance, since the computation requires more CPU cycles.

Phase I modes

Between Security Gateways, there are two modes for IKE phase I. These modes only apply to IKEv1:

- Main Mode
- Aggressive Mode

If aggressive mode is *not* selected, the Security Gateway defaults to main mode, performing the IKE negotiation using six packets; aggressive mode performs the IKE negotiation with three packets.

Main mode is preferred because:

- Main mode is partially encrypted, from the point at which the shared DH key is known to both peers.
- Main mode is less susceptible to **Denial of Service** (DoS) attacks. In main mode, the DH computation is performed *after* authentication. In aggressive mode, the DH computation is performed parallel to authentication. A peer that is not yet authenticated can force processor intensive Diffie-Hellman computations on the other peer.



Note - Use aggressive mode when a Check Point Security Gateway needs to negotiate with third party VPN solutions that do not support main mode.

When dealing with remote access, IKE has additional modes:

- *Hybrid mode*. Hybrid mode provides an alternative to IKE phase I, where the Security Gateway is allowed to authenticate using certificates and the client via some other means, such as SecurID. For more information on Hybrid mode, see: Introduction to Remote Access VPN.
- *Office mode*. Office mode is an extension to the IKE protocol. Office Mode is used to resolve routing issues between remote access clients and the VPN domain. During the IKE negotiation, a special mode called *config mode* is inserted between phases I and II. During config mode, the remote access client requests an IP address from the Security Gateway. After the Security Gateway assigns the IP address, the client creates a virtual adapter in the Operating System. The virtual adapter uses the assigned IP address. For further information, see: Office Mode (on page 166).

Renegotiating IKE & IPSec Lifetimes

IKE phase I is more processor intensive than IKE phase II, since the Diffie-Hellman keys have to be produced and the peers authenticated each time. For this reason, IKE phase I is performed less frequently. However, the IKE SA is only valid for a certain period, after which the IKE SA must be renegotiated. The IPSec SA is valid for an even shorter period, meaning many IKE phase II's take place.

The period between each renegotiation is known as the **lifetime**. Generally, the shorter the lifetime, the more secure the IPSec tunnel (at the cost of more processor intensive IKE negotiations). With longer lifetimes, future VPN connections can be set up more quickly. By default, IKE phase I occurs once a day; IKE phase II occurs every hour but the time-out for each phase is configurable.

The IPSec lifetime can also be configured according to Kilo Bytes by using **GuiDBedit** to edit the **objects_5_0.c** file. The relevant properties are under the community set:

- **ike_p2_use_rekey_kbytes**. Change from **false** (default) to **true**.
- **ike_p2_rekey_kbytes**. Modify to include the required rekeying value (default 50000).

Perfect Forward Secrecy

The keys created by peers during IKE phase II and used for IPSec are based on a sequence of random binary digits exchanged between peers, and on the DH key computed during IKE phase I.

The DH key is computed once, then used a number of times during IKE phase II. Since the keys used during IKE phase II are based on the DH key computed during IKE phase I, there exists a mathematical relationship between them. For this reason, the use of a single DH key may weaken the strength of subsequent keys. If one key is compromised, subsequent keys can be compromised with less effort.

In cryptography, **Perfect Forward Secrecy** (PFS) refers to the condition in which the compromise of a current session key or long-term private key does *not* cause the compromise of earlier or subsequent keys. Security Gateways meet this requirement with a PFS mode. When PFS is enabled, a fresh DH key is generated during IKE phase II, and renewed for each key exchange.

However, because a new DH key is generated during each IKE phase I, no dependency exists between these keys and those produced in subsequent IKE Phase I negotiations. Enable PFS in IKE phase II only in situations where extreme security is required.

The DH group used during PFS mode is configurable between groups 1, 2, 5 and 14, with group 2 (1042 bits) being the default.



Note - PFS mode is supported only between gateways, not between Security Gateways and remote access clients.

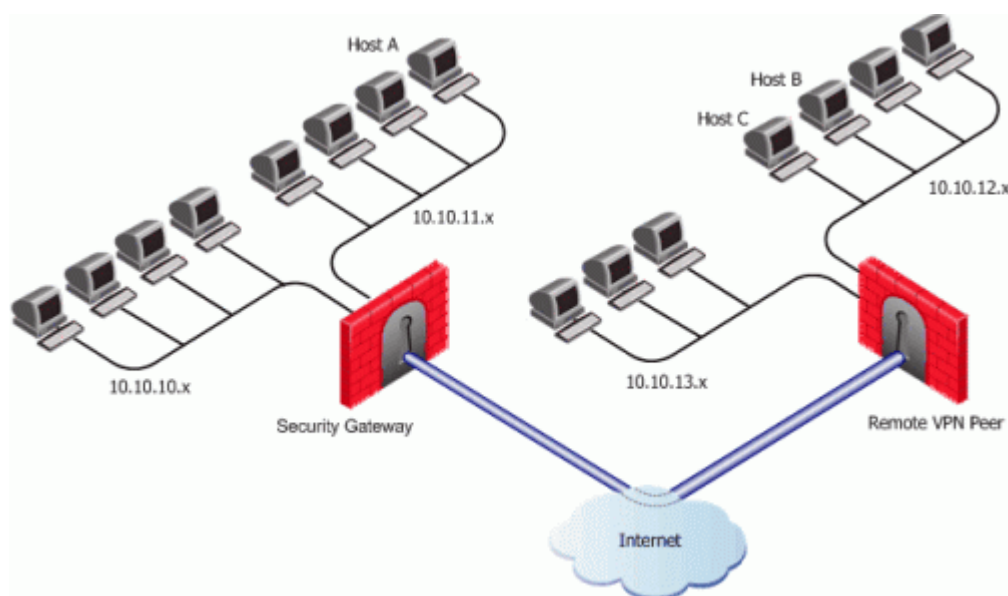
IP Compression

IP compression is a process that reduces the size of the data portion of the TCP/IP packet. Such a reduction can cause significant improvement in performance. IPsec supports the *Flate/Deflate* IP compression algorithm. Deflate is a smart algorithm that adapts the way it compresses data to the actual data itself. Whether to use IP compression is decided during IKE phase II. IP compression is not enabled by default.

IP compression is important for SecuRemote/SecureClient users with slow links. For Example, dialup modems do compression as a way of speeding up the link. Security Gateway encryption makes TCP/IP packets appear "mixed up". This kind of data cannot be compressed and bandwidth is lost as a result. If IP compression is enabled, packets are compressed *before* encryption. This has the effect of recovering the lost bandwidth.

Subnets and Security Associations

By default, a VPN tunnel is never created just for the hosts machines involved in the communication, but for the complete subnets, the hosts reside on.

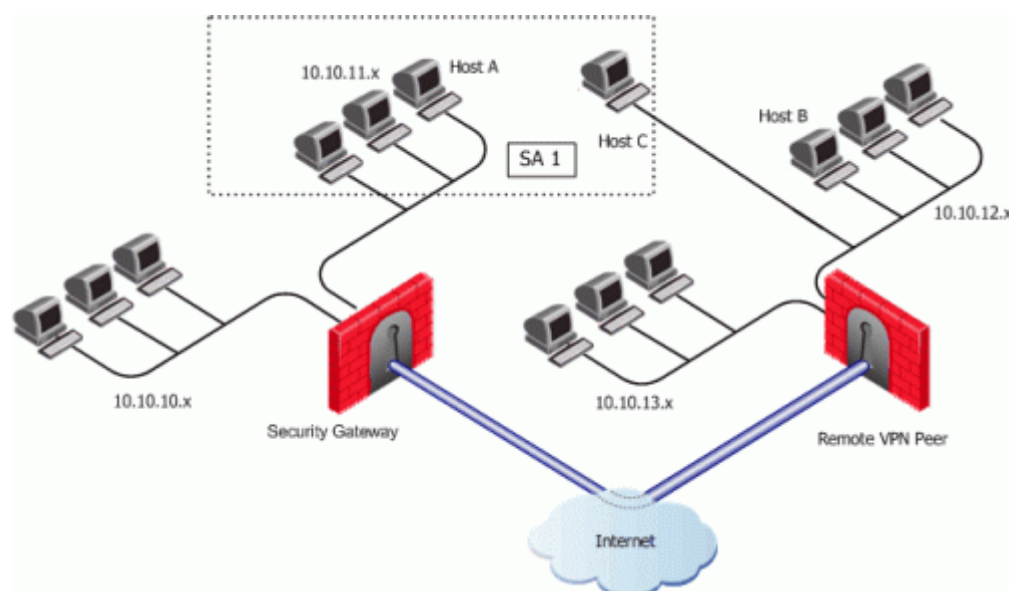


A Security Gateway protects a network consisting of two subnets (10.10.10.x, and 10.10.11.x, with netmask 255.255.255.0 for both). A second Security Gateway, the remote peer, protects subnets 10.10.12.x and 10.10.13.x, with netmask 255.255.255.0.

Because a VPN tunnel is created by default for complete subnets, four SA's exist between the Security Gateway and the peer Security Gateway. When Host A communicates with Host B, an SA is created between Host A's subnet and Host B's subnet.

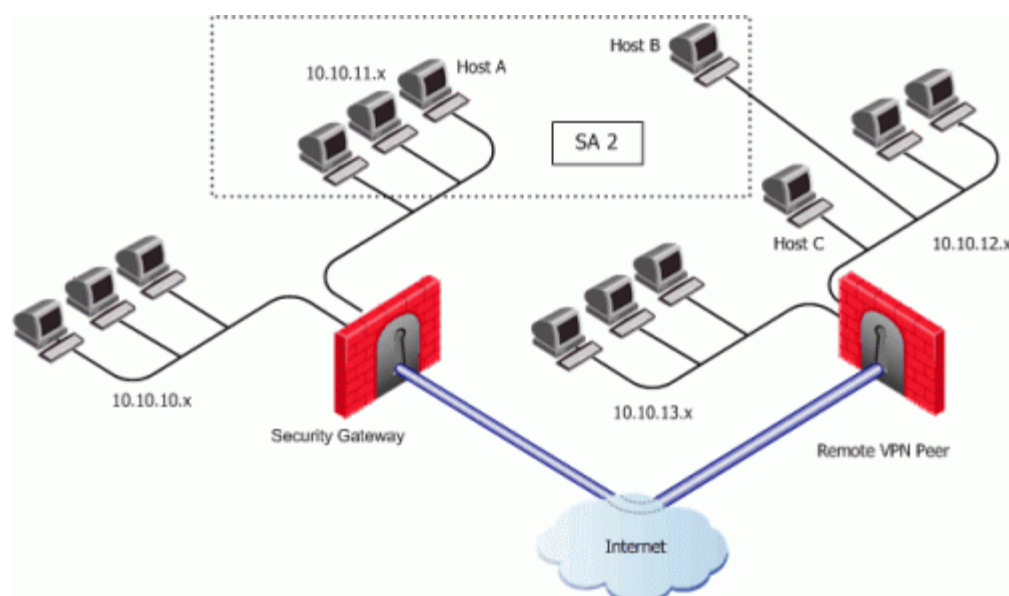
Unique SA Per Pair of Peers

By disabling the **Support Key exchange for subnets** option on each Security Gateway, it is possible to create a *unique* Security Association per pair of peers.



If the Security Gateway is configured to **Support key exchange for subnets** and the option remains unsupported on the remote peer, when host A communicates with host C, a Security Association (SA 1) will be negotiated between host A's subnet and host C's IP address. The same SA is then used between any host on the 10.10.11.x subnet and Host C.

When host A communicates with host B, a separate Security Association (SA 2) is negotiated between host A's subnet and host B. As before, the same SA is then used between any host in 10.10.11.x subnet and Host B.



When **Support Key exchange for subnets** is not enabled on communicating Security Gateways, then a security association is negotiated between individual IP addresses; in effect, a unique SA per host.

IKE DoS Protection

Understanding DoS Attacks

Denial of Service (DoS) attacks are intended to reduce performance, block legitimate users from using a service, or even bring down a service. They are not direct security threats in the sense that no confidential

data is exposed, and no user gains unauthorized privileges. However, they consume computer resources such as memory or CPU.

Generally, there are two kinds of DoS attack. One kind consists of sending malformed (garbage) packets in the hope of exploiting a bug and crashing the service. In the other kind of DoS attack, an attacker attempts to exploit a vulnerability of the service or protocol by sending well-formed packets. IKE DoS attack protection deals with the second kind of attack.

IKE DoS Attacks

The IKE protocol requires that the receiving Security Gateway allocates memory for the first IKE Phase 1 request packet that it receives. The Security Gateway replies, and receives another packet, which it then processes using the information gathered from the first packet.

An attacker can send many IKE first packets, while forging a different source IP address for each. The receiving Security Gateway is obliged to reply to each, and assign memory for each. This can consume all CPU resources, thereby preventing connections from legitimate users.

The attacker sending IKE packets can pretend to be a machine that is allowed to initiate IKE negotiations, such as a Check Point Security Gateway. This is known as an identified source. The attacker can also pretend to have an IP address that the receiving Security Gateway does not know about, such as a SecuRemote/SecureClient, or a Check Point Security Gateway with a dynamic IP address. This is known as an unidentified source.

Defense Against IKE DoS Attacks

When the number of simultaneous IKE negotiations handled exceeds the accepted threshold, it concludes that it is either under load or experiencing a Denial of Service attack. In such a case, the Security Gateway can filter out peers that are the probable source of a potential Denial of Service attack. The following sections describe different types of defenses against IKE DoS attacks.

Stateless Protection Against IKE DoS Attacks

A Security Gateway prevents IKE DoS Attacks by delaying allocation of Security Gateway resources until the peer proves itself to be legitimate. The following process is called stateless protection:

If the Security Gateway concludes that it is either under load or experiencing a Denial of Service attack, and it receives an IKE request, it replies to the alleged source with a packet that contains a number that only the Security Gateway can generate. The Security Gateway then "forgets" about the IKE request. In other words, it does not need to store the IKE request in its memory (which is why the protection is called "Stateless").

The machine that receives the packet is required to reinitiate the IKE request by sending an IKE request that includes this number.

If the Security Gateway receives an IKE request that contains this number, the Security Gateway will recognize the number as being one that only it can generate, and will only then continue with the IKE negotiation, despite being under load.

If the Check Point Security Gateway receives IKE requests from many IP addresses, each address is sent a different unique number, and each address is required to reinitiate the IKE negotiation with a packet that includes that number. If the peer does not reside at these IP addresses, this unique number will never reach the peer. This will thwart an attacker who is pretending to send IKE requests from many IP addresses.

IKE DoS attack protection is not available for third party Security Gateways. Under heavy load, third party Security Gateways and clients (such as Microsoft IPsec/L2TP clients) may be unable to connect.

Using Puzzles to Protect Against IKE DoS Attacks

Stateless protection is appropriate when the IKE packet appears to come from an identified source, that is, a machine that is allowed to initiate IKE negotiations, such as a Check Point Security Gateway.

An unidentified source is an IP address that the receiving Security Gateway does not recognize, such as a SecuRemote/SecureClient, or a Check Point Security Gateway with a dynamic IP address. An attacker may well have control of many unidentified IP addresses, and may be able to reply to stateless packets from all these addresses. Therefore, if an attack comes from an unidentified source, another approach is required.

The Security Gateway can require that the source of the IKE request solves a computationally intensive puzzle. Most computers can solve only a very few of these puzzles per second, so that an attacker would only be able to send very few IKE packets per second. This renders a DoS attack ineffective.

IKE DoS attack protection is not available for Third party Security Gateways. Under heavy load, they may be unable to connect.

SmartDashboard IKE DoS Attack Protection Settings

To protect against IKE DoS attacks, edit the SmartDashboard **IKE Denial of Service Protection** settings, in the **VPN >Advanced** page of the **Global Properties**.

- **Support IKE DoS protection from identified source** — The default setting for identified sources is **Stateless**. If the Security Gateway is under load, this setting requires the peer to respond to an IKE notification in a way that proves that the IP address of the peer is not spoofed. If the peer cannot prove this, the Security Gateway does not begin the IKE negotiation.
If the source is identified, protecting using **Puzzles** is over cautious, and may affect performance. A third possible setting is **None**, which means no DoS protection.
- **Support IKE DoS protection from unidentified source** — The default setting for unidentified sources is **Puzzles**. If the Security Gateway is under load, this setting requires the peer to solve a mathematical puzzle. Solving this puzzle consumes peer CPU resources in a way that makes it difficult to initiate multiple IKE negotiations simultaneously.
For unidentified sources, **Stateless** protection may not be sufficient because an attacker may well control all the IP addresses from which the IKE requests appear to be sent. A third possible setting is **None**, which means no DoS protection.

Advanced IKE Dos Attack Protection Settings

Advanced IKE DoS attack protection can be configured on the Security Management server using the **GuiDBedit** command line or using GuiDBedit, the Check Point Database Tool. Configure the protection by means of the following Global Properties.

ike_dos_threshold

Values: 0-100. Default: 70. Determines the percentage of maximum concurrent ongoing negotiations, above which the Security Gateway will request DoS protection. If the threshold is set to 0, the Security Gateway will always request DoS protection.

ike_dos_puzzle_level_identified_initiator

Values: 0-32. Default: 19. Determines the level of the puzzles sent to known peer Security Gateways. This attribute also determines the maximum puzzle level a Security Gateway is willing to solve.

ike_dos_puzzle_level_unidentified_initiator

Values: 0-32. Default: 19. Determines the level of the puzzles sent to unknown peers (such as SecuRemote/SecureClients and DAIP Security Gateways). This attribute also determines the maximum puzzle level that DAIP Security Gateways and SecuRemote/SecureClients are willing to solve.

ike_dos_max_puzzle_time_gw

Values: 0-30000. Default: 500. Determines the maximum time in milliseconds a Security Gateway is willing to spend solving a DoS protection puzzle.

ike_dos_max_puzzle_time_daip

Values: 0-30000. Default: 500. Determines the maximum time in milliseconds a DAIP Security Gateway is willing to spend solving a DoS protection puzzle.

ike_dos_max_puzzle_time_sr

Values: 0-30000. Default: 5000. Determines the maximum time in milliseconds a SecuRemote is willing to spend solving a DoS protection puzzle.

ike_dos_supported_protection_sr

Values: None, Stateless, Puzzles. Default: Puzzles. When downloaded to SecuRemote/SecureClient, it controls the level of protection the client is willing to support.

Security Gateways use the **ike_dos_protection_unidentified_initiator** property (equivalent to the SmartDashboard Global Property: **Support IKE DoS Protection from unidentified Source**) to decide what protection to require from remote clients, but SecuRemote/SecureClient clients use the **ike_dos_protection**. This same client property is called **ike_dos_supported_protection_sr** on the Security Gateway.

Protection After Successful Authentication

You can configure fields in GuiDBedit to protect against IKE DoS attacks from peers who may authenticate successfully and then attack a Security Gateway. These settings are configured in the Global Properties table and not per Security Gateway. By default these protections are off. Once you enter a value, they will be activated.

To limit the amount of IKE Security Associations (SA's) that a user can open, configure the following fields:

| Type of VPN | Field | Recommended Value |
|--------------|------------------------------------|-------------------|
| Site to site | number_of_ISAKMP_SAs_kept_per_peer | 5 |
| Remote user | number_of_ISAKMP_SAs_kept_per_user | 5 |

To limit the amount of tunnels that a user can open per IKE, configure the following fields:

| Type of VPN | Field | Recommended Value |
|--------------|-------------------------------------|-------------------|
| Site to site | number_of_ipsec_SAs_per_IKE_SA | 30 |
| Remote user | number_of_ipsec_SAs_per_user_IKE_SA | 5 |

Client Properties

Some Security Gateway properties change name when they are downloaded to SecuRemote/SecureClient. The modified name appears in the Userc.C file, as follows:

Property Names

| Property Name on Gateway | User.C Property name on Client |
|---|--|
| ike_dos_protection_unidentified_initiator (Equivalent to the SmartDashboard Global Property: Support IKE DoS Protection from unidentified Source) | ike_dos_protection or ike_support_dos_protection |
| ike_dos_supported_protection_sr | ike_dos_protection |
| ike_dos_puzzle_level_unidentified_initiator | ike_dos_acceptable_puzzle_level |
| ike_dos_max_puzzle_time_sr | ike_dos_max_puzzle_time |

Configuring Advanced IKE Properties

IKE is configured in two places:

- On the VPN community network object (for IKE properties).
- On the Security Gateway network object (for subnet key exchange).

On the VPN Community Network Object

1. From the **VPN Community Properties > Encryption** page, select:
 - **Encryption Method** - For IKE phase I and II.
 - **IKEv2 only** - Only support encryption using IKEv2. Security Gateways in this community cannot access peer gateways that support IKEv1 only.
 - **Prefer IKEv2, support IKEv1** - If a peer supports IKEv2, the Security Gateway will use IKEv2. If not, it will use IKEv1 encryption. This is recommended if you have a community of older and new Check Point Security Gateways.
 - **IKEv1 only** - IKEv2 is not supported.
 - **Encryption Suite** - The methods negotiated in IKE phase 2 and used in IPSec connections. Select the option for best interoperability with other vendors in your environment.
 - **VPN-A or VPN B** - See RFC 4308 for more information.
 - **Suite-B GCM-128 or 256** - See RFC 6379 for more information.
 - If you require algorithms other than those specified in the other options, select **Custom** and click **Advanced** to select properties for IKE Phase 1 and 2.
2. From the **VPN Community Properties > Advanced Settings > Advanced VPN Properties** page, select:
 - Which Diffie-Hellman group to use.
 - When to renegotiate the IKE Security Associations.
 - Whether to use **aggressive mode** (Main mode is the default).
 - Whether to use **Perfect Forward Secrecy**, and with which Diffie-Hellman group.
 - When to renegotiate the IPSec security associations.
 - Whether to use **Support IP compression**.
 - Whether to disable NAT inside the VPN community.

On the Gateway Network Object

- On the **VPN Advanced** page, select one of the options in the **VPN Tunnel Sharing** section. There are several settings for controlling the number of VPN tunnels between peer gateways:
 - **Use the community settings** - The number of VPN tunnels created follows the settings configured on the community's Tunnel Management page.
 - **Custom settings:**
 - **One VPN tunnel per each pair of hosts** - A VPN tunnel is created for every session initiated between every pair of hosts.
 - **One VPN tunnel per subnet pair** - Once a VPN tunnel has been opened between two subnets, subsequent sessions between the same subnets will share the same VPN tunnel. This is the default setting and is compliant with the IPSec industry standard.
 - **One VPN tunnel per Gateway pair** - One VPN tunnel is created between peer gateways and shared by all hosts behind each peer gateway.
- On the **Capacity Optimization** page, you can maximize VPN throughput by limiting the following connection parameters:
 - **Maximum concurrent IKE negotiations**
 - **Maximum concurrent runnels**

If you have many employees working remotely, you may want to raise the default values.

Chapter 3

Introduction to Site to Site VPN

In This Chapter

| | |
|---|----|
| The Need for Virtual Private Networks | 24 |
| Special Considerations for Planning a VPN Topology | 33 |
| Configuring Site to Site VPNs | 33 |
| Configuring a VPN with External Security Gateways Using PKI | 35 |
| Configuring a VPN with External Security Gateways Using a Pre-Shared Secret | 37 |
| How to Authorize Firewall Control Connections in VPN Communities | 38 |

The Need for Virtual Private Networks

Communicating parties need a connectivity platform that is not only fast, scalable, and resilient but also provides:

- Confidentiality
- Integrity
- Authentication

Confidentiality

Only the communicating parties must be able to read the private information exchanged between them.

Authentication

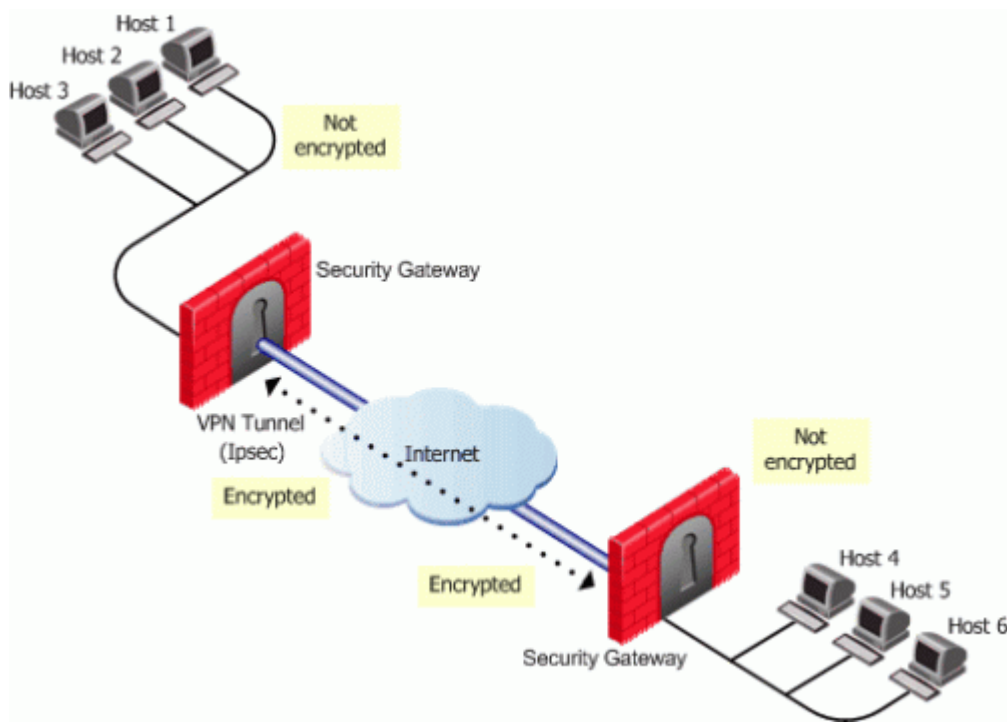
The communicating parties must be sure they are connecting with the intended party.

Integrity

The sensitive data passed between the communicating parties is unchanged, and this can be proved with an integrity check.

How it Works

In the Figure, host 1 and host 6 need to communicate. The connection passes in the clear between host 1 and the local Security Gateway. From the source and destination addresses of the packet, the Security Gateway determines that this should be an encrypted connection. If this is the first time the connection is made, the local Security Gateway initiates an IKE negotiation with the peer Security Gateway in front of host 6. During the negotiation, both Security Gateways authenticate each other, and agree on encryption methods and keys. After a successful IKE negotiation, a VPN tunnel is created. From now on, every packet that passes between the Security Gateways is encrypted according to the IPSec protocol. IKE supplies authenticity (Security Gateways are sure they are communicating with each other) and creates the foundation for IPSec. Once the tunnel is created, IPSec provides privacy (through encryption) and integrity (via one-way hash functions).



After a VPN tunnel has been established:

- A packet leaves the source host and reaches the Security Gateway.
- The Security Gateway encrypts the packet.
- The packet goes down the VPN tunnel to the second Security Gateway. In actual fact, the packets are standard IP packets passing through the Internet. However, because the packets are encrypted, they can be considered as passing through a private "virtual" tunnel.
- The second Security Gateway decrypts the packet.
- The packet is delivered in the clear to the destination host. From the hosts' perspectives, they are connecting directly.

For more information regarding the IKE negotiation, see: [IPSEC & IKE](#) (on page 13).

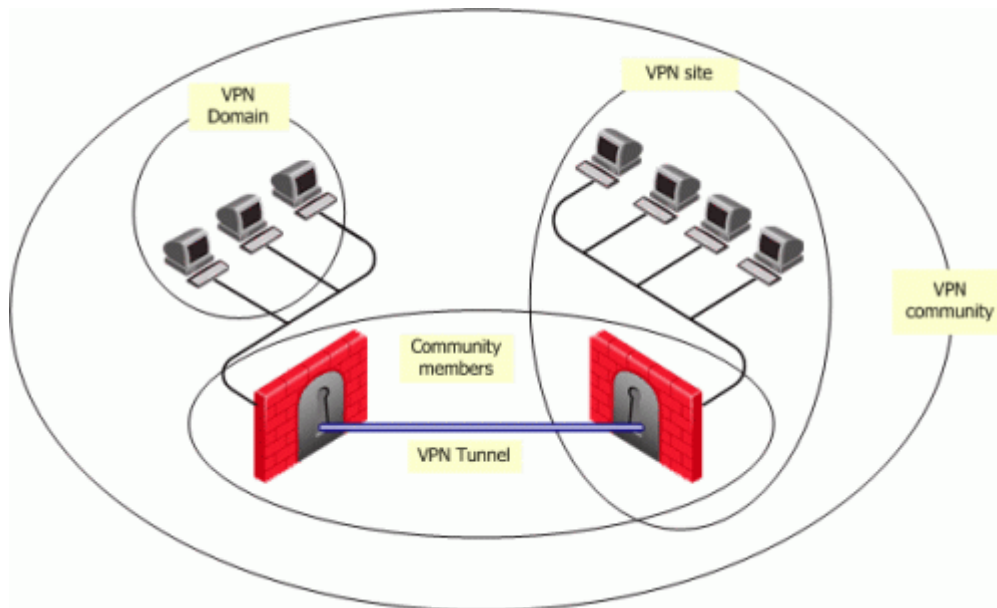
VPN Communities

Creating VPN tunnels between Security Gateways is made easier through the configuration of VPN communities. A VPN community is a collection of VPN enabled gateways capable of communicating via VPN tunnels.

To understand VPN Communities, a number of terms need to be defined:

- *VPN Community member*. Refers to the Security Gateway that resides at one end of a VPN tunnel.
- *VPN domain*. Refers to the hosts behind the Security Gateway. The VPN domain can be the whole network that lies behind the Security Gateway or just a section of that network. For example a Security Gateway might protect the corporate LAN and the DMZ. Only the corporate LAN needs to be defined as the VPN domain.

- *VPN Site.* Community member plus VPN domain. A typical VPN site would be the branch office of a bank.
- *VPN Community.* The collection of VPN tunnels/links and their attributes.
- *Domain Based VPN.* Routing VPN traffic based on the encryption domain behind each Security Gateway in the community. In a star community, satellite Security Gateways can communicate with each other through center Security Gateways.
- *Route Based VPN.* Traffic is routed within the VPN community based on the routing information, static or dynamic, configured on the Operating Systems of the Security Gateways.



The methods used for encryption and ensuring data integrity determine the type of tunnel created between the Security Gateways, which in turn is considered a characteristic of that particular VPN community.

A Security Management server can manage multiple VPN communities, which means communities can be created and organized according to specific needs.

Remote Access Community

A Remote Access Community is a type of VPN community created specifically for users that usually work from remote locations, outside of the corporate LAN. This type of community ensures secure communication between users and the corporate LAN. For more information, see: [Introduction to Remote Access VPN](#) (on page [143](#)).

Authentication Between Community Members

Before Security Gateways can exchange encryption keys and build VPN tunnels, they first need to authenticate to each other. Security Gateways authenticate to each other by presenting one of two types of "credentials":

- **Certificates.** Each Security Gateway presents a certificate which contains identifying information of the Security Gateway itself, and the Security Gateway's public key, both of which are signed by the trusted CA. For convenience, the Check Point product suite installs its own Internal CA that automatically issues certificates for all internally managed Security Gateways, requiring no configuration by the user. In addition, the Check Point Product Suite supports other PKI solutions. For more information, see: [Public Key Infrastructure](#) (on page [40](#)).
- **Pre-shared secret.** A pre-shared is defined for a pair of Security Gateways. Each Security Gateway proves that it knows the agreed upon pre-shared secret. The pre-shared secret can be a mixture of letters and numbers, a password of some kind.

Considered more secure, certificates are the preferred means. In addition, since the Internal CA on the Security Management server automatically provides a certificate to each Check Point Security Gateway it manages, it is more convenient to use this type of authentication.

However, if a VPN tunnel needs to be created with an externally managed Security Gateway (a gateway managed by a different Security Management server) the externally managed Security Gateway:

- Might support certificates, but certificates issued by an external CA, in which case both Security Gateways need to trust the other's CA. (For more information, see: [Configuring a VPN with External Security Gateways Using PKI](#) (on page 35).)
- May not support certificates; in which case, VPN supports the use of a "pre-shared secret." For more information, see: [Configuring a VPN with External Security Gateways Using a Pre-Shared Secret](#) (on page 37).

A "secret" is defined per external Security Gateway. If there are five internal Security Gateways and two externally managed Security Gateways, then there are two pre-shared secrets. The two pre-shared secrets are used by the five internally managed Security Gateways. In other words, all the internally managed Security Gateways use the same pre-shared secret when communicating with a particular externally managed Security Gateway.

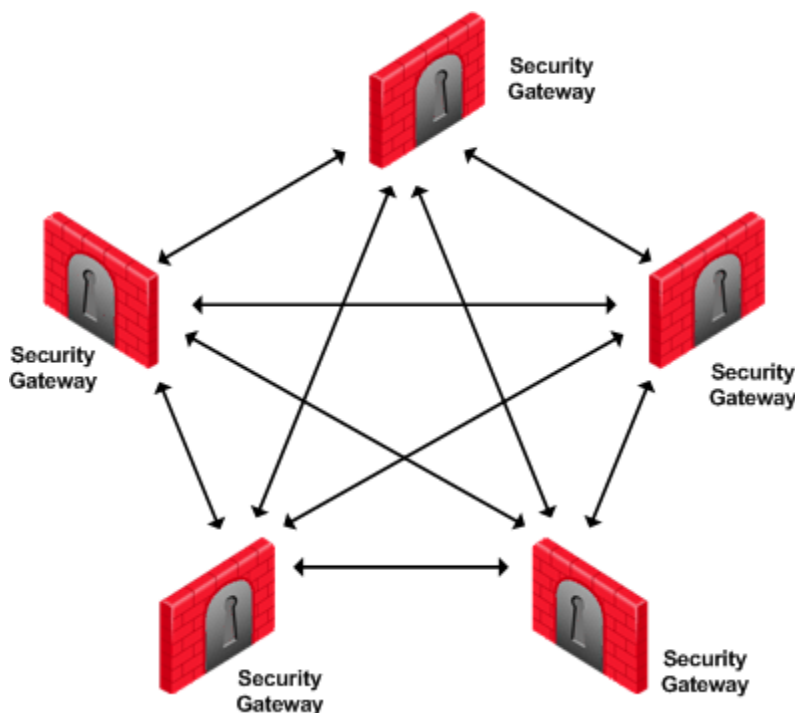
VPN Topologies

The most basic topology consists of two Security Gateways capable of creating a VPN tunnel between them. Security Management server's support of more complex topologies enables VPN communities to be created according to the particular needs of an organization. Security Management server supports two main VPN topologies:

- Meshed
- Star

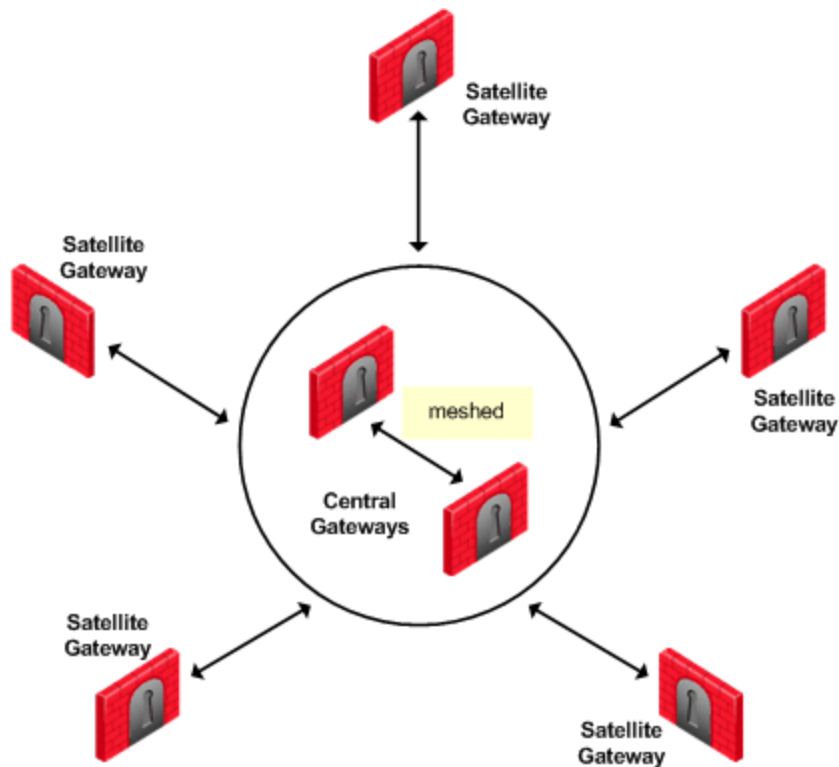
Meshed VPN Community

A Mesh is a VPN community in which a VPN site can create a VPN tunnel with any other VPN site in the community:



Star VPN Community

A star is a VPN community consisting of central Security Gateways (or "hubs") and satellite Security Gateways (or "spokes"). In this type of community, a satellite can create a tunnel only with other sites whose Security Gateways are defined as central.



A satellite Security Gateway cannot create a VPN tunnel with a Security Gateway that is also defined as a satellite Security Gateway.

Central Security Gateways can create VPN tunnels with other Central Security Gateways only if the **Mesh center Security Gateways** option has been selected on the **Central Security Gateways** page of the **Star Community Properties** window.

Dynamically Assigned IP Security Gateways

A Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway where the external interface's IP address is assigned dynamically by the ISP. Creating VPN tunnels with DAIP Security Gateways are only supported by using certificate authentication. Peer Security Gateways identify internally managed DAIP Security Gateways using the DN of the certificate. Peer Security Gateways identify externally managed DAIP Security Gateways and 3rd party DAIP Security Gateways using the *Matching Criteria* configuration.

DAIP Security Gateways may initiate a VPN tunnel with non-DAIP Security Gateways. However, since a DAIP Security Gateway's external IP address is always changing, peer Security Gateways cannot know in advance which IP address to use to connect to the DAIP Security Gateway. As a result, a peer Security Gateway cannot initiate a VPN tunnel with a DAIP Security Gateway unless DNS Resolving is configured on the DAIP Security Gateway. For more information, see Link Selection (on page 97).

If the IP on the DAIP Security Gateway changes during a session, it will renegotiate IKE using the newly assigned IP address.

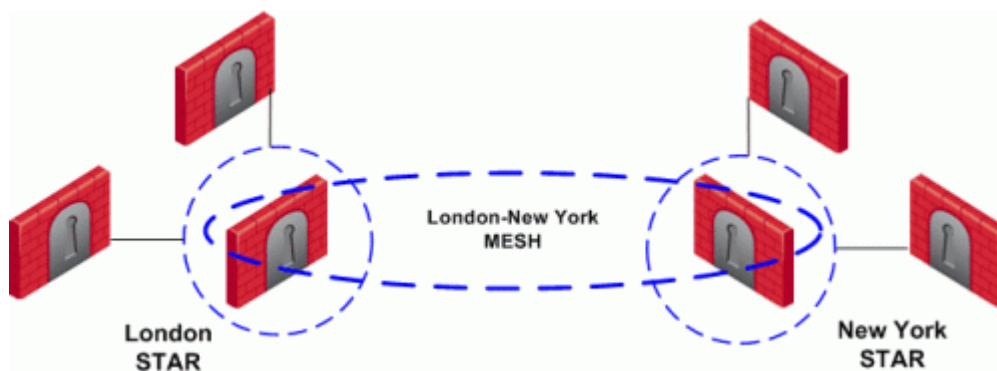
In a star community when VPN routing is configured, DAIP Security Gateways cannot initiate connections from their external IP through the center Security Gateway(s) to other DAIP Security Gateways or through the center to the Internet. In this configuration, connections from the encryption domain of the DAIP are supported.

Choosing a Topology

Which topology to choose for a VPN community depends on the overall policy of the organization. For example, a meshed community is usually appropriate for an Intranet in which only Security Gateways which are part of the internally managed network are allowed to participate; Security Gateways belonging to company partners are not.

A Star VPN community is usually appropriate when an organization needs to exchange information with networks belonging to external partners. These partners need to communicate with the organization but not with each other. The organization's Security Gateway is defined as a "central" Security Gateway; the partner Security Gateways are defined as "satellites."

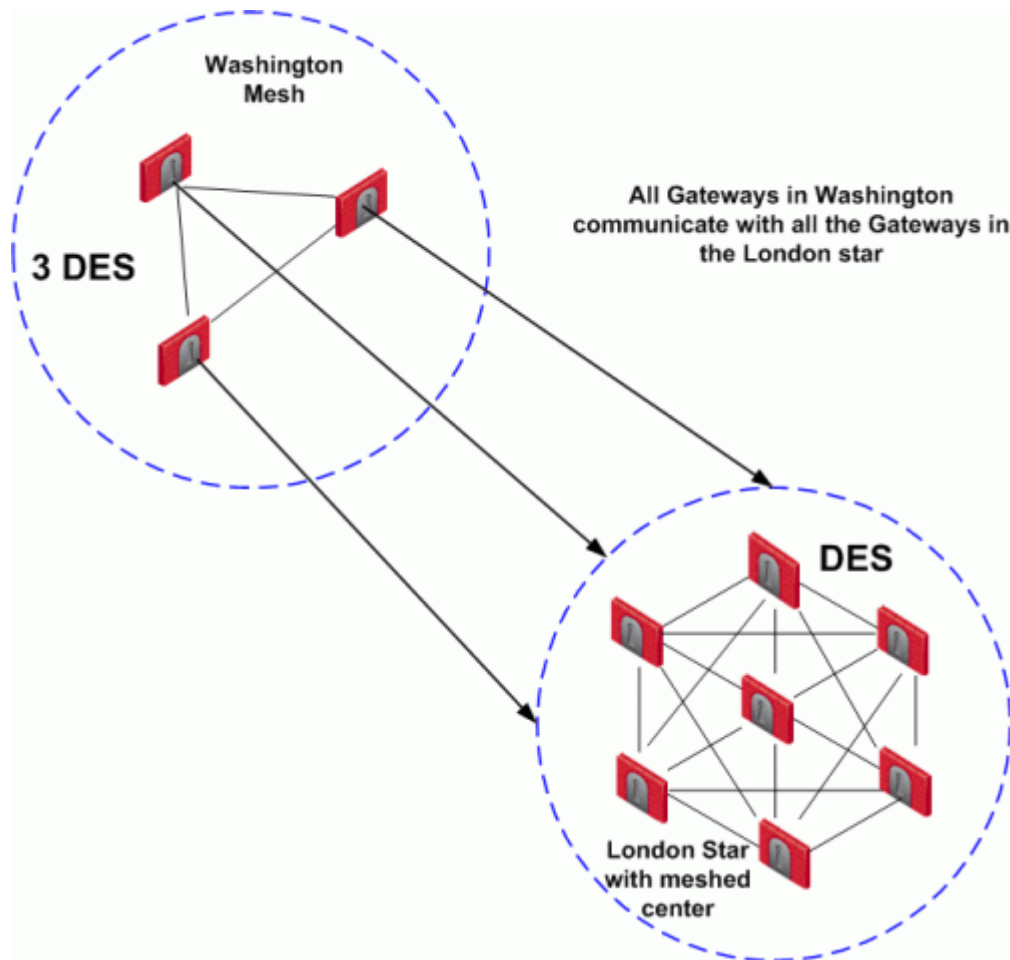
For more complex scenarios, consider a company with headquarters in two countries, London and New York. Each headquarters has a number of branch offices. The branch offices only need to communicate with the HQ in their country, not with each other; only the HQ's in New York and London need to communicate directly. To comply with this policy, define two star communities, London and New York. Configure the London and New York Security Gateways as "central" Security Gateways. Configure the Security Gateways of New York and London branch offices as "satellites." This allows the branch offices to communicate with the HQ in their country. Now create a third VPN community, a VPN mesh consisting of the London and New York Security Gateways.



Topology and Encryption Issues

Issues involving topology and encryption can arise as a result of an organization's policy on security, for example the country in which a branch of the organization resides may have a national policy regarding encryption strength. For example, policy says the Washington Security Gateways should communicate using 3DES for encryption. Policy also states the London Security Gateways must communicate uses DES as the encryption algorithm.

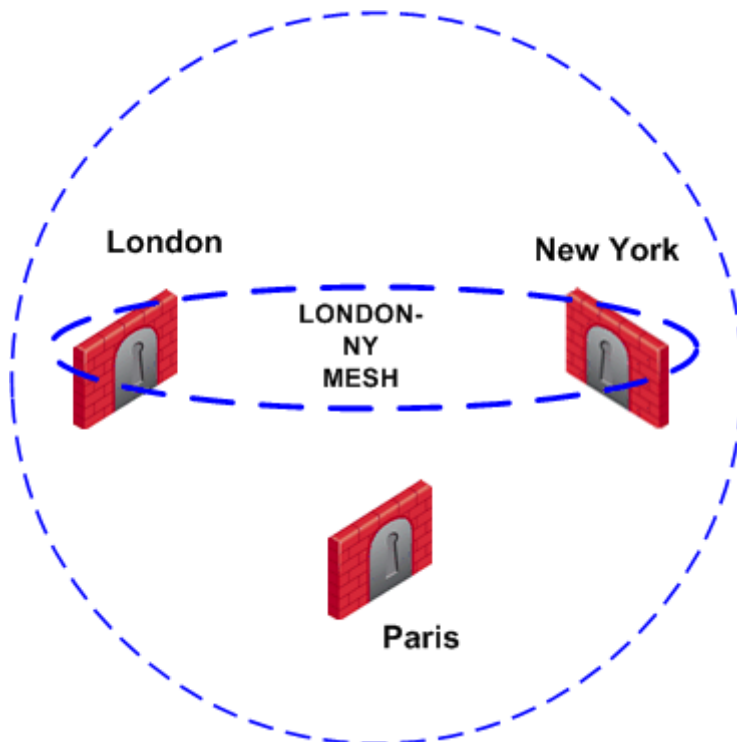
In addition, the Washington and London Security Gateways need to communicate with each other using the weaker DES. Consider the solution:



In this solution, Security Gateways in the Washington mesh are also defined as satellites in the London star. In the London star, the central Security Gateways are *meshed*. Security Gateways in Washington build VPN tunnels with the London Security Gateways using DES. Internally, the Washington Security Gateways build VPN tunnels using 3DES.

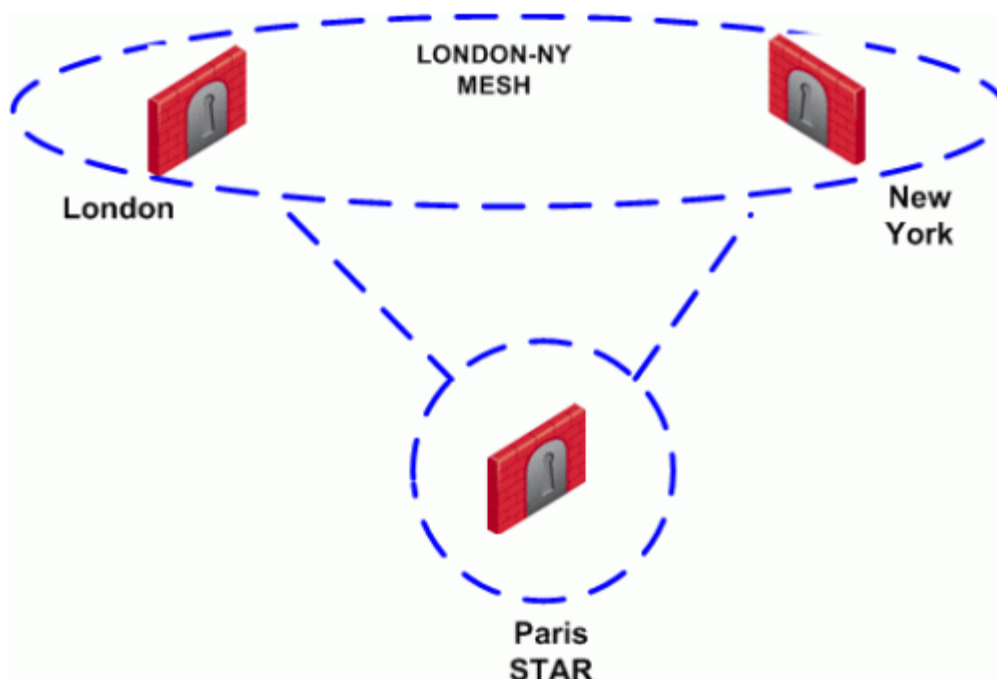
Special Condition for VPN Security Gateways

Individually, Security Gateways can appear in many VPN communities; however, two Security Gateways that can create a VPN link between them in one community cannot appear in another VPN community in which they can *also* create a link. For example:



The London and New York Security Gateways belong to the London-NY Mesh VPN community. To create an additional VPN community which includes London, New York, and Paris is not allowed. The London and New York Security Gateways cannot appear "together" in more than one VPN community.

Two Security Gateways that can create a VPN link between them in one community can appear in another VPN community provided that they are *incapable* of creating a link between them in the second community. For example:



London and New York Security Gateways appear in the London-NY mesh. These two Security Gateways also appear as Satellite Security Gateways in the Paris Star VPN community. In the Paris Star, satellite Security Gateways (London and NY) can *only* communicate with the central Paris Security Gateway. Since

the London and New York satellite Security Gateways *cannot* open a VPN link between them, this is a valid configuration.

Access Control and VPN Communities

Configuring Security Gateways into a VPN community does not create a de facto access control policy between the Security Gateways. The fact that two Security Gateways belong to the same VPN community does not mean the Security Gateways have access to each other.

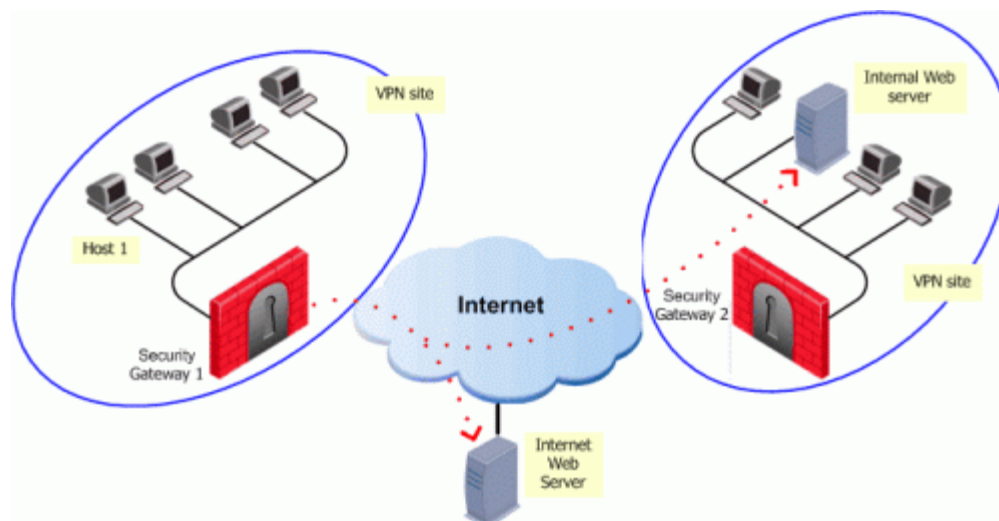
The configuration of the Security Gateways into a VPN community means that *if* these Security Gateways are allowed to communicate via an access control policy, then that communication is encrypted. Access control is configured in the Security Policy Rule Base.

Using the VPN column of the Security Policy Rule Base, it is possible to create access control rules that apply *only* to members of a VPN community, for example:

| Source | Destination | VPN | Service | Action |
|--------|-------------|-------------|---------|--------|
| Any | Any | Community_A | HTTP | Accept |

The connection is matched only if all the conditions of the rule are true, that is - it must be an HTTP connection between a source and destination IP address within VPN Community A. If any one of these conditions is not true, the rule is not matched. If all conditions of the rule are met, the rule is matched and the connection allowed.

It is also possible for a rule in the Security Policy Rule Base to be relevant for both VPN communities and host machines *not* in the community. For example:



The rule in the Security Policy Rule base allows an HTTP connection between any internal IP with any IP:

| Source | Destination | VPN | Service | Action |
|----------------------|-------------|-----|---------|--------|
| Any_internal_machine | Any | Any | HTTP | Accept |

A HTTP connection between host 1 and the Internal web server behind Security Gateway 2 matches this rule. A connection between the host 1 and the web server on the Internet also matches this rule; however, the connection between host 1 and the internal web server is a connection between members of a VPN community and passes encrypted; the connection between host 1 and the Internet web server passes in the clear.

In both cases, the connection is simply matched to the Security Policy Rule; whether or not the connection is encrypted is dealt with on the VPN level. *VPN is another level of security separate from the access control level.*

Accepting all Encrypted Traffic

If you select **Accept all encrypted traffic** on the **General** page of the VPN community **Properties** window, a new rule is added to the Security Policy Rule Base. This rule is neither a regular rule or an implied rule, but an *automatic community rule*, and can be distinguished by its "beige" colored background.

Routing Traffic within a VPN Community

VPN routing provides a way of controlling how VPN traffic is directed. There are two methods for VPN routing:

- Domain Based VPN
- Route Based VPN

Domain Based VPN

This method routes VPN traffic based on the encryption domain behind each Security Gateway in the community. In a star community, this allows satellite Security Gateways to communicate with each other through center Security Gateways. Configuration for Domain Based VPN is performed directly through SmartDashboard. For more information, see Domain Based VPN (on page 53).

Route Based VPN

Traffic is routed within the VPN community based on the routing information, static or dynamic, configured on the Operating Systems of the Security Gateways. For more information, see Route Based VPN (on page 61).



Note - If both Domain Based VPN and Route Based VPN are configured, then Domain Based VPN will take precedence.

Excluded Services

In the VPN **Communities Properties** window **Excluded Services** page, you can select services that are *not* to be encrypted, for example Firewall control connections. Services in the clear means "do not make a VPN tunnel for this connection". For further information regarding control connections, see: How to Authorize Firewall Control Connections in VPN Communities (on page 38). Note that *Excluded Services* is not supported when using *Route Based VPN*.

Special Considerations for Planning a VPN Topology

When planning a VPN topology it is important to ask a number of questions:

1. Who needs secure/private access?
2. From a VPN point of view, what will be the structure of the organization?
3. Internally managed Security Gateways authenticate each other using certificates, but how will externally managed Security Gateways authenticate?
 - Do these externally managed Security Gateways support PKI?
 - Which CA should be trusted?

Configuring Site to Site VPNs

VPN communities can be configured in either traditional or simplified mode. In *Traditional mode*, one of the actions available in the Security Policy Rule Base is **Encrypt**. When encrypt is selected, all traffic between the Security Gateways is encrypted. Check Point Security Gateways are more easily configured through the use of VPN communities — otherwise known as working in *Simplified Mode*. For more information regarding traditional mode, see: Traditional Mode VPNs (on page 130).

Migrating from Traditional Mode to Simplified Mode

To switch from Traditional mode to Simplified mode (For more information, see [Converting a Traditional Policy to a Community Based Policy](#) (on page 137)):

Select **Policy > Convert to > Simplified VPN**.

or

1. On the **Global Properties > VPN** page, select either **Simplified mode to all new Security Policies**, or **Traditional or Simplified per new Security Policy**. **File > Save**. If you do not save, you are prompted to do so. Click **OK**.
2. **File > New...** The **New Policy Package** window opens.
3. Create a name for the new security policy package and select **Firewall and Address Translation**.

In the Security Policy Rule base, a new column marked **VPN** appears and the **Encrypt** option is *no longer available* in the **Action** column. You are now working in Simplified Mode.

Configuring a Meshed Community Between Internally Managed Gateways

Internally managed VPN communities can use one of two possible topologies; meshed or star. To configure an internally managed VPN meshed community, create the Security Gateways and then add them to the community:

1. In the **Network Objects** tree, right click **Network Objects > New > Check Point > Security Gateway...** Select **Simple mode (wizard)** or **Classic mode**. The **Check Point Security Gateway properties** window opens.
 - a) On the **General Properties** page, after naming the object and supplying an IP address, select **VPN** and establish SIC communication.
 - b) On the **Topology** page, click **Add** to add interfaces. Once an interface appears in the table, clicking **Edit...** opens the **Interface Properties** window.
 - c) In the **Interface Properties** window, define the general properties of the interface and the topology of the network behind it.
 - d) On the **Topology** page, **VPN Domain** section, define the VPN domain as all the machines behind the Security Gateway based on the topology information or manually defined:
 - (i) As an address range.
 - (ii) As a network.
 - (iii) As a group that can be a combination of address ranges, networks, and even other groups.

(There are instances where the VPN domain is a group which contains only the Security Gateway itself, for example where the Security Gateway is acting as a backup to a primary Security Gateway in an MEP environment.)

The network Security Gateway objects are now configured, and need to be added to a VPN community.



Note - There is nothing to configure on the **VPN** page, regarding certificates, since internally managed Security Gateways automatically receive a certificate from the internal CA.

2. On the **Network objects** tree, select the **VPN Communities** tab.
 - a) Right-click **Site to Site**.
 - b) From the short-cut menu, select **New Site To Site... > Meshed**. The **Meshed Communities Properties** window opens.
 - c) On the **General** page, select **Accept all encrypted traffic** if you need all traffic between the Security Gateways to be encrypted. If not, then create appropriate rules in the Security Policy Rule Base that allows encrypted traffic between community members.
 - d) On the **Participating Security Gateways** page, add the Security Gateways created in step 1.

A VPN tunnel is now configured. For more information on other options, such as **VPN Properties**, **Advanced Properties**, and **Shared Secret**, see: IPSEC & IKE (on page 13)

- If you did not select **Accept all encrypted traffic** in the community, build an access control policy, for example:

| Source | Destination | VPN | Service | Action |
|--------|-------------|------------------|---------|--------|
| Any | Any | Meshed community | Any | Accept |

Where "Meshed community" is the VPN community you have just defined.

Configuring a Star VPN Community

A star VPN community is configured in much the same way as a meshed community, the difference being the options presented on the **Star Community Properties** window:

- On the **General > Advanced Settings > VPN Routing** page, select **To center only**.
- On the **Central Security Gateways** page, **Add...** the central Security Gateways.
- On the **Central Security Gateways** page, select **Mesh central Security Gateways** if you want the central Security Gateways to communicate.
- On the **Satellite Security Gateways** page, click **Add...** to add the satellite Security Gateways.

Confirming a VPN Tunnel Successfully Opens

To make sure that a VPN tunnel has successfully opened:

- Edit the VPN rule and Select **log** as the tracking option.
- Open the applicable connection.
- Open SmartView Tracker and examine the logs. A successful connection appears as encrypted.

Configuring a VPN with External Security Gateways Using PKI

Configuring a VPN with external Security Gateways (those managed by a different Security Management server) is more involved than configuring a VPN with internal Security Gateways (managed by the same Security Management server). This is because:

- Configuration is performed separately in two distinct systems.
- All details must be agreed and coordinated between the administrators. Details such as the IP address or the VPN domain topology cannot be detected automatically but have to be supplied manually by the administrator of the peer VPN Security Gateways.
- The gateways are likely to be using different Certificate Authorities (CAs). Even if the peer VPN Security Gateways use the Internal CA (ICA), it is still a different CA.

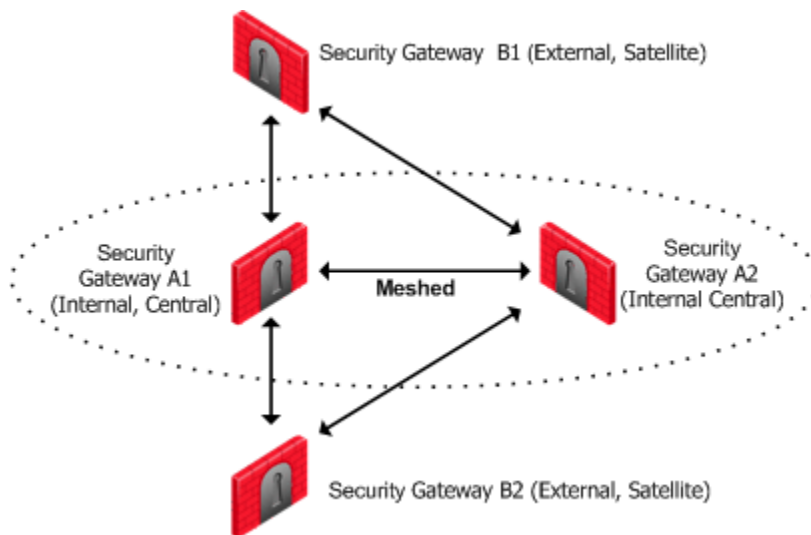
There are various scenarios when dealing with externally managed Security Gateways. The following description tries to address typical cases and assumes that the peers work with certificates. If this is not the case refer to Configuring a VPN with External Security Gateways Using a Pre-Shared Secret (on page 37).



Note - Configuring a VPN using PKI and certificates is more secure than using pre-shared secrets.

Although an administrator may choose which community type to use, the Star Community is more natural for a VPN with externally managed Security Gateways. The Internal Security Gateways will be defined as the central Security Gateways while the external ones will be defined as the satellites. The decision whether to mesh the central, internal Security Gateways or not depends on the requirements of the organization. The diagram below shows this typical topology.

Note that this is the Topology from the point of view of the administrator of Security Gateways A1 and A2. The Administrator of Security Gateways B1 and B2 may well also define a Star Topology, but with B1 and B2 as his central Security Gateways, and A1 and A2 as satellites.



The configuration instructions require an understanding of how to build a VPN. The details can be found in: Introduction to Site to Site VPN (on page 24).

You also need to understand how to configure PKI. See Public Key Infrastructure (on page 40).

To configure VPN using certificates, with the external Security Gateways as satellites in a star VPN Community:

1. Obtain the certificate of the CA that issued the certificate for the peer VPN Security Gateways, from the peer administrator. If the peer Security Gateway is using the ICA, you can obtain the CA certificate using a web browser from:

http://<IP address of peer Security Gateway or Management Server>:18264

2. In SmartDashboard, define the CA object for the CA that issued the certificate for the peer. See Enrolling with a Certificate Authority (on page 44).
3. Define the CA that will issue certificates for your side if the Certificate issued by ICA is not appropriate for the required VPN tunnel.

You may have to export the CA certificate and supply it to the peer administrator.

4. Define the Network Object(s) of the Security Gateway(s) that are internally managed. In particular, be sure to do the following:
 - In the **General Properties** page of the Security Gateway object, select **VPN**.
 - In the **Topology** page, define the **Topology**, and the **VPN Domain**. If the VPN Domain does not contain all the IP addresses behind the Security Gateway, define the VPN domain manually by defining a group or network of machines and setting them as the VPN Domain.
5. If the ICA certificate is not appropriate for this VPN tunnel, then in the **VPN** page, generate a certificate from the relevant CA (see Enrolling with a Certificate Authority (on page 44).)
6. Define the Network Object(s) of the externally managed Security Gateway(s).

- If it is not a Check Point Security Gateway, define an Interoperable Device object from: **Manage > Network Objects... > New... > Interoperable Device...**
- If it is a Check Point Security Gateway, In the **Network Objects** tree, right click and select **New > Check Point > Externally Managed Security Gateway....**

7. Set the various attributes of the peer Security Gateway. In particular, be sure to do the following:
 - In the **General Properties** page of the Security Gateway object, select **VPN** (for an Externally Managed Check Point Security Gateway object only).
 - in the **Topology** page, define the **Topology** and the **VPN Domain** using the VPN Domain information obtained from the peer administrator. If the VPN Domain does not contain all the IP addresses behind the Security Gateway, define the VPN domain manually by defining a group or network of machines and setting them as the VPN Domain.
 - In the **VPN** page, define the **Matching Criteria**. specify that the peer must present a certificate signed by its own CA. If feasible, enforce details that appear in the certificate as well.
8. Define the Community. The following details assume that a Star Community was chosen, but a Meshed Community is an option as well. If working with a Meshed community, ignore the difference between the Central Security Gateways and the Satellite Security Gateways.

- Agree with the peer administrator about the various IKE properties and set them in the **VPN Properties** page and the **Advanced Properties** page of the community object.
 - Define the Central Security Gateways. These will usually be the internally managed ones. If there is no another Community defined for them, decide whether or not to mesh the central Security Gateways. If they are already in a Community, do not mesh the central Security Gateways.
 - Define the Satellite Security Gateways. These will usually be the external ones.
9. Define the relevant access rules in the Security Policy. Add the Community in the **VPN** column, the services in the **Service** column, the desired **Action**, and the appropriate **Track** option.
 10. Install the Security Policy.

Configuring a VPN with External Security Gateways Using a Pre-Shared Secret

Configuring VPN with external Security Gateways (those managed by a different Security Management server) is more involved than configuring VPN with internal Security Gateways (managed by the same Security Management server) because:

- Configuration is done separately in two distinct systems.
- All details must be agreed and coordinated between the administrators. Details such as the IP address or the VPN domain topology cannot be detected automatically but have to be supplied manually by the administrator of the peer VPN Security Gateways.

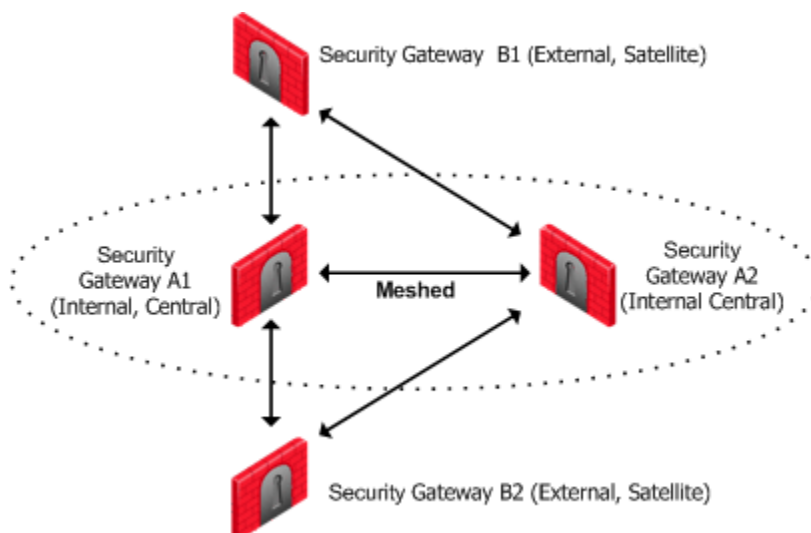
There are various scenarios when dealing with externally managed Security Gateways. The following description tries to address typical cases but assumes that the peers work with pre-shared secrets. If this is not the case refer to Configuring a VPN with External Security Gateways Using PKI (on page 35).



Note - Configuring a VPN using PKI and certificates is considered more secure than using pre-shared secrets.

Although an administrator may choose which community type to use, the Star Community is more natural for a VPN with externally managed Security Gateways. The Internal Security Gateways will be defined as the central Security Gateways while the external ones will be defined as the satellites. The decision whether to mesh the central, internal Security Gateways or not depends on the requirements of the organization. The diagram below shows this typical topology.

Note that this is the Topology from the point of view of the administrator of Security Gateways A1 and A2. The administrator of Security Gateways B1 and B2 may well also define a Star Topology, but with B1 and B2 as his central Security Gateways, and A1 and A2 as satellites.



The configuration instructions require an understanding of how to build a VPN. The details can be found in: Introduction to Site to Site VPN (on page 24).

To configure a VPN using pre-shared secrets, with the external Security Gateways as satellites in a star VPN Community, proceed as follows:

1. Define the Network Object(s) of the Security Gateway(s) that are internally managed. In particular, be sure to do the following:
 - In the **General Properties** page of the Security Gateway object, select **VPN**.
 - In the **Topology** page, define the **Topology**, and the **VPN Domain**. If the VPN Domain does not contain all the IP addresses behind the Security Gateway, define the VPN domain manually by defining a group or network of machines and setting them as the VPN Domain.
2. Define the Network Object(s) of the externally managed Security Gateway(s).
 - If it is not a Check Point Security Gateway, define an Interoperable Device object from: **Manage > Network Objects... > New... > Interoperable Device...**
 - If it is a Check Point Security Gateway, In the **Network Objects** tree, right click and select **New > Check Point > Externally Managed Security Gateway....**
3. Set the various attributes of the peer Security Gateway. In particular, be sure to do the following:
 - In the **General Properties** page of the Security Gateway object, select **VPN** (for an Externally Managed Check Point Security Gateway object only).
 - in the **Topology** page, define the **Topology** and the **VPN Domain** using the VPN Domain information obtained from the peer administrator. If the VPN Domain does not contain all the IP addresses behind the Security Gateway, define the VPN domain manually by defining a group or network of machines and setting them as the VPN Domain.
4. Define the Community. The following details assume that a Star Community was chosen, but a Meshed Community is an option as well. If working with a Mesh community, ignore the difference between the Central Security Gateways and the Satellite Security Gateways.
 - Agree with the peer administrator about the various IKE properties and set them in the **VPN Properties** page and the **Advanced Properties** page of the community object.
 - Define the Central Security Gateways. These will usually be the internally managed ones. If there is no another Community defined for them, decide whether or not to mesh the central Security Gateways. If they are already in a Community, do not mesh the central Security Gateways.
 - Define the Satellite Security Gateways. These will usually be the external ones.
5. Agree on a pre-shared secret with the administrator of the external Community members. Then, in the **Shared Secret** page of the community, select **Use Only Shared Secret for all External Members**. For each external peer, enter the pre-shared secret.
6. Define the relevant access rules in the Security Policy. Add the Community in the **VPN** column, the services in the **Service** column, the desired **Action**, and the appropriate **Track** option.
7. Install the Security Policy.

How to Authorize Firewall Control Connections in VPN Communities

Check Point Nodes communicate with other Check Point Nodes by means of control connections. For example, a control connection is used when the Security Policy is installed from the Security Management server to a Security Gateway. Also, logs are sent from Security Gateways to the Security Management server across control connections. Control connections use Secure Internal Communication (SIC).

Control connections are allowed using Implied Rules in the Security Rule Base. Implied Rules are added to or removed from the Security Rule Base, by selecting or clearing options in the **Firewall Implied Rules** page of the SmartDashboard Global Properties.

Some administrators prefer not to rely on implied rules, and instead prefer to define explicit rules in the Security Rule Base.

Why Turning off FireWall Implied Rules Blocks Control Connections

If you turn off implicit rules, you may not be able to install a Policy on a remote Security Gateway. Even if you define explicit rules in place of the implied rules, you may still not be able to install the policy:



The administrator wishes to configure a VPN between Security Gateways A and B by configuring SmartDashboard. To do this, the administrator must install a Policy from the Security Management server to the Security Gateways.

1. The Security Management server successfully installs the Policy on Security Gateway A. As far as gateway A is concerned, Security Gateways A and B now belong to the same VPN Community. However, B does not yet have this Policy.
2. The Security Management server tries to open a connection to Security Gateway B in order to install the Policy.
3. Security Gateway A allows the connection because of the explicit rules allowing the control connections, and starts IKE negotiation with Security Gateway B to build a VPN tunnel for the control connection.
4. Security Gateway B does not know how to negotiate with A because it does not yet have the Policy. Therefore Policy installation on Security Gateway B fails.

The solution for this is to make sure that control connections do not have to pass through a VPN tunnel.

Allowing Firewall Control Connections Inside a VPN

If you turn off implied rules, you must make sure that control connections are not changed by the Security Gateways. To do this, add the services that are used for control connections to the **Excluded Services** page of the Community object.



Note - Although control connections between the Security Management server and the Security Gateway are not encrypted by the community, they are nevertheless encrypted and authenticated using Secure Internal Communication (SIC).

Discovering Which Services are Used for Control Connections

1. In the main menu, select **View > Implied Rules**.
2. In the Global Properties **FireWall** page, verify that 'control connections' are accepted.
3. Examine the Security Rule Base to see what Implied Rules are visible. Note the services used in the Implied Rules.

Chapter 4

Public Key Infrastructure

In This Chapter

| | |
|---|----|
| Need for Integration with Different PKI Solutions | 40 |
| Supporting a Wide Variety of PKI Solutions | 40 |
| Special Considerations for PKI | 47 |
| Configuration of PKI Operations | 47 |
| Configuring OCSP | 51 |

Need for Integration with Different PKI Solutions

X.509-based PKI solutions provide the infrastructure that enables entities to establish trust relationships between each other based on their mutual trust of the Certificate Authority (CA). The trusted CA issues a certificate for an entity, which includes the entity's public key. Peer entities that trust the CA can trust the certificate — because they can verify the CA's signature — and rely on the information in the certificate, the most important of which is the association of the entity with the public key.

IKE standards recommend the use of PKI in VPN environments, where strong authentication is required.

A Security Gateway taking part in VPN tunnel establishment must have an RSA key pair and a certificate issued by a trusted CA. The certificate contains details about the module's identity, its public key, CRL retrieval details, and is signed by the CA.

When two entities try to establish a VPN tunnel, each side supplies its peer with random information signed by its private key and with the certificate that contains the public key. The certificate enables the establishment of a trust relationship between the Security Gateways; each gateway uses the peer Security Gateway's public key to verify the source of the signed information and the CA's public key to validate the certificate's authenticity. In other words, the validated certificate is used to authenticate the peer.

Every deployment of Check Point Security Management server includes an Internal Certificate Authority (ICA) that issues VPN certificates for the VPN modules it manages. These VPN certificates simplify the definition of VPNs between these modules.

Situations can arise when integration with other PKI solutions is required, for example:

- A VPN must be established with a Security Gateway managed by an external Security Management server. For example, the peer Security Gateway belongs to another organization which utilizes Check Point products, and its certificate is signed by its own Security Management server's ICA.
- A VPN must be established with a non-Check Point VPN entity. In this case, the peer's certificate is signed by a third-party CA.
- An organization may decide, for whatever reason, to use a third party CA to generate certificates for its Security Gateways.

Supporting a Wide Variety of PKI Solutions

Check Point Security Gateways support many different scenarios for integrating PKI in VPN environments.

- **Multiple CA Support for Single VPN Tunnel** – Two Security Gateways present a certificate signed by different ICAs.
- **Support for non-ICA CAs** – In addition to ICA, Security Gateways support the following Certificate Authorities:
 - External ICA - The ICA of another Security Management server

- Other OPSEC certified PKI solutions
- **CA Hierarchy** – CAs are typically arranged in a hierarchical structure where multiple CAs are subordinate to a root authority CA. A subordinate CA is a Certificate Authority certified by another Certificate Authority. Subordinate CA's can issue certificates to other, more subordinate CAs, forming a certification chain or hierarchy.

PKI and Remote Access Users

The Check Point Suite supports certificates not only for Security Gateways but for users as well. For more information, see Introduction to Remote Access VPN for information about user certificates.

PKI Deployments and VPN

Following are some sample CA deployments:

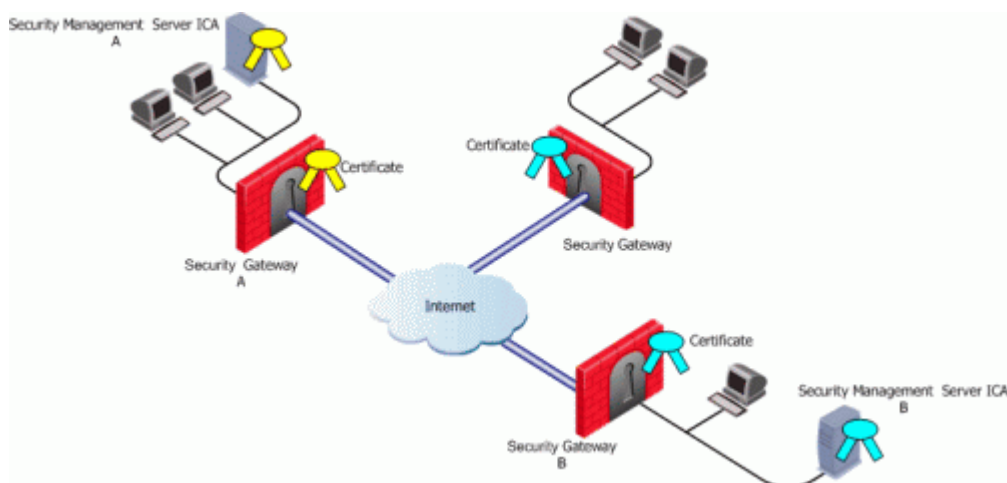
- Simple Deployment - internal CA
- CA of an external Security Management server
- CA services provided over the Internet
- CA on the LAN

Simple Deployment – Internal CA

When the VPN tunnel is established between Security Gateways managed by the same Security Management server, each peer has a certificate issued by the Security Management server's ICA.

CA of An External Security Management Server

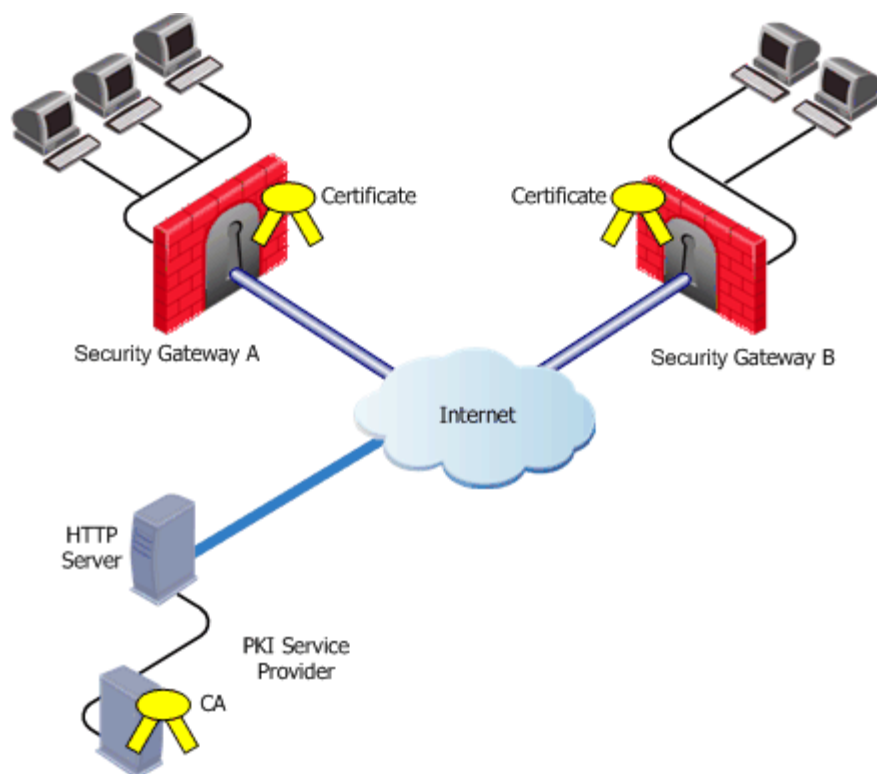
If a Check Point Security Gateway is managed by an external Security Management Server (for example, when establishing a VPN tunnel with another organization's VPN modules), each peer has a certificate signed by its own Security Management server's ICA.



Security Management Server A issues certificates for Security Management Server B that issues certificates for Security Gateway B.

CA Services Over the Internet

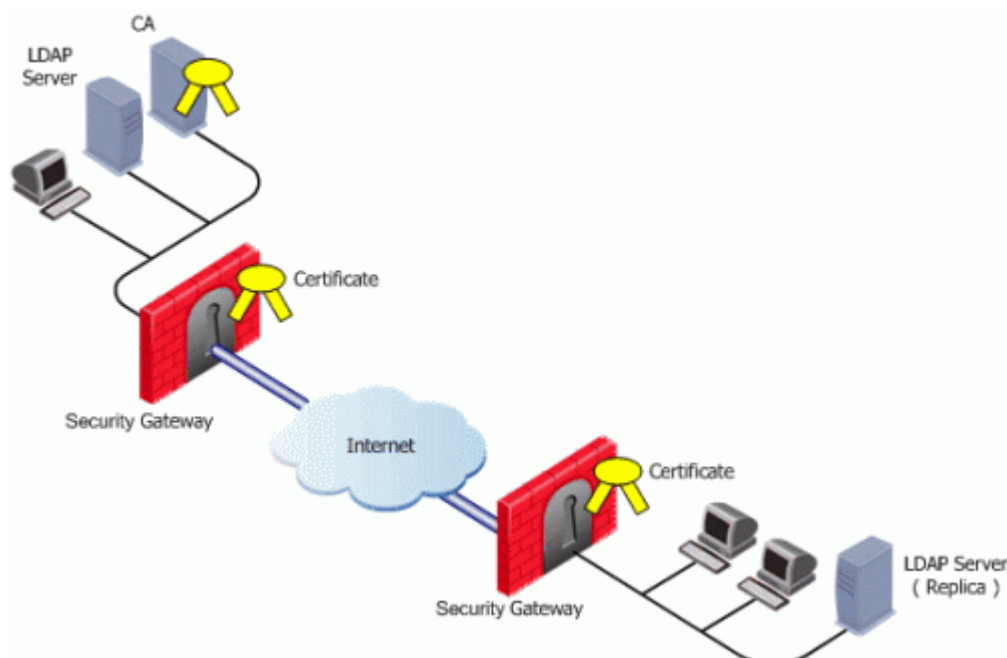
If the certificate of a Security Gateway is issued by a third party CA accessible over the Internet, CA operations such as registration or revocation are usually performed through HTTP forms. CRLs are retrieved from an HTTP server functioning as a CRL repository.



Security Gateways A and B receive their certificates from a PKI service provider accessible via the web. Certificates issued by external CA's may be used by Security Gateways managed by the same Security Management server to verification.

CA Located on the LAN

If the peer VPN Security Gateway's certificate is issued by a third party CA on the LAN, the CRL is usually retrieved from an internal LDAP server, as shown:



Trusting An External CA

A trust relationship is a crucial prerequisite for establishing a VPN tunnel. However, a trust relationship is possible only if the CA that signs the peer's certificate is "trusted." Trusting a CA means obtaining and validating the CA's own certificate. Once the CA's Certificate has been validated, the details on the CA's certificate and its public key can be used to both obtain and validate other certificates issued by the CA.

The Internal CA (ICA) is automatically trusted by all modules managed by the Security Management server that employs it. External CAs (even the ICA of another Check Point Security Management server) are not automatically trusted, so a module must first obtain and validate an external CA's certificate. The external CA must provide a way for its certificate to be imported into the Security Management server.

If the external CA is:

- The ICA of an external Security Management server, see the *R75.40 Security Management Server Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk67581>) for further information
- An OPSEC Certified CA, use the CA options on the **Servers and OSPEC Applications** tab to define the CA and obtain its certificate

Subordinate Certificate Authorities

A subordinate CA is a Certificate Authority certified by another Certificate Authority. Subordinate CAs can issue certificates to other, more subordinate CAs, in this way forming a certification chain or hierarchy. The CA at the top of the hierarchy is the root authority or root CA. Child Certificate Authorities of the root CA are referred to as Subordinate Certificate Authorities.

With the CA options on the **Servers and OSPEC Applications** tab, you can define either a Certificate Authority as either Trusted or Subordinate. Subordinate CAs are of the type OPSEC, and not trusted.

Enrolling a Managed Entity

Enrollment means obtaining a certificate from a CA, that is, requesting that the CA issue a certificate for an entity.

The process of enrollment begins with the generation of a key pair. A certificate request is then created out of the public key and additional information about the module. The type of the certificate request and the rest of the enrollment process depends on the CA type.

The case of an internally managed Security Gateway is the simplest, because the ICA is located on the Security Management server machine. The enrollment process is completed automatically.

To obtain a certificate from an OPSEC Certified CA, Security Management server takes the module details and the public key and encodes a PKCS#10 request. The request (which can include *SubjectAltName* for OPSEC certificates and Extended Key Usage extensions) is delivered to the CA manually by the administrator. Once the CA issues the certificate the administrator can complete the process by importing the certificate to the Security Management server.

A certificate can also be obtained for the Security Gateway using Automatic Enrollment. With Automatic Enrollment, you can automatically issue a request for a certificate from a trusted CA for any Security Gateway in the community. Automatic Enrollment supports the following protocols:

- **SCEP**
- **CMPV1**
- **CMPV2**



Note - During SCEP enrollment, some HTTP requests may be larger than 2K, and may be dropped by the HTTP protocol inspection mechanism if enabled (**Web Intelligence > HTTP Protocol Inspection > HTTP Format Sizes**). A change of the default value will be required to enable these HTTP requests. If enrollment still fails, enrollment must be done manually. For more information, see the *R75.40 IPS Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk67581>).

Validation of a Certificate

When an entity receives a certificate from another entity, it must:

1. Verify the certificate signature, i.e. verify that the certificate was signed by a trusted CA. If the certificate is not signed directly by a trusted CA, but rather by a subsidiary of a trusted CA, the path of CA certificates is verified up to the trusted CA.
2. Verify that the certificate chain has not expired.
3. Verify that the certificate chain is not revoked. A CRL is retrieved to confirm that the serial number of the validated certificate is not included among the revoked certificates.

In addition, VPN verifies the validity of the certificate's use in the given situation, confirming that:

- The certificate is authorized to perform the required action. For example, if the private key is needed to sign data (e.g., for authentication) the **KeyUsage** extension on the certificate – if present – is checked to see if this action is permitted.
- The peer used the correct certificate in the negotiation. When creating a VPN tunnel with an externally managed module, the administrator may decide that only a certificate signed by a specific CA from among the trusted CAs can be accepted. (Acceptance of certificates with specific details such as a *Distinguished Name* is possible as well).

Revocation Checking

There are two available methods useful in determining the status of a certificate:

1. CRL
2. Online Certificate Status Protocol (OCSP)

Enrolling with a Certificate Authority

A certificate is automatically issued by the ICA for all internally managed entities that are VPN capable. That is, after the administrator has checked the **VPN** option in the **Check Point Products** area of a network objects **General Properties** tab.

The process for obtaining a certificate from an OPSEC PKI or External Check Point CA is identical.

Manual Enrollment with OPSEC Certified PKI

To create a PKCS#10 Certificate Request:

1. Create the CA object, as described in Trusting an OPSEC Certified CA (on page 48).
2. Open the **VPN** tab of the relevant Network Object.
3. In the **Certificate List** field click **Add...**
The **Certificate Properties** window is displayed.
4. Enter the **Certificate Nickname**
The nickname is only an identifier and has no bearing on the content of the certificate.
5. From the **CA to enroll from** drop-down box, select the direct OPSEC CA/External CheckPoint CA that will issue the certificate.



Note - The list displays only those subordinate CA's that lead directly to a trusted CA and the trusted CAs themselves. If the CA that issues the certificate is a subordinate CA that does not lead directly to a trusted CA, the subordinate CA will not appear in the list.

6. Choose the appropriate method for Key Pair creation and storage. See Distributed Key Management and Storage for more information (see "[Distributed Key Management and Storage](#)" on page 47).
7. Click **Generate...**
The **Generate Certificate Properties** window is displayed.
8. Enter the appropriate DN.
The final DN that appears in the certificate is decided by the CA administrator.
If a **Subject Alternate Name** extension is required in the certificate, check the **Define Alternate Name** check box.

Adding the object IP as Alternate name extension can be configured as a default setting by selecting in **Global Properties > SmartDashboard Customization > Configure > Certificates and PKI properties**, the options:

add_ip_alt_name_for_opsec_certs

add_ip_alt_name_for_ICA_certs

The configuration in this step is also applicable for Internal CA's.

9. Click **OK**.

The public key and the DN are then used to DER-encode a PKCS#10 Certificate Request.

10. Once the Certificate Request is ready, click **View...**

The **Certificate Request View** window appears with the encoding.

11. Copy the whole text in the window and deliver it to the CA.

The CA administrator must now complete the task of issuing the certificate. Different CAs provide different ways of doing this, such as an advanced enrollment form (as opposed to the regular form for users). The issued certificate may be delivered in various ways, for example email. Once the certificate has arrived, it needs to be stored:

- a) Go to the **Severs and OPSEC Applications** tab of the network object, select the appropriate CA object.
- b) Open the OPEC PKI tab, click **Get...** and browse to the location in which the certificate was saved.
- c) Select the appropriate file and verify the certificate details.
- d) Close object and save.

Automatic Enrollment with the Certificate Authority

On the OPSEC PKI tab of the CA object, make sure **Automatically enroll certificate** is selected and SCEP or CMP are chosen as the connecting protocol. Then:

1. On the relevant network object, open the **VPN** tab.
2. In the **Certificates List** section, click **Add...**
The **Certificate Properties** window opens.
3. Enter a **Certificate Nickname** (any string used as an identifier)
4. From the drop-down menu, select the CA that issues the certificate.



Note - The menu shows only trusted CAs and subordinate CAs that lead directly to a trusted CA. If the CA that issues the certificate is a subordinate CA that does not lead directly to a trusted CA, it is not in the menu.

5. Select a method for key pair generation and storage.
6. Click **Generate**, and select **Automatic enrollment**.
The **Generate Keys and Get Automatic Enrollment Certificate** window opens.
 - Supply the **Key Identifier** and your secret **authorization code**.
 - Click **OK**.
7. When the certificate appears in the **Certificates List** on the network objects VPN page, click **View** and either **Copy to Clipboard** or **Save to File** the text in the **Certificate Request View** window.
8. Send the request to CA administrator.
Different Certificate Authorities provide different means for doing this, for example an advanced enrollment form on their website. The issued certificate can be delivered in various ways, such as email. Once you have received the certificate, save it to disk.
9. On the **VPN** tab of the network object, select the appropriate certificate in the **Certificates List**, and click **Complete...**
10. Browse to the folder where you stored the issued certificate, select the certificate and verify the certificate details.
11. Close the network object and **Save**.

Enrolling through a Subordinate CA

When enrolling through a subordinate CA:

- Supply the password of the subordinate CA which issues the certificate, not the CA at the top of the hierarchy
- The subordinate CA must lead directly to a trusted CA

CRL

VPN can retrieve the CRL from either an HTTP server or an LDAP server. If the CRL repository is an HTTP server, the module uses the URL published in the CRL **Distribution Point** extension on the certificate and opens an HTTP connection to the CRL repository to retrieve the CRL.

If the CRL repository is an LDAP server, VPN attempts to locate the CRL in one of the defined LDAP account units. In this scenario, an LDAP account unit must be defined. If the CRL **Distribution Point** extension exists, it publishes the DN of the CRL, namely, the entry in the Directory under which the CRL is published or the LDAP URI. If the extension does not exist, VPN attempts to locate the CRL in the entry of the CA itself in the LDAP server.

OCSP

Online Certificate Status Protocol (OCSP) enables applications to identify the state of a certificate. OCSP may be used for more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. When OCSP client issues a status request to an OCSP server, acceptance of the certificate in question is suspended until the server provides a response.

In order to use OCSP, the root CA must be configured to use this method instead of CRL. This setting is inherited by the subordinate CA's.

CRL Prefetch-Cache

Since the retrieval of CRL can take a long time (in comparison to the entire IKE negotiation process), VPN stores the CRLs in a CRL cache so that later IKE negotiations do not require repeated CRL retrievals.

The cache is pre-fetched:

- every two hours
- on policy installation
- when the cache expires

If the pre-fetch fails, the previous cache is not erased.



Note - The ICA requires the use of a CRL cache.

An administrator can shorten the lifetime of a CRL in the cache or even to cancel the use of the cache. If the CRL Cache operation is cancelled, the CRL must be retrieved for each subsequent IKE negotiation, thus considerably slowing the establishment of the VPN tunnel. Because of these performance implications, it is recommend that CRL caching be disabled only when the level of security demands continuous CRL retrieval.

Special Considerations for the CRL Pre-fetch Mechanism

The CRL pre-fetch mechanism makes a "best effort" to obtain the most up to date list of revoked certificates. However, after the **cpstop**, **cpstart** commands have been executed, the cache is no longer updated. The Security Gateway continues to use the old CRL for as long as the old CRL remains valid (even if there is an updated CRL available on the CA). The pre-fetch cache mechanism returns to normal functioning only after the old CRL expires and a new CRL is retrieved from the CA.

In case there is a requirement that after **cpstop**, **cpstart** the CRL's will be updated immediately, proceed as follows:

- After executing **cprestart**, run **crl_zap** to empty the cache, or:
- In **Global Properties > SmartDashboard Customization > Configure > Check Point CA properties > select: flush_crl_cache_file_on_install**.

When a new policy is installed, the cache is flushed and a new CRL will be retrieved on demand.

CRL Grace Period

Temporary loss of connection with the CRL repository or slight differences between clocks on the different machines may cause valid of CRLs to be considered invalid—and thus the certificates to be invalid as well. VPN overcomes this problem by supplying a CRL Grace Period. During this period, a CRL is considered valid even if it is not valid according to the CLR validity time.

Special Considerations for PKI

Using the Internal CA vs. Deploying a Third Party CA

The Internal CA makes it easy to use PKI for Check Point applications such as site-to-site and remote access VPNs. However, an administrator may prefer to continue using a CA that is already functioning within the organization, for example a CA used to provide secure email, and disk encryption.

Distributed Key Management and Storage

Distributed Key Management (DKM) provides an additional layer of security during the key generation phase. Instead of the Security Management server generating both public and private keys and downloading them to the module during a policy installation, the management server instructs the module to create its own public and private keys and send (to the management server) only its public key. The private key is created and stored on the module in either a hardware storage device, or via software that emulates hardware storage. Security Management server then performs certificate enrollment. During a policy installation, the certificate is downloaded to the module. The private key never leaves the module.

Local key storage is supported for all CA types.

DKM is supported for all enrollment methods, and can be configured as a default setting by selecting in **Global Properties > SmartDashboard Customization > Configure > Certificates and PKI properties**, the option: **use_dkm_cert_by_default**



Note - Generating certificates for Edge devices does not support DKM and will be generated locally on the management even if **use_dkm_cert_by_default** is configured.

Configuration of PKI Operations

Trusting a CA – Step-By-Step

This section describes the procedures for obtaining a CA's own certificate, which is a prerequisite for trusting certificates issued by a CA.

In order to trust a CA, a CA server object has to be defined. The following sections deal with the various configuration steps required in different scenarios.

Trusting an ICA

A VPN module automatically trusts the ICA of the Security Management server that manages it. No further configuration is required.

Trusting an Externally Managed CA

An externally managed CA refers to the ICA of another Security Management server. The CA certificate has to be supplied and saved to disk in advance. To establish trust:

1. Open **Manage > Servers and OPSEC Applications**

- The **Servers and OPSEC Application** window opens.
2. Choose **New > CA**
Select **Trusted...**
The **Certificate Authority Properties** window opens.
 3. Enter a **Name** for the CA object and in the **Certificate Authority Type** drop-down box select the **External Check Point CA**.
 4. Go to the **External Check Point CA** tab and click **Get...**
 5. Browse to where you saved the peer CA certificate and select it.
VPN reads the certificate and displays its details. Verify the certificate's details. Display and validate the SHA-1 and MD5 fingerprints of the CA certificate.
 6. Click **OK**.

Trusting an OPSEC Certified CA

The CA certificate has to be supplied and saved to the disk in advance.



Note - In case of SCEP automatic enrollment, you can skip this stage and fetch the CA certificate automatically after configuring the SCEP parameters.

The CA's Certificate must be retrieved either by downloading it using the CA options on the **Servers and OSPEC Applications** tab, or by obtaining the CA's certificate from the peer administrator in advance.

Then define the CA object according to the following steps:

1. Open **Manage > Servers and OPSEC Applications**.
The **Servers and OPSEC Application** window opens.
2. Choose **New > CA**.
Select **Trusted** or **Subordinate**.
The **Certificate Authority Properties** window opens.
3. Enter a **Name** for the CA object, in the **Certificate Authority Type** drop-down box select the **OPSEC PKI**.
4. On the **OPSEC PKI** tab:
 - For automatic enrollment, select **automatically enroll certificate**.
 - From the **Connect to CA with protocol**, select the protocol used to connect with the certificate authority, either SCEP, CMPV1 or CMPV2.



Note - For entrust 5.0 and later, use CMPV1

5. Click **Properties**.
 - If you chose **SCEP** as the protocol, in the **Properties for SCEP protocol** window, enter the CA identifier (such as example.com) and the Certification Authority/Registration Authority URL.
 - If you chose cmpV1 as the protocol, in the **Properties for CMP protocol - V1** window, enter the appropriate IP address and port number. (The default port is 829).
 - If you chose cmpV2 as the protocol, in the **Properties for CMP protocol -V2** window, decide whether to use direct TCP or HTTP as the transport layer.
6. Choose a method for retrieving CRLs from this CA.
If the CA publishes CRLs on HTTP server choose **HTTP Server(s)**. Certificates issued by the CA must contain the CRL location in an URL in the **CRL Distribution Point** extension.
If the CA publishes CRL on LDAP server, choose **LDAP Server(s)**. In this case, you must define an LDAP Account Unit as well. See the *Security Management Server Administration Guide* for more details about defining an LDAP object.
Make sure that **CRL retrieval** is checked in the **General** tab of the **LDAP Account Unit Properties** window.

Certificates issued by the CA must contain the LDAP DN on which the CRL resides in the CRL distribution point extension.

7. Click **Get**.
8. If SCEP is configured, it will try to connect to the CA and retrieve the certificate. If not, browse to where you saved the peer CA certificate and select it.
VPN reads the certificate and displays its details. Verify the certificate's details. Display and validate the SHA-1 and MD5 fingerprints of the CA certificate.
9. Click **OK**.

Certificate Revocation (All CA Types)

A certificate issued by the Internal Certificate Authority is revoked when the certificate object is removed. Otherwise, certificate revocation is controlled by the CA administrator using the options on the **Advanced** tab of the CA object. In addition, the certificate must be removed from the module.

To remove the certificate:

1. Open the **VPN** tab of the relevant Network Object.
2. In the **Certificate List** field select the appropriate certificate and click **Remove**.

A certificate cannot be removed if Smart Center server infers from other settings that the certificate is in use, for example, that the module belongs to one or more VPN communities and this is the module's only certificate.

Certificate Recovery and Renewal

When a certificate is revoked or becomes expired, it is necessary to create another one or to refresh the existing one.

Recovery and Renewal with Internal CA

Removal of a compromised or expired certificate automatically triggers creation of a new certificate, with no intervention required by the administrator. To manually renew a certificate use the **Renew...** button on the VPN page of the Security Gateway object.



Note - A Security Gateway can have only one certificate signed by one CA. When the new certificate is issued, you will be asked to replace the existing certificate signed by the same CA.

CA Certificate Rollover

CA Certificate Rollover is a VPN-1 feature that enables rolling over the CA certificates used to sign client and Security Gateway certificates for VPN traffic, without risk of losing functionality at transition.

To achieve a gradual CA certificate rollover, CA Certificate Rollover enables VPN-1 support for multiple CA certificates generated by third-party OPSEC-compliant CAs, such as Microsoft Windows CA. By using multiple CA certificates, you can gradually rollover client and Security Gateway certificates during a transitional period when client and Security Gateway certificates signed by both CA certificates are recognized.

When a certificate is added to a CA that already has a certificate, the new certificate is defined as Additional and receives an index number higher by one than the highest existing certificate index number. The original certificate is defined as Main.

Only additional certificates can be removed. CA Certificate Rollover provides tools for adding and removing certificates, and for changing the status of a certificate from additional to main and from main to additional.

CA Certificate Rollover is for rolling over CA certificates with different keys. To add a CA certificate using the same key as the existing CA certificate (for example, to extend its expiration date), just Get the certificate from the OPSEC PKI tab of the CA properties, and do not use CA Certificate Rollover.

Managing a CA Certificate Rollover

By using multiple CA certificates, you can gradually rollover client and Security Gateway certificates during a transitional period when client and Security Gateway certificates signed by both CA certificates are recognized.

This section describes a recommended workflow for the most common scenario. For full details of the CLI commands, see CA Certificate Rollover CLI (on page 50).

Before you begin:

In SmartDashboard, define a third-party OPSEC-compliant CA, such as Microsoft Windows CA, that is capable of generating multiple CA certificates. Generate the main CA certificate and define it in SmartDashboard.

To roll over with a new CA certificate:

1. Generate from the third-party CA a second CA certificate in DER format (PEM is not supported), with different keys than the previous CA certificate. Copy the certificate to the Security Management Server.
2. Log into the Security Management Server, and stop Check Point processes:
`cpstop`
3. Back up the Security Management Server database:
`vpn mcc backup`
4. Add the new CA certificate to the Security Management Server database's definitions for the third-party CA:
`vpn mcc add <CA> <CertificateFile>`
5. <CA> is the name of the CA as defined in the Security Management Server database. <CertificateFile> is the certificate filename or path.
6. The new CA certificate should now be defined as additional #1. Make sure with "`vpn mcc lca`" or "`vpn mcc show`" ("CA Certificate Rollover CLI" on page 50).
7. Start Check Point processes:
`cpstart`
8. Install policy on all Security Gateways.

Use the new additional CA certificate to sign client certificates.

For performance reasons, as long as most clients are still using certificates signed by the old CA certificate, you should leave the new CA certificate as the additional one and the old certificate as the main one. As long as the new CA certificate is not the main CA certificate, do not use it to sign any Security Gateway certificates.

CA Certificate Rollover CLI

CA Certificate Rollover uses the VPN Multi-Certificate CA command set, as detailed in this section. VPN Multi-Certificate CA configuration commands should not be run when SmartDashboard or Database Tool are logged in to the Security Management Server, or when Check Point processes are running.

To see usage instructions in the CLI, run the following without arguments:

```
vpn mcc
```

Adding Matching Criteria to the Validation Process

While certificates of an externally managed VPN entity are not handled by the local Security Management server, you can still configure a peer to present a particular certificate when creating a VPN tunnel:

1. Open the **VPN** page of the externally managed VPN entity.
2. Click **Matching Criteria...**
3. Choose the desired characteristics of the certificate the peer is expected to present, including:
 - The CA that issued it
 - The exact DN of the certificate
 - The IP address that appears in the **Subject Alternate Name** extension of the certificate. (This IP address is compared to the IP address of the VPN peer itself as it appears to the VPN module during the IKE negotiation.)

- The e-mail address appearing in the **Subject Alternate Name** extension of the certificate

CRL Cache Usage

To cancel or modify the behavior of the CRL Cache:

1. Open the **Advanced Tab** of the Certificate Authority object.
2. To enable the CRL cache, check **Cache CRL on the module**.
The cache should not be disabled for the ICA. In general, it is recommended that the cache be enabled for all CA types. The cache should be disabled (for non-ICAs) only if stringent security requirements mandate continual retrieval of the CRL.
3. If CRL Cache is enabled, choose whether a CRL is deleted from the cache when it expires or after a fixed period of time (unless it expires first). The second option encourages retrieval of a CRL more often as CRLs may be issued more frequently than the expiry time. By default a CRL is deleted from the cache after 24 hours.



Note - The ICA requires the use of a CRL cache, and should never be disabled.

See: CRL Prefetch-Cache (on page 46) for information about CRL caching.

Modifying the CRL Pre-Fetch Cache

The behavior of the Pre-fetch catch can be altered via the Global properties:

1. **Global Properties > SmartDashboard Customization > Configure...** button
The **Advanced Configuration** window opens.
2. Select Check Point CA Properties:

Configuring CRL Grace Period

Set the CRL Grace Period values by selecting **Policy > Global Properties > VPN > Advanced**. The Grace Period can be defined for both the periods before and after the specified CRL validity period.

Configuring OCSP

In order to use OCSP, the CA object must be configured to the OCSP revocation checking method instead of CRL's.

Using **GuiDBedit**, modify the field **oscp_validation** to **true**. Set to true, this CA will check the validation of the certificate using OCSP. This is configured on the root CA and is inherited by the subordinate CA's.

To configure a trusted OCSP server using GuiDBedit of objectc.c:

1. Create a new server object of the type **oscp_server**.
2. Configure the OCSP servers URL and the certificate.
3. In the CA object, configure **oscp_server**. Add a reference to the OCSP server object created and install policy.

Site-to-Site VPN

In This Section

| | |
|---|-----|
| Domain Based VPN | 53 |
| Route Based VPN | 61 |
| Tunnel Management | 77 |
| Route Injection Mechanism | 82 |
| Wire Mode | 88 |
| Directional VPN Enforcement | 93 |
| Link Selection | 97 |
| Multiple Entry Point VPNs | 117 |
| Traditional Mode VPNs | 130 |
| Converting a Traditional Policy to a Community Based Policy | 137 |

Chapter 5

Domain Based VPN

In This Chapter

| | |
|--|----|
| Overview of Domain-based VPN | 53 |
| VPN Routing and Access Control | 53 |
| Configuring Domain Based VPN | 54 |

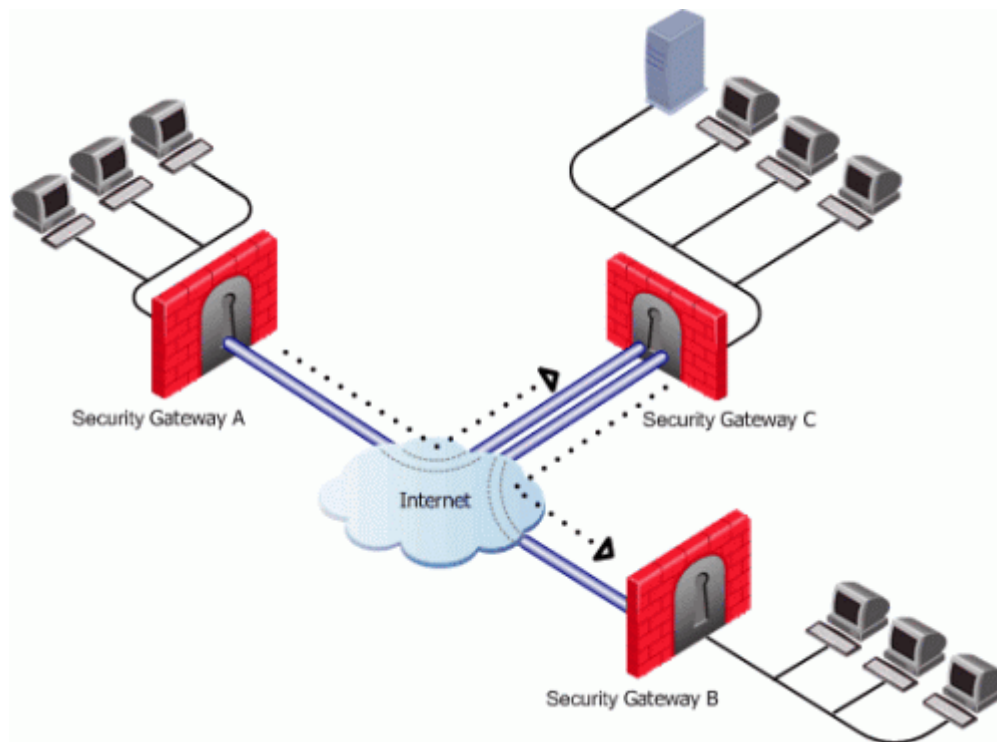
Overview of Domain-based VPN

Domain Based VPN is a method of controlling how VPN traffic is routed between Security Gateway modules and remote access clients within a community.

To route traffic to a host behind a Security Gateway, an encryption domain must be configured for that Security Gateway.

Configuration for VPN routing is performed either directly through SmartDashboard or by editing the VPN routing configuration files on the Security Gateways.

In the figure, one of the host machines behind Security Gateway A initiates a connection with a host machine behind Security Gateway B. For either technical or policy reasons, Security Gateway A cannot establish a VPN tunnel with Security Gateway B. Using VPN Routing, both Security Gateways A and B can establish VPN tunnels with Security Gateway C, so the connection is routed through Security Gateway C.



VPN Routing and Access Control

VPN routing connections are subject to the same access control rules as any other connection. If VPN routing is correctly configured but a Security Policy rule exists that does not allow the connection, the connection is dropped. For example: a Security Gateway has a rule which forbids all FTP traffic from inside the internal network to anywhere outside. When a peer Security Gateway opens an FTP connection with this Security Gateway, the connection is dropped.

For VPN routing to succeed, a single rule in the Security Policy Rule base must cover traffic in both directions, inbound and outbound, and on the central Security Gateway. To configure this rule, see [Configuring the 'Accept VPN Traffic Rule'](#) (see "[Configuring the 'Accept VPN Traffic Rule'](#)" on page 55).

Configuring Domain Based VPN

Common VPN routing scenarios can be configured through a VPN star community, but not all VPN routing configuration is handled through SmartDashboard. VPN routing between Security Gateways (star or mesh) can also be configured by editing the configuration file `$FWDIR/conf/vpn_route.conf`.

VPN routing cannot be configured between Security Gateways that do not belong to a VPN community.

Configuring VPN Routing for Security Gateways through SmartDashboard

For simple hubs and spokes (or if there is only one Hub), the easiest way is to configure a VPN star community in SmartDashboard:

1. On the **Star Community properties** window, **Central Security Gateways** page, select the Security Gateway that functions as the "Hub".
2. On the **Satellite Security Gateways** page, select Security Gateways as the "spokes", or satellites.
3. On the **VPN Routing** page, **Enable VPN routing for satellites** section, select one of these options:
 - **To center and to other Satellites through center.** This allows connectivity between the Security Gateways, for example if the spoke Security Gateways are DAIP Security Gateways, and the Hub is a Security Gateway with a static IP address.
 - **To center, or through the center to other satellites, to internet and other VPN targets.** This allows connectivity between the Security Gateways as well as the ability to inspect all communication passing through the Hub to the Internet.
4. Create an appropriate access control rule in the Security Policy Rule Base. Remember: one rule must cover traffic in both directions.
5. NAT the satellite Security Gateways on the Hub if the Hub is used to route connections from Satellites to the Internet.

The two DAIP Security Gateways can securely route communication through the Security Gateway with the static IP address.

To configure the VPN routing **for SmartLSM Security Gateways**:

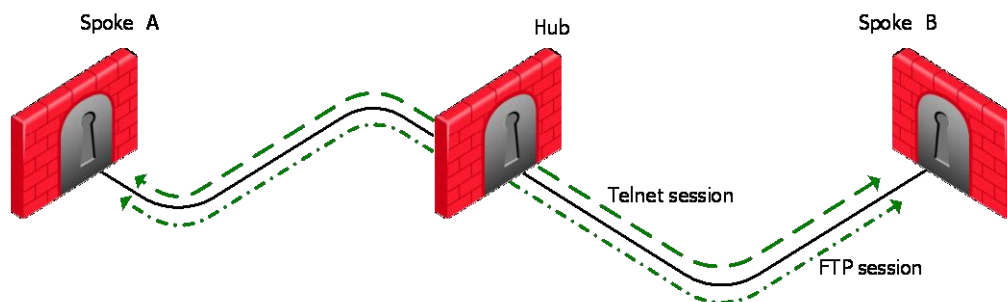
1. Create a network object that contains the VPN domains of all the Security Gateways managed by SmartProvisioning.
2. Edit the `vpn_route.conf` file, so that this network object appears in the **destination** column (the center Security Gateway of the star community).
3. Install this `vpn_route.conf` file on all LSM profiles that participate in the VPN community.

Configuration via Editing the VPN Configuration File

For more granular control over VPN routing, edit the `vpn_route.conf` file in the `conf` directory of the Security Management server.

The configuration file, `vpn_route.conf`, is a text file that contains the name of network objects. The format is: **Destination, Next hop, Install on Security Gateway** (with tabbed spaces separating the elements).

Consider a simple VPN routing scenario consisting of Hub and two Spokes (Figure 5-3). All machines are controlled from the same Security Management server, and all the Security Gateways are members of the same VPN community. Only Telnet and FTP services are to be encrypted between the Spokes and routed through the Hub:



Although this could be done easily by configuring a VPN star community, the same goal can be achieved by editing **vpn_route.conf**:

| Destination | Next hop router interface | Install on |
|-----------------|---------------------------|------------|
| Spoke_B_VPN_Dom | Hub_C | Spoke_A |
| Spoke_A_VPN_Dom | Hub_C | Spoke_B |

In this instance, Spoke_B_VPN_Dom is the name of the network object group that contains spoke B's VPN domain. Hub C is the name of the Security Gateway enabled for VPN routing. Spoke_A_VPN_Dom is the name of the network object that represents Spoke A's encryption domain. For an example of how the file appears:

```
Spoke_B_VPN_DOM  Hub_C      Spoke_A
Spoke_A_VPN_DOM  Hub_C      Spoke_B
```

Configuring the 'Accept VPN Traffic Rule'

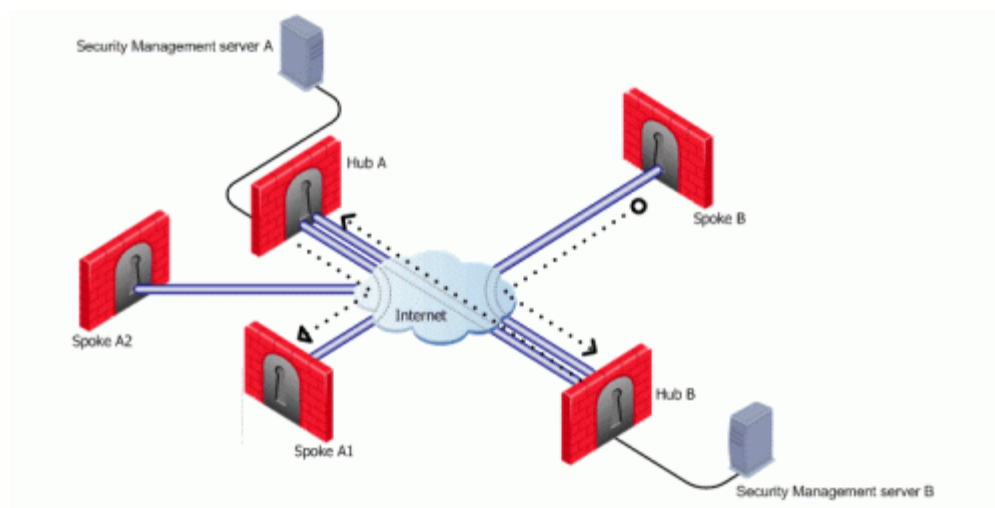
In SmartDashboard:

1. Double click on a Star or Meshed community.
2. On the **General** properties page, select the **Accept all encrypted traffic** checkbox.
3. In a Star community, click **Advanced** to choose between accepting encrypted traffic on **Both center and satellite Security Gateways** or **Satellite Security Gateways only**.
4. Click **OK**.

A rule will appear in the Rule Base that will accept VPN traffic between the selected Security Gateways.

Configuring Multiple Hubs

Consider two Hubs, A and B. Hub A has two spokes, spoke_A1, and spoke_A2. Hub B has a single spoke, spoke_B. In addition, Hub A is managed from Security Management server A, while Hub B is managed via Security Management server B:



For the two VPN star communities, based around Hubs A and B:

- Spokes A1 and A2 need to route all traffic going outside of the VPN community through Hub A
- Spokes A1 and A2 also need to route all traffic to one another through Hub A, the center of their star community
- Spoke B needs to route all traffic outside of its star community through Hub B

A_community is the VPN community of A plus the spokes belonging to A. B_community is the VPN community. Hubs_community is the VPN community of Hub_A and Hub_B.

Configuring VPN Routing and Access Control on Security Management server A

The `vpn_route.conf` file on Security Management server 1 looks like this:

| Destination | Next hop router interface | Install on |
|------------------|---------------------------|------------|
| Spoke_B_VPN_Dom | Hub_A | A_Spokes |
| Spoke_A1_VPN_Dom | Hub_A | Spoke_A2 |
| Spoke_A2_VPN_Dom | Hub_A | Spoke_A1 |
| Spoke_B_VPN_Dom | Hub_B | Hub_A |

Spokes A1 and A2 are combined into the network group object "A_spokes". The appropriate rule in the Security Policy Rule Base looks like this:

| Source | Destination | VPN | Service | Action |
|--------|-------------|--|---------|--------|
| Any | Any | A_Community B_Community Hubs_Community | Any | Accept |

Configuring VPN Routing and Access Control on Security Management server B

The `vpn_route.conf` file on Security Management server 2 looks like this:

| Destination | Next hop router interface | Install On |
|------------------|---------------------------|------------|
| Spoke_A1_VPN_Dom | Hub_B | Spoke_B |
| Spoke_A2_VPN_Dom | Hub_B | Spoke_B |
| Spoke_A1_VPN_Dom | Hub_A | Hub_B |
| Spoke_A2_VPN_Dom | Hub_A | Hub_B |

The appropriate rule in the Security Policy Rule Base looks like this:

| Source | Destination | VPN | Service | Action |
|--------|-------------|--|---------|--------|
| Any | Any | B_Community A_Community Hubs_Community | Any | Accept |

For both `vpn_route.conf` files:

- "A_Community" is a star VPN community comprised of Hub_A, Spoke_A1, and Spoke_A2
- "B_Community" is a star VPN community comprised of Hub_B and Spoke_B
- "Hubs-Community" is a *meshed* VPN community comprised of Hub_A and Hub_B (it could also be a star community with the central Security Gateways meshed).



VPN for a SmartLSM Profile

If branch office Security Gateways are managed by SmartProvisioning as SmartLSM Security Gateways, enable VPN routing for a hub and spoke configuration by editing the `vpn_route.conf` file on the Security Management server.

To configure VPN For a single SmartLSM Profile with multiple gateways:

- In SmartDashboard, create a **Group** that contains the encryption domains of all the satellite SmartLSM Security Gateways and call it **Robo_domain**
- Create a **Group** that contains all the Center Security Gateways and call it **Center_gws**
- In `vpn_route.conf`, add the rule:

| | | |
|-------------|------------|--------------|
| Destination | Router | Install on |
| Robo_Domain | Center_gws | Robo_profile |

If access to the SmartLSM Security Gateway through the VPN tunnel is required, the Security Gateway's external IP address should be included in the ROBO_domain.

Multiple router Security Gateways are now supported on condition that:

- the Security Gateways are listed under "install on" in `vpn_route.conf` or
- the satellites Security Gateways are selected in SmartDashboard

VPN with One or More LSM Profiles

You can configure a VPN star community between two SmartLSM Profiles. The procedures below show a SmartLSM Profile Gateway and Cluster. You can also configure the community with two SmartLSM Profile

Clusters or two SmartLSM Profile Gateways. All included SmartLSM Profile Gateways and Clusters must have the IPsec VPN blade enabled.

The procedure requires configuration in:


- SmartDashboard
- Security Management Server CLI
- SmartProvisioning Console
- Center Gateway CLI

Using SmartDashboard

In SmartDashboard create network objects that represent the VPN community members and their networks. You must create a star community with **To center and to other satellites through center** as the selected option for **VPN Routing**.

To configure a VPN star community between two SmartLSM Profiles in SmartDashboard:

1. Create and configure a SmartLSM Profile Cluster.
 - When you configure the topology, make the interface names the same as the actual gateway's interface names.
2. Create and configure a SmartLSM Profile Gateway.
3. Create a regular Security Gateway to be the Center Gateway.

 **Note** - Security Gateway 80 gateways cannot be the Center Gateway.
4. Create a VPN Star Community: **VPN Communities** tab > Right-click and select **New > Site to Site > Star**.
 - a) Select **Center Gateways** from the tree.
 - b) Click **Add** and select the Security Gateway that you created to be the Center Gateway.
 - c) Select **Satellite Gateways** from the tree.
 - d) Click **Add** and select the SmartLSM Profile Cluster and SmartLSM Profile Gateway (or second cluster).
 - e) Select **Advanced Settings > VPN Routing** from the tree.
 - f) Select **To center and to other satellites through center**.
5. Create a **Network** object that represents the internal network of each satellite in the VPN community.
 - a) From the Network Objects tree, right-click **Networks** and select **Network**.
 - b) In the **Network Address** field, enter the IP address that represents the internal IP address of the satellite. If the satellite is a cluster, enter the internal Virtual IP.
6. Create a **Node** object that represents the external IP address of each satellite in the VPN community.
 - a) From the Network Objects tree, right-click **Nodes** and select **Node > Gateway**.
 - b) In the **IP Address** field, enter the IP address that represents the external IP address of the satellite. If the satellite is a cluster, enter the external Virtual IP.
7. Create a **Group** object that represents the networks for each satellite object:
 - a) From the Network Objects tree, right-click and select **New > Groups > Simple Group**.
 - b) Enter a **Name** for the group that is unique for one satellite.
 - c) Select the **Network** object that you created for that satellite's internal network and click **Add**.
 - d) Select the **Node** object that you created for that satellite's external IP address and click **Add**.
8. Create a **Group** object that represents the Center Gateway.
 - a) From the Network Objects tree, right-click and select **New > Groups > Simple Group**.
 - b) Enter a **Name** for the group that is unique for the Center Gateway.
 - c) Select the Gateway object and click **Add**.

Using the CLI

Edit the routing table of the Domain Management Server or Security Management Server to enable two SmartLSM Profile Gateways or Clusters to communicate with each other through the Center Gateway. Do this in the `vpn_route.conf` file in the CLI.

To edit the `vpn_route.conf` file:

- Open the `vpn_route.conf` file.
 - In a Multi-Domain Security Management environment, on a Domain Management Server:
 - If satellites are 80 series Gateways or Clusters:
`/var/opt/CPmds-<version>/customers/<Domain Management Server_name>/CPSG80CMP-<version>/conf/vpn_route.conf`
 - If satellites are on a different SecurePlatform appliance or open server:
`/opt/CPmds-<version>/customers/<Domain Management Server_name>/CPsuite-<version>/fw1/conf/vpn_route.conf`
 - In a Security Management Server environment:
 - If satellites are 80 series Gateways or Clusters:
`/opt/CPSG80CMP-<version>/conf/vpn_route.conf`
 - If satellites are on a different SecurePlatform appliance or open server:
`/opt/CPsuite-<version>/fw1/conf/vpn_route.conf`
- If two SmartLSM Gateways on different LSM Gateway profiles will communicate with each other through the Center gateway, edit the file:

| | | |
|--|------------------|------------------------------|
| # destination | router | [install on] |
| <Simple Group Name of internal network of SmartLSM Gateway> | <Center Gateway> | <Name of second LSM Profile> |
| <Simple Group Name of internal network of second SmartLSM Gateway> | <Center Gateway> | <Name of LSM Profile> |

- If more than one SmartLSM Gateway in the same LSM Profile will communicate with each other through the Center gateway, edit the file:

| | | |
|---|------------------|-----------------------|
| # destination | router | [install on] |
| <Simple Group Name of internal network of SmartLSM Gateway> | <Center Gateway> | <Name of LSM Profile> |

- Install policy on the SmartLSM Profiles and on the Center Gateway.

Completing the Configuration

Complete the configuration in the SmartProvisioning Console and the CLI of the Center Gateway.

To complete the VPN configuration:

- Open the SmartProvisioning GUI Console.
- Create a new SmartLSM Cluster or Gateway based on the type of device you have. Select **File > New >** select an option.
- Generate a VPN certificate for each Gateway or Cluster member:
 - Open the cluster or gateway object > **VPN** tab.
 - Select **Use Certificate Authority Certificate**.
 - Click **Generate**.
 - Do these steps again for each cluster member.



Note - If topology information, including date and time, changes after you generate the certificate, you must generate a new certificate in the **VPN** tab and update the gateway (**Actions > Update Gateway**).

- In the CLI of the Center Gateway, run: `LSMenabler on`
- In the SmartProvisioning GUI Console, right-click the Center Gateway and select **Actions > Update Gateway**.

6. In the **Topology** tab of each object, make sure that the topology of provisioned objects is correct for each device:
 - Make sure that the interfaces have the same IP addresses as the actual gateways.
 - Make sure that the external and internal interfaces are recognized and configured correctly as "External" and "Internal".
 - If the interfaces show without IP addresses, click: **Get Actual Settings**.
7. In the **Topology** tab, configure the VPN domain:
 - For SmartLSM Profile Gateways choose an option.
 - For SmartLSM Profile Clusters, select **Manually defined** and manually add the encryption domains that you want to include.
8. **Push Policy**.

All traffic between the satellites and Center Gateway is encrypted.

Chapter 6

Route Based VPN

In This Chapter

| | |
|---|----|
| Overview of Route-based VPN | 61 |
| VPN Tunnel Interface (VTI) | 62 |
| Using Dynamic Routing Protocols | 63 |
| Configuring Numbered VTIs | 63 |
| VTIs in a Clustered Environment | 65 |
| Configuring VTIs in a Clustered Environment | 65 |
| Enabling Dynamic Routing Protocols on VTIs | 71 |
| Configuring Anti-Spoofing on VTIs | 74 |
| Configuring a Loopback Interface | 74 |
| Configuring Unnumbered VTIs | 74 |
| Routing Multicast Packets Through VPN Tunnels | 75 |

Overview of Route-based VPN

The use of VPN Tunnel Interfaces (VTI) introduces a new method of configuring VPNs called *Route Based VPN*. This method is based on the notion that setting up a VTI between peer Security Gateways is much like connecting them directly.

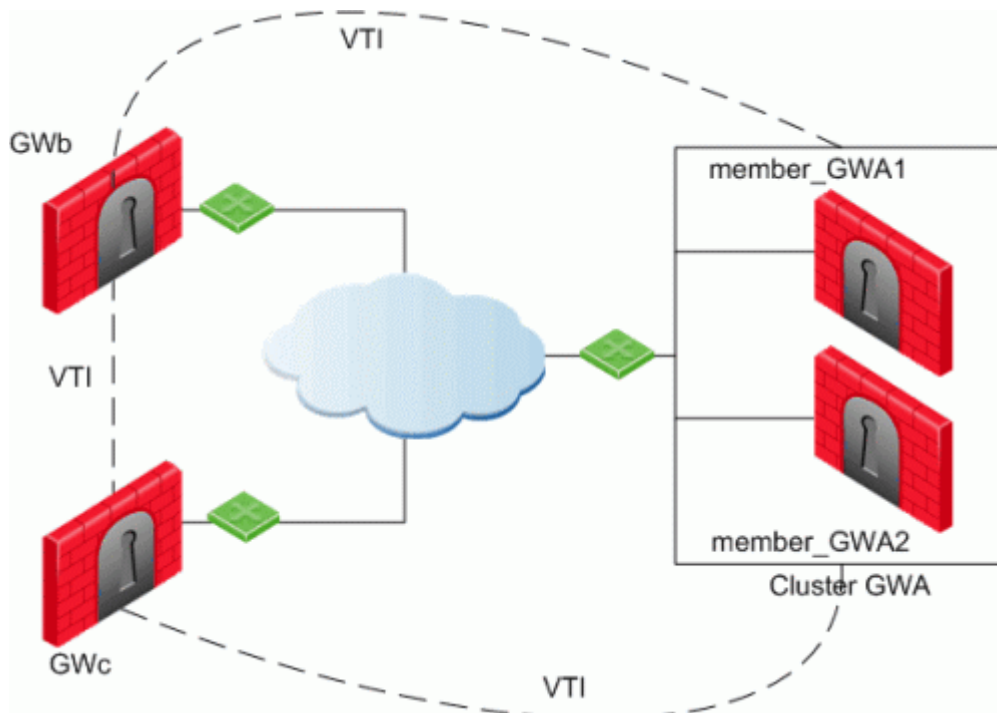
A VTI is an operating system level virtual interface that can be used as a Security Gateway to the encryption domain of the peer Security Gateway. Each VTI is associated with a single tunnel to a Security Gateway. The tunnel itself with all its properties is defined, as before, by a VPN Community linking the two Security Gateways. The peer Security Gateway should also be configured with a corresponding VTI. The native IP routing mechanism on each Security Gateway can then direct traffic into the tunnel just as it would for any other type of interface.

All traffic destined to the encryption domain of a peer Security Gateway, will be routed through the "associated" VTI. This infrastructure allows dynamic routing protocols to use VTIs. A dynamic routing protocol daemon running on the Security Gateway can exchange routing information with a neighboring routing daemon running on the other end of an IPSec tunnel, which appears to be a single hop away.

Route Based VPN is supported using SecurePlatform and IPSO 3.9 platforms only and can only be implemented between two Security Gateways within the same community.

VPN Tunnel Interface (VTI)

A VPN Tunnel Interface is a virtual interface on a Security Gateway that is related to a VPN tunnel and connects to a remote peer. You create a VTI on each Security Gateway that connects to the VTI on a remote peer. Traffic routed from the local Security Gateway via the VTI is transferred encrypted to the associated peer Security Gateway.



In this scenario:

- There is a VTI connecting Cluster GWA and GWb
- There is a VTI connecting Cluster GWA and GWc
- There is a VTI connecting GWb and GWc

A virtual interface behaves like a point-to-point interface directly connected to the remote peer. Traffic between network hosts is routed into the VPN tunnel using the IP routing mechanism of the Operating System. Security Gateway objects are still required, as well as VPN communities (and access control policies) to define which tunnels are available. However, VPN encryption domains for each peer Security Gateway are no longer necessary. The decision whether or not to encrypt depends on whether the traffic is routed through a virtual interface. The routing changes dynamically if a dynamic routing protocol (OSPF/BGP) is available on the network.



Note - For NGX (R60) and above, the dynamic routing suite has been incorporated into SecurePlatform Pro. The administrator runs a daemon on the Security Gateway to publish the changed routes to the network.

When a connection that originates on GWb is routed through a VTI to GWc (or servers behind GWc) and is accepted by the implied rules, the connection leaves GWb in the clear with the local IP address of the VTI as the source IP address. If this IP address is not routable, return packets will be lost.

The solution for this issue is:

- configure a static route on GWb that redirects packets destined to GWc from being routed through the VTI.
- not including it in any published route
- adding route maps that filter out GWc's IP addresses.

Having excluded those IP addresses from route-based VPN, it is still possible to have other connections encrypted to those addresses (i.e. when not passing on implied rules) by using domain based VPN definitions.

The VTI may be configured in two ways:

- Numbered
- Unnumbered

Numbered VTI

You configure a local and remote IP address for each numbered VPN Tunnel Interface (VTI). For each Security Gateway, you configure a local IP address, a remote address, and the local IP address source for outbound connections to the tunnel. The remote IP address must be the local IP address on the remote peer Security Gateway. More than one VTI can use the same IP Address, but they cannot use an existing physical interface IP address.

Numbered interfaces are supported for SecurePlatform and Gaia operating systems.

Unnumbered VTI

For unnumbered VTIs, you define a proxy interface for each Security Gateway. Each Security Gateway uses the proxy interface IP address as the source for outbound traffic. Unnumbered interfaces let you assign and manage one IP address for each interface. Proxy interfaces can be physical or loopback interfaces.

Unnumbered interfaces are supported for Gaia and IPSO (3.9 and higher) platforms.

Using Dynamic Routing Protocols

VTIs allow the ability to use Dynamic Routing Protocols to exchange routing information between Security Gateways. The Dynamic Routing Protocols supported are:

1. BGP4
2. OSPF
3. RIPv1 (SecurePlatform Pro only)
4. RIPv2 (SecurePlatform Pro only)

Configuring Numbered VTIs

Route Based VPN is supported using SecurePlatform and IPSO 3.9 platforms only and can only be implemented between two Security Gateways within the same community.

Enabling Route Based VPN

If you configure a Security Gateway for Domain Based VPN and Route Based VPN, Domain Based VPN takes precedence by default. To force Route Based VPN to take priority, you must create a dummy (empty) group and assign it to the VPN domain.

To force Route-Based VPN to take priority:

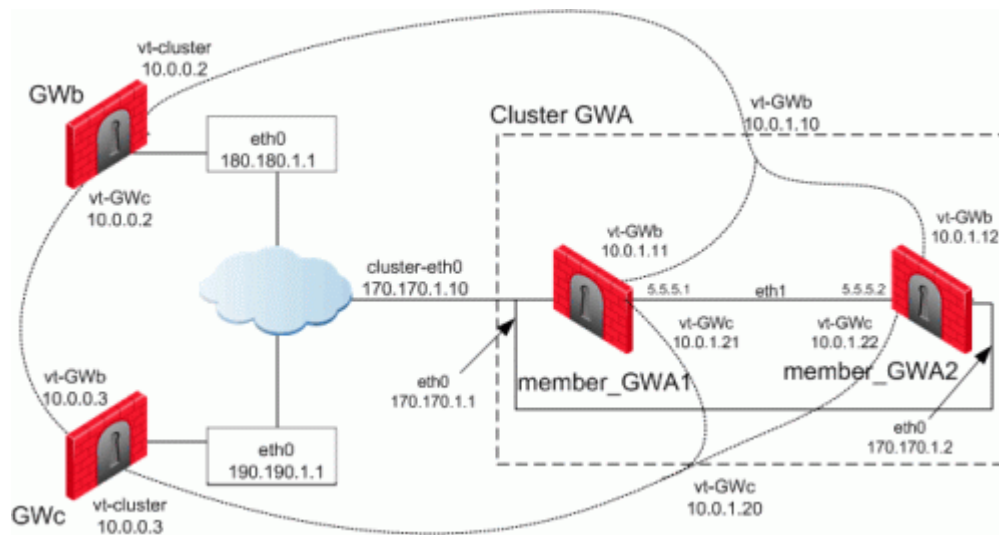
1. In SmartDashboard, select **Manage > Network Objects**.
2. Select a Check Point Security Gateway and right-click **Edit**.
3. In the **Properties** list, click **Topology**.
4. In the **VPN Domain** section, select **Manually define**.
5. Click **New > Group > Simple Group**.
6. Enter a name in the **Name** field and click **OK**.

Numbered VTIs

Using the new VPN Command Line Interface (VPN Shell), the administrator creates a VPN Tunnel Interface on the enforcement module for each peer Security Gateway, and "associates" the interface with a peer

Security Gateway. The VPN Tunnel Interface may be numbered or unnumbered. For more information on the VPN Shell, see [VPN Shell](#) (on page 289).

Every numbered VTI is assigned a local IP Address and a remote IP Address. Prior to configuration, a range of IP Addresses must be configured to assign to the VTIs.



A VTI connects:

- Cluster GWA and GWb
- Cluster GWA and GWc
- GWb and GWc

The devices in this scenario are:

ClusterXL:

- Cluster GWA
- member_GWA1
- member_GWA2

VPN Modules:

- GWb
- GWc

IP Configurations:

- Cluster GWA
- member_GWA1
- External Unique IP eth0: 170.170.1.1/24
- External VIP eth0: 170.170.1.10/24
- Sync Interface eth1: 5.5.5.1/24
- IP of VTI vt-GWb: Local: 10.0.1.11, Remote: 10.0.0.2
- VIP of VTI vt-GWb: 10.0.1.10
- IP of VTI vt-GWc: Local: 10.0.1.21, Remote: 10.0.0.3
- VIP of VTI vt-GWc: 10.0.1.20
- member_GWA2
- External Unique IP eth0: 170.170.1.2/24
- External VIP eth0: 170.170.1.10/24
- Sync Interface eth1: 5.5.5.1/24

- IP of VTI vt-GWb: Local: 10.0.1.12, Remote: 10.0.0.2
- VIP of VTI vt-GWb: 10.0.1.10
- IP of VTI vt-GWc: Local: 10.0.1.22, Remote: 10.0.0.3
- VIP of VTI vt-GWc: 10.0.1.20
- GWb
- External Unique IP eth0: 180.180.1.1/24
- IP of VTI vt-ClusterGWa: Local: 10.0.0.2, Remote: 10.0.1.10
- IP of VTI vt-GWc: Local: 10.0.0.2, Remote: 10.0.0.3
- GWc
- External Unique IP eth0: 190.190.1.1/24
- IP of VTI vt-ClusterGWa: Local: 10.0.0.3, Remote: 10.0.1.20
- IP of VTI vt-GWb: Local: 10.0.0.3, Remote: 10.0.0.2

VTIs in a Clustered Environment

When configuring numbered VTIs in a clustered environment, a number of issues need to be considered:

- Each member must have a unique source IP address.
- Every interface on each member requires a unique IP address.
- All VTIs going to the same remote peer must have the same name.
- Cluster IP addresses are required.

Configuring VTIs in a Clustered Environment

The following sample configurations use the same Security Gateway names and IP addresses used referred to in: Numbered VTIs (on page [63](#))

Configuring member_GWA1

```

----- Access the VPN shell Command Line Interface
[member_GWa2]# vpn shell
?                - This help
..               - Go up one level
quit            - Quit
[interface      ] - Manipulate tunnel interfaces
[show           ] - Show internal data
[tunnels        ] - Manipulate tunnel data
----- Add vt-GWb
VPN shell:[/] > /interface/add/numbered 10.0.1.12 10.0.0.2
GWb
Interface 'vt-GWb' was added successfully to the system
----- Add vt-GWc
VPN shell:[/] > /interface/add/numbered 10.0.1.22 10.0.0.3
GWc
Interface 'vt-GWc' was added successfully to the system
----- Verify configuration
VPN shell:[/] > /show/interface/detailed all
vt-GWb          Type:numbered   MTU:1500
                  inet addr:10.0.1.12  P-t-P:10.0.0.2
Mask:255.255.255.255
                  Peer:GWb  Peer ID:180.180.1.1  Status:attached

vt-GWc          Type:numbered   MTU:1500
                  inet addr:10.0.1.22  P-t-P:10.0.0.3
Mask:255.255.255.255
                  Peer:GWc  Peer ID:190.190.1.1  Status:attached

VPN shell:[/] > /quit
[member_GWa2]# ifconfig vt-GWb
vt-GWb          Link encap:IPIP Tunnel  HWaddr
                  inet addr:10.0.1.12  P-t-P:10.0.0.2
Mask:255.255.255.255
                  UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500
Metric:1
                  RX packets:0 errors:0 dropped:0 overruns:0
frame:0
                  TX packets:1 errors:0 dropped:0 overruns:0
carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:0 (0.0 b)  TX bytes:36 (36.0 b)

[member_GWa2]# ifconfig vt-GWc
vt-GWc          Link encap:IPIP Tunnel  HWaddr
                  inet addr:10.0.1.22  P-t-P:10.0.0.3
Mask:255.255.255.255
                  UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500
Metric:1
                  RX packets:0 errors:0 dropped:0 overruns:0
frame:0
                  TX packets:1 errors:0 dropped:0 overruns:0
carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:0 (0.0 b)  TX bytes:36 (36.0 b)

```

Configuring member_GWA2

```

----- Access the VPN shell Command Line Interface
[member_GWa2]# vpn shell
?                - This help
..               - Go up one level
quit            - Quit
[interface      ] - Manipulate tunnel interfaces
[show           ] - Show internal data

```

```
[tunnels      ] - Manipulate tunnel data
----- Add vt-GWb
VPN shell:[/] > /interface/add/numbered 10.0.1.12 10.0.0.2
GWb
Interface 'vt-GWb' was added successfully to the system
----- Add vt-GWc
VPN shell:[/] > /interface/add/numbered 10.0.1.22 10.0.0.3
GWc
Interface 'vt-GWc' was added successfully to the system
----- Verify configuration
VPN shell:[/] > /show/interface/detailed all
vt-GWb      Type:numbered  MTU:1500
             inet addr:10.0.1.12  P-t-P:10.0.0.2
Mask:255.255.255.255
             Peer:GWb  Peer ID:180.180.1.1  Status:attached

vt-GWc      Type:numbered  MTU:1500
             inet addr:10.0.1.22  P-t-P:10.0.0.3
Mask:255.255.255.255
             Peer:GWc  Peer ID:190.190.1.1  Status:attached

VPN shell:[/] > /quit
[member_GWa2]# ifconfig vt-GWb
vt-GWb      Link encap:IPIP Tunnel  HWaddr
             inet addr:10.0.1.12  P-t-P:10.0.0.2
Mask:255.255.255.255
             UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500
Metric:1
             RX packets:0 errors:0 dropped:0 overruns:0
frame:0
             TX packets:1 errors:0 dropped:0 overruns:0
carrier:0
             collisions:0 txqueuelen:0
             RX bytes:0 (0.0 b)  TX bytes:36 (36.0 b)

[member_GWa2]# ifconfig vt-GWc
vt-GWc      Link encap:IPIP Tunnel  HWaddr
             inet addr:10.0.1.22  P-t-P:10.0.0.3
Mask:255.255.255.255
             UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500
Metric:1
             RX packets:0 errors:0 dropped:0 overruns:0
frame:0
             TX packets:1 errors:0 dropped:0 overruns:0
carrier:0
             collisions:0 txqueuelen:0
             RX bytes:0 (0.0 b)  TX bytes:36 (36.0 b)
```

When configuring a VTI in a clustered environment and an interface name is not specified, a name is provided. The default name for a VTI is "vt-[peer Security Gateway name]". For example, if the peer Security Gateway's name is Server_2, the default name of the VTI is 'vt-Server_2'. For peer Security Gateways that have names that are longer than 12 characters, the default interface name is the last five characters plus a 7 byte hash of the peer name calculated to give the interface a unique name.

After configuring the VTIs on the cluster members, it is required to configure in the SmartConsole the VIP of these VTIs.

In SmartDashboard:

1. Select **Manage > Network Objects**.
2. Select the Check Point Cluster and right click **Edit**.
3. In **Topology** window, click **Edit Topology**.
4. Click **Get all members' topology**.

The VTIs are shown in the topology.

Note that the Edit Topology window lists the members of a VTI on the same line if the following criteria match:

- Remote peer name
- Remote IP address
- Interface name

5. Configure the VTI VIP in the **Topology** tab.

6. Click **OK** and install policy.

Configuring GWb

```

----- Access the VPN shell Command Line Interface
[GWb]# vpn shell
?                - This help
..               - Go up one level
quit             - Quit
[interface      ] - Manipulate tunnel interfaces
[show           ] - Show internal data
[tunnels        ] - Manipulate tunnel data
----- Add vt-GWa
VPN shell:[/] > /interface/add/numbered 10.0.0.2 10.0.1.10
GWa
Interface 'vt-GWa' was added successfully to the system
----- Add vt-GWc
VPN shell:[/] > /interface/add/numbered 10.0.0.2 10.0.0.3
GWc
Interface 'vt-GWc' was added successfully to the system
----- Verify configuration
VPN shell:[/] > /show/interface/detailed all
vt-GWa          Type:numbered  MTU:1500
                  inet addr:10.0.0.2  P-t-P:10.0.1.10
Mask:255.255.255.255
                  Peer:GWa  Peer ID:170.170.1.10  Status:attached

vt-GWc          Type:numbered  MTU:1500
                  inet addr:10.0.0.2  P-t-P:10.0.0.3
Mask:255.255.255.255
                  Peer:GWc  Peer ID:190.190.1.1  Status:attached

VPN shell:[/] > /quit
[GWb]# ifconfig vt-GWa
vt-GWa          Link encap:IPIP Tunnel  HWaddr
                  inet addr:10.0.0.2  P-t-P:10.0.1.10
Mask:255.255.255.255
                  UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500
Metric:1
                  RX packets:0 errors:0 dropped:0 overruns:0
frame:0
                  TX packets:1 errors:0 dropped:0 overruns:0

```

```
carrier:0
    collisions:0 txqueuelen:0
    RX bytes:0 (0.0 b)  TX bytes:36 (36.0 b)

[GWb]# ifconfig vt-GWc
vt-GWc    Link encap:IPIP Tunnel  HWaddr
          inet addr:10.0.0.2  P-t-P:10.0.0.3
Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500
Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
frame:0
          TX packets:1 errors:0 dropped:0 overruns:0
carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:36 (36.0 b)
```

Configuring GWc

```

----- Access the VPN shell Command Line Interface
[GWc]# vpn shell
?                - This help
..               - Go up one level
quit             - Quit
[interface      ] - Manipulate tunnel interfaces
[show           ] - Show internal data
[tunnels        ] - Manipulate tunnel data
----- Add vt-GWa
VPN shell:[/] > /interface/add/numbered 10.0.0.3 10.0.1.20
GWa
Interface 'vt-GWa' was added successfully to the system
----- Add vt-GWb
VPN shell:[/] > /interface/add/numbered 10.0.0.3 10.0.0.2
GWb
Interface 'vt-GWb' was added successfully to the system
----- Verify configuration
VPN shell:[/] > /show/interface/detailed all
vt-GWa          Type:numbered  MTU:1500
                  inet addr:10.0.0.3  P-t-P:10.0.1.20
Mask:255.255.255.255
                  Peer:GWa  Peer ID:170.170.1.10  Status:attached

vt-GWb          Type:numbered  MTU:1500
                  inet addr:10.0.0.3  P-t-P:10.0.0.2
Mask:255.255.255.255
                  Peer:GWb  Peer ID:180.180.1.1  Status:attached

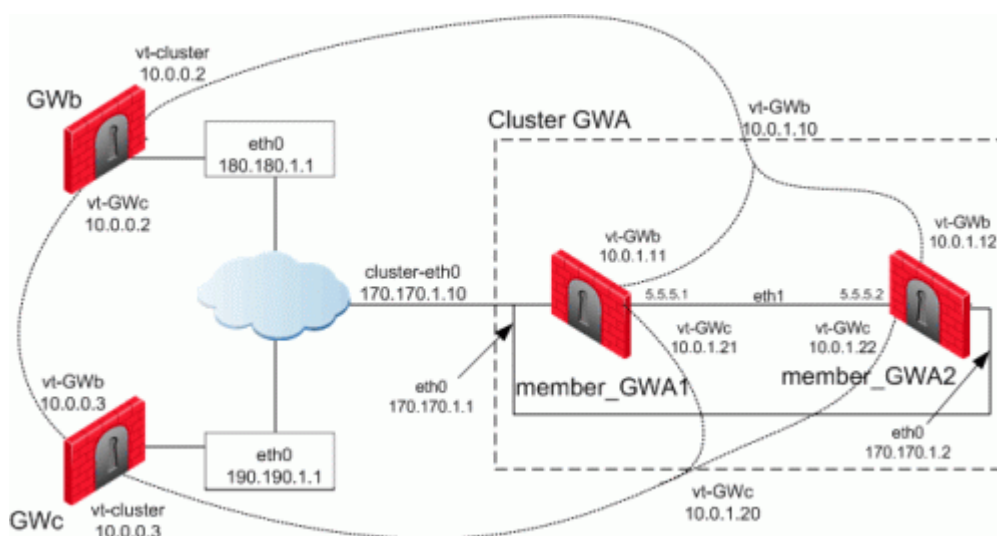
VPN shell:[/] > /quit
[GWc]# ifconfig vt-GWa
vt-GWa          Link encap:IPIP Tunnel  HWaddr
                  inet addr:10.0.0.3  P-t-P:10.0.1.20
Mask:255.255.255.255
                  UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500
Metric:1
                  RX packets:0 errors:0 dropped:0 overruns:0
frame:0
                  TX packets:1 errors:0 dropped:0 overruns:0
carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:0 (0.0 b)  TX bytes:36 (36.0 b)

[GWc]# ifconfig vt-GWb
vt-GWb          Link encap:IPIP Tunnel  HWaddr
                  inet addr:10.0.0.3  P-t-P:10.0.0.2
Mask:255.255.255.255
                  UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500
Metric:1
                  RX packets:0 errors:0 dropped:0 overruns:0
frame:0
                  TX packets:1 errors:0 dropped:0 overruns:0
carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:0 (0.0 b)  TX bytes:36 (36.0 b)

```

Enabling Dynamic Routing Protocols on VTIs

Using the example:



The following tables illustrate how the OSPF dynamic routing protocol is enabled on VTIs both for single members and for cluster members using SecurePlatform. Note that the network commands for single members and cluster members are not the same.

For more information on advanced routing commands and syntaxes, see the *Check Point Advanced Routing Suite - Command Line Interface* book.

To learn about enabling dynamic routing protocols on VTIs in Gaia environments, see VPN Tunnel Interfaces in the *R75.40 Gaia Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk67581>).

When peering with a Cisco GRE enabled device, a point to point GRE tunnel is required. Use the following command to configure the tunnel interface definition:

```
ip ospf network point-to-point
```

Dynamic Routing on member_GWA1

```

----- Launch the Dynamic Routing Module
[member_GWA1]# expert
Enter expert password:

You are in expert mode now.

[Expert@member_GWA1]# cligated
localhost>enable
localhost#configure terminal
----- Enable OSPF and provide an OSPF router ID
localhost(config)#router ospf 1
localhost(config-router-ospf)#router-id 170.170.1.10
----- Define interfaces/IP's on which OSPF runs (Use
the cluster IP as defined in topology) and the area ID for
the interface/IP
localhost(config-router-ospf)#network 10.0.1.10 0.0.0.0
area 0.0.0.0
localhost(config-router-ospf)#network 10.0.1.20 0.0.0.0
area 0.0.0.0
----- Redistribute kernel routes (this is only here as
an example, please see the dynamic routing book for more
specific commands concerning redistribution of routes)
localhost(config-router-ospf)#redistribute kernel
localhost(config-router-ospf)#exit
localhost(config)#exit
----- Write configuration to disk
localhost#write memory
IU0 999 Configuration written to '/etc/gated.ami'
localhost#quit

```

Dynamic Routing on member_GWA2

```

----- Launch the Dynamic Routing Module
[member_GWA2]# expert
Enter expert password:

You are in expert mode now.

[Expert@member_GWA2]# cligated
localhost>enable
localhost#configure terminal
----- Enable OSPF and provide an OSPF router ID
localhost(config)#router ospf 1
localhost(config-router-ospf)#router-id 170.170.1.10
----- Define interfaces/IP's on which OSPF runs (Use
the cluster IP as defined in topology) and the area ID for
the interface/IP
localhost(config-router-ospf)#network 10.0.1.10 0.0.0.0
area 0.0.0.0
localhost(config-router-ospf)#network 10.0.1.20 0.0.0.0
area 0.0.0.0
----- Redistribute kernel routes (this is only here as
an example, please see the dynamic routing book for more
specific commands concerning redistribution of routes)
localhost(config-router-ospf)#redistribute kernel
localhost(config-router-ospf)#exit
localhost(config)#exit
----- Write configuration to disk
localhost#write memory
IU0 999 Configuration written to '/etc/gated.ami'
localhost#quit

```

Dynamic Routing on GWb

```

----- Launch the Dynamic Routing Module

```



```
[GWb]# expert
Enter expert password:

You are in expert mode now.

[Expert@GWb]# cligated
localhost>enable
localhost#configure terminal
----- Enable OSPF and provide an OSPF router ID
localhost(config)#router ospf 1
localhost(config-router-ospf)#router-id 180.180.1.1
----- Define interfaces/IP's on which OSPF runs (Use
the cluster IP as defined in topology) and the area ID for
the interface/IP
localhost(config-router-ospf)#network 10.0.1.10 0.0.0.0
area 0.0.0.0
localhost(config-router-ospf)#network 10.0.0.3 0.0.0.0 area
0.0.0.0
----- Redistribute kernel routes (this is only here as
an example, please see the dynamic routing book for more
specific commands concerning redistribution of routes)
localhost(config-router-ospf)#redistribute kernel
localhost(config-router-ospf)#exit
localhost(config)#exit
----- Write configuration to disk
localhost#write memory
IU0 999 Configuration written to '/etc/gated.ami'
localhost#quit
```

Dynamic Routing on GWC

```
----- Launch the Dynamic Routing Module
[GWc]# expert
Enter expert password:

You are in expert mode now.

[Expert@GWc]# cligated
localhost>enable
localhost#configure terminal
----- Enable OSPF and provide an OSPF router ID
localhost(config)#router ospf 1
localhost(config-router-ospf)#router-id 190.190.1.1
----- Define interfaces/IP's on which OSPF runs (Use
the cluster IP as defined in topology) and the area ID for
the interface/IP
localhost(config-router-ospf)#network 10.0.1.20 0.0.0.0
area 0.0.0.0
localhost(config-router-ospf)#network 10.0.0.2 0.0.0.0 area
0.0.0.0
----- Redistribute kernel routes (this is only here as
an example, please see the dynamic routing book for more
specific commands concerning redistribution of routes)
localhost(config-router-ospf)#redistribute kernel
localhost(config-router-ospf)#exit
localhost(config)#exit
----- Write configuration to disk
localhost#write memory
IU0 999 Configuration written to '/etc/gated.ami'
localhost#quit
```

Configuring Anti-Spoofing on VTIs

In SmartDashboard:

1. Select **Manage > Network Objects**.
2. Select the Check Point Security Gateway and right click **Edit**.
3. In the Properties list, click **Topology**.
4. Click **Get > Interfaces** to read the interface information on the Security Gateway machine.
5. Select an interface, and click **Edit**.
6. In the Interface Properties window, click **Topology**.
7. In the **IP Addresses behind peer Security Gateway that are within reach of this interface** section, select:
 - **Not Defined** to accept all traffic.
 - **Specific** to choose a particular network. The IP addresses in this network will be the only addresses accepted by this interface.
8. In the **Perform Anti-Spoofing based on interface topology** section, select **Don't check packets from:** to ensure anti-spoof checks do not take place for addresses from certain internal networks coming into the external interface. Define a network object that represents those internal networks with valid addresses, and from the drop-down list, select that network object.
Objects selected in the **Don't check packets from:** drop-down menu are disregarded by the anti-spoofing enforcement mechanism.
9. Under **Spoof Tracking** select **Log**, and click **OK**.

Configuring a Loopback Interface

When a VTI connects an IPSO machine and a SecurePlatform machine, a loopback interface must be configured and defined in the Topology tab of the Security Gateway.

In IPSO Network Voyager:

1. Login and the IPSO homepage appears.
2. Click **Interface Configuration**.
3. On the **Configuration** page, click **Interfaces**.
4. On the **Interface Configuration** page, click **loop0**.
5. On the **Physical Interface loop0** page, enter an IP address in the **Create a new loopback interface with IP address** field and the value '30' in the **Reference mask length** field.
6. Click **Apply**.
The **Physical Interface loop0** page refreshes and displays the newly configured loopback interface.
7. Click **Save**.

Configuring Unnumbered VTIs

The IPSO platform supports unnumbered VTIs in a VRRP HA configuration, active-passive mode only.

If the VPN Tunnel Interface is unnumbered, local and remote IP addresses are not configured. This interface is associated with a proxy interface from which the virtual interface inherits an IP address. Traffic initiated by the Security Gateway and routed through the virtual interface will have the physical interface's IP Address as the source IP.

Working with unnumbered interfaces eliminates the need to assign two IP addresses per interface (the local IP, and the remote IP Address), and the need to synchronize this information among the peers.

Unnumbered interfaces are only supported on the IPSO 3.9 and higher platforms.

In IPSO Network Voyager:

1. Login.
2. Click **Config**.
3. On the **Configuration** page, click **Check Point Firewall-1**.
4. On the next page, click **FWVPN Configuration**.

5. On the **FWVPN Tunnel Configuration** page, enter the name of the Security Gateway you want to connect to in the **Peer GW Object Name** field.
Select a proxy interface from the **Proxy** drop down menu.
6. Click **Apply**.
7. The new interface is now listed on the **FWVPN Tunnel Configuration** page.

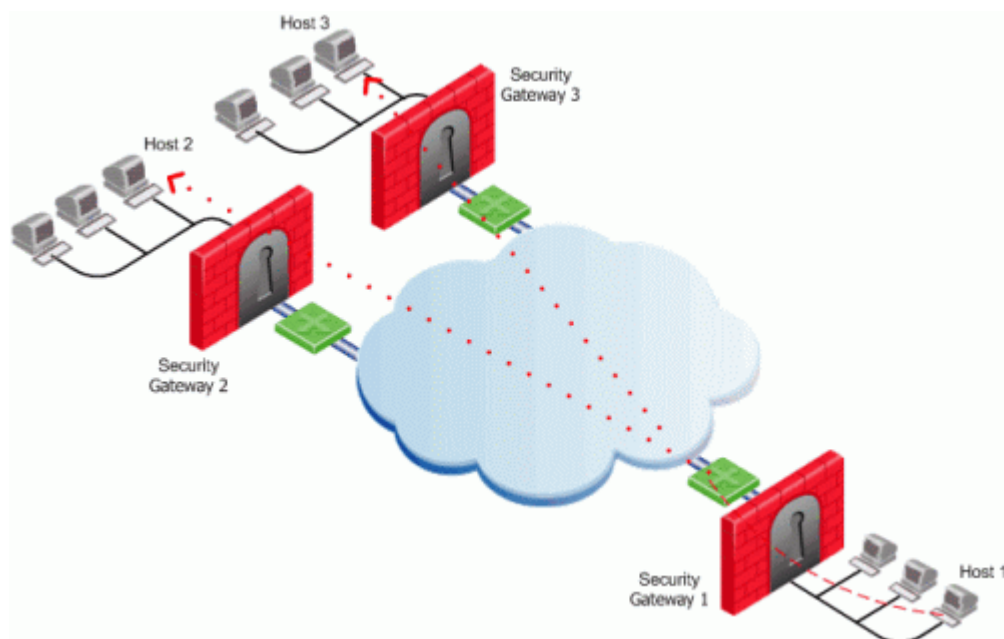
Routing Multicast Packets Through VPN Tunnels

Multicast is used to transmit a single message to a select group of recipients. IP Multicasting applications send one copy of each datagram (IP packet) and address it to a group of computers that want to receive it. This technique addresses datagrams to a group of receivers (at the multicast address) rather than to a single receiver (at a unicast address). The network is responsible for forwarding the datagrams to only those networks that need to receive them. For more information on Multicasting, see "Multicast Access Control" in the *R75.40 Firewall Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk67581>).

Multicast traffic can be encrypted and forwarded across VPN tunnels that were configured using VPN tunnel interfaces (virtual interfaces associated with the same physical interface). All participant Security Gateways, both on the sending and receiving ends, must have a virtual interface for each VPN tunnel and a multicast routing protocol must be enabled on all participant Security Gateways.

For more information on virtual interfaces, see *Configuring a Virtual Interface Using the VPN Shell* (on page 289).

In the figure:



- Security Gateway 1 has a virtual interface configured for the VPN tunnel linked with Security Gateway 2 and another virtual interface for the VPN tunnel linked with Security Gateway 3.
- Host 1 behind Security Gateway 1 initiates a multicast session destined to the multicast group address which consists of Host 2 behind Security Gateway 2 and to Host 3 behind Security Gateway 3.

To enable multicast service on a Security Gateway functioning as a rendezvous point, add a rule to the security policy of that Security Gateway to allow only the specific multicast service to be accepted unencrypted, and to accept all other services only through the community. Corresponding access rules enabling multicast protocols and services should be created on all participating Security Gateways. For example:

| Source | Destination | VPN | Service | Action | Track |
|--------------------|--------------------|-------------|-------------|--------|-------|
| Multicast_Gateways | Multicast_Gateways | Any Traffic | igmp pim | accept | log |

| Source | Destination | VPN | Service | Action | Track |
|-------------|-------------------------|------------------|-------------------------|--------|-------|
| Sample_Host | Multicast_Group_Address | Sample_Community | Multicast_Service_Group | accept | log |

Chapter 7

Tunnel Management

In This Chapter

[Overview of Tunnel Management](#)

77

[Configuring Tunnel Features](#)

79

Overview of Tunnel Management

A Virtual Private Network (VPN) provides a secure connection, typically over the Internet. VPNs accomplish this by creating an encrypted tunnel that provides the same security available as in a private network. This allows workers who are in the field or working at home to securely connect to a remote corporate server and also allows companies to securely connect to branch offices and other companies over the Internet. The VPN tunnel guarantees:

- authenticity, by using standard authentication methods.
- privacy, by encrypting data.
- integrity, by using standard integrity assurance methods.

Types of tunnels and the number of tunnels can be managed with the following features:

- *Permanent Tunnels* - This feature keeps VPN tunnels active allowing real-time monitoring capabilities.
- *VPN Tunnel Sharing* - This feature provides greater interoperability and scalability between Security Gateways. It also controls the number of VPN tunnels created between peer Security Gateways.

The status of all VPN tunnels can be viewed in SmartView Monitor. For more information on monitoring see the *Monitoring Tunnels* chapter in the *R75.40 SmartView Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk67581>).

Permanent Tunnels

As companies have become more dependent on VPNs for communication to other sites, uninterrupted connectivity has become more crucial than ever before. Therefore it is essential to make sure that the VPN tunnels are kept up and running. Permanent Tunnels are constantly kept active and as a result, make it easier to recognize malfunctions and connectivity problems. Administrators can monitor the two sides of a VPN tunnel and identify problems without delay.

Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. A VPN tunnel is monitored by periodically sending "tunnel test" packets. As long as responses to the packets are received the VPN tunnel is considered "up." If no response is received within a given time period, the VPN tunnel is considered "down." Permanent Tunnels can only be established between Check Point Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:

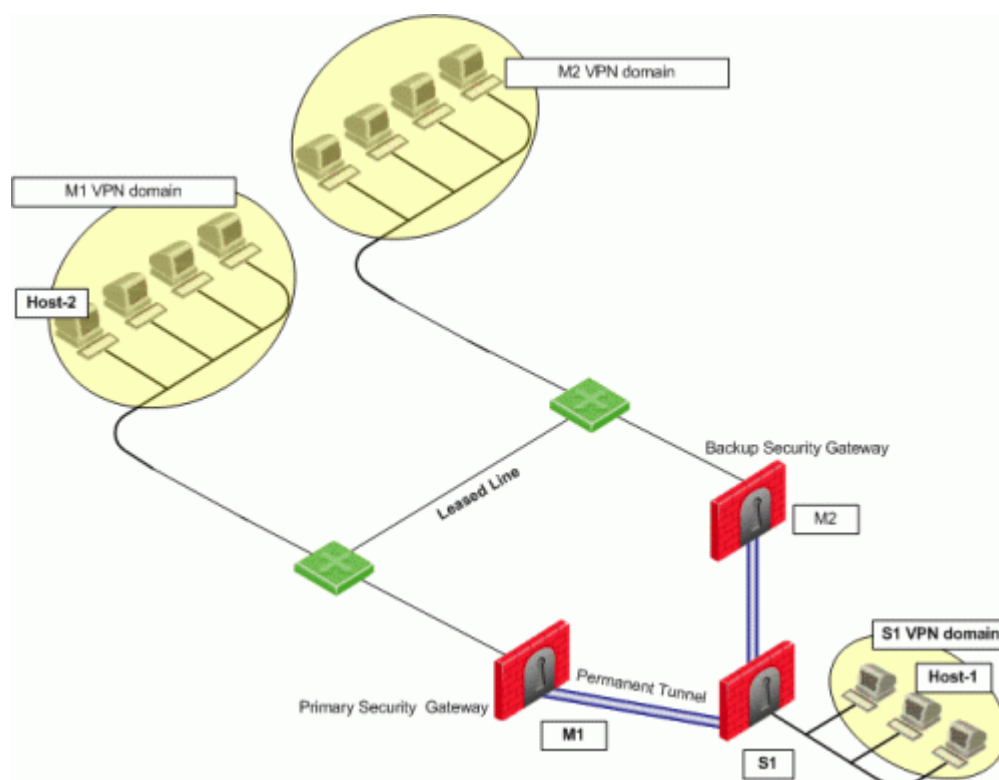
- Can be specified for an entire community. This option sets every VPN tunnel in the community as permanent.
- Can be specified for a specific Security Gateway. Use this option to configure specific Security Gateways to have permanent tunnels.
- Can be specified for a single VPN tunnel. This feature allows configuring specific tunnels between specific Security Gateways as permanent.

Permanent Tunnels in a MEP Environment

In a *Multiple Entry Point* (MEP) environment, VPN tunnels that are active are rerouted from the predefined primary Security Gateway to the backup Security Gateway if the primary Security Gateway becomes unavailable. When a Permanent Tunnel is configured between Security Gateways in a MEPed environment where RIM is enabled, the satellite Security Gateways see the center Security Gateways as "unified." As a

result, the connection will not fail but will fail over to another center Security Gateway on a newly created permanent tunnel. For more information on MEP see Multiple Entry Point VPNs (on page 117).

In this scenario:



- Host 1, residing behind Security Gateway S1, is communicating through a Permanent Tunnel with Host 2, residing behind Security Gateway M1.
- M1 and M2 are in a MEPed environment.
- M1 and M2 are in a MEPed environment with Route Injection Mechanism (RIM) enabled.
- M1 is the Primary Security Gateway and M2 is the Backup Security Gateway.

In this case, should Security Gateway M1 become unavailable, the connection would continue through a newly created permanent tunnel between S1 and M2.

Tunnel Testing for Permanent Tunnels

Tunnel test is a proprietary Check Point protocol that is used to test if VPN tunnels are active. A packet has an arbitrary length, with only the first byte containing meaningful data - this is the 'type' field.

The 'type' field can take any of the following values:

- Test
- Reply
- Connect
- Connected

Tunnel testing requires two Security Gateways - one configured as a pinger and one as a responder. A pinger Security Gateway uses the VPN daemon to send encrypted "tunnel testing" packets to Security Gateways configured to listen for them. A responder Security Gateway is configured to listen on port 18234 for the special tunnel testing packets.

The pinger sends type 1 or 3. The responder sends a packet of identical length with type 2 or 4 respectively. During the 'connect' phase, "tunnel test" is used in two ways:

1. A 'connect' message is sent to the Security Gateway. Receipt of a 'connected' message is the indication that the connection succeeded. The 'connect' messages are retransmitted for up to 10 seconds after the IKE negotiation is over if no response is received.

2. A series of 'test' messages with various lengths is sent so as to discover the PMTU (Path Maximum Transmission Unit) of the connection. This may also take up to 10 seconds. This test is executed to ensure that TCP packets that are too large are not sent. TCP packets that are too large will be fragmented and slow down performance.

Security Gateways with version R54 and forward can be either a pinger or responder. In a MEP environment, center Security Gateways can only be responders.

Security Gateways with Embedded NG 5.0 and forward can be pingers or responders. Older versions of this software can only be responders.

3rd party Security Gateways cannot be a pinger or responder.

VPN Tunnel Sharing

Since various vendors implement IPSec tunnels using a number of different methods, administrators need to cope with different means of implementation of the IPSec framework.

VPN Tunnel Sharing provides interoperability and scalability by controlling the number of VPN tunnels created between peer Security Gateways. There are three available settings:

- **One VPN tunnel per each pair of hosts**
- **One VPN tunnel per subnet pair**
- **One VPN tunnel per Security Gateway pair**

Configuring Tunnel Features

To configure Tunnel Management options, proceed as follows:

1. In SmartDashboard, click **Manage > VPN Communities**. The **VPN Communities** window will appear.
2. Select the community (star or meshed) to be configured and click **Edit...**
3. Click **Tunnel Management**.

The **Tunnel Management** window is displayed.

- for Permanent Tunnels, see Permanent Tunnels (on page 77).
- for Tracking, see Tracking Options (on page 80).
- for VPN Tunnel Sharing, see VPN Tunnel Sharing (on page 80).

Permanent Tunnels

In the **Community Properties** window on the **Tunnel Management** page, select **Set Permanent Tunnels** and the following Permanent Tunnel modes are then made available:

- **On all tunnels in the community**
- **On all tunnels of specific Security Gateways**
- **On specific tunnels in the community**

To configure all tunnels as permanent, select **On all tunnels in the community**. Clear this option to terminate all Permanent Tunnels in the community.

To configure On all tunnels of specific Security Gateways:

1. Select **On all tunnels of specific Security Gateways** and click **Select Security Gateways**.
The **Select Security Gateways** window is displayed.
To terminate Permanent Tunnels connected to a specific Security Gateway, highlight the Security Gateway and click **Remove**.
2. To configure the Tracking options for a specific Security Gateway, highlight a Security Gateway and click on **Security Gateway Tunnels Properties**.

To configure On specific tunnels in the community:

1. Select **On specific tunnels in the community** and click **Select Permanent Tunnels**.
The **Select Permanent Tunnels** window opens.
2. Click in the cell that intersects the Security Gateways where a permanent tunnel is required.

3. Click **Selected Tunnel Properties** and the **Tunnel Properties** window is displayed.
To terminate the Permanent Tunnel between these two Security Gateways, clear **Set these tunnels to be permanent tunnels**.
4. Click **OK**.

Advanced Permanent Tunnel Configuration

In SmartDashboard:

1. Click **Policy > Global Properties**.
The **Global Properties** window is displayed.
2. Select **SmartDashboard Customization** from the properties list.
3. In the **Advanced Configuration** section, click **Configure**.
The **Advanced configuration** window is displayed.
4. Click **VPN Advanced Properties > Tunnel Management** to view the five attributes that may be configured to customize the amount of tunnel tests sent and the intervals in which they are sent:
 - **life_sign_timeout** - Designate the amount of time the tunnel test runs without a response before the peer host is declared 'down.'
 - **life_sign_transmitter_interval** - Set the time between tunnel tests.
 - **life_sign_retransmissions_count** - When a tunnel test does not receive a reply, another test is resent to confirm that the peer is 'down.' The Life Sign Retransmission Count is set to how many times the tunnel test is resent without receiving a response.
 - **life_sign_retransmissions_interval** - Set the time between the tunnel tests that are resent after it does not receive a response from the peer.
 - **cluster_status_polling_interval** - (Relevant for HA Clusters only) - Set the time between tunnel tests between a primary Security Gateway and a backup Security Gateway. The tunnel test is sent by the backup Security Gateway. When there is no reply, the backup Security Gateway will become active.

Tracking Options

Several types of alerts can be configured to keep administrators up to date on the status of the VPN tunnels. The Tracking settings can be configured on the **Tunnel Management** page of the **Community Properties** screen for all VPN tunnels or they can be set individually when configuring the permanent tunnels themselves. The different options are **Log**, **Popup Alert**, **Mail Alert**, **SNMP Trap Alert**, and **User Defined Alert**. Choosing one of these alert types will enable immediate identification of the problem and the ability to respond to these issues more effectively.

Terminating Permanent Tunnels

Once a Permanent Tunnel is no longer required, the tunnel can be shut down. Permanent Tunnels are shut down by deselecting the configuration options to make them active and re-installing the policy.

VPN Tunnel Sharing

For a VPN community, the configuration is set on the **Tunnel Management** page of the **Community Properties** window.

For a specific Security Gateway, the configuration is set on the **VPN Advanced** page of the Security Gateway's properties window.

VPN Tunnel Sharing provides greater interoperability and scalability by controlling the number of VPN tunnels created between peer Security Gateways. Configuration of VPN Tunnel Sharing can be set on both the VPN community and Security Gateway object.

- **One VPN Tunnel per each pair of hosts** - A VPN tunnel is created for every session initiated between every pair of hosts.
- **One VPN Tunnel per subnet pair** - Once a VPN tunnel has been opened between two subnets, subsequent sessions between the same subnets will share the same VPN tunnel. This is the default setting and is compliant with the IPsec industry standard.

- **One VPN Tunnel per Security Gateway pair**- One VPN tunnel is created between peer Security Gateways and shared by all hosts behind each peer Security Gateway.

In case of a conflict between the tunnel properties of a VPN community and a Security Gateway object that is a member of that same community, the "stricter" setting is followed. For example, a Security Gateway that was set to **One VPN Tunnel per each pair of hosts** and a community that was set to **One VPN Tunnel per subnet pair**, would follow **One VPN Tunnel per each pair of hosts**.

Chapter 8

Route Injection Mechanism

In This Chapter

| | |
|--|----|
| Overview of Route Injection | 82 |
| Automatic RIM | 82 |
| Custom Scripts | 83 |
| Injecting Peer Security Gateway Interfaces | 85 |
| Configuring RIM | 85 |
| Configuring RIM on Gaia | 87 |

Overview of Route Injection

Route Injection Mechanism (RIM) enables a Security Gateway to use dynamic routing protocols to propagate the encryption domain of a VPN peer Security Gateway to the internal network and then initiate back connections. When a VPN tunnel is created, RIM updates the local routing table of the Security Gateway to include the encryption domain of the VPN peer.

RIM can only be enabled when permanent tunnels are configured for the community. Permanent tunnels are kept alive by tunnel test packets. When a Security Gateway fails to reply, the tunnel will be considered 'down.' As a result, RIM will delete the route to the failed link from the local routing table, which triggers neighboring dynamic routing enabled devices to update their routing information accordingly. This will result in a redirection of all traffic destined to travel across the VPN tunnel, to a pre-defined alternative path.

There are two possible methods to configure RIM:

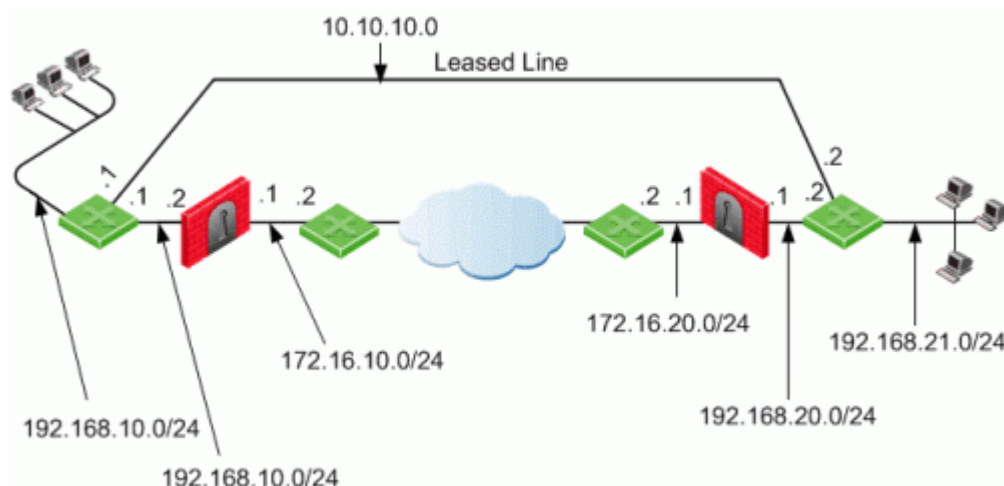
- Automatic RIM - RIM automatically injects the route to the encryption domain of the peer Security Gateways.
- Custom Script - Specify tasks for RIM to perform according to specific needs.

Route injection can be integrated with MEP functionality (which route return packets back through the same MEP Security Gateway). For more information on MEP, see Multiple Entry Point VPNs (on page 117).

Automatic RIM

Automatic RIM can be enabled using the GUI when the operating system on the Security Gateway is SecurePlatform, IPSO or Linux. Although a custom script can be used on these systems, no custom-written scripts are required.

In this scenario:



- Security Gateways 1 and 2 are both RIM and have a dynamic routing protocol enabled.
- R1 and R4 are enabled routers.
- When a VPN tunnel is created, RIM updates the local routing tables of Security Gateway 1 and gateway 2 to include the encryption domain of the other Security Gateway.
- Should the VPN tunnel become unavailable, traffic is redirected to the leased line.

The routing tables for the Security Gateways and routers read as follows. Entries in bold represent routes injected into the Security Gateways local routing tables by RIM:

For Security Gateway 1:

| Destination | Netmask | Security Gateway | Metric |
|---------------------|----------------------|--------------------|----------|
| 0.0.0.0 | 0.0.0.0 | 172.16.10.2 | 1 |
| 192.168.21.0 | 255.255.255.0 | 172.16.10.2 | 1 |
| 192.168.11.0 | 255.255.255.0 | 192.168.10.1 | 1 |

Security Gateway 2:

| Destination | Netmask | Security Gateway | Metric |
|---------------------|----------------------|--------------------|----------|
| 0.0.0.0 | 0.0.0.0 | 172.16.20.2 | 1 |
| 192.168.11.0 | 255.255.255.0 | 172.16.20.2 | 1 |
| 192.168.21.0 | 255.255.255.0 | 192.168.20.1 | 1 |

R1 (behind Security Gateway 1):

| Destination | Netmask | Security Gateway | Metric |
|--------------|---------------|------------------|--------|
| 0.0.0.0 | 0.0.0.0 | 192.168.10.2 | 1 |
| 192.168.21.0 | 255.255.255.0 | 192.168.10.2 | 1 |
| 192.168.21.0 | 255.255.255.0 | 0.10.10.2 | 2 |

R4 (behind Security Gateway 2):

| Destination | Netmask | Security Gateway | Metric |
|--------------|---------------|------------------|--------|
| 0.0.0.0 | 0.0.0.0 | 192.168.20.2 | 1 |
| 192.168.11.0 | 255.255.255.0 | 192.168.20.2 | 1 |
| 192.168.11.0 | 255.255.255.0 | 10.10.10.1 | 2 |

Custom Scripts

Custom scripts can be run on any Security Gateway in the community. These scripts are executed whenever a tunnel changes its state, i.e. goes "up" or "down." Such an event, for example, can be the trigger that initiates a dial-up connection.

A script template **custom_rim** (with a **.sh** or **.bat** extension depending on the operating system) is provided in the **\$FWDIR/Scripts** directory. The basic script (for SecurePlatform, IPSO, or Linux only):

Sample customized script for SecurePlatform, IPSO, or Linux

```
#!/bin/sh

# This script is invoked each time a tunnel is configured
# with the RIM option
# and the tunnel changed state.
#
# You may add your custom commands to be invoked here.

# Parameters read from command line.
RIM_PEER_Security_Gateway=$1
RIM_NEW_STATE=$2
RIM_HA_STATE=$3
RIM_FIRST_TIME=$4
RIM_PEER_ENC_NET=$5

case "${RIM_NEW_STATE}" in
    up)
        # Place your action for tunnels that came up
        ;;
    down)
        # Place your action for tunnel that went down
        ;;
esac
```

For Windows platforms, the script takes the form of a batch file:

Sample customized script for Windows

```
@echo off

rem . This script is invoked each time a tunnel is
rem . configured with the RIM option
rem . and the tunnel changed state.
rem .
rem . You may add your custom commands to be invoked here.

rem . Parameters read from command line.
set RIM_PEER_Security_Gateway=%1
set RIM_NEW_STATE=%2
set RIM_HA_STATE=%3
set RIM_FIRST_TIME=%4
set RIM_PEER_ENC_NET=%5

goto RIM_%RIM_NEW_STATE%

:RIM_up
rem . Place your action for tunnels that came up
goto end

:RIM_down
rem . Place your action for tunnel that went down
goto end

:end
```

Where:

- RIM_PEER_Security_Gateway: Peer Security Gateway
- RIM_NEW_STATE: Change in the state of the Security Gateway, i.e. up or down.
- RIM_HA_STATE: State of a single Security Gateway in a cluster (i.e., standby or active).
- RIM_FIRST_TIME: The script is executed separately for each network within the peer's encryption domain. Although the script might be executed multiple times on a peer, this parameter will only be transferred to the script with the value of '1' the first time the script runs on the peer. The value '1' indicates that this is the first time this script is being executed. The next time the script is executed, it is

transferred with the value of '0' and the parameter is disregarded. For example, you may send an email alert to the system administrator the moment a tunnel goes down.

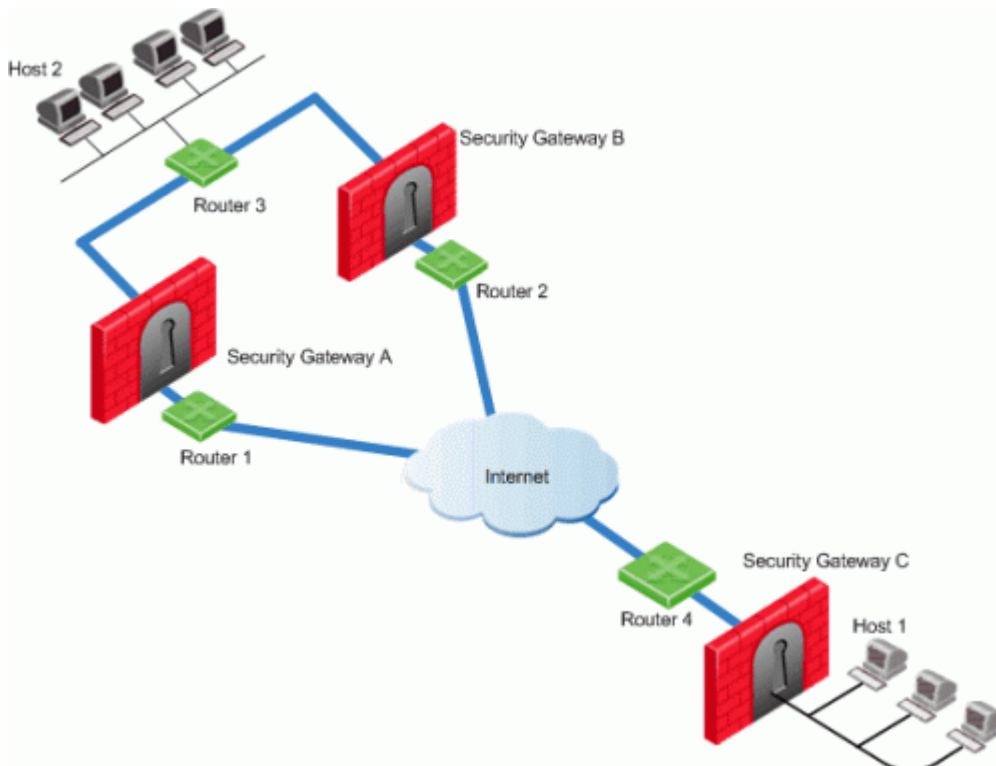
- `RIM_PEER_ENC_NET`: VPN domain of the VPN peer.

Injecting Peer Security Gateway Interfaces

The `RIM_inject_peer_interfaces` flag is used to inject into the routing tables the IP addresses of the peer Security Gateway in addition to the networks behind the Security Gateway.

For example, after a VPN tunnel is created, RIM injects into the local routing tables of both Security Gateways, the encryption domain of the peer Security Gateway. However, when RIM enabled Security Gateways communicate with a Security Gateway that has Hide NAT enabled, the peer's interfaces need to be injected as well.

In this scenario:



- Security Gateways A and B are both RIM enabled and Security Gateway C has Hide NAT enabled on the external interface ("hiding" all the IP addresses behind it).
- Host 1, behind Security Gateway C, initiates a VPN tunnel with Host 2, through Security Gateway A.
- Router 3 holds routes to all the hosts behind Security Gateway C. Router 3 however, does not have the Hide NAT IP address of Security Gateway C and as a result, cannot properly route packets back to host 1.

This solution for routing the packets back properly is twofold:

1. Select the flag `RIM_inject_peer_interfaces` in the **Global Properties** page. This flag will inject router 3 with all of the IP addresses of Security Gateway C including the Hide NAT address.
2. Configure the router not to propagate the information injected to other Security Gateways. If the router is not configured properly, using the example in Figure 8-4, could result in Security Gateway B routing traffic to Security Gateway C through Security Gateway A.

Configuring RIM

Configuring RIM in a Star Community:

1. Open the **Star Community properties > Tunnel Management** page.

2. In the **Permanent Tunnels** section, select **Set Permanent Tunnels**. The following Permanent Tunnel modes are then made available:
 - **On all tunnels in the community**
 - **On all tunnels of specific Security Gateways**
 - **On specific tunnels in the community**

For more information on these options, see Permanent Tunnels (on page 77).

When choosing tunnels, keep in mind that RIM can only be enabled on tunnels that have been configured to be permanent. **On all tunnels in the community** must be selected if MEP is enabled on the community. To configure permanent tunnels, see Configuring Tunnel Features (on page 79).

1. Select **Enable Route Injection Mechanism (RIM)**.

2. Click **Settings...**

The **Route Injection Mechanism** Settings window opens

Decide if:

- RIM should run automatically on the central or satellite Security Gateways (SecurePlatform, IPSO or Linux only).
- A customized script should be run on central or satellite Security Gateways whenever a tunnel changes its states (goes up or down).

For tracking options, see Tracking Options (on page 80).

3. If a customized script is run, edit **custom_rim** (.sh or .bat) script in the **\$FWDIR/Scripts** directory on each of the Security Gateways.

Configuring RIM in a Meshed Community:

1. Open the **Meshed Community properties > Tunnel Management** page.

In the **Permanent Tunnels** section, select **Set Permanent Tunnels**. The following Permanent Tunnel modes are then made available:

- **On all tunnels in the community**
- **On all tunnels of specific Security Gateways**
- **On specific tunnels in the community**

For more information on these options, see Permanent Tunnels (on page 77).

When choosing tunnels, keep in mind that RIM can only be enabled on tunnels that have been configured to be permanent. To configure permanent tunnels, see Configuring Tunnel Features (on page 79).

1. Select **Enable Route Injection Mechanism (RIM)**.

2. Click **Settings...**

The **Route Injection Mechanism** Settings window open

Decide if:

- RIM should run automatically on the Security Gateways (SecurePlatform, IPSO or Linux only).
- A customized script should be run on the Security Gateway whenever a tunnel changes its state (goes up or down).

For tracking options, see Tracking Options (on page 87).

3. If a customized script is run, edit **custom_rim** (.sh or .bat) script in the **\$FWDIR/Scripts** directory on each of the Security Gateways.

Enabling the RIM_inject_peer_interfaces flag

To enable the RIM_inject_peer_interfaces flag:

1. In SmartDashboard, click **Policy > Global Properties**.
2. Go to **SmartDashboard Customization > Configure > VPN Advanced Properties > Tunnel Management**.
3. Select **RIM_inject_peer_interfaces**.
4. Click **OK**.

Tracking Options

Several types of alerts can be configured to keep administrators up to date on the status of Security Gateways. The Tracking settings can be configured on the **Route Injection Mechanism Settings** page. The different options are **Log**, **Popup Alert**, **Mail Alert**, **SNMP Trap Alert**, and **User Defined Alert**.

Configuring RIM on Gaia

In Gaia, the Route Injection Mechanism adds routes directly to the kernel. For the routes to remain in the Kernel, you must configure this option.

To set kernel routes using the CLI:

1. Run: `set kernel-routes on.`
2. Run: `save config.`

To set kernel routes using the WebUI:

1. In the tree view, click **Advanced Routing > Routing Options**.
2. In the **Kernel Options** area, select the **Kernel Routes** option.
3. Click **Apply**.

Gaia Gateways in a Star VPN Community

For RIM to work, the Gaia gateways in a star VPN community must publish the routes of the satellite networks to the router. For Gaia gateways to publish routes, run these CLI commands on all gateways at the center of the community:

1. `set routemap <Routemap Name> id <ID Number>`
For example:
`set routemap RIM id 5`
2. `set routemap <Routemap Name> id <ID Number> match protocol kernel`
For example:
`set routemap RIM id 5 match protocol kernel`
3. `Set ospf export-routemap <Routemap Name> preference 1 on`
For example:
`set ospf export-routemap RIM preference 1 on`
4. `set routemap <Routemap Name> id <ID Number> allow`
For example:
`set routemap RIM id 5 allow`
5. `set routemap <Routemap Name> id <ID Number> on`
For example:
`set routemap RIM2 id 10 on`
6. `set routemap <Routemap Name> id <ID Number> match nexthop <IP of OSPF Interface of the other RIM GW> on`
For example:
`set routemap RIM2 id 10 match nexthop <10.16.50.3> on`
7. `set routemap <Routemap Name> id <ID Number> restrict`
For example:
`set routemap RIM2 id 10 restrict`
8. `set ospf import-routemap <Routemap Name> preference 1 on`
For example:
`set ospf import-routemap RIM2 preference 1 on`
9. `save config`

Chapter 9

Wire Mode

In This Chapter

| | |
|--------------------------------------|----|
| Overview of Wire Mode | 88 |
| Wire Mode Scenarios | 88 |
| Special Considerations for Wire Mode | 91 |
| Configuring Wire Mode | 91 |

Overview of Wire Mode

Wire Mode improves connectivity by allowing existing connections to fail over successfully by bypassing firewall enforcement. Traffic within a VPN community is, by definition, private and secure. In many cases, the firewall and the rule on the firewall concerning VPN connections is unnecessary. Using *Wire Mode*, the firewall can be bypassed for VPN connections by defining internal interfaces and communities as "trusted".

When a packet reaches a Security Gateway, the Security Gateway asks itself two questions regarding the packet(s):

Is this information coming from a "trusted" source?

Is this information going to a "trusted" destination?

If the answer to both questions is yes, and the VPN Community to which both Security Gateways belong is designated as "*Wire Mode* enabled," stateful inspection is not enforced and the traffic between the trusted interfaces bypasses the firewall. Since no stateful inspection takes place, no packets can be discarded. The VPN connection is no different from any other connection along a dedicated wire. This is the meaning of "*Wire Mode*." Since stateful inspection no longer takes place, dynamic routing protocols (which do not survive state verification in non-wire mode configuration) can now be deployed. *Wire Mode* thus facilitates Route Based VPN. For information on Route Based VPN, see Route Based VPN (on page 61).

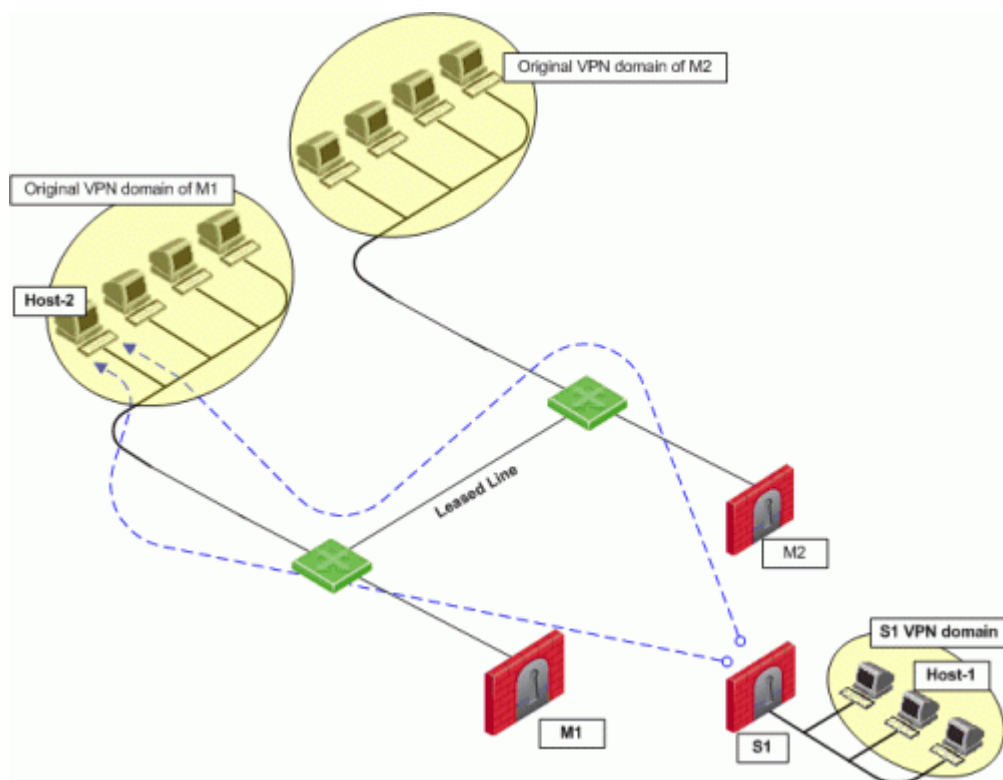
Wire Mode is supported for NGX (R60) Security Gateways and forward.

Wire Mode Scenarios

Wire mode can be used to improve connectivity and performance in different infrastructures. This section describes scenarios that benefit from the implementation of wire mode.

Wire Mode in a MEP Configuration

In this scenario:

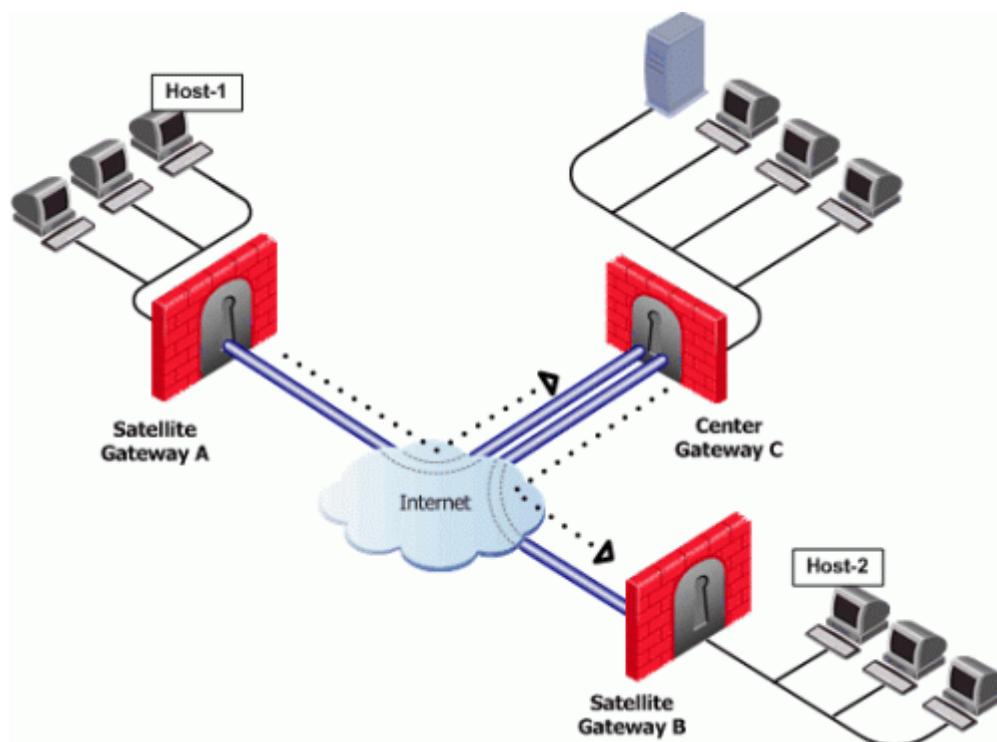


- Security Gateway M1 and Security Gateway M2 are both wire mode enabled and have trusted internal interfaces.
- The community where Security Gateway M1 and Security Gateway M2 reside, is wire mode enabled.
- Host 1, residing behind Security Gateway S1 is communicating through a VPN tunnel with Host 2 residing behind Security Gateway M1.
- MEP is configured for Security Gateway M1 and Security Gateway M2 with Security Gateway M1 being the primary Security Gateway and Security Gateway M2 as the backup. For more information on MEP see, Multiple Entry Point VPNs (on page 117).

In this case, if Security Gateway M1 goes down, the connection fails over to Security Gateway M2. A packet leaving Host 2 will be redirected by the router behind Security Gateway M1 to Security Gateway M2 since Security Gateway M2 is designated as the backup Security Gateway. Without wire mode, stateful inspection would be enforced at Security Gateway M2 and the connection would be dropped because packets that come into a Security Gateway whose session was initiated through a different Security Gateway, are considered "out-of-state" packets. Since Security Gateway M2's internal interface is "trusted," and wire mode is enabled on the community, no stateful inspection is performed and Security Gateway M2 will successfully continue the connection without losing any information.

Wire Mode with Route Based VPN

In this scenario:



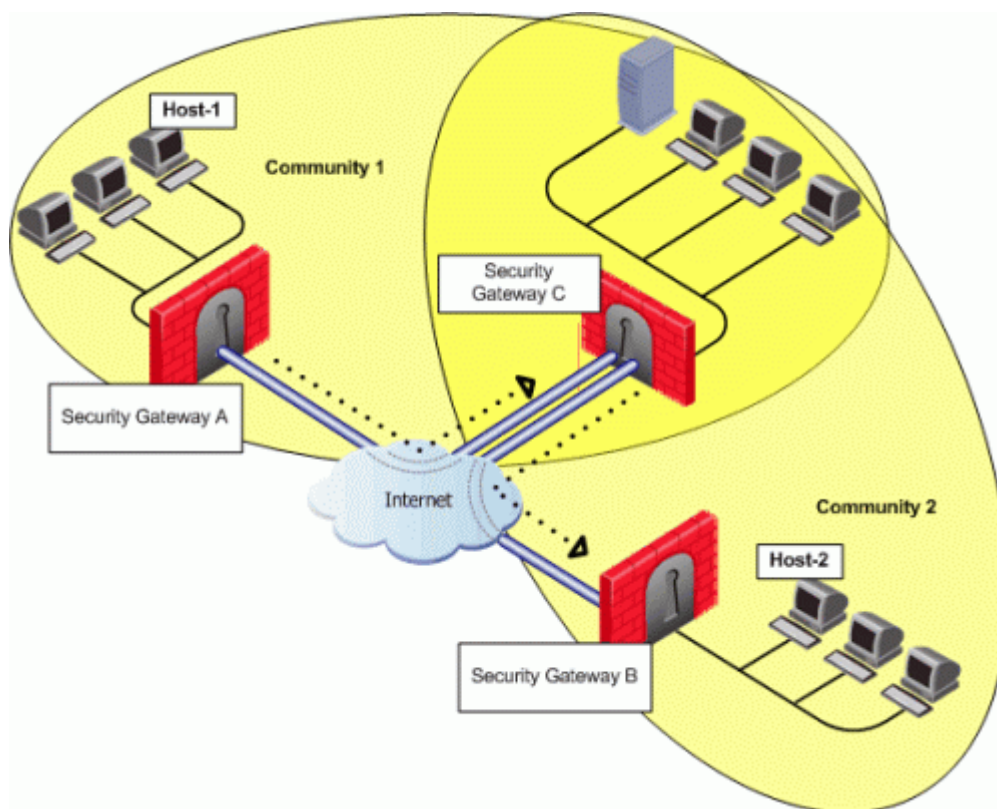
- Wire mode is enabled on Center Security Gateway C (without an internal trusted interface specified).
- The community is wire mode enabled.
- Host 1 residing behind Satellite Security Gateway A wishes to open a connection through a VPN tunnel with Host 2 behind Satellite Security Gateway B.

In a satellite community, Center Security Gateways are used to route traffic between Satellite Security Gateways within the community.

In this case, traffic from the Satellite Security Gateways is only rerouted by Security Gateway C and cannot pass through Security Gateway C's firewall. Therefore, stateful inspection does not need to take place at Security Gateway C. Since wire mode is enabled on the community and on Security Gateway C, making them trusted, stateful inspection is bypassed. Stateful inspection, however, does take place on Security Gateways A and B.

Wire Mode Between Two VPN Communities

In this scenario:



- Security Gateway A belongs to Community 1.
- Security Gateway B belongs to Community 2.
- Security Gateway C belongs to Communities 1 and 2.
- Wire mode is enabled on Center Security Gateway C (without an internal trusted interface specified).
- Wire mode is enabled on both communities.
- Host 1 residing behind Satellite Security Gateway A wishes to open a connection through a VPN tunnel with Host 2 behind Satellite Security Gateway B.

Wire mode can also be enabled for routing VPN traffic between two Security Gateways which are not members of the same community. Security Gateway C is a member of both communities and therefore recognizes both communities as trusted. When host 1 behind Security Gateway A initiates a connection to host 2 behind Security Gateway B, Security Gateway C is used to route traffic between the two communities. Since the traffic is not actually entering Security Gateway C, there is no need for stateful inspection to take place at that Security Gateway. Stateful inspection, however, does take place on Security Gateways A and B.

Special Considerations for Wire Mode

Wire mode is supported on SecurePlatform, IPSO, and Gaia platforms.

Configuring Wire Mode

Wire mode is configured in two places:

1. Community Properties (meshed or star)
2. Security Gateway Properties

Enabling Wire Mode on a VPN Community

1. In SmartDashboard, click **Manage > VPN Communities**. The **VPN Communities** window appears.

2. Select the community to be configured and click **Edit...**
3. Double-click **Advanced Settings** to view the various options.
4. Click **Wire Mode**.
The **Wire Mode** window opens.
5. To enable Wire Mode on the community, select **Allow uninspected encrypted traffic between Wire mode interfaces of the Community's members**.
6. To enable Wire Mode Routing, select **Wire Mode Routing - Allow members to route uninspected encrypted traffic in VPN routing configurations**.

Enabling Wire Mode on a Specific Security Gateway

1. In SmartDashboard, click **Manage > Network Objects**. The **Network Objects** window will appear.
2. Select the Security Gateway to be configured and click **Edit...**
3. Double-click **VPN** to expand **VPN** tree. Select the **VPN Advanced** to display the VPN Advanced window.
4. To enable Wire Mode on the Security Gateway, select **Support Wire Mode**.
5. Click **Add** to include the interfaces to be trusted by the selected Security Gateway.
6. Click **Log Wire mode traffic** to log wire mode activity.

Chapter 10

Directional VPN Enforcement

In This Chapter

| | |
|---|----|
| Overview of Directional VPN | 93 |
| Directional Enforcement within a Community | 93 |
| Configurable Objects in a Direction | 94 |
| Directional Enforcement between Communities | 95 |
| Configuring Directional VPN Within a Community | 95 |
| Configuring Directional VPN Between Communities | 96 |

Overview of Directional VPN

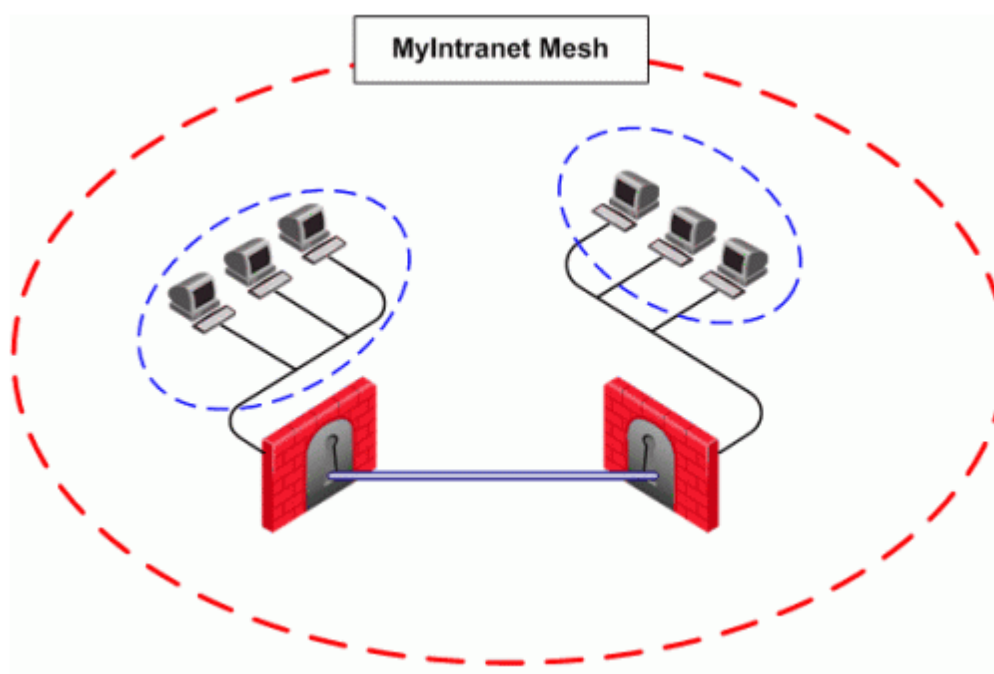
When a VPN community is selected in the VPN column of the Security Policy Rule Base, the source and destination IP addresses can belong to any of the Security Gateways in the community. In other words, the traffic is bidirectional; any of the Security Gateways can be the source of a connection, any of the Security Gateways can be the destination endpoint. But what if the administrator (in line with the company's security policy) wished to enforce traffic in one direction only? Or to allow encrypted traffic to or from Security Gateways *not* included in the VPN community? To enable enforcement within VPN communities, VPN implements Directional VPN.

Directional VPN specifies where the source address must be, and where the destination address must be. In this way, enforcement can take place:

- Within a single VPN community
- Between VPN communities

Directional Enforcement within a Community

The figure shows a simple meshed VPN community called *MyIntranet*. VPN traffic within the MyIntranet Mesh is bidirectional; that is, either of the Security Gateways (or the hosts behind the Security Gateways in the VPN domains) can be the source or destination address for a connection.










| Source | Destination | VPN | Service | Action | Track |
|--------|-------------|--|---------|--------|-------|
| Any | Any | MyIntranet => MyIntranet MyIntranet => internal_clear internal_clear => MyIntranet | telnet | accept | log |
| Any | Any | MyIntranet | telnet | accept | log |

The match conditions are represented by a series of compound objects. The match conditions enforce traffic in the following directions:

- To and from the VPN Community via VPN routing (**MyIntranet => MyIntranet**)
- From the Community to the local VPN domains (**MyIntranet => internal_clear**)
- From the local VPN domains to the VPN community (**internal_clear => MyIntranet**)

Configurable Objects in a Direction

The table shows all the objects that can be configured in a direction, including three new objects created for Directional VPN:

| Name of Object | Meaning |
|---|--|
|  Remote_Access_Community | Remote Access community |
|  SiteToSiteVPN | Regular Star/Mesh Community |
|  Any Traffic | Any traffic |
|  All_GwToGw | All Gateway to Gateway traffic |
|  All_Communities | All communities (new object) |
|  External_clear | For traffic outside the community |
|  Internal_clear | For traffic between local domains within the community |



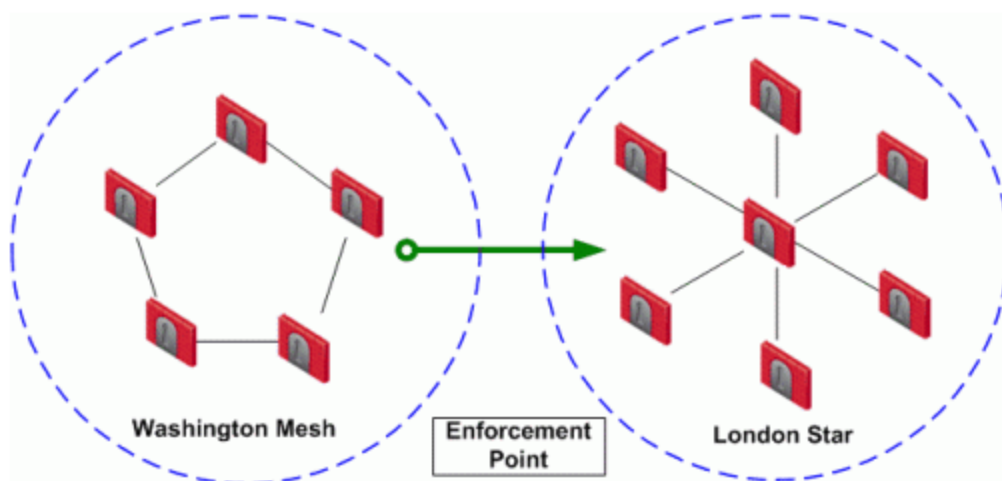
Note - Clear text connections originating from the following objects are not subject to enforcement:

- Any Traffic
- External_clear
- Internal_clear

There is *no limit* to the number of VPN directions that can be configured on a single rule. In general, if you have many directional enforcements, consider replacing them with a standard bidirectional condition.

Directional Enforcement between Communities

VPN Directional enforcement can take place between VPN communities. Consider two VPN communities, *Washington* and *London*:



| Source | Destination | VPN | Service | Action |
|--------|-------------|----------------------|---------|--------|
| Any | Any | Washington => London | Any | accept |

Washington is a Mesh community, and London is a VPN Star. In the VPN column of the Security Policy Rule Base, a directional VPN rule has been implemented. This means that for a VPN connection to match this rule, the source of the connection must be in the Washington Mesh, and the destination host must be within the London Star.

This does not mean that "return" or "back" connections are not allowed from London to Washington (the three-way handshake at the start of every TCP connection demands return connections), only that the *first packet* must originate within the Washington Mesh. If a host within the London Star tries to open a connection to a host in the Washington Mesh, the connection is dropped.

This directional enforcement does not affect the topology of either Washington or London. The enforcement can be thought of as taking place somewhere between the two communities.

Configuring Directional VPN Within a Community

To configure Directional VPN within a community:

1. In **Global Properties > VPN page > Advanced > Select Enable VPN Directional Match in VPN Column**.
2. In the VPN column of the appropriate rule, right-click on the VPN community. From the pop-up menu, select **Edit Cell...**
The **VPN Match Conditions** window opens.
3. Select **Match traffic in this direction only**, and click **Add...**
The **Directional VPN Match Condition** window opens.
4. In the **Match on traffic reaching the Security Gateway from:** drop-down box, select the object for **internal_clear**. (the source).
5. In the **Match on traffic leaving the Security Gateway to:** box, select the relevant community object (the destination).
6. Add another directional match in which the relevant community object is both the source and destination.
This allows traffic from the local domain to the community, and within the community.
7. Click **OK**.

Configuring Directional VPN Between Communities

To configure Directional VPN between communities:

1. In **Global Properties > VPN page > Advanced >** Select **Enable VPN Directional Match in VPN Column**.
2. Right-click inside the VPN column of the appropriate rule. From the pop-up menu, select **Edit Cell...** or **Add Direction...**
The **VPN Match Conditions** window opens.
3. Click **Add...**
The **Directional VPN Match Conditions** window opens:
4. From the drop-down box on the left, select the source of the connection.
5. From the drop-down box on the right, select the connection's destination.
6. Click **OK**.

Chapter 11

Link Selection

In This Chapter

| | |
|---|-----|
| Link Selection Overview | 97 |
| Configuring IP Selection by Remote Peer | 97 |
| Configuring Outgoing Route Selection | 99 |
| Configuring Source IP Address Settings | 101 |
| Outgoing Link Tracking | 101 |
| Link Selection Scenarios | 101 |
| Service Based Link Selection | 105 |
| Trusted Links | 109 |
| On Demand Links (ODL) | 112 |
| Link Selection and ISP Redundancy | 113 |
| Link Selection with non-Check Point Devices | 115 |

Link Selection Overview

Link Selection is a method used to determine which interface is used for incoming and outgoing VPN traffic as well as the best possible path for the traffic. Using the Link Selection mechanisms, the administrator can choose which IP addresses are used for VPN traffic on each Security Gateway.

Link Selection has many configuration options to enable you to control VPN traffic. These options include:

- Use probing to choose links according to their availability
- Use Load Sharing for Link Selection to distribute VPN traffic over available links (for Security Gateways of version R71 and higher)
- Use Service Based Link Selection to control bandwidth use (for Security Gateways of version R71 and higher)

Configuration settings for remote access clients can be configured together or separately from the Site-to-Site configuration. For more information, see [Link Selection for Remote Access Clients](#) (on page 224).

Configuring IP Selection by Remote Peer

There are several methods that can determine how remote peers resolve the IP address of the local Security Gateway. These settings are configured in **Security Gateway Properties > IPsec VPN > Link Selection**. Remote peers can connect to the local Security Gateway with these settings.

Always Use This IP Address:

Configure a certain IP address that is always used. The options are:

- **Main address** - The VPN tunnel is created with the Security Gateway main IP address, specified in the **IP Address** field on the **General Properties** page of the Security Gateway.
- **Selected address from topology table** - The VPN tunnel is created with the Security Gateway using a selected IP address chosen from the drop down menu that lists the IP addresses configured in the **Topology** page of the Security Gateway.
- **Statically NATed IP** - The VPN tunnel is created using a NATed IP address. This address is not required to be listed in the topology tab.

Calculate IP Based on Network Topology:

This method calculates the IP address used for the VPN tunnel by network topology, based on the location of the remote peer.

Use DNS Resolving:

This method is required for Dynamically Assigned IP (DAIP) Security Gateways. A VPN tunnel to a DAIP Security Gateway can only be initiated using DNS resolving since the IP address of the DAIP Security Gateway cannot be known in advance. If using this method for a non-DAIP Security Gateway, the IP address must be defined in the **Topology** tab. Without DNS resolving, a DAIP Security Gateway can only initiate the first connection between two peers. The second connection can be initiated by the peer Security Gateway as long as the IP address of the DAIP Security Gateway has not changed. The options are:

- **Full hostname** - Enter the full Fully Qualified Domain Name (FQDN). The DNS host name that is used is "Security Gateway_name.domain_name." For example, if the object name is "john" and the domain name is "smith.com" then the FQDN will be "john.smith.com."
- **Security Gateways name and domain name (specified in global properties)** - The Security Gateway name is derived from the **General Properties** page of the Security Gateway and the domain name is derived from the Global Properties page.

Use Probing. Redundancy Mode:

When more than one IP address is available on a Security Gateway for VPN, Link Selection may employ the RDP probing method to determine which link will be used. The RDP probing method is implemented using a proprietary protocol that uses UDP port 259. This protocol is proprietary to Check Point and works only between Check Point entities. (Note that it does not comply with RDP as specified in RFC 908/1151). IP addresses you do not want to be probed (i.e., internal IP addresses) may be removed from the list of IP's to be probed. Once a Security Gateway maps the links' availability, a link selection per connection can be made according to the following redundancy modes:

- **High Availability** (default setting)
In High Availability mode the VPN tunnel uses the first IP address to respond, or the primary IP address if a primary IP is configured and active. If the chosen IP address stops responding, the connection fails over to another responding IP address. If a primary IP address is configured, the VPN tunnel will stay on the backup IP address until the primary one becomes available again.
Note that if **one time probing** is configured, the VPN tunnel will stay on the first chosen IP address until the next time policy is installed. See **ongoing probing and onetime probing** methods below.
- **Load Sharing**
In Load Sharing mode the encrypted traffic is distributed among all available links. Every new connection ready for encryption uses the next available link in a round robin manner. When a link becomes unavailable, all of its connections are distributed among the other available links. A link's availability is determined using RDP probing.
The peer Security Gateway that responds to the connection will route the reply traffic through the same route that it was received on, as long as that link is available.
Although the VPN tunnel traffic can be routed through multiple links in Load Sharing mode, only one VPN tunnel is generated. IKE sessions are arbitrarily routed through one of the available links.
Load Sharing is supported on Security Gateways of version R71 and higher. If a Security Gateway of version R71 or higher is configured to use the Load Sharing redundancy mode, Security Gateways of versions before R71 will use the High Availability redundancy mode when routing traffic to the R71 or higher Security Gateways.
Load Sharing is supported on all platforms for incoming traffic. For outgoing traffic, VPN traffic between peers with Load Sharing configuration is not accelerated by IPSO acceleration devices. Load Sharing is not supported on UTM-1 Edge devices.

Probing Settings:

Additional settings related to probing are set in **Link Selection > IP Selection by Remote Peer > Use probing > Configure > Probing Settings**

- **Probe all addresses defined in the topology tab** - choose to include all addresses defined in the topology tab for the Security Gateway in the probing
- **Probe the following addresses** - Specify the addresses that you want to include in the probing.
- **Primary address** - Optionally, to choose a primary address, select the check box and choose one of the included IP addresses from the drop down menu as the Primary Address. A primary IP address is only used with the High Availability probing mode. If Load Sharing is configured, the primary address is ignored. Enabling a primary IP address has no influence on the IP selected for outgoing VPN traffic. If the remote Security Gateway connects to a peer Security Gateway that has a primary IP address

defined, then the remote Security Gateway will connect to the primary address (if active) regardless of network speed (latency) or route metrics.

- **Use probing method**

Choose one of the following probing methods.

- **Using ongoing probing** (default setting) - When a session is initiated, all possible destination IP addresses continuously receive RDP packets. The RDP probing is activated when a connection is opened and continues as a background process.
- **Using one time probing** - When a session is initiated, all possible destination IP addresses receive an RDP session to test the route. These results are used until the next time that a policy is installed.



Note - UDP RDP packets are not encrypted. The RDP mechanism only tests connectivity.

Last Known Available Peer IP Address

The IP address used by a Security Gateway during a successful IKE negotiation with a peer Security Gateway, is used by the peer Security Gateway as the destination IP address for the next IPSec traffic and IKE negotiations that it initiates. This is only the case when the Link Selection configuration does not use probing.

Configuring Outgoing Route Selection

For outbound traffic, there are different methods that can be used to determine which path to use when connecting with a remote peer. These settings are configured in **Security Gateway Properties > IPSec VPN > Link Selection**.

When Initiating a Tunnel

- **Operating system routing table** (default setting) - Using this method, the routing table is consulted for the available route with the lowest metric and best match for the VPN tunnel traffic.
- **Route based probing** - This method also consults the routing table for an available route with the lowest metric and best match. However, before a route is chosen, it is tested for availability using RDP probing. The Security Gateway then selects the best match (highest prefix length) active route with the lowest *metric*. This method is recommended when there is more than one external interface.

If you selected the **IP Selection by Remote Peer** setting of **Use probing** with **Load Sharing**, it also affects **Route based probing** link selection. In this case, **Route based probing** distributes the outgoing encrypted traffic among all available links. All possible links to the peer Security Gateway are derived from the routing table and the link's availability is tested using RDP probing. Every new connection ready for encryption uses the next available link in a round robin manner.

Route based probing enables the use of **On Demand Links (ODL)**, which are triggered upon failure of all primary links. You can run a script to activate an **On Demand Link** when all other links with higher priorities become unavailable. For more information, see On Demand Links ("[On Demand Links \(ODL\)](#)" on page 112).

For IKE and RDP sessions, Route based probing uses the same IP address and interface for responding traffic.

Route based probing is supported on the SecurePlatform, Linux, and IPSO platforms. VPN traffic between peers with Load Sharing probing mode and Route Based probing configuration will not be accelerated by IPSO acceleration devices.

When Responding to a Remotely Initiated Tunnel

When responding to a remotely initiated tunnel, there are two options for selecting the interface and next hop that are used. *These settings are only relevant for IKE and RDP sessions.*

These settings are configured in **Link Selection > Outgoing Route Selection > Setup > Link Selection - Responding Traffic** window.

- **Use outgoing traffic configuration** - Select this option to choose an interface using the same method selected in the **Outgoing Route Selection** section of the **Link Selection** page.

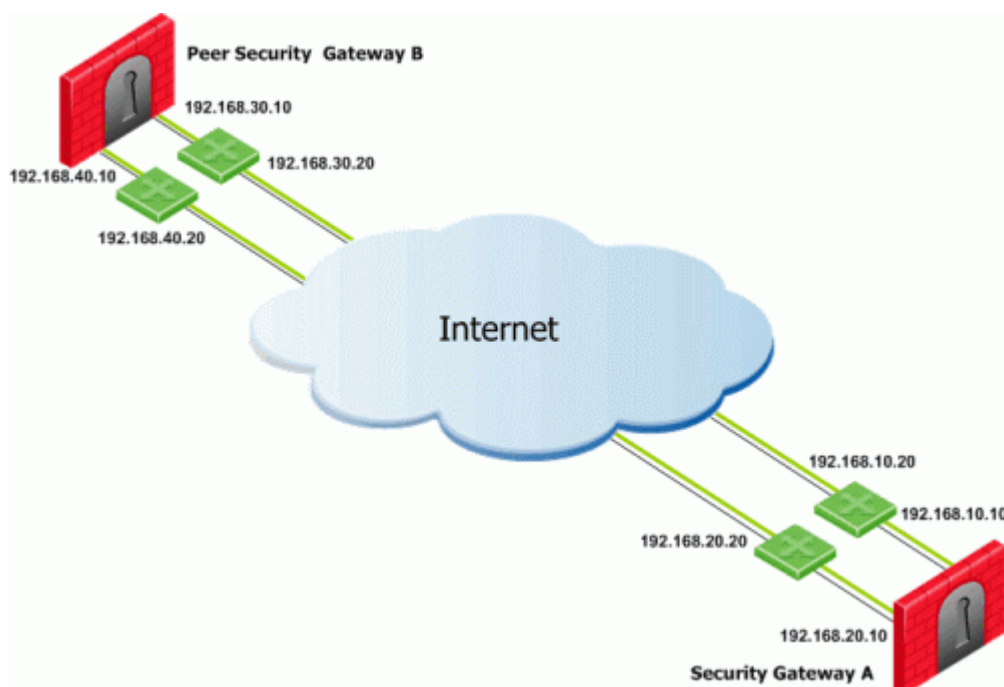
- **Reply from the same interface** - This option sends the returning traffic through the same interface and next hop it that it arrived in.



Note - When Route Based Probing is enabled, **Reply from the same interface** is the selected method and cannot be changed.

Using Route Based Probing

The local Security Gateway, using RDP probing, considers all possible routes between itself and the remote peer Security Gateway. The Security Gateway then decides on the most effective route between the two Security Gateways:



In this scenario, Security Gateway A has two external interfaces, 192.168.10.10 and 192.168.20.10. Peer Security Gateway B also has two external interfaces: 192.168.30.10 and 192.168.40.10.

For Security Gateway A, the routing table reads:

| Destination | Netmask | Next hop | Metric |
|---------------|---------------|---------------|--------|
| 192.168.40.10 | 255.255.255.0 | 192.168.10.20 | 1 |
| 192.168.40.10 | 255.255.255.0 | 192.168.20.20 | 2 |
| 192.168.30.10 | 255.255.255.0 | 192.168.10.20 | 3 |
| 192.168.30.10 | 255.255.255.0 | 192.168.20.20 | 4 |

For Security Gateway B, the routing table reads:

| Destination | Netmask | Next hop | Metric |
|---------------|---------------|---------------|--------|
| 192.168.20.10 | 255.255.255.0 | 192.168.40.20 | 1 |
| 192.168.20.10 | 255.255.255.0 | 192.168.30.20 | 2 |
| 192.168.10.10 | 255.255.255.0 | 192.168.40.20 | 3 |
| 192.168.10.10 | 255.255.255.0 | 192.168.30.20 | 4 |

If all routes for outgoing traffic from Security Gateway A are available, the route from 192.168.10.10 to 192.168.40.10 has the lowest metric (highest priority) and is therefore the preferred route.

Configuring Source IP Address Settings

The source IP address used for outgoing packets can be configured for sessions initiated by the Security Gateway. These settings are configured in **Security Gateway Properties > IPSec VPN > Link Selection > Outgoing Route Selection > Source IP address settings**.

When initiating a VPN tunnel, set the source IP address using one of the following:

- **Automatic (derived from the method of IP selection by remote peer)** - The source IP address of outgoing traffic is derived from the method selected in the **IP Selection by Remote Peer** section.
 - If **Main address** or **Selected address from topology table** are chosen in the **IP Selection by Remote Peer** section, then the source IP when initiating a VPN tunnel is the IP specified for that method.
 - If **Calculate IP based on network topology**, **Statically NATed IP**, **Use DNS resolving** or **Use probing** is chosen in the **IP Selection by Remote Peer** section, then the source IP when initiating a VPN tunnel is the IP address of the chosen outgoing interface.
- **Manual:**
 - **Main IP address** - The source IP is derived from the **General Properties** page of the Security Gateway.
 - **Selected address from topology table** - The selected IP from the drop down menu becomes the source IP.
 - **IP address of chosen interface** - The source IP is the same IP of the interface where the traffic is being routed through.

These settings are relevant for RDP and IKE sessions. When responding to an IKE session, use the **reply_from_same_IP (default: true)** attribute to follow the settings in the **Source IP address settings** window or to respond from the same IP.



Note - When Route Based Probing is enabled, **reply_from_same_IP** will be seen as **true**.

Outgoing Link Tracking

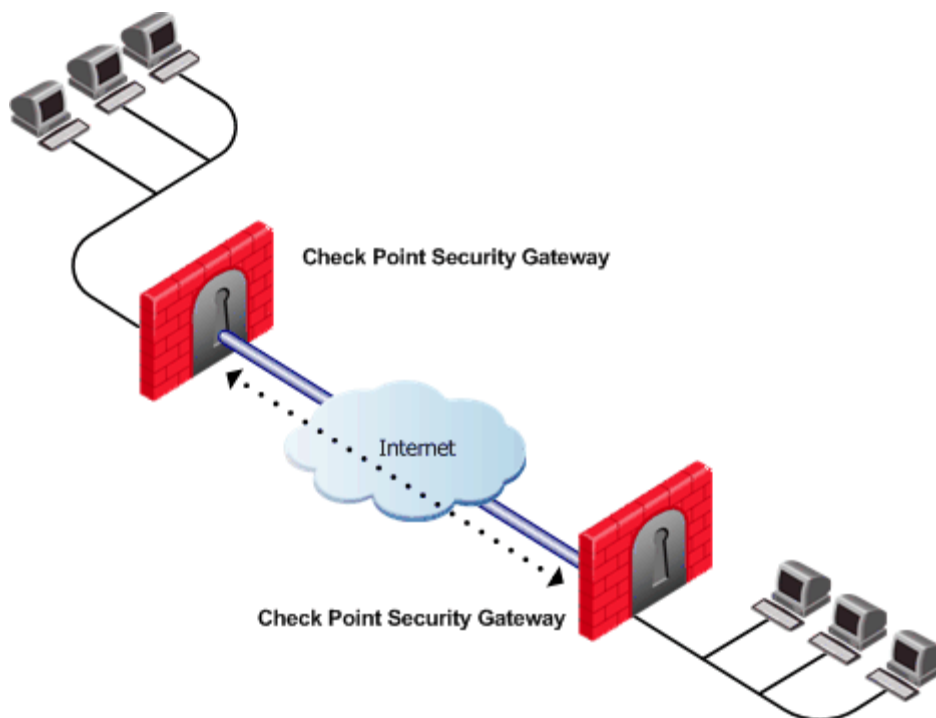
When **Outgoing link tracking** is activated on the local Security Gateway, the Security Gateway sends a log for every new resolving decision performed with one of its remote VPN peers. If **Use Probing** is configured on the local Security Gateway for Remote Peer resolving, or if Route Based Probing is activated on the local Security Gateway, log entries are also created for all resolving changes. For example, if a link in use becomes unavailable and a new available link is chosen, a log entry is issued.

Link Selection Scenarios

Link Selection can be used in many environments. This section describes various scenarios and how Link Selection should be configured in each scenario.

Gateway with a Single External Interface

This is the simplest scenario, where the local Security Gateway has a single external interface for VPN:



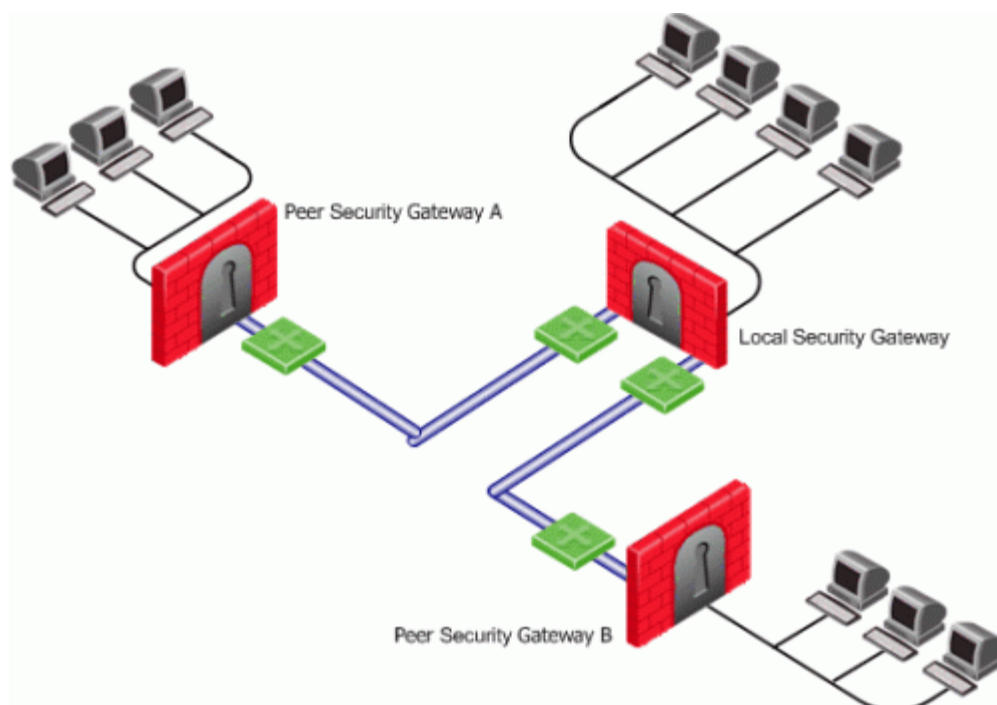
How do peer Security Gateways select an IP address on the local Security Gateway for VPN traffic?

Since there is only one interface available for VPN, to determine how remote peers determine the IP address of the local Security Gateway, select the following from the **IP Selection by Remote Peer** section of the Link Selection page:

- Select **Main address** or choose an IP address from the **Selected address from topology table** drop down menu.
- If the IP address is located behind a static NAT device, select **Statically NATed IP**.

Gateway with Several IP Addresses Used by Different Parties

In this scenario, the local Security Gateway has a point-to-point connection from two different interfaces. Each interface is used by a different remote party:

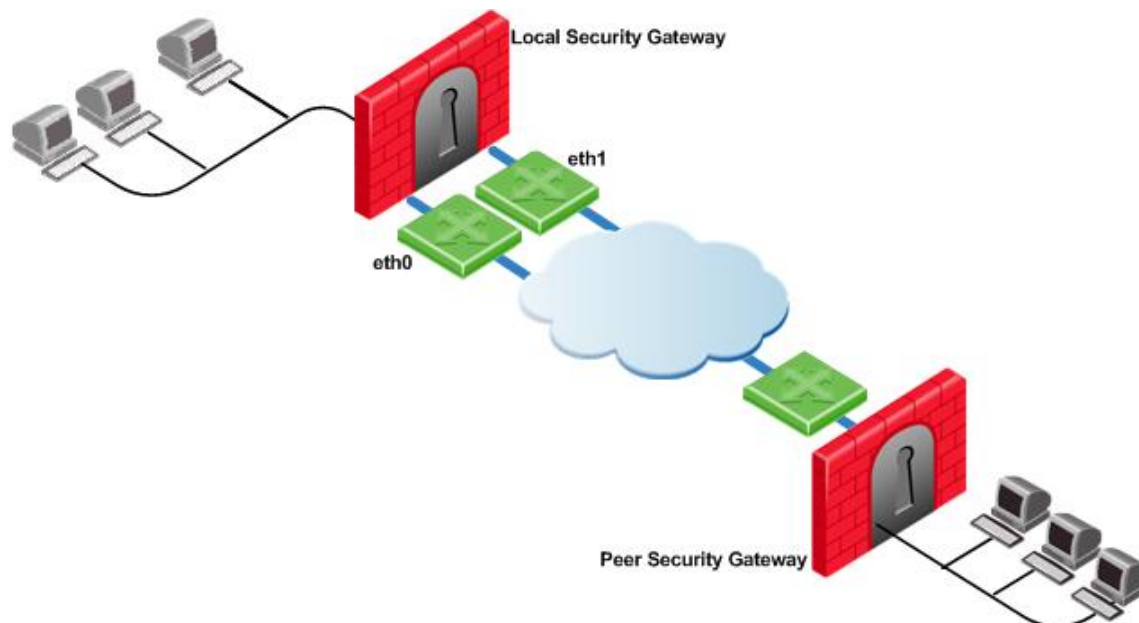


The local Security Gateway has two IP addresses used for VPN. One interface is used for VPN with a peer Security Gateway A and one interface for peer Security Gateway B.

To determine how peer Security Gateways discover the IP address of the local Security Gateway, enable **one-time probing** with **High Availability** redundancy mode. Since only one IP is available for each peer Security Gateway, probing only has to take place one time.

Gateway with an Interface Behind a Static NAT Device

In this scenario, the local Security Gateway has two external interfaces available for VPN. The address of interface eth0 is being translated using a NAT device:



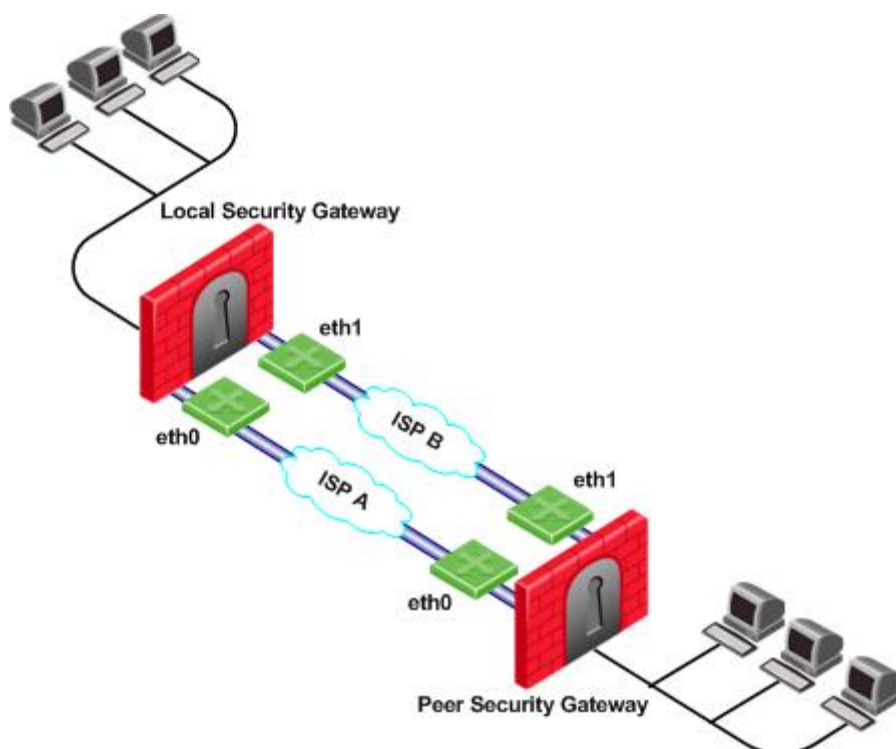
To determine how peer Security Gateways discover the IP address of the local Security Gateway, use **ongoing probing** with **High Availability** redundancy mode. In order for the Static NAT IP address to be probed, it must be added to the **Probe the following addresses** list in the **Probing Settings** window.

Utilizing Load Sharing

Depending on your configuration, there are many ways to use Load Sharing to distribute VPN traffic among available links between the local and peer Security Gateways.

Load Sharing with Multiple External Interfaces on Each End

In the following scenario, the local and peer Security Gateways each have two external interfaces available for VPN traffic.

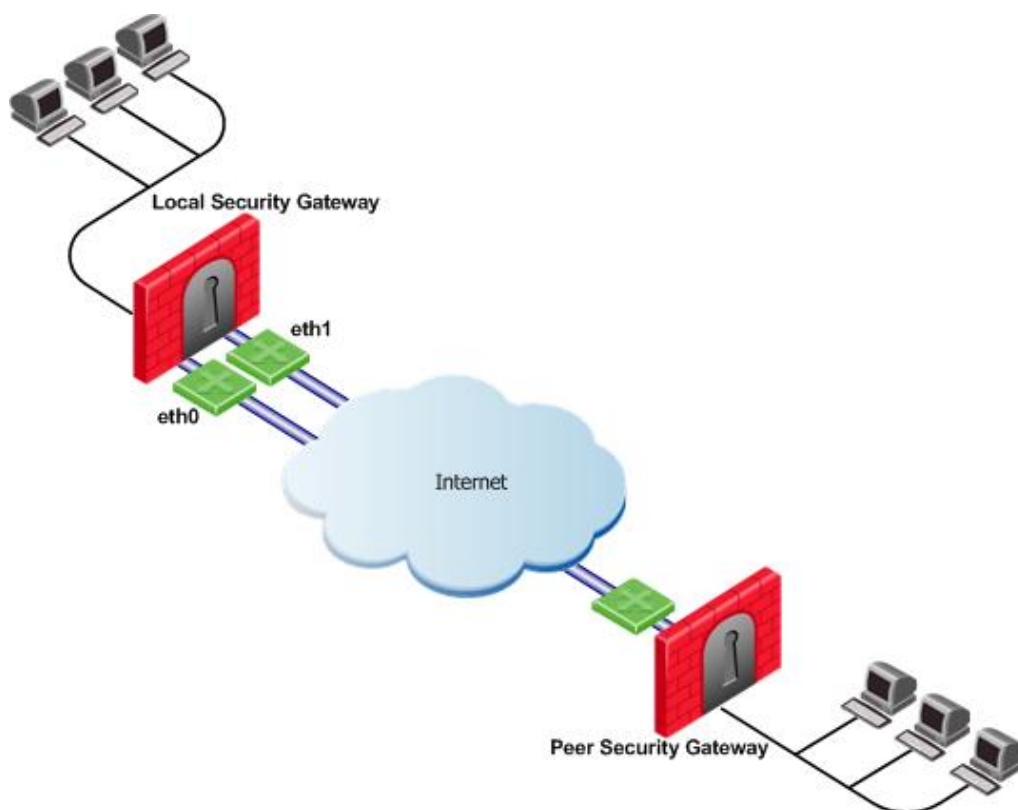


To utilize both external interfaces by distributing VPN traffic among all available links, use the Probing redundancy mode of **Load Sharing** on both Security Gateways. You can also specify that only certain external interfaces should be probed by putting only those interfaces in the **Probe the following addresses** list in the **Probing Settings** window. If one link goes down, traffic will automatically be rerouted through the other link.

To enable this configuration, make sure that your routing table allows packet flow back and forth between both eth0 interfaces and packet flow back and forth between both eth1 interfaces. Then Link Selection can reroute the VPN traffic between these available links.

Load Sharing with Multiple External Interfaces on One End

In the following scenario, the local Security Gateway has two external interfaces available for VPN traffic. The peer Security Gateway has one external interface for VPN traffic.



To utilize both external interfaces and distribute VPN traffic between the available links, use the Probing redundancy mode of **Load Sharing** on the local Security Gateway. Then the peer Security Gateway will distribute its outgoing VPN traffic between interfaces eth0 and eth1 of the local Security Gateway.

If the default, **Operating system routing table**, setting in the **Outgoing Route Selection** section is selected, the local Security Gateway will only use one of its local interfaces for outgoing VPN traffic; the route with the lowest metric and best match to reach the single IP address of the peer Security Gateway, according to the routing table.

If you want to distribute the outgoing VPN traffic on both outbound links from the local Security Gateway as well, select **Route Based Probing** in the Outgoing Route Selection on the Link Selection page of the local Security Gateway.

Service Based Link Selection

Service Based Link Selection enables administrators to control outgoing VPN traffic and bandwidth use by assigning a service or a group of services to a specific interface for outgoing VPN routing decisions. The encrypted traffic of an outgoing connection is routed through the configured interface according to the traffic's service. The links to the peer Security Gateway are derived from the routing table and the link's availability is tested using RDP probing.

If all links through the interface assigned to a specific service stop responding to RDP probing, a link failover will occur by default, as in any other probing mode. When a link through the assigned interface is restored, new outgoing connections are assigned to it, while existing connections are maintained over the backup link until they are completed.

It is possible to configure the traffic of a specific service not to fail over. In this case, traffic of the configured service will only be routed through interfaces assigned to this service, even if these interfaces stop responding to RDP.

If the same service is assigned to more than one interface, this service's traffic is distributed between the configured interfaces. Every new outgoing encrypted connection uses the next available link in a round robin manner.

All traffic from services that are not assigned to a specific interface is distributed among the remaining interfaces. If all links through these interfaces are down, the traffic is distributed among the interfaces that are configured for specific services.

Service Based Link Selection configuration requires enabling the following features:

- IP Selection by Remote Peer – Load Sharing probing mode
- Outgoing Route Selection – Route based probing
- Service Based Link Selection configuration file on the management server

Service Based Link Selection is supported on Security Gateways of version R71 and higher. It is supported on the SecurePlatform, Linux, and IPSO platforms. VPN traffic between peers with Service Based Link Selection configuration is not accelerated by IPSO acceleration devices. Service Based Link Selection is not supported on UTM-1 Edge devices.

Configuring Service Based Link Selection

To configure Service Based Link Selection:

1. In the **Link Selection** page, in the IP Selection by Remote Peer section, select:
 - **Use probing. Redundancy mode**
 - **Load Sharing**
2. In the Outgoing Route Selection section, select **Route based probing**.

Edit the Service Based Link Selection configuration in the `$FWDIR/conf/vpn_service_based_routing.conf` configuration file on the management server.

Fill in each line in the configuration file to specify the target Security Gateway, the interface for outgoing routing, and the service (or services group) to route through this interface. Use the names defined in the SmartDashboard GUI. Fill in all of the details for each Security Gateway on which you want to configure Service Based Link Selection.

The fields are:

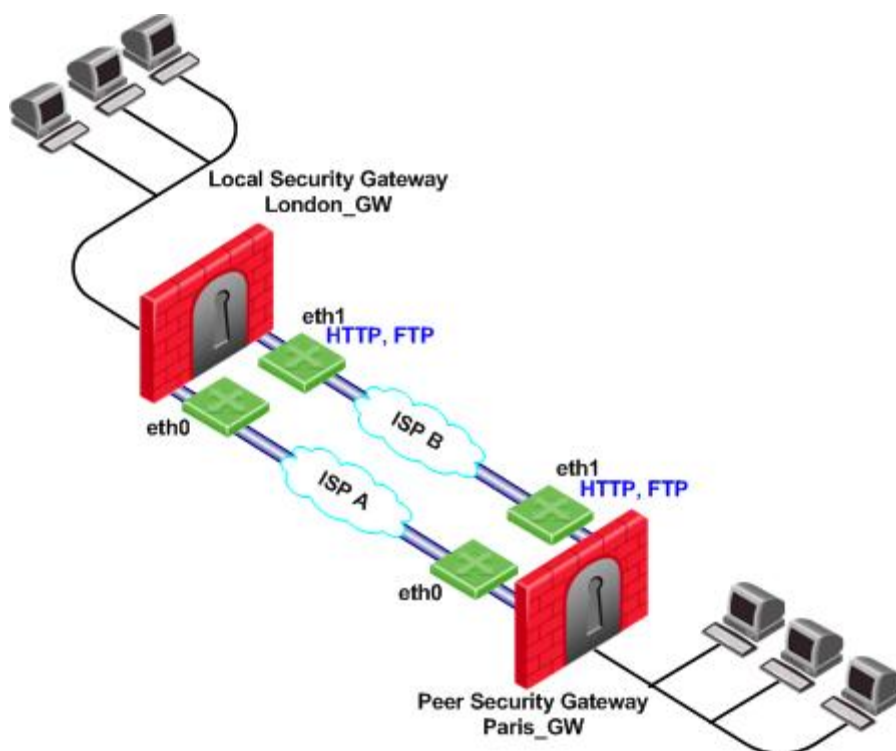
- **Gateway** – Security Gateway name (the name of the VPN Security Gateway or the cluster)
- **Interface** – Interface name
- **Service** – Service or services group name
- **dont_failover** – (Optional) If this string is present, traffic of the configured service will only be routed through interfaces configured for this service and will not fail over to another interface.

Service Based Link Selection Scenarios

The following scenarios provide examples of how Service Based Link Selection can be utilized.

Service Based Link Selection with Two Interfaces on Each End

In the scenario below, the local and peer Security Gateways each have two external interfaces for VPN traffic.



In this example, interface eth1 of both Security Gateways is dedicated to HTTP and FTP traffic. All other traffic is routed to interface eth0.

If the available link through eth1 stops responding to RDP probing, HTTP and FTP traffic will fail over to eth0. It is possible to specify that HTTP and FTP traffic should only be routed through eth1 even if the link through eth1 stops responding. Specify this by including the `dont_failover` flag when editing the Service Based Link Selection configuration file.

All other traffic that is not HTTP or FTP will be routed through eth0. If the link through eth0 stops responding to RDP probing, all traffic will be routed through eth1.

The Service Based Link Selection configuration file for this environment should appear as follows:

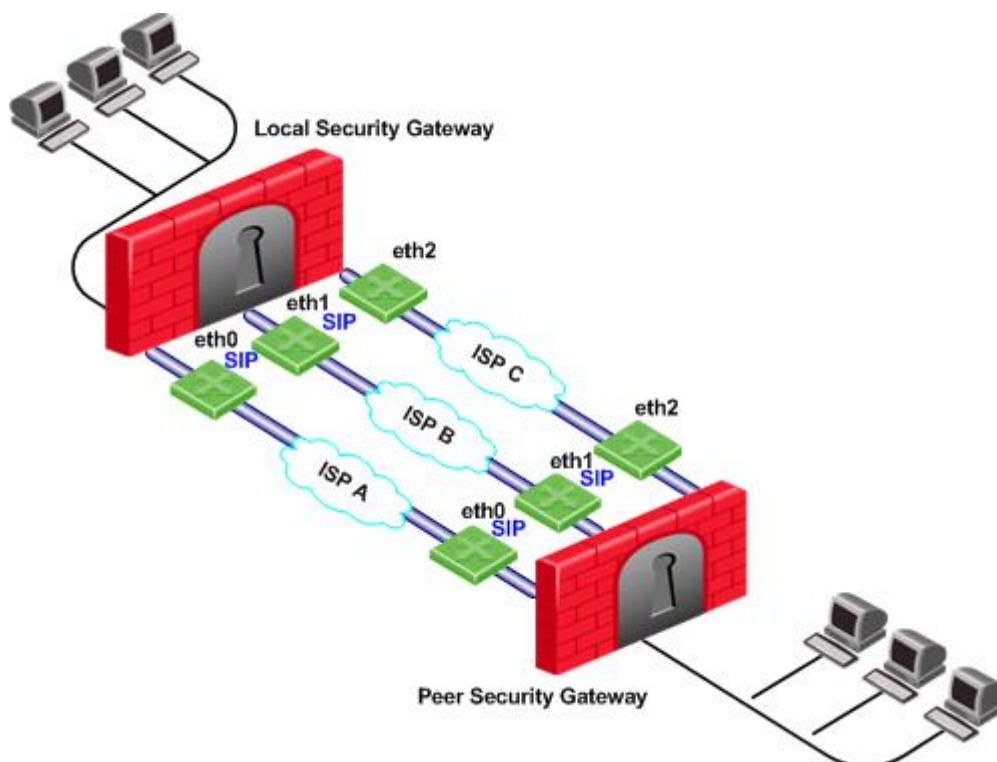
| Gateway ===== | Interface ===== | Service ===== | [dont_failover] ===== |
|------------------|--------------------|------------------|--------------------------|
| London_GW | eth1 | http | |
| London_GW | eth1 | ftp | |
| Paris_GW | eth1 | http | |
| Paris_GW | eth1 | ftp | |

Alternatively, in SmartDashboard, you can create a Services Group that includes HTTP and FTP services. In the example below, this group is called **http_ftp_grp**. Using this group, the Service Based Link Selection configuration file for this environment should appear as follows:

| Gateway ===== | Interface ===== | Service ===== | [dont_failover] ===== |
|------------------|--------------------|------------------|--------------------------|
| London_GW | eth1 | http_ftp_grp | |
| Paris_GW | eth1 | http_ftp_grp | |

Service Based Link Selection with Multiple Interfaces on Each End

In the following scenario, the local and peer Security Gateways each have three external interfaces available for VPN.

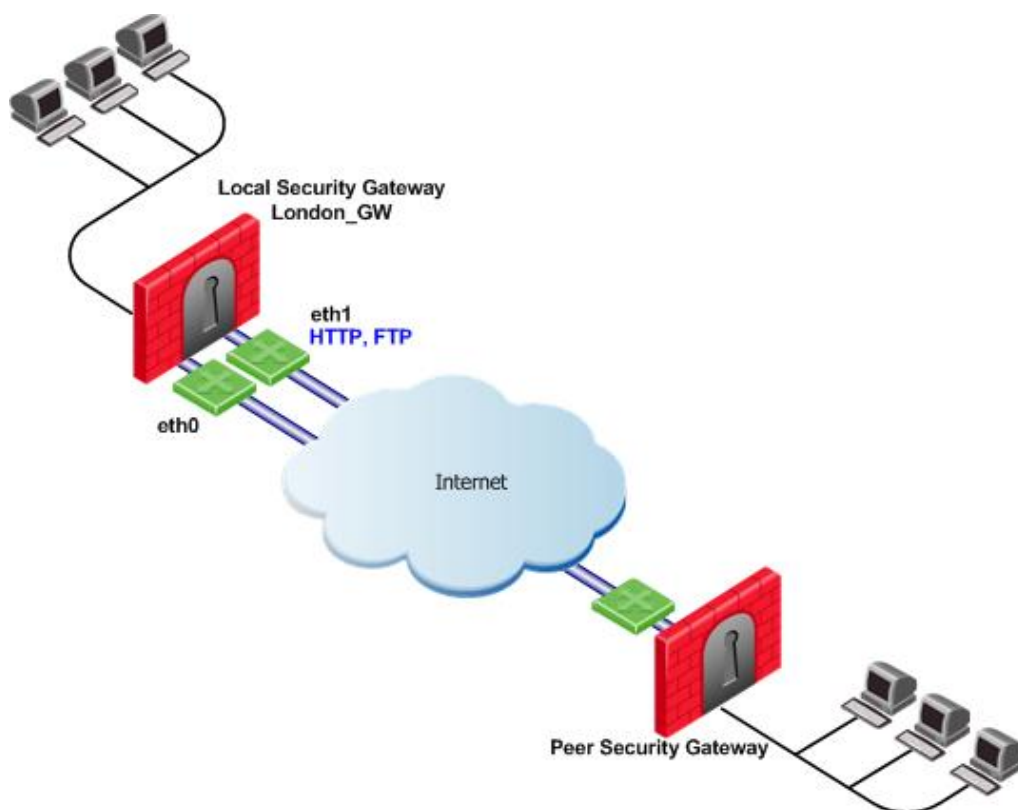


To utilize all three external interfaces and distribute the VPN traffic among the available links, Link Selection Load Sharing and Route based probing should be enabled. To control your bandwidth use, dedicate one or more links to a specific service or services using Service Based Link Selection. In this scenario, interfaces eth0 and eth1 of both Security Gateways are dedicated to SIP traffic. SIP traffic is distributed between eth0 and eth1. All other traffic is routed through eth2.

If either the link through eth0 or the link through eth1 stops responding to RDP probing, SIP traffic will fail over to the other SIP interface. If the link through eth2 stops responding to RDP probing, all traffic will be routed through eth0 or eth1.

Service Based Link Selection with Two Interfaces on One End

In the following scenario, the local Security Gateway has two external interfaces available for VPN traffic. The peer Security Gateway has a single external interface for VPN traffic.



To utilize all external interfaces and distribute the VPN traffic among the available links, Link Selection Load Sharing and Route based probing should be enabled on the local Security Gateway, **London_GW**. To control your bandwidth use, dedicate interface eth1 of the local Security Gateway to HTTP and FTP traffic using Service Based Link Selection. The local Security Gateway will route outgoing HTTP and FTP connections through interface eth1. All other traffic, not HTTP or FTP, will be routed through eth0.

In this scenario, HTTP and FTP traffic should not fail over. HTTP and FTP traffic should only be routed through interface eth1, even if the link through interface eth1 stops responding to RDP probing. This is configured by specifying the `dont_failover` flag.

The Service Based Link Selection configuration file for this environment should appear as follows:

| Gateway | Interface | Service | [dont_failover] |
|-----------|-----------|---------|-----------------|
| ===== | ===== | ===== | ===== |
| London_GW | eth1 | http | dont_failover |
| London_GW | eth1 | ftp | dont_failover |

Since the Service Based Link Selection configuration is only relevant for outgoing traffic of the local Security Gateway, the peer Security Gateway can send HTTP and FTP traffic to either interface of the local Security Gateway. The outgoing VPN traffic of the peer Security Gateway is distributed between interfaces eth0 and eth1 of the local Security Gateway.

Trusted Links

Trusted Links allows you to set an interface as "trusted" for VPN traffic so that traffic sent on that link will not be encrypted. You may want to set up a trusted link if you are confident that the link is already encrypted and secure and you do not need a second encryption.

If you configure an interface as trusted, traffic routed through that interface will be sent unencrypted, while traffic sent through other interfaces will still be encrypted.

Trusted interfaces should be configured symmetrically on the local and peer Security Gateways. If only one side of the link is configured as trusted for VPN traffic, clear traffic received by a non-trusted interface will be dropped by the peer Security Gateway.

If you have configured a specific link as trusted for VPN traffic and you are using probing, the probing method considers all links, including the trusted link, when choosing a link for a connection. The probing method chooses the link according to the configured redundancy mode, High Availability or Load Sharing, and according to whether Service Based Link Selection is configured. If the trusted link is chosen for a connection, the traffic is not encrypted. If another, non-trusted, link is chosen, the traffic is encrypted.

In an MEP configuration, trusted links are only supported for connections initiated by a peer Security Gateway to a MEP Security Gateway. Unencrypted VPN connections routed through a trusted interface and initiated by a MEP Security Gateway may be dropped by the peer Security Gateway.

Trusted links are not supported in Traditional mode. In Traditional mode, trusted link settings are ignored and VPN traffic is always encrypted.

Trusted links are supported on Security Gateways of version R71 and higher.



Note - Trusted links are not supported by IPSO acceleration devices. IPSO acceleration devices ignore trusted links settings and will encrypt traffic routed through these links.

Configuring Trusted Links

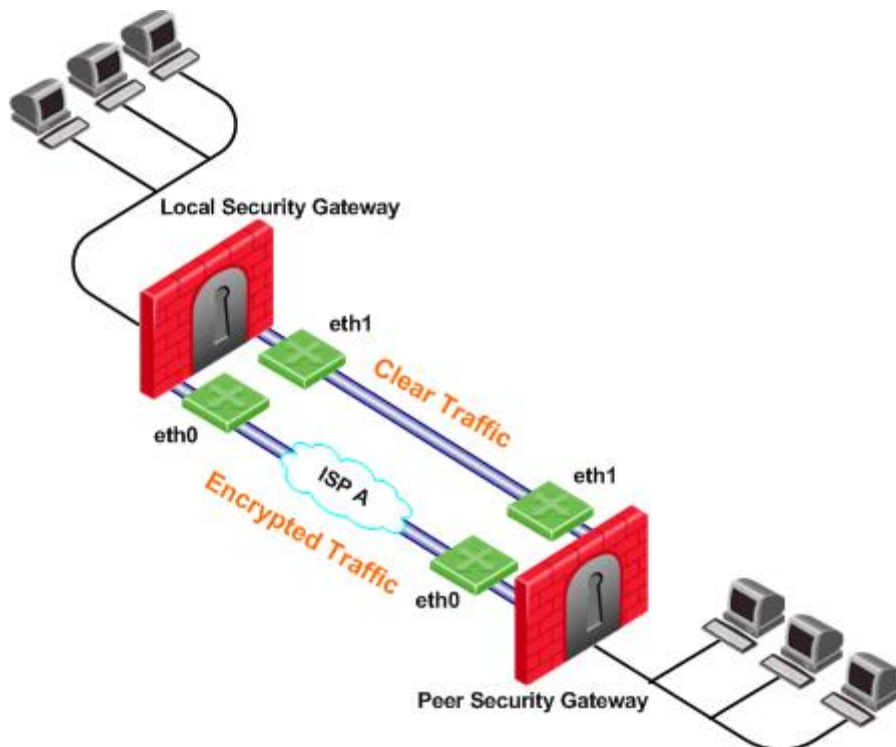
Use GuiDBedit, the Check Point Database Tool to configure Trusted Links.

To configure a trusted link:

1. In GuiDBedit go to **Network objects > network_objects**.
2. Select the Security Gateway that you want to edit.
3. Search for the interface that you want to configure as trusted from within the interfaces set. The interface name appears in the `officialname` attribute
4. Within the trusted interface set, change the value of the `vpn_trusted` attribute to `true` (default value: `false`).
5. Configure trusted interfaces symmetrically on the peer Security Gateways. If only one side of the link is configured as trusted for VPN traffic, clear traffic received by a non-trusted interface will be dropped by the peer Security Gateway.
6. Save changes.

Trusted Links Scenarios

In the following scenario, both the local and peer Security Gateways have two external interfaces available for VPN traffic. Interface eth1 on both Security Gateways has been configured as a trusted interface. Therefore traffic sent from eth1 of the local Security Gateway will be sent unencrypted and will be accepted by interface eth1 of the peer Security Gateway, and vice versa.

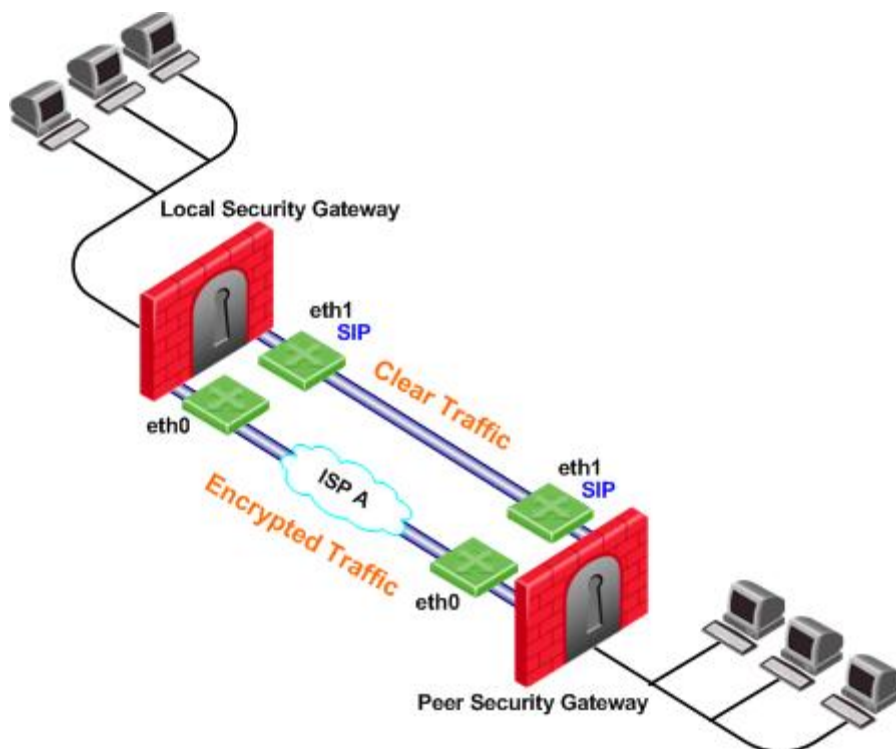


If the probing redundancy mode is High Availability and the trusted link is configured as the **Primary IP address**, the trusted link will be used for VPN traffic. If the trusted link stops responding to RDP probing, the link through Interface eth0 will be used for VPN traffic and traffic will be encrypted.

If the probing redundancy mode is Load Sharing, the VPN traffic will be distributed between the available links. Connections routed through interface eth0 will be encrypted while connections routed through the trusted link will not be encrypted.

Using Trusted Links with Service Based Link Selection

In the following scenario, the local and peer Security Gateways have two external interfaces available for VPN traffic. Interface eth1 on both Security Gateways is configured as a trusted interface for VPN traffic since encryption is not needed on that link. In addition, interface eth1 of both Security Gateways is dedicated to SIP traffic using Service Based Link Selection.

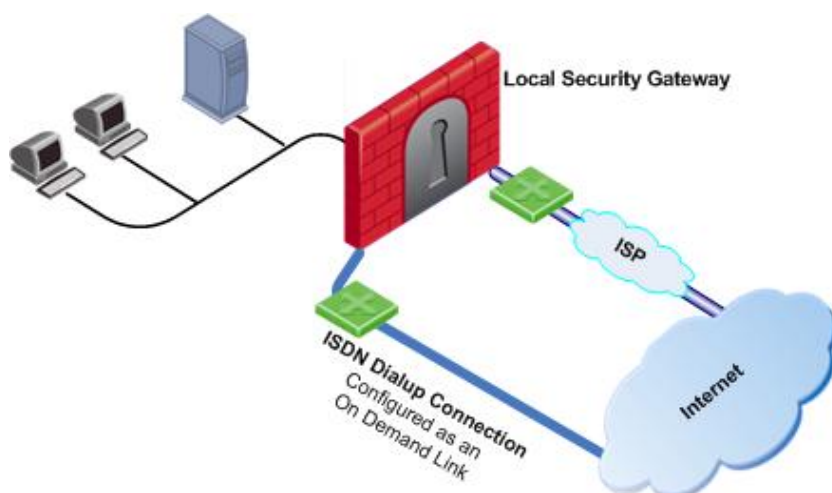


SIP traffic is routed through the trusted link between the two eth1 interfaces and will not be encrypted. If the trusted link stops responding to RDP probing, SIP traffic will be routed through the eth0 interfaces and will be encrypted.

All other traffic that is not SIP is encrypted and routed through the interface eth0 link. However, if interface eth0 stops responding to RDP probing, all the traffic will be routed through the trusted link and will not be encrypted.

On Demand Links (ODL)

Route based probing enables use of an On Demand Link (ODL), which is triggered upon failure of all primary links. When a failure is detected, a custom script is used to activate the ODL and change the appropriate routing information. The ODL's metric must be set to be larger than a configured minimum in order for it to be considered an ODL.



The Security Gateway has two external links for Internet connectivity: one to an ISP, the other to an ISDN dialup. The ISDN dialup connection is configured as an On Demand Link.

On the Security Gateway, the Route Based Probing mechanism probes all of the non-On Demand Links and selects the active link with the lowest metric. In this case, it probed the ISP link. A script is run to activate the On Demand Link when all other links with higher priorities become unavailable. When the link becomes available again, a shut down script is run automatically and the connection continues through the link with the ISP.



Note - On Demand Links are probed only once using a single RDP session. Fail over between On Demand Links is not supported.

Configuring On Demand Links

You can enable On Demand Links only if you enabled Route Based Probing. Configure On Demand Links commands in GuiDBedit, the Check Point Database Tool.

Configuring On Demand Links

| Property | Description |
|--|--|
| <code>use_on_demand_links</code> | Enables on-demand links. The default is FALSE. Change to TRUE. |
| <code>on_demand_metric_min</code> | Defines the minimum metric level for an on-demand link. This value must be equal to or higher than the configured minimum metric. |
| <code>on_demand_initial_script</code> | The name of the on-demand script, which runs when all not-on-demand routes stop responding. Put the script in the <code>\$FWDIR/conf</code> directory. |
| <code>on_demand_shutdown_script</code> | This script is run when the failed links become available. Put the script in the <code>\$FWDIR/conf</code> directory. |

If you do not want to use GuiDBedit, you can configure the `use_on_demand_links` and `on_demand_metric_min` commands in SmartDashboard:

1. In SmartDashboard, click **Policy > Global Properties > SmartDashboard Customization > Configure**.
2. In **VPN Advanced Properties**, click **Link Selection**.
3. Click `use_on_demand_links` to enable On Demand Links.
4. Set the minimum metric level for an On Demand Link next to the `on_demand_metric_min` command.

Link Selection and ISP Redundancy

ISP Redundancy enables reliable Internet connectivity by allowing a single or clustered Security Gateway to connect to the Internet via redundant ISP connections. As part of standard VPN installation, it offers two modes of operation that are configured in **Check Point > Security Gateway > Topology > ISP Redundancy**:

- **Load Sharing** mode connects to both ISPs while sharing the load of outgoing connections between the ISPs according to a designated weight assignment. New connections are randomly assigned to a link. If a link fails, all new outgoing connections are directed to the active link. This configuration effectively increases the WAN bandwidth while providing connectivity protection. The assigned ISP Links weight is only supported for firewall traffic.
- **Primary/Backup** mode connects to an ISP through the primary link, and switches to a backup ISP if the primary ISP link fails. When the primary link is restored, new outgoing connections are assigned to it, while existing connections are maintained over the backup link until they are complete.

The settings configured in the **ISP Redundancy** window are by default, applied to the **Link Selection** page and will overwrite any pre-existing configuration. The following settings carry over:

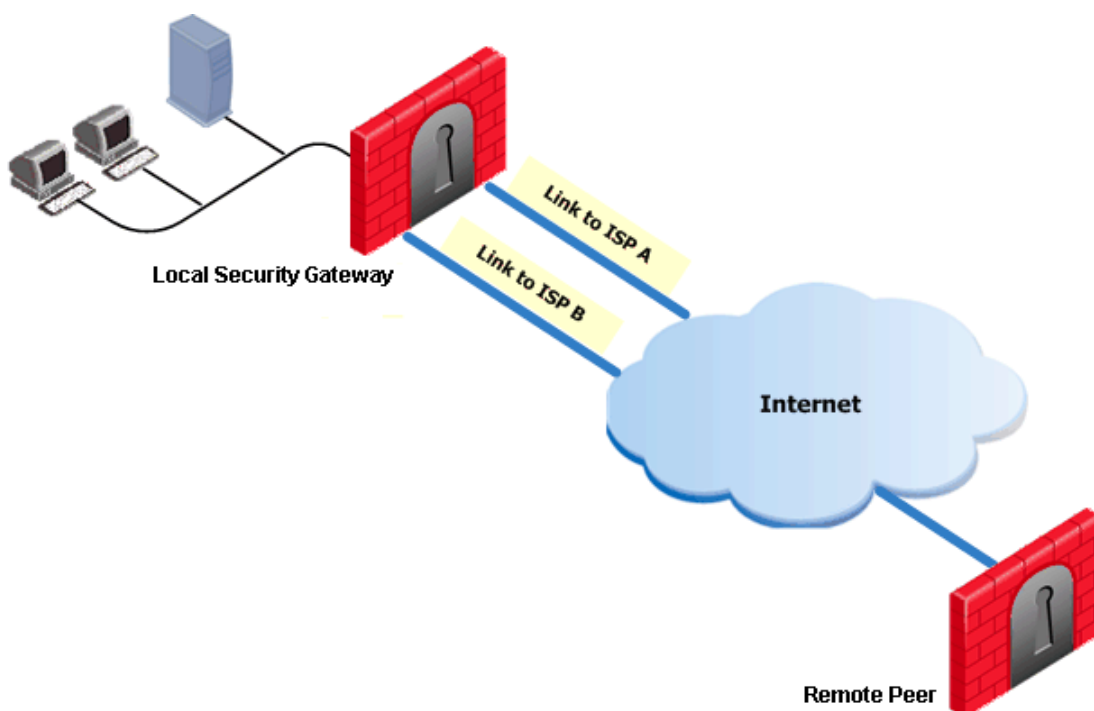
- When ISP Redundancy is configured, the default setting in the Link Selection page is **Use ongoing probing**. However, Link Selection only probes the ISPs configured in the **ISP Redundancy** window. This enables connection failover of the VPN tunnel if connectivity to one of the Security Gateway interfaces fails.

- If the ISP Redundancy mode is **Load Sharing**, the Probing redundancy mode in the Link Selection page is also **Load Sharing**.
- If the ISP Redundancy mode is **Primary/Backup**, the Probing redundancy mode in the Link Selection page is **High Availability**.
 - The Primary ISP link of the ISP redundancy is set as the Primary Address of the Link Selection probing. The Primary Address is set under: **IP Selection by Remote Peer > Use Probing > Configure** (or **View** if the settings are derived from the ISP Redundancy settings).

If you do not want the ISP Redundancy settings to affect the Link Selection settings, on the ISP Redundancy page, clear the check box that says **Apply settings to VPN traffic** and configure the required VPN settings on the **Link Selection** page. This may apply when you want to route VPN traffic differently than the firewall traffic. For example, if you want to use Load Sharing for firewall traffic and High Availability for VPN traffic, or if you want to use different primary ISPs for firewall and VPN traffic.

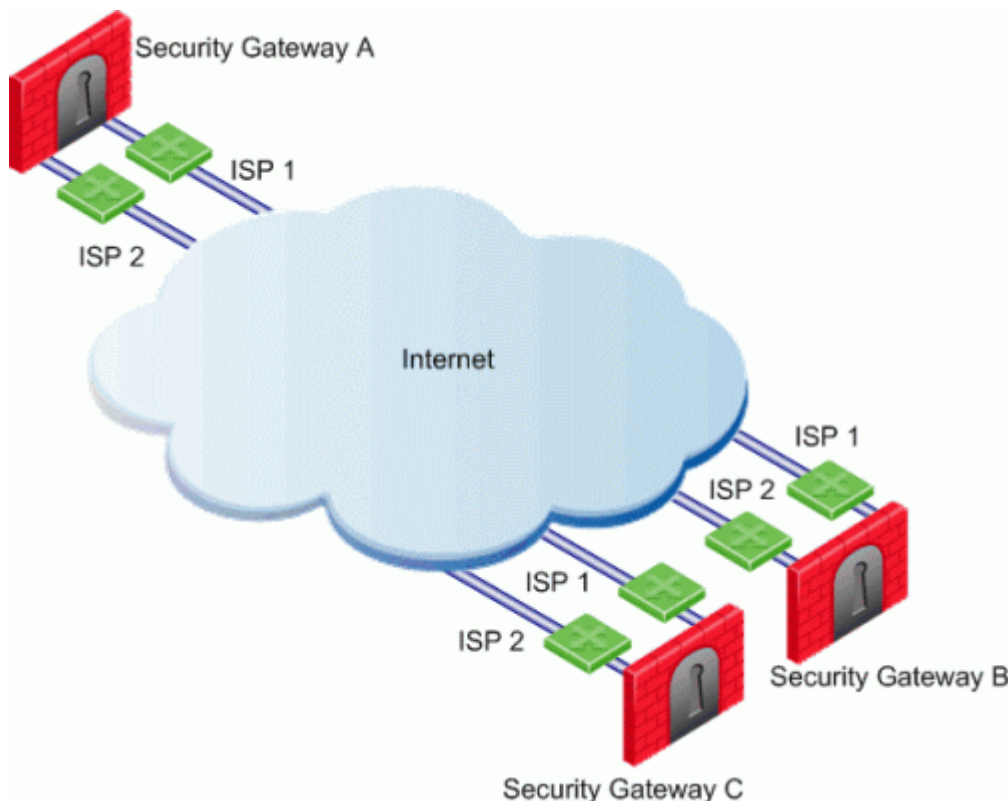
Link Selection and ISP Redundancy Scenarios

In the following scenario, the local Security Gateway maintains links to ISPs A and B, both of which provide connectivity to the Internet using ISP Redundancy.



In the **Topology > ISP Redundancy** window, configure the ISP Redundancy settings, such as ISP Links and Redundancy mode. The ISP Redundancy settings are applied by default to VPN traffic. The derived Link Selection settings are visible in the **IPSec VPN > Link Selection** window.

In the following scenario, the **Apply settings to VPN traffic** on the **ISP Redundancy** page was cleared and there are different settings configured for Link Selection and ISP Redundancy.



In this scenario:

- Security Gateways A, B, and C each have two interfaces configured as ISP links.
- **ISP Redundancy** is configured on Security Gateway A.
- Security Gateway A should use ISP 1 in order to connect to Security Gateway B and ISP 2 in order to connect to Security Gateway C. If one of the ISP links becomes unavailable, the other ISP should be used.

In this scenario, the administrator of Security Gateway A needs to:

- Uncheck the **Apply settings to VPN traffic** box in the **ISP Redundancy** window.
- Reconfigure the **Outgoing Route Selection** to **Route Based Probing** in the **Link Selection** window.
- Configure the routing table so that ISP 1 is the highest priority for peer Security Gateway B and ISP 2 has the highest priority for peer Security Gateway C.

Link Selection with non-Check Point Devices

RDP probing, the probing method used for certain Link Selection features, is proprietary to Check Point and only works between Check Point entities. It is not supported with non-Check Point devices.

Since RDP probing is not active on non-Check Point gateways, the following results apply if a Check Point Security Gateway sends VPN traffic to a non-Check Point gateway:

- **Use probing** cannot be used by locally managed Check Point Security Gateways to determine the IP address of non-Check Point devices. Any of the other methods available from the **IP Selection by Remote Peer** section can be used.
- **Load Sharing** and **Service Based Link Selection** do not work with non-Check Point gateways. If Load Sharing or Service Based Link Selection is enabled on the local Security Gateway, but the peer is a non-Check Point device, the local Security Gateway will only use one link to the non-Check Point device: the best match (highest prefix length) link with the lowest metric.
- If **Route based probing** is selected as the **Outgoing Route Selection** method, for VPN traffic to a non-Check Point device, the local Security Gateways will always use the best match (highest prefix length) link with the lowest metric.

Chapter 12

Multiple Entry Point VPNs

In This Chapter

| | |
|------------------------|-----|
| Overview of MEP | 117 |
| Explicit MEP | 118 |
| Implicit MEP | 123 |
| Routing Return Packets | 125 |
| Special Considerations | 126 |
| Configuring MEP | 126 |

Overview of MEP

Multiple Entry Point (MEP) is a feature that provides a high availability and load sharing solution for VPN connections. A Security Gateway on which the VPN module is installed provides a single point of entry to the internal network. It is the Security Gateway that makes the internal network "available" to remote machines. If a Security Gateway should become unavailable, the internal network too, is no longer available. A MEPed environment has two or more Security Gateways both protecting and enabling access to the same VPN domain, providing peer Security Gateways with uninterrupted access.

VPN High Availability Using MEP or Clustering

Both MEP and Clustering are ways of achieving High Availability and load sharing. However:

- Unlike the members of a ClusterXL Security Gateway Cluster, there is no physical restriction on the location of MEPed Security Gateways. MEPed Security Gateways can be geographically separated machines. In a cluster, the clustered Security Gateways need to be in the same location, directly connected via a *sync* interface.
- MEPed Security Gateways can be managed by different Security Management servers; cluster members must be managed by the same Security Management server.
- In a MEP configuration there is no "state synchronization" between the MEPed Security Gateways. In a cluster, all of the Security Gateways hold the "state" of all the connections to the internal network. If one of the Security Gateways fails, the connection passes seamlessly over (performs *failover*) to another Security Gateway, and the connection continues. In a MEPed configuration, if a Security Gateway fails, the current connection is lost and one of the backup Security Gateways picks up the *next* connection.
- In a MEPed environment, the decision which Security Gateway to use is taken on the remote side; in a cluster, the decision is taken on the Security Gateway side.

Implementation

MEP is implemented via a proprietary *Probing Protocol* (PP) that sends special UDP RDP packets to port 259 to discover whether an IP is reachable. This protocol is proprietary to Check Point and does not conform to RDP as specified in RFC 908/1151.



Note - These UDP RDP packets are not encrypted, and only test the availability of a peer.

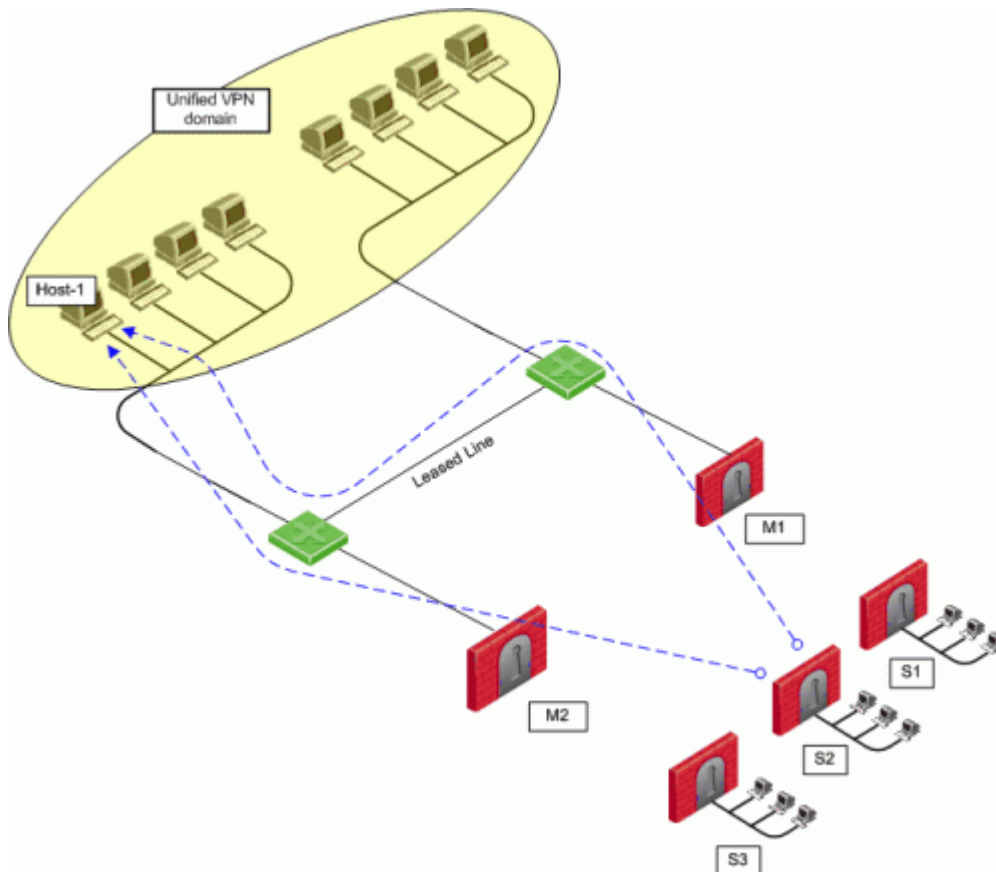
The peer continuously probes or polls all MEPed Security Gateways in order to discover which of the Security Gateways are "up", and chooses a Security Gateway according to the configured selection mechanism. Since RDP packets are constantly being sent, the status of all Security Gateways is known and updated when changes occur. As a result, all Security Gateways that are "up" are known.

There are two available methods to implement MEP:

- Explicit MEP - Only Star communities with more than one central Security Gateway can enable explicit MEP, providing multiple entry points to the network behind the Security Gateways. When available, Explicit MEP is the recommended method.
- Implicit MEP - Implicit MEP is supported in all scenarios where fully or partially overlapping encryption domains exist or where Primary-Backup Security Gateways (on page 125) are configured. When upgrading from a version prior to NGX (R60) where Implicit MEP was already configured, the settings previously configured will remain.

Explicit MEP

In a site to site Star VPN community, explicit MEP is configured via the community object. When MEP is enabled, the satellites consider the "unified" VPN domain of all the Security Gateways as the VPN domain for each Security Gateway. This unified VPN domain is considered the VPN domain of each Security Gateway:



In the figure, a Star VPN community has two central Security Gateways, M1 and M2 (for which MEP has been enabled) and three satellite Security Gateways — S1, S2, and S3. When S2 opens a connection with host-1 (which is behind M1 and M2), the session will be initiated through either M1 or M2. Priority amongst the MEP Security Gateways is determined by the MEP entry point selection mechanism.

If M2 is the selected entry point and becomes unavailable, the connection to host-1 fails over to M1. Returning packets will be rerouted using RIM or IP Pool NAT. For more information about returning packets, see Routing Return Packets (on page 125).

There are four methods used to choose which of the Security Gateways will be used as the entry point for any given connection:

- Select the closest Security Gateway to source (First to respond)
- Select the closest Security Gateway to destination (By VPN domain)
- Random Selection (for Load distribution)
- Manually set priority list (MEP rules)

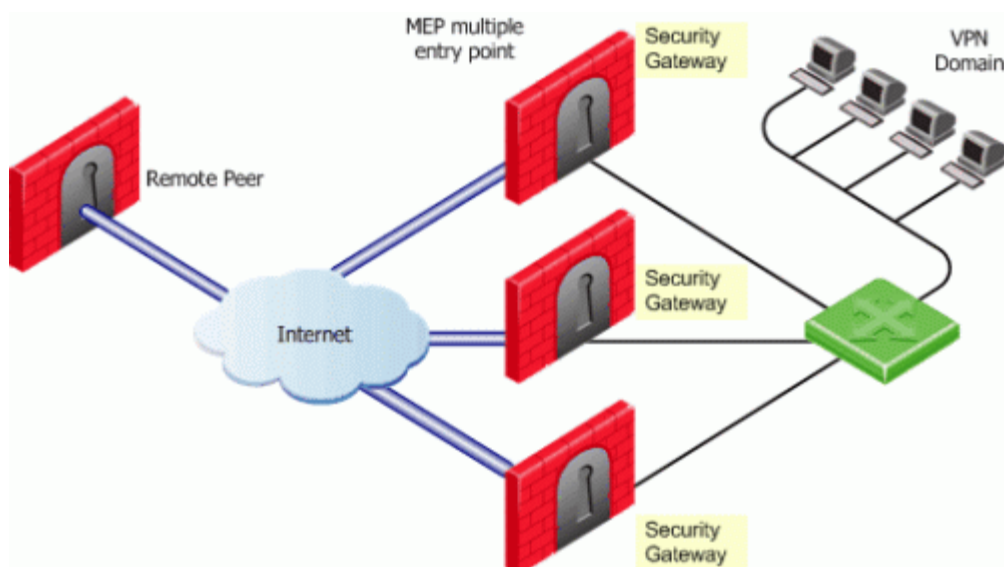
If either "By VPN domain" or "Manually set priority list" is selected, then **Advanced** options provide additional granularity.

MEP Selection Methods

- **First to Respond**, in which the first Security Gateway to reply to the peer Security Gateway is chosen. An organization would choose this option if, for example, the organization has two Security Gateways in a MEPed configuration - one in London, the other in New York. It makes sense for peers located in England to try the London Security Gateway first and the NY Security Gateway second. Being geographically closer to the peers in England, the London Security Gateway will be the first to respond, and becomes the entry point to the internal network. See: First to Respond (on page 124).
- **VPN Domain**, is when the destination IP belongs to a particular VPN domain, the Security Gateway of that domain becomes the chosen entry point. This Security Gateway becomes the primary Security Gateway while other Security Gateways in the MEP configuration become its backup Security Gateways. See: By VPN Domain (on page 120).
- **Random Selection**, in which the remote peer randomly selects a Security Gateway with which to open a VPN connection. For each IP source/destination address pair, a new Security Gateway is randomly selected. An organization might have a number of machines with equal performance abilities. In this case, it makes sense to enable load distribution. The machines are used in a random and equal way. See: Random Selection (on page 120).
- **Manually set priority list**, Security Gateway priorities can be set manually for the entire community or for individual satellite Security Gateways. See: Manually Set Priority List (on page 121).

First to Respond

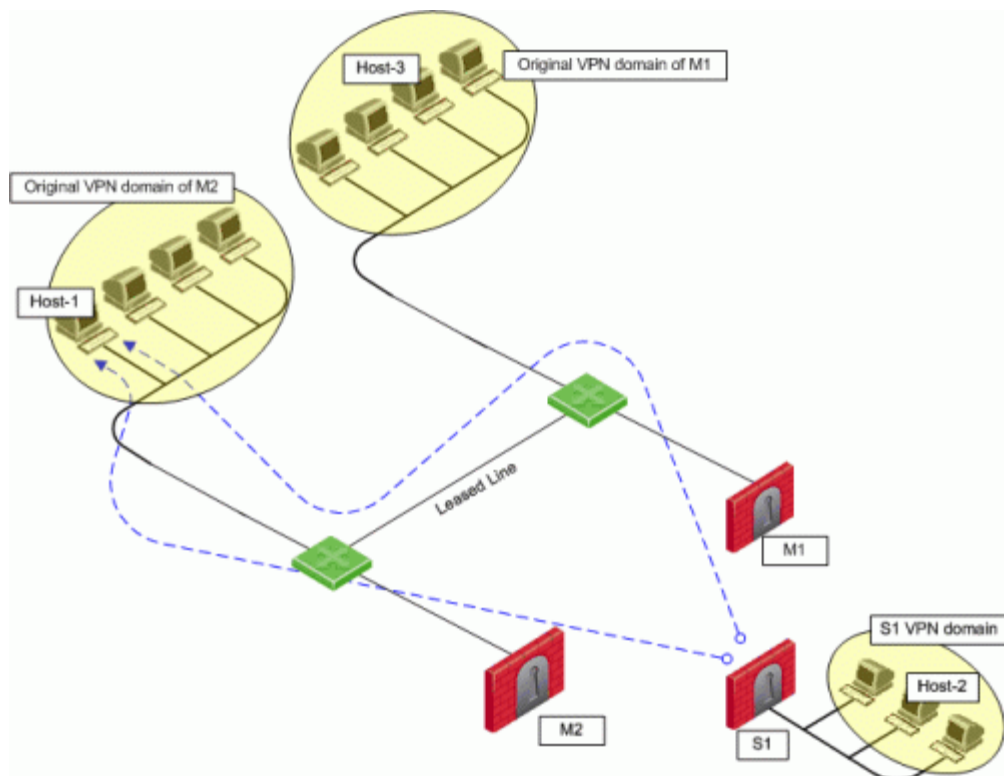
When there is no primary Security Gateway, all Security Gateways share "equal priority". When all Security Gateway's share "equal priority":



- Remote peers send RDP packets to all the Security Gateways in the MEP configuration.
- The first Security Gateway to respond to the probing RDP packets gets chosen as the entry point to network. The idea behind *first to respond* is proximity. The Security Gateway which is "closer" to the remote peer responds first.
- A VPN tunnel is opened with the first to respond. All subsequent connections pass through the chosen Security Gateway.
- If the Security Gateway ceases to respond, a new Security Gateway is chosen.

By VPN Domain

Prior to enabling MEP, each IP address belonged to a specific VPN domain. Using *By VPN Domain*, the Security Gateway of that domain becomes the chosen entry point. In the figure, the VPN Star community has two central MEPed Security Gateways (M1 and M2, each of which *have their own VPN domains*), and remote satellite S1.



Host-2 (in the VPN domain of satellite S1) initiates a connection with host-1. The connection can be directed through either M1 or M2. However, host-1 is within M2's original VPN domain. For this reason, M2 is considered the Security Gateway "closest" to the destination IP Address. M2 is therefore considered the primary Security Gateway and M1 the backup Security Gateway for Host-1. If there were additional Security Gateways in the center, these Security Gateways would also be considered as backup Security Gateways for M2.

If the VPN domains have fully or partially overlapping encryption domains, then more than one Security Gateway will be chosen as the "closest" entry point to the network. As a result, more than one Security Gateway will be considered as "primary." When there are more than one primary or backup Security Gateways available, the Security Gateway is selected using an additional selection mechanism. This advanced selection mechanism can be either (See Advanced Settings (on page 122)):

- First to Respond
- Random Selection (for load distribution)

For return packets you can use RIM on the center Security Gateways. If RIM is also enabled, set a metric with a lower priority value for the leased line than the VPN tunnel. The satellite S1 might simultaneously have more than one VPN tunnel open with the MEPed Security Gateways, for example M2 as the chosen entry point for host-1 and M1 as the chosen entry point for host-3. While both M1 and M2 will publish routes to host-1 and host-3, the lower priority metric will ensure the leased line is used only when one of the Security Gateways goes down.

Random Selection

Using this method, a different Security Gateway is randomly selected as an entry point for incoming traffic. Evenly distributing the incoming traffic through all the available Security Gateways can help prevent one Security Gateway from becoming overwhelmed with too much incoming traffic.

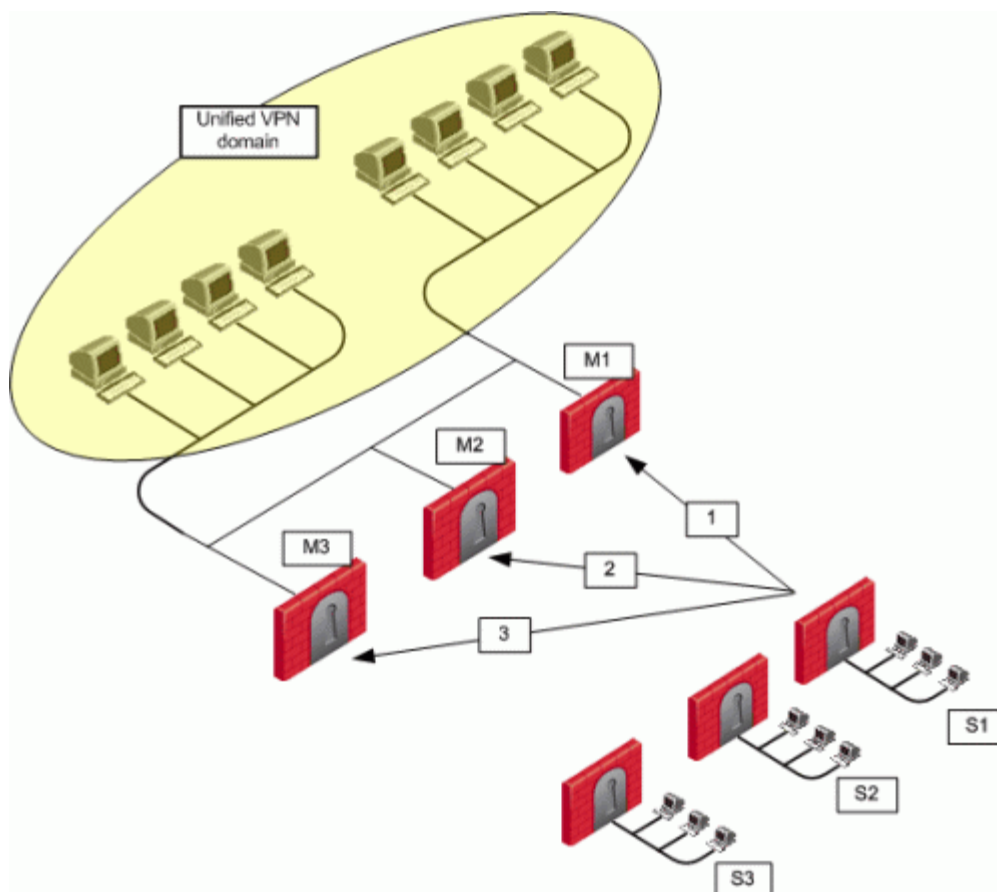
The Security Gateways are probed with RDP packets, as in all other MEP configurations, to create a list of responding Security Gateways. A Security Gateway is randomly chosen from the list of responding Security Gateways. If a Security Gateway stops responding, another Security Gateway is (randomly) chosen.

A new Security Gateway is randomly selected for every source/destination IP pair. While the source and destination IP's remain the same, the connection continues through the chosen Security Gateway.

In such a configuration, RIM is not supported. IP Pool NAT must be enabled to ensure return packets are correctly routed through the chosen Security Gateway.

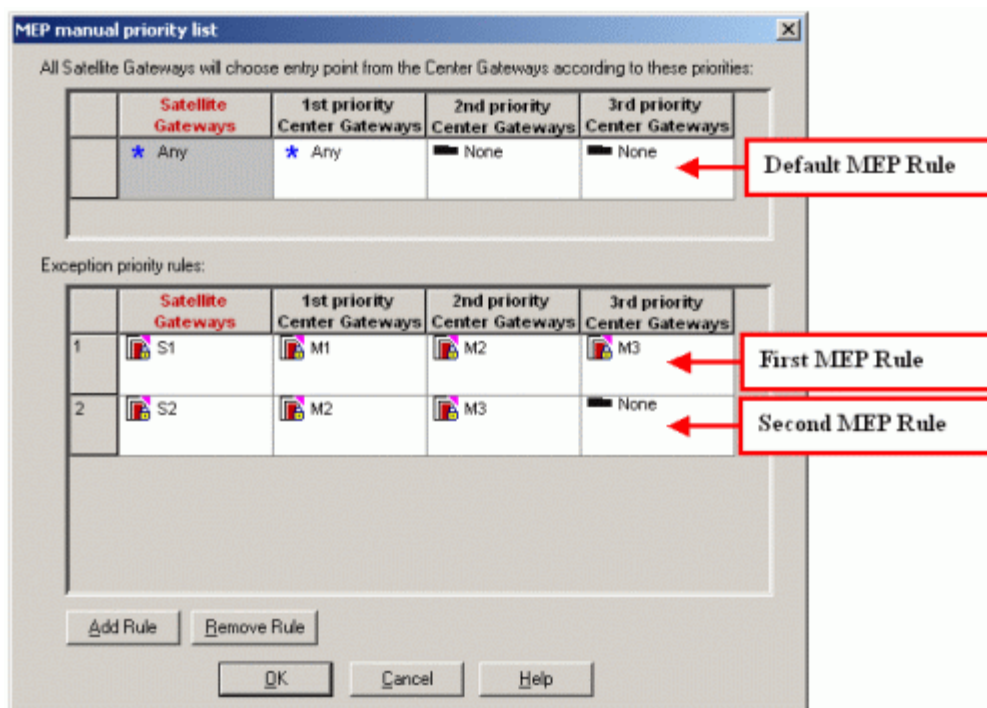
Manually Set Priority List

The Security Gateway that will be chosen (from the central Security Gateways in the star community) as the entry point to the core network can be controlled by manually setting a priority per source Security Gateway. Each priority constitutes a MEP Rule:



In the figure, three MEP members (M1, M2, M3) provide entry points to the network for three satellite Security Gateways (S1, S2, S3). Satellite S1 can be configured to try the Security Gateways in the following order: M1, M2, M3, giving the highest priority to M1, and the lowest priority to M3. Satellite S2 can be configured to try the Security Gateways in the following order: M2, M3 (but not to try M1).

Each of these priorities constitutes a MEP rule in the **MEP manual priority list** window:



The **MEP manual priority list** window is divided into the default rule, and rules which provide exceptions to the default rule. The default MEP rule takes effect when:

- No MEP rules are defined
- When the source of the connection cannot be found in the **Exception priority rules**

The **Exception priority rules** section contains three priority levels: primary, secondary, and tertiary. While there are only three priority levels,

- The same priority can be assigned to several central Security Gateways
- The same rule can be assigned to several satellite Security Gateways
- A priority level can be left blank

In the second MEP rule below:

| | Satellite Gateways | 1st priority Center Gateways | 2nd priority Center Gateways | 3rd priority Center Gateways |
|---|---------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 1 | S1 | M1 | M2 | M3 |
| 2 | S2 S3 | M2 | M3 M1 | None |

central Security Gateways M3 and M1 have equal priority. The same rule is being applied to satellites S2 and S3.

When more than one Security Gateway is assigned the same priority level, which Security Gateway will be chosen is resolved according to the **Advanced** settings. See Advanced Settings (on page 122).

Advanced Settings

In some instances, more than one Security Gateway is available in the center with no obvious priority between them. For example — as shown in Figure 12-6 — more than one Security Gateway is assigned "second" priority. In this scenario, **Advanced** options are used to decide which Security Gateway is chosen: *First to Respond*, or *Random Selection*. (Choose Random selection to enable load balancing between the Security Gateways.)

When "manually set priority list" is the MEP selection mechanism, *RIM is supported*. RIM can be configured with "manually set priority list" because the "random selection" mechanism available on the **Advanced** button is different from the random selection mechanism used for MEP.

For the "random selection" mechanism employed for MEP, a different Security Gateway is selected for each IP source/destination pair. For the random selection mechanism available from the **Advanced** button, a single MEP entry point is randomly selected and then used for all connections, and does not change according to source/destination pair. Load distribution is therefore achieved since every satellite Security Gateway is randomly assigned a Security Gateway as its entry point. This makes it possible to enable RIM at the same time.

Tracking

If the tracking option is enabled for MEP, the following information is logged by each satellite Security Gateway:

- The resolved peer Security Gateway (a Security Gateway in the MEP)
- The priority of the resolved Security Gateway (primary, secondary, tertiary)
- Whether the resolved Security Gateway is responding

For example, in the scenario shown in the Manually Set Priority List (on page 121) section, satellite S1 opens a connection to the VPN domain that includes Security Gateways M1, M2, and M3. M1 is the resolved peer. If tracking is enabled, the log reads:

```
Resolved peer for tunnel from S1 to the MEP that contains
M1, M2, and M3, is: M1 (Primary Security Gateway,
responding).
```

Implicit MEP

There are three methods to implement implicit MEP:

- *First to Respond*, in which the first Security Gateway to reply to the peer Security Gateway is chosen. An organization would choose this option if, for example, the organization has two Security Gateways in a MEPed configuration - one in London, the other in New York. It makes sense for VPN-1 peers located in England to try the London Security Gateway first and the NY Security Gateway second. Being geographically closer to VPN peers in England, the London Security Gateway is the first to respond, and becomes the entry point to the internal network. See: First to Respond (on page 124).
- *Primary-Backup*, in which one or multiple backup Security Gateways provide "high availability" for a primary Security Gateway. The remote peer is configured to work with the primary Security Gateway, but switches to the backup Security Gateway if the primary goes down. An organization might decide to use this configuration if it has two machines in a MEP environment, one of which is stronger than the other. It makes sense to configure the stronger machine as the primary. Or perhaps both machines are the same in terms of strength of performance, but one has a cheaper or faster connection to the Internet. In this case, the machine with the better Internet connection should be configured as the primary. See: Primary-Backup Security Gateways (on page 125).
- *Load Distribution*, in which the remote VPN peer randomly selects a Security Gateway with which to open a connection. For each IP source/destination address pair, a new Security Gateway is randomly selected. An organization might have a number of machines with equal performance abilities. In this case, it makes sense to enable load distribution. The machines are used in a random and equal way. See: Random Selection (on page 120).

Implicit MEP is supported if the Security Gateways with overlapping encryption domains are in the same community. If they are located in different communities, only one of the Security Gateways will be used for this encryption domain.



Note - When upgrading from a version prior to NGX R60 where Implicit MEP was already configured, the settings previously configured will remain.

First to Respond

When there is no primary Security Gateway, all Security Gateways share "equal priority." When all Security Gateways share "equal priority":

- Remote VPN peers send RDP packets to all the Security Gateways in the MEP configuration.
- The first Security Gateway to respond to the probing RDP packets gets chosen as the entry point to network. The idea behind *first to respond* is "proximity". The Security Gateway which is "closer" to the remote VPN peer responds first.
- A VPN tunnel is opened with the first to respond. All subsequent connections pass through the chosen Security Gateway.
- If the Security Gateway ceases to respond, a new Security Gateway is chosen.

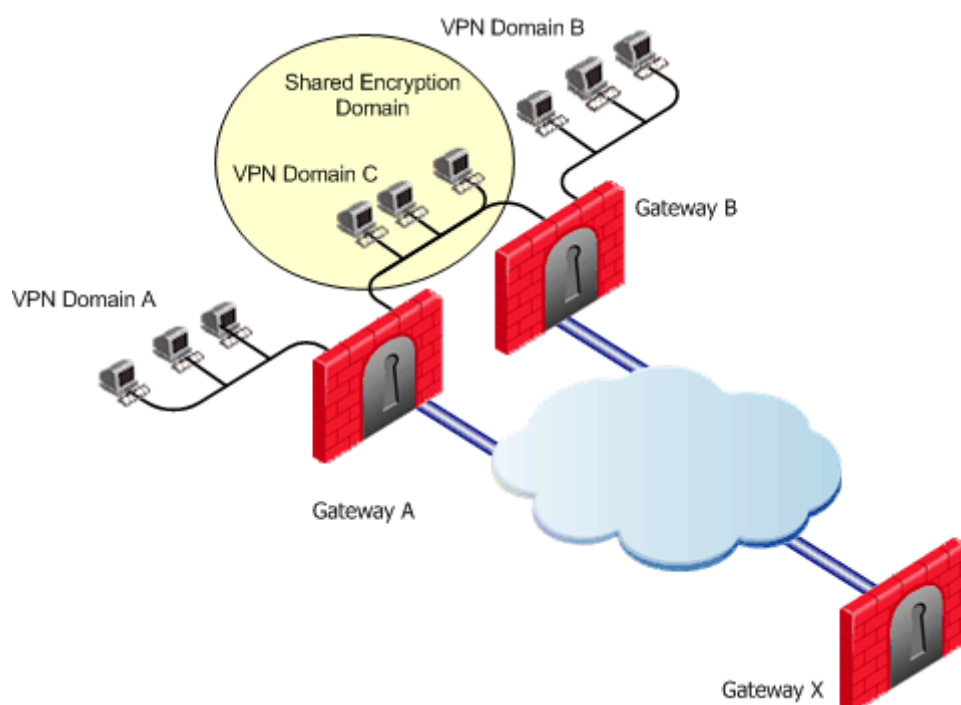
In a star community, RDP packets are sent to the Security Gateways and the first to respond is used for routing only when:

There is more than one center Security Gateway, **and**

One of the following VPN routing options was selected:

- **To center and to other satellites through center**
 - **To center, or through the center to other satellites, to internet and other VPN targets**
- This setting is found on the **Community Properties > VPN Advanced > VPN Routing** page.

In this scenario:



- MEP is **not** enabled on the community
- First to respond method is used
- Security Gateway X accesses VPN domain A through Security Gateway A
- Security Gateway X accesses VPN domain B through Security Gateway B
- Security Gateway X accesses VPN domain C through Security Gateway A or B

In a star community, RDP packets are sent to the Security Gateways and the first to respond is used for routing when:

There is more than one center Security Gateway, **and**

One of the following VPN routing options was selected:

- **To center and to other satellites through center**

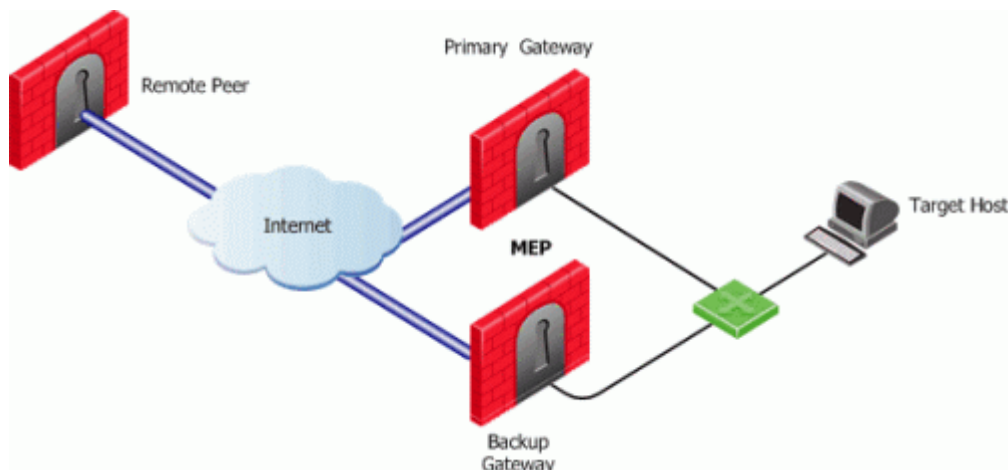
- To center, or through the center to other satellites, to internet and other VPN targets

This setting is found on the **Community Properties > VPN Advanced > VPN Routing** page.

Primary-Backup Security Gateways

Backup Security Gateways provide redundancy for primary Security Gateways. If the primary Security Gateway fails, connections go through the backup.

In this scenario:



The first Security Gateway is configured as the "primary," and the second Security Gateway as the "backup." If the primary Security Gateway fails, for whatever reason, the remote VPN peer detects that the link has gone down and works through the backup Security Gateway. The backup gateway inherits the complete VPN domain of the primary. Failover within an existing connection is not supported; the current connection is lost.

When the primary Security Gateway is restored, new connections go through the primary Security Gateway while connections that already exist will continue to work through the backup Security Gateway.



Note - When using the Primary-Backup Security Gateways method, the encryption domains should not overlap

Load Distribution

To prevent any one Security Gateway from being flooded with connections, the connections can be evenly shared amongst all the Security Gateways to distribute the load. When all Security Gateways share equal priority (no primary) and are MEPed to the *same* VPN domain, it is possible to enable load distribution between the Security Gateways. The Security Gateways are probed with RDP packets, as in all other MEP configurations, to create a list of responding Security Gateways. A Security Gateway is randomly chosen from the list of responding Security Gateways. If a Security Gateways stops responding, a new Security Gateway is (randomly) chosen.

A new Security Gateway is randomly selected for every source/destination IP pair. While the source and destination IP's remain the same, the connection continues through the chosen Security Gateway.

Routing Return Packets

To make sure return packets are routed correctly, the MEPed Security Gateway can make use of either:

- IP pool NAT (static NAT) or
- Route Injection Mechanism

IP Pool Network Address Translation (NAT)

IP pool NAT is a type of NAT in which source IP addresses from remote VPN domains are mapped to an IP address drawing from a pool of registered IP addresses. In order to maintain symmetric sessions using MEPed Security Gateways, the MEPed Security Gateway performs NAT using a range of IP addresses

dedicated to that specific Security Gateway and should be routed within the internal network to the originating Security Gateway. When the returning packets reach the Security Gateway, the Security Gateway restores the original source IP address and forwards the packets to the source.

RIM

Route Injection Mechanism (RIM) enables a Security Gateway to use a dynamic routing protocol to propagate the encryption domain of a VPN peer Security Gateway to the internal network. When a VPN tunnel is created, RIM updates the local routing table of the Security Gateway to include the encryption domain of the VPN peer.

When a tunnel to a MEPed Security Gateway goes down, the Security Gateway removes the appropriate "return route" from its own local routing table. This change is then distributed backwards to the routers behind the Security Gateway.

RIM is based both on the ability of the Security Gateway to update its local routing table, and the presence of the a dynamic routing protocol to distribute the change to the network behind the Security Gateway. There is little sense in enabling RIM on the Security Gateway if a dynamic routing protocol is not available to distribute changes.

When MEP is enabled, RIM can be enabled only if permanent tunnels are enabled for the whole community. In a MEP configuration RIM is available when using the *First to Respond*, *Manual set priority list*, and *VPN Domain* mechanisms. In the first two options, satellite Security Gateways "see" the center Security Gateways as unified as if one tunnel is connecting them. As a result, only the chosen MEP Security Gateway will inject the routes. In *VPN Domain* MEP, it could be that all MEP Security Gateways will inject the routes, which requires configuring the routers behind the MEP Security Gateways to return packets to the correct Security Gateway.

RIM is not available when *Random Selection* is the selected entry point mechanism.

For more information on RIM, see [Route Injection Mechanism](#) (on page 82).

Special Considerations

1. If one of the central Security Gateways is an externally managed Security Gateway:
 - The VPN domain of the central Security Gateways will not be automatically inherited by an externally managed Security Gateway
 - The RIM configuration will not be automatically downloaded
2. UTM-1 Edge Security Gateways cannot be configured as a MEP Security Gateway but can connect to MEPed Security Gateways.
3. DAIP Security Gateways require DNS resolving in order to be configured as MEP Security Gateways.

Configuring MEP

To configure MEP, decide on:

1. The MEP method
 - Explicit MEP - See [Explicit MEP](#) (on page 118).
 - Implicit MEP - See [Implicit MEP](#) (on page 123).
1. If required, method for returning reply packets:
 - IP pool NAT
 - RIM - To configure RIM, see [Configuring RIM](#) (on page 85).

Configuring Explicit MEP

Explicit MEP is only available in Site-to-Site Star VPN communities where multiple central Security Gateways are defined.

To configure MEP:

1. Open the **Star Community properties page > Advanced Settings > MEP (Multiple Entry Point)**:
Select **Enable center Security Gateways as MEP**.
2. Select an entry point mechanism:

- First to respond
- By VPN domain
- Random selection
- Manual priority list

If "By VPN domain" or "Manually set priority list" is selected, click **Advanced** to resolve how more than one Security Gateway with equal priority should be selected.

If "Manually set priority list" is selected, click **Set** to create a series of MEP rules.

3. Select a tracking option, if required.

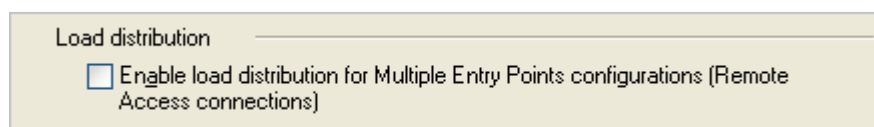
Configuring Implicit MEP

Configuring Implicit First to Respond

When more than one Security Gateway leads to the same (overlapping) VPN domain, they are in a MEP configuration. The first Security Gateway to respond is chosen. To configure *first to respond*, define that part of the network that is shared by all the Security Gateways into a single group and assign that group as the VPN domain.

Before you begin, make sure that **Load Distribution** is not selected on SmartDashboard > **Global Properties > Remote Access** :

- NGX R65 and R70: **VPN Basic**
- R71 and higher: **VPN Advanced**



To configure First to Respond MEP:

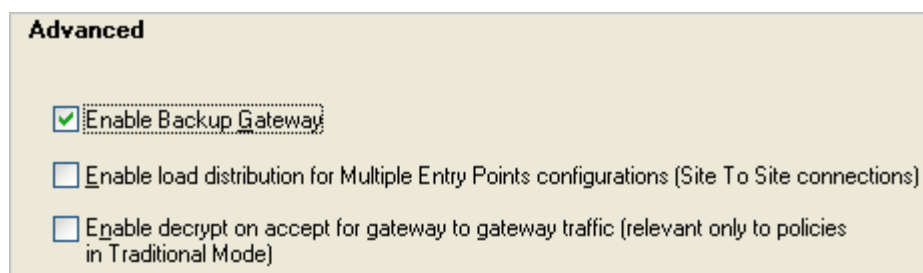
1. Find out which Security Gateways are in the VPN domain. In the VPN CLI, run:
`vpn overlap_endom`
2. Create a host group and assign all these Security Gateways to it.
3. On the **Properties** window of each Security Gateway network object, **Topology** page > **VPN Domain** section, select **Manually defined** and then select the host group of MEP gateways.
4. Click **OK**.
5. Install the policy.

Configuring Implicit Primary-Backup

Configure the VPN Domain that includes the Primary gateway and another domain that includes only the backup gateway. Configure each gateway as either the Primary gateway or a backup gateway.

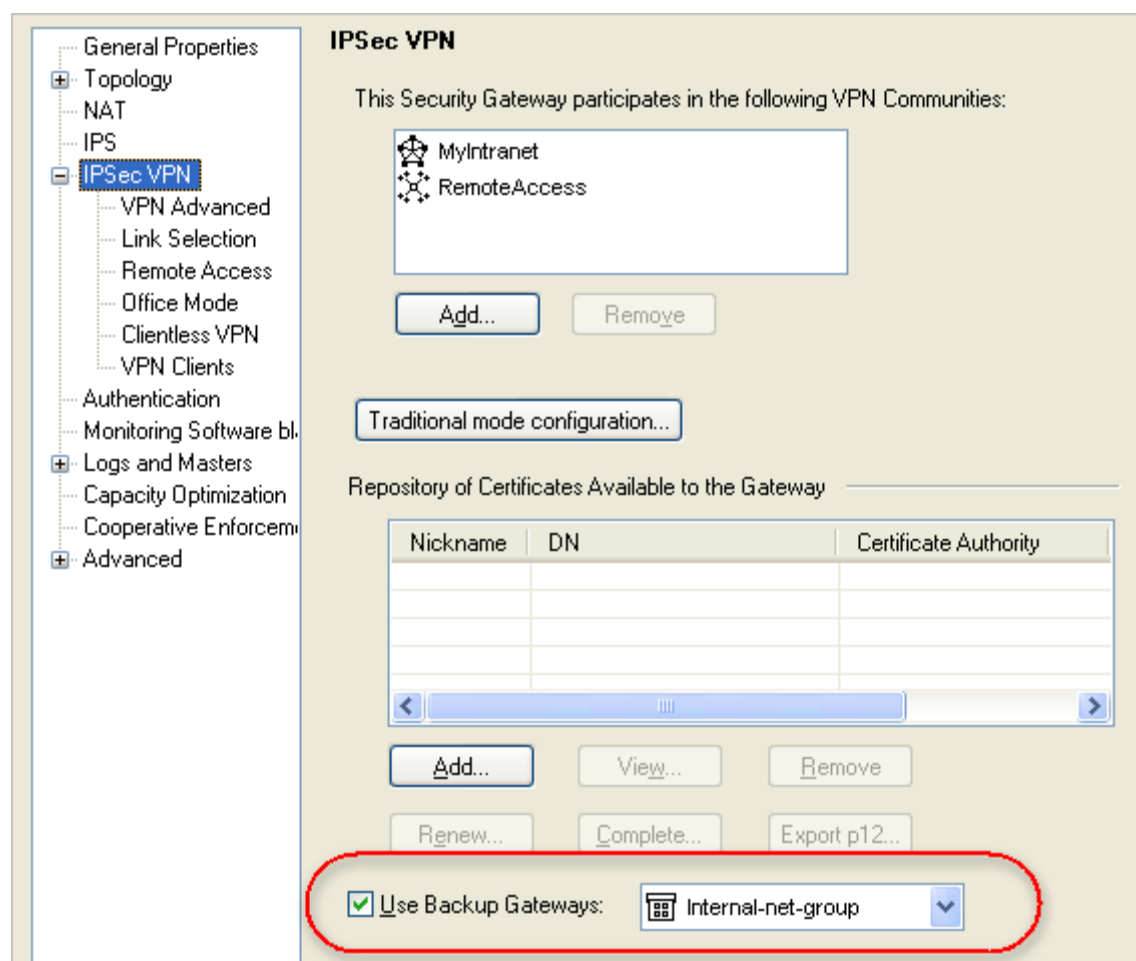
To configure the primary gateway:

1. Open **Global Properties** window > **VPN > Advanced**, select **Enable Backup Gateway**.



2. In the network objects tree, **Groups** section, create a group of gateways to act as backup gateways.
3. Open the VPN properties of the Primary gateway:
 - NGX R65 and R70: Gateway properties > **VPN**
 - R71 and higher: Gateway properties > **IPSec VPN**

4. Select **Use Backup Gateways**, and select the group of backup gateways.



This gateway is the primary gateway for this VPN domain.

5. For each backup gateway, make a VPN domain that does not include IP addresses that are in the Primary VPN domain or the other backup domains.
If the backup gateway already has a VPN domain, you must make sure that its IP addresses do not overlap with the other VPN domains.
 - a) Create a group of IP addresses not in the other domains, or a group that consists of only the backup gateway.
 - b) On the **Properties** window of the backup network object > **Topology** > **VPN Domain** section, select **Manually defined**.
 - c) Select the group.
6. Click **OK**.
7. Install the policy.

Configuring Implicit Load Distribution

To configure implicit MEP for random gateway selection:

1. Open **Global Properties**.
2. Open **IPSec VPN > Advanced** (or **VPN > Advanced**).
3. Select **Enable load distribution for Multiple Entry Point configurations (Site to Site connections)**.
4. Define the same VPN domain for all the gateways:
 - a) Create a group of the gateways.
 - b) On the **Properties** window of each gateway network object > **Topology** > **VPN Domain** section, select **Manually defined**.
 - c) Select the group.
5. Click **OK**.

6. Install the policy.

Configuring IP Pool NAT

To configure IP pool NAT:

1. In **Global Properties > NAT** page, select **Enable IP Pool NAT**.
2. Set tracking options for address exhaustion and for address allocation and release. Then:
3. For each Security Gateway, create a network object that represents the IP pool NAT addresses for that Security Gateway. The IP pool can be a network, group, or address range. For example:
 - On the network objects tree, right-click **Network Objects** branch > **New > Address Range...** The Address Range Properties window opens.
 - On the **General** tab, enter the first IP and last IP of the address range.
 - Click **OK**. In the network objects tree, **Address Ranges** branch, the new address range appears.
4. On the Security Gateway object where IP pool NAT translation is performed, **Security Gateway Properties** window, **NAT > IP Pool NAT** page, select either
 - **Allocate IP Addresses** from, and select the address range you created, OR
 - **Define IP Pool addresses on Security Gateway interfaces**. If you choose this option, you need to define the IP Pool on each required interface, in the **Interface Properties** window, **IP Pool NAT** tab.
5. In the **IP Pool NAT** page, select either (or all):
 - **Use IP Pool NAT for VPN clients connections**
 - **Use IP Pool NAT for Security Gateway to Security Gateway connections**
 - **Prefer IP Pool NAT over Hide NAT**
6. Click **Advanced...**
 - Decide after how many minutes unused addressees are returned to the IP pool.
 - Click **OK** twice.
7. Edit the routing table for each internal router, so that packets with an IP address assigned from the NAT pool are routed to the appropriate Security Gateway.

Chapter 13

Traditional Mode VPNs

In This Chapter

| | |
|---|-----|
| Introduction to Traditional Mode VPNs | 130 |
| VPN Domains and Encryption Rules | 131 |
| Defining VPN Properties | 132 |
| Internally and Externally Managed Security Gateways | 132 |
| Considerations for VPN Creation | 132 |
| Configuring Traditional Mode VPNs | 132 |

Introduction to Traditional Mode VPNs

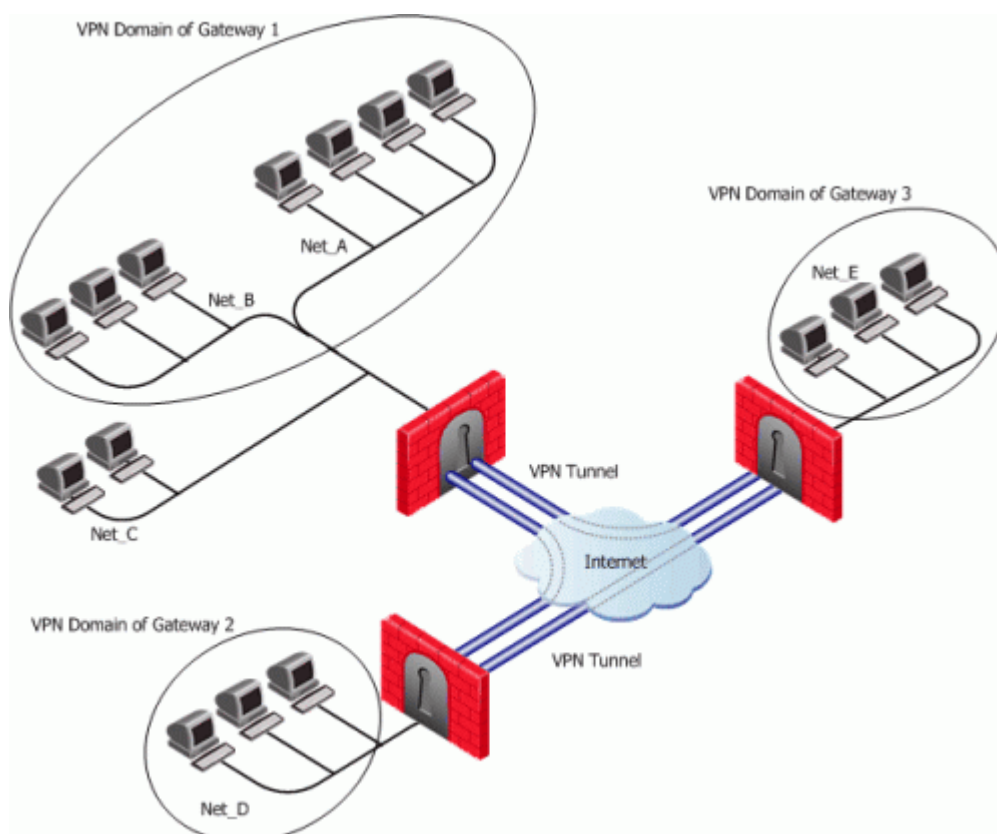
The Simplified Mode lets you maintain and create simpler, less error prone and more secure VPNs. It also makes it easier to understand the VPN topology of an organization, and to understand who is allowed to communicate with whom. In addition, new VPN features such as VPN routing are supported only with a Simplified Mode Security Policy.

However, organizations that have large VPN deployments with complex networks may prefer to maintain existing VPN definitions and continue to work within Traditional Mode until they are able to migrate their policies to Simplified Mode.

For guidelines on how to convert Traditional Mode VPNs to Simplified Mode, see [Converting a Traditional Policy to a Community Based Policy](#) (on page [137](#)).

VPN Domains and Encryption Rules

The figure depicts a VPN between Security Gateways, and the VPN Domain of each Security Gateway. Net_A and Net_B are the VPN Domain of Security Gateway 1, Net_D is the VPN Domain of Security Gateway 2, and Net_E is the VPN Domain of Security Gateway 3.



The Table below shows how the VPN is implemented in a rule. in Traditional VPN Mode. A single rule with the Encrypt rule action, deals with both access control and encryption.

Example Encrypt rule in a Traditional Rule Base

| Source | Destination | Service | Action | Track | Install On |
|--------|-------------|-------------|---------|-------|--------------------|
| Net_A | Net_A | My_Services | Encrypt | Log | Security Gateway 1 |
| Net_E | Net_E | | | | Gateway 3 |

A connection that matches an Encrypt rule is *encrypted* (or *decrypted*) and forwarded by the Security Gateways enforcing the policy. Sometimes, a connection may match the encrypt rule, but will not be encrypted. Consider the following rule:

Encrypt rule where encryption does not take place

| Source | Destination | Service | Action | Track | Install On |
|--------|-------------|-------------|---------|-------|----------------|
| X | Y | My_Services | Encrypt | Log | Policy targets |

If the source or the destination are behind the Security Gateway, but are not in the VPN Domain of the Security Gateway, the connection is *dropped*.

For example, if Source X is in Net_C and Destination Y is in Net_D, Security Gateway 1 drops the connection because the Action says Encrypt but the connection cannot be encrypted because the source is not in the VPN Domain of Security Gateway 1.

If the source and destination are inside the VPN Domain of the same Security Gateway. In this case, the connection is *accepted in the clear*.

For example, if Source X is in Net_A and Destination Y is in Net_B, the connection originates at X and reaches the Security Gateway, which forwards the response back to Y. The connection is not encrypted because there is no peer Security Gateway for Y that could decrypt the connection. A SmartView Tracker log is issued "**Both endpoints are in the Encryption Domain**".

Defining VPN Properties

It is possible to use different encryption methods between the same Security Gateways. Different connections between two Security Gateways can be encrypted using different methods. This is because different IKE phase 2 properties can be defined per Encrypt rule.

IKE Phase 1 properties are defined per Security Gateway.

Internally and Externally Managed Security Gateways

The Security Gateways at each end of a VPN tunnel can be managed by the same Security Management server or by different Security Management servers. A Security Gateway that is managed by the Security Management server is called an internal Security Gateway. If it is managed by a different Security Management server it is called an external Security Gateway.

If the peer Security Gateway is external, you must obtain certain details about that Security Gateway from the peer administrator, and configure them in SmartDashboard.

Considerations for VPN Creation

There are many ways of setting up a VPN. Before starting, a number of issues need to be considered, such as choosing the:

- Authentication method
- Certificate authority

Choosing the Authentication Method

Before Security Gateways can create a VPN tunnel, they need to authenticate to each other. This authentication is performed either by means of certificates or with a pre-shared secret. Certificates are considered to be a stronger form of authentication.

Choosing the Certificate Authority

If the Security Gateways use certificates, the certificates can be issued either by the Internal Certificate Authority (ICA) on the Security Management server, or by a third party OPSEC certified CA.

The Internal CA makes it very easy to use PKI for Check Point applications such as site-to-site and remote access VPNs. However, an administrator may prefer to continue using a CA that is already used within the organization, for generalized applications such as secure email, and disk encryption.

If the Security Gateways are both internally managed and use certificates for authentication, the easiest strategy is for both Security Gateways to present a certificate signed by the Internal CA.

Configuring Traditional Mode VPNs

Editing a Traditional Mode Policy

An existing Traditional Mode policy will open in Traditional Mode. To start a new Traditional Mode policy, proceed as follows.

1. In the **Global Properties** window, **VPN** page, select either **Traditional mode to all new Security Policies** or **Traditional or Simplified per new Security Policy**, and save the policy.

Assuming you selected **Traditional or Simplified per new Security Policy**:

1. From the **File** menu, select **New**. The **New Policy Package** window opens.
2. Give the new policy package a name.

3. Select **Security and Address Translation**.
 4. In the VPN configuration method area, select **Traditional mode** and click **OK**.
- In the Security Policy Rule Base, notice that one of the available Actions is **Encrypt**.

Configuring VPN Between Internal Gateways using ICA Certificates

Defining the Security Gateways

1. For each Security Gateway that is to be part of the VPN define a Check Point Security Gateway object. In the Network Objects tree, right click and select **New > Check Point > Security Gateway....**
2. In the **General Properties** page of the Check Point Security Gateway object, select **VPN**.
3. In the **Communication** window, establish Secure Internal Communication.
4. In the **Topology** page, define the IP address, network mask, and anti-spoofing for every Security Gateway interface
5. Still on the **Topology** page, define the **VPN Domain**. select either:
 - **All IP Addresses behind Security Gateway based on Topology information** or
 - **Manually defined**. Either select an existing network or group from the drop-down list or create a new group of machines or networks by clicking **New...**
6. In the **VPN** page, **Certificate List** area, **Add** a certificate issued by the ICA.
7. Still on the **VPN** page, click **Traditional mode configuration**. The **Traditional mode IKE properties** window opens.
 - In the **Support authentication methods** area, select **Public Key Signatures**. To specify that the Security Gateway will only use certificates issued by the ICA, click **Specify** and select the ICA.
 - Select IKE Phase 1 encryption and data integrity methods or accept the checked defaults.

Defining the Encrypt Rule

1. In the Security Rule Base, define the Encrypt rule(s).
2. If you wish to change the IKE Phase 2 properties for this rule, double click the **Encrypt** action and make the required changes.

VPN Between Internal Gateways Using Third Party CA Certificates

Obtain the CA certificate, and define the Certificate Authority (CA) object. For details, see Enrolling with a Certificate Authority (on page [44](#)).

Defining the Security Gateways

1. Define the Check Point Security Gateway object. In the Network Objects tree, right click and select **New > Check Point > Security Gateway....**
2. In the **General Properties** page, select either **VPN**.
3. In the **Communication** window, establish Secure Internal Communication.
4. In the **Topology** page, define the IP address, network mask, and anti-spoofing for every Security Gateway interface.
5. Still on the **Topology** page, define the **VPN Domain**. select either:
 - **All IP Addresses behind Security Gateway based on Topology information** or
 - **Manually defined**. Either select an existing network or group from the drop-down list, or create a new network or group by clicking **New....**
6. In the **VPN** page, **Certificate List** area, **Add** a certificate issued by the certificate authority defined in step 1. For details, see Enrolling with a Certificate Authority (on page [44](#)).
7. Still on the **VPN** page, click **Traditional mode configuration**. The **Traditional mode IKE properties** window opens.
 - In the **Support authentication methods** area, select **Public Key Signatures**. To specify that the Security Gateway will only use certificates issued by the CA specified in step 1, click **Specify** and select the CA.
 - Select IKE Phase 1 encryption and data integrity methods or accept the checked defaults.
8. Repeat step 2 to step 8 for each Security Gateway taking part in the VPN.

Defining the Encrypt Rule

1. In the Security Rule Base, define the Encrypt rule(s).
2. If you wish to change the IKE Phase 2 properties for this rule, double click the **Encrypt** action and make the required changes.

Configuring VPN with Externally Managed Gateways Using Certificates

Obtain Information from the Peer Administrator

Obtain the Security Gateway topology and VPN Domain information about the externally managed Security Gateways from the peer administrator.

You must also agree on authentication, encryption and data integrity methods for the VPN.

You must also obtain the CA certificate of the peer, either from the peer administrator or directly from the peer CA.

Defining the CAs

1. Obtain the CA certificate and create the Certificate Authority (CA) object for the internally managed Security Gateways. For details, see Enrolling with a Certificate Authority (on page 44).
2. Define the CA object for the externally managed Security Gateways, and configure it using the peer CA certificate.

Defining the Internally Managed Security Gateways

1. Create the Check Point Security Gateway object. In the Network Objects tree, right click and select **New > Check Point > Security Gateway....**
2. In the **General Properties** page, select either **VPN**.
3. In the **Communication** window, establish Secure Internal Communication.
4. In the **Topology** page, define the IP address, network mask, and anti-spoofing for every Security Gateway interface.
5. Still on the **Topology** page, define the **VPN Domain**. select either:
 - **All IP Addresses behind Security Gateway based on Topology information** or
 - **Manually defined**. Either select an existing network or group from the drop-down list, or create a new network or group by clicking **New....**
6. In the **VPN** page, **Certificate List** area, **Add** a certificate issued by the certificate authority defined in step 1. For details, see Enrolling with a Certificate Authority (on page 44).
7. Still on the **VPN** page, click **Traditional mode configuration**. The **Traditional mode IKE properties** window opens.
 - In the **Support authentication methods** area, select **Public Key Signatures**. To specify that the Security Gateway will only use certificates issued by the CA specified in step 1, click **Specify** and select the CA.
 - Select IKE Phase 1 encryption and data integrity methods or accept the checked defaults.
8. Repeat step 3 to step 9 for each internally managed Security Gateway.

Defining the Externally Managed Security Gateways

1. Create the externally managed Security Gateway object:
 - If it is a Check Point Security Gateway, in the **Network Objects** tree, right click and select **New > Check Point > Externally Managed Security Gateway....**
 - If it is not a Check Point Security Gateway, select **Manage > Network Objects.. .> New...> Interoperable Device....**
2. For an external Check Point Security Gateway only: In the **General Properties** page, select **VPN**.
3. Using the topology information supplied by the peer administrator, in the **Topology** page, manually define the IP address and network mask for every Security Gateway interface.
4. Using the VPN Domain information supplied by the peer administrator, define the VPN domain in the **VPN Domain** section of the Topology page. Either select **All IP Addresses behind Security Gateway based on Topology information** or manually define a group of machines or a network and set them as the VPN domain.

5. On the **VPN** page, click **Traditional mode configuration**. The **Traditional mode IKE properties window** opens.
 - Select IKE Phase 1 encryption and integrity methods (in coordination with the peer Security Gateway's administrator) or accept the defaults.
 - In the **Support authentication methods** area, select **Public Key signatures**.
6. On the VPN page, click **Matching Criteria....** The **Certificate Matching Criteria** window opens. The configurations settings in this window force the externally managed Security Gateway to present a certificate from a defined CA, and require that the details on the certificate match those specified here. This is enforced by the internally managed Security Gateways during IKE negotiation.

Defining the Encrypt Rule

1. In the Security Rule Base, define the Encrypt rule(s).
2. If you wish to change the IKE Phase 2 properties for this rule, double click the **Encrypt** action and make the required changes.

Configuring a VPN using a Pre-Shared Secret

When using a pre-shared secret to authenticate Security Gateways, you need to enable each Security Gateway in the VPN for pre-shared secrets. Then, on each Security Gateway, define a pre-shared secret for each of the other Security Gateways. However, for each pair of Security Gateways, you only need to define the pre-shared secrets for the pair on one of the Security Gateways.

For example, in a VPN with four Security Gateways, A,B, C and D, there will be six secrets: A-B, A-C, A-D, B-C, B-D and C-D.

- On A define the secrets for B, C and D.
- On B define the secrets for C and D.
- On C define the secret for D.

The following procedure applies to both internal and external Security Gateways. When working with externally managed Security Gateways, the administrator of the peer external Security Gateways must configure his or her Security Gateways appropriately.

Obtain Information from the Peer Administrator

If working with externally managed Security Gateways, obtain from the peer administrator the external Security Gateway topology and VPN Domain information.

You must also agree on the pre-shared secrets, and on authentication, encryption and data integrity methods for the VPN.

Defining the Security Gateways

1. Define the Security Gateway object.
 - If the Security Gateway is an internal Security Gateway, define a Check Point Security Gateway object. In the Network Objects tree, right click and select **New > Check Point > Security Gateway....**
 - If the Security Gateway is externally managed:
 - If it is a Check Point Security Gateway, In the **Network Objects** tree, right click and select **New > Check Point > Externally Managed Security Gateway....**
 - If it is not a Check Point Security Gateway, select **Manage > Network Objects... > New... > Interoperable Device....**
2. For an internally managed Security Gateway or for a Check Point externally managed Security Gateway, in the **General Properties** page of the Security Gateway object, select **VPN**.
3. For an internally managed Security Gateway only, in the **Communication** window, establish Secure Internal Communication.
4. In the **Topology** page, define the IP address, network mask, and anti-spoofing for every Security Gateway interface
5. Still on the **Topology** page, define the **VPN Domain**. select either:
 - **All IP Addresses behind Security Gateway based on Topology information** or

- **Manually defined.** Either select an existing network or group from the drop-down list or create a new group of machines or networks by clicking **New...**
6. In the **VPN** page, click **Traditional mode configuration**. The **Traditional mode IKE properties** window opens.
 - In the **Support authentication methods** area, select **Pre-shared Secret**, click **Edit Secrets....** Only peer Security Gateways which support pre-shared secrets appear in the list.
 - Type a secret for each peer Security Gateway.
 - Select IKE phase 1 encryption and data integrity methods or accept the checked defaults.
 7. Repeat step 1 to step 6 for each Security Gateway taking part in the VPN.

Defining the Encrypt Rule

1. In the Security Rule Base, define the Encrypt rule(s).
2. If you wish to change the IKE Phase 2 properties for this rule, double click the **Encrypt** action and make the required changes.

Chapter 14

Converting a Traditional Policy to a Community Based Policy

In This Chapter

| | |
|---|-----|
| Introduction to Converting to Simplified VPN Mode | 137 |
| How Traditional VPN Mode Differs from a Simplified VPN Mode | 137 |
| How an Encrypt Rule Works in Traditional Mode | 138 |
| Principles of the Conversion to Simplified Mode | 139 |
| Placing the Security Gateways into the Communities | 139 |
| Conversion of Encrypt Rule | 139 |

Introduction to Converting to Simplified VPN Mode

Building VPNs using Simplified Mode has many benefits. Simplified Mode makes it possible to maintain and create simpler, and therefore less error prone and more secure VPNs.

Simplified Mode separates the VPN definitions from the Access Control Security Policy. This makes it easier to understand the VPN topology of an organization, and to understand who is allowed to securely communicate with who. In addition, such as VPN routing are supported only with a Simplified Mode Security Policy.

In order to manage all existing policies in a unified way and utilize the latest features of the current release, it is recommended to convert Traditional Mode Security Policies to Simplified Mode. For new policies, it is recommended to use Simplified Mode, the default option.

A security policy configured in Traditional Mode can be converted to the Simplified VPN Mode using the Security Policy Converter Wizard.

After using the converter wizard, it is possible to greatly simplify many security policies by moving rules and grouping rules together.

The process is simple, and both automatic and manual changes are explained here in detail. The intention is to give you the confidence to move your Traditional VPN Policies to the Simplified VPN Mode.

To start the converter wizard, save the Policy, and from the SmartDashboard main menu, select **Policy > Convert to > Simplified VPN...**

How Traditional VPN Mode Differs from a Simplified VPN Mode

A Traditional Mode Security Policy differs from a Simplified Mode Policy in the following ways:

In Traditional VPN Mode, a single rule, with the Encrypt rule action, deals with both access control and encryption. VPN properties are defined per Security Gateway.

In Simplified VPN Mode, the Security Rule Base deals only with access control. In other words, the Rule Base determines only what is allowed. VPN properties, on the other hand, are dealt with per VPN community.

VPN communities are groups of Security Gateways. The community defines the encryption methods for the VPN. All communication between community members is encrypted, and all other communication is not encrypted.

Simplified VPN Mode and communities are described in Introduction to Site to Site VPN (on page 24).

The simplified VPN policy makes it easier for the administrator to configure a VPN. However, Traditional policies allow VPNs to be created with greater granularity than Simplified policies, because

- Whether or not to encrypt can be defined per rule (source, destination and service)

- Simplified policies requires all the connections between two Security Gateways to encrypted using the same methods, using the Community definitions.

What this means is that after running the wizard, some manual optimization of the Rule Base may be required.

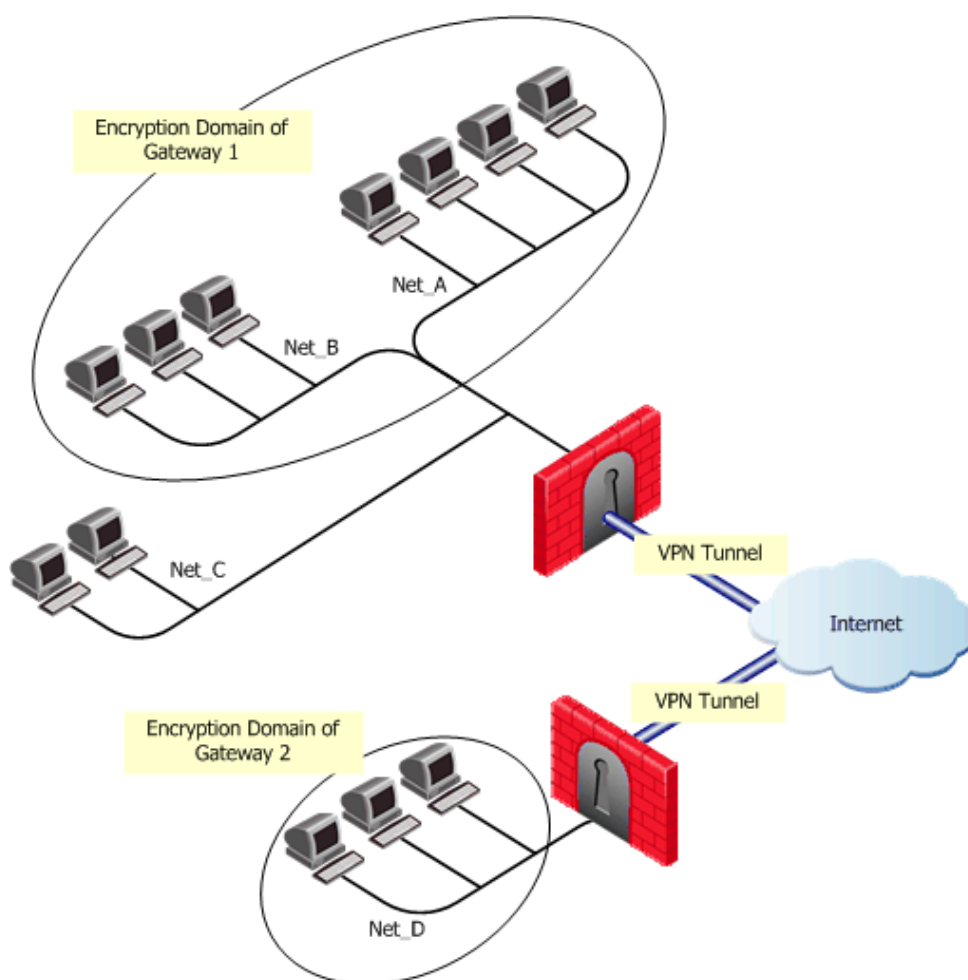


Note - The terms "VPN Domain" and "Encryption Domain" mean the same thing. Usually, "VPN Domain" is used in the context of Simplified policies, and "Encryption Domain" for Traditional policies.

How an Encrypt Rule Works in Traditional Mode

When a Traditional policy is converted to a Simplified policy, an Encrypt rule is converted to rules that use communities. In order to understand the conversion, it is important to understand how an Encrypt rule works.

The following figure will be used to understand the conversion, and the limitations of the conversion process. It shows a VPN between Security Gateways, and the Encryption Domain of each Security Gateway. Net_A and Net_B are the encryption Domain of Security Gateway 1, and Net_D is the encryption Domain of Security Gateway 2.



The following table shows how the VPN is implemented in an Encrypt rule.

Sample Encrypt rule in a Traditional Rule Base

| Source | Destination | Service | Action | Track | Install On |
|--------|-------------|-------------|---------|-------|----------------|
| X | Y | My_Services | Encrypt | Log | Policy Targets |

A connection that matches an Encrypt rule is *encrypted* (or *decrypted*) and forwarded by the Security Gateways enforcing the policy. There are two exceptions:

If the source or the destination are behind the Security Gateway, but are not in the VPN Domain of the Security Gateway, the connection is *dropped*.

For example, referring to Figure B-1 and Table B-1, if Source X is in Net_C and Destination Y is in Net_D, Security Gateway 1 drops the connection. This is because the Action says Encrypt but the connection cannot be encrypted because the source is not in the Encryption Domain of Security Gateway 1.

If the source and destination are inside the encryption Domain of the same Security Gateway. In this case, the connection is *accepted in the clear*.

For example, referring to Figure B-1 and Table B-1, if Source X is in Net_A and Destination Y is in Net_B, the connection originates at X and reaches the Security Gateway, which forwards the response back to Y. The connection is not encrypted because there is no peer Security Gateway for Y that could decrypt the connection. A SmartView Tracker log is issued **"Both endpoint are in the Encryption Domain"**.

Principles of the Conversion to Simplified Mode

The converter Wizard attempts to maintain the best possible balance between connectivity and security, by using the following principles:

- Refuse all traffic that could have been refused in traditional Mode. This may mean that some connections may be dropped that were allowed by the traditional rule base.
- Encrypt at least all traffic that would be encrypted in traditional policy. This means that the converted policy may encrypt more connections than the original policy.

What this means is that not all traditional policies can be converted in a way that exactly preserves the policy that is specified in the Security Rule Base. The converted rule(s) in the Simplified VPN can under certain circumstances behave somewhat differently than the encryption rule for Traditional VPNs (described in [How an Encrypt Rule Works in Traditional Mode](#) (on page 138)).

Running the converter is a simple two or three step process. After running the wizard, you should review the Security Rule Base to make sure that it has maintained its required functionality, and optimize it if needed.

Placing the Security Gateways into the Communities

The first step in converting a traditional VPN to a simplified VPN is to create VPN communities that describe the topology of the organization. The conversion wizard requires the administrator to place Security Gateways into communities. It cannot do this automatically because it is very difficult to deduce from the traditional policy what communities should be defined between Security Gateways.

The wizard allows you define communities, and to drag-and-drop Security Gateways into the communities. Referring to Figure B-1, the administrator must make Security Gateway 1 and Security Gateway 2 members of the same community by dragging both the Security Gateway objects into the same site-to-site community object.

You may prefer to create several communities with different encryption properties to reflect the way that the traditional VPN policy works.

If no communities have been previously defined, there are by default two predefined, empty community objects. One is a site-to-site VPN "intranet" community (a Mesh community), and the other is a remote access community. If these are the only two Communities, the wizard gives you the choice of simply placing all Security Gateways into the Site-to-Site Community, and placing all Remote Access Security Gateways into the Remote Access Community.

Conversion of Encrypt Rule

After Security Gateways have been placed into Communities, the Encrypt rules are converted. The converted rule base preserves the behavior of the Encrypt rule in Simplified VPN Mode to the greatest extent possible.

Encrypt rules are converted by the Conversion wizard to two rules:

A converted rule in a simplified Rule Base

| Source | Destination | VPN | Service | Action | Track | Install On |
|--------|-------------|--------------|-------------|--------|-------|----------------|
| X | Y | All_GW_to_GW | My_Services | Accept | Log | Policy Targets |
| X | Y | Any | My_Services | Drop | Log | Policy Targets |

The first rule says that the connection is matched and is allowed, if the connection originates at X and its destination is Y, within any Site-to-Site Community.

The second rule says that if a connection originates at X and has the destination Y, but is not encrypted (or decrypted) by any site-to-site community, the connection should be dropped.

The second rule (the Drop rule) is needed where either the source or the destination are not in the VPN Domain. In the Traditional policy, the Encrypt rule would drop this connection. If there were no drop rule in the Simplified policy, the connection may be matched to and allowed by a rule further down in the Rule Base.

When the Converted Rule Base is too Restrictive

This translation of Encrypt rules into two Simplified Mode rule is at least as restrictive as the original rule. However, in the converted Rule Base, some connections that were matched to and allowed by the original rule may be dropped. This may happen with connections between two hosts in the encryption domain of the same Security Gateway.

For example, in the Traditional mode rule, shown below, connections from a node in Net_A to a Node in Net_B are allowed:

Sample Encrypt Rule in a Traditional Rule Base

| Source | Destination | Service | Action | Track | Install On |
|--------|-------------|-------------|---------|-------|----------------|
| X | Y | My_Services | Encrypt | Log | Policy Targets |

After the conversion to Simplified mode, a node in Net_A to a Node in Net_B will be dropped by the converted Rule Base. This is because community rules define traffic between VPN Domains, and do not relate to traffic within a VPN Domain.

Converted Rule in a Simplified Rule Base

| Source | Destination | VPN | Service | Action | Track | Install On |
|--------|-------------|--------------|-------------|--------|-------|----------------|
| X | Y | All_GW_to_GW | My_Services | Accept | Log | Policy Targets |
| X | Y | Any | My_Services | Drop | Log | Policy Targets |

To allow these connections in the converted rule-base, you must explicitly allow them. To do this, add one rule between the first rule and the second rule, for each policy target appearing in the "install on" field. For example, the two Rules in the table above become three rules below:

Manually Added Rule in the converted Encrypt Rule Base

| Source | Destination | VPN | Service | Action | Track | Install On |
|--------|-------------|--------------|-------------|--------|-------|----------------|
| X | Y | All_GW_to_GW | My_Services | Accept | Log | Policy Targets |
| Net_A | Net_B | Any | My_Services | Accept | Log | Gateway 1 |
| X | Y | Any | My_Services | Drop | Log | Policy Targets |

In most cases it is not necessary to add these rules. Only add them when connections inside the encryption domain are matched by the Encrypt rule. An indication of this is the appearance of the log in SmartView Tracker **"Both endpoints are in the Encryption Domain."**

Conversion of Client Encrypt Rules

Each Client Encrypt rule translates to a single rule that preserves the behavior of the client Encrypt rule. For example, the Traditional Mode rule in the following table allows Remote Access users to access Net_D.

Remote Access Rule in Traditional Mode

| Source | Destination | Service | Action | Track |
|------------------|-------------|-------------|----------------|-------|
| All_Users@alaska | Net_D | My_Services | Client Encrypt | Log |

The translated rule is shown in the following table. The Remote Access community is put in the VPN field, and the Action of the rule is Accept:

Translated Remote Access Rule in Simplified Mode

| Source | Dest. | VPN | Service | Action | Track |
|------------------|-------|-------------------------|-------------|--------|-------|
| All_Users@alaska | Net_D | Remote Access Community | My_Services | Accept | Log |

Conversion of Auth+Encrypt Rules

In a Traditional Mode policy, Auth+Encrypt Rules are rules with User, Client or Session Authentication, together with **Add Encryption** selected in the Action of the Rule.

For Auth+Encrypt rules, as shown with Client Authentication in the following table, the Source specifies both a restriction on the source location, and also the authorized users. Any connection matching the rule must be authenticated and encrypted. If encryption is not possible, the connection is dropped.

Auth+Encrypt Rule in Traditional Mode

| Source | Destination | Service | Action | Track |
|------------------|-------------|-------------|-------------|-------|
| All_Users@alaska | Net_D | My_Services | Client_Auth | Log |

Since the identification of users is possible only in authentication rules, and not in drop rules, it is not possible to define a rule that drops connections that were not encrypted.

Add the Services that should not be encrypted inside the Community to the Excluded Services list. For example, if you have explicitly defined implied rules in the Traditional Policy. See [How to Authorize Firewall Control Connections in VPN Communities](#) (on page 38).

Because of this, Auth+Encrypt rules cannot be automatically translated in such a way that the translated Rule Base is at least as restrictive as the original rule. Instead, the Converter wizard translates Auth+Encrypt rules to a single rule, and does not add a Drop rule, as shown in the following table. This is a security problem, because connections that match the Source location, where the users authenticated successfully, but were not encrypted, may be accepted further down in the translated Rule Base if some later rule specifies Accept for the same Source.

Insecure Translated Auth+Encrypt Rule in Simplified Mode

| Source | Dest. | VPN | Service | Action | Track |
|------------------|-------|------------|-------------|-------------|-------|
| All_Users@alaska | Net_D | All_GwToGw | My_Services | Client Auth | Log |

When the converter encounters Auth+Encrypt rules, it warns the administrator by displaying an error stating that the converter cannot translate such rules automatically. In this case it is important to review the translated rule base before installing it, in order to avoid security breaches. It may be necessary to add rules to make sure that all the traffic that was previously dropped by the original Rule Base is dropped in the translated Rule Base.

How the Converter Handles Disabled Rules

If a rule in the Traditional VPN Rule Base was disabled, the translated rule in the simplified Rule Base will also be disabled.

After Running the Wizard

After running the Wizard, examine the Rule Base to see that it has retained the desired functionality, and if necessary, optimize the Rule Base, and make other changes, as follows. These points have been covered in the earlier discussion, but are summarized here for convenience:

Take out Unneeded Drop Rules

In some cases you can delete the second Drop rule generated by the conversion of an Encrypt rule because it will never match any connection, and the first rule is sufficient. This is the case for rules where the following are true:

- The source and destination are located in the encryption domain of Security Gateways appearing in the "Installed on" column of the rule.
- A Community links all Security Gateways protecting addresses in the Source and also links Security Gateways protecting addresses in the Destination.

Another case where you can delete the second Drop rule generated by the conversion of an Encrypt rule is where connections that do not match the first rule are dropped by rules that appear later in the Rule Base. Sometimes you can group several Drop rules generated by the conversion of several Encrypt rules into a single Drop rule.

Add Rules Allowing Communication Inside the VPN Domain

Connections matching Encrypt rules where both endpoints are located inside the encryption domain of the same Security Gateway, are accepted in a Traditional Rule Base. To achieve the same effect in the simplified rule base, you must manually add rules that accept the traffic inside the encryption domains of the Security Gateways. In most cases it is not necessary to add these rules. Add them if you see the SmartView Tracker log message: **"Both endpoint are in the Encryption Domain"**.

Auth+Encrypt Rules

Auth+Encrypt rules are not converted automatically. When such rules appear in the Rule Base, review the converted Rule Base and make sure that the security of these rules are maintained.

Remote Access VPN

In This Section

| | |
|---|-----|
| Check Point Remote Access Solutions | 144 |
| Remote Access VPN Overview | 149 |
| VPN for Remote Access Considerations | 155 |
| Configuring Remote Access VPN | 157 |
| Office Mode | 166 |
| Packaging SecureClient | 180 |
| Desktop Security | 185 |
| Layer Two Tunneling Protocol (L2TP) Clients | 187 |
| Secure Configuration Verification | 195 |
| VPN Routing - Remote Access | 219 |
| Link Selection for Remote Access Clients | 224 |
| Using Directional VPN for Remote Access | 225 |
| Remote Access Advanced Configuration | 227 |
| Multiple Entry Point for Remote Access VPNs | 234 |
| Userc.C and Product.ini Configuration Files | 238 |
| SSL Network Extender | 249 |
| Resolving Connectivity Issues | 271 |

Chapter 15

Check Point Remote Access Solutions

In This Chapter

| | |
|-----------------------------------|-----|
| Providing Secure Remote Access | 144 |
| Types of Solutions | 144 |
| Remote Access Solution Comparison | 145 |
| Summary of Remote Access Options | 146 |

Providing Secure Remote Access

In today's business environment, it is clear that workers require remote access to sensitive information from a variety of locations and a variety of devices. Organizations must also make sure that their corporate network remains safe and that remote access does not become a weak point in their IT security.

This chapter:

- Gives you information about Check Point's secure remote access options.
- Helps you decide which remote access client or clients best match your organization's requirements.
- Shows you where to get more information.

Types of Solutions

All of Check Point's Remote Access solutions provide:

- Enterprise-grade, secure connectivity to corporate resources.
- Strong user authentication.
- Granular access control.

Factors to consider when choosing remote access solutions for your organization:

- **Client-Based vs. Clientless** - Does the solution require a Check Point client to be installed on the endpoint computer or is it clientless, for which only a web browser is required. You might need multiple solutions within your organization to meet different needs.
- **Secure Connectivity and Endpoint Security** - Which capabilities does the solution include?
 - **Secure Connectivity** - Traffic is encrypted between the client and VPN gateway. After users authenticate, they can access the corporate resources that are permitted to them in the access policy. All Check Point solutions supply this.
 - **Endpoint Security** - Endpoint computers are protected at all times, even when there is no connectivity to the corporate network. Some Check Point solutions supply this.

Client-Based vs. Clientless

Check Point remote access solutions have different types of installation:

- **Client-based** - Must be installed on endpoint computers and devices before they can establish remote connections. Clients are usually installed on managed device, such as a company-owned computer. Clients supply access to all types of corporate resources.
- **Clientless** - Users connect through a web browser. Clientless solutions can be used on most computers, such as company-owned, personal, or public computers. No additional client is required on the endpoint computer. Clientless solutions usually supply access to web-based corporate resources.
- **On demand client** - Users connect through a web browser. When necessary, a client is automatically installed on the endpoint computer through the browser. On demand clients can be used on most

computers, such as company-owned, personal, or public computers. Clients supply access to all types of corporate resources.

All of these installation types use two encryption protocols, IPsec and SSL, to create secure remote access connections.

To meet the most requirements, a secure remote access solution can include IPsec and SSL VPN capabilities. The IPsec VPN Software Blade and Mobile Access Software Blade for SSL VPN can be enabled from one Check Point gateway.

All Check Point clients can work through NAT devices, hotspots, and proxies in situations with complex topologies, such as airports or hotels.

Secure Connectivity and Endpoint Security










You can combine secure connectivity with additional features to protect the network or endpoint computers.

- **Secure Connectivity** - Traffic is encrypted between the client and VPN gateway and strong user authentication is supported. All Check Point solutions supply this.
These solutions require licenses based on the number of users connected at the same time.
- **Security Verification for Endpoint computers** - Makes sure that devices connecting to the gateway meet security requirements. Endpoint machines that are not compliant with the security policy have limited or no connectivity to corporate resources. Some Check Point solutions supply this.
- **Endpoint Security:**
 - **Desktop Firewall** - Protects endpoint computers at all times with a centrally managed security policy. This is important because remote clients are not in the protected network and traffic to clients is only inspected if you have a Desktop Firewall. Some Check Point solutions supply this
 - **More Endpoint Security Capabilities** - Check Point solutions can include more Endpoint Security capabilities, such as anti-malware, disk encryption and more.

These solutions require licenses based on the number of clients installed.

Remote Access Solution Comparison

Details of the newest version for each client and a link for more information are in sk67820 (<http://supportcontent.checkpoint.com/solutions?id=sk67820>).

| Name | Supported Operating Systems | Client or Clientless | Encryption Protocol | Security Verification for Endpoint Devices | Desktop Firewall on Endpoint Devices |
|--|-----------------------------|--|---------------------|---|---|
| Mobile Access Web Portal | Windows, Linux, Mac | Clientless | SSL |  | |
| SSL Network Extender for Mobile Access Blade | Windows, Linux, Mac OS | On-demand Client through Mobile Access Portal) | SSL |  | |
| Check Point Mobile for iPhone and iPad | iOS | Client | SSL | | |
| Check Point Mobile VPN for iOS | iOS | Client | IPsec / SSL | | |
| Check Point Mobile for Android | Android | Client | SSL | | |
| SecuRemote | Windows | Client | IPsec | | |
| Check Point Mobile for Windows | Windows | Client | IPsec |  | |
| Endpoint Security VPN for Windows | Windows | Client | IPsec |  |  |
| Endpoint Security VPN for Mac | Mac OS | Client | IPsec | |  |
| Endpoint Security Suite Remote Access VPN Blade | Windows | Client | IPsec |  |  |
| Check Point GO VPN | Windows | Clientless - Requires a Check Point GO device | SSL |  | |

Summary of Remote Access Options

Below is a summary of each Remote Access option that Check Point offers. All supply secure remote access to corporate resources, but each has different features and meets different organizational requirements.

Details of the newest version for each client and a link for more information are in sk67820 (<http://supportcontent.checkpoint.com/solutions?id=sk67820>).

Mobile Access Web Portal

The Mobile Access Portal is a clientless SSL VPN solution. It is recommended for users who require access to corporate resources from home, an internet kiosk, or another unmanaged computer. The Mobile Access Portal can also be used with managed devices.

It provides:

- Secure Connectivity
- Security Verification

The Mobile Access Portal supplies access to web-based corporate resources. You can use the on-demand client, SSL Network Extender, through the Portal to access all types of corporate resources.

Required Licenses: Mobile Access Software Blade on the gateway.

Supported Platforms: Windows, Mac OS X, Linux

Where to Get the Client: Included with the Security Gateway (sk67820)

SSL Network Extender

SSL Network Extender is a thin SSL VPN on-demand client installed automatically on the user's machine through a web browser. It supplies access to all types of corporate resources.

SSL Network Extender has two modes:

- **Network Mode** - Users can access all application types (Native-IP-based and Web-based) in the internal network. To install the Network Mode client, users must have administrator privileges on the client computer.
Supported Platforms: Windows, Mac OS X, Linux
- **Application Mode** - Users can access most application types (Native-IP-based and Web-based) in the internal network, including most TCP applications. The user does not require administrator privileges on the endpoint machine.
Supported Platforms: Windows

Required Licenses:

Mobile Access Software Blade on the gateway

Where to Get the Client: Included with the Security Gateway (sk67820)

SecuRemote

SecuRemote is a secure, but limited-function IPsec VPN client. It provides secure connectivity.

Required Licenses: IPsec VPN Software Blade on the gateway. It is a **free** client and does not require additional licenses.

Supported Platforms: Windows

Where to Get the Client: Check Point Support Center (sk67820)

Check Point Mobile for Windows

Check Point Mobile for Windows is an IPsec VPN client. It is best for medium to large enterprises that do not require an Endpoint Security policy.

It provides:

- Secure Connectivity
- Security Verification

Required Licenses: IPsec VPN and Mobile Access Software Blades on the gateway.

Supported Platforms: Windows

Where to Get the Client: Check Point Support Center (sk67820)

Endpoint Security VPN

Endpoint Security VPN is an IPsec VPN client that replaces SecureClient. It is best for medium to large enterprises.

It provides:

- Secure Connectivity
- Security Verification
- Endpoint Security that includes an integrated Desktop Firewall, centrally managed from the Security Management Server.

Required Licenses: The IPsec VPN Software Blade on the gateway, an Endpoint Container license, and an Endpoint VPN Software Blade license on the Security Management Server.

Supported Platforms: Windows

Where to Get the Client: Check Point Support Center (sk67820)



Note - Endpoint Security VPN on Mac OS X includes a Desktop Firewall but not Security Verification.

Endpoint Security Suite

The Endpoint Security Suite simplifies endpoint security management by unifying all endpoint security capabilities in a single console. Optional Endpoint Security Software Blades include: Firewall, Compliance Full Disk Encryption, Media Encryption & Port Protection, and Anti-Malware & Program Control. As part of this solution, the Remote Access VPN Software Blade provides full, secure IPsec VPN connectivity.

The Endpoint Security suite is best for medium to large enterprises that want to manage the endpoint security of all of their endpoint computers in one unified console.

Required Licenses: Endpoint Security Container and Management licenses and an Endpoint VPN Software Blade on the Security Management Server.

Supported Platforms: Windows

Where to Get the Client: Check Point Support Center (sk67820)

Check Point Mobile for iPhone and iPad

Check Point Mobile for iPhone and iPad is an SSL VPN client. It supplies secure connectivity and access to web-based corporate resources and Exchange ActiveSync.

Check Point Mobile for iPhone and iPad is ideal for mobile workers who have iPhone or iPad devices.

Required Licenses: Mobile Access Software Blade on the gateway

Supported Platforms: iOS

Where to Get the Client: Apple App Store

Check Point Mobile for Android

Check Point Mobile for Android is an SSL VPN client. It supplies secure connectivity and access to web-based corporate resources and Exchange ActiveSync.

Check Point Mobile for Android is ideal for mobile workers who have Android devices.

Required Licenses: Mobile Access Software Blade on the gateway

Supported Platforms: Android

Where to Get the Client: Android Market

Check Point GO

Check Point GO is a portable workspace with virtualized Windows applications, on a secure and encrypted USB Flash Drive. Users insert the USB device into a host PC and securely access their workspace and corporate resources through SSL VPN technology.

Check Point GO is ideal for mobile workers, contractors, and disaster recovery. The virtual workspace is segregated from the host PC and controls the applications and data that can run in Check Point GO.

It provides:

- Secure Connectivity
- Security Verification

Required Licenses: IPsec VPN Software Blade on the gateway and Check Point GO devices.

Supported Platforms: Windows

Where to Get the Client: Check Point Support Center (sk67820)

Chapter 16

Remote Access VPN Overview

In This Chapter

| | |
|-------------------------------------|-----|
| Remote Access VPN Overview | 149 |
| SecureClient Remote Access Solution | 149 |
| Need for Remote Access VPN | 154 |

Remote Access VPN Overview

Whenever users access the organization from remote locations, it is essential that the usual requirements of secure connectivity be met but also the special demands of remote clients, for example:

- The IP of a remote access client might be unknown.
- The remote access client might be connected to a corporate LAN during the working day and connected to a hotel LAN during the evening, perhaps hidden behind some kind of NATing device.
- The remote client might need to connect to the corporate LAN via a wireless access point.
- Typically, when a remote client user is out of the office, they are not protected by the current security policy; the remote access client is both exposed to Internet threats, and can provide a way into the corporate network if an attack goes through the client.

To resolve these issues, a security framework is needed that ensures remote access to the network is properly secured.

Check Point's Remote Access VPN solutions enable you to create a VPN tunnel between a remote user and your organization's internal network. The VPN tunnel guarantees:

- Authenticity, by using standard authentication methods
- Privacy, by encrypting data
- Integrity, by using industry-standard integrity assurance methods

Check Point Remote Access Clients extend VPN functionality to remote users, enabling users to securely communicate sensitive information to networks and servers over the VPN tunnel, using LAN, wireless LAN and various dial-up (including broadband) connections. Users are managed either in the internal database of the Security Gateway or via an external LDAP server.

After a user is authenticated, a transparent secured connection is established.

SecureClient Remote Access Solution



Note - SecureClient is a legacy client. See Check Point Remote Access Solutions (on page 144) for more options.

Enhancing SecuRemote with SecureClient Extensions

SecureClient is a remote access client that includes and extends SecuRemote by adding a number of features:

- Security features
- Connectivity features
- Management features

Security Features

- A Desktop Security Policy. See: Desktop Security (on page 185).
- Logging and Alerts
- Secure Configuration Verification (SCV); (see: Secure Configuration Verification (on page 195))

Connectivity Features

- Office mode addresses (see: Office Mode (on page 166)).
- Visitor mode (see: Resolving Connectivity Issues (on page 271)).
- Hub mode. (see: Hub Mode (VPN Routing for Remote Clients (see "Hub Mode (VPN Routing for Remote Clients)" on page 220)).)

Management Features

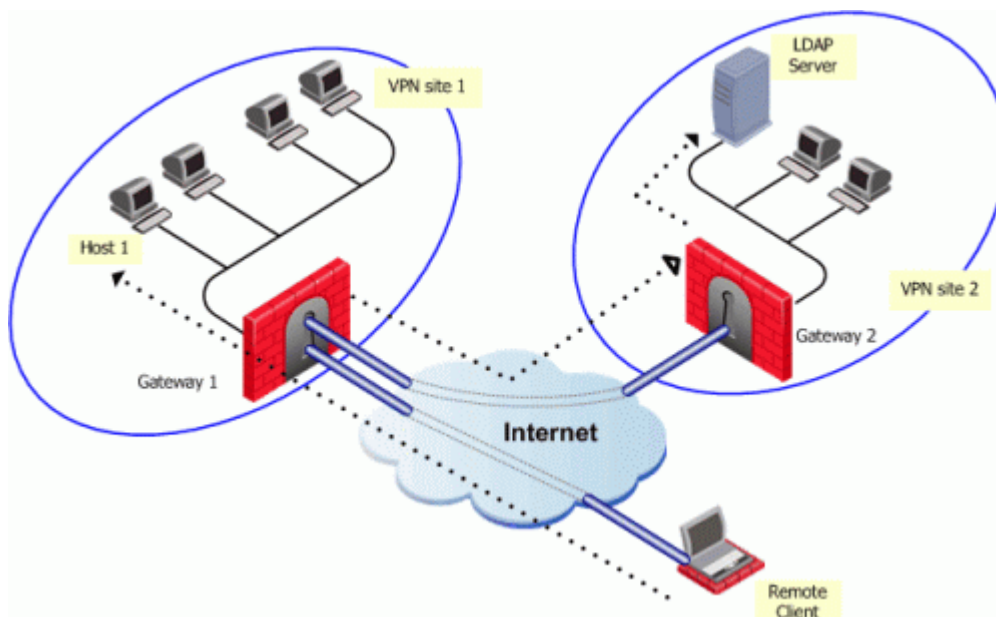
- Automatic software distribution.
- Advanced packaging and distribution options (see: Packaging SecureClient (on page 180)).
- Diagnostic tools

Establishing a Connection Between a Remote User and a Security Gateway

To allow the user to access a network resource protected by a Security Gateway, a VPN tunnel establishment process is initiated. An IKE (Internet Key Exchange) negotiation takes place between the peers.

During IKE negotiation, the peers' identities are authenticated. The Security Gateway verifies the user's identity and the client verifies that of the Security Gateway. The authentication can be performed using several methods, including digital certificates issued by the Internal Certificate Authority (ICA). It is also possible to authenticate using third-party PKI solutions, pre-shared secrets or third party authentication methods (for example, SecurID, RADIUS etc.).

After the IKE negotiation ends successfully, a secure connection (a VPN tunnel) is established between the client and the Security Gateway. All connections between the client and the Security Gateway's VPN domain (the LAN behind the Security Gateway) are encrypted inside this VPN tunnel, using the IPSec standard. Except for when the user is asked to authenticate in some manner, the VPN establishment process is transparent.



In the figure, the remote user initiates a connection to Security Gateway 1. User management is not performed via the VPN database, but an LDAP server belonging to VPN Site 2. Authentication takes place during the IKE negotiation. Security Gateway 1 verifies that the user exists by querying the LDAP server behind Security Gateway 2. Once the user's existence is verified, the Security Gateway then authenticates

the user, for example by validating the user's certificate. Once IKE is successfully completed, a tunnel is created; the remote client connects to Host 1.

If the client is behind the Security Gateway (for example, if the user is accessing the corporate LAN from a company office), connections from the client to destinations that are also behind the LAN Security Gateway are not encrypted.

Remote Access Community

A Check Point Remote Access community enables you to quickly configure a VPN between a group of remote users and one or more Security Gateways. A Remote Access community is a virtual entity that defines secure communications between Security Gateways and remote users. All communications between the remote users and the Security Gateways' VPN domains are secured (authenticated and encrypted) according to the parameters defined for Remote Access communications in SmartDashboard Global Properties.

Identifying Elements of the Network to the Remote Client

Clients need to know the elements of the organization's internal network before it can handle encrypted connections to and from network resources. These elements, known as a *topology*, are downloaded from any Security Gateway managed by the Security Management server.

A site's topology information includes IP addresses on the network and host addresses in the VPN domains of other Security Gateways controlled by the same Security Management server. If a destination IP is inside the site's topology, the connection is passed in a VPN tunnel.

When the user creates a site, the client automatically contacts the site and downloads topology information and the various configuration properties defined by the administrator for the client. This connection is secured and authenticated using IKE over SSL. The site's topology has a validity timeout after which the client would download an updated topology. The network administrator can also configure an *automatic* topology update for remote clients. This requires no intervention by the user.

Connection Mode

The remote access clients connect with Security Gateways using Connect mode.

During connect mode, the remote user deliberately initiates a VPN link to a specific Security Gateway. Subsequent connections to any host behind other Security Gateways will transparently initiate additional VPN links as required.

Connect mode offers:

- **Office mode**, to resolve routing issues between the client and the Security Gateway. See, Office Mode (on page 166).
- **Visitor mode**, for when the client needs to tunnel all client to Security Gateway traffic through a regular TCP connection on port 443.
- **Routing all traffic through Security Gateway (Hub mode)**, to achieve higher levels of security and connectivity.
- **Auto connect**, when an application tries to open a connection to a host behind a Security Gateway, the user is prompted to initiate a VPN link to that Security Gateway. For example, when the e-mail client tries to access the IMAP server behind Security Gateway X, SecureClient prompts the user to initiate a tunnel to that Security Gateway.
- **User profiles (Location Profiles)**. See: User Profiles (on page 151).

User Profiles

Mobile users are faced with a variety of connectivity issues. During the morning they find themselves connected to the LAN of a partner company; during the evening, behind some kind of NATing device employed by the hotel where they are staying.

Different user profiles are used to overcome changing connectivity conditions. Users create their own profiles, or the network administrator creates a number of profiles for them. If the administrator creates a profile, the profile is downloaded to the client when the user updates the site topology. The user selects

which profile to work with from a list. For example, a profile that enables UDP encapsulation in order to cope with some NATing device, or a profile that enables *Visitor mode* when the remote client must tunnel the VPN connection over port 443. The policy server used to download the Desktop Security Policy is also contained in the profile.

Access Control for Remote Access Community

Typically the administrator needs to define a set of rules that determines access control to and from the network. This is also true for remote access clients belonging to a remote access community. Policy rules must be created in order to control the way remote clients access the internal network via the Security Gateway. (Membership of a community does not give automatic access to the network.)

The Security Gateway's Security Policy Rule Base defines access control; in other words, whether a connection is allowed. Whether a connection is encrypted is determined by the community. If both the source and the destination belong to the community, the connection is encrypted; otherwise, it is not encrypted. For example, consider a rule that allows FTP connections. If a connection matching the rule is between community members, the connection is encrypted. If the connection is not between community members, the connection is not encrypted.

The Security Gateway's Security Policy controls access to resources behind the Security Gateway, protects the Security Gateway and the networks behind it. Since the remote client is not behind the Security Gateway, it is not protected by the Security Gateway's Security Policy. Remote access using SecureClient can be protected by a Desktop Security Policy. See Desktop Security (on page [185](#)).

Client-Security Gateway Authentication Schemes

Authentication is a key factor in establishing a secure communication channel among Security Gateways and remote clients. Various authentication methods are available, for example:

- Digital certificates
- Pre-shared secrets
- Other authentication methods (made available via Hybrid mode)

Digital Certificates

Digital Certificates are the most recommended and manageable method for authentication. Both parties present certificates as a means of proving their identity. Both parties verify that the peer's certificate is valid (i.e. that it was signed by a known and trusted CA, and that the certificate has not expired or been revoked).

Digital certificates are issued either by Check Point's Internal Certificate Authority or third-party PKI solutions. Check Point's ICA is tightly integrated with VPN and is the easiest way to configure a Remote Access VPN. The ICA can issue certificates both to Security Gateways (automatically) and to remote users (generated or initiated).

Using the ICA, generate a certificate and transfer it to the user "out-of-band." Alternatively, initiate the certificate generation process on Security Management server. The process is completed independently by the user. The administrator can also initiate a certificate generation on the ICA management tool (the only option available if users are defined on an LDAP server).

It is also possible to use third-party Certificate Authorities to create certificates for authentication between Security Gateways and remote users. The supported certificate formats are PKCS#12, CAPI, and *Entrust*.

Users can also be provided with a hardware token for storing certificates. This option offers the advantage of higher level of security, since the private key resides only on the hardware token.

As part of the certificate validation process during the IKE negotiation, both the client and the Security Gateway check the peer's certificate against the *Certificate Revocation List* (CRL) published by the CA which issued the certificate. If the client is unable to retrieve a CRL, the Security Gateway retrieves the CRL on the client's behalf and transfers the CRL to the client during the IKE negotiation (the CRL is digitally signed by the CA for security).

Pre-Shared Secret

This authentication method has the advantage of simplicity, but it is less secure than certificates. Both parties agree upon a password before establishing the VPN. The password is exchanged "out-of-band", and

reused multiple times. During the authentication process, both the client and Security Gateway verify that the other party knows the agreed-upon password.



Note - Passwords configured in the pre-shared secret tab are used in hybrid mode IKE and not in pre-shared secret mode. Pre-shared secret IKE mode is used for working with 4.1 Clients.

Other Authentication Methods Available via Hybrid Mode

Different organizations employing various means of user authentication may wish to utilize these means for remote access. Hybrid mode is an IKE mode that supports an asymmetrical way of authentication to address this requirement. Using Hybrid mode, the user employs one of the methods listed below to authenticate to the Security Gateway. In return, the Security Gateway authenticates itself to the client using strong, certificate-based authentication. Authentication methods which can be used in Hybrid mode are all those supported for normal user authentication in VPN, namely:

- **One Time Password** — The user is challenged to enter the number displayed on the Security Dynamics SecurID card. There are no scheme-specific parameters for the SecurID authentication scheme. The VPN module acts as an ACE/Agent 5.0. For agent configuration.
SoftID (a software version of RSA's SecurID) and various other One Time Password cards and USB tokens are also supported.
- **Security Gateway - Password** — The user is challenged to enter his or her password held on the Security Gateway.
- **OS Password** — The user is challenged to enter his or her Operating System password.
- **RADIUS** — The user is challenged for the correct response, as defined by the RADIUS server.
- **TACACS** — The user is challenged for the correct response, as defined by the TACACS or TACACS+ server.
- **SAA**. SAA is an OPSEC API extension to Remote Access Clients that enables third party authentication methods, such as biometrics, to be used with Endpoint Security VPN, Check Point Mobile for Windows, and SecuRemote.

Configuring Authentication

On the Security Gateway, you can configure authentication in one of two places:

- In the **Gateway Properties** window of a gateway in **Authentication**. In the **Authentication** page, you can allow access to users who authenticate with a **Check Point Password**, **SecurID**, **OS Password**, **RADIUS** server, or **TACACS** server. Authentication using Client Certificates from the Internal Certificate Authority is enabled by default in addition to the selected method.
- Some blades have their own authentication settings. Configure this in the **Gateway Properties** window of a gateway under **<name of the blade> > Authentication**. For example, configure the authentication method for IPsec VPN clients in **Gateway Properties > IPsec VPN > Authentication**. If you select an authentication method for the blade, that is the method that all users must use to authenticate to that blade. You can configure other authentication methods that users must use for different blades on different pages.

If you do not make a selection on the **Authentication** page for a specific blade, the Security Gateway takes authentication settings for the blade from the main gateway Authentication page.



Note - In previous releases there was no option to configure an authentication setting for a specific blade. But from R75 and higher, if you configure an authentication method for a specific blade, the settings on this page do not apply at all to that blade.

How the Gateway Searches for Users

If you configure authentication for a blade from the main Security Gateway **Legacy Authentication** page, the Security Gateway searches for users in a standard way when they try to authenticate. The gateway searches:

1. The internal users database.
2. If the specified user is not defined in this database, the gateway queries the User Directory (LDAP) servers defined in the Account Unit one at a time, and according to their priority.

3. If the information still cannot be found, the gateway uses the external users template to see if there is a match against the generic profile. This generic profile has the default attributes applied to the specified user.

If you configure an authentication method for a specific blade, the gateway searches for users according to the user groups that are used for authorization in that blade.

For example, in Mobile Access, the gateway looks at the Mobile Access policy to see which user groups are part of the policy. When the gateway tries to authenticate a user, it starts to search for users in the databases related to those user groups.

In IPsec VPN, the gateway looks at the Remote Access VPN Community to see which user groups are included. It starts to search for users in the databases related to those user groups.

A search based on the authentication scheme is faster, with better results. You can have users with the same user name in unrelated groups. The gateway will know which user is relevant for the blade based on the user groups.

Advanced Features

Remote Access VPN supports other advanced features such as:

- Resolving connectivity and routing issues. See: Office Mode (on page [166](#)), and Resolving Connectivity Issues (on page [271](#)).
- IP-per-user/group.
- L2TP clients.

Alternatives to SecuRemote/SecureClient

To avoid the overhead of installing and maintaining client software, Check Point also provides the SSL Network Extender, a simple-to-implement thin client installed on the user's machine via a web browser. The browser connects to an SSL enabled web server and downloads the thin client as an ActiveX component. Installation is automatic.

Need for Remote Access VPN

Whenever users access the organization from remote locations, it is essential that the usual requirements of secure connectivity be met but also the special demands of remote clients, for example:

- The IP of a remote access client might be unknown.
- The remote access client might be connected to a corporate LAN during the working day and connected to a hotel LAN during the evening, perhaps hidden behind some kind of NATing device.
- The remote client might need to connect to the corporate LAN via a wireless access point.
- Typically, when a remote client user is out of the office, they are not protected by the current security policy; the remote access client is both exposed to Internet threats, and can provide a way into the corporate network if an attack goes through the client.

To resolve these issues, a security framework is needed that ensures remote access to the network is properly secured.

Chapter 17

VPN for Remote Access Considerations

In This Chapter

| | |
|--|-----|
| Policy Definition for Remote Access | 155 |
| User Certificate Creation Methods when Using the ICA | 155 |
| Multiple Certificates per User | 155 |
| Internal User Database vs. External User Database | 155 |
| NT Group/RADIUS Class Authentication Feature | 156 |

When designing Remote Access VPN, consider the following issues:

Policy Definition for Remote Access

There must be a rule in the Security Policy Rule Base that grants remote users access to the LAN. Consider which services are allowed. Restrict those services that need to be restricted with an explicit rule in the Security Policy Rule Base.

User Certificate Creation Methods when Using the ICA

Check Point's Internal Certificate Authority (ICA) offers two ways to create and transfer certificates to remote users:

1. The administrator **generates** a certificate in Security Management server for the remote user, saves it to removable media and transfers it to the client "out-of-band."
2. The administrator **initiates** the certificate process on the Security Management server (or ICA management tool), and is given a registration key. The administrator transfers the registration key to the user "out-of-band." The client establishes an SSL connection to the ICA (using the CMC protocol) and completes the certificate generation process using the registration key. In this way:
 - Private keys are generated on the client.
 - The created certificate can be stored as a file on the machine's hard-drive, on a CAPI storage device, or on a hardware token.

This method is especially suitable for geographically spaced-remote users.

Multiple Certificates per User

Check Point VPN lets you define many certificates for each user. This lets users connect from different devices without the necessity to copy or move certificates from one device to another. Users can also connect from different devices at the same time.

Internal User Database vs. External User Database

Remote Access functionality includes a flexible user management scheme. Users are managed in a number of ways:

- **INTERNAL** - A Security Gateway can store a static password in its local user database for each user configured in Security Management server. No additional software is needed.
- **LDAP** - LDAP is an open industry standard that is used by multiple vendors. Check Point products integrate LDAP with Check Point User Directory. Manage the users externally on the LDAP server, and changes are reflected on the SmartDashboard. Security Gateways query the User Directory data for authentication.

- **RADIUS** - Remote Authentication Dial-In User Service (RADIUS) is an external authentication scheme that provides security and scalability by separating the authentication function from the access server. When employing RADIUS as an authentication scheme, the Security Gateway forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, authenticates the users. The RADIUS protocol uses UDP for communications with the Security Gateway. RADIUS Servers and RADIUS Server Group objects are defined in SmartDashboard.
- **SecurID Token Management ACE/Server** - Developed by RSA Security, SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA ACE/Server, and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time-use access code that changes every minute or so. When a user attempts to authenticate to a protected resource, that one-time-use code must be validated by the ACE/Server.
When employing SecurID as an authentication scheme, the Security Gateway forwards authentication requests by remote users to the ACE/Server. ACE manages the database of RSA users and their assigned hard or soft tokens. The VPN module acts as an ACE/Agent 5.0, which means that it directs all access requests to the RSA ACE/Server for authentication. For agent configuration see ACE/Server documentation.

The differences between user management on the internal database, and User Directory:

- User Directory is done externally and not locally.
- If you change User Directory templates the change is applied to users dynamically, immediately.

NT Group/RADIUS Class Authentication Feature

Authentication can take place according to NT groups or RADIUS classes. In this way, remote access users are authenticated according to the remote access community group they belong to.



Note - Only NT groups are supported, not Active Directory.

Chapter 18

Configuring Remote Access VPN

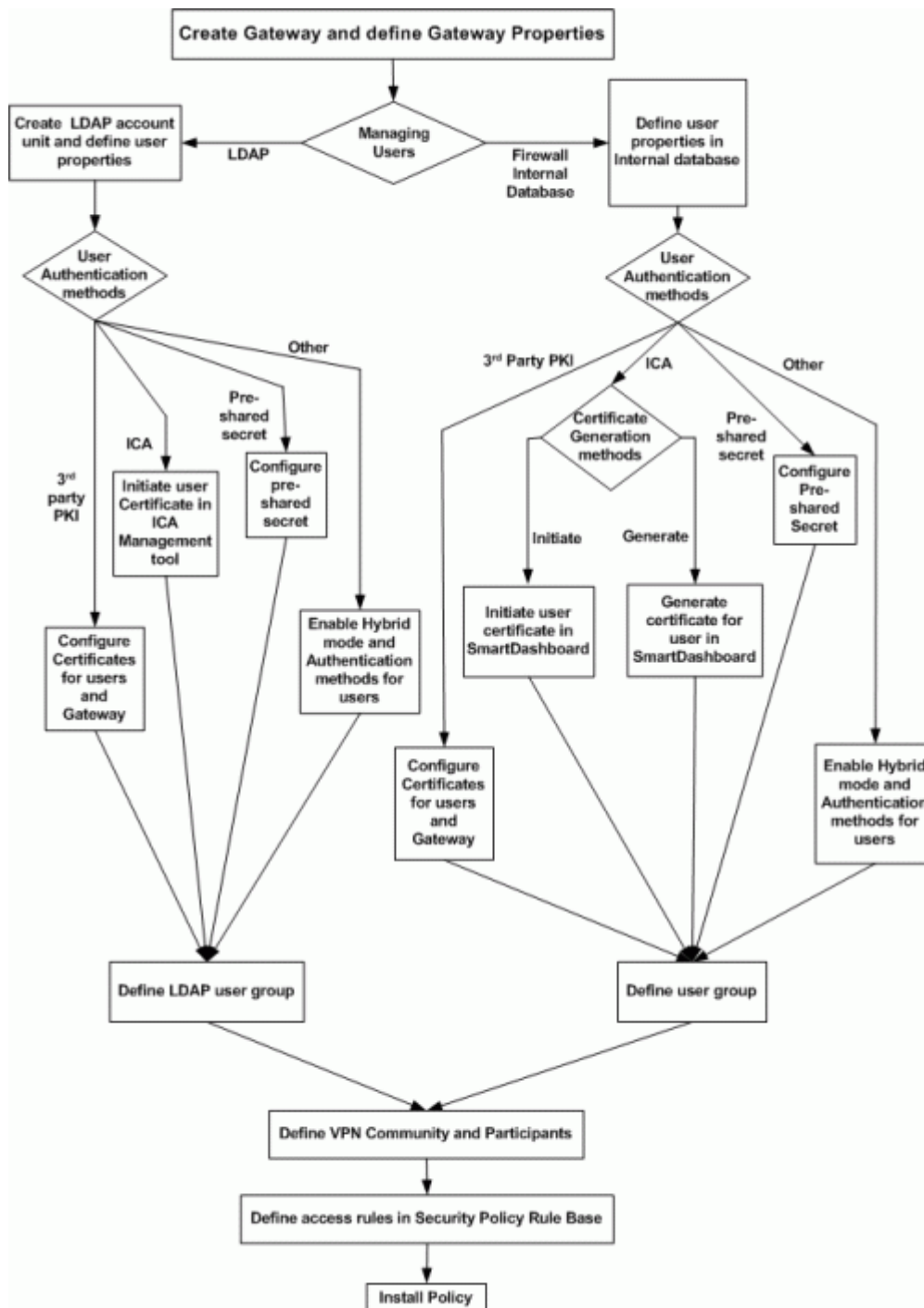
In This Chapter

| | |
|---|-----|
| Remote Access VPN Workflow | 158 |
| Creating Remote Access VPN Certificates for Users | 158 |
| Creating and Configuring the Security Gateway | 160 |
| Defining User and Authentication Methods in LDAP | 160 |
| Enrolling User Certificates - ICA Management Tool | 160 |
| Configuring Certificates Using Third Party PKI | 160 |
| Enabling Hybrid Mode and Methods of Authentication | 161 |
| Configuring Authentication for NT groups and RADIUS Classes | 161 |
| Using a Pre-Shared Secret | 162 |
| Defining an LDAP User Group | 162 |
| Defining a User Group | 162 |
| Defining a VPN Community and its Participants | 162 |
| Defining Access Control Rules | 162 |
| Installing the Policy | 162 |
| User Certificate Management | 163 |
| Modifying Encryption Properties for Remote Access VPN | 163 |
| Working with RSA Hard and Soft Tokens | 164 |

This section includes procedures and explanations for configuring Remote Access VPN.

Remote Access VPN Workflow

This section shows the Remote Access VPN Workflow.



Start at the top, with *Create Security Gateway and define Security Gateway properties*, and trace a route down to *Install policy*. Sections following the chart detail step-by-step procedures for each phase.

Creating Remote Access VPN Certificates for Users

This section contains procedures for creating Remote VPN user certificates and sending them to end users. There are two basic procedures for supplying remote access VPN certificates to users.

- **Sending a P12 File:**
 - The administrator creates a p12 certificate file and sends it to users.
 - The user saves the p12 file on the device and specifies the certificate using a remote VPN Client.

- Users authenticate by entering a certificate password when starting a remote access VPN connection.
- **Using a Registration key:**
 - The administrator creates a registration key and sends it to the user.
 - The user enrolls the certificate by entering the registration key in a Remote Access VPN client. The user can optionally save the p12 file to the device. The user must do this in an administrator-defined period of time.
 - End users authenticate using this certificate. A password can also be required according to the security policy settings. If the user saves the p12 file to the device, a password is always necessary.

Enabling a User Certificate

To enable a user certificate:

1. In SmartDashboard, click the **Firewall** tab.
2. Go to the **Users and Administrators** tab.
3. Create a new user or double-click an existing user.
4. In the **User Properties** window, click the **Encryption** tab.
5. In the **Encryption** pane, click **Edit**.
6. In the **IKE Phase 2 Properties** window, click the **Authentication** tab and select **Public key**.
7. Click **OK** to close this window.

Creating a P12 Certificate File

After creating a user certificate, you must then make this certificate available to remote access users. Use this procedure to create a p12 certificate.


To create a p12 certificate file for remote access VPN users:

1. Create the user certificate ("[Enabling a User Certificate](#)" on page 159).
2. In the **User Properties** window, click **Certificates**.
3. In the **Certificates** pane, click **New**.
4. Select **Certificate file (.p12)**.
5. In the **Certificate File (.P12)** window, enter and confirm the certificate password.
6. Optionally, enter descriptive text in the **Comment** field.
7. Click **OK** and enter a path to save the p12 file.
The new certificate shows in the **Certificate**. The status is set to **Valid**.
8. Send the .p12 file to the end user by secure email or other secure means.

Creating Certificate Registration Key

After creating a user certificate, you must then make this certificate available to remote access users. Use this procedure to create a certificate registration key that lets the user enroll the certificate for use with a device.

To create a certificate registration key:

1. Create the user certificate ("[Enabling a User Certificate](#)" on page 159).
2. In the **User Properties** window, click **Certificates**.
3. In the **Certificates** pane, click **New**.
4. Select **Registration key for certificate enrollment**.
5. In the **Registration Key for Certificate Enrollment** window, select the number of days before the certificate expires.
Click the email icon  to send the registration key to the user.
6. Optionally, enter descriptive text in the **Comment** field.

Instructions for End Users

Remote Access VPN users can use many different clients to connect to network resources. It is the administrator's responsibility to give appropriate instructions to end users to make sure that they successfully enroll the certificate.

The Creating Certificates ("[Creating Remote Access VPN Certificates for Users](#)" on page 158) section gives some general procedural guidelines that apply to many VPN clients. For detailed instructions, refer to the VPN client documentation.

Creating and Configuring the Security Gateway

1. In SmartDashboard, create a Security Gateway network object.
2. On the **General Properties** page, select **VPN**.
3. Initialize a secure communication channel between the VPN module and the Security Management server by clicking **Communication**
4. On the **Topology** page, define the interfaces and the VPN domain.

The ICA automatically creates a certificate for the Security Gateway.

Defining User and Authentication Methods in LDAP

1. Obtain and install a license that enables the VPN module to retrieve information from an LDAP server.
2. Create an LDAP account unit.
3. Define users as LDAP users. A new network object for LDAP users is created on the Users tree. (The LDAP users also appear in the objects list window to the right.)

For more information see: LDAP and User Management in the *R75.40 Security Management Server Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk67581>).

Enrolling User Certificates - ICA Management Tool

To use the ICA Management to enroll a user certificate:

1. In SmartDashboard, click the **Firewall** tab.
2. Go to the **Users and Administrators** tab.
3. Create a new user or double-click an existing user.
4. Double-click a user to open the property window.
5. On the **Encryption** tab, click **Edit**.
6. In the **IKE phase 2 properties** window **Authentication** tab, select **Public Key**.
7. Enroll the user certificate using the **ICA management tool**. For more information, see the *R75.40 Security Management Server Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk67581>).

Configuring Certificates Using Third Party PKI

Using third party PKI involves creating:

- A certificate for the user and
- A certificate for the Security Gateway

You can use a third-party OPSEC PKI certificate authority that supports the PKCS#12, CAPI or Entrust standards to issue certificates for Security Gateways and users. The Security Gateway must trust the CA and have a certificate issued by the CA.

For users managed on an LDAP server, the full distinguished name (DN) which appears on the certificate is the same as the user's name. But if the user is managed on the internal database, the user name and DN on the certificate will not match. For this reason, the user name in the internal database must be either the full DN which appears on the certificate or just the name which appears in the CN portion of the certificate. For example, if the DN which appears on the certificate is:

CN=John, OU=Finance, O=Widget Enterprises, C=US

The name of the user on the internal database must be either:

- **John**, or:
- **CN=John, OU=Finance, O=Widget Enterprises, C=US**



Note - The DN on the certificate must include the user's LDAP branch. Some PKI solutions do not include (by default) the whole branch information in the subject DN, for example the DN only includes the common name. This can be rectified in the CA configuration.

To use a third-party PKI solution:

1. On the **User properties** window, **Encryption** tab, click **Edit...** The **IKE phase 2 properties** window opens. On the **Authentication** tab, select **Public key**.
2. Define the third party Certificate Authority as an object in SmartDashboard. See Enrolling with a Certificate Authority (on page 44).
3. Generate a certificate for your Security Gateway from the third party CA. For more information, see: Enrolling with a Certificate Authority (on page 44).
4. Generate a certificate for the remote user from the third party CA. (Refer to relevant third party documentation for details.) Transfer the certificate to the user.
5. In **Global Properties, Authentication** window, add or disable suffix matching.
For users with certificates, it is possible to specify that only certificates with a specified suffix in their DN are accepted. This feature is enabled by default, and is required only if:
 - Users are defined in the internal database, *and*
 - The user names are not the full DN.

All certificates DN's are checked against this suffix.



Note - If an hierarchy of Certificate Authorities is used, the chain certificate of the user must reach the same root CA that the Security Gateway trusts

Enabling Hybrid Mode and Methods of Authentication

Hybrid mode allows the Security Gateway and remote access client to use different methods of authentication. To enable Hybrid Mode:

From **Policy > Global Properties > Remote Access > VPN - Basic** select **Hybrid Mode**.

Defining User Authentication Methods in Hybrid Mode

1. On the **User Properties** window, **Authentication** tab, select an appropriate authentication scheme.
2. Enter authentication credentials for the user.
3. Supply the user ("out-of-band") with these credentials.

Configuring Authentication for NT groups and RADIUS Classes

To enable this group authentication feature:

1. Set the **add_radius_groups** property in **objects.C** to "true",
2. Define a generic* profile, with RADIUS as the authentication method.
3. Create a rule in the Policy rule base whose "source" is this group of remote users that authenticate using NT Server or RADIUS.

Office Mode IP assignment file

This method also works for Office Mode. The group listed in the **ipassignment.conf** file points to the group that authenticates using NT group authentication or RADIUS classes. See: Office Mode via ipassignment.conf File (see "[Office Mode through the ipassignment.conf File](#)" on page 176).

Using a Pre-Shared Secret

When using pre-shared secrets, the remote user and Security Gateway authenticate each other by verifying that the other party knows the shared secret: the user's password. To enable the use of pre-shared secrets:

1. In **Policy > Global Properties > Remote Access > VPN — Basic**, select **Pre-Shared Secret (For SecuRemote/SecureClient users)**.
2. Deselect **Hybrid Mode**.
3. For each user, go to the **Encryption** tab of the **User Properties** window, select **IKE** and click **Edit...** to display the **IKE Phase 2 Properties** window.
4. In the **Authentication** tab, enable **Password (Pre-Shared Secret)** and enter the pre-shared secret into the **Password (Pre-shared secret)** and **Confirm Password** fields.
5. Inform the user of the password "out-of-band".

Defining an LDAP User Group

See: *LDAP and User Management* in the *R75.40 Security Management Server Administration Guide*. (<http://supportcontent.checkpoint.com/solutions?id=sk67581>)

Defining a User Group

In SmartDashboard, create a group for remote access users. Add the appropriate users to this group.

Defining a VPN Community and its Participants

1. On the VPN Communities tree, double-click **Remote_Access_Community**. The **Remote Access Community Properties** window opens.
2. On the **Participating Security Gateways** page, **Add...** Security Gateways participating in the Remote Access Community.
3. On the **Participating User Groups** page, **Add...** the group that contains the remote access users.

Defining Access Control Rules

Access control is a layer of security not connected with VPN. The existence of a remote access community does not mean that members of that community have free automatic access to the network. Appropriate rules need to be created in the Security Policy Rule Base blocking or allowing specific services.

1. Create a rule in the Security Policy Rule Base that deals with remote access connections.
2. Double-click the entry in the VPN column. The **VPN Match Conditions** window opens.
3. Select **Only connections encrypted in specific VPN Communities**.
4. Click **Add...** to include a specific community in this Security Policy Rule.
5. Define services and actions. For example, to allow remote access users to access the organization's SMTP server, called SMTP_SRV, create the following rule:

| Source | Destination | VPN | Service | Action | Track |
|--------|-------------|-------------------------|---------|--------|-------|
| Any | SMTP_SRV | Remote_Access_Community | SMTP | Accept | Log |

Installing the Policy

Install the policy and instruct the users to create or update the site topology.

User Certificate Management

Managing user certificates involves:

- Tracing the status of the user's certificate
- Automatically renewing a certificate
- Revoking certificates

Tracing the Status of User's Certificate

The status of a user's certificate can be traced at any time in the **Certificates** tab of the user's Properties window. The status is shown in the **Certificate state** field. If the certificate has not been generated by the user by the date specified in the **Pending until** field, the registration key is deleted.

If the user is defined in LDAP, then tracing is performed by the ICA management tool.

Automatically Renewing a Users' Certificate

ICA certificates for users can be automatically renewed a number of days before they expire. The client initiates a certificate renewal operation with the CA before the expiration date is reached. If successful, the client receives an updated certificates.

To configure automatic certificate renewal:

1. Select **Policy > Global Properties > Remote Access > Certificates**.
2. Select **Renew users internal CA certificates** and specify a time period. The time period is the number of days before the user's certificate is about to expire in which the client will attempt to renew the certificate.
3. Install the Security Policy.
4. Instruct the user to update the site's topology.

Revoking Certificates

The way in which certificates are revoked depends on whether they are managed internally or externally, via LDAP.

For internally managed Users

When a user is deleted, their certificate is automatically revoked. Certificates can be disabled or revoked at any time.

If you initiated a certificate generation that was not completed by the user, you can disable the pending certificate by clicking **Disable** in the **Certificates** tab of the **User Properties** window.

If the certificate is already active, you can revoke it by clicking **Revoke** in the **Certificates** tab of the **User Properties** window.

For Users Managed in LDAP

If users are managed in LDAP, certificates are revoked using the ICA management tool.

Modifying Encryption Properties for Remote Access VPN

The encryption properties of the users participating in a Remote Access community are set by default. If you must modify the encryption algorithm, the data integrity method and/or the Diffie-Hellman group, you can either do this globally for all users or configure the properties per user.

To modify the user encryption properties globally:

1. Select **Policy > Global Properties > Remote Access > VPN - (IKE Phase 1)**.
Configure the appropriate settings:

- **Support encryption algorithms** - Select the encryption algorithms that will be supported with remote hosts.
 - **Use encryption algorithms** - Choose the encryption algorithm that will have the highest priority of the selected algorithms. If given a choice of more than one encryption algorithm to use, the algorithm selected in this field will be used.
 - **Support Data Integrity** - Select the hash algorithms that will be supported with remote hosts to ensure data integrity.
 - **Use Data Integrity** - The hash algorithm chosen here will be given the highest priority if more than one choice is offered.
 - **Support Diffie-Hellman groups** - Select the Diffie-Hellman groups that will be supported with remote hosts.
 - **Use Diffie-Hellman group** - SecureClient users utilize the Diffie-Hellman group selected in this field.
- To enforce the global encryption properties for some users while being able to modify them for specific users go to **Policy > Global Properties > Remote Access > VPN - (IPSEC Phase 2)**:
2. Set the required properties in the window and disable **Enforce Encryption Algorithm and Data Integrity on all users**.
 3. In the **Encryption** tab of the **User Properties** window select **IKE** and click **Edit**.
The **IKE Phase 2 Properties** window is displayed.
 4. Select the **Encryption** tab.
 5. If you want the encryption and data integrity algorithms of the user to be taken from the **Global Properties** definitions, select **Defined in the Remote Access VPN** page of the **Global Properties** window. If you want to customize the algorithms for this user, select **Defined below** and select the appropriate encryption and data integrity algorithms.

Working with RSA Hard and Soft Tokens

If you use SecurID for authentication, you must manage the users on RSA's ACE management server. ACE manages the database of RSA users and their assigned hard or soft tokens. SecureClient contacts the site's Security Gateway. The Security Gateway contacts the ACE Server for user authentication information. This means:

- The remote users must be defined as RSA users on the ACE Server.
- On the Security Gateway, the SecurID users must be placed into a group with an external user profile account that specifies SecurID as the authentication method.

SecurID Authentication Devices

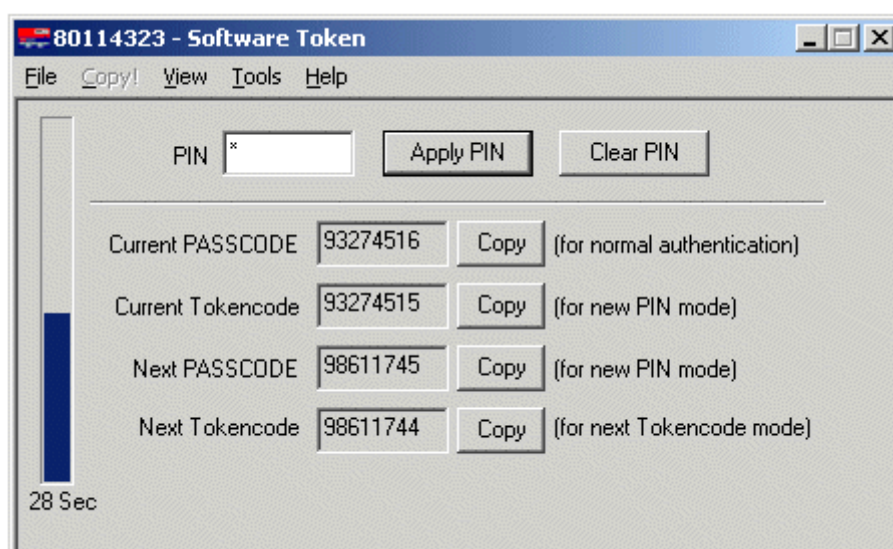
Several versions of SecurID devices are available. The older format is a small device that displays a numeric code, called a *tokencode*, and time bars. The token code changes every sixty seconds, and provides the basis for authentication. To authenticate, the user must add to the beginning of the tokencode a special password called a PIN number. The time bar indicates how much time is left before the next tokencode is generated. The remote user is requested to enter both the PIN number and tokencode into SecureClient's connection window.

The newer format resembles a credit card, and displays the tokencode, time bars and a numeric pad for typing in the PIN number. These type of device mixes the tokencode with the entered PIN number to create a *Passcode*. SecureClient requests only the passcode.

SoftID operates the same as the passcode device but consists only of software that sits on the desktop.



The Advanced view displays the tokencode and passcode with COPY buttons, allowing the user to cut and paste between softID and SecureClient:



SoftID and SecureClient

For remote users to successfully use RSA's softID:

1. The administrator creates the remote users on the Ace Server
2. "Out-of-band", the administrator distributes the SDTID token file (or several tokens) to the remote users.
3. The remote user imports the tokens.
4. The following **userc.c** property on SecureClient must be set in the OPTIONS section:
support_rsa_soft_tokens (true)

When users login, they must enter the Token Serial Number and PIN.

Chapter 19

Office Mode

In This Chapter

| | |
|---|-----|
| The Need for Remote Clients to be Part of the LAN | 166 |
| Office Mode | 166 |
| Enabling IP Address per User | 171 |
| Office Mode Considerations | 174 |
| Configuring Office Mode | 174 |

The Need for Remote Clients to be Part of the LAN

As remote access to internal networks of organizations becomes widespread, it is essential that remote users are able to access as many of the internal resources of the organization as possible. Typically, when remote access is implemented, the client connects using an IP address locally assigned by, for example, an ISP. The client may even receive a non-routable IP which is then hidden behind a NATing device. Because of this, several problems may arise:

- Some networking protocols or resources may require the client's IP address to be an internal one. Router ACLs (access lists), for example, might be configured to allow only specific or internal IP addresses to access network resources. This is difficult to adjust without knowing the a remote client's IP address in advance.
- When assigned with a non-routable IP address a conflict may occur, either with similar non-routable addresses used on the corporate LAN, or with other clients which may receive the same IP address while positioned behind some other hiding NAT device.
For example, if a client user receives an IP of 10.0.0.1 which is entered into the headers of the IPSec packet. The packet is NATed. The packet's new source IP is 192.168.17.5. The Security Gateway decapsulates the NATed IP and decrypts the packet. The IP address is reverted to its original source IP of 10.0.0.1. If there is an internal host with the same IP, the packet will probably be dropped (if anti-spoofing is turned on). If there is no duplicate IP, and the packet is forwarded to some internal server, the server will then attempt to reply to an non-existent address.
- Two remote users are assigned the same IP address by an ISP (for example, two users are accessing the organization from hotels which provide internal addresses and NAT them on the outbound). Both users try to access the internal network with the same IP address. The resources on the internal network of the organization may have difficulty distinguishing between the users.

Office Mode

Office Mode enables a Security Gateway to assign a remote client an IP address. The assignment takes place once the user connects and authenticates. The assignment lease is renewed as long as the user is connected. The address may be taken either from a general IP address pool, or from an IP address pool specified per user group. The address can be specified per user, or via a DHCP server, enabling the use of a name resolution service. With DNS name resolution, it is easier to access the client from within the corporate network.

It is possible to allow all your users to use Office Mode, or to enable the feature for a specific group of users. This can be used, for example, to allow privileged access to a certain group of users (e.g., administrators accessing the LAN from remote stations). It is also useful in early integration stages of Office Mode, allowing you time to "pilot" this feature on a specific group of users, while the rest of the users continue to work in the traditional way.

Office Mode is supported with the following:

- SecureClient
- Endpoint Connect

- SSL Network Extender
- Crypto
- L2TP

How Office Mode Works

When you connect to the organization, an IKE negotiation is initiated automatically to the Security Gateway. When using Office Mode, a special IKE mode called *config mode* is inserted between phase 1 and phase 2 of IKE. During config mode, the client requests an IP from the Security Gateway. Several other parameters are also configurable this way, such as a DNS server IP address, and a WINS server IP address.

After the Security Gateway allocates the IP address, the client assigns the IP to a Virtual Adapter on the Operating system. The routing of packets to the corporate LAN is modified to go through this adapter. Packets routed in this way bear the IP address assigned by the Security Gateway as their source IP address. Before exiting through the real adapter, the packets will be IPSec encapsulated using the external IP address (assigned to the real adapter) as the source address. In this way, non-routable IP addresses can be used with Office Mode; the Office Mode non-routable address is concealed within the IPSec packet.

For Office Mode to work, the IP address assigned by the Security Gateway needs to be routable to that Security Gateway from within the corporate LAN. This will allow packets on the LAN being sent to the client to be routed back through the Security Gateway. (See also: Office Mode and Static Routes in a Non-flat Network (on page [169](#))).



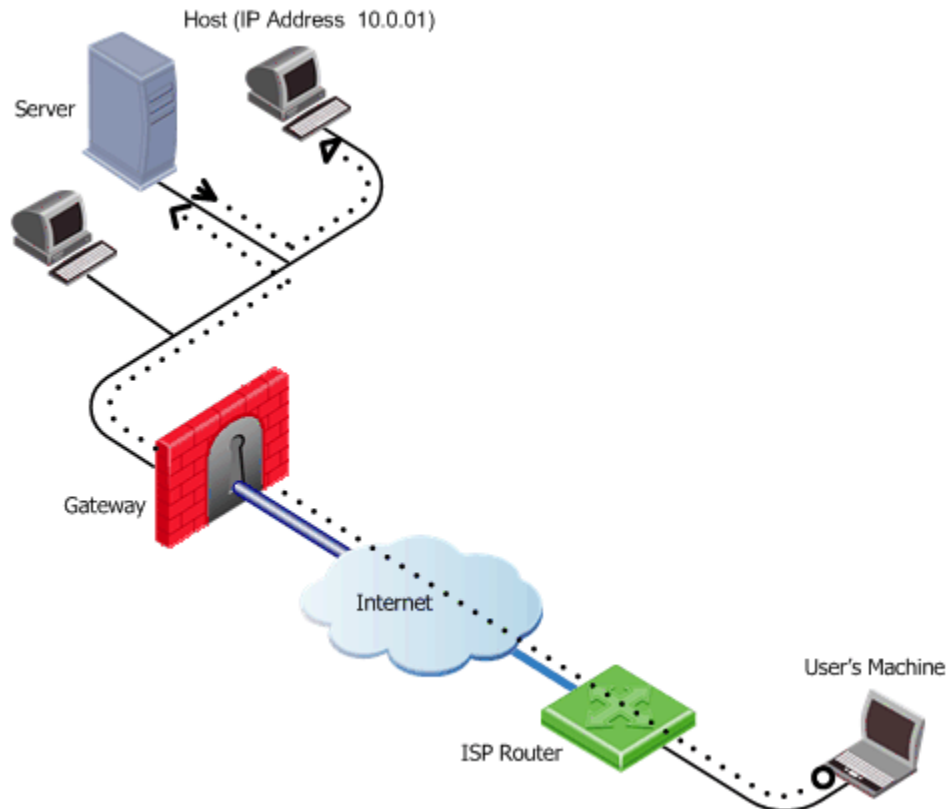
Note - A remote user with SecuRemote only is not supported in Office Mode.

A Closer Look

The following steps illustrate the process taking place when a remote user connected through Office Mode wishes to exchange some information with resources inside the organization:

- The user is trying to connect to some resource on the LAN, thus a packet destined for the internal network is to be sent. This packet is routed through the virtual interface that Office Mode had set up, and bears the source IP address allocated for the remote user.
- The packet is encrypted and builds a new encapsulating IP header for it. The source IP of the encapsulating packet is the remote client's original IP address, and its destination is the IP address of the Security Gateway. The encapsulated packet is then sent to the organization through the Internet.
- The Security Gateway of the organization receives the packet, decapsulates and decrypts it, revealing the original packet, which bears the source IP allocated for the remote user. The Security Gateway then forwards the decapsulated packet to its destination.
- The internal resource gets a packet seemingly coming from an internal address. It processes the packet and sends response packets back to the remote user. These packets are routed back to the (internal) IP address assigned to the remote user.

- The Security Gateway gets the packet, encrypts and encapsulates it with the remote users' original (routable) IP address and returns the packet back to the remote user:



- The remote host uses the Office mode address in the encapsulated packet and 10.0.0.1 in the encapsulating header.
- The packet is NATed to the new source address: 192.168.17.5
- The Security Gateway decapsulates the NATed IP address and decrypts the packet. The source IP address is the Office Mode address.
- The packet is forwarded to the internal server, which replies correctly.

Assigning IP Addresses

The internal IP addresses assigned by the Security Gateway to the remote user can be allocated using one of the following methods:

- IP Pool
- DHCP Server

IP Pool

The System Administrator designates a range of IP addresses to be utilized for remote client machines. Each client requesting to connect in Office Mode is provided with a unique IP address from the pool.

IP Assignment Based on Source IP Address

IP addresses from the IP pool may be reserved and assigned to remote users based on their source IP address. When a remote host connects to the Security Gateway, its IP address is compared to a predefined range of source IP addresses. If the IP address is found to be in that range, then it is assigned an Office Mode IP address from a range dedicated for that purpose.

The IP addresses from this reserved pool can be configured to offer a separate set of access permissions given to these remote users.

DHCP Server

A Dynamic Host Configuration Protocol (DHCP) server can be used to allocate IP addresses for Office Mode clients. When a remote user connects to the Security Gateway using Office Mode, the Security

Gateway requests the DHCP server to assign the user an IP address from a range of IP addresses designated for Office Mode users.

Security Gateway DHCP requests can contain various client attributes that allow DHCP clients to differentiate themselves. The attributes are pre configured on the client side operating system, and can be used by different DHCP servers in the process of distributing IP addresses. Security Gateways DHCP request can contain the following attributes:

- Host Name
- Fully Qualified Domain Name (FQDN)
- Vendor Class
- User Class

RADIUS Server

A RADIUS server can be used for authenticating remote users. When a remote user connects to a Security Gateway, the username and password are passed on to the RADIUS server, which checks that the information is correct, and authenticates the user. The RADIUS server can also be configured to allocate IP addresses.



Note - Authentication and IP assignment must be performed by the same RADIUS server.

Office Mode and Static Routes in a Non-flat Network

A flat network is one in which all stations can reach each other without going through a bridge or a router. One segment of a network is a "flat network". A static route is a route that is manually assigned by the system administrator (to a router) and needs to be manually updated to reflect changes in the network.

If the LAN is non-flat (stations reach each other via routers and bridges) then the OM address of the remote client must be statically assigned to the routers so that packets on the LAN, destined for the remote client, are correctly routed to the Security Gateway.

IP Address Lease duration

When a remote user's machine is assigned an Office mode IP address, that machine can use it for a certain amount of time. This time period is called the "IP address lease duration." The remote client automatically asks for a lease renewal after half of the IP lease duration period has elapsed. If the IP lease duration time is set to 60 minutes, a renewal request is sent after 30 minutes. If a renewal is given, the client will request a renewal again after 30 minutes. If the renewal fails, the client attempts again after half of the remaining time, for example, 15 minutes, then 7.5 minutes, and so on. If no renewal is given and the 60 minutes of the lease duration times out, the tunnel link terminates. To renew the connection the remote user must reconnect to the Security Gateway. Upon reconnection, an IKE renegotiation is initiated and a new tunnel created.

When the IP address is allocated from a predefined IP pool on the Security Gateway, the Security Gateway determines the IP lease duration period. The default is 15 minutes.

When using a DHCP server to assign IP addresses to users, the DHCP server's configuration determines the IP lease duration. When a user disconnects and reconnects to the Security Gateway within a short period of time, it is likely that the user will get the same IP address as before.

Using Name Resolution - WINS and DNS

To facilitate access of a remote user to resources on the internal network, the administrator can specify WINS and DNS servers for the remote user. This information is sent to the remote user during IKE config mode along with the IP address allocation information, and is used by the remote user's operating system for name-to-IP resolution when the user is trying to access the organization's internal resources.

Anti Spoofing

With Anti Spoofing, a network administrator configures which IP addresses are expected on each interface of the Security Gateway. Anti-spoofing ensures IP addresses are only received or transmitted in the context

of their respective Security Gateway interfaces. Office Mode poses a problem to the anti-spoofing feature, since a client machine can connect and authenticate through several interfaces, e.g. the external interface to the Internet, or the wireless LAN interface; thus an Office Mode IP address may be encountered on more than one interface. Office Mode enhances Anti Spoofing by making sure an encountered Office Mode IP address is indeed assigned to the user, authenticated on the source IP address on the IPSec encapsulating packet, i.e. the external IP.

Using Office Mode with Multiple External Interfaces

Typically, routing is performed before encryption in VPN. In some complex scenarios of Office Mode, where the Security Gateway may have several external interfaces, this might cause a problem. In these scenarios, packets destined at a remote user's virtual IP address will be marked as packets that are supposed to be routed through one external interface of the Security Gateway. Only after the initial routing decision is made do the packets undergo IPSEC encapsulation. After the encapsulation, the destination IP address of these packets is changed to the original IP address of the client. The routing path that should have been selected for the encapsulated packet might be through a different external interface than that of the original packet (since the destination IP address changed), in which case a routing error occurs. Office Mode has the ability to make sure that all Office Mode packets undergo routing *after* they are encapsulated.

Office Mode Per Site

After a remote user connects and receives an Office Mode IP address from a Security Gateway, every connection to that Security Gateways encryption domain will go out with the Office Mode IP as the internal source IP. The Office Mode IP is what hosts in the encryption domain will recognize as the remote user's IP address.

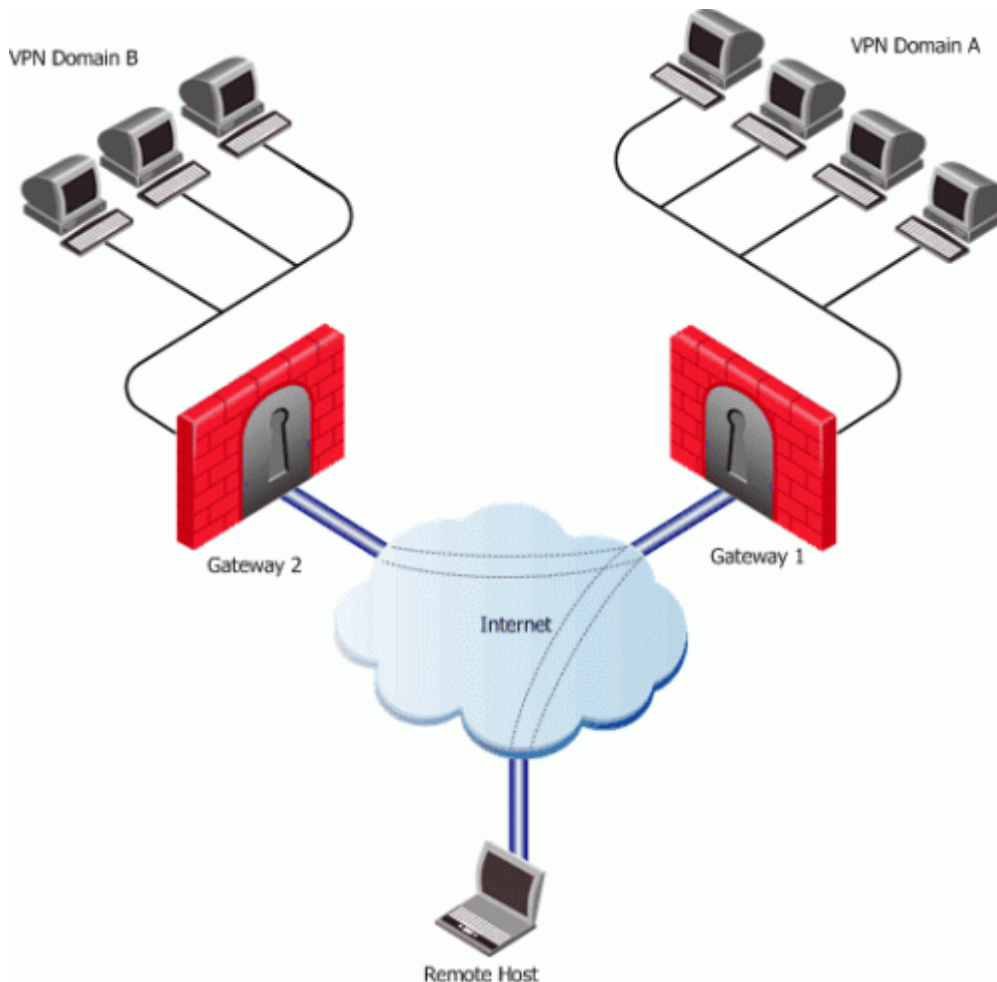
The Office Mode IP address assigned by a specific Security Gateway can be used in its own encryption domain and in neighboring encryption domains as well. The neighboring encryption domains should reside behind Security Gateways that are members of the same VPN community as the assigning Security Gateway. Since the remote hosts' connections are dependent on the Office Mode IP address it received, if the Security Gateway that issued the IP becomes unavailable, all the connections to the site will terminate.

In order for all Security Gateways on the site to recognize the remote users Office Mode IP addresses, the Office Mode IP range must be known by all of the Security Gateways and the IP ranges must be routable in all the networks. However, when the Office Mode per Site feature is in use, the IP-per-user feature cannot be implemented.



Note - When Office Mode per Site is activated, Office Mode Anti-Spoofing is not enforced.

In this scenario:



- The remote user makes a connection to Security Gateway 1.
- Security Gateway 1 assigns an Office Mode IP address to the remote user.
- While still connected to Security Gateway 1, the remote user can make a connection to hosts behind Security Gateway 2 using the Office Mode IP address issued by Security Gateway 1.

Enabling IP Address per User

Enabling IP Address per User

In some configurations, a router or other device restricts access to portions of the network to specified IP addresses. A remote user connecting in Office Mode must be able to ensure that he or she is allocated an IP address which will allow the connection to pass through the router.



Note - If this feature is implemented, it is imperative to enable anti-spoofing for Office Mode. See Anti Spoofing (on page 169) for more information.

There are two ways to implement this feature, depending on whether IP addresses are allocated by a DHCP server or IP Pool.

The Solution

There are two ways to implement this feature, depending on whether IP addresses are allocated by a DHCP server or IP Pool.

DHCP Server

If Office Mode addresses are allocated by a DHCP server, proceed as follows:

1. Open the Check Point object from the Objects Tree.
2. In the **Object Properties > IPSec VPN > Office Mode** page:
 - Enable Office Mode (either for all users or for the relevant group)
 - Select a DHCP server and under **MAC address for DHCP allocation**, select **calculated per user name**
3. Install the Policy on the Security Gateway.
4. On the Security Gateway, run this command to obtain the MAC address assigned to the user.

```
vpn macutil <username>
```
5. On the DHCP Server make a new reservation, specifying the IP address and MAC address, assigning the IP address for the exclusive use of the given user.

ipassignment.conf File

The **\$FWDIR/conf/ipassignment.conf** file on the Security Gateway, is used to implement the IP-per-user feature. It allows the administrator to assign specific addresses to specific users or specific ranges to specific groups when they connect using Office Mode or L2TP clients.

For an explanation of the file's syntax, see the comments (the lines beginning with the # character) in the sample file below.



Note - This file must be *manually* added to all Security Gateways.

Sample ipassignment.conf File

```
# This file is used to implement the IP-per-user feature.
It allows the
# administrator to assign specific addresses to specific
users or specific
# ranges to specific groups when they connect using Office
Mode or L2TP.
#
# The format of this file is simple: Each line specifies
the target
# Security Gateway, the IP address (or addresses) we wish
to assign and the user
# (or group) name as in the following examples:
#
# Security Gateway      Type    IP Address
User Name
# =====
# Paris-GW,             10.5.5.8,
Jean
# Brasilia,            addr    10.6.5.8,
Joao # comments are allowed
# Miami,               addr    10.7.5.8,
CN=John,OU=users,O=cpmgt.acme.com.gibeuu
# Miami                range   100.107.105.110-100.107.105.119/24
Finance
# Miami                net     10.7.5.32/28
Accounting
#
# Note that real records do not begin with a pound-sign
(#), and the commas
# are optional. Invalid lines are treated as comments.
Also, the
# user name may be followed by a pound-sign and a comment.
#
# The first item is the Security Gateway name. This could
be a name, an IP
# address or an asterisk (*) to signify all Security
Gateways. A gateway will
# only honor lines that refer to it.
#
# The second item is a descriptor. It can be 'addr',
'range' or 'net'.
# 'addr' specifies one IP for one user. This prefix is
optional.
# 'range' and 'net' specify a range of addresses. These
prefixes are
# required.
#
# The third item is the IP address or addresses. In the
case of a single
# address, it is specified in standard dotted decimal
format.
# ranges can be specified either by the first and last IP
address, or using
# a net specification. In either case you need to also
specify the subnet
# mask length ('/24' means 255.255.255.0). With a range,
this is the subnet
# mask. With a net it is both the subnet mask and it also
determines the
# addresses in the range.
#
# The last item is the user name. This can be a common name
if the
# user authenticates with some username/password method
```

```
(like hybrid
# or MD5-Challenge) or a DN if the user authenticates with
a
# certificate.
```

Office Mode Considerations

Before implementing Office mode, consider the following:

IP pool Versus DHCP

The question of whether IP addresses should be assigned by the Firewall (using IP pools) or by a DHCP server is a network administration and financial issue. Some network administrators may prefer to manage all of their dynamic IP addresses from the same location. For them, a central DHCP server might be preferable. Moreover, DHCP allows a cluster to assign all the addresses from a single pool, rather than have a different pool per cluster member as you have to with Firewall IP pools. On the other hand, purchasing a DHCP server can be viewed by some as an unnecessary financial burden, in which case the IP pool option might be preferred.

Routing Table Modifications

IP addresses, assigned by Office Mode need to be routed by the internal LAN routers to the Security Gateway (or Security Gateway cluster) that assigned the address. This is to make sure packets, destined to remote access Office Mode users, reach the Security Gateway in order to be encapsulated and returned to the client machine. This may require changes to the organization's routing tables.

Using the Multiple External Interfaces Feature

Enabling this feature instructs Office Mode to perform routing decisions *after* the packets are encapsulated using IPSEC, to prevent routing problems discussed in Using Office Mode with Multiple External Interfaces (on page 170). This feature adds new checks and changes to the routing of packets through the Security Gateway, and has an impact on performance. As a result, it is recommended to use this feature only when:

- The Security Gateway has multiple external interfaces, *and*
- Office Mode packets are routed to the wrong external interface.

Configuring Office Mode

Before configuring Office Mode the assumption is that standard VPN Remote Access has already been configured. For more details on how to configure VPN Remote Access, see Introduction to Remote Access VPN.

Before starting the Office Mode configuration, you must select an internal address space designated for remote users using Office Mode. This can be any IP address space, as long as the addresses in this space do not conflict with addresses used within the enterprise domain. It is possible to choose address spaces which are not routable on the Internet, such as 10.x.x.x.

The basic configuration of Office Mode is using IP pools. The configuration of Office Mode using DHCP for address allocation can be found in Office Mode ? DHCP Configuration (see "[Office Mode — DHCP Configuration](#)" on page 177).

Office Mode — IP Pool Configuration

To deploy the basic Office Mode (using IP pools):

1. Create a network object to represent the IP Pool, by selecting **Manage > Network Objects > New > Network**.
2. In the **Network Properties — General** tab, set the IP pool range of addresses as follows:
 - a) In **Network Address** specify the first address to be used (e.g. 10.130.56.0).

- b) In **Net Mask** enter the subnet mask according to the amount of addresses you wish to use (entering 255.255.255.0, for example, this will designate all 254 IP addresses from 10.130.56.1 till 10.130.56.254 for Office Mode addresses.)
 - c) Changes to the **Broadcast Address section** and the **Network Properties — NAT** tab are not necessary.
 - d) Close the network object properties window.
3. Open the Security Gateway object through which the remote users will connect to the internal network and select the **IPSec VPN > Office Mode** page. Enable **Office Mode** for either all users or for a certain group.
 - a) In the **Allocate IP from network** select the IP Pool network object you have previously created.
 - b) **IP lease duration** — specify the duration in which the IP is used by the remote host.
 - c) Under **Multiple Interfaces**, specify whether you want routing to be done after the encapsulation of Office Mode packets, allowing traffic to be routed correctly when your Security Gateway has multiple external interfaces.
 - d) Select **Anti-Spoofing** if you wish the firewall to check that Office Mode packets are not spoofed.

It is possible to specify which WINS and DNS servers Office Mode users should use. To specify WINS and/or DNS servers, continue to step 3. Otherwise skip to step 6.



Note - WINS and DNS servers should be set on the Security Management server machine only when IP pool is the selected method.

1. Create a DNS server object, by selecting **Manage > Network Objects > New > Node > Host** and specify the DNS machine's name, IP address and subnet mask. Repeat this step if you have additional DNS servers.
2. Create a WINS server object, by selecting **Manage > Network objects > New > Node > Host** and specify the WINS machine's name, IP address and subnet mask. Repeat this step if you have additional WINS servers.
3. In the **Check Point Security Gateway — IPsec VPN > Office Mode** page, in the **IP Pool** section click the "**optional parameters**" button.
 - a) In the **IP Pool Optional Parameters** window, select the appropriate objects for the primary and backup DNS and WINS servers.
 - b) In the **Domain name** field, specify the suffix of the domain where the internal names are defined. This instructs the Client as per what suffix to add when it addresses the DNS server (e.g. example.com).
4. Install the Policy.
5. Make sure that all the internal routers are configured to route all the traffic destined to the internal address space you had reserved to Office Mode users through the Security Gateway. For instance, in the example above it is required to add routes to the class C sub network of 10.130.56.0 through the Security Gateway's IP address.

In addition to the steps mentioned for the Security Gateway side configuration, a few configuration steps have to be performed on the client side in order to connect to the Security Gateway in Office Mode.

Configuring IP Assignment Based on Source IP Address

The settings for the IP Assignment Based on Source IP Address feature are configured by editing a plain text file called **user.def**. This file is located in the **\FWDIR\conf** directory of the Security Management server which manages the enforcement modules used for remote access.

A range of source IP addresses must be defined along with a corresponding range of Office Mode addresses. The **\FWDIR\conf\user.def** file can contain multiple definitions for multiple modules.

The first range defined per line is the source IP address range. The second range defined per line is the Office Mode IP address range.

```
all@module1 om_per_src_range= { <10.10.5.0, 10.10.5.129; 1.1.1.5, 1.1.1.87>,
                                <10.10.9.0, 10.10.9.255; 1.1.1.88, 1.1.1.95> };
all@module2 om_per_src_range= { <70.70.70.4, 70.70.70.90; 8.8.8.6, 8.8.8.66> };
```

In this scenario:

- (10.10.5.0, 10.10.5.129), (10.10.9.0, 10.10.9.255), and (70.70.70.4, 70.70.70.90) are the VPN remote clients source IP address ranges
- (1.1.1.5, 1.1.1.87), (1.1.1.88, 1.1.1.95), and (8.8.8.6, 8.8.8.66) are the Office Mode IP addresses that will be assigned to the remote users whose source IP falls in the range defined on the same line.
- For example: A user with a source IP address between 10.10.5.0 and 10.10.5.129, will receive an Office Mode address between 1.1.1.5 and 1.1.1.87.

IP Assignment Based on Source IP Address is enabled using a flag in the `\FWDIR\conf\objects_5_0.C` file. Add the following flag:

om_use_ip_per_src_range (followed by value)

One of the following values should be applied to the flag:

- **[Exclusively]** - If the remote hosts IP is not found in the source range, remote user does not get an Office Mode IP address.
- **[True]** - If the remote hosts IP is not found in the source IP range, the user will get an Office Mode IP address using another method.
- **[False]** (default)- The flag is not used.

Office Mode through the ipassignment.conf File

It is possible to over-ride the Office Mode settings created on Security Management server by editing a plain text file called **ipassignment.conf** in the `\FWDIR\conf` directory of the VPN module. The module uses these Office Mode settings and not those defined for the object in Security Management server.

ipassignment.conf can specify:

- An **IP per user/group**, so that a particular user or user group always receives the same Office Mode address. This allows the administrator to assign specific addresses to users, or particular IP ranges/networks to groups when they connect using Office Mode.
- A different **WINS server** for a particular user or group
- A different **DNS server**
- Different **DNS domain suffixes** for each entry in the file.

```
#
# Gateway      Type  IP Address      User Name
# =====
# Paris-GW,    addr  10.5.5.8,      Jean
# Brazil,      addr  10.6.5.8, wins=(192.168.3.2,192.168.3.3) Joao
# Miami,       addr  10.7.5.8, dns=(192.168.3.7,192.168.3.8)
CN=John,OU=users,O=cpmngmt.acme.com.gibeuu
# Miami       range 100.107.105.110-100.107.105.119/24 Finance
# Miami       net  10.7.5.32/28 suffix=(acct.acme.com) Accounting
# comments are allowed
```

The diagram illustrates the configuration file with callouts for various settings:

- WINS**: Points to the `wins=(192.168.3.2,192.168.3.3)` entry for the Brazil gateway.
- Specific IP per user**: Points to the `addr` type entries for individual users (Jean, Joao).
- DNS**: Points to the `dns=(192.168.3.7,192.168.3.8)` entry for the Miami gateway.
- Domain Suffix**: Points to the `suffix=(acct.acme.com)` entry for the Miami net range.
- Specific IP per group**: Points to the `range` and `net` type entries for groups (Finance, Accounting).

Subnet masks and Office Mode Addresses

You cannot use the **ipassignment.conf** file to assign a subnet mask to a single user. If using IP pools, the mask is taken from the network object, or defaults to 255.255.255.0 if using DHCP.

Checking the Syntax

The syntax of the ipassignment file can be checked using the command **ipfile_check**.

From a shell prompt run: **vpn ipfile_check ipassignment.conf**

The two parameters are:

- **warn**. Display errors
- **detail**. Show all details

For example:

```
[user@Checkpoint conf]# vpn ipfile_check ipassignment.conf warn
Reading file records...
```

```
Invalid IP address specification in line 0057
```

```
Invalid IP address specification in line 0058
```

```
Invalid subnet in line 0060
```

```
[user@Checkpoint conf]# vpn ipfile_check ipassignment.conf detail
Reading file records...
```

```
Line 0051 is a comment (starts with #)
```

```
Line 0052 is a comment (starts with #)
```

```
Line 0053 is a comment (starts with #)
```

```
Line 0054 is a comment (starts with #)
```

```
Line 0055 is a comment (starts with #)
```

```
Line 0056 ignored because it is empty
```

```
Invalid IP address specification in line 0057
```

```
Invalid IP address specification in line 0058
```

```
line 0059 is OK. User="paul"
```

```
Invalid subnet in line 0060
```

```
line 0061 is OK. Group="dns=1.1.1.1
```

```
Line 0062 ignored because it is empty
```

```
Line 0063 ignored because it is empty
```

```
Could not read line 64 in conf file - maybe EOF
```

```
[user@Checkpoint conf]#
```

Office Mode — DHCP Configuration

1. When DHCP is the selected mode, DNS and WINS parameters are downloaded from the DHCP server. If using Office Mode in DHCP mode and you wish to supply the user with DNS and/or WINS information, make sure that the DNS and/or WINS information on your DHCP server is set to the correct IP addresses.
2. On your DHCP server's configuration, make sure that you have designated an IP address space for Office Mode users (e.g., 10.130.56.0).
3. Create a new node object by selecting **Manage > Network objects > New > Node > Host**, representing the DHCP server and specify the machine's name, IP address and subnet mask.
4. Open the Security Gateway object through which the remote users will connect to the internal network and select the **IPSec VPN > Office Mode** page. Enable Office Mode to either all users or to a certain group.

- Check the **Automatic (use DHCP)** option.
 - Select the DHCP object you have previously created.
 - In the **Virtual IP address for DHCP server replies**, specify an IP address from the sub network of the IP addresses which are designated for Office Mode usage (e.g. 10.130.56.254). Since Office Mode supports DHCP Relay method for IP assignment, you can direct the DHCP server as to where to send its replies. The routing on the DHCP server and that of internal routers must be adjusted so that packets from the DHCP server to this address are routed through the Security Gateway.
 - If you wish to use the Anti-Spoofing feature, continue to step 5, otherwise skip to step 7.
5. Create a network object to represent the address space you've allocated for Office Mode on your DHCP server, by selecting **Manage > Network Objects > New > Network**.
In the **Network Properties — General** tab, set the DHCP address range as follows:
 - In **Network Address** specify the first address that is used (e.g. 10.130.56.0).
 - In **Net Mask** enter the subnet mask according to the amount of addresses that is used (entering 255.255.255.0, for example, designates that all 254 IP addresses from 10.130.56.1 until 10.130.56.254 are set aside for remote host Office Mode addresses on the DHCP server).
 - Changes to the **Broadcast Address** section and the **Network Properties — NAT** tab are not necessary.
 - Close the network object properties window.
 6. Return to the Security Gateway object, open the **IPSec VPN > Office Mode** page. In the **Additional IP addresses for Anti-Spoofing**, select the network object you have created with the IP address range you have set aside for Office Mode on the DHCP server.
 7. Install the policy.
 8. Make sure that all the internal routers are configured to route all the traffic destined to the internal address space you had reserved to Office Mode users through the Security Gateway. For instance, in the example above it is required to add routes to the class C sub network of 10.130.56.0 through the Security Gateway's IP address.

In addition to the steps mentioned for the Security Gateway side configuration, a few configuration steps have to be performed on the client side in order to connect to the Security Gateway in Office mode.



Note - Office Mode is supported only in Connect Mode.

Office Mode - Using a RADIUS Server

To configure the RADIUS server to allocate IP addresses:

1. In SmartDashboard, click **Manage > Servers and OPSEC Applications**.
2. Select RADIUS server and click **Edit**.
The **RADIUS Server Properties** window appears.
3. Click the **RADIUS Accounting** tab.
4. Select **Enable IP Pool Management**.
5. Select the service the RADIUS server uses to communicate with remote users.

To configure the RADIUS server to perform authentication for remote users:

1. In SmartDashboard, click **Manage > Network Objects**.
2. Select Security Gateway and click **Edit**.
3. In Security Gateway properties, select **IPSec VPN > Office Mode**.
4. In the **Office Mode Method** section, select **From the RADIUS server used to authenticate the user**.
5. Click **OK**.

Office Mode Configuration on SecureClient

On the client's machine the following steps should be performed in order to connect to the Security Gateway using Office mode:

1. Right click the **SecureClient** icon in the system tray. From the pop-up menu, select **Configure**.
2. Select **Tools > Configure Connection Profile > Advanced** and select **Support Office Mode**.
3. Click **OK**, **Save** and **Close** and then select **Exit** from your **File** menu.

4. Double click your **SecureClient** icon on the bottom right side of your screen. If you're using a dial-up connection to connect to the Security Gateway select Use Dial-up and choose the name of your dial-up connection profile from the drop-down menu (it is assumed that such a profile already exists. If dial-up is not used (i.e. connection to the Security Gateway is done through a network interface card) proceed to step 5.
5. Select **Connect** to connect to the organization using Office Mode.

The administrator can simplify configuration, by configuring a profile in advance and providing it to the user.

Office Mode per Site

1. In SmartDashboard, click **Policy > Global Properties > Remote Access > VPN - Advanced**.
The VPN - Advanced page shows the office Mode Settings.
2. In the **Office Mode** section, select **Use first allocated Office Mode IP address for all connections to the Security Gateways of the site**.
3. Click **OK**.

Chapter 20

Packaging SecureClient

In This Chapter

| | |
|--|-----|
| Introduction: The Need to Simplify Remote Client Installations | 180 |
| The Check Point Solution - SecureClient Packaging Tool | 180 |
| Creating a Preconfigured Package | 181 |
| Configuring MSI Packaging | 182 |

Introduction: The Need to Simplify Remote Client Installations

As remote access to organizations becomes more widespread, administration of the remote client software becomes more difficult. Users often lack the technical expertise to configure the software themselves, requiring administrators to provide support for large numbers of users, many of whom may be geographically dispersed and using a wide variety of platforms. The administrator's task is even more difficult if the organization has several groups of users, each of which requires a different configuration.

Administrators need a tool to automate the configuration of software to large user communities. This tool must enable the administrator to preconfigure the software, so that users do not have to do this themselves.

The Check Point Solution - SecureClient Packaging Tool

Overview

The SecureClient Packaging Tool enables the administrator to create pre-configured SecureClient installation packages. Users can then use the configured package to install the software without being required to configure details, ensuring that users cannot inadvertently misconfigure their SecureClient software.

Pre-packaging can be done using either the:

- Check Point Packaging Tool Wizard
- MSI Packaging

The benefits of packaging are:

- Configuration (site creation, connection and encryption parameter specification, etc.) is performed by professional administrators, rather than by unsophisticated and error-prone users.
- Installation and support overhead are greatly reduced.
- Users' security configurations are more uniform across the organization, because they are pre-defined by the administrator rather than specified by each user individually.
- The administrator can more quickly respond to security threats by automatically updating remote users' security software.

How Does Packaging Tool Work?

Packaging Tool combines a client installation package (for example, the generic SecureClient installation package) with a package profile to create a preconfigured SecureClient package. The administrator can then distribute the package to the users.

The administrator can pre-configure the client's installation and configuration settings, such as the connection mode to the VPN Security Gateway (Connect/Transparent), encryption properties and more. These settings are saved in a package profile, and can then be used for configuring packages.

The administrator can create different package profiles for different user groups. For example, the administrator can create one profile with the configuration parameters for Windows XP users, and another for Windows 98 users. The administrator can save all the profiles in a central database.

To allow the client to connect to the organization from the moment it is installed, the administrator can specify Partial Topology information for a site, that is, the IP address of the site or of its Security Management server. This information is included in the package. The first time the user connects to and authenticates to the site, the site's full topology is downloaded to the client.

The SecureClient package can also include scripts to be run after the installation of SecureClient.

The MSI Packaging Solution

MSI is a standard file format for application distribution in a Windows environment. Once a profile is created, it is saved and may be distributed to SecuRemote and SecureClient users.

The MSI package installs SecuRemote/SecureClient Extended View with default settings and can be customized using the command line based tool - **cpmsi_tool**.

Split Installation

When used with 3rd party software distribution systems, the connection to the distribution server is broken once the SecuRemote/SecureClient kernel is installed; the result is that the distribution server is not aware that the installation ended.

In order to resolve such cases a Split Install feature is available.

Creating a Preconfigured Package

The Packaging Tool wizard guides an administrator through the process of creating a preconfigured SecureClient installation package. Each package can contain a different combination of a SecureClient version and a pre-configured profile.

You create a package in two essential stages:

1. Configuring and saving a package profile. The profile contains all the settings to be installed by the package by default.
2. Applying the profile to an existing installation package, thus creating a properly preconfigured package.

Creating a New Package Profile

1. To create a new profile, Select **Profile > New**. Enter the profile details and press **Next**.
2. The Packaging Tool wizard will guide you through the next several windows, in which you should configure different parameters regarding the user's profile, such as policy, encryption, topology (including Partial Topology information), certificates, client installation and logon parameters (SDL/Gina DLLs). For information about these features, see the relevant chapters in the documentation.
3. After pre-configuring all of the client's settings, you will be presented with the **Finish** screen. In this screen you can decide if Packaging Tool should continue to create a new package containing the changes as they appear in the profile or finish the process of profile generation without creating a new package. The options in this screen are:
 - **No, Create Profile only** — The profile will be created according to the setting you have pre-defined in the wizard and you will be returned to the main Packaging Tool window.
 - **Yes, Create profile and generate package** — If you choose this option the profile you've created will be saved and you will be taken to the package generation wizard. For instructions regarding this wizard, proceed to Generating a Package (on page [181](#)).

You can always create packages from a saved profile at a later time.

Generating a Package

This section describes how to generate a SecureClient package according to the settings defined in a package profile.

Preparation

If you have not already prepared a base package, do so now, as follows:

1. Obtain an original SecureClient installation package. This package will be the base package, upon which the Packaging Tool will create the new custom SecureClient package.
2. Copy the clean SecureClient package to an empty directory. If the package is zipped or tarred you should unpack the package to the empty directory.

Once you have a base package, proceed as follows:

1. Run the SecureClient package generation wizard. You can run the wizard immediately after creating a new package profile (by selecting **Yes, Create profile and generate package**), or from the main Packaging Tool window by highlighting a previously created profile and selecting **Profile>Generate**.
2. You will be asked to enter a package source and destination folders.
Under **Package source folder**, select the directory in which the original SecureClient installation you prepared in step 2 is located. Make sure you select the directory in which the SecureClient setup files actually exist and not a higher level directory.
Under **Package destination folder and file name**, select an empty directory to which the new package will be copied, and enter a name for the file being generated.
Press **Next** to continue to the next window.
3. If the package details cannot be extracted from the package, enter the package details (operating system type, SecureClient version and service pack) when prompted. If the package details conflict with another package, a prompt asks you to approve the replacement of the older package with the newer one.

The Packaging Tool will perform the actions you requested.

Adding Scripts to a Package

To specify that a script should be run after the user installs or uninstalls SecureClient, proceed as follows:

1. Edit the **product.ini** file.
2. To specify a post-installation script, add the file's name to the **[install]** section.
3. To specify a post-uninstallation script, add the file's name to the **[uninstall]** section.

The script should be accessible through the OS **PATH** variable.

The script is not part of the package, and should be transferred to the client separately.

Configuring MSI Packaging

To customize a profile used for remote users save the **.msi** file provided by Check Point. Once the file is saved, configurable files may be extracted from the file, customized, and then placed back into the file.

To edit one of the configurable files:

1. Use **cpmsi_tool <SC-MSI-package-name> out <file-name>** to extract the file from the package.
2. Customize the file.
3. Use **cpmsi_tool <SC-MSI-package-name> in <file-name>** to insert the file back into the package.

The configurable files are:

- **product.ini**
- **userc.c**
- **userc.set**
- **reg.ini**
- **SecuRemoteAuthenticate.wav**
- **SecuRemoteConnected.wav**
- **SecuRemoteDisconnected.wav**
- **SecuRemoteFailed.wav**

- **logo.bmp**
- **logging.bat**
- **install_boot_policy.bat**
- **collect.bat**
- **scvins.bat**
- **scvuins.bat**
- **msfw.bat**
- **harden.bat**

Add and Remove Files in Package

To add new files to the package:

cpmsi_tool <SC-MSI-package-name> add <file-name>

To remove a newly added file:

cpmsi_tool <SC-MSI-package-name> remove <file-name>

Installation Command Line Options

The following are the command line parameters.

| Parameter | Description |
|--------------------|--------------------|
| /i pkg_name | Install |
| /x pkg_name | Uninstall |
| /q | Quiet installation |
| /!*v log_file_name | Collect logs |

Split Installation

To activate:

1. Set **SplitKernellInstall=0** in the **product.ini** file.
2. Install the product except for the kernel.
3. An automatic reboot, initiated by the end user, will occur.
4. After the reboot, the automatic kernel installation takes place.
5. A second automatic reboot will occur

Debug

In order to debug the MSI installation, run the **/!*v log_file_name_parameter**. **log_file_name** and **install_securemote.elg** are used for troubleshooting.

Zone Labs Endpoint Security Client

When installing the SecureClient MSI package with Zone Labs integration, use the following syntax:

msiexec /i <package_name> [ZL=1] [INSTALLDIR=<install_dir>] [/qr/qb/qb!]

- **package_name** - the SecureClient msi package name
- **ZL=1** - install with Zone Labs configuration

- `INSTALLDIR=<install_dir>` - the folder where the package is installed
- `[/qr/qb/qb!]` - standard MSI UILevel support used for silent installation.

Using this command, the **product.ini** file is automatically modified.

Chapter 21

Desktop Security

In This Chapter

| | |
|---------------------------------|-----|
| The Need for Desktop Security | 185 |
| Desktop Security Considerations | 185 |
| Configuring Desktop Security | 186 |

The Need for Desktop Security

A Security Gateway protects a network by enforcing a Security Policy on the traffic to and from that network that passes through the Security Gateway. A remote client, located outside the protected network, is vulnerable to attack because traffic to the remote client does not pass through the Security Gateway — no Security Policy is enforced on this traffic.

There is a further danger: an attacker might gain access to a protected network by compromising a remote client, which may in turn compromise the protected network (for example, by relaying a virus through the VPN tunnel). Even if the Security Gateway enforces a very restrictive Security Policy, the LAN remains vulnerable to attacks routed through unprotected remote clients.

Desktop Security Considerations

Desktop Security Considerations

You should carefully plan your users policy, properly balancing considerations of security and convenience. The policy should allow the desktop users to work as freely as possible, but at the same time make it hard to attack the remote user's desktop. Here are some points to consider:

- You should not explicitly allow any service to be opened to clients (i.e. allow a service in the inbound policy), unless the user has a specific server running on that port. Even if you do allow connections to be opened to the client, be very careful about who is allowed to open the connection, and from where.
- A restrictive policy (e.g., allow only POP3, IMAP and HTTP and block all the rest) will make it more difficult for your users to work. If you allow only specific services in the outbound policy and block all the rest, every time you will find out that a certain service is needed by your users, you will have to change the outbound policy and make sure the clients poll the new policy. The best way to implement the outbound policy is to use rules only to block specific problematic services (such as Netbus) and allow the rest.
- Outbound connections to the encryption domain of the organization are always encrypted, even if the outbound rule for the service specifies "accept".
- Keep in mind that the implied rules (see Implied Rules) may allow or block services which were not explicitly handled in previous rules. For example, if your client runs a server on his machine, you must create an explicit rule allowing the connection to the client's machine. If you do not, the connection will be blocked by the inbound implicit block rule.

Avoiding Double Authentication for Policy Server

When using Policy Server High Availability, it is possible that users will connect to the organization through one Security Gateway and to a Policy Server which is installed on a different module. In this case they will be prompted twice for authentication — once for the Security Gateway module and the other for the Policy Server. If a user usually connects to the organization through a specific Security Gateway, and this Security Gateway has a Policy Server module installed on it, this double authentication can be avoided by configuring the user's profile to use the **High Availability among all Policy Servers, trying selected first** option, and selecting the primary Policy Server as that one the Security Gateway through which the user usually connects to the organization. This way, after the user authenticates to the Security Gateway, he will

automatically be authorized to download the security policy from the Policy Server installed on that Security Gateway.

Configuring Desktop Security

Desktop Security must be configured on the server and on the client machine.

Server Side Configuration

1. Install the Policy Server add-on module from the Check Point installation DVD. The Policy Server add-on should be installed only on machines that have Security Gateway modules installed on them.
2. Open the Security Gateway object on which you have installed a Policy Server and select the **General Properties** tab. In the **Check Point Products** section select **SecureClient Policy Server**.
3. Go to the **Authentication** tab. In the **Policy Server > Users** section select a group of users that is allowed to retrieve policies from this Policy Server.
4. Repeat steps 2 and 3 for each additional Policy Server.
5. Go to **Policy > Global Properties** and select the **Remote Access** tab. In **Revert to default policy after**, select the time-out for desktop security policies (see Policy Renewal).
6. In the policy selection toolbar, select **Desktop Security**.
7. Configure the inbound rules. Using the **Rules>Add Rule** menu item, you can add rules to the policy. In inbound rules, the SecureClient (the desktop) is the destination, and you can specify the users to which the rule is to be applied.
8. Configure the outbound rules. In outbound rules, the SecureClient (the desktop) is the source, and you can specify the users to which the rule is to be applied.
9. Install the policy. Be sure to install both the Advanced Security policy on the Security Gateways and the Desktop Security policy on your Policy Servers.

Client Side Configuration

1. Double click the SecureClient icon at the bottom right side of your desktop and press **Properties**.
2. Choose **Logon to Policy Server** if you wish to logon to a Policy Server automatically after connecting to a site.
3. Select **Support Policy Server High Availability** if your site has several Policy Servers and you want SecureClient to attempt to load balance between them. If you choose to use this feature you must select one of the following:
 - **High Availability among all servers, trying selected first** — Select the primary Policy Server.
 - **High Availability only among selected servers** — Select the servers to which you wish to connect.

As an administrator, you can eliminate the user's need to configure these steps by creating a custom profile for them.

Chapter 22

Layer Two Tunneling Protocol (L2TP) Clients

In This Chapter

| | |
|--|-----|
| The Need for Supporting L2TP Clients | 187 |
| Solution - Working with L2TP Clients | 187 |
| Considerations for Choosing Microsoft IPsec/L2TP Clients | 190 |
| Configuring Remote Access for Microsoft IPsec/L2TP Clients | 191 |

The Need for Supporting L2TP Clients

For some organizations there are clear benefits to be gained by using the Microsoft IPsec client for remote access to internal network, rather than the more feature rich and secure Check Point SecuRemote/SecureClient.

Reasons for using the Microsoft L2TP IPsec client include the fact that is an inherent part of many Windows operating systems, does not require an additional client to be installed, and is free.

Solution - Working with L2TP Clients

Introduction to L2TP Clients

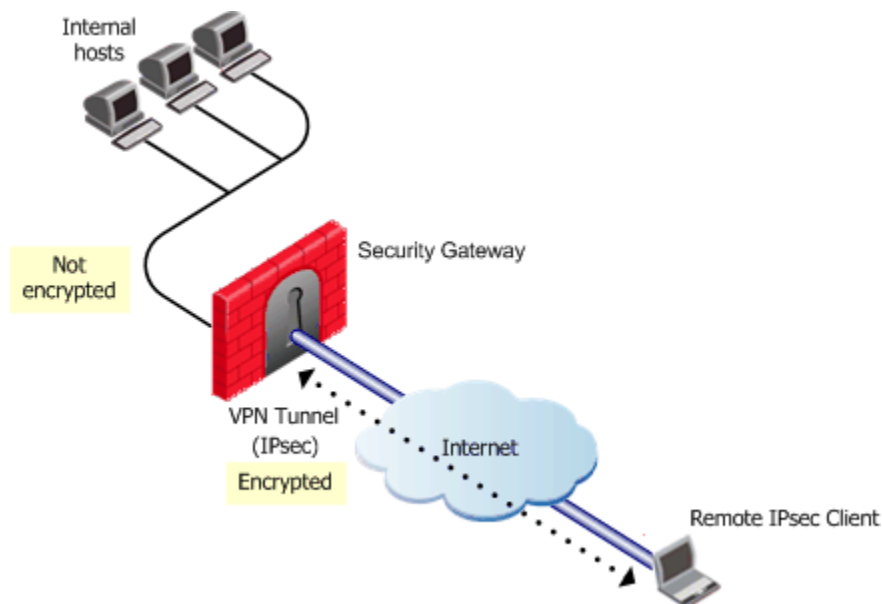
Check Point Security Gateways can create VPNs with a number of third party IPsec clients. This explanation focuses on the Microsoft IPsec/L2TP client.

You can access a private network through the Internet by using a virtual private network (VPN) connection with the Layer Two Tunneling Protocol (L2TP). L2TP is an industry-standard Internet tunneling protocol.

Creating a Remote Access environment for users with Microsoft IPsec/L2TP clients is based on the same principles as those used for setting up Check Point Remote Access Clients. It is highly recommended to read and understand Introduction to Remote Access VPN before attempting to configure Remote Access for Microsoft IPsec/L2TP clients.

Establishing a VPN between a Microsoft IPsec/L2TP Client and a Check Point Gateway

To allow the user at the Microsoft IPsec/L2TP client to access a network resource protected by a Security Gateway, a VPN tunnel is established between the Microsoft IPsec/L2TP client and the Security Gateway, as shown below.



The process of the VPN establishment is transparent to the user, and works as follows:

1. A user at an Microsoft IPsec/L2TP client initiates a connection to a Security Gateway.
2. The Microsoft IPsec/L2TP client starts an IKE (Internet Key Exchange) negotiation with the peer Security Gateway in order to initiate construction of an encrypted tunnel.
3. During IKE negotiation, the identities of the remote client machine and the Security Gateway are authenticated. This authentication is performed by means of certificates. Both sides send their certificates to each other as means of proving their identity. This ensures that a connection can be made only from the authenticated machine.
4. Both peers exchange encryption keys, and the IKE negotiation ends.
5. Encryption is now established between the client and the Security Gateway. All connections between the client and the Security Gateway are encrypted inside this VPN tunnel, using the IPsec standard.
6. The Client starts a short L2TP negotiation, at the end of which the client can pass to the Security Gateway L2TP frames that are IPsec encrypted and encapsulated.
7. The Security Gateway now authenticates the user at the Microsoft IPsec/L2TP client. This authentication is in addition to the client machine authentication in step 3. This identification can happen via two methods.
 - A Certificate
 - An MD5 challenge, whereby the user is asked to enter a username and a password (pre-shared secret)
8. The Security Gateway allocates to the remote client an Office Mode IP address to make the client routable to the internal network. The address can be allocated from all of the Office Mode methods.
9. The Microsoft IPsec/L2TP client connects to the Security Gateway, and can browse and connect to locations in the internal network.

Behavior of an L2TP Connection

When using an IPsec/L2TP client, it is not possible to connect to organization and to the outside world at the same time.

This is because when the client is connected to the Security Gateway, all traffic that leaves the client is sent to the Security Gateway, and is encrypted, whether or not it is intended to reach the protected network behind the Security Gateway. The Security Gateway then drops all encrypted traffic that is not destined for the encryption domain of the Security Gateway.

Security Gateway Requirements for IPSec/L2TP

In order to use Microsoft IPSec/L2TP clients, the Security Gateway must be set up for remote access. The setup is very similar to that required for remote access using Check Point Remote Access Clients, and involves creating a Remote Access community that includes the Security Gateway(s) and the user groups.

An additional requirement is to configure the Security Gateway to supply addresses to the clients by means of the Office Mode feature.

L2TP Global Configuration

Certain settings related to L2TP authentication can be configured globally for Security Gateways of version R71 and higher. These settings are configured using GuiDBedit, the Check Point Database Tool.

All L2TP clients can be configured to use a Pre-shared key for IKE in addition to the standard user authentication.



Note - IKE Security Authority created for L2TP cannot be used for regular IPSec traffic.

Authentication of Users and Client Machines

There are two methods used to authenticate an L2TP connection:

- Using Legacy Authentication
- Using certificates

Authentication Methods

L2TP clients can use any of the following Authentication schemes to establish a connection:

- Check Point password
- OS password
- RADIUS
- LDAP
- TACACS

Using a username and password verifies that a user is who they claim to be. All users must be part of the Remote Access community and be configured for Office Mode.

Certificates

During the process of establishing the L2TP connection, two sets of authentication are performed. First, the *client machine* and the *Security Gateway* authenticate each other's identity using certificates. Then, the *user* at the client machine and the *Security Gateway* authenticate each other using either certificates or a pre-shared secret.

The Microsoft IPSec/L2TP client keeps separate certificates for IKE authentication of the client machine, and for user authentication.

On the Security Gateway, if certificates are used for user authentication, then the Security Gateway can use the same certificate or different certificates for user authentication and for the IKE authentication.

Certificates for both clients and users can be issued by the same CA or a different CA. The users and the client machines are defined separately as users in SmartDashboard.

Certificates can be issued by:

- The Internal Certificate Authority (ICA) on the Security Management server, *or*
- An OPSEC certified Certificate Authority.

The certificates must use the PKCS#12 format, which is a portable format for storing or transporting private keys and certificates. The certificates are transferred to and stored on the client machine.

Authenticating the Client Machine During IKE

The Microsoft IPSec/L2TP client machine needs a certificate to authenticate itself to the Security Gateway during IKE negotiation.

It is possible to have only one certificate for all client machines, but you will then not be able to identify the machine that the user logged on from. For example, SmartView Tracker would show "user=bob, machine=generic_laptop" rather than "user=bob, machine=bob_laptop".

The computer account (we call it the machine account) must use PKI and must be in the Remote Access community. It is not affected by the authentication scheme in the Remote Access tab in the GUI. It may or may not be a good idea to use the same certificate (and "machine" user) for all clients. You can use an internal CA certificate with no problem for this user. It makes no difference if the authentication tab is defined or not.

The user account is more important, because that is the basis for rule matches and logs. This may use either MD5-challenge (passwords) or certificates. If you choose MD5-challenge, the certificate selection in the remote access tab is irrelevant. As for the user definition, it makes no difference how, if at all, the authentication tab is defined. The password is always the shared secret defined in the encryption tab. Note that this behavior differs from that of Secure Client, where passwords in the authentication tab override shared secrets from the encryption tab.

The client machine administrator must install the certificate in the machine certificate store.

Authenticating the User

Connecting with Microsoft IPSec/L2TP clients requires that every user be authenticated. Users can be authenticated with:

- Certificates, or
- Using an MD5 challenge, whereby the user is asked to enter a username and a password (pre-shared secret). The user must be informed of the password "out-of-band"

The user certificate can be easily added to the user certificate store. If the user certificate is on a Smart Card, plugging it into the client machine will automatically place the certificate into the certificate store.

User Certificate Purposes

It is possible to make sure that PKI certificates are used only for a defined *purpose*. A certificate can have one or more purposes, such as "client authentication", "server authentication", "IPSec" and "email signing". Purposes appear in the *Extended Key Usage extension* in the certificate.

The certificates used for IKE authentication do not need any purposes. For the user authentication, the Microsoft IPSec/L2TP client requires that

- The user certificate must have the "client authentication" purpose.
- The Security Gateway certificate must have the "server authentication" purpose.

Most CAs (including the ICA) do not specify such purposes by default. This means that the CA that issues certificates for IPSec/L2TP clients must be configured to issue certificates with the appropriate purposes (in the Extended Key Usage extension).

It is possible to configure the ICA on the Security Management server so that the certificates it issues will have these purposes. For OPSEC certified CAs, it is possible to configure the Security Management server to create a certificate request that includes purposes (in the Extended Key Usage extension).

It is also possible to configure the Microsoft IPSec/L2TP clients so that they do not validate the Security Gateway's certificate during the L2TP negotiation. This is not a security problem because the client has already verified the Security Gateway certificate during IKE negotiation.

Considerations for Choosing Microsoft IPSec/L2TP Clients

Check Point Endpoint Security VPN is much more than a personal firewall. It is a complete desktop security solution that allows the administrator to define a full desktop security policy for the client. IPSec/L2TP clients are more basic remote clients, and for some organizations may provide an adequate set of capabilities.

When using an IPSec/L2TP client, it is not possible to connect to organization and to the outside world at the same time. For some organizations, this may be an appropriate connection policy as it effectively

dedicates the machine to being connected to the organization. Check Point Remote Access Clients on the other hand, make it possible to be connected to the organization and to the Internet at the same time.

Configuring Remote Access for Microsoft IPsec/L2TP Clients

Establishing a Remote Access VPN for Microsoft IPsec/L2TP clients requires configuration to be performed both on the Security Gateway and on the client machine. The configuration is the same as setting up Check Point Remote Access Clients, with a few additional steps. It is highly recommended to read and understand Introduction to Remote Access VPN before configuring Remote Access for Microsoft IPsec/L2TP clients.

The general procedure is as follows:

1. Using SmartDashboard, configure a Remote Access environment, including generating authentication credentials (normally certificates) for the users.
2. Generate certificates to authenticate the client machines.
3. Configure support for Office Mode and L2TP on the Security Gateway.
4. On the client machine, place the user certificate in the User Certificate Store, and the client machine certificate in the Machine Certificate Store.
5. On the client machine, set up the Microsoft IPsec/L2TP client connection profile.

Configuration details are described in the following sections.

General Configuration Procedure

Configuring a Remote Access Environment

Follow the instructions in VPN for Remote Access Configuration.

Defining the Client Machines and their Certificates

1. Define a user that corresponds to each client machine, or one user for all machines, and generate a certificate for each client machine user. The steps are the same as those required to define users and their certificate.
2. Add users that correspond to the client machines to a user group, and add the user group to the Remote Access VPN community.

Configuring Office Mode and L2TP Support

1. Configure Office Mode. For detailed instructions, see Configuring Office Mode (on page [174](#)).
2. On the Security Gateway object, **IPsec VPN > Remote Access** page, check **Support L2TP**.
3. Select the **Authentication Method** for the users:
 - To use certificates, choose **Smart Card or other Certificates (encryption enabled)**.
 - To use a username and a shared secret (password), choose **MD5-challenge**.
4. For **Use this certificate**, select the certificate that the Security Gateway presents in order to authenticate itself to users. This certificate is used if certificates are the chosen **Authentication Method** for users, in step 3.

Preparing the Client Machines

1. In the Windows **Services** window of the client machine, make sure that the **IPsec Policy Agent** is running. It should preferably be set to Automatic.
2. Make sure that no other IPsec Client is installed on the machine.

Placing the Client Certificate in the Machine Certificate Store

1. Log in to the client machine with administrator permissions.
2. Run the Microsoft Management Console. Click **Start > Run**
3. Type: **MMC**, and press Enter.

4. Select **Console > Add/Remove Snap-In**.
5. In the **Standalone** tab, click **Add**.
6. In the **Add Standalone Snap-in** window, select **Certificates**.
7. In the **Certificates snap-in** window, select **Computer account**.
8. In the **Select Computer** window select the computer (whether local or not) where the new certificates have been saved.
9. Click **Finish** to complete the process and click **Close** to close the **Add/Remove Snap-in** window.
10. The MMC **Console** window is displayed, where a new certificates branch has been added to the Console root.
11. Right-click on the **Personal** entry of the **Certificates** branch and select **All Tasks > Import**. A Certificate Import Wizard is displayed.
12. In the Certificate Import Wizard, browse to the location of the certificate.
13. Enter the certificate file password.
14. In the **Certificate Store** window make sure that the certificate store is selected automatically based on the certificate type.
15. Select **Finish** to complete the Import operation.

Using the MMC, the certificate can be seen in the certificate store for the "Local Computer".

Placing the User Certificate in the User Certificate Store

1. On the client machine, double-click on the user's certificate icon (the **.p12** file) in the location where it is saved. A Certificate Import Wizard is displayed
2. Enter the password.
3. In the **Certificate Store** window make sure that the certificate store is selected automatically based on the certificate type.
4. Select **Finish** to complete the Import operation.

Using the MMC, the certificate can be seen in the certificate store for the "current user".

Setting up the Microsoft IPsec/L2TP Client Connection Profile

Once the Client machine's certificate and the user's certificate have been properly distributed, set up the L2TP connection profile.

1. In the client machine, right-click on the **My Network Places** icon on the desktop and select **Properties**.
2. In the **Network and Dial-up Connections** window, select **Make New Connection**. The Network Connection Wizard is displayed.
3. In the **Network Connection Type** window: On Windows 2000 machines select **Connect to a private network through the Internet**. On Windows XP machines select **VPN or dial-up**, and in the next window select **VPN**.
4. In the **Destination Address** window, enter the IP address or the resolvable host name of the Security Gateway.
5. In the **Connection Availability** window, make the new connection available **For all users** or **Only for myself**.
6. In the closing window, provide a name for the new connection, for example, *L2TP_connection*.
7. The **Connect** window for the new connection type is displayed.

To complete the L2TP connection configuration, proceed as follows. Note that the order is important:

1. In the **Connect** window, click **Properties**.
2. In the **Networking** tab, select the L2TP server.
3. In the **Security** tab, choose **Advanced > Settings**, and select **Use extensible Authentication protocols** or **Allow these protocols**.

If you select **Use extensible Authentication protocols**: Choose either **MD5-challenge**, or **Smart Card or other Certificates (encryption enabled)**. Make the same choice as made on the Security Gateway.

If you select **Allow these protocols**: Choose **Unencrypted password (PAP)**.

For more information, see Configuring Office Mode and L2TP Support (on page 191).

4. Click **OK** to save the configured settings and to return to the **Connect** window.
5. In the **Connect** window, enter the user name and password or select a certificate.

Configuring User Certificate Purposes

A CA that issues certificates for IPSec/L2TP clients must be configured to issue certificates with the appropriate purposes.

Alternatively, the Microsoft IPSec/L2TP Client can be set to not require the "Server Authentication" purpose on the Security Gateway certificate.

To configure the CA to Issue Certificates with Purposes

1. If using the ICA, run the ICA Management Tool.
 - Change the property **IKE Certificate Extended Key Usage** property to the value 1, to issue Security Gateway certificates with the "server authentication" purpose.
 - Change the property **IKE Certificate Extended Key Usage** to the value 2 to issue user certificates with the "client authentication" purpose.

If using an OPSEC certified CA to issue certificates, use the **DBedit** command line or the graphical Database Tool to change the value of the global property **cert_req_ext_key_usage** to 1. This will cause the Security Management server to request a certificate that has purposes (Extended Key Usage extension) in the certificate.
2. Using SmartDashboard, issue a new certificate for the Security Gateway. (In the **VPN** page, in the **Certificate List** section click **Add**. A new **Certificate Properties** window opens.) Look at the certificate properties and check that the Extended Key Usage Extension appears in the certificate.
3. In the **Remote Access** page of the Security Gateway object, in the **L2TP Support** section, select the new certificate.

To Configure the Microsoft IPSec/L2TP Clients so they do not Check for the "Server Authentication" Purpose

The following procedure tells the Microsoft IPSec/L2TP Client not to require the "Server Authentication" purpose on the Security Gateway certificate.

1. In the client machine, right-click on the **My Network Places** icon on the desktop and select **Properties**.
2. In the **Network and Dial-up Connections** window, double click the L2TP connection profile.
3. Click **Properties**, and select the **Security** tab.
4. Select **Advanced (custom settings)**, and click **Settings**.
5. In the **Advanced Security Settings** window, under **Logon security**, select **Use Extensible Authentication Protocol (EAP)**, and click **Properties**.
6. In the **Smart Card or other Certificate Properties** window, uncheck **Validate server certificate**, and click **OK**.



Note - The client validates all aspects of the Security Gateway certificate, during IKE authentication, other than the "Server Authentication" purpose.

Making the L2TP Connection

1. Click on **Connect** to make the L2TP connection.
2. To view the IP address assigned to the connection, either view the **Details** tab in the connection **Status** window, or use the **ipconfig /all** command.

For More Information

For more information about how to configure advanced capabilities for Microsoft IPSec/L2TP clients, see

- Non-Private Client IP Addresses (on page [227](#)).
- Enabling IP Address per User (on page [171](#)).
- Back Connections (Server to Client) (on page [232](#)).

The L2TP protocol is defined in RFC 2661. Encryption of L2TP using IPSec is described in RFC 3193. For information about the L2TP protocol and the Microsoft IPSec/L2TP client, see the Network and Dial Up Connections Help in Windows 2000 and XP.

Chapter 23

Secure Configuration Verification

In This Chapter

| | |
|--|-----|
| The Need to Verify Remote Client's Security Status | 195 |
| The Secure Configuration Verification Solution | 195 |
| Considerations regarding SCV | 198 |
| Configuring SCV | 198 |



Note - The procedures in this section are relevant for SecureClient. For other clients, see the most updated documentation for that client (<http://supportcontent.checkpoint.com/solutions?id=sk67820>).

The Need to Verify Remote Client's Security Status

Network and Firewall administrators can easily control computers inside their organization. In a Microsoft domain based environment, this is done by controlling the user's privileges through the network domain controller. The administrator can disable hazardous components such as Java and ActiveX controls in browsers, install Anti-Virus checkers and make sure they are running correctly.

In the case of remote users, the administrator's options are limited, because remote users access the organization from outside the LAN (e.g., across the Internet), and are usually unable to connect to the domain. The administrator cannot control and verify their configuration through the domain controller.

For example, suppose the remote user has ActiveX enabled, and connects to a website containing a malicious ActiveX control which infects his or her computer. When the remote user connects to the organization's LAN, the LAN becomes vulnerable as well.

Even a properly configured Desktop Security Policy, important as it is, does not afford protection against this type of attack, because the attack does not target a vulnerability in the access control to the user's machine, but rather takes advantage of the vulnerable configuration of applications on the client.

The Secure Configuration Verification Solution

Introducing Secure Configuration Verification

Secure Configuration Verification (SCV) enables the administrator to monitor the configuration of remote computers, to confirm that the configuration complies with the organization's Security Policy, and to block connectivity for machines that do not comply. SCV does not replace the Desktop Security Policy, but complements it. SCV strengthens enterprise security by ensuring SecureClient machines are configured in accordance with the enterprise Security Policy.

SCV is a platform for creating and using SCV checks. SCV checks include sets of conditions that define a securely configured client system, such as the user's browser configuration, the current version of the Anti-Virus software installed on the desktop computer, the proper operation of the personal firewall policy, *etc.* These security checks are performed at pre-defined intervals by SecureClient. Depending on the results of the SCV checks, the Security Gateway decides whether to allow or block connections from the client to the LAN.

Check Point's SCV solution comes with a number of predefined SCV checks for the operating system and user's browser, and it also allows OPSEC partners, such as Anti-Virus software manufacturers, to add SCV checks for their own products.

How does SCV work?

SCV works in six steps:

1. Installing SCV plugins on the client.
2. Configuring and SCV Policy on the Security Management server.
3. Downloading the SCV Policy to the Client.
4. Verifying the SCV Policy.
5. Runtime SCV checks.
6. Making the organizational Security Policy SCV aware.

Installing SCV Plugins on the Client

SCV checks are performed through special DLLs which check elements of the client's configuration and return the results of these checks. An SCV application registers its SCV DLLs in the system registry.

The first step in configuring SCV is for the administrator to install the applications that provide the SCV checks on the client. During installation, these applications register themselves as SCV plug-ins and write a hash value of their SCV DLLs to prevent tampering.

Configuring an SCV Policy on the Security Management server

An SCV Policy is a set of rules or conditions based on the checks that the SCV plug-ins provide. These conditions define the requested result for each SCV check, and on the basis of the results, the client is classified as securely configured or non-securely configured. For example, an administrator who wishes to disallow a file-sharing application would define a rule in the SCV Policy verifying that the file-sharing application process is not running.



Note - The SCV check described in this example is among the pre-defined SCV checks included with Security Management server (see Check Point SCV Checks (on page 197)). This check must be configured to test for the specific process.

If *all* the SCV tests return the required results, the client is considered to be securely configured. If even one of the SCV tests returns an unexpected result, the client is considered to be non-securely configured.

Downloading the SCV Policy to the Client

When SecureClient downloads its Desktop Policy from the Policy Server, it downloads its SCV Policy at the same time.

Verifying the SCV Policy

After downloading the SCV Policy, SecureClient confirms that the SCV DLL's specified in the SCV Policy have not been tampered with by calculating their hash values and comparing the results with the hash values specified for the DLLs when they were installed (see [Installing SCV Plugins on the Client](#) (see "Installing SCV Plugins on the Client" on page 196)).

Runtime SCV Checks

At regular intervals (default is every 15 seconds), SecureClient performs the SCV checks specified in the SCV Policy by invoking the SCV DLLs, and compares the results to the SCV Policy. The SCV Policy can be configured to display a popup notification on non-securely configured clients and/or send a log to the Security Management server.

Making the Organizational Security Policy SCV-Aware

SecureClient is now able to determine whether the client is securely configured. Once all the organization's clients have been configured according to the previous steps, the administrator specifies the actions to be taken on the Security Gateway based on the client's SCV status. For example, the administrator can specify that non-securely configured clients cannot access some or all of the resources on the corporate LAN, protecting the organization from the dangers associated with the client's poor security configuration.

The administrator can choose whether to enforce SCV for remote clients. If SCV is enforced, only securely configured clients are allowed access under the rule. If SCV is not enforced, all clients are allowed access under the rule.

In simplified mode, this is configured globally. In traditional mode, this is configured individually for each rule. See [Server Side Configuration](#) (on page 199) for more information.

When the client connects to a Security Gateway, an IKE negotiation takes place between SecureClient and the Security Gateway. If the Security Gateway's Security Policy requires an SCV check to be made, the Security Gateway holds the connection while it checks if the client is securely configured (SCVed). If the Security Gateway already knows the client's SCV status (i.e., the SCV status was checked in the last 5 minutes), then:

- If the client is securely configured, the Security Gateway allows the connection.
- If the client is not securely configured, the Security Gateway either drops the connection, or accepts and logs it (this behavior is configurable).

If the Security Gateway does not know the client's SCV status, it initiates an SCV check by sending an ICMP unreachable error message containing an SCV query to the client. When a client gets this SCV query, it tries to determine its SCV status. In Connect mode, the client also connects to a Policy Server to download an updated SCV Policy. In parallel, when the client gets the SCV query, it starts sending SCV status replies to the Security Gateway via UDP port 18233 every 20 seconds for 5 minutes. These replies are used as a keep-alive mechanism, in order to keep the user's connection alive in the Security Gateway's state tables while the client is trying to determine its SCV status. The keep alive packets also allow the user to open subsequent connections in the 5 minute period in which they are sent without a need for further SCV queries. When the client determines its SCV status, it sends an SCV reply containing the status back to the Security Gateway via UDP port 18233. When the Security Gateway receives the SCV status of the user, it decides how to handle the user's connection.

SCV Checks

Check Point SCV Checks

A number of SCV checks are provided as part of the SecureClient installation, including:

- **SC_VER_SCV** — a version check that verifies that the SecureClient version is up to date, according to the administrator's specification.
- **Network Configuration Monitor** — verifies that:
 - the Desktop Policy is enforced by SecureClient on all network interface cards
 - non-IP protocols are not enabled on any interface
- **OS Monitor** — verifies the remote user's Operating System version, Service Pack, and Screen Saver configuration (activation time, password protection, etc.).
- **HotFix Monitor** — verifies that operating system security patches are installed, or not installed.
- **Group Monitor** — verifies whether the user had logged on the machine and that the user is a member of certain Domain User Groups specified by the administrator.
- **Process Monitor** — checks whether a specified process is running on the client machine (e.g. that a file sharing application is not running, or that Anti-Virus software is running). Process Monitor may also check whether a process is not running.
- **user_policy_scv** — checks the state of the desktop policy, i.e. whether the user is logged on to a policy server, and whether the desktop policy is recent.
- **Browser Monitor** — verifies the Internet Explorer version and specific IE configuration settings, such as various Java and ActiveX options.
- **Registry Monitor** — verifies that a certain key or value is present in the system registry. RegMonitor may check not only for the existence/exclusion of keys but also their content.
- **ScriptRun** — runs a specified executable on SecureClient machine and tests the return code of the executable (e.g. a script that checks whether a certain file is present and sets a return code accordingly). ScriptRun can run a script which performs additional configuration checks.
- **Anti-Virus Monitor** — detects whether an Anti-Virus program is running and checks its version. Supported Anti-Virus programs: Norton, Trend Office Scan, and McAfee.
- **SCVMonitor** — verifies the version of the SCV product, specifically the versions of the SCV DLLs installed on the client's machine.

- **HWMonitor** — verifies the CPU type, family, and model.

Third Party SCV Checks

SCV checks can be written by third party vendors using Check Point's OPSEC SCV SDK. After these applications are installed, the administrator can use these SCV checks in the SCV Policy.

Additional Script Elements

- **SCVpolicy** — selects SCV checks out of the ones defined in SCVNames (see: SCVNames (on page 202)) that will run on the user's desktop.
- **SCVGlobalParams** — is used to define general SCV parameters.

A network administrator can easily enable a set of specific SCV checks (e.g. only check that the user's SecureClient is enforcing a security policy) or as many SCV checks as required (e.g. all of the above SCV checks). The SCV checks are performed independently by the SCV Dynamic Link Libraries, and SecureClient checks their status through the SCV plugins every 15 seconds, and determines whether the user is securely configured or not. If one or more of the tests fails, the SecureClient is considered to be non-securely configured.



Note - To enforce a specific SCV check, set the parameters of the check in the SCVNames section, and include the name of the check in SCVPolicy

Considerations regarding SCV

The following sections describe things that are important to know before configuring SCV.

Planning the SCV Policy

The file **\$FWDIR/conf/local.scv** on the Security Management server contains a sample of a basic SCV policy for checks that are supplied with any SCV installation. You can review this file to help you decide which SCV tests to perform. If you need additional SCV checks for OPSEC products, such as Anti-Virus and Endpoint security SCV checks, visit: <http://www.opsec.com>.

User Privileges

To implement SCV effectively, it is suggested that you consider not to allow your remote users to have administrative privileges on their desktops. Giving the users administrative privileges can allow them to change system settings and cause SCV tests to fail. A desktop which fails an SCV check is a potential security threat to the organization.

For example, as an administrator you may want to configure the user's browser not to allow him to download Java applets from websites. A normal user will not be able to download these applets, but a user with administrative privileges can override the browser's configuration. A properly defined SCV policy can indicate that the browser's configuration had changed and trigger a proper action on the Security Gateway side. However, if the user is allowed by the Security Gateway to pass to the LAN - either by a wrong configuration of the SCV policy or lack of enforcement of the user's SCV status on the Security Gateway side - then the user's desktop will become a potential security risk to the LAN.

The SCV policy itself is protected. Users can not change the SCV policy definition files they receive, even if they have administrative rights. The SCV policy files supplied to the client are signed before arriving to the client and checked against their signature by SecureClient. If the signatures do not match, the SCV check fails.

Configuring SCV

Configuring SCV involves setting it up on the server, setting it up on the client, and configuring SCV policy.

Server Side Configuration

1. First you need to configure several general parameters regarding SCV. Open your SmartDashboard and go to **Policy > Global Properties** and select the **Remote Access > Secure Configuration Verification (SCV)** tab. This tab has several options:
 - **Apply Secure Configurations on Simplified Mode** - specifies whether all remote access rules in the simplified policy mode should have the SCV flag turned on.
 - **Upon Verification failure** - specifies the action that should be performed when the client fails one or more SCV checks. The options are to Block the client's connection or to Accept it and send a log about the event.
 - **Basic configuration verification on client's machine** - specifies whether SecureClient should perform SCV checks to determine whether the policy is installed on all network interfaces cards on the client's desktop, and whether only TCP/IP protocols are installed on these interfaces.
 - **Configurations Violation Notification on client's machine** - specifies whether a log record should be saved on the Security Management server machine indicating that a remote user is not SCVed (this is a general indication, without a specification of a certain SCV check the user's desktop had failed).
2. Close the **Global Properties** screen.
3. If you are using simplified mode (the mode that supports VPN communities), skip this step. If you are using traditional mode, edit your Security Policy Rule base and add SCV checks for your remote access rules (Client Encrypt or Client Auth rules). To enable SCV for a remote access rule, right click on the action tab of the rule and choose **Edit properties > Apply rule Only if Desktop Configuration is Verified**. Close the properties screen by pressing **OK**.
4. Edit the **local.scv** file in the **\$FWDIR/conf** directory and configure the SCV policy. For more information, see SCV Policy Syntax (on page 199) and The local.scv Sets (on page 202).
5. Install the policy - in the policy install dialog box select the Advanced Security policy for the Security Gateways and the Desktop Security policy for the Policy Servers.

Client Side Configuration

1. If you intend to use an OPSEC SCV application, install the application on the client and enable the application's integration with SCV (see the application's documentation for information on how to do this).
2. Start SecureClient and connect to the Security Gateway to receive the SCV Policy. See: Desktop Security for more information.

SCV Policy Syntax

The SCV Policy is configured by the administrator in the text file **\$FWDIR/conf/local.scv**. This file can be edited either manually by the administrator using a text editor or using a tool called SCVEditor, available at: <http://www.opsec.com>. The **local.scv** file is a policy file, containing sets, subsets and expressions.



Note - In general, you can use the pre-defined checks (in the SCVNames section of the **local.scv** file) as templates and list the modified checks in the SCVPolicy section, without writing new SCV subsets.

Sets and Sub-sets

Each set has a certain purpose which was predefined for it. For example, one set can be used to define certain parameters, another could specify certain actions that should take place in a certain event etc. Sets are differentiated by their names and hierarchy in a recursive manner. Each set can have a sub-set, and each sub-set can have a sub-set of its own and so on. Subsets can also contain logical expressions. Sets and sub-sets with more than one sub-sets/conditions are delimited by left and right parentheses **()**, and start with the set/sub-set name. Differentiation between sub-sets/expressions with the same hierarchy is done using the colon **:**. For example:


```
(SetName
  :SubSetName1 (
    :ExpressionName1_1 (5)
    :ExpressionName1_2 (false)
  )
  :SubSetName2 (
    :ExpressionName2_1 (true)
    :SubSetName2_1 (
      :ExpressionName2_1_1 (10)
    )
  )
)
```

In the example above the set named **SetName** has two subsets: **SubSetName1** and **SubSetName2**. **SubSetName1** has two conditions in it (**ExpressionName1_1** and **ExpressionName1_2**). **SubSetName2** has one condition (**ExpressionName2_1**) and one subset (**SubSetName2_1**) in it. **SubSetName2_1** has one condition as well (**ExpressionName2_1_1**).

Expressions

Expressions are evaluated by checking the value of the expression (which corresponds to an SCV check) and comparing it with the value defined for the expression (the value in the parentheses). For example, in the browser monitor SCV check provided with SecureClient, you can specify the following expression:

```
:browser_major_version (5)
```

This expression checks whether the version of the Internet Explorer browser installed on the client is 5.x. If the (major) version is 5, this expression is evaluated as true, otherwise it is evaluated as false. The name of the expression (e.g. "browser_major_version") is determined by the SCV application and is supplied by manufacturer.

If several expressions appear one after the other, they are logically ANDed, meaning that only if all expressions are evaluated as true, then the value of all of them taken together is true. Otherwise (if even one of the expressions is false), the value of all of them is false. For example:

```
:browser_major_version (5)
:browser_minor_version (0)
```

These expressions are ANDed. If the version of Internet Explorer is 5 AND the minor version is 0 (i.e. version 5.0), then the result is true, otherwise it is false. If the version of Internet Explorer is, for example, 4.0, then the first expression is false and the second one is true, and the result of both of them is false.

Sometimes, some expressions can influence the way in which others are evaluated. For example:

```
:browser_major_version (5)
:browser_minor_version (0)
:browser_version_operand (">=")
```

These expressions are ANDed, but the third expression influences the way that the first and second ones are evaluated. In the example above, if the version of Internet Explorer is greater than or equal to (">=") 5.0, then the result is true, otherwise it is false. If the version of Internet Explorer is, for example, 4.5, then the result is false, if the version is 5.1 or higher than the result is true.

Logical Sections

As mentioned earlier, subsequent expressions are automatically ANDed. However, sometimes it is necessary to perform a logical OR between expressions, instead of logical AND. This is done by using labels:

The **begin_or (orX)** label - this label starts a section containing several expressions. The end of this section is marked by a **end (orX)** label (**X** should be replaced with a number which differentiates between different sections OR sections). All of expressions inside this section are logically ORed, producing a single value for the section. For example:

```
:begin_or(or1)
:browser_major_version (5)
:browser_major_version (6)
:end(or1)
```

This section checks whether the version of Internet Explorer is 5 OR 6 - if it is then the result is true, otherwise it is false.

The **begin_and (andX)** label - this label is similar to the **begin_or (orX)** label, but the expressions inside are evaluated and logically ANDed. The end of this section is marked by a **end (andX)** or the **end (orX)** label. As mentioned earlier, simple subsequent expressions are automatically ANDed. The reason that this label exists is to allow nested ANDed sections inside ORed sections. For example, if an administrator considers old browsers as secure since they do not have a lot of potentially unsafe components, and new browsers as secure, since they contain all the latest security patches, he can define the following SCV rules:

```
:begin_or (or1)
:begin_and (and1)
:browser_major_version (5)
:browser_minor_version (0)
:browser_version_operand (">=")
:end (and1)
:begin_and (and2)
:browser_major_version (3)
:browser_minor_version (0)
:browser_version_operand ("<=")
:end (and2)
:end (or1)
```

In the example above, the first AND section checks whether the version of IE ≥ 5.0 , the second AND section checks whether the version of IE is ≤ 3.0 and they are ORed. The entire example is evaluated as true only if the version of IE is larger than (or equal to) 5.0 OR lower than (or equal to) 3.0.

Expressions and Labels with Special Meanings

There are several expressions and labels which have special meaning:

- **begin_admin (admin)** - this label starts a section defining several actions which are performed only if the client is considered as non-SCVed by previous expressions in the subset (i.e. if previous expressions in the subset have returned a value of false). The end of this section is marked by the **end (admin)** label.
- **send_log (type)** - This expression is used as part of the **begin_admin (admin) - end (admin)** section, and determines whether to send a log to the Security Management server (and the client's diagnostic tool) specifying that the client is not SCVed.

The word **type** should be replaced by the type of log to send, such as **log/alert**. Alert means sending a log to the Security Management server, while log means sending the log to the remote client's diagnostic tool.

- **mismatchmessage ("Message")** - This expression is used as part of the **begin_admin (admin) - end (admin)** section, and specifies that a popup message should be shown on the remote user's desktop, indicating the problem. The text in the inverted commas (**Message**) should be replaced by a meaningful text which should instruct the client about the possible sources of the problem and the action he should perform.

For example:

```
:browser_major_version (5)
:browser_minor_version (0)
:browser_version_operand (">=")
:begin_admin (admin)
:send_log (alert)
:mismatchmessage ("The version of your Internet Explorer
browser is old. For security reasons, users with old
browsers are not allowed to access the local area network
of the organization. Please upgrade your Internet Explorer
to version 5.0 or higher. If you require assistance in
upgrading or additional information on the subject, please
contact your network administrator")
:end (admin)
```

In this example, if the user's IE browser's version is lower than 5.0, an alert is sent to the Security Management server machine and a popup message is shown to the user with indication of the problem.

The local.scv Sets

The **local.scv** policy file contains one set called SCVObject. This set must always be present and contains all the subsets which deal with the SCV checks and parameters. Currently SCVObject has 3 subsets:

- **SCVNames** - This section is the main SCV policy definition section, in which all of the SCV checks and actions are defined. This is the definition part of the SCV policy, and doesn't actually determine the SCV checks that will be performed. In this section sets of tests are defined. Later on, the administrator will choose from these sets those he wants to run on the user's desktop.
- **SCVPolicy** - This section specifies the names of the SCV checks that should actually be performed on the client's machine, from the SCV checks defined in **SCVNames**.
- **SCVGlobalParams** - This section contains some global SCV parameters.

SCVNames

In this section the administrator specifies the names and different checks for the SCV products. Here is a general definition of an SCV check subset of SCVNames:

```
: (SCVCheckName1
    :type (plugin)
    :parameters (
        :Expression1 (value)
        :Expression2 (value)
        :begin_admin (admin)
        :send_log (alert)
        :mismatchmessage ("Failure Message")
        :end (admin)
    )
)
```

The test section begins with the name of the SCV check (SCVCheckName1). SCVCheckName1 defines the name of the set of tests. It is defined in the SCV application and should be provided by the SCV manufacturer. The **type (plugin)** expression specifies that the test is performed by an SCV DLL plugin. The **parameters** subset is where the SCV rules and actions are defined. The **type (plugin)** expression and the **parameters** subset should always be specified when defining a subset of SCV checks (such as SCVCheckName1).

SCVPolicy

This section defines the names of the SCV checks that should be enforced (the names are part of the SCV check names specified in SCVNames). This section's general structure is:

```
:SCVPolicy (
    : (SCVCheckName1)
    : (SCVCheckName2)
)
```

Note - there is a space between the colon (:) and the opening brace.

The Difference between SCVNames and SCVPolicy

- The SCVNames section defines the different parameters for the checks.
- The SCVPolicy section states which checks are enforced.

To enforce a specific SCV check:

- Set the check's parameters in SCVNames.
- Include the name of the check in SCVPolicy.

SCVGlobalParams

This section includes global parameters for SCV.

```
:SCVGlobalParams (
    :enable_status_notifications (true)
    :status_notifications_timeout (10)
    :disconnect_when_not_verified (false)
    :block_connections_on_unverified (false)
    :scv_policy_timeout_hours (24)
    :enforce_ip_forwarding (true)
    :not_verified_script ("myscript.bat")
    :not_verified_script_run_show (true)
    :not_verified_script_run_admin (false)
    :not_verified_script_run_always (false)
    :allow_non_scv_clients (false)
    :block_scv_client_connections (false)
)
```

A Complete Example of a local.scv File

Following is a complete example of a **local.scv** file.

Note that in the following example the internal syntax of some of the SCV subsets differs from the syntax described earlier. SCV policy syntax has evolved in recent versions, while these SCV checks were written

using the old syntax. For example, in the **sc_ver_scv** subset, the **begin_admin (admin) - end (admin)** section does not exist. In addition, the **mismatchmessage** expression which was in this section is replaced with **MismatchMessage** (using capital letters) expression. The syntax and operation of **MismatchMessage** is similar to the one specified for **mismatchmessage**, although it does not appear in a **begin_admin (admin) - end (admin)** section.

Another difference in the **sc_ver_scv** subset compared to the syntax explained above concerns the **EnforceBuild_XX_Operand** and **SecureClient_XX_BuildNumber** expressions. These expressions are not ANDed but rather evaluated automatically in accordance with the operating system the user has. For example, if the user has a Windows 2000 system, only the **EnforceBuild_2K_Operand** and **SecureClient_2K_BuildNumber** expressions are evaluated, and the expressions relating to different operating systems are not.

Some other minor changes from the described syntax appear in the **local.scv** policy file. You can review the changes in the default **local.scv** policy file. In general, you can use the pre-defined checks (in the **SCVNames** section) as templates and list the modified checks in the **SCVPolicy** section, without writing new SCV subsets.



Note - To enforce a specific SCV check, set the parameters of the check in the **SCVNames** section, and include the name of the check in **SCVPolicy**.

Sample

```
(SCVObject
  :SCVNames (
    : (user_policy_scv
      :type (plugin)
      :parameters (
        )
      )
    : (BrowserMonitor
      :type (plugin)
      :parameters (
        :browser_major_version (5)
        :browser_minor_version (0)
        :browser_version_operand (">=")
        :browser_version_mismatchmessage ("Please upgrade your
Internet browser.")
        :intranet_download_signed_activex (disable)
        :intranet_run_activex (disable)
        :intranet_download_files (disable)
        :intranet_java_permissions (disable)
        :trusted_download_signed_activex (disable)
        :trusted_run_activex (disable)
        :trusted_download_files (disable)
        :trusted_java_permissions (disable)
        :internet_download_signed_activex (disable)
        :internet_run_activex (disable)
        :internet_download_files (disable)
      )
    )
  )
)
```

```

:internet_java_permissions (disable)
:restricted_download_signed_activex (disable)
:restricted_run_activex (disable)
:restricted_download_files (disable)
:restricted_java_permissions (disable)
:send_log (alert)
:internet_options_mismatch_message ("Your Internet browser
settings do not meet policy requirements\nPlease check the following
settings:\n1. In your browser, go to Tools -> Internet Options -> Security.\n2.
For each Web content zone, select custom level and disable the following items:
DownLoad signed ActiveX, Run ActiveX Controls, Download Files and Java
Permissions.")
)
)
: (OsMonitor
:type (plugin)
:parameters (
:os_version_mismatchmessage ("Please upgrade your operating
system.")
:enforce_screen_saver_minutes_to_activate (3)
:screen_saver_mismatchmessage ("Your screen saver settings do
not meet policy requirements\nPlease check the following settings:\n1. Right
click on your desktop and select properties.\n2. Select the Screen Saver
tab.\n3. Under Wait choose 3 minutes and check the Password Protection box.")
:send_log (log)
:major_os_version_number_9x (4)
:minor_os_version_number_9x (10)
:os_version_operand_9x (">=")
:service_pack_major_version_number_9x (0)
:service_pack_minor_version_number_9x (0)
:service_pack_version_operand_9x (">=")
:major_os_version_number_nt (4)
:minor_os_version_number_nt (0)
:os_version_operand_nt ("==")
:service_pack_major_version_number_nt (5)
:service_pack_minor_version_number_nt (0)
:service_pack_version_operand_nt (">=")
:major_os_version_number_2k (5)
:minor_os_version_number_2k (0)
:os_version_operand_2k ("==")
:service_pack_major_version_number_2k (0)
:service_pack_minor_version_number_2k (0)
:service_pack_version_operand_2k (">=")
:major_os_version_number_xp (5)
:minor_os_version_number_xp (1)
:os_version_operand_xp ("==")

```

```

        :service_pack_major_version_number_xp (0)
        :service_pack_minor_version_number_xp (0)
        :service_pack_version_operand_xp (">=")
    )
)
: (ProcessMonitor
    :type (plugin)
    :parameters (
        :begin_or (or1)
            :AntiVirus1.exe (true)
            :AntiVirus2.exe (true)
        :end (or1)
        :IntrusionMonitor.exe (true)
        :ShareMyFiles.exe (false)
        :begin_admin (admin)
            :send_log (alert)
            :mismatchmessage ("Please check that the following
processes are running:\n1. AntiVirus1.exe or AntiVirus2.exe\n2.
IntrusionMonitor.exe\n\nPlease check that the following process is not
running\n1. ShareMyFiles.exe")
        :end (admin)
    )
)
: (groupmonitor
    :type (plugin)
    :parameters (
        :begin_or (or1)
            :begin_and (1)
                : "builtin\administrator" (false)
                : "BUILTIN\Users" (true)
            :end (1)
            :begin_and (2)
                : "builtin\administrator" (true)
                : "BUILTIN\Users" (false)
            :end (and2)
        :end (or1)
        :begin_admin (admin)
            :send_log (alert)
            :mismatchmessage ("You are using SecureClient with a
non-authorized user.\nMake sure you are logged on as an authorized user.")
            :securely_configured_no_active_user (false)
        :end (admin)
    )
)

```

```

: (HotFixMonitor
  :type (plugin)
  :parameters (
    :147222 (true)
    :begin_admin (admin)
    :send_log (alert)
    :mismatchmessage ("Please install security patch
Q147222.")
  :end (admin)
)
)
: (AntiVirusMonitor
  :type (plugin)
  :parameters (
    :type ("Norton")
    :Signature (">=20020819")
    :begin_admin (admin)
    :send_log (alert)
    :mismatchmessage ("Please update your AntiVirus (use
the LiveUpdate option).")
  :end (admin)
)
)
: (HWMonitor
  :type (plugin)
  :parameters (
    :cputype ("GenuineIntel")
    :cpumodel ("9")
    :cpufamily ("6")
    :begin_admin (admin)
    :send_log (alert)
    :mismatchmessage ("Your machine must have an\nIntel(R)
Centrino(TM) processor installed.")
  :end (admin)
)
)
: (ScriptRun
  :type (plugin)
  :parameters (
    :exe ("VerifyScript.bat")
    :begin_admin (admin)
    :send_log (alert)
    :mismatchmessage ("Verification script has determined
that your configuration does not meet policy requirements.")

```

```

        :end (admin)
    )
)
: (RegMonitor
    :type (plugin)
    :parameters (
        :value ("Software\TrendMicro\PC-
cillinNTCorp\CurrentVersion\Misc.\PatternVer>=414")
        :begin_admin (admin)
        :send_log (alert)
        :mismatchmessage ("Please update your AntiVirus (use
the LiveUpdate option).")
        :end (admin)
    )
)
: (SCVMonitor
    :type (plugin)
    :parameters (
        :scv_version ("54014")
        :begin_admin (admin)
        :send_log (alert)
        :mismatchmessage ("Please upgrade your Secure
Configuration Verification products package.")
        :end (admin)
    )
)
: (sc_ver_scv
    :type (plugin)
    :parameters (
        :Default_SecureClientBuildNumber (52032)
        :Default_EnforceBuildOperand ("==")
        :MismatchMessage ("Please upgrade your SecureClient.")
        :EnforceBuild_9X_Operand (">=")
        :SecureClient_9X_BuildNumber (52030)
        :EnforceBuild_NT_Operand ("==")
        :SecureClient_NT_BuildNumber (52032)
        :EnforceBuild_2K_Operand (">=")
        :SecureClient_2K_BuildNumber (52032)
        :EnforceBuild_XP_Operand (">=")
        :SecureClient_XP_BuildNumber (52032)
    )
)
)
:SCVPolicy (

```



```

: (BrowserMonitor)
: (HWMonitor)
: (AntiVirusMonitor)
)
:SCVGlobalParams (
:enable_status_notifications (false)
:status_notifications_timeout (10)
:disconnect_when_not_verified (false)
:block_connections_on_unverified (false)
:scv_policy_timeout_hours (24)
:enforce_ip_forwarding (true)
:not_verified_script (")
:not_verified_script_run_show (false)
:not_verified_script_run_admin (false)
:not_verified_script_run_always (false)
:not_verified_script_run_always (false)
:allow_non_scv_clients (false)
)

```

When using this file, it is important to maintain the same indentation/nesting format.

Common Attributes

Typically, an administrator might need to change only a few of the common parameters (SCV checks) contained in the SCV policy file.

SCV Checks

Anti-Virus monitor

Parameters:

- Type ("av_type")

Type of Anti-Virus. For example, "Norton", "VirusScan", "OfficeScan", or "ZoneLabs".

- Signature(x)

Required Virus definition file signature. The signature's format depends on the AntiVirus type. For example, on Norton Antivirus the signature maybe be ">=20031020". (The format for Norton's AV signature is "yyyymmdd").

For TrendMicro Officescan, the signature maybe "<650"

For McAfee's VirusScan, use signature (">404291") for a signature greater than 4.0.4291

For Zone Labs, use signature (">X.Y.Z") where X = Major Version, Y = Minor Version, and Z = Build Number of the .dat signature file.

AntiVirusMonitor does not support "begin_or" and the "begin_and" syntax. See: Expressions and Labels with Special Meanings (on page [201](#)).

BrowserMonitor

Parameters:

- browser_major_version (5)

Major version number of Internet Explorer. If this field does not exist in the local.scv file, or if this value is 0, the IE'S version will not be checked as part of the BrowserMonitor check.

- browser_minor_version (0)

Internet Explorer's minor version number.

- `browser_version_operand (">=")`

The operator used for checking the Internet Explorer's version number.

- `browser_version_mismatchmessage ("Please upgrade your Internet Browser.")`

Message to be displayed in case of a non-verified configuration for the Internet Explorer's version.

- `intranet_download_signed_activex (enable)`

The maximum permission level that IE should have for downloading signed ActiveX controls from within the local Intranet.

- `intranet_run_activex (enable)`

The maximum permission level that IE should have for running signed ActiveX controls from within the local Intranet.

- `intranet_download_files (enable)`

The maximum permission level that IE should have for downloading files from within the local Intranet.

- `intranet_java_permissions (low)`

The maximum security level that IE Explorer should have for running java applets from within the local Intranet.

(low) means a low security level.

- `trusted_download_signed_activex (enable)`

The maximum permission level that IE should have for downloading signed ActiveX controls from trusted zones.

- `trusted_run_activex (enable)`

The maximum permission level that IE should have for running signed ActiveX controls from trusted zones.

- `trusted_download_files (enable)`

The maximum permission level that IE should have for downloading files from trusted zones.

- `trusted_java_permissions (medium)`

The maximum security level that IE should have for running java applets from trusted zones.

- `internet_download_signed_activex (disable)`

The maximum permission level that IE should have for downloading signed ActiveX controls from the Internet.

- `Internet_run_activex (disable)`

The maximum permission level that IE should have for running signed ActiveX controls from the Internet.

- `internet_download_files (disable)`

The maximum permission level that IE should have for downloading files from the Internet.

- `internet_java_permissions (disable)`

The maximum security level that IE should have for running java applets from the Internet.

- `restricted_download_signed_activex (disable)`

The maximum permission level that IE should have for downloading signed ActiveX controls from restricted zones.

- `restricted_run_activex (disable)`

The maximum permission level that IE should have for running signed ActiveX controls from restricted zones.

- `restricted_download_files` (disable)
The maximum permission level that IE should have for downloading files from restricted zones.
- `restricted_java_permissions` (disable)
The maximum security level that IE should have for running java applets from restricted zones.
- `send_log` (type)
Determines whether to send a log to Security Management server for specifying that the client is not “SCVed.”

This SCV check does not support the “begin admin/end admin” parameter section.

The (type) section should be replaced by (log) or (alert)

- `internet_options_mismatch_message` (“Your Internet browser settings do not meet policy requirements”)

Mismatch message for the Internet Explorer settings.

BrowserMonitor can be configured to check only Internet Explorer’s version, or only the browser’s settings for a certain zone. For example, if none of the following parameters appear:

- `restricted_download_signed_activex`
- `restricted_run_activex`
- `restricted_download_files`
- `restricted_java_permissions`

then **BrowserMonitor** will not check the restricted zones’ security settings. In similar fashion, if the parameter “browser_major_version” does not appear or is equal to zero, then IE’s version number is not checked.

BrowserMonitor does not support the “begin_or” and the “begin_and” syntax, and does not support the admin parameters. See also: Expressions and Labels with Special Meanings (on page 201).

For the script for checking Internet Explorer Service Pack, see Script for Internet Explorer Service Pack below.

Groupmonitor

Parameters

- `“builtin\administrator”` (false)
A name of a user group. The user has to belong to this group in order for the machine configuration to be verified.
- `securely_configured_no_active_user` (true)
Specifies whether the machine’s configuration may be considered verified when no user is logged on. The default value is false.

HotFixMonitor

Parameters

- `HotFix_Number` (true)
A number of a system HotFix to be checked. In order for the machine to be verified, the HotFix should be installed, for example: “823980(true)” verifies that Microsoft’s RPC patch is installed on the operating system.
- `HotFix_Name` (true)
The full name of a system HotFix to be checked. In order for the machine to be verified, the HotFix should be installed, for example: “KB823980(true)” verifies that Microsoft’s RPC patch is installed on the operating system.

Not all the mentioned fields for **HotFixMonitor** need to appear in the local.scv file. Some of them may not appear at all, or may appear more than once. These fields may also be ORed and ANDed. In this way, multiple HotFixes can be checked, and the results ORed or ANDed for extra flexibility.

HWMonitor

Parameters

- `cputype` ("GenuineIntel")
The CPU type as described in the vendor ID string. The string has to be exactly 12 characters long. For example: "GenuineIntel", or "AuthenticAMD", or "aaa bbb ccc " where spaces count as a character.
- `cpufamily`(6)
The CPU family.
- `cpumodel`(9)
The CPU model.

HWMonitor does not support the "begin_or" and the "begin_and" syntax. See also: Expressions and Labels with Special Meanings (on page 201).

OsMonitor

Parameters

- `enforce_screen_saver_minutes_to_activate` (3)
Time in minutes for the screen saver to activate. If the screen saver does not activate within this time period, then the client is not considered verified. In addition, the screen saver must be password protected.
- `screen_saver_mismatchmessage` ("Your screen saver settings do not meet policy requirements")
Mismatch message for the screen saver check. The screen saver will not be checked if the property "enforce_screen_saver_minutes_to_activate" does not appear, or if the time is set to zero.
- `send_log` (type)
Determines whether to send a log to Security Management server for specifying that the client is not "SCVed."
This SCV check does not support the "begin admin/end admin" parameter section.
The (type) section should be replaced by (log) or (alert)
- `major_os_version_number_9x` (4)
Specifies the major version required for 9x operating systems to be verified.
- `minor_os_version_number_9x` (10)
Specifies the minor version required for 9x operating systems to be verified.
- `os_version_operand_9x` (">=")
Operator for checking the operating system's version on 9x.
- `service_pack_major_version_number_9x` (0)
Specifies the major service pack's version required for 9x operating system's to be verified.
- `service_pack_minor_version_number_9x` (0)
Specifies the minor service pack's version required for 9x operating systems to be verified.
- `service_pack_version_operand_9x` (">=")
Operator for checking the operating system's service pack on 9x.
- `major_os_version_number_nt` (4)
Specifies the major version required for Windows NT operating systems to be verified.
- `minor_os_version_number_nt` (10)
Specifies the minor version required for Windows NT operating systems to be verified.
- `os_version_operand_nt` (">=")
Operator for checking the operating system's version on Windows NT.

- `service_pack_major_version_number_nt (0)`
Major service pack version required for Windows NT operating systems to be verified
- `service_pack_minor_version_number_nt (0)`
Minor service pack version required for Windows NT operating systems to be verified
- `service_pack_version_operand_nt (">=")`
Operator for checking the operating system's service pack on Windows NT
- `major_os_version_number_2k (4)`
Specifies the major version required for Windows 2000 operating systems to be verified.
- `minor_os_version_number_2k (10)`
Specifies the minor version required for Windows 2000 operating systems to be verified.
- `os_version_operand_2k (">=")`
Operator for checking the operating system's version on Windows 2000
- `service_pack_major_version_number_2k (0)`
Specifies major service pack version required for Windows 2000 operating systems to be verified.
- `service_pack_minor_version_number_2k (0)`
Specifies minor service pack version required for Windows 2000 operating systems to be verified.
- `service_pack_version_operand_2k (">=")`
Operator for checking the operating system's service pack on Windows 2000
- `major_os_version_number_xp (4)`
Specifies the major version required for Windows XP operating systems to be verified.
- `minor_os_version_number_xp (10)`
Specifies the minor version required for Windows XP operating systems to be verified.
- `os_version_operand_xp (">=")`
Operator for checking the operating system's service pack on Windows XP
- `service_pack_major_version_number_xp (0)`
Specifies the major service pack version required for Windows XP operating systems to be verified.
- `service_pack_minor_version_number_xp (0)`
Specifies the minor service pack version required for Windows XP operating systems to be verified.
- `service_pack_version_operand_xp (">=")`
Operator for checking the operating system's service pack on Windows XP.
- `os_version_mismatches ("Please upgrade your operating system")`
Message to be displayed in case of a non-verified configuration for the operating system's version/service pack. The operating system's version and service pack will not be checked if none of the parameters appear in the scv file.
- `:major_os_version_number_2003 (5)`
Specifies the major version required for Windows 2003 operating systems to be verified.
- `:minor_os_version_number_2003 (2)`
Specifies the minor version required for Windows 2003 operating systems to be verified.
- `:os_version_operand_2003 ("==")`
Operator for checking the operating system's service pack on Windows 2003
- `:service_pack_major_version_number_2003 (0)`

Specifies the major service pack version required for Windows 2003 operating systems to be verified.

- `:service_pack_minor_version_number_2003 (0)`

Specifies the minor service pack version required for Windows 2003 operating systems to be verified.

- `:service_pack_version_operand_2003 (">=")`

Operator for checking the operating system's service pack on Windows 2003

OsMonitor can be configured to check only the screen saver's configuration, or only the operating system's version and service pack. For example, if none of the following parameters appear:

- `major_os_version_number_xp`
- `minor_os_version_number_xp`
- `os_version_operand_xp`
- `service_pack_major_version_number_xp`
- `service_pack_minor_version_number_xp`
- `service_pack_version_operand_xp`

then **OsMonitor** will not check the system's version and service pack on Windows XP platforms.

Similarly, if the parameter "enforce_screen_saver_minutes_to_activate" does not appear, then the screen saver's configuration is not checked.

OSMonitor does not support the "begin_or" and the "begin_and" syntax. See also: Expressions and Labels with Special Meanings (on page 201).

ProcessMonitor

Parameters

- `ProcessName.exe (true)`

A process the administrator would like to check. If the value is true, the process needs to be running for the machine to be verified. If the value is false, the process should not be running for the machine to be verified.

ProcessMonitor can also be used to check for the existence/exclusion of more than one process. The fields may be ANDed or ORed for flexibility.

RegMonitor

Parameters

- `PredefinedKeys (HIVE)`

Specify the registry hive from one of the following choices:

- `HKEY_CURRENT_USER`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`

If one of the hives is not specified, then `HKEY_LOCAL_MACHINE` is used.

To configure a check for `HKEY_CLASSES_ROOT`, use `HKEY_LOCAL_MACHINE\Software\Classes` and `HKEY_CURRENT_USER\Software\Classes`.

- `value (registry_value_path)`

The path of a registry `DWORD`, under the hive specified by the predefined keys will be checked. The value should be an operator followed by a number, e.g. "Software\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.\PatternVer>=414"

The syntax for the value parameter is:

```
:value ("pathOPval")
```

For example:

```
:value ("Software\...\PaternVer>=414")
```

- `string (registry_string_path)`

The path of a registry string, under the hive specified by the predefined keys will be checked. The string's value is compared to the given value, in the way that DWORDs are compared.

- `keyexist (registry_key_path)`

The path of a registry key to check if the key exists, under the hive specified by the predefined keys will be checked. The key must exist if the machine is to be verified.

- `keynexist (registry_key_path)`

The path of a registry key to be checked for exclusion, under the hive specified by the predefined keys will be checked. For the machine to be verified, the key should not exist.

- `allow_no_user (default: true)`

This parameter is valid only when a user is logged in to the machine.

Since SC services and SCV checks run also when no user is logged on, a decision should be taken if the check passed or failed.

If no user is logged on to the machine, and a running RegMonitor check is configured to monitor `HKEY_CURRENT_USER`, the behavior is according to the flag `allow_no_user`.

If `allow_no_user` is true, the check will PASS.

If `allow_no_user` is false, the check will FAIL.

This attribute is not, by default, included in the `local.scv` file. If the attribute does not exist in the file, then the default setting used is also true.

Configuring this attribute is done via `local.scv`. For example:

```
: (RegMonitor
    :type (plugin)
    :parameters (
        :keyexist
        ("HKEY_CURRENT_USER\Software\CheckPoint")
        :allow_no_user (true)
        :begin_admin (admin)
        :send_log (alert)
        :mismatchmessage ("mismatch
message ")
        :end (admin)
    )
)
```

Not all the mentioned fields for **RegMonitor** need to appear in the `local.scv` file. Some of them may not appear at all, or may appear more than once. These fields may also be ORed and ANDed. In this way, multiple registry entries can be checked, and the results ORed or ANDed for extra flexibility.

Script for Internet Explorer Service Pack

RegMonitor can be configured to check the version and service pack of Internet Explorer. The script looks as follows:

```
: (RegMonitor
    :type (plugin)
    :parameters (
        :begin_or (or1)
        :keynexist
        ("Software\Microsoft\Internet Explorer")
        :string
        ("Software\Microsoft\Internet Explorer\Version>=6")
        :begin_and (and1)
        :string
        ("Software\Microsoft\Internet Explorer\Version>=5.5")
        :string
        ("Software\Microsoft\Windows\CurrentVersion\Internet
```

```

Settings\MinorVersion>=SP2")
                                :string
("Software\Microsoft\Windows\CurrentVersion\Internet
Settings\MinorVersion<=SP9")
                                :end_and (and1)
                                :begin_and (and2)
                                :string
("Software\Microsoft\Internet Explorer\Version>=5.5")
                                :string
("Software\Microsoft\Windows\CurrentVersion\Internet
Settings\MinorVersion>=;SP2")
                                :string
("Software\Microsoft\Windows\CurrentVersion\Internet
Settings\MinorVersion<=;SP9")
                                :end_and (and2)
:and_or (or1)
                                :begin_admin (admin)
                                :send_log (alert)
                                :mismatchmessage
("Your IE must be at least version 5.5 with SP2.")
                                :end (admin)
)
)

```

SCVMonitor

Parameters

- `scv_version(">=541000076")`

Represents the SCV product's build number. This is the version of the DLLs in charge of the SCV checks. This number differs from the build number of SecureClient. SCV products can be upgraded, and maybe updated without updating SecureClient.

The string is an operator followed by the DLL's version number in the format "vvshhhbbb". For example, if you want the DLL version to be at least 54.1.0.220, the syntax should be:

```
scv_version (">=541000220")
```

SCVMonitor does not support the "begin_or" and the "begin_and" syntax. See also: Expressions and Labels with Special Meanings (on page [201](#)).

ScriptRun

Parameters

- `exe ("VerifyScript.bat")`

Runs an executable. Supply the name of the executable, and the full path to the executable.

- `run_as_admin ("no")`

Determines whether the verification script is run with administrator privileges. The default is "no". The only other value is "yes".

- `run_timeout (10)`

Time (in seconds) to wait for the executable to finish. If the executable does not finish within the set time, the process is considered as a failure, and the machine categorized as "not verified". The default value is zero, which is the same as "no timeout".

ScriptRun does not support the "begin_or" and the "begin_and" syntax. See also: Expressions and Labels with Special Meanings (on page [201](#)).

sc_ver_scv

Parameters

- `Default_SecureClientBuildNumber (52032)`

Build number for SecureClient. This build number is checked (with the specified operator) only if no specific build number is to be checked for a particular platform.

- `Default_EnforceBuildOperand ("==")`

Operator for comparing the local.scv's build number with the client build number.

- `MismatchMessage ("Please upgrade your SecureClient")`

Mismatch message to be displayed when the SecureClient's build does not match the local.scv's configuration.

- `EnforceBuild_9x_Operand (">=")`

Operator for comparing the local.scv's build number with the client build number on Windows 9x platforms.

- `SecureClient_9x_BuildNumber (52030)`

SecureClient build number for windows 9x platforms.

- `EnforceBuild_NT_Operand ("==")`

Operator for comparing the local.scv's build number with the client build number on WindowsNT platforms.

- `SecureClient_NT_BuildNumber (52030)`

SecureClient build number for WindowsNT platforms.

- `EnforceBuild_2K_Operand (">=")`

Operator for comparing the local.scv's build number with the client build number on Windows 2000 platforms.

- `SecureClient_2K_BuildNumber (52030)`

SecureClient build number for Windows 2000 platforms.

- `EnforceBuild_XP_Operand (">=")`

Operator for comparing the local.scv's build number with the client build number on Windows XP platforms.

- `SecureClient_XP_Buildnumber (52030)`

SecureClient build number for Windows XP platforms.

sc_ver_scv does not support the "begin_or" and the "begin_and" syntax. See also: Expressions and Labels with Special Meanings (on page [201](#)).

user_policy_scv

Parameters

- `logged_on_to_policy_server (true/false)`

Specifies whether the user has to be logged on to a Policy Server to be considered SCVed.

- `policy_refresh_rate ("168")`

Time, in hours, for which the desktop policy remains valid. After 168 hours the desktop policy is not considered valid, and the user is no longer SCVed. If this parameter is not specified, the policy is not checked for freshness.

- `mismatchmessage ("Place a message here")`

The message displayed when the user_policy_scv check fails.

- `dont_enforce_while_connecting`

If this parameter is present, the user is considered SCVed while connecting to the Security Gateway. The user is considered SCVed only for the duration of the connect process.

SCVGlobalParams

Parameters

For all boolean parameters (true or false), the values should not be enclosed in quotation marks.

- `enable_status_notifications` (true/false)

If “true”, SecureClient displays a balloon window when the Desktop is not SCVed. On windows 9x and NT, where balloons are not supported, popups appear.

- `status_notifications_timeout` ()

The number of seconds the balloon window (see previous parameter) will be displayed.

- `disconnect_when_not_verified` (true/false)

If “true”, SecureClient will disconnect from the site when the Desktop is not SCVed.

- `block_connections_on_unverified` (true/false)

If “true”, SecureClient will drop all open connections when the Desktop is not SCVed.



Note - This parameter, if true, blocks all connections to the machine, not just those connections to and from the VPN site.

- `scv_policy_timeout_hours` ()

The period (in hours) during which the SCV policy is considered valid since the last logon to the Policy Server. When this timeout is about to expire SecureClient will attempt to logon to the Policy Server to get a new SCV policy.

Possible values are between 1 and 504 hours(21 days). The default value is 168 hours (one week). If you set the value to 0, the SCV policy never expires (no time-out).

- `enforce_ip_forwarding` (true/false)

If “true” the IP Forwarding between network interface cards on the user’s desktop must be disabled for the user to be considered SCVed.

- `ip_forwarding_mismatchmessage` (“Message string placed here”)

The value is a string displayed when ip forwarding is enabled. For example:
`ip_forwarding_mismatchmessage` (“Please....etc”)

This is relevant only if ip forwarding is part of the SCV checks, that is, if the parameter is defined as True.

- `not_verified_script` (“script_name.bat”)

The name of executable that will be run when the Desktop is not SCVed. The next three parameters provide more options related to the running of the executable.

- `not_verified_script_run_show` (true/false)

If “true”, the executable’s progress will be displayed in an onscreen window.

- `not_verified_script_run_admin` (true/false)

If “true”, the executable will run with administrator privileges.

- `not_verified_script_run_always` (true/false)

If “true”, the executable will run every time the Desktop is not SCVed. If “false”, it will run once per SecureClient session.

- `:allow_non_scv_clients` (true/false)

If “true”, the client will send a verified state to the enforcing Security Gateway even if the OS does not support SCV.

Chapter 24

VPN Routing - Remote Access

In This Chapter

| | |
|--|-----|
| The Need for VPN Routing | 219 |
| Check Point Solution for Greater Connectivity and Security | 219 |
| Configuring VPN Routing for Remote Access VPN | 222 |

The Need for VPN Routing

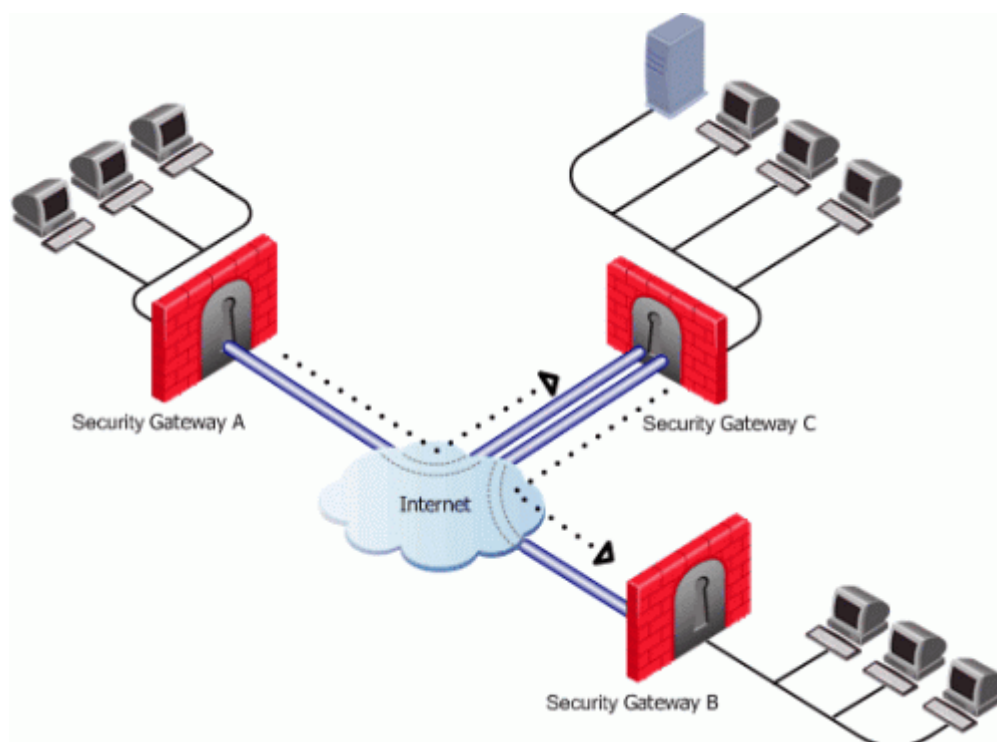
There are a number of scenarios in which a Security Gateway or remote access clients cannot connect directly to another Security Gateway (or clients). Sometimes, a given Security Gateway or client is incapable of supplying the required level of security. For example:

- Two Security Gateways with **dynamically assigned IP addresses** (DAIP Security Gateways). Hosts behind either Security Gateway need to communicate; however, the changing nature of the IP addresses means the two DAIP Security Gateways cannot open VPN tunnels. At the moment of tunnel creation, the exact IP address of the other is unknown.
- Remote access client users wish to have a private conversation using **Voice-over-IP** (VoIP) software or utilize other client-to-client communication software such as Microsoft NetMeeting. Remote access clients cannot open connections directly with each other, only with configured Security Gateways.

In all cases, a method is needed to enhance connectivity and security.

Check Point Solution for Greater Connectivity and Security

VPN routing provides a way of controlling how VPN traffic is directed. VPN routing can be implemented with Security Gateway modules and remote access clients. Configuration for VPN routing is performed either directly through SmartDashboard (in simple cases) or by editing the VPN routing configuration files on the Security Gateways (in more complex scenarios).



In the figure above, one of the host machines behind Security Gateway A needs to connect with a host machine behind Security Gateway B. For either technical or policy reasons, Security Gateway A cannot open a VPN tunnel with Security Gateway B. However, both Security Gateways A and B can open VPN tunnels with Security Gateway C, so the connection is routed through Security Gateway C.

As well as providing enhanced connectivity and security, VPN routing can ease network management by hiding a complex network of Security Gateways behind a single Hub.

Hub Mode (VPN Routing for Remote Clients)

VPN routing for remote access clients is enabled via Hub Mode. In Hub mode, all traffic is directed through a central Hub. The central Hub acts as a kind of router for the remote client. Once traffic from remote access clients is directed through a Hub, connectivity with other clients is possible as well as the ability to inspect the subsequent traffic for content.

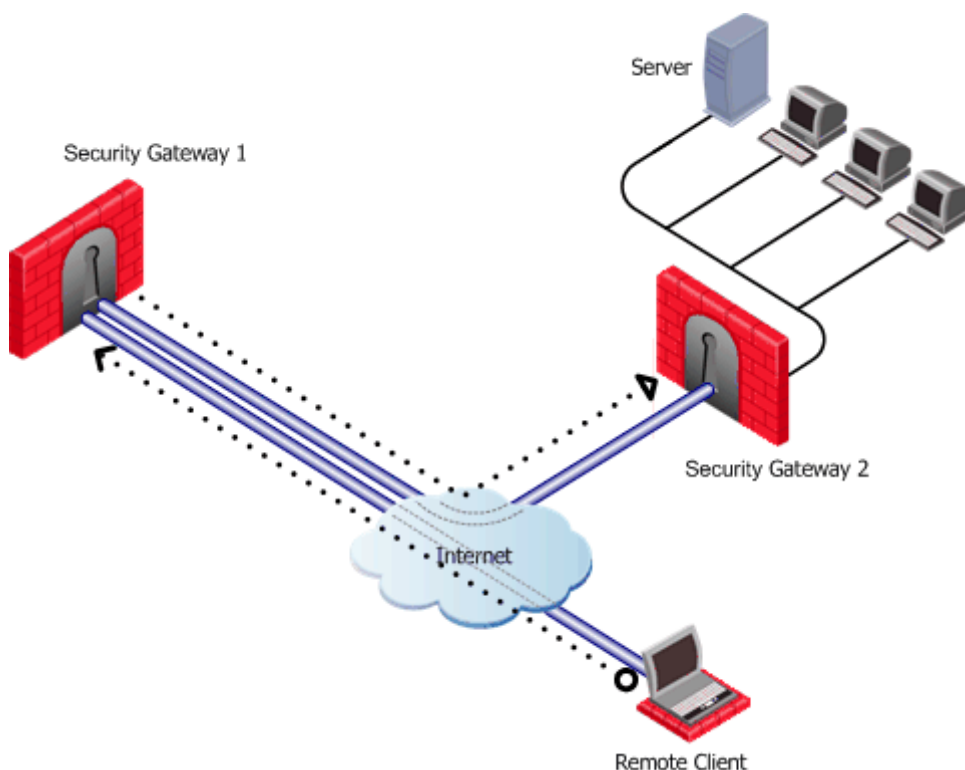
When using Hub mode, enable Office mode. If the remote client is using an IP address supplied by an ISP, this address might not be fully routable. When Office mode is used, rules can be created that relate directly to Office mode connections.



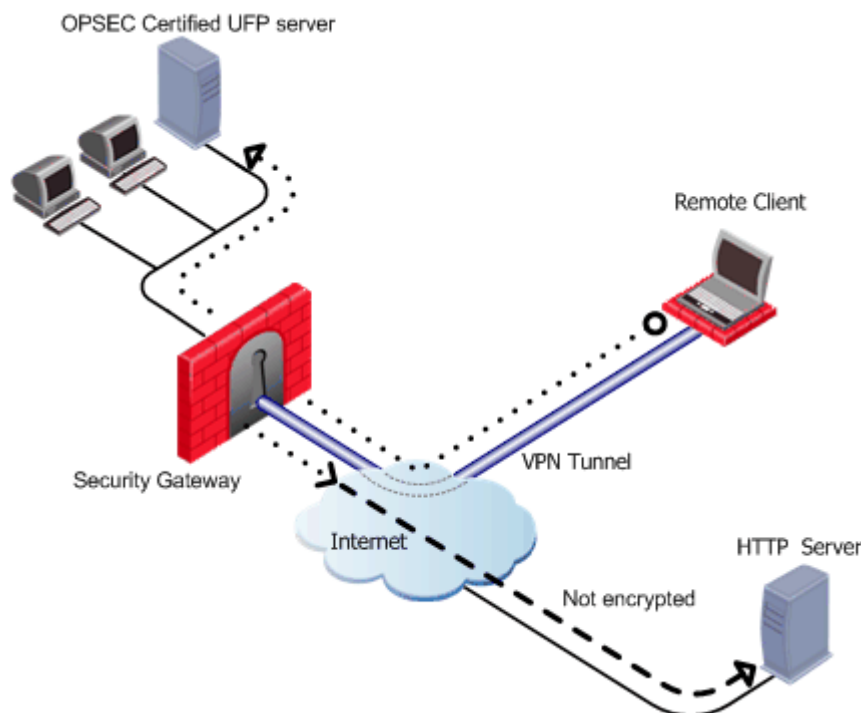
Note - Office mode is not supported in SecuRemote.

Allowing Clients to Route all Traffic Through a Security Gateway

In the following figure, the remote client needs to connect with a server behind Security Gateway 2. Company policy states that all connections to this server must be inspected for content. For whatever reason, Security Gateway 2 cannot perform the required content inspection. When all the traffic is routed through Security Gateway 1, connections between the remote client and the server can be inspected.



Suppose the same remote client needs to access an HTTP server on the Internet. The same company policy regarding security still applies.



The remote client's traffic is directed to the Security Gateway where it is directed to the UFP (URL Filtering Protocol) server to check the validity of the URL and packet content, since the Security Gateway does not possess URL-checking functionality. The packets are then forwarded to the HTTP server on the Internet.

NATing the address of the remote client behind the Security Gateway prevents the HTTP server on the Internet from replying directly to the client. If the remote client's address is not NATed, the remote client will not accept the clear reply from the HTTP server.

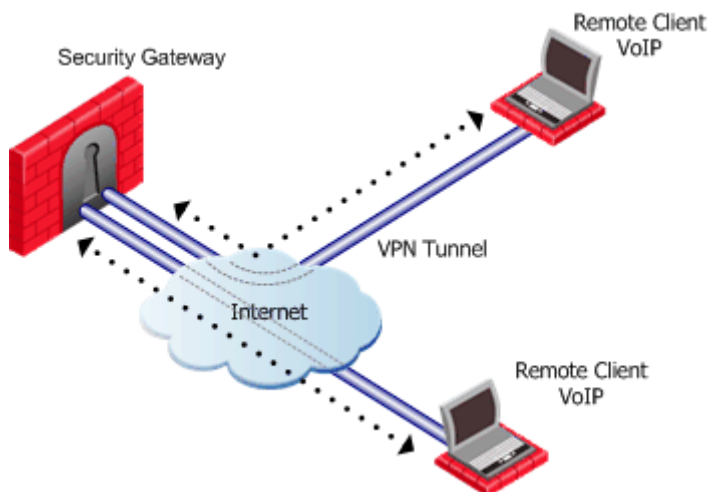
Remote Client to Client Communication

Remote client to client connectivity is achieved in two ways:

- By routing all the traffic through the Security Gateway.
- Including the Office Mode range of addresses in the VPN domain of the Security Gateway.

Routing all Traffic through the Security Gateway

Two remote users use VoIP software to hold a secure conversation. The traffic between them is directed through a central Hub, as shown in the following figure.

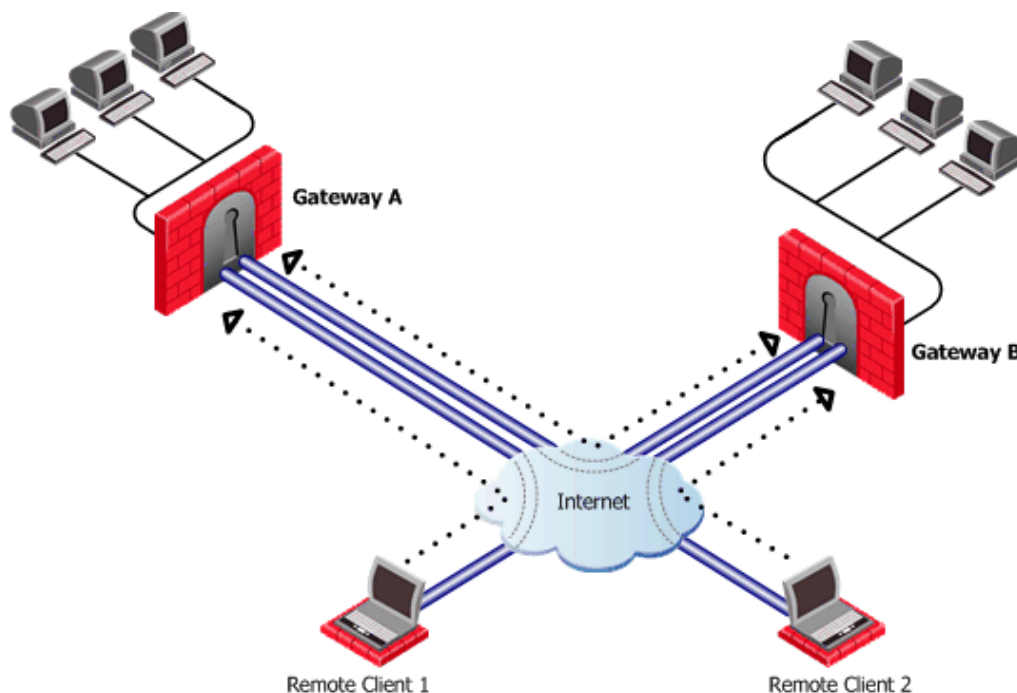


For this to work:

- **Allow VPN clients to route traffic through this gateway** must be enabled on the Security Gateway.

- The remote client must be configured with a profile that enables all traffic to be routed through the Security Gateway.
- Remote clients are working in connect mode.

If the two remote clients are configured for Hub mode with different Security Gateways, the routing takes place in three stages - each remote client to its designated Security Gateway, then between the Security Gateways:



In the figure above, remote client 1 is configured for Hub mode with Security Gateway A. Remote client 2 is configured for Hub mode with Security Gateway B. For the connection to be routed correctly:

- Office mode *must* be enabled.
- VPN configuration files on both Security Gateways must include the Office Mode address range used by the other. In Figure 24-5, the VPN configuration file on Security Gateway A directs all traffic aimed at an Office Mode IP address of Security Gateway B towards Security Gateway B. A connection leaves Remote Client1 and is sent to Security Gateway A. From gateway A the connection is redirected to Security Gateway B. Security Gateway B once more redirects the traffic towards Remote Client2. The reply from Remote Client2 follows the same path but in reverse.
- Office mode addresses used by both Security Gateways must be non-overlapping.

Configuring VPN Routing for Remote Access VPN

Common VPN routing scenarios can be configured through a VPN star community, but not all VPN routing configuration is handled through SmartDashboard. VPN routing between Security Gateways (star or mesh) can be also be configured by editing the configuration file `$FWDIR/conf/vpn_route.conf`.

VPN routing cannot be configured between Security Gateways that do not belong to a VPN community.

Enabling Hub Mode for Remote Access clients

1. On the **Remote Access** page of the **Security Gateway properties** window, **Hub Mode configuration** section, select **Allow SecureClient to route all traffic through this Security Gateway**.
2. On the Properties window of the **Remote Access** community, **Participating Security Gateways** page, set the Security Gateway that functions as the "Hub".
3. On the **Participant User Groups** page, select the remote clients.
4. Create an appropriate access control rule in the Security Policy Rule Base. VPN routing traffic is handled in the Security Policy Rule Base as a single connection, matched to *one rule only*.
5. Configure the profile on the remote client to route all communication through the designated Security Gateway.

Configuration of Client to Client Routing by Including the Office Mode Range of Addresses in the VPN Domain of the Security Gateway

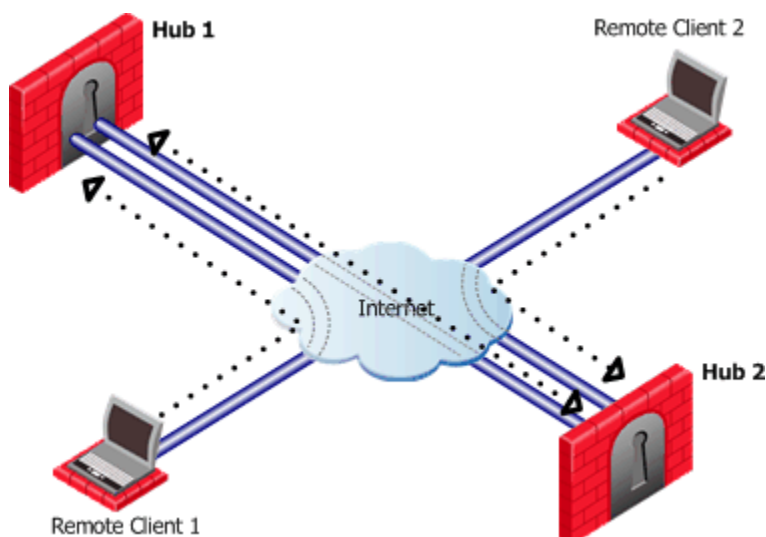
To configure VPN routing for remote access clients via the VPN domain, add the Office mode range of addresses to the VPN domain of the Security Gateway:

1. In SmartDashboard, create an address range object for the Office Mode addresses.
2. Create a group that contains both the VPN domain and Office mode range.
3. On the **General properties** window of the Security Gateway object > **Topology** page > **VPN domain** section, select **Manually defined**.
4. Select the group that contains both the VPN domain of the Security Gateway and the Office mode addresses.

The remote clients must connect to the site and perform a site update before they can communicate with each other.

Client to Client via Multiple Hubs Using Hub Mode

The figure below shows two remote clients each configured to work in Hub mode with a different Security Gateway:



Remote Client 1 works in Hub mode with Hub 1. Remote Client 2 works in Hub mode with the Hub 2. In order for VPN routing to be performed correctly:

- Remote clients must be working in Office mode
- Office mode address range of each Security Gateway must be included in the `vpn_route.conf` file installed on the other Security Gateway.

| Destination | Next hop router interface | Install On |
|-----------------------|---------------------------|------------|
| Hub1_OfficeMode_range | Hub1 | Hub2 |
| Hub2_OfficeMode_range | Hub2 | Hub1 |

When Remote Client 1 communicates with Remote Client 2:

- The traffic first goes to the Hub 1, since Remote Client 1 is working in Hub mode with Hub 1.
- Hub 1 identifies Remote Client 2's IP address as belonging to the Office mode range of Hub 2.
- The **vpn_route.conf** file on Hub 1 identifies the next hop for this traffic as Hub 2.
- The traffic reaches the Hub 2; Hub 2 redirects the communication to Remote Client 2.

Chapter 25

Link Selection for Remote Access Clients

In This Chapter

| | |
|---|-----|
| Overview | 224 |
| Configuring Link Selection for Remote Access Only | 224 |

Overview

Link Selection is a method used to determine which interface to use for incoming and outgoing VPN traffic and the best possible path for the traffic. Using Link Selection, you choose which IP addresses are used for VPN traffic on each Security Gateway.

Load Sharing and Service Based Link Selection are not supported when the peer is a Remote Access Client. If the Probing Redundancy mode configuration is Load Sharing and the peer is a remote access client, High Availability will be enforced for the client's tunnel. For more information on *Link Selection*, see *Link Selection* (on page 97).

Configuring Link Selection for Remote Access Only

Link selection is configured on each Security Gateway in the **Security Gateway Properties > IPSec VPN > Link Selection** window. The settings apply to

- Security Gateway to Security Gateway connections, and to
- remote access client to Security Gateway connections.

You can configure Link Selection for remote users separately. These settings override the settings configured on the Link Selection page. For more about Link Selection options, see *Link Selection* (on page 97).

To configure separate Link Selection settings for remote access VPN:

1. Using GuiDBedit, the Check Point Database Tool, select the Security Gateway object.
2. Change the value `apply_resolving_mechanism_to_SR` to `false` on the Security Gateway object.
3. Edit the `ip_resolution_mechanism` attribute to determine how remote access clients resolve the IP address of the local Security Gateway. Add one of the following:
 - `mainIpVpn` - Always use the main IP address specified in the **IP Address** field on the **General Properties** page of the Security Gateway
 - `singleIpVpn` - The VPN tunnel is created with the Security Gateway using an IP address set in `single_VPN_IP_RA`
 - `singleNATIpVPN` - The VPN tunnel is created using a NATed IP address set in `single_VPN_IP_RA`
 - `topologyCalc` - Calculate the IP address used for the VPN tunnel by network topology based on the location of the remote peer
 - `oneTimeProb` - Use one time probing to determine which link will be used.
 - `ongoingProb` - Use ongoing probing to determine which link will be used.
4. If you are using ongoing or one time probing, also edit these parameters:
 - `interface_resolving_ha_primary_if` - The primary IP address used for one-time / ongoing probing.
 - `use_interface_IP` - Set to **true** if all IP addresses defined in topology tab should be probed. Set to **false** if the manual list of IP addresses should be probed.
 - `available_VPN_IP_list` - A List of IP addresses that should be probed. (This list is used only if the value of `use_interface_IP` is `false`).
5. Save changes.

Chapter 26





Using Directional VPN for Remote Access

In This Chapter

| | |
|--|-----|
| Directional VPN in RA Communities | 225 |
| Configuring Directional VPN with Remote Access Communities | 226 |

Directional VPN in RA Communities

With Directional VPN configured for Remote Access communities, the option exists to reject connections to or from a particular network object. See these rules:

| NO. | SOURCE | DESTINATION | VPN | SERVICE | ACTION |
|-----|--------|-------------|---|---------|--|
| | * Any | * Any |  Remote_Access_Community  MyIntranet | * Any |  drop |
| | * Any | * Any |  Remote_Access_Community  Any Traffic | * Any |  accept |

| Source | Destination | VPN | Service | Action |
|--------|-------------|---|---------|--------|
| Any | Any | Remote_Access_Community => MyIntranet | Any | drop |
| Any | Any | Remote_Access_Community => Any Traffic | Any | accept |

Connections are not allowed between remote users and hosts within the "MyIntranet" VPN community. Every other connection originating in the Remote Access Community, whether inside or outside of the VPN communities, is allowed.

User Groups as the Destination in RA communities

User groups can be placed in the destination column of a rule. This makes:

- Configuring client to client connections easier
- Configuring "back connections" between a remote client and a Security Gateway possible.

The figure below shows a directional rule for remote access communities which allows return "back" connections.

| NO. | SOURCE | DESTINATION | VPN | SERVICE | ACTION |
|-----|--------|--|---|---------|--|
| 1 | * Any |  Remote_Users@Any |  Any Traffic  Remote_Access_Community | * Any |  accept |

| Source | Destination | VPN | Service | Action |
|--------|------------------|---|---------|--------|
| Any | Remote_Users@Any | Any Traffic => Remote_Access_Community | Any | accept |

To include user groups in the destination column of a rule:

- The rule must be directional
- In the VPN column, the Remote Access community must be configured as the endpoint destination

Configuring Directional VPN with Remote Access Communities

To configure Directional VPN with Remote Access communities:

1. In **Global Properties > VPN** page > **Advanced** > Select **Enable VPN Directional Match in VPN Column**.
2. Right-click inside the VPN column of the appropriate rule, and select **Edit...** or **Add Direction** from the pop-up menu.
The **VPN Match Conditions** window opens.
3. Click **Add**.
The **Directional VPN Match Conditions** window opens.
4. From the drop-down box on the right, select the source of the connection.
5. From the drop-down box on the left, select the connection's destination.
6. Click **OK**.

Chapter 27

Remote Access Advanced Configuration

In This Chapter

| | |
|--|-----|
| Non-Private Client IP Addresses | 227 |
| Preventing a Client Inside the Encryption Domain from Encrypting | 228 |
| Authentication Timeout and Password Caching | 231 |
| Secure Domain Logon (SDL) | 231 |
| Back Connections (Server to Client) | 232 |
| Auto Topology Update (Connect Mode only) | 233 |
| How to Work with non-Check Point Firewalls | 233 |
| Resolving Internal Names with the SecuRemote DNS Server | 233 |



Note - The procedures in this section are relevant for SecureClient. For other clients, see the most updated documentation for that client (<http://supportcontent.checkpoint.com/solutions?id=sk67820>).

Non-Private Client IP Addresses

Suppose a Remote Access Client user connects from behind a NAT device, using a non-private IP address that belongs to another organization. During the life of the connection, the Security Gateway routes all traffic intended for that non-private IP address to the client user, even traffic intended for the real owner of the IP address.

Solving Remote Access Issues

Set the `vpn_restrict_client_phase2_id` in the `Objects_5_0.C` file to the appropriate value, as follows:

| value | meaning |
|----------------|--|
| om_only | Clients behind NAT devices can only connect using Office Mode. |
| private_and_om | Clients can connect using either: <ul style="list-style-type: none">• using Office Mode, <i>or</i>• when using private IP addresses (where the meaning of "private" is specified in the NAT page of the Global Properties window) |
| none | This setting (the default) does not address the problem described above. |



Note - If the user is restricted to Office Mode or to the use of a private IP address, and attempts another type of connection, the connection will be dropped and a log will be sent to the SmartView Tracker.

Preventing a Client Inside the Encryption Domain from Encrypting

The Problem

If a Remote Access Client located inside the VPN domain of one Security Gateway opens a connection to a host inside the VPN domain of another Security Gateway, the connection will be encrypted twice (once by the client and again by the Security Gateway) and decrypted only once (by the peer Security Gateway).

The Solution

To prevent this from happening, configure the client not to encrypt if both the client and the host (the end-points of the connection) are in the VPN domains of Security Gateways managed by the same Security Management server.

To do this, enable the `send_clear_traffic_between_encryption_domains` property in `objects_5_0.C`.



Note - If you enable this feature, ensure that a VPN is defined between the Security Gateways. This feature is disabled when more than one site is defined on the client.

When the Client Has a Private Address

If the `send_clear_traffic_between_encryption_domains` property is enabled, a problem can arise when the Security Gateway's VPN domain includes private addresses, where the meaning of "private" is specified in the **Non Unique IP Address Ranges** page of the **Global Properties** window.

If the client connects from outside the VPN domain (for example, from a hotel) and is assigned (by the ISP or a NAT device) a private IP address which happens to be in the Security Gateway's VPN domain, then the client will not encrypt when connecting to the VPN domain, and the connection will be dropped because it is in the clear.

You can configure the client to encrypt this traffic as follows:

- To encrypt traffic from private addresses, enable the `send_clear_except_for_non_unique` property in `objects_5_0.C`.
- To encrypt traffic from specific IP addresses, proceed as follows:
 1. Define a group consisting of those addresses.
 2. Enable the `send_clear_except_for_specific_addresses` property in `objects_5_0.C`.
 3. Set `send_clear_except_for_address_group` to the name of the group defined in step 1.



Note - This feature is disabled when more than one site is defined on the client.

Working in Connect Mode While Not Connected

For users connected in Connect Mode, you can reduce the frequency of authentication by enabling the `allow_clear_traffic_while_disconnected` property in `objects_5_0.C`. The client will then not encrypt traffic to the peer encryption domain *when not connected*. This will prevent unnecessary authentication when connecting to unencrypted services in the peer encryption domain.

For example, if the site includes both private and public HTTP servers, there is no need to encrypt traffic to the public site. To prevent a user from unnecessarily authenticating only because she is an internal user, configure the following two rules in the Desktop Policy:

| Source | Destination | Service | Action |
|-------------------|-------------------|---------|---------|
| encryption domain | encryption domain | Any | Accept |
| Any | encryption domain | Any | Encrypt |

| Source | Destination | Service | Action |
|--------|-------------|---------|--------|
|--------|-------------|---------|--------|



Note - If you enable this feature, you must ensure that a VPN is defined between the Security Gateways. This feature applies only to Connect Mode. This feature is disabled when more than one site is defined in the client.

Authentication Timeout Interval

To specify the length of time between re-authentications, select **Policy > Global Properties - Remote Access** and in the **Authentication Timeout** section, enter a value in **Validation timeout**. Alternatively, check **Use default value**.

For Connect Mode, the countdown to the timeout begins from the time that the Client is connected.

Password Caching

When the timeout expires, the user will be asked to authenticate again. If password-caching is enabled, clients will supply the cached password automatically and the authentication will take place transparently to the user. In other words, the user will not be aware that re-authentication has taken place.

Password caching is possible only for multiple-use passwords. If the user's authentication scheme implement one-time passwords (for example, SecurID), then passwords cannot be cached, and the user will be asked to re-authenticate when the authentication time-out expires. For these schemes, this feature should *not* be implemented.

Password caching is specified in the client's **Authentication** window.

Enabling and Disabling Secure Domain Logon

To enable Secure Domain Logon (SDL), select **Enable Secure Domain Logon** from the **Passwords** menu.

Note the following:

- If you are using WINS (see WINS (Connect Mode Only (see "[WINS \(Connect Mode Only\)](#)" on page 230))), configure WINS *before* enabling SDL.
- Do not change the machine domain configuration when Secure Domain Logon is enabled.

Domain Controller Name Resolution

If clients are configured in Connect Mode and Office Mode, clients automatically resolve the NT domain name using dynamic WINS.

Otherwise, clients resolve the NT domain name using either LMHOSTS or WINS.

LMHOSTS

The LMHOSTS name resolution service can be used in both LAN and dial-up configurations as follows:

Enter the relevant information (see below) the `$FWDIR/conf/dnsinfo.C` file on the Security Gateway, and install the policy.

Syntax for LMHOSTS Configuration

```
(
  :LMdata (
    : (
      :ipaddr (<IP address>)
      :name (<host name>)
      :domain (<domain name>)
    )
    : (
      :ipaddr (<IP address>)
      :name (<host name>)
```

```

        :domain (<domain name>)
    )
)

```

When the topology is updated, the name resolution data will be automatically transferred to the `dnsinfo` entry of the `userc.c` file and then to its `LMHOSTS` file.

WINS (Connect Mode Only)

The WINS name resolution service can be used in dial-up configurations only. It is not supported on Win 9x platforms.

To use the WINS, proceed as follows on the virtual adapter:

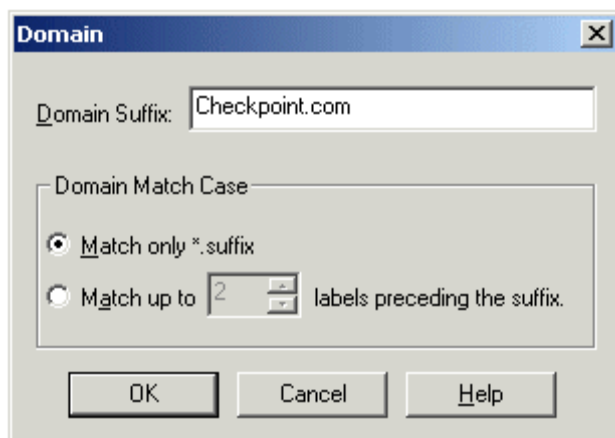


Important - You must do this *before* enabling SDL. See Enabling and Disabling Secure Domain Logon (on page 229).

1. Specify the primary and, optionally, the secondary WINS servers protected by the Security Gateway.
2. Reboot the machine.

Configuring the SecuRemote DNS Server

1. Create a new **SecuRemote DNS Server** from the Objects Tree. Select **Servers and OPSEC** and right-click **Servers > New > SecuRemote DNS**.
2. In the **SecuRemote DNS Properties** window
 - **General** tab — Configure the general settings of the SecuRemote DNS Server as well as the host on which the SecuRemote DNS Server.
 - **Domains** tab — Add new domains or edit and remove existing domains.



3. In the **Domain** tab, define the domain suffix and the matching rule. Names in the domain that correspond to the rule will be resolved by the SecuRemote DNS Server. All other names will be resolved by the SecuRemote client's default DNS server.
 - Specify the **Domain Suffix** for which the SecuRemote DNS Server will resolve the internal names (for example, checkpoint.com).
 - Select **Match only *.suffix** to specify that the maximum number of labels resolved will be 1.
For example, if **Domain Suffix** is "checkpoint.com" and **Match only *.suffix** is selected (that is, the maximum prefix label count is in effect 1) then the SecuRemote DNS Server will be used to resolve "www.checkpoint.com" and "whatever.checkpoint.com" but not "www.internal.checkpoint.com."
 - Select **Match up to...labels preceding the suffix** to increase the number of labels to be matched.
For example, if **Domain Suffix** is "checkpoint.com" and **Match up to...labels preceding the suffix** is selected and set to 3, then the SecuRemote DNS Server will be used to resolve "www.checkpoint.com" and "www.internal.checkpoint.com" but not "www.internal.inside.checkpoint.com".

Additional Considerations

Split DNS is disabled in the following cases:

- In Connect mode, while disconnected.
To override, set `disable_split_dns_when_disconnected` in the SecuRemote/SecureClient `userc.C` file to `false`.
- In connect mode, while connected in Office Mode.
To override, set `disable_split_dns_in_om` in the SecuRemote/SecureClient `userc.C` file to `false`.

Authentication Timeout and Password Caching

The Problem

Users consider multiple authentications during the course of a single session to be a nuisance. At the same time, these multiple authentications are an effective means of ensuring that the session has not been hijacked (for example, if the user steps away from the client for a period of time). The problem is finding the correct balance between convenience and security.

The Solution

Multiple authentication can be reduced by two means:

- Increasing the authentication timeout interval
- Caching the user's password

Secure Domain Logon (SDL)

The Problem

When a SecuRemote/SecureClient user logs on to a domain controller, the user has not yet entered his or her SecuRemote/SecureClient credentials and so the connection to the domain controller is not encrypted.

The Solution

When the Secure Domain Logon (SDL) feature is enabled, then after the user enters the OS user name and password (but before the connection to the domain controller is started), **SecuRemote Client User Authentication** window is displayed. When the user enters the SecuRemote/SecureClient credentials, the connection to the domain controller takes place over an encrypted tunnel.

Configuring SDL Timeout

Because SDL depends on the synchronization of concurrent processes, flexibility in defining timeouts is important.

The SDL Timeout feature of Secure Domain Logon allows you to define the period during which a user must enter his or her domain controller credentials. When the allocated time expires and no cached information is used (if applicable), the logon fails.

The timeout is controlled by the `sdl_netlogon_timeout` (<value in seconds>) parameter in the file `Objects_5_0.C`.



Note - This feature is not applicable if **Auto Local Logon** is enabled (Connect Mode Only).

Cached Information

When the SecuRemote/SecureClient machine successfully logs on to a domain controller, the user's profile is saved in cache. This cached information will be used if subsequent logons to the domain controller fail, for whatever reason.

To configure this option in the client registry, proceed as follows:

1. Go to `HKLM\Software\Microsoft\Windows NT\Current Version\Winlogon`.
2. Create a new key `CachedLogonCount` with the valid range of values from 0 to 50. The value of the key is the number of previous logon attempts that a server will cache.

A value of 0 disables logon caching and any value above 50 will only cache 50 logon attempts.

Configuring Secure Domain Logon

1. Configure the SecuRemote Client to use LMHOSTS (all platforms) or WINS (all platforms except Win 9x).
2. For Win NT and Win 2000, configure the SDL timeout.
3. Define the site where the domain controller resides and download/update the topology.
4. If the client is not already a domain member, configure the machine as a domain member.
5. For Win NT and 2000:
 - Enable Auto Local Logon (optional)
 - Enable Secure Domain Logon
6. Reboot the computer and logon.

Using Secure Domain Logon

After you have rebooted the computer:

1. When the Windows NT **Logon** window is displayed, enter the operating system credentials.
2. Click **OK**.
The SecuRemote **Logon** window is displayed.
3. Enter the SecuRemote credentials in the defined time (see Configuring SDL Timeout (on page 231)).

If you fail to logon and no cached information is used, wait one minute and try again.

If SDL is already configured on the client, the administrator can customize SecuRemote/SecureClient installation packages with SDL enabled by default, thereby relieving the user of the need to configure SDL manually. This can be done in two ways:

- Create a self-extracting client package using the SecureClient Packaging Tool (see Packaging SecureClient (on page 180)) and select **Enable Secure Domain Logon (SDL)** in the **Operating System Logon** window or
- Edit the `product.ini` file in the SecuRemote installation package by setting the value of **EnableSDL** to **1**. See User.C and Product.ini Configuration Files (on page 238) for more information.

Back Connections (Server to Client)

Back connections (connections from the server to the client) are required by certain applications, such as Xterm. These connections do not have to be explicitly defined in the Rule Base. To achieve this, when a user logs on to a site, the username and IP address are stored in an authentication database for 15 minutes (this time frame is configurable). During this time, all back connections from server to client are allowed. After this time, back connections are sent in clear.

Sending Keep-Alive Packets to the Server

To enable the 15 minute interval, configure back connections so that Keep Alive transmissions are sent by the client to the server. This is especially necessary when a NAT device is used.

By sending Keep Alive packets, the IP Address maintained in the authentication database is constantly renewed. In the **Remote Access** page of the **Global Properties** window, check **Enable back connections**

(from Security Gateway to client) and specify a value for **Send Keep-Alive packet to the Security Gateway**.

Auto Topology Update (Connect Mode only)

You can configure SecuRemote Clients to automatically update a site's topology either when starting SecuRemote or just before the IKE key exchange in the **Remote Access** page of the **Global Properties** window.

In this window, the system administrator can:

- **Update topology every ... hours** — The site's topology will be updated before the next key exchange if the defined period has elapsed since the last topology update.

The following features become available if **Update topology every ... hours** is enabled:

- **Automatic update** — If enabled, the site will be updated after the key exchange (according to the value of **Update topology every ... hours**). This will allow to avoid prompting the user to update sites.
- **Upon VPN-1 SecuRemote/SecureClient startup** — If enabled, the user will be prompted to update the topology when the SecuRemote Client starts. If the user is not connected to the network when the SecuRemote Client starts, he or she can reject the prompt. In this case the topology will be automatically updated after the next key exchange with the site.

How to Work with non-Check Point Firewalls

If a SecuRemote/SecureClients is located behind a non-Check Point firewall, the following ports must be opened on the firewall to allow SecuRemote/SecureClient traffic to pass:

| port | explanation |
|--------------------|---|
| UDP port 500 | Always, even if using IKE over TCP |
| TCP port 500 | Only if using IKE over TCP |
| IP protocol 50 ESP | Unless always using UDP encapsulation |
| UDP port 2746 | Only if using MEP, interface resolving or interface High Availability |
| UDP port 259 | Only if using MEP, interface resolving or interface High Availability |

Resolving Internal Names with the SecuRemote DNS Server

The Problem

The SecuRemote/SecureClient must resolve the names of internal hosts (behind the Security Gateway) with non-unique IP addresses using an internal DNS server.

The Solution

The simplest solution is to use Connect Mode and Office Mode. Otherwise, use the split DNS feature by defining a SecuRemote DNS Server.

The SecuRemote DNS Server is an object that represents an internal DNS server that can be used to resolve internal names with unregistered, (RFC 1981-style) IP addresses. It is best to encrypt the DNS resolution of these internal names. Not all DNS traffic should be encrypted, as this would mean that every DNS resolution would require authentication.

Chapter 28

Multiple Entry Point for Remote Access VPNs

In This Chapter

| | |
|---|-----|
| The Need for Multiple Entry Point Security Gateways | 234 |
| The Check Point Solution for Multiple Entry Points | 234 |
| Disabling MEP | 236 |
| Configuring MEP | 236 |
| Configuring Preferred Backup Security Gateway | 237 |
| Disabling MEP | 237 |



Note - The procedures in this section are relevant for SecureClient. For other clients, see the most updated documentation for that client (<http://supportcontent.checkpoint.com/solutions?id=sk67820>).

The Need for Multiple Entry Point Security Gateways

The Security Gateway provides a single point of entry to the internal network. It is the Security Gateway that makes the internal network "available" to remote machines. If the Security Gateway fails, the internal network is no longer available. It therefore makes good sense to have **Multiple Entry Points** (MEP) to the same network.

The Check Point Solution for Multiple Entry Points

In a MEPed environment, more than one Security Gateway is both protecting and giving access to the same VPN domain. How a remote user selects a Security Gateway in order to reach a destination IP address depends on how the MEPed Security Gateways have been configured, which in turn depends on the requirements of the organization.

For more information, see Multiple Entry Point VPNs (on page 117).

The Check Point solution for multiple entry points is based on a proprietary **Probing Protocol** (PP) that tests Security Gateway availability. The MEPed Security Gateways do not have to be in the same location; they can be widely-spaced, geographically.



Note - In a MEPed Security Gateway environment, the only remote client supported is the Check Point SecuRemote/SecureClient.

SecureClient Connect Profiles and MEP

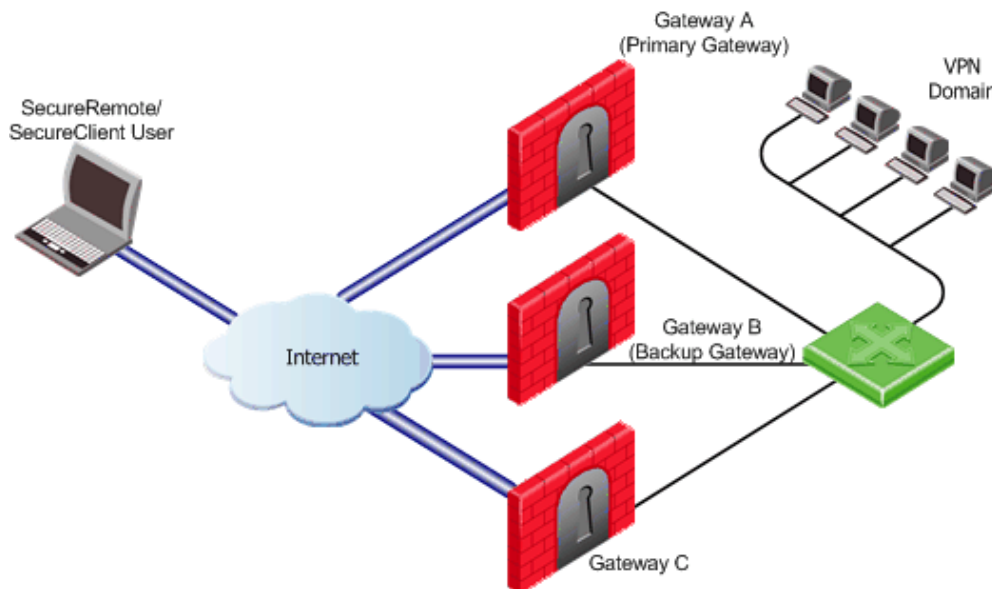
There are three methods used to choose which Security Gateway will be used as the entry point for any given connection:

- **First to reply.** In a First to Reply MEP environment, SecureClient attempts to connect to the Security Gateway configured in the profile. If the configured Security Gateway does not reply, the first Security Gateway to respond is chosen.
- **Primary/Backup.** With this method, SecureClient attempts to connect to the Primary Security Gateway first. If the Primary Security Gateway does not reply, SecureClient attempts to connect to the Backup Security Gateway. If the Backup Security Gateway does not reply, there are no further attempts to connect.

- **Random Selection.** In a Load Sharing MEP environment, SecureClient randomly selects a Security Gateway and assigns the Security Gateway priority. The remote peer stays with this chosen Security Gateway for all subsequent connections to host machines within the VPN domain. Load distribution takes place on the level of "different clients", rather than the level of "endpoints in a connection". In addition, SecureClient ignores whatever Security Gateway is configured as the "connect to Security Gateway" in the profile.

Preferred Backup Security Gateway

Preferred Backup Security Gateway allows remote hosts to choose which Security Gateway in the MEP configuration will be the backup Security Gateway. All other Security Gateways in the MEP configuration will be ignored should the first two Security Gateways become unavailable.



In this scenario:

- The VPN Domain is behind three Security Gateways: A, B and C.
- Security Gateway A is the Primary Security Gateway.
- Security Gateway B is the Backup Security Gateway when Security Gateway A is not available.
- Should Security Gateway A and Security Gateway B become unavailable, the remote host will not attempt to connect to Security Gateway C.

Visitor Mode and MEP

Since the RDP Security Gateway discovery mechanism used in a MEPed environment runs over UDP, this creates a special challenge for SecureClient in Visitor Mode, since all traffic is tunneled over a regular TCP connection.

In a MEPed environment:

- The RDP probing protocol is not used; instead, a special Visitor Mode handshake is employed.
- When a MEP failover occurs, SecureClient disconnects and the user needs to reconnect to the site in the usual way.
- In a *Primary-Backup* configuration, the connection will failover to the backup Security Gateway should the primary Security Gateway become unavailable. Even if the Primary Security Gateway is restored, the connection does not return to the primary Security Gateway.
- All the gateways in the MEP:

Must support visitor mode.

The user must be working with a Visitor Mode enabled profile.

Routing Return Packets

To make sure return packets are routed correctly, the MEPed Security Gateway makes use of IP pool NAT.

IP Pool NAT

IP pool NAT is a type of NAT in which source IP addresses from remote VPN domains are mapped to an IP address drawing from a pool of registered IP addresses. In order to maintain symmetric sessions using MEPed Security Gateways, the MEPed Security Gateway performs NAT using a range of IP addresses dedicated to that specific Security Gateway and should be routed within the internal network to the originating Security Gateway. When the returning packets reach the Security Gateway, the Security Gateway restores the original source IP address and forwards the packets to the source.



Note - When Office Mode is enabled, there is no need to configure IP Pool NAT since Office Mode dynamically assigns IP's to remote hosts.

Disabling MEP

When MEP is disabled, MEP RDP probing and fail over will not be performed. As a result, remote hosts will connect to the Security Gateway defined without considering the MEP configuration.

Configuring MEP

To configure MEP, decide on the MEP selection method:

- First to Respond
- Primary/Backup
- Load Distribution

First to Respond

When more than one Security Gateway leads to the same (overlapping) VPN domain, they are considered MEPed by the remote peer, and the first Security Gateway to respond to the probing protocol is chosen. To configure *first to respond*, define that part of the network that is shared by all the Security Gateways into a single group and assign that group as the VPN domain.

On the **Properties** window of each Security Gateway network object, **Topology** page > **VPN Domain** section, select **Manually defined**, and define the *same* VPN domain for all Security Gateways.

Primary-Backup

1. In the **Global Properties** window, **VPN > Advanced** page, select **Enable Backup Security Gateway**.
2. In the network objects tree, **Groups** section, create a group consisting of the Security Gateways that act as backup Security Gateways.
3. On the **VPN** page of the network object selected as the Primary Security Gateway, select **Use Backup Security Gateways**, and select the group of backup Security Gateways from the drop-down box. This Security Gateway now functions as the primary Security Gateway for a specific VPN domain.
4. Define the VPN for the backup Security Gateway(s). Backup Security Gateways do not always have a VPN domain of their own. They simply back-up the primary.
 - If the backup Security Gateway does not have a VPN domain of its own, the VPN domain should include only the backup Security Gateway itself:
 - On the **Properties** window of the backup network object, **Topology** page > **VPN Domain** section, select **Manually defined**.
 - Select a group or network that contains only the backup Security Gateway.
 - If the backup *does* have a VPN domain:
 - Verify that the IP address of the backup Security Gateway is *not* included in the VPN domain of the primary.
 - For each backup Security Gateway, define a VPN domain that does *not* overlap with the VPN domain of any other backup Security Gateway.



Note - There must be no overlap between the VPN domain of the primary Security Gateway and the VPN domain of the backup Security Gateway(s); that is, no IP address can belong to both.

5. Configure IP pool NAT to handle return packets. See: Configuring Return Packets (on page 237).

Load Distribution

1. In the **Global Properties** window, **Remote Access > VPN Basic** page, **Load distribution** section, select **Enable load distribution for Multiple Entry Point configurations (Remote Access connections)**.
2. Define the same VPN domain for all Security Gateways.

Checking this option also means that load distribution is dynamic, that is the remote client randomly selects a Security Gateway.

Configuring Return Packets

Return packets are handled with IP pool NAT addresses belonging to the Security Gateway.

Configuring IP pool NAT

In **Global Properties > NAT** page, select **Enable IP Pool NAT for SecuRemote/SecureClient and Security Gateway to Security Gateway connections**. Then:

1. For each Security Gateway, create a network object that represents the IP pool NAT addresses for that Security Gateway. The IP pool can be a network, group, or address range. For an address range, for example:
 - On the network objects tree, right-click **Network Objects** branch > **New > Address Range...** The **Address Range Properties** window opens.
 - On the **General** tab, enter the first IP and last IP of the address range.
 - Click **OK**. In the network objects tree, **Address Ranges** branch, the new address range appears.
2. On the Security Gateway object where IP pool NAT translation is performed, **Security Gateway Properties** window, **NAT** page, **IP Pools (for Security Gateways)** section, select either (or both):
 - **Use IP Pool NAT for VPN client connections.**
 - **Use IP Pool NAT for Security Gateway to Security Gateway connections.**
 - In the **Allocate IP Addresses from** field, select the address range you created.
 - Decide after how many minutes unused addressees are returned to the IP pool.
 - Click **OK**.
3. Edit the routing table of each internal router, so that packets with an IP address assigned from the NAT pool are routed to the appropriate Security Gateway.

Configuring Preferred Backup Security Gateway

In SmartDashboard:

1. Click **Manage > Remote Access > Connection Profiles**.
2. Select existing profile and click **Edit** or click **New > Connection Profile**.
The **Connection Profile Properties** opens.
3. In the **Connect to Security Gateway** and **Backup Security Gateway** fields, use the drop down menu to select the Security Gateways that will function as the primary and backup Security Gateways for this profile.
4. Click **OK**.

Disabling MEP

Disabling MEP is configured by setting the following GuiDBedit command to **true**:

- desktop_disable_mep

Chapter 29

Userc.C and Product.ini Configuration Files

In This Chapter

| | |
|---|-----|
| Introduction to Userc.C and Product.ini | 238 |
| Userc.C File Parameters | 239 |
| Product.ini Parameters | 246 |



Note - This section is only relevant for SecureClient.

Introduction to Userc.C and Product.ini

The VPN administrator can use the Packaging Tool to produce customized SecuRemote/SecureClient packages for distribution to end-users. The Packaging Tool changes the behavior of SecuRemote/SecureClient by changing the values of the properties in the `Userc.C` and `Product.ini` files contained in the package.

However, not all of the properties in these files can be changed using the Packaging Tool. It is possible to changes the behavior of SecuRemote/SecureClient by manually editing the `Userc.C` and `Product.ini` files in the SecuRemote/SecureClient package, before distributing the package to end users.

The Userc.C File

The `Userc.C` configuration text file contains has three sections. *Global*, *Managers*, and *Security Gateways*.

- **Global**— Properties that are not specific to the site (managed by a single Security Management server) or to the peer Security Gateway. It does not change on the client machine. To change the Global Properties section of the objects database, do *not* make any manual changes to the Global section of **userc.C**. Either edit the SmartDashboard Global Properties, or use the **DBedit** command line or the graphical Database Tool on the Security Management server.
- **Managers** — Properties that apply per Security Management server. Updated whenever the end user performs a Site Update.
- **Security Gateway**— Properties that are specific to a particular Security Gateway. Updated whenever the end user performs a Site Update.

The section of the file where each parameter resides is indicated in the `Userc.C` file parameter tables (below), in the column labeled **Location in Userc.C**.

Structure of Userc.C

The **Userc.C** configuration text file contains has three sections. *Global*, *Managers*, and *Security Gateways*.

- **Global**— Properties that are not specific to the site (managed by a single Security Management server) or to the peer Security Gateway. It does not change on the client machine. To change the Global Properties section of the objects database, do *not* make any manual changes to the Global section of **userc.C**. Either edit the SmartDashboard Global Properties, or use the **DBedit** command line or the graphical Database Tool on the Security Management server.
- **Managers** — Properties that apply per Security Management server. Updated whenever the end user performs a Site Update.
- **Security Gateway**— Properties that are specific to a particular Security Gateway. Updated whenever the end user performs a Site Update.

The section of the file where each parameter resides is indicated in the **Userc.C** file parameter tables (below), in the column labeled **Location in Userc.C**.

How Userc.C Is Automatically Updated

When the Security Policy is installed on the Security Gateways, the objects database is also installed on the Security Gateways. The part of the database that relates to remote clients is sent to the Topology Server on the Security Gateway. When the clients perform a Site Update, they are actually downloading the Topology information from the Topology server, which updates the Managers and Security Gateway sections of **userc.C** on the clients. The file is stored on the client machine in the **SecuRemote\database** directory. The parameters appear in the **options** section.

How to Manually Edit Userc.C

Do not make any manual changes to the Global section of **userc.C**.

Manually edit the Managers and Security Gateway sections of **userc.C** as follows:

1. Extract **userc.C** from the original SecuRemote/SecureClient **tgz** format installation package.
2. Edit the **userc.C** parameters, as needed.



Important - SecuRemote/SecureClient performs minimal syntax checking for the **userc.C** file. If a parameter is edited incorrectly, the file may become corrupted, and sites may need to be redefined.

3. Recreate the **tgz** file.

The Product.ini file

The **Product.ini** configuration text file contains mostly properties that relate to the package installation. The properties are fixed. The **Product.ini** file is read only upon installation of the SecuRemote/SecureClient.

To change products.ini use the Packaging Tool, or if necessary, edit the file manually as follows:

1. Extract **products.ini** from the original SecuRemote/SecureClient **tgz** format installation package.
2. Perform the required manual editing of **products.ini**.
3. Recreate the **tgz** file. This is the SecuRemote/SecureClient package for end-users.

Userc.C File Parameters

The following lists describe the parameters included in the **Userc.C** configuration file, arranged by the features that the parameters relate to.

SecureClient



Note - **Bold** indicates the default value. *Global*, *Managers*, or *Security Gateway* indicates the location in **Userc.C**. See The **Userc.C** File (on page 238). Do not manually edit Global properties.

- **default_ps (n.n.n.n)** — Specifies the IP address of the default Policy Server. If this property exists, SecureClient will automatically log on to the Policy Server (with IP n.n.n.n) when it is launched, relieving the user of the need to manually log on to the Policy Server — *Global*.
- **manual_slan_control (true, false)** — Disabling this property will remove the **Disable Policy** menu items from the **Policy** menu — *Global*.
- **allow_clear_in_enc_domain (true, false)** — If enabled, unencrypted connections will be accepted by SecureClient NG over Encrypt desktop rules and by SecureClient 4.1 running **Encrypted Only** or **Outgoing and Encrypted** policy, as long as both the source and the destination IP addresses are in the encryption domain of a single Security Gateway — *Global*.

- `disable_stateful_dhcp` (**true, false**) — As long as this attribute is false, DHCP packets will be allowed by SecureClient regardless of the enforced Desktop Security policy. If you set this attribute to true, DHCP will be allowed only if the Desktop Security policy allows it explicitly. This requires SecureClient version 4.1 to run a policy of **Allow All** and SecureClient NG to have DHCP enabled through specific rules — *Global*.
- `block_conns_on_erase_passwords` (**true, false**) — If true, the **Close VPN** option will replace **Erase Password** in the SecureClient's **Passwords** menu and the button will appear in the toolbar. Selecting **Close VPN** or clicking the above button will result in blocking all encrypted connections — *Managers*.
- `enable_automatic_policy_update` (**true, false**) — Specifies whether Automatic Policy Update is enabled or not — *Managers*.
- `silent_policy_update` (**true, false**) — If true, the client will not prompt the user to update the policy upon client startup, even if the time specified in `automaic_policy_update_frequency` has passed. The client will still attempt to update the policy after successful key exchange — *Managers*.
- `PS_HA` (**true, false**) — Use backup Policy Servers on logon failure — *Managers*.
- `PS_LB` (**true, false**) — If true will randomize policy server — list so not all clients will try to connect to the same policy server — *Managers*.
- `LB_default_PS` (**true, false**) — If true, when `default_ps(x.x.x.x)` is set it will go to a random Policy Server in the same site (found by examining topology) — *Managers*.
- `no_policy` (**true, false**) — Indicates disable policy state — *Global*.
- `policy_expire` (**60**) — Timeout of policy, in minutes. This property can also be controlled in SmartDashboard — *Managers*.
- `retry_frequency` (**30**) — If logged in to a Policy Server, but failed to re-logon after half the expiry time, this parameter (in seconds) specifies the amount of time before retrying logon. On each attempt all Policy Servers are tried — *Managers*.
- `automaic_policy_update_frequency` (**10080**) — Controls how frequently (in seconds) SecureClient should update policy files — *Managers*.
- `suppress_all_balloons` (**true, false**) - which controls all balloon messages. If the flag is set to true, no message balloons are displays. If false, all balloons are displayed. Note that the balloon's messages will still appear in the `.tde` files and will be logged in the Status Dialog's MessageViewer.
- `sdl_browse_cert` (**true, false**) - When set to false, the browse certificate in "change authentication" is disabled. When set to true, the browse dialog in SDL mode is restricted, you can only browse files, not create, change or launch applications.
- `disconnect_when_in_enc_domain` (**true, false**)- If the client is connected to a site, and an interface appears with an IP address located within one of the Security Gateway's VPN domains, the client is disconnected. A message balloon explains why.
- `open_full_diagnostic_tool` (**true, false**) - When set to false, SC will open only log-view of diagnostic. When set to true, SC will open full diagnostic. In any case, the full diagnostic tool will open from the start menu.
- `tt_failure_show_notification` (**true, false**) - If **fail_connect_on_tt_failure** is false, (meaning that a connection will succeed even though tt failed) then a string notification of tt-failure will show in the connection progress details because of this flag.
- `simplified_client_route_all_traffic` (**true, false**) - This attribute determines whether the Simplified Client performs connections using route-all-traffic or not.
- `scv_allow_sr_clients` (**true, false**)- If set to true, SecuRemote clients, which by default are not SCV verified, will send a verified state to the enforcing Security Gateway.
- `use_profile_ps_configuration` (**true, false**) - Set to true to enable remote users to connect to one Security Gateway and logon to a Policy Server behind another Security Gateway.
- `force_route_all_in_profile` (**true, false**) — If set to true, profiles created by the user will have the "route all traffic" option selected and grayed in the profile creation/edit dialog. - *Global*
- `enable_mode_switching` (**true, false**) - If set to true, client has the option to switch between *Extended View* and *Compact View*.

HotSpot Registration

- `enabled` (**true, false**) - Set to **true** to enable a user to perform Hotspot registration.
- `log` (**true, false**) - Set to **true** to send logs with the list of IP addresses and ports accessed during registration.
- `connect_timeout` (600) - Maximum number of seconds to complete registration.
- `max_ip_count` (5) - Maximum number of IP addresses allowed during registration.
- `block_hotspot_after_connect` (**true, false**) - If set to **true** upon successful connect, the recorded ports and addresses will not remain open.
- `max_trials` (0) - This value represents the maximum number of unsuccessful hotspot registration attempts that an end user may perform. Once this limit is reached, the user will not be allowed to attempt registration again. The counter is reset upon reboot, or upon a successful VPN connect. In addition, if you modify the **max_trials** value, the modification will take affect only upon successful connect, or reboot.
If the **max_trials** value is set to 0, an unlimited number of trials is allowed.
- `local_subnets` (**true, false**) - **Restrict access to local subnets only.**
- `ports` (80, 443, 8080) - Restrict access to specific ports.

Encryption



Note - indicates the default value. *Global, Managers, or Security Gateway* indicates the location in Userc.C. See The Userc.C File (on page 238). Do not manually edit Global properties.

- `use_cert` (**true, false**) — Specifies whether Use Certificate will be checked in the **IKE Authentication** window — *Global*.
- `use_entelligence` (**true, false**) — Specifies whether SecuRemote should attempt to use the Entrust Entelligence toolkit, if installed — *Global*.
- `entrust_inifile` — Full path to a non-default entrust.ini file, to be used by SecuRemote/SecureClient when working with entrust certificates — *Global*.
- `certfile` — Name of the last certificate used — *Global*.
- `gettopo_port` (**264**) — Which port to use for topology update — *Global*.
- `pwd_erase_on_time_change` (**true, false**) — Performs **Erase Passwords** when the user changes the system clock — *Global*.
- `force_udp_encapsulation` (**true, false**) — Indicates whether UDP encapsulation is used (transparent, and active profile in connect mode). Also used in Connect Mode to create the default profile — *Global*.
- `support_tcp_ike` (**true, false**) — Indicates whether TCP over IKE is used (transparent, and active profile in connect mode). Also used in Connect Mode to create the default profile — *Global*.
- `support_tcp_ike` (**true/false/use_site_default**) — Determine whether or not to attempt IKE over TCP — *Security Gateway*.
- `support_ip_assignment` (**true, false**) — Indicates whether Office Mode is used (transparent, and active profile in connect mode). Also used in connect mode to create the default profile — *Global*.
- `ChangeUDPSport` (**true, false**) — If the value of both flags `ChangeUDPSport` and `force_udp_encapsulation` is true, a random source port is used for IKE packets, and another random source port is used for UDP encapsulation packets — *Global*.
- `uencapport` (**2746**) — Specifies the port to be used on the UDP encapsulated packets when using UDP encapsulation — *Security Gateway*.
- `ChangeIKEPort` (**true, false**) — If true, do not bind to port 500. Instead, use router port and use address translation to make it seem as if the connection originated from port 500. This parameter allows

other client applications (such as IPSO and Microsoft) to use that port. Note if the port is taken, another port will be used — *Global*.

- `send_clear_traffic_between_encryption_domains` (**true, false**) — if true and the source and the destination are behind encryption domains (not same domains), packets will be sent clear. This feature is enabled only if a single site is defined — *Managers*.
- `send_clear_except_for_non_unique` (**true, false**) — If true, `send_clear_traffic_between_encryption_domains` will not function for IP addresses which are defined as NAT private addresses.
- `send_clear_except_for_specific_addresses` (**true, false**) — If true, `send_clear_traffic_between_encryption_domains` will not function for IP addresses which are defined in `send_clear_except_for_address_group` — *Managers*.
- `send_clear_except_for_address_group` — Address group specification for `send_clear_except_for_specific_addresses` — *Managers*.
- `dns_encrypt` (**true, false**) — Overwrites the encrypting attribute received in the topology in the `dnsinfo` section.
- `disable_split_dns_when_in_om` (**true, false**) — Disable split DNS when in Office Mode — *Global*.
- `disable_split_dns_when_disconnected` (**true, false**) — Disable split DNS when disconnected — *Global*.
- `disconnect_on_IKE_SA_expiry` (**true, false**) — In connect mode, if the IKE timeout expires and this property is **true**, disconnect instead of erasing the passwords — *Global*.
- `renew_users_ica_cert` (**true, false**) — Specifies whether users be able to renew their certificates (explicitly or implicitly) — *Managers*.
- `renew_users_ica_cert_days_before` (**1-1000**) **60** — How many days before expiration to start and perform an implicit renewal — *Managers*.
- `upgrade_fp1_and_below_users_ica_cert` (**true, false**) — Whether or not to implicitly renew certificates that were issued before NG FP2 — *Managers*.
- `ike_negotiation_timeout` (**36**) — Determines the maximum time in seconds that the IKE engine will wait for a response from the peer before timing out. This is the maximum interval between successive packets, and not the maximum negotiation lifetime — *Managers*.
- `phase2_proposal` (**large**, small) — Determines the size of the proposal sent by the client in Quick Mode, packet 1. This property is for backwards compatibility. NG FP3 and higher clients use `phase2_proposal_size` — *Managers*.
- `phase2_proposal_size` (**large**, small) — Determines the size of the proposal sent by NG FP3 or higher clients in Quick Mode, packet 1. If the value is missing the value of `phase2_proposal` is taken instead. NG FP3 clients will try a large proposal after a small proposal attempt fails — *Managers*.
- `vpn_peer_ls` (**true, false**) — In a MEP fully overlapping encryption domain configuration, if this property is **TRUE**, a Security Gateway will be chosen randomly between the MEP Security Gateways and will be given priority — *Managers*.
- `ike_support_dos_protection` (**true, false**) — Determines whether the client is willing to respond to a DoS protection request, by restarting Main Mode using a stateless protection. Equivalent to the SmartDashboard Global Property: Support IKE DoS Protection from unidentified Source — *Managers*.
- `sr_don't_check_crl` (**true, false**) — Do not check the CRL of the certificate — *Managers*.
- `crl_start_grace` (610200) — SecuRemote/SecureClient may accept CRLs that are not yet valid — *Managers*.
- `crl_end_grace` (1209600) — SecuRemote/SecureClient may accept CRLs that have recently expired — *Managers*.
- `site_default_tcp_ike` (**true, false**) — Determines the site default for attempting IKE over TCP. Each Security Gateway has a property: "supports_tcp_ike" (true, false or use_site_default). If the value is set to 'use_site_default' then the management property `site_default_tcp_ike` is used by the client to determine whether to attempt IKE over TCP or not — *Managers*.

- `suppress_ike_keepalive` (**true**, false) — If the IPsec keepalive is turned on, and the value of the property "suppress_ike_keepalive" is false, empty UDP packets will be sent to the Security Gateway (destination port 500). The UDP keepalive packets are sent only if there is an IKE SA with the peer and if UDP encapsulation was chosen — Managers.
- `default_phase1_dhgrp` — This field indicates which DH group to use for IKE phase 1 before the client has a topology. If the flag does not exist, group 2 will be used — Global.
- `to_expire` (**true**, false) — Whether or not to have a timeout for the phase2 IKE authentication. This property can also be controlled in SmartDashboard — Managers.
- `expire` (120) — Timeout of IKE phase2. This property can also be controlled in SmartDashboard — Managers.
- `ICA_ip_address` — The IP address of the Internal CA — Global.
- `allow_capi` (**true**, false) — Allow the disabling of CAPI storage to Internal CA registration — Global.
- `allow_p12` (**true**, false) — Allow the disabling of p12 file storage to Internal CA registration — Global.
- `trust_whole_certificate_chain` (**true**, false) — This attribute improve connectivity where there is a Certificate hierarchy, and the CA trusted by the Security Gateway is a subordinate CA (not necessarily a direct subordinate) of the client trusted CA. Without this flag, both the Security Gateway and the client must trust exactly the same CA — Global.
- `is_subnet_support` (**true**, false) — If turned on, IPsec SA will be valid for a subnet, otherwise it will be valid for a specific address — Security Gateway.
- `ISAKMP_hybrid_support` (**true**, false) — If turned on, when the authentication pop up appears, the user will have the option to choose between Hybrid mode and certificates as an authentication mode. (Otherwise the user will have the option to choose between certificates and pre-shared secret) — Security Gateway.
- `resolve_multiple_interfaces` (**true**, false) — If 'resolve_interface_ranges' (static interface resolving) is disabled or failed, and this property is turned on, then dynamic interface resolving will be done when addressing this Security Gateway. In this case the interfaces of the Security Gateway will be probed once — Security Gateway.
- `interface_resolving_ha` (**true**, false) — If dynamic interface resolving is used (see `resolve_multiple_interfaces`) and this property is turned on- the interfaces of the Security Gateway will be probed per connection to see if they are live — Security Gateway.
- `isakmp.ipcomp_support` (**true**, false) — If the peer Security Gateway is a least NG and the client is SecureClient (and not SecuRemote) then: — If the client is in "send small proposal" mode and this property is turned on then IP compression will be proposed. (If the client is in "send large proposal" mode then IP compression will be offered regardless of the value of this property) — Security Gateway.
- `supports_tcp_ike` (use_site_default) — If IKE over TCP is configured on the client AND either this property is 'true' or it's 'use_site_default' and site_default_tcp_ike is 'true', then IKE phase 1 will be done over TCP — Security Gateway.
- `supportSRikeMM` (**true**, false) — When the authentication method is PKI, if this property is false, Main mode is not supported — Security Gateway.

Multiple Entry Point



Note - **Bold** indicates the default value. *Global*, *Managers*, or *Security Gateway* indicates the location in Userc.C. See The Userc.C File (on page 238). Do not manually edit Global properties.

`resolver_ttl` (10) — Specifies how many seconds SecuRemote will wait before deciding that a Security Gateway is down — Global.

`active_resolver` (**true**, false) — Specifies whether SecuRemote should periodically check the Security Gateway status. Active Security Gateway resolving may cause the dial-up connection to try to connect to an ISP. Turning this property off will avoid problems associated with this behavior — Global.

`resolver_session_interval` (30) — Specifies for how many seconds the Security Gateway status (up or down) remains valid — Global, Managers.

Encrypted Back Connections



Note - Bold indicates the default value. *Global*, *Managers*, or *Security Gateway* indicates the location in Userc.C. See The Userc.C File (on page 238). Do not manually edit Global properties.

- `keep_alive` (**true**, false) — Specifies whether the Security Gateway will maintain session key information for the Client, to allow encrypted back connections at any time. This property can also be controlled in SmartDashboard — Global, Managers.
- `keep_alive_interval` (20) — When `keep_alive` is true, SecuRemote will ping the Security Gateway every *n* seconds, where *n* is the number specified by the `keep_alive_interval` property. This property can also be controlled in SmartDashboard — Global.

Topology



Note - Bold indicates the default value. *Global*, *Managers*, or *Security Gateway* indicates the location in Userc.C. See The Userc.C File (on page 238). Do not manually edit Global properties.

- `topology_over_IKE` (**true**, false) — Specifies whether New Site in SecuRemote will use IKE to authenticate the user. If this property is set to true, IKE will be used, either using Hybrid Authentication (i.e., any authentication method chosen in the Authentication tab of the user properties) or using certificates. If this property is set to False, SSL will be used (as in version 4.1), and users will need IKE pre-shared secret or certificate configured to define a new site — Global, Managers.
- `encrypt_db` (**true**, false) — Specifies whether the topology information in userc.C is maintained in encrypted format — Global.
- `silent_topo_update` (**true**, false) — Used for backwards compatibility, when working with servers that do not pass the property per site. This property can also be controlled in SmartDashboard — Global, Managers.
- `silent_update_on_connect` (**true**, false) — Tries to perform an update with the Security Gateway to which a connection is being attempted, before connecting (applies to IPSO clients) — Global.
- `update_topo_at_start` (**true**, false) — If the timeout expires, update the topology upon start up of the SecuRemote/SecureClient GUI application — Global, Managers.

NT Domain Support



Note - Bold indicates the default value. *Global*, *Managers*, or *Security Gateway* indicates the location in Userc.C. See The Userc.C File (on page 238). Do not manually edit Global properties.

- `no_clear_tables` (**true**, false) — Setting this property to true will enable the opening of new encrypted connections with the Encryption Domain after SecuRemote/SecureClient has been closed by logoff or shutdown, as long as encryption keys have been exchanged, and are still valid. This may be necessary when using a Roaming Profile with NT domains, since the PC tries to save the user's profile on the Domain Controller during logoff and shutdown, after SecuRemote/SecureClient has been closed by Windows. This feature should be used in conjunction with "keep_alive" (see Encrypted Back Connections (on page 244)), to ensure that valid encryption keys exist at all times — Global.
- `connect_domain_logon` (**true**, false) — Global. Setting this attribute to true enables clients using Connect Mode to log on to a Domain Controller via SDL. The user should do the following in order to logon to the Domain Controller:
 - a) Log on to the local Windows machine.
 - b) Connect to the organization.
 - c) Logoff and log back on (within five minutes after logoff) to the protected Domain Controller, using the encrypted connection.

**Note -**

- Enabling this setting will keep the client Connected to the organization for five minutes after the user logs off Windows.
- This feature was introduced before SDL in connect mode was introduced. In versions where SDL is supported, this property is used only for domain roaming profile support.
- `sdl_main_timeout` (60000) — In connect mode this property specifies the amount of time to wait for user to successfully connect or cancel the connect dialog — Global.

Miscellaneous



Note - Bold indicates the default value. *Global*, *Managers*, or *Security Gateway* indicates the location in Userc.C. See The Userc.C File (on page 238). Do not manually edit Global properties.

- `enable_kill` (**true**, false) — Specifies whether the user can Stop SecuRemote/SecureClient. If this option is set to false, Stop VPN-1 SecuRemote or Stop VPN-1 SecureClient does not appear in the File menu or when right-clicking on the system tray icon — Global.
- `use_ext_auth_msg` (**true**, false) — Specifies whether SecuRemote/SecureClient will show custom messages in the authentication window upon success or failure. The messages should be placed in a file named AuthMsg.txt located in the SecuRemote directory (typically in Program Files\CheckPoint). See the AuthMsg.txt file in the SecuRemote package for more details — Global.
- `use_ext_logo_bitmap` (**true**, false) — Specifies whether SecuRemote/SecureClient will show a custom bitmap in the authentication window. The file should be named logo.bmp and should be placed in the SecuRemote directory (usually located under Program Files\CheckPoint) — Global.
- `guilibs` — Used to specify SAA DLL, and is documented in this context — Global.
- `pwd_type` (now, later) — Used internally to indicates now or later auth dialog state. Do not modify — Global.
- `connect_mode_erase_pwd_after_update` (true, false) — Erase password after a site update in Connect Mode. Used with `silent_update_on_connect` — Global.
- `disable_mode_transition` (**true**, false) — Do not enable user to switch between modes via GUI or command line — Global.
- `connect_api_support` (**true**, false) — Indicates SecuRemote/SecureClient mode. Set to true in order to work with the Connect API — Global.
- `connect_mode` — Indicates SecuRemote/SecureClient mode. True for connect mode — Global.
- `allow_clear_traffic_while_disconnected` (**true**, false) — Topology is not loaded when disconnected, ensuring that there are no popups on the LAN when disconnected — Global.
- `stop_connect_when_silent_update_fails` (**true**, false) — If trying to connect in `silent_update_on_connect` mode, and the topology update fails, the connection will fail — Global.
- `go_online_days_before_expiry` (0) — The number of days before Entrust automatic key rollover (certificate renewal). Zero equals never — Global.
- `go_online_always` (**true**, false) — When true, will attempt the LDAP (entrust.ini) protocol after successful IKE negotiation — Global.
- `implicit_disconnect_threshold` (900) — When losing connectivity on physical adapter, SecuRemote/SecureClient keeps the connected state for the amount of time (in seconds) specified by `implicit_disconnect_threshold`. If the time elapses, or if connectivity resumes with a different IP address, SecuRemote/SecureClient disconnects. This is useful in network environments with frequent network disconnection, such as wireless — Global.
- `active_test` — Active tests configuration — Global.

- `log_all_blocked_connections` — Used internally to indicate the mode, and reflects the state of the GUI checkbox. Do not modify — Global.
- `cache_password` — Used internally to save the state of the checkbox called "Remember password, as per site settings". Do not modify — Global.
- `dns_xlate` (**true**, false) — Turn off the split DNS feature. May be needed in versions prior to NG FP3. In later versions, split DNS is not used by default when in Office Mode — Global.
- `FTP_NL_enforce` (0, 1, 2) — Indicates the strictness of the FTP inspection (0 -no check, 1- default check: Multiple newline characters allowed, 2-strict check: no multiple newline characters allowed — Global.
- `show_disabled_profiles` (**true**, false) — In connect mode, if the IKE timeout expires and this property is TRUE, disconnect instead of erasing the passwords — Global.
- `post_connect_script` — Specify full path for a script that SecuRemote/SecureClient will run after a connection has been established (Connect Mode only) — Managers.
- `post_connect_script_show_window` (**true**, false) — Specifies whether or not the post-connect script will run in a hidden window — Managers.
- `list_style` — How the site icons are presented in the main frame window — Global.
- `mac_xlate` (**true**, false) — Needs to be set to true to support Split DNS where traffic to the "real" DNS server may not be routed the same way as traffic to the "split" DNS server. The most common scenario is "real" DNS server on the same subnet as the client. Split DNS modifies the IP destination of the packet, but not the MAC destination. With `mac_xlate` set to true, the MAC destination address is set to the address of the default Security Gateway — Global.
- `mac_xlate_interval` — How frequently a check is made for the default Security Gateway's MAC address (see `mac_xlate`) — Global.
- `sda_implicit` (**true**, false) — The working mode of the Software Distribution Agent (SDA). True = implicit, false = explicit — Global, Managers.
- `sda_implicit_frequency` — The frequency (in minutes) with which the Software Distribution Agent (SDA) connects to ASD server to check for updates — Global, Managers.
- `sr_build_number`, `sr_sw_url_path`, `sr_sw_url_path_9x`, `sr_build_number_9x`, `sr_sw_url_path_nt`, `sr_build_number_nt`, `sr_sw_url_path_w2k`, `sr_build_number_w2k` — On the Security Management server machine, the names are `desktop_sw_version`, `desktop_build_number`, etc. These attributes help SecureClient decide if it needs to upgrade itself — Managers.
- `install_id_nt`, `install_id_9x`, `install_id_w2k` — Installation IDs — Managers.

Product.ini Parameters

The following are the parameters included in the `Product.ini` configuration file.

| Parameter (bold indicates the default) | Meaning |
|--|---|
| OverwriteConfiguration=0/1 | Sets the value for Update or Overwrite choice during upgrade. The default value (0) means Update is chosen. |
| ShowUpdateOverwrite=0/1 | Show the Update or Overwrite window to the user during installation. If the window is not shown to the user, the value placed in OverwriteConfiguration will be used. |
| PathAskUser=0/1 | Show the Choose Installation Destination window to the user during installation. If the window is not shown to the user, the default value chosen by InstallShield will be used (usually this will be C:\Program Files\CheckPoint\SecuRemote). |

| Parameter (bold indicates the default) | Meaning |
|--|---|
| DesktopSecurityAskUser=0/1 | Show the Desktop Security window to the user during installation. If the window is not shown to the user, the value placed in DesktopSecurityDefault will be used. |
| DesktopSecurityDefault=0/1 | Sets the value for Desktop Security installation. A value of 1 means that SecureClient will be installed, while a value of 0 means that SecuRemote will be installed. |
| InstallDialupOnly=0/1 | Sets the value for binding to All Adapters or to Dialup Adapters only. A value of 0 means that the installation will bind to All Adapters. |
| ShowNetworkBindings=0/1 | Show the Adapter Bindings window to the user during installation. If the window is not shown to the user, the value placed in InstallDialupOnly will be used. |
| ShowReadmeFile=0/1 | Show the Readme window to the user - this window asks the user whether he/she would like to view the readme file before finishing the installation. A value of 0 means that the window will not be shown to the user, and the readme file will not be read during installation. |
| ShowBackgroundImage=0/1 | Determine whether the background image will be displayed during installation. |
| ShowSetupInfoDialogs=0/1 | Determine whether informative InstallShield dialogs (which require no user interaction) will be displayed. |
| DisableCancelInstall=0/1 | An option to disable the Cancel operation from the installation dialogs. |
| ShowRestart=0/1 | Determine whether Do you want to restart dialog will be shown. |
| RestartAfterInstall=0/1 | 0 - Do no restart after installation, 1- Restart after installation. |
| ShowRebootWarning=0/1 | Suppress the message "The installation will complete after reboot". |
| IncludeBrandingFiles=0/1 | Determines whether the files authmsg.txt and logo.bmp (used for customizing the Authentication dialog) will be copied during installation. See the userc.C options section for more details on use_ext_auth_msg and use_ext_logo_bitmap . |
| EnableSDL=0/1 | Sets the value of Secure Domain Logon (SDL) during installation. If the value is 1, SDL will be enabled during installation. |
| SdlNetlogonTimeout (Seconds/0) | Set timeout for the operating system Net Logon, if 0 do not change the current value. |
| Support3rdPartyGina=0/1 | SecuRemote Client NG allows using third party GINA DLLs for authentication. If this property is not selected, the Windows GINA DLL will be used by default. Enabling this property may conflict with SDL operation if a third party GINA DLL is used. |
| EnablePolicyView=0/1 | Enable the Policy View in the SecureClient Diagnostics application. |
| EnableLogView=0/1 | Enable the Log View in the SecureClient Diagnostics application. |
| EnableDiagnosticsView=0/1 | Enable the Diagnostics View in the SecureClient Diagnostics application. |

| Parameter (bold indicates the default) | Meaning |
|--|--|
| ShowKernellInstallation=0/1 | Determines whether or not the driver installation dialog is displayed. |
| OverwriteEntlNI=0/1 | Determines whether existing entrust.ini files will be overwritten by the entrust.ini files in the installation. A value of 1 indicates that the existing entrust.ini file will be overwritten. |
| DefaultPath (Full path) | Default: C:\Program Files\CheckPoint\SecuRemote. |
| ConnectMode=0/1 | Set default client mode: 0 - transparent, 1- connect mode. |

Chapter 30

SSL Network Extender

In This Chapter

| | |
|---|-----|
| Introduction to the SSL Network Extender | 249 |
| How the SSL Network Extender Works | 250 |
| Commonly Used Concepts | 250 |
| Special Considerations for the SSL Network Extender | 251 |
| Configuring the SSL Network Extender | 253 |
| SSL Network Extender User Experience | 259 |
| Troubleshooting SSL Network Extender | 269 |

Introduction to the SSL Network Extender

Whenever users access the organization from remote locations, it is essential that not only the usual requirements of secure connectivity be met but also the special demands of remote clients. These requirements include:

- **Connectivity:** The remote client must be able to access the organization from various locations, even if behind a NATing device, Proxy or Firewall. The range of applications available must include web applications, mail, file shares, and other more specialized applications required to meet corporate needs.
- **Secure connectivity:** Guaranteed by the combination of authentication, confidentiality and data integrity for every connection.
- **Usability:** Installation must be easy. No configuration should be required as a result of network modification. The given solution should be seamless for the connecting user.

To resolve these issues, a secure connectivity framework is needed to ensure that remote access to the corporate network is securely enabled.

The SSL (Secure Socket Layer) Network Extender is a simple-to-implement remote access solution. A thin client is installed on the user's machine. (The SSL Network Extender client has a much smaller size than other clients.) It is connected to an SSL enabled web server that is part of the Enforcement Module. By default, the SSL enabled web server is disabled. It is activated by using the SmartDashboard, thus enabling full secure IP connectivity over SSL. The SSL Network Extender requires a server side configuration only, unlike other remote access clients. Once the end user has connected to a server, the thin client is downloaded as an ActiveX component, installed, and then used to connect to the corporate network using the SSL protocol.

It is much easier to deploy a new version of the SSL Network Extender client than it is to deploy a new version of other conventional clients.



Note - If the Mobile Access blade is active on a Security Gateway, SSL Network Extender works through Mobile Access and not IPsec VPN. In this case, SSL Network Extender must be configured through the Mobile Access blade. If you already had SSL Network Extender configured on an IPsec VPN Security Gateway and then you enable the Mobile Access blade, you must reconfigure SSL Network Extender for the Mobile Access blade.

How the SSL Network Extender Works

The SSL Network Extender solution comprises a thin client installed on the user's Desktop/Laptop and an SSL enabled web server component, integrated into the Security Gateway.

To enable connectivity for clients using the SSL Network Extender - a Security Gateway must be configured to support SecuRemote/SecureClient, in addition to a minor configuration specific to SSL Network Extender.

The SSL Network Extender may be installed on the user's machine by downloading it from a Security Gateway, R55 HFA10 (or higher).

Commonly Used Concepts

This section briefly describes commonly used concepts that you will encounter when dealing with the SSL Network Extender. It is strongly recommended that you review the "Remote Access VPN" section of this book before reading this guide.

Remote Access VPN

Refers to remote users accessing the network with client software such as SecuRemote/SecureClient, SSL clients, or third party IPSec clients. The Security Gateway provides a *Remote Access Service* to the remote clients.

Remote Access Community

A Remote Access Community, a Check Point concept, is a type of VPN community created specifically for users that usually work from remote locations, outside of the corporate LAN.

Office Mode

Office Mode is a Check Point remote access VPN solution feature. It enables a Security Gateway to assign a remote client an IP address. This IP address is used only internally for secure encapsulated communication with the home network, and therefore is not visible in the public network. The assignment takes place once the user connects and authenticates. The assignment lease is renewed as long as the user is connected. The address may be taken either from a general IP address pool, or from an IP address pool specified per user group, using a configuration file.

Visitor Mode

Visitor Mode is a Check Point remote access VPN solution feature. It enables tunneling of *all* client-to-Security Gateway communication through a regular TCP connection on port **443**. Visitor mode is designed as a solution for firewalls and Proxy servers that are configured to block IPSec connectivity.

Endpoint Security on Demand

Endpoint Security on demand (ESOD) may be used to scan endpoint computers for potentially harmful software before allowing them to access the internal application. When end users access the SSL Network Extender for the first time, they are prompted to download an ActiveX component that scans the end user machine for Malware. The scan results are presented both to the Security Gateway and to the end user. SSL Network Extender access is granted/denied to the end user based on the compliance options set by the administrator.

ESOD Policy per User Group

Since there are many different kinds of threats to your network's security, different users may require different configurations in order to guard against the increasing number and variety of threats. The ability to configure a variety of ESOD policies enables the administrator to customize the software screening process between different user groups.

Screened Software Types

ESOD can screen for the Malware software types listed in the following table:

| Software Type | Description |
|----------------------------|---|
| Worms | Programs that replicate over a computer network for the purpose of disrupting network communications or damaging software or data. |
| Trojan horses | Malicious programs that masquerade as harmless applications. |
| Hacker tools | Tools that facilitate a hacker's access to a computer and/or the extraction of data from that computer. |
| Keystroke loggers | Programs that record user input activity (that is, mouse or keyboard use) with or without the user's consent. Some keystroke loggers transmit the recorded information to third parties. |
| Adware | Programs that display advertisements, or records information about Web use habits and store it or forward it to marketers or advertisers without the user's authorization or knowledge. |
| Browser plug-ins | Programs that change settings in the user's browser or adds functionality to the browser. Some browser plug-ins change the default search page to a pay-per-search site, change the user's home page, or transmit the browser history to a third party. |
| Dialers | Programs that change the user's dialup connection settings so that instead of connecting to a local Internet Service Provider, the user connects to a different network, usually a toll number or international phone number. |
| 3rd party cookies | Cookies that are used to deliver information about the user's Internet activity to marketers. |
| Other undesirable software | Any unsolicited software that secretly performs undesirable actions on a user's computer and does not fit any of the above descriptions. |

Special Considerations for the SSL Network Extender

This section lists SSL Network Extender special considerations, such as pre-requisites, features and limitations:

Pre-Requisites

The SSL Network Extender pre-requisites are listed below:

Client-side Pre-Requisites

The SSL Network Extender client-side pre-requisites are listed below:

- Remote client must be running the following:
- Windows 2000 Pro
- Windows XP Home Edition and Pro
- Windows Vista
- Linux RHEL 3.0
- Linux Suse 9 and up
- Red Hat Linux 7.3

- Mac OSX Tiger
- Remote client must use the following. Each must allow ActiveX or Java Applet.
- Internet Explorer version 5.0 or higher
- FireFox
- Safari
- First time client installation, uninstall and upgrade requires administrator privileges on the client computer.

Server-Side Pre-Requisites

The SSL Network Extender server-side pre-requisites are listed below:

- The SSL Network Extender is a server side component, which is part of a specific Enforcement Module, with which the SSL Network Extender is associated. It may be enabled on the Security Gateway, already configured to serve as a Remote Access SecureClient Security Gateway.
- The specific Security Gateway must be configured as a member of the Remote Access Community, and configured to work with Visitor Mode. This will not interfere with SecureClient functionality, but will allow SecureClient users to utilize Visitor Mode.
- The same access rules are configured for both SecureClient and SSL Network Extender users.
- If you want to use Endpoint Security on Demand, you should install the ESOD server or the ESOD configuration tool. Customers can download the ESOD server from <http://www.checkpoint.com/products/clientless/index.html> along with its documentation.

Features

The SSL Network Extender features are listed below:

- Easy installation and deployment.
- Intuitive and easy interface for configuration and use.
- The SSL Network Extender mechanism is based on Visitor Mode and Office Mode.
- Automatic proxy detection is implemented.
- Small size client: Download size of SSL Network Extender package < 400K; after installation, size of SSL Network Extender on disk is approximately 650K.
- All Security Gateway authentication schemes are supported: Authentication can be performed using a certificate, Check Point password or external user databases, such as SecurID, LDAP, RADIUS and so forth.
- At the end of the session, no information about the user or Security Gateway remains on the client machine.
- Extensive logging capability, on the Security Gateway, identical to that in VPN-1 SecuRemote/SecureClient.
- High Availability Clusters and Failover are supported.
- SSL Network Extender Upgrade is supported.
- The SSL Network Extender supports the RC4 encryption method.
- Users can authenticate using certificates issued by any trusted CA that is defined as such by the system administrator in SmartDashboard.
- SSL Network Extender is now supported on IPSO.
- Endpoint Security on Demand prevents threats posed by Malware types, such as Worms, Trojan horses, Hacker's tools, Key loggers, Browser plug-ins, Adwares, Third party cookies, and so forth.
- SSL Network Extender can be configured to work in Hub Mode. VPN routing for remote access clients is enabled via Hub Mode. In Hub mode, all traffic is directed through a central Hub.

Configuring the SSL Network Extender

The following sections describe how to configure the server. Load Sharing Cluster Support, customizing the Web GUI, upgrading the SSL Network Extender client and Installation for Users without Administrator privileges are also discussed.

Configuring the Server

Before configuring the server, verify that you have a valid license for the SSL Network Extender.

Use `cpconfig` to verify that you have a valid license for the SSL Network Extender. Check Point software is activated with a License Key. You can obtain this License Key by registering the Certificate Key that appears on the back of the software media pack, in the Check Point Support Center (<http://supportcenter.checkpoint.com>).

Server-Side Configuration

The SSL Network Extender requires only server side configuration

Configuring the Security Gateway as a Member of the Remote Access Community

1. Open SmartDashboard, select the Security Gateway object on the Network Object tab of the Objects Tree.

The **General Properties** window is displayed.

2. Verify that the **IPsec VPN** blade is selected and click **OK**.
3. Select **VPN in the objects tree on the left hand side**.
4. Verify that the module participates in the Remote Access Community. If not, add the module to the Remote Access Community.
5. In the **Topology Tab** of the **Security Gateway Properties** page, configure the VPN Domain for SSL Network Extender, in the same way that you configure it for SecureClient



Note - You can use the VPN Domain to configure SSL Network Extender to work in Hub Mode. All traffic is then directed through a central Hub. You can also use the "Set domain for Remote Access Community ..." button on the same tab to create different encryption domain for Remote Access clients that connect to the Security Gateway (see Configuring Selective Routing).

6. Configure Visitor Mode, as described in the "Resolving Connectivity Issues" chapter. Configuring Visitor Mode doesn't interfere with regular SecureClient users' functionality. It merely allows SecureClient users to enable Visitor Mode. (For a description of Visitor Mode, refer to Visitor Mode (on page 276).)



Note - The SSL Network Extender uses TCP 443 (SSL) to establish a secure connection with VPN. The IPSO platform uses TCP 443 (SSL) for remote administration purposes. Another port may be assigned to the SSL Network Extender, however, this is not recommended, as most proxies do not allow ports other than 80 and 443. Instead, it is strongly recommended that you assign the IPSO platform web user interface to a port other than 443.

7. To change a Voyager port on an IPSO platform, run:

```
voyager -e x -S <port number> (x represents the encryption level.)
```

For more information, run: `voyager -h`

8. Select **IPSec VPN > Office Mode**.
9. Configure Office Mode, as described in the "Office Mode" chapter. (For a description, refer to Office Mode (on page 166).)



Note - Office Mode support is mandatory on the Security Gateway side

10. Configure Users and Authentication.

Configuring the Gateway to Support the SSL Network Extender



Note - If the Mobile Access blade is active on a Security Gateway, SSL Network Extender works through Mobile Access and not IPsec VPN. In this case, SSL Network Extender must be configured through the Mobile Access blade. If you already had SSL Network Extender configured on an IPsec VPN Security Gateway and then you enable the Mobile Access blade, you must reconfigure SSL Network Extender for the Mobile Access blade.

To configure the SSL Network Extender:



Note - You must configure each Security Gateway that will be using the SSL Network Extender

1. Select **Remote Access > SSL Network Extender**.
2. Select **SSL Network Extender**.
3. Select the server side certificate with which the Security Gateway will authenticate from the drop-down list.
4. Click **OK**.

Configuring the SSL Network Extender

1. Select **Policy > Global Properties > Remote Access > SSL Network Extender**. The **SSL Network Extender Global Properties** window is displayed.
2. Select the user authentication method, employed by the SSL Network Extender, from the drop-down list. The options are:
 - **Certificate:** The system will authenticate the user *only* via a certificate. Enrollment is not allowed.
 - **Certificate with enrollment:** The system will authenticate the user *only* via a certificate. Enrollment is allowed. If the user does not have a certificate, he/she can enroll using a registration key, received previously from the system administrator.
 - **Legacy:** (Default) The system authenticates the user via his/her **Username** and **Password**.
 - **Mixed:** The system attempts to authenticate the user via a certificate. If the user does not have a valid certificate, the system attempts to authenticate the user via his/her **Username** and **Password**.

Management of Internal CA Certificates

If the administrator has configured **Certificate with Enrollment** as the user authentication scheme, the user can create a certificate for his/her use, by using a registration key, provided by the system administrator.

To create a user certificate for enrollment:

1. Follow the procedure described in "The Internal Certificate Authority (ICA) and the ICA Management Tool" in the *R75.40 Security Management Server Administration Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk67581>).



Note - In this version, enrollment to an External CA is not supported.

2. Browse to the ICA Management Tool site, **<https://<mngmt IP>:18265>**, and select **Create Certificates**.
3. Enter the user's name, and click **Initiate** to receive a Registration Key, and send it to the user.

When the user attempts to connect to the SSL Network Extender, without having a certificate, the **Enrollment** window is displayed, and he/she can create a certificate for his/her use by entering the Registration Key, received from the system administrator.

For a description of the user login experience, refer to Downloading and Connecting the Client (on page 260).



Note - The system administrator can direct the user to the URL, **<http://<IP>/registration.html>**, to allow the user to receive a Registration Key and create a certificate, even if they do not wish to use the SSL Network Extender, at this time.

4. You can determine whether the SSL Network Extender will be upgraded automatically, or not. Select the client upgrade mode from the drop-down list. The options are:
 - **Do not upgrade:** Users of older versions will not be prompted to upgrade.

- **Ask user:** (Default) Ask user whether or not to upgrade, when the user connects.
- **Force upgrade:** Every user, whether users of older versions or new users will download and install the newest SSL Network Extender version.



Note - The Force Upgrade option should only be used in cases where the system administrator is sure that all the users have administrator privileges. Otherwise, the user will not be able to connect to and use the SSL Network Extender.

For a description of the user upgrade experience, refer to Downloading and Connecting the Client (on page 260).

5. You can determine whether the SSL Network Extender client will support the RC4 encryption method, as well as 3DES. (RC4 is a faster encryption method.) Select the supported encryption method from the drop-down list. The options are:
 - **3DES only:** (Default) The SSL Network Extender client supports 3DES, only.
 - **3DES or RC4:** The SSL Network Extender client supports the RC4 encryption method, as well as 3DES.
6. You can determine whether the SSL Network Extender will be uninstalled automatically, when the user disconnects. Select the desired option from the drop-down list. The options are:
 - **Keep installed:** (Default) Do not uninstall. If the user wishes to uninstall the SSL Network Extender, he/she can do so manually.
 - **Ask user whether to uninstall:** Ask user whether or not to uninstall, when the user disconnects.
 - **Force uninstall:** Always uninstall automatically, when the user disconnects.

For a description of the user disconnect experience, refer to Uninstall on Disconnect (on page 265).



Note - The Uninstall on Disconnect feature will not ask the user whether or not to uninstall, and will not uninstall the SSL Network Extender, if a user has entered a suspend/hibernate state, while he/she was connected.

7. You can determine whether Endpoint Security on Demand will be activated, or not. When ESOD is activated, users attempting to connect to the SSL Network Extender will be required to successfully undergo an ESOD scan before being allowed to access the SSL Network Extender. Select the desired option from the drop-down list. The options are:
 - None
 - Endpoint Security on Demand

Fetching the xml Configuration File

After installing the ESOD server and configuring it, you must fetch the xml config file from the ESOD server by performing the following steps:

1. Open a browser on any machine.
2. Browse to **http://<site ip>/<site name or virtual directory>/sre/ report.asp** and save the displayed XML file to disk, using **Save As**.
3. Copy the XML file to `$FWDIR/conf/extender/request.xml` on the Security Gateway.

Upgrading ESOD



Note - At present, the Dynamic ESOD Update feature is not supported.

You can manually upgrade ESOD as follows:

1. Replace the `ICSScanner.cab` file, under `$FWDIR/conf/extender`, with the new package.
2. Edit the file `ics.html`, under `$FWDIR/conf/extender`, as follows:
3. Search for `#Version=` and replace the current value with the new version.
4. Save.

Configuring ESOD Policies

On the Security Management server:



Note - Make sure that Endpoint Security on Demand is enabled in the **Global Properties > Remote Access > SSL Network Extender** page.

1. Navigate to the `$FWDIR/lib` directory.
2. Backup the `vpn_table.def` file.
3. Change the file name `vpn_table_HFA.def` to `vpn_table.def`.

On the Security Gateway:

1. Using the ESOD server, or ESOD configuration Tool (which can be downloaded from the Check Point download center), create xml policy files for each group and place them in `$FWDIR/conf/extender`.
2. You can create a default policy file, named `request.xml`. This is only optional, and will be used when no group is given.
3. In the `$FWDIR/conf` folder, create a file called `ics.group`. This should be a text file, in which, each row lists a group name and its policy xml file.

Example of **ics.group** file:

```
Group1 group1.xml
Group2 group2.xml
Group3 defGroup.xml
Group4 defGroup.xml
```

Important notes about the `ics.group` file:

- The group name must be the same as its name in SmartDashboard.
 - Several groups can register to the same xml file.
 - Each group must appear only once in the `ics.group` file.
 - Only groups that are listed in the `ics.group` file will use their specific xml files. Groups that are not listed in the `ics.group` file will try to use the default policy, located in the `request.xml` file. If the `request.xml` file does not exist, an error will be returned.
- The default xml file, `request.xml`, cannot appear in the `ics.group` file.
1. After creating the `ics.group` file (or after any change has been made), install policy.
 2. Run `cpstop` and then `cpstart` on the Security Gateway.
 3. Each user should be assigned the specific URL that matches his group. The URL should be in the format: `https://hostIP/<groupName>_ics.html`
For example, all users belonging to "group1" will surf to the assigned URL:
`https://10.10.10.10/group1_ics.html`.

For troubleshooting tips, see Troubleshooting (see "[Troubleshooting SSL Network Extender](#)" on page 269).

Load Sharing Cluster Support

The SSL Network Extender provides Load Sharing Cluster Support.

To provide Load Sharing Cluster Support:

1. Double-click the **Security Gateway Cluster Object** on the **Network Object** tab of the Objects Tree. The **Security Gateway Cluster Properties** window is displayed.



Note - A Load Sharing Cluster must have been created before you can configure use of sticky decision function.

2. Select **Cluster XL**. The **Cluster XL** tab is displayed.
3. Click **Advanced**. The **Advanced Load Sharing Configuration** window is displayed.

4. Select **Use Sticky Decision Function**. When the client connects to the cluster, all its traffic will pass through a single Security Gateway. If that member Security Gateway fails, the client will reconnect transparently to another cluster member and resume its session.
5. Select **Security Gateway Cluster Object > Remote Access > Office Mode**. When defining Office Mode, for use with Load Sharing Clusters, only the **Manual (using IP pool)** method is supported.

Customizing the SSL Network Extender Portal

You can modify the SSL Network Extender Portal by changing skins and languages.

Configuring the Skins Option

To configure the Skins Option:

The **skin** directory is located under `$FWDIR/conf/extender` on the SSL Network Extender Security Gateways.

There are two subdirectories. They are:

- **chkp**: contains skins that Check Point provides by default. At upgrade, this subdirectory may be overwritten.
- **custom**: contains skins defined by the customer. If **custom** does not exist yet, create it. At upgrade, this subdirectory is not overwritten. New skins are added in this subdirectory.

Disabling a Skin

1. Enter the specific skin subdirectory, under **custom**, that is to be disabled and create a file named **disable**. This file may be empty.
2. If the specific skin does not exist under **custom**, create it and then create a file within it named **disable**.
3. Install Policy. The next time that the user connects to the SSL Network Extender portal, this skin will not be available to him/her.

Example

```
cd $FWDIR/conf/extender/skin/custom
mkdir skin1
touch disable
```

Install Policy.

Creating a Skin

1. Enter the **custom** subdirectory.
2. Create a folder with the desired skin name.



Note - Verify that this name is not already used in **chkp**. If it is, the new skin definition will override the existing skin definition (as long as the new skin definition exists). Once you have deleted the new skin definition, the **chkp** skin definition will once again be used.

Each skin folder must contain the following five style sheets:

- **help_data.css**: The main OLH page uses this style sheet.
- **help.css**: The inner frame on the OLH page uses this style sheet.
- **index.css**: The ESOD pages, and the main SSL Network Extender portal page use this style sheet.
- **style.css**: All login pages use this style sheet.
- **style_main.css**: The main SSL Network Extender Connection page, Proxy Authentication page and Certificate Registration page use this style sheet.



Note - It is recommended that you copy the aforementioned files from another **chkp** skin, and then modify them as desired.

3. Install Policy after creating the new skin.

Example

Add your company logo to the main SSL Network Extender portal page.

```
cd $FWDIR/conf/extender/skin/custom
```

```
mkdir <skin_name>
```

```
cd <skin_name>
```

```
copy ../../chkp/skin2/* .
```

Place logo image file in this directory

Edit `index.css`.

Goto `.company_logo` and replace the existing URL reference with a reference to the new logo image file.

Save.

Install Policy.



Note - No spaces are allowed in the `<skin_name>`

Configuring the Languages Option

To configure the Languages Option:

The `languages` directory is located under `$FWDIR/conf/extender` on the SSL Network Extender Security Gateways.

There may be two subdirectories. They are:

- `chkp`: contains languages that Check Point provides by default. At upgrade, this subdirectory may be overwritten.
- `custom`: contains languages defined by the customer. If `custom` does not exist yet, create it. At upgrade, this subdirectory is not overwritten. New languages are added in this subdirectory.

Disabling a Language

1. Enter the specific language subdirectory, under `custom`, that is to be disabled (if it exists) and create a file named `disable`. This file may be empty.
2. If the specific language does not exist under `custom`, create it and then create a file within it named `disable`.
3. Install Policy. The next time that the user connects to the SSL Network Extender portal, this language will not be available to him/her.

Adding a Language

1. Enter the `custom` subdirectory.
2. Create a folder with the desired language name.



Note - Verify that this name is not already used in `chkp`. If it is, the new language definition will override the existing language definition (as long as the new language definition exists). Once you have deleted the new language definition, the `chkp` language definition will once again be used.

3. Copy the `messages.js` file of an existing `chkp` language to this folder.
4. Edit the `messages.js` file and translate the text bracketed by quotation marks.
5. Save.
6. Install Policy after adding the new language.

Example

```
cd $FWDIR/conf/extender/language
```

```
mkdir custom
```

```
cd custom
mkdir <language_name>
cd <language_name>
copy ../../chkp/english/messages.js
```

Edit the `messages.js` file and translate the text bracketed by quotation marks.

Save.

In `custom/english/messages.js`, add a line as follows:

```
<language_name>="translation of language_name";
```

Install Policy.



Note - No spaces are allowed in the `<language_name>`

Modifying a Language

1. Enter the `custom` subdirectory.
2. Create a folder with a language name that matches the `chkp` language folder to be modified.
3. Create an empty `messages.js` file, and insert only those messages that you want to modify, in the following format:

```
<variable_name>="<desired text>";
```



Note - For reference, refer to the `messages.js` file, located in `chkp/<language>`.

Installation for Users without Administrator Privileges

The SSL Network Extender usually requires Administrator privileges to install the ActiveX component. To allow users that do not have Administrator privileges to use the SSL Network Extender, the Administrator can use his/her remote corporate installation tools (such as, Microsoft SMS) to publish the installation of the SSL Network Extender, as an MSI package, in configuring the SSL Network Extender.

To prepare the SSL Network Extender MSI package:

1. Move the `extender.cab` file, located in `$FWDIR/conf/extender`, to a Windows machine and open the file using WinZip.
2. Extract the `cpextender.msi`, and use as an MSI package, for remote installation.

On Windows Vista, Mac and Linux, it is possible to install SSL Network Extender for users that are not administrators, if the user knows the admin password. In this case, perform a regular SSL Network Extender installation and supply the administrator password when asked.

SSL Network Extender User Experience

This section describes the user experience, including downloading and connecting the SSL Network Extender client, importing a client certificate, and uninstalling on disconnect.

Configuring Microsoft Internet Explorer

Check Point SSL Network Extender uses ActiveX controls and cookies to connect to applications via the Internet. These enabling technologies require specific browser configuration to ensure that the applications are installed and work properly on your computer. The Trusted Sites Configuration approach includes the SSL Network Extender Portal as one of your Trusted Sites. This approach is highly recommended, as it does not lessen your security. Please follow the directions below to configure your browser.

Trusted Sites Configuration

1. In Internet Explorer, select **Tools > Internet Options > Security**.
2. Select **Trusted sites**.
3. Click **Sites**.
4. Enter the URL of the SSL Network Extender Portal and click **Add**.
5. Click **OK** twice.

About ActiveX Controls

ActiveX controls are software modules, based on Microsoft's Component Object Model (COM) architecture. They add functionality to software applications by seamlessly incorporating pre-made modules with the basic software package.

On the Internet, ActiveX controls can be linked to Web pages and downloaded by an ActiveX-compliant browser. ActiveX controls turn Web pages into software pages that perform like any other program.

The SSL Network Extender can use ActiveX control in its applications. To use ActiveX you must download the specific ActiveX components required for each application. Once these components are loaded, you do not need to download them again unless upgrades or updates become available. If you do not want to use an ActiveX component you may work with a Java Applet.



Note - You must have Administrator rights to install or uninstall software on Windows XP Professional, as well as on the Windows 2000 operating systems.

Downloading and Connecting the Client

The following section discusses how to download and connect the SSL Network Extender.

To Download the Client:

1. Using Internet Explorer, browse to the SSL Network Extender portal of the Security Gateway at <https://<GW name or IP>>. The following Security Alert message may be displayed

The site's security certificate has been issued by an authority that you have not designated as a trusted CA. Before you connect to this server, you must trust the CA that signed the server certificate. (The system administrator can define which CAs may be trusted by the user.) You can view in the certificate in order to decide if you wish to proceed.



Note - The administrator can direct the user to the URL, <http://<mngmt IP>:18264>, to install this CA certificate, thereby establishing trust, and avoiding future displays of this message.

2. Click **Yes**.

If Endpoint Security on Demand is enabled, the **ESOD web page** is displayed.

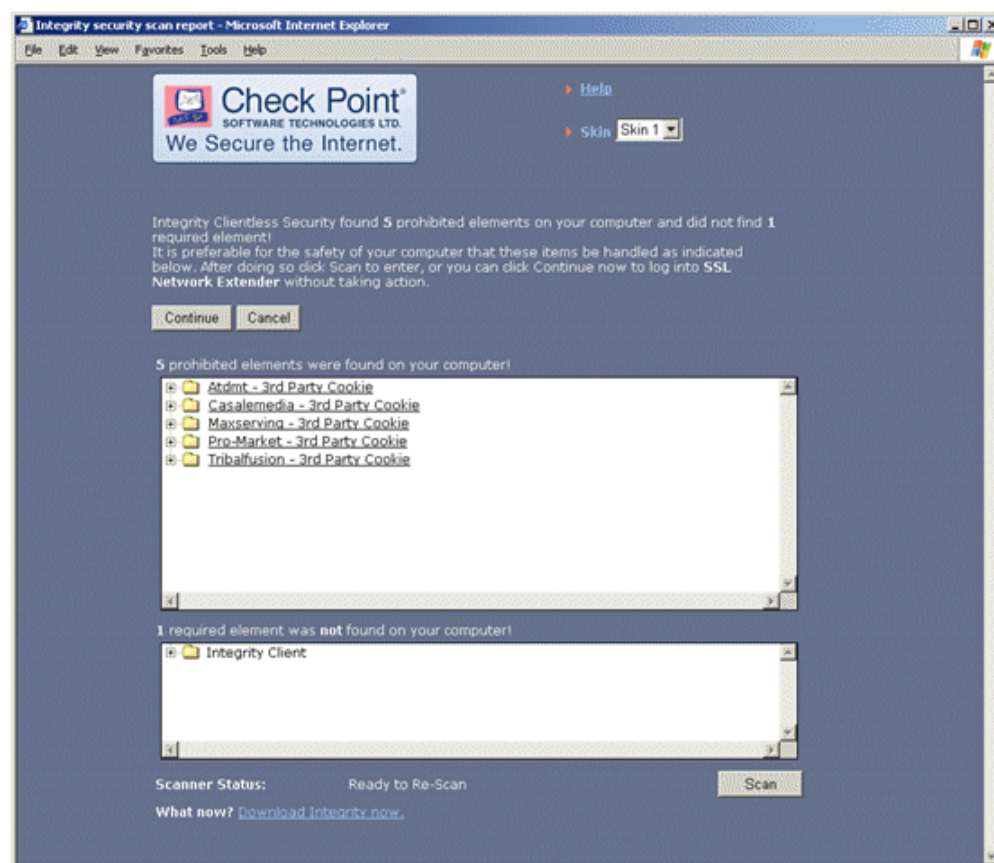
If this is the first time that the user is scanned with ESOD, the user should install the ESOD ActiveX object.

If this is the first time that ESOD is used, the following **Server Confirmation** window appears. The user is asked to confirm that the listed ESOD server is identical to the organization's site for remote access.

3. Click one of the following:

- **No:** an error message is displayed and the user is denied access.
- **Yes:** the ESOD client continues the software scan. Moreover, if the **Save this confirmation for future use** check box is selected, the **Server Confirmation** window will not appear the next time the user attempts to login.

Once the user has confirmed the ESOD server, an automatic software scan takes place on the client's machine. Upon completion, the scan results and directions on how to proceed are displayed as shown below.



ESOD not only prevents users with potentially harmful software from accessing your network, but also requires that they conform to the corporate antivirus and firewall policies, as well. A user is defined as having successfully passed the ESOD scan only if he/she successfully undergoes scans for *Malware*, *Anti-Virus*, and *Firewall*. Each malware is displayed as a link, which, if selected, redirects you to a data sheet describing the detected malware. The data sheet includes the name and a short description of the detected malware, what it does, and the recommended removal method/s.

The options available to the user are configured by the administrator on the ESOD server. The options are listed in the following table:

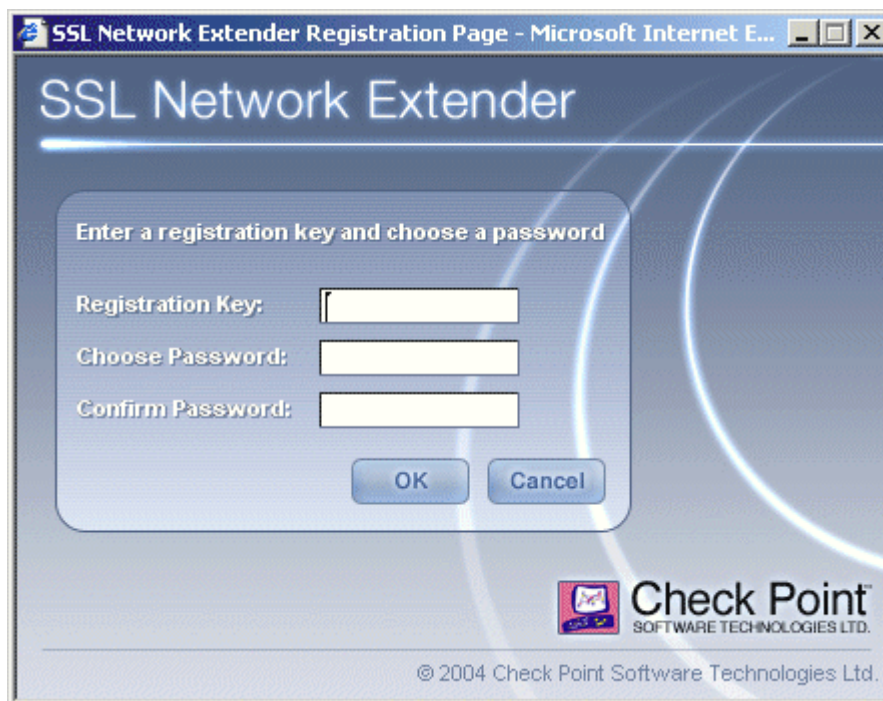
| Scan Option | Description |
|-------------|--|
| Scan Again | Allows a user to rescan for malware. This option is used in order to get refreshed scan results, after manually removing an undesired software item. |
| Cancel | Prevents the user from proceeding with the portal login, and closes the current browser window. |
| Continue | Causes the ESOD for Mobile Access client to disregard the scan results and proceed with the log on process. |

- From the **Scan Results**, you can select a different language from the **Language** drop-down list. If you change languages, while connected to the SSL Network Extender portal, you will be informed that if you continue the process you will be disconnected, and must reconnect.
- From the **Scan Results**, you can select a different skin from the **Skin** drop-down list. You can change skins, while connected to the SSL Network Extender portal.
- Click **Continue**.
 - If the configured authentication scheme is **User Password Only**, an **SSL Network Extender Login** window is displayed.
Enter the **User Name** and **Password** and click **OK**.



Note - If user authentication has been configured to be performed via a 3rd party authentication mechanism, such as SecurID or LDAP, the Administrator may require the user to change his/her PIN, or Password. In such a case, an additional Change Credentials window is displayed, before the user is allowed to access the SSL Network Extender.

- If the configured authentication scheme is **Certificate without Enrollment**, and the user already has a certificate. If the user does not already have a certificate, access is denied.
- If the configured authentication scheme is **Certificate with Enrollment**, and the user does not already have a certificate, the **Enrollment** window is displayed:



Enter the **Registration Key** and select PKCS#12 Password.

Click **Ok**. The PKCS#12 file is downloaded.

At this point the user should open the file and utilize the Microsoft Certificate Import wizard as follows.



Note - It is strongly recommended that the user set the property **Do not save encrypted pages to disk** on the **Advanced** tab of the **Internet Properties** of Internet Explorer. This will prevent the certificate from being cached on disk.

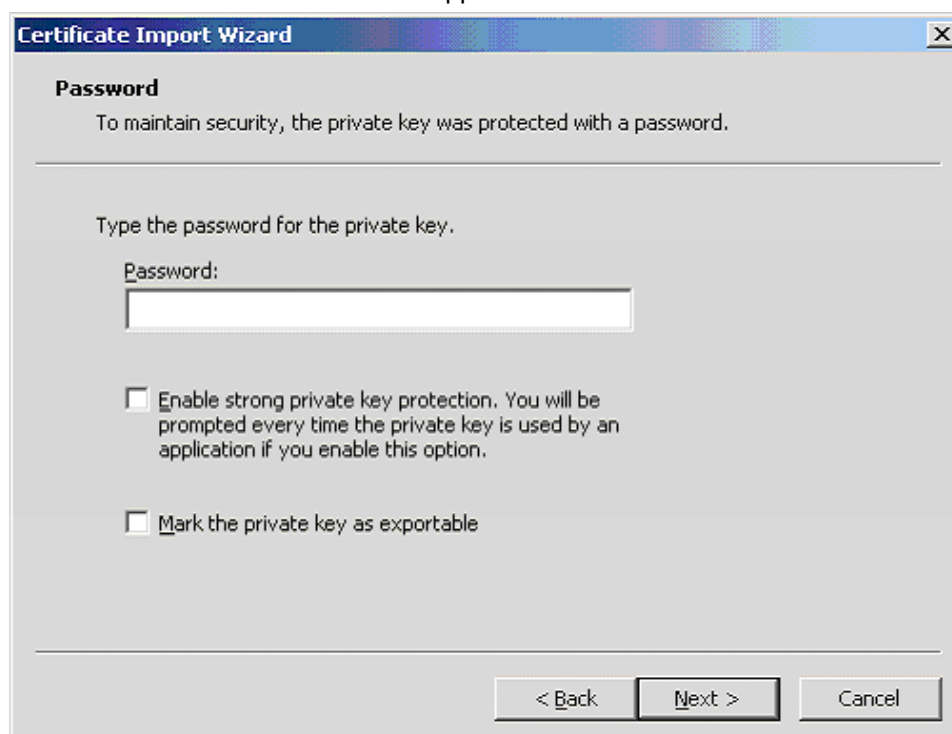
Importing a Client Certificate with the Microsoft Certificate Import Wizard to Internet Explorer

Importing a client certificate to Internet Explorer is acceptable for allowing access to either a home PC with broadband access, or a corporate laptop with a dial-up connection. The client certificate will be automatically used by the browser, when connecting to an SSL Network Extender Security Gateway.

To import a client certificate:

1. Open the downloaded PKCS#12 file. The following **Certificate Import Wizard** opens.
2. Click **Next**. The **File to Import** window appears:
The P12 file name is displayed.

- Click **Next**. The **Password** window appears:



It is strongly recommended that the user enable **Strong Private Key Protection**. The user will then be prompted for consent/credentials, as configured, each time authentication is required. Otherwise, authentication will be fully transparent for the user.

- Enter your password, click **Next** twice. If the user enabled **Strong Private Key Protection**, the following **Importing a New Private Exchange Key** window appears:

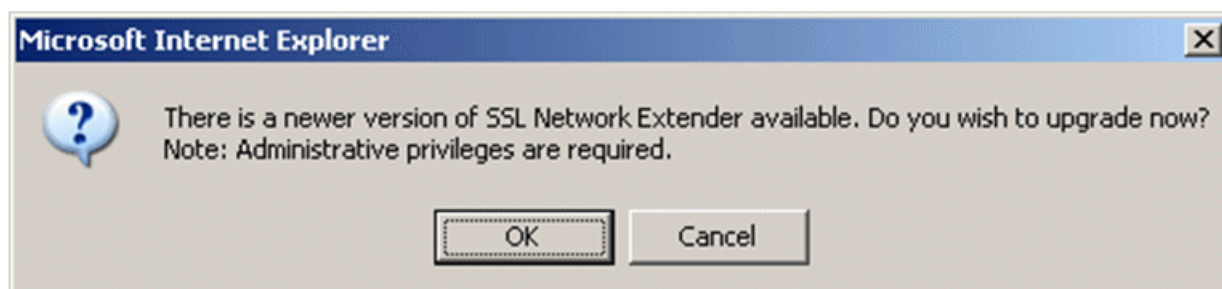


- If you click **OK**, the Security Level is assigned the default value **Medium**, and the user will be asked to consent each time the certificate is required for authentication.
 - If you click **Set Security Level**, the **Set Security Level** window appears. Select either **High** or **Medium** and click **Next**.
- Click **Finish**. The **Import Successful** window appears.
 - Click **OK**.
 - Close and reopen your browser. You can now use the certificate that has now been imported for logging in.

8. If you are connecting to the SSL Security Gateway for the first time, a VeriSign certificate message appears, requesting the user's consent to continue installation.

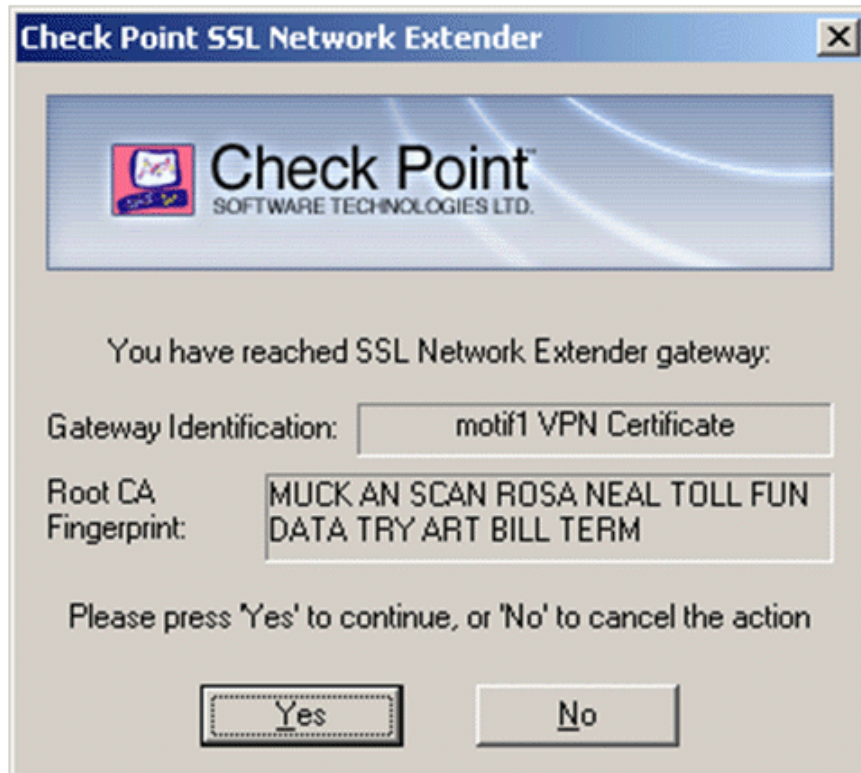


- If you connect using Java Applet, a Java security message will appear. Click **Yes**.
- If the system administrator configured the upgrade option, the following Upgrade Confirmation window is displayed:



- If you click **OK**, you must reauthenticate and a new SSL Network Extender version is installed.
- If you click **Cancel**, the SSL Network Extender connects normally. (The **Upgrade Confirmation** window will not be displayed again for a week.) The **SSL Network Extender** window appears. A **Click here to upgrade** link is displayed in this window, enabling the user to upgrade even at this point. If you click on the **Click here to upgrade** link, you must reauthenticate before the upgrade can proceed.

9. At first connection, the user is notified that the client will be associated with a specific Security Gateway. Click **Yes**.



The server certificate of the Security Gateway is authenticated. If the system Administrator has sent the user a *fingerprint*, it is strongly recommended that the user verify that the root CA fingerprint is identical to the fingerprint, sent to him/her.

The system Administrator can view and send the fingerprint of all the trusted root CAs, via the **Certificate Authority Properties** window in SmartDashboard.

10. If the user is using a proxy server that requires authentication, the **Proxy Authentication** pop-up is displayed. The user must enter his/her proxy username and password, and click **OK**.
11. If you are connected with Windows Vista, a **Windows Firewall** message will appear. Click **Unblock**.
You may work with the client as long as the **SSL Network Extender Connection** window, shown below, remains open, or minimized (to the System tray).

Once the SSL Network Extender is initially installed, a new Windows service named Check Point SSL Network Extender and a new virtual network adapter are added. This new network adapter can be seen by typing `ipconfig /all` from the Command line.



Note - The settings of the adapter and the service must not be changed. IP assignment, renewal and release will be done automatically.

Both the virtual network adapter and the Check Point SSL Network Extender service are removed during the product uninstall.



Note - The Check Point SSL Network Extender service is dependent on both the virtual network adapter and the DHCP client service. Therefore, the DHCP client service must not be disabled on the user's computer.

There is no need to reboot the client machine after the installation, upgrade, or uninstall of the product.

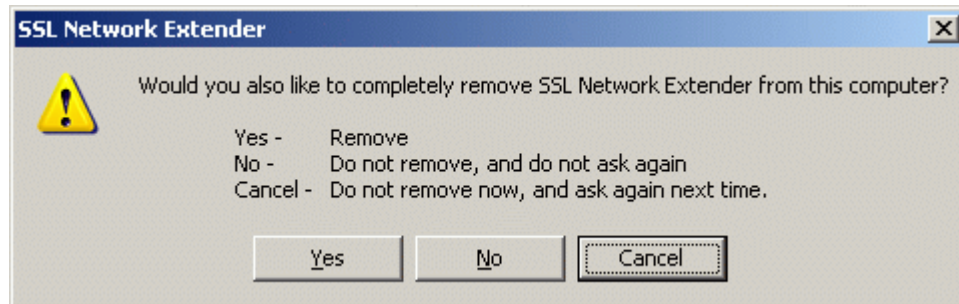
12. When you finish working, click **Disconnect** to terminate the session, or when the window is minimized, right-click the icon and click **Disconnect**. The window closes.

Uninstall on Disconnect

If the administrator has configured **Uninstall on Disconnect** to ask the user whether or not to uninstall, the user can configure **Uninstall on Disconnect** as follows.

To set Uninstall on Disconnect:

1. Click **Disconnect**. The **Uninstall on Disconnect** window is displayed, as shown in the following figure.



2. Click **Yes** to Uninstall.
If you select **Cancel**, the SSL Network Extender will not be uninstalled.
If you click **Yes**, the **Uninstall on Disconnect** window will be displayed the next time the user connects to the SSL Network Extender.

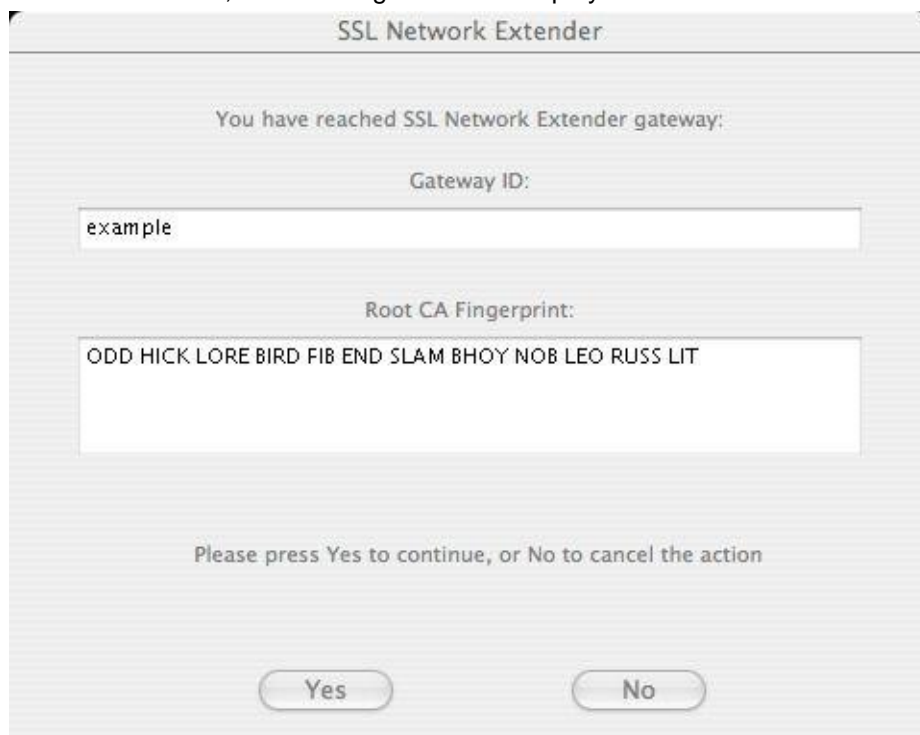
Using SSL Network Extender on Linux / Mac Operating Systems

There are two methods to access Network Applications using Linux.:

- Java
- Command Line

Java

1. When connecting for the first time, the SSL Network Extender installation archive package is downloaded.
This process is similar to the Windows Java installation.
2. If the user does not have root permissions, the user is prompted to enter a root password in order to install the package. Enter the password and press **Enter**.
After the installation is finished, the applet will try to connect.
If it is the first time, the following window is displayed:



If the system Administrator has sent the user a fingerprint, it is strongly recommended that the user verify that the server certificate fingerprint is identical to the **Root CA Fingerprint** seen in the window.

3. Click **Yes** to confirm.

Command Line

To download the SSL Network Extender installation archive package:

1. In the **Network Applications Settings** window, click on **click here** in the sentence **For Linux command line SSL Network Extender installation click here**. The Shell archive package is downloaded to the users home directory.

Before running the installation script, make sure execute permissions are available on the file. Use the command **chmod +x snx_install.sh** to add execution permissions.

2. Download the SSL Network Extender manual installation.

The following links will appear:

- Download MSI installation package for Windows
- Download command line SSL Network Extender for Linux
- Download command line SSL Network Extender for Macintosh

3. Select the appropriate operating system.

The Shell archive package is downloaded to the user's home directory.

4. To execute the installation script run `snx_install.sh`.

If the user does not have root permissions, the user is prompted to enter a root password in order to install the package. Enter the password and press **Enter**.

5. To connect after installation, perform the following steps in the command Line:

----- Connect using the SNX command

```
Server_1:/ snx -s <server name> -u <user name>
```

Check Point's Linux SNX

build 5416000XX

----- Enter Password

Please enter your password:

SNX authentication:

Please confirm the connection to Security Gateway: <server name>

Root CA fingerprint: MOOD TREK ALP EEL FILM MESH RUBY BELA MACE

TEND DRY PUT

----- Accept Fingerprint if it is valid

Do you accept? [y]es/[N]o: y

SNX - connected

Session parameters:

=====

Office Mode IP : 9.1.3.9

DNS Server : 19.18.17.16

DNS Suffix : domain.com

Timeout : 10 minutes

6. To disconnect after installation perform the following steps in the command line:

----- Disconnect by running the following

```
Server_1:/ snx -d
```

SNX - Disconnecting... done.

SSL Network Extender Command Attributes

Command Attributes for SSL Network Extender

| Attributes | Description |
|--|--|
| snx -f <configuration file> | Run SSL Network Extender using parameters defined in a configuration file other than the default name or location. |
| snx -d | Disconnect from Mobile Access |
| snx -s <server> | Specify server IP or hostname |

| Attributes | Description |
|--|---|
| snx -u <username> | Specify a valid user |
| snx -c <certificate file> | Specify which certificate is used to authenticate. |
| snx -l <CA directory> | Define the directory where CA's certificates are stored. |
| snx -p <port> | Change the HTTPS port. (default port is TCP 443). |
| snx -g | Enable debugging. snx.elg log file is created. |
| snx -e <cipher> | Force a specific encryption algorithm. Valid values - RC4 and 3DES. |

Configuration File Attributes

It is possible to predefine SSL Network Extender attributes by using a configuration file (`.snxrc`) located in the users home directory. When the SSL Network Extender command SSL Network Extender is executed, the attributed stored in the file are used by the SSL Network Extender command. To run a file with a different name execute the command `snx -f <filename>`.

Configuration File Attributes

| Attributes | Description |
|--------------------|--|
| server | Change the HTTPS port. (default port is TCP 443). |
| sslport | Change the HTTPS port. (default port is TCP 443). |
| username | Specify a valid user |
| certificate | Specify which certificate is used to authenticate |
| calist | Define the directory where CA's certificates are stored. |
| reauth | Enable reauthentication. Valid values -{yes, no} |
| debug | Enable debugging. <code>snx.elg</code> log file is created. Valid values {yes, no}. To activate debugging when running java, create a <code>.snxrc</code> file with the line <code>debug yes</code> in the home directory. |
| cipher | Force a specific encryption algorithm. Valid values: RC4 and 3DES |
| proxy_name | Define a Proxy hostname |
| proxy_port | Define a proxy port |
| proxy_user | Define a proxy user |
| proxy_pass | Define a password for proxy authentication |



Note - Proxy information can only be configured in the configuration file and not directly from the command line.

Removing an Imported Certificate

If you imported a certificate to the browser, it will remain in storage until you manually remove it. It is strongly recommended that you remove the certificate from a browser that is not yours.

To remove the imported certificate:

1. In the **Internet Options** window of your browser, access the **Content** tab.
2. Click **Certificates**. The **Certificates** window is displayed:
3. Select the certificate to be removed, and click **Remove**.

Troubleshooting SSL Network Extender

The following sections contain tips on how to resolve issues that you may encounter when using SSL Network Extender.

SSL Network Extender Issues

1. **All user's packets destined directly to the external SSL Network Extender Security Gateway will not be encrypted by the SSL Network Extender.**

If there is a need to explicitly connect to the gateway through the SSL tunnel, connect to the internal interface, which is part of the encryption domain.

2. **The SSL Network Extender gateway allows users to authenticate themselves via certificates. Therefore, when connecting to the SSL Network Extender gateway, the following message may appear: "The Web site you want to view requests identification. Select the certificate to use when connecting."**

In order not to display this message to the users, two solutions are proposed:

On the client computer, access the Internet Explorer. Under **Tools > Options > Security** tab, select **Local intranet > Sites**. You can now add the SSL Network Extender gateway to the Local intranet zone, where the Client Authentication pop-up will not appear. Click **Advanced**, and add the gateway's external IP or DNS name to the existing list.

On the client computer, access the Internet Explorer. Under **Tools > Options > Security** tab, select **Internet Zone > Custom Level**. In the **Miscellaneous** section, select **Enable** for the item **Don't prompt for client certificate selection when no certificates or only one certificate exists**. Click **OK**. Click **Yes** on the Confirmation window. Click **OK** again.



Note - This solution will change the behavior of the Internet Explorer for all Internet sites, so if better granularity is required, refer to the previous solution.

3. **If the client computer has SecuRemote/SecureClient software installed, and is configured to work in 'transparent mode', and its encryption domain contains SSL Network Extender gateway, or otherwise overlaps with the SSL Network Extender encryption domain, the SSL Network Extender will not function properly.**

To resolve this, disable the overlapping site in SecuRemote/SecureClient.

4. **If the client computer has SecuRemote/SecureClient software installed, and is configured to work in 'connect mode', and its encryption domain contains SSL Network Extender gateway, or otherwise overlaps with the SSL Network Extender encryption domain, the SSL Network Extender will not function properly.**

To resolve this, verify that the flag `allow_clear_traffic_while_disconnected` is **True** (which is the default value).

5. **SSL Network Extender connections cannot pass SCV rules. SecureClient users must be differentiated from SSL Network Extender users in order to allow the SecureClient connections to pass the SCV rules.**

One way to do this is to use the SCV capabilities in the rulebase. In **Traditional Mode** you can configure two types of rules, by selecting the Apply Rule Only if Desktop Configuration Options are verified. The selected (SCV) rules will pass only SecureClient connections, while the rules that were not selected will pass SecureClient and SSL Network Extender connections. When using **Simplified Mode**, the Administrator may specify services that will be excluded from SCV checking. Both SecureClient and SSL Network Extender clients attempting to access such services will be allowed access, even when not SCV verified. SCV will not be enforced on specified services for both types of clients.

ESOD Issues

1. **User did not pass the scan (a 'Continue' button is not displayed).**

The user probably did not match the policy requirements.

- If using "ESOD per User Group" feature – Verify that the user is using the correct policy.
- According to the policy, Explain the user how to remove the elements that are blocking him.

2. **User cannot access the given URL for his specific group.**

- Make sure that the group listed in the URL is listed in the ics.group file, with the correct xml file.
- Make sure that the xml file that is assigned to the group exists in **\$FWDIR/conf/extender**.
- Make sure Install Policy has been made since the ics.group file has changes.

3. **User has passed the ESOD scan, but gets a "Wrong ESOD Scan" error when trying to connect.**

This means that the user has passed the scan intended for a group that he does not belong to.

- Verify that the user is using the correct URL.
- Look at the SmartView Tracker. The log should state which xml file the user used for the scan.
- Make sure that this file is the same as the user's group file. If not, direct the user to the correct URL.

Chapter 31

Resolving Connectivity Issues

In This Chapter

| | |
|---|-----|
| The Need for Connectivity Resolution Features | 271 |
| Check Point Solution for Connectivity Issues | 271 |
| Overcoming NAT Related Issues | 271 |
| Overcoming Restricted Internet Access | 276 |
| Configuring Remote Access Connectivity | 279 |

The Need for Connectivity Resolution Features

While there are a few connectivity issues regarding VPN between Security Gateways, remote access clients present a special challenge. Remote clients are, by their nature, mobile. During the morning they may be located within the network of a partner company, the following evening connected to a hotel LAN or behind some type of enforcement or NATing device. Under these conditions, a number of connectivity issues can arise:

- Issues involving NAT devices that do not support fragmentation.
- Issues involving service/port filtering on the enforcement device

Check Point Solution for Connectivity Issues

Check Point resolves NAT related connectivity issues with a number of features:

- IKE over TCP
- Small IKE phase II proposals
- UDP encapsulation
- IPSec Path Maximum Transmission Unit (IPSec PMTU)

Check Point resolves port filtering issues with **Visitor Mode** (formally: *TCP Tunneling*).

Other Connectivity Issues

Other connectivity issues can arise, for example when a remote client receives an IP address that matches an IP on the internal network. Routing issues of this sort are resolved using Office mode. For more information see: Office Mode (on page [166](#)).

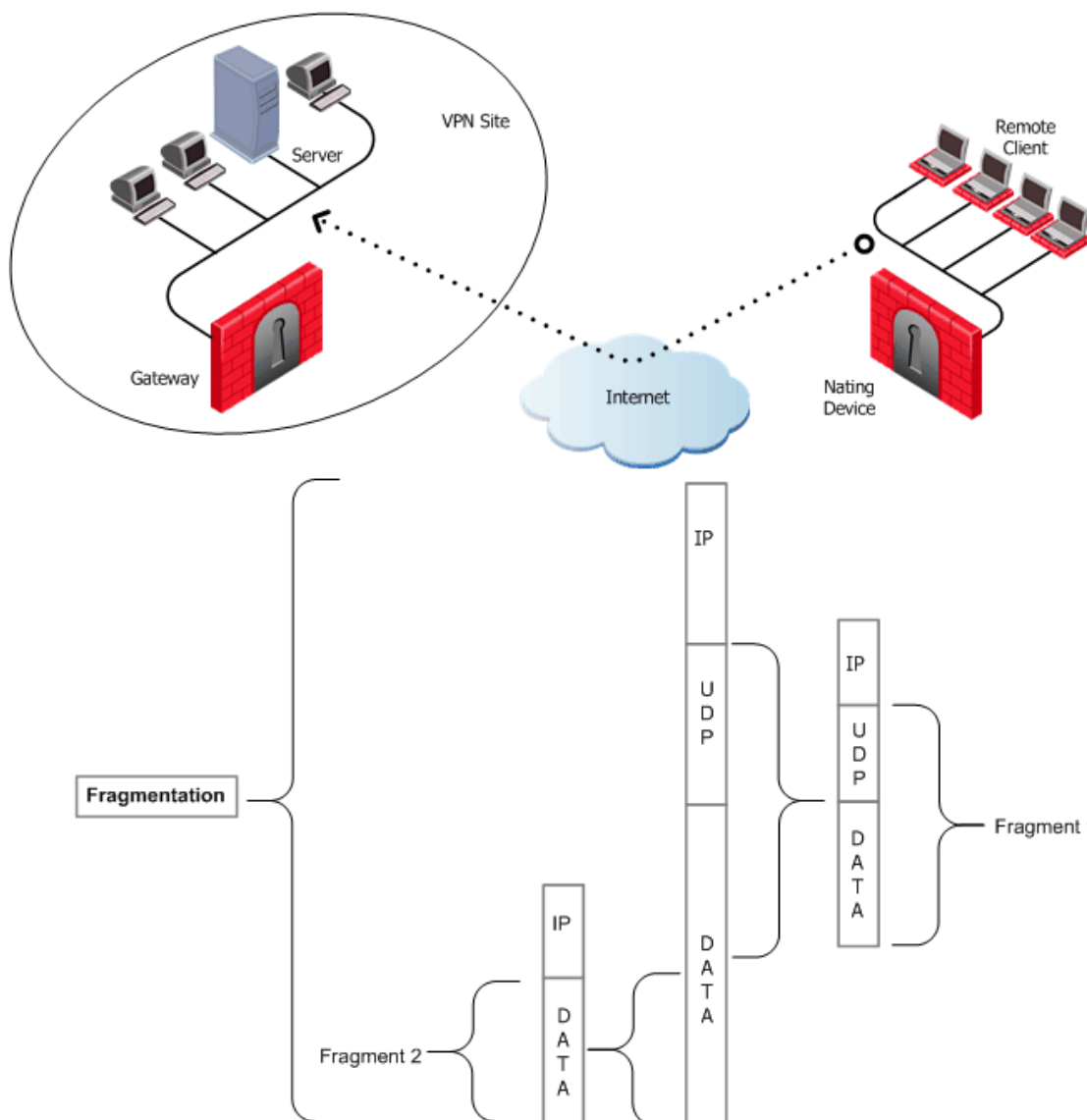
Other issues, such as Domain Name Resolution involving DNS servers found on an internal network protected by a Security Gateway, are resolved with *Split DNS*. For more information on Split DNS see: Remote Access Advanced Configuration (on page [227](#)).

Overcoming NAT Related Issues

NAT related issues arise with *hide* NAT devices that do not support packet fragmentation.

When a remote access client attempts to create a VPN tunnel with its peer Security Gateway, the IKE or IPSec packets may be larger than the Maximum Transmission Unit (MTU) value. If the resulting packets are greater than the MTU, the packets are fragmented at the Data Link layer of the Operating System's TCP/IP stack.

Problems arise when the remote access client is behind a hide NAT device that does not support this kind of packet fragmentation:



Hide NAT not only changes the IP header but also the port information contained in the UDP header. In Figure 31-1, the UDP packet is too long so the remote client fragments the packet. The first fragment consists of the IP header plus the UDP header and some portion of the data. The second fragment consists of only the IP header and the second data fragment. The NATing device does not know how to wait for all the fragments, reassemble and NAT them.

When the first fragment arrives, the NAT device successfully translates the address information in the IP header, and port information in the UDP header and forwards the packet. When the second fragment arrives, the NATing device cannot translate the port information because the second packet does not contain a UDP header; the packet is dropped. The IKE negotiation fails.

During IKE phase I

To understand why large UDP packets arise, we need to take a closer look at the first phase of IKE. During IKE phase I, the remote access client and Security Gateway attempt to authenticate each other. One way of authenticating is through the use of certificates. If the certificate or Certificate Revocation List (CRL) is long, large UDP packets result, which are then fragmented by the operating system of the remote client.



Note - If the VPN peers authenticate each other using pre-shared secrets, large UDP packets are not created; however, certificates are more secure, and thus recommended.

IKE Over TCP

IKE over TCP solves the problem of large UDP packets created during IKE phase I. The IKE negotiation is performed using TCP packets. TCP packets are not fragmented; in the IP header of a TCP packet, the DF flag ("do not fragment") is turned on. A full TCP session is opened between the peers for the IKE negotiation during phase I.

During IKE phase II

A remote access client does not have a policy regarding methods of encryption and integrity. Remote access clients negotiate methods for encryption and integrity via a series of proposals, and need to negotiate *all* possible combinations with the Security Gateway. This can lead to large UDP packets which are once again fragmented by the remote client's OS before sending. The NAT device in front of the remote client drops the packet that has no UDP header (containing port information). Again, the IKE negotiation fails.

Why not use IKE over TCP again, as in phase I?

IKE over TCP solves the fragmentation problem of long packets, but in phase II there are times when the Security Gateway needs to *initiate* the connection to the remote client. (Only the remote client initiates phase I, but either side can identify the need for a phase II renewal of keys; if the Security Gateway identifies the need, the Security Gateway initiates the connection.)

If the Security Gateway initiates the connection, the Security Gateway knows the IP address of the NATing device, but cannot supply a port number that translates to the remote client *behind* the NATing device. (The port number used during previous connections is only temporary, and can quickly change.) The NATing device cannot forward the connection correctly for the remote client; the connection initiated by the Security Gateway fails.

It is possible to use IKE over TCP, but this demands a TCP connection to be always open; the open session reserves the socket on the Security Gateway, taking up valuable system resources. The more reasonable solution is to keep open the port on the NATing device by sending UDP "keep alive" packets to the Security Gateway, and then performing IKE phase II in the usual way. However, there is still a need to shorten the UDP packets to prevent possible fragmentation.

Small IKE Phase II Proposals

Both Security Gateway and remote peer start the IKE negotiation by proposing a small number of methods for encryption and integrity. The more common methods are included in the small proposals.

If proposals match between the remote client and the Security Gateway, the proposed methods are used; if no match is found, a greater number of proposals are made. Usually a match is found with the small proposals, and fragmentation is no longer an issue. However, there are cases where a match is not found, and a larger number of proposals need to be made. (This will most likely happen in instances where the remote Security Gateway uses AES-128 for encryption, and AES-128 is not included in the small proposals.)

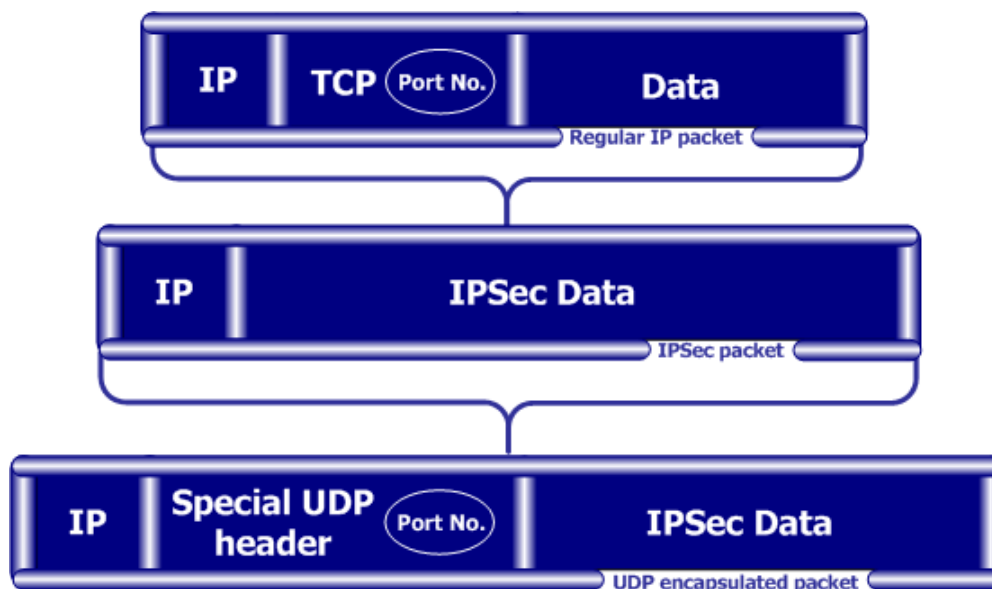
A greater number of proposals can result in larger UDP packets. These larger packets are once again fragmented at the Data Link Layer of the TCP/IP stack on the client, and then discarded by the hide NAT device that does not support fragmentation. In the case of AES-128, this method of encryption can be included in the small proposals by defining AES-128 as the preferred method.

During IPSec

NAT Traversal (UDP Encapsulation for Firewalls and Proxies)

Having successfully negotiated IKE phases I and II, we move into the IPSec stage. Data payloads encrypted with (for example) 3DES and hashed (for integrity) with MD5, are placed within an IPSec packet. However, this IPSec packet no longer contains a TCP or UDP header. A hide NAT device needs to translate the port information inside the header. The TCP/UDP header has been encrypted along with the data payload and can no longer be read by the NATing device.

A port number needs to be added; UDP Encapsulation is a process that adds a special UDP header that contains readable port information to the IPSec packet:



- IPSec packet encrypts the port information contained in the TCP header of a regular IP packet
- UDP encapsulation adds a UDP header containing another port number

The new port information is not the same as the original. The port number 2746 is included in both the source and destination ports. The NAT device uses the source port for the hide operation but the destination address and port number remains the same. When the peer Security Gateway sees 2746 as the port number in the destination address, the Security Gateway calls a routine to decapsulate the packet.

IPSec Path Maximum Transmission Units

IPSec Path MTU is a way of dealing with IPSec packet fragmentation. The Data Link layer imposes an upper limit on the size of the packets that can be sent across the physical network, **the Maximum Transmission Unit**, or MTU. Before sending a packet, the TCP/IP stack of the operating system queries the local interface to obtain its MTU. The IP layer of the TCP/IP stack compares the MTU of the local interface with the size of the packet and fragments the packet if necessary.

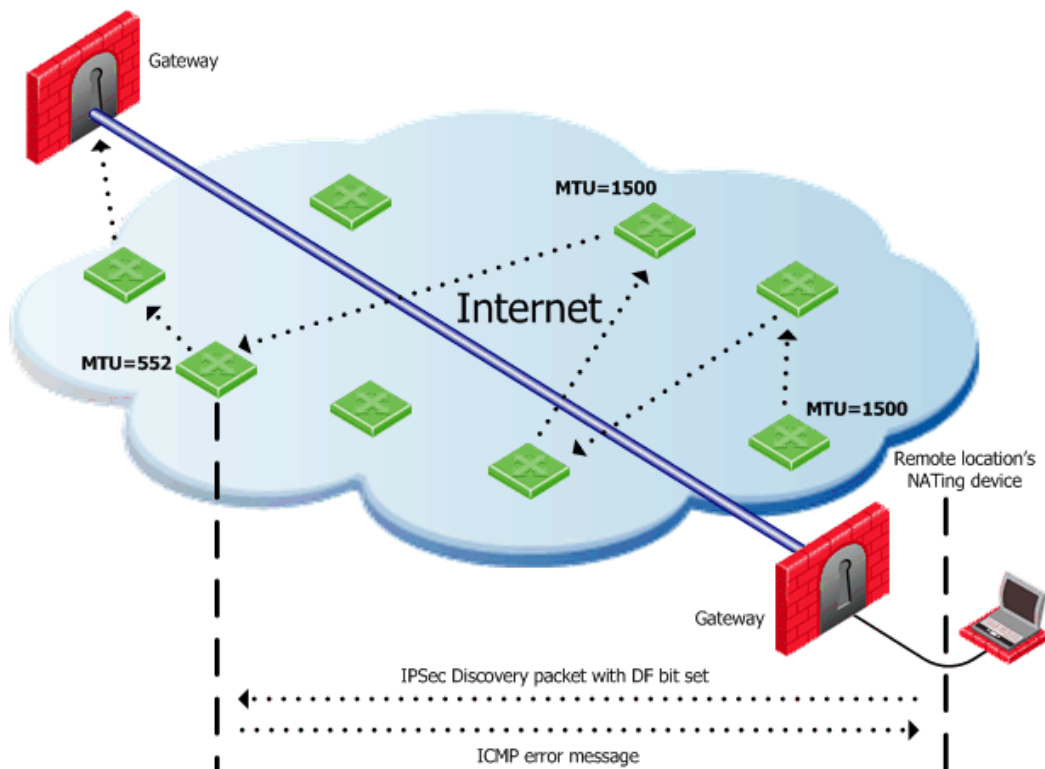
When a remote client is communicating across multiple routers with a Security Gateway, it is the smallest MTU of *all* the routers that is important; this is the *path MTU* (PMTU), and for remote access clients there is a special *IPSec PMTU* discovery mechanism to prevent the OS of the client from fragmenting the IPSec packet if the IPSec packet is too large.

However, the PMTU between the remote client and the Security Gateway will not remain constant, since routing across the Internet is dynamic. The route from Security Gateway to client may not be the same in both directions, hence each direction may have its own PMTU. VPN handles this in two ways:

- Active IPSec PMTU
- Passive IPSec PMTU

Active IPsec PMTU

After IKE phase II but before the IPsec stage, the remote access client sends special discovery IPsec packets of various sizes to the Security Gateway. The DF (do not fragment) bit on the packet is set. If a packet is longer than any router's MTU, the router drops the packet and sends an ICMP error message to the remote client. From the largest packet not fragmented, the remote client resolves an appropriate PMTU. This PMTU is not conveyed directly to the OS. Unknown to the operating system, during the TCP three-way handshake, the Maximum Segment Size (MSS) on the SYN and SYN-ACK packets are changed to reflect the PMTU. This is known as *Active IPsec PMTU*.



Passive IPsec PMTU

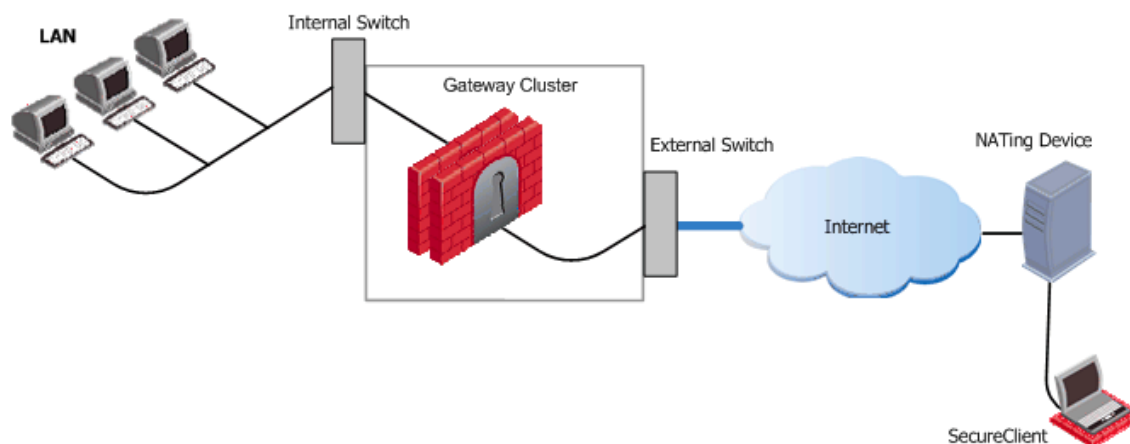
Passive IPsec PMTU solves the problem of dynamic Internet routing. Passive IPsec PMTU is a process that occurs when either side receives an ICMP error message resulting from a change in the routing path. Since routes change dynamically on the Internet, if a different router needs to fragment the packet that has the DF bit set, the router discards the packet and generates an ICMP "cannot fragment" error message. The error message is sent to the VPN peer that sent the packet. When the peer receives this error message, the peer decreases the PMTU and retransmits.



Note - From the system administrator's perspective, there is nothing to configure for PMTU; the IPsec PMTU discovery mechanism, both active and passive, runs automatically.

NAT and Load Sharing Clusters

In the following figure, the remote client is behind a NATing device and connecting to a load-sharing cluster:



For the connection to survive a failover between cluster members, the "keep alive" feature must be enabled in **Global Properties > Remote Access > Enable Back connections from gateway to client**

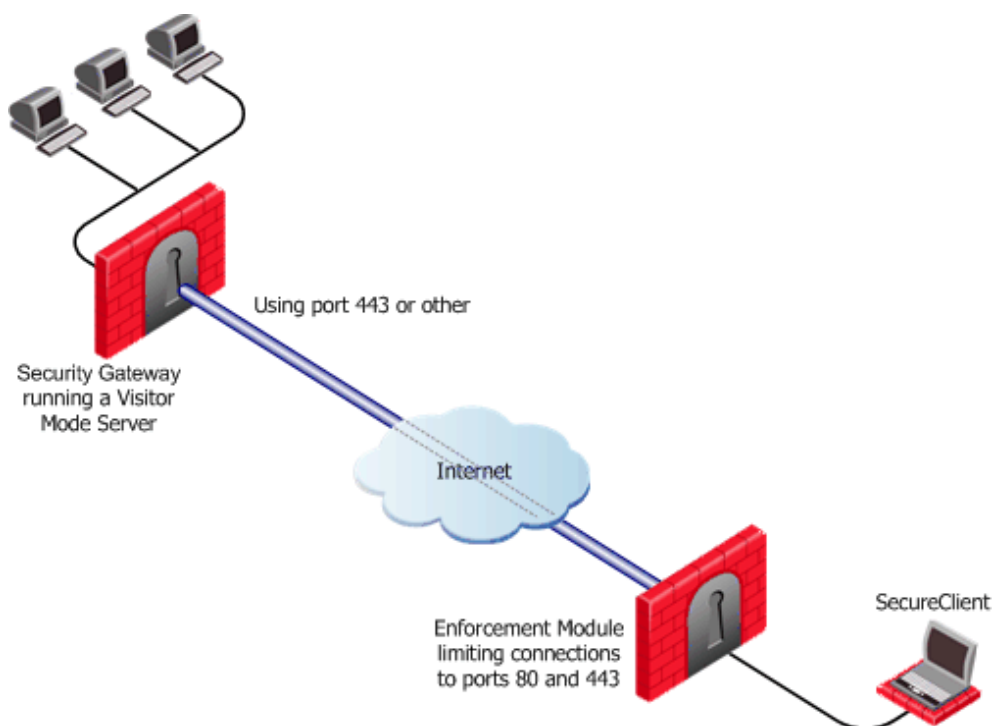
This is also true if the NATing is performed on the Security Gateway cluster side.

Overcoming Restricted Internet Access

When a user connects to the organization from a remote location such as hotel or the offices of a customer, Internet connectivity may be limited to web browsing using the standard ports designated for HTTP, typically port 80 for HTTP and port 443 for HTTPS. Since the remote client needs to perform an IKE negotiation on port 500 or send IPSec packets (which are not the expected TCP packets; IPSec is a different protocol), a VPN tunnel cannot be established in the usual way. This issue is resolved using **Visitor Mode**, formally known as *TCP Tunneling*.

Visitor Mode

Visitor Mode tunnels *all* client-to-Security Gateway communication through a regular TCP connection on port 443.



All required VPN connectivity (IKE, IPsec, etc.) between the Client and the Server is tunneled inside this TCP connection. This means that the peer Security Gateway needs to run a Visitor Mode (TCP) server on port 443.

**Note -**

- Even if the remote location's gateway in the figure above is not a Check Point product (a Security Gateway from another vendor) Visitor mode will still tunnel a connection through it.
- While in Visitor Mode, you cannot define a new site.
- Topology update takes place only if the last connection used a profile that enabled Visitor Mode.

Number of Users**To obtain optimal performance of the Visitor Mode server:**

- Minimize the number of users allowed Visitor Mode if performance degrades
- Increase the number of sockets available on the OS by editing the appropriate values, for example the socket descriptor on Linux systems

Allocating Customized Ports

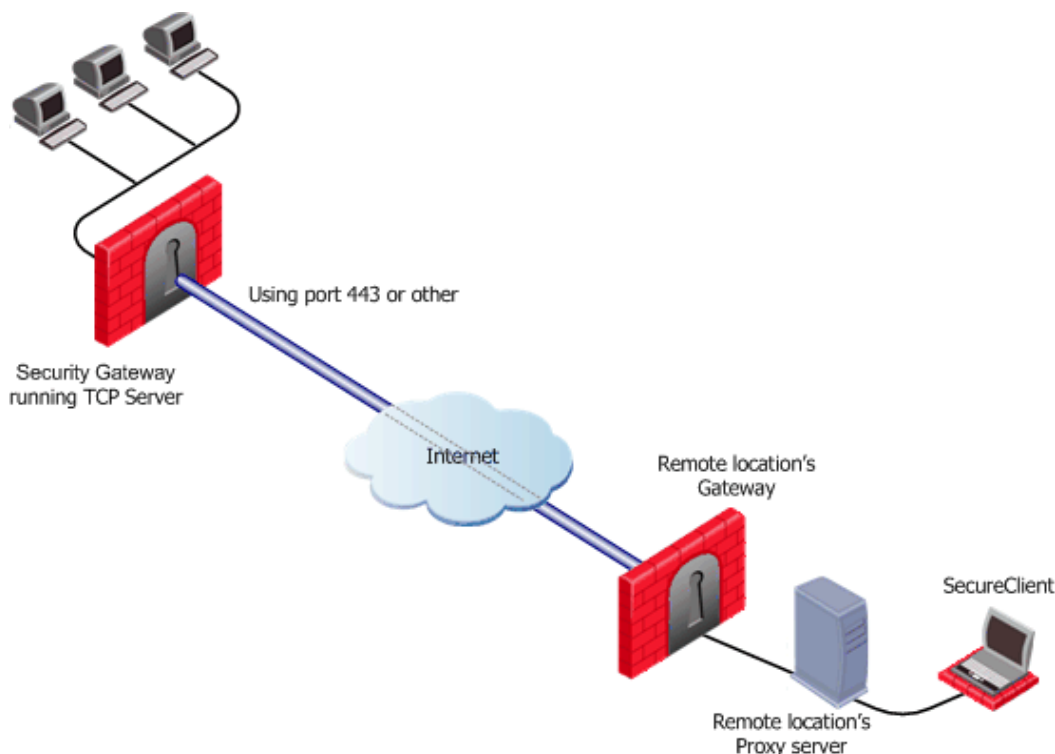
The organization decides that it would like to use a customized port for the Visitor Mode Server other than the typically designated port 443. In this scenario, another port that is *mutually agreed* upon by *all* the remote locations and the home organization, can be used for Visitor Mode. This solution works well with business partners; the partner simply agrees to open a port for the visitor Mode connections. If the chosen port is not represented by a pre-defined service in SmartDashboard, this service must be created in order for the port to be used. If a port has been mutually agreed upon, and there is a proxy, configure the proxy to allow traffic destined to this port.



Note - All partner Security Gateways must agree on the *same* allocated port, since the visitor Mode server on the peer gateway will be listening on only one port.

Visitor Mode and Proxy Servers

Visitor Mode can still be utilized in instances where the remote location runs a proxy server. In this scenario, the remote user enables Visitor Mode connections to pass through the proxy server.



Visitor Mode When the Port 443 is Occupied By an HTTPS Server

If the designated port is already in use, for example reserved for HTTPS connections by a Server at the organization's Security Gateway, a log is sent "**Visitor Mode Server failed to bind to xxx.xxx.xxx.xxx:yy (either port was already taken or the IP address does not exist)**" to Security Management server.

If the peer Security Gateway is *already* running a regular HTTP server that also listens on the standard HTTPS port 443, then it must be set up with two external interfaces, both of which have public IP addresses — one for the HTTP server, and one for the Visitor Mode server. This second routable address can be achieved in two ways:

- installing an additional network interface for the Visitor Mode server, or
- by utilizing a virtual IP on the same network interface which is blocking the port.

On the Security Gateway object running the Visitor Mode server, **General Properties > Remote Access page >** there is a setting for **Allocated IP address**. All the available IP addresses can be configured to listen on port 443 for Visitor Mode connections.

Visitor Mode with SecurePlatform/IPSO

SecurePlatform running on Linux and IPSO boxes are installed with a pre-configured HTTPS server; the server runs on the Security Gateway and listens on port 443. Installing an additional network interface or utilizing a virtual IP for the Visitor Mode server is not relevant since these HTTPS servers automatically bind to all available IP addresses.

In this case, it is preferable to reserve 443 for Visitor Mode, since users connecting, for example, from a hotel, may only be allowed to connect via ports 80 and 443. These pre-configured HTTPS servers need to be allocated ports that do not conflict with the Visitor Mode server.

Visitor Mode in a MEPed Environment

Visitor Mode also works in a MEPed environment. For more information, see: Visitor Mode and MEP (on page 235).

Interface Resolution

For *interface resolution* in a Visitor Mode environment, it is recommended to use static IP resolution or dedicate a single interface for Visitor Mode.



Note - Visitor mode is only supported for Internet Explorer 4.0 and up

Configuring Remote Access Connectivity

The following section describe how to configure Remote Access connectivity in SmartDashboard and DBedit.

Configuring IKE Over TCP

1. For the Security Gateway, open **Global Properties > Remote Access** page > **VPN-Basic** sub-page > **IKE over TCP** section. Select **Gateways support IKE over TCP**.
2. Enable IKE over TCP in a connection profile; the remote user works in connect mode to automatically receive the profile. To configure:
 - a) From the file menu, **Manage > Remote Access > Connection profiles...** the **Connection Profiles** window opens. Click **New...**
 - b) **Connection Profile Properties** window opens. On the **Advanced** tab, select **Support IKE over TCP**.

If the user is not working in connect mode, the user has to manually enable IKE over TCP on the client.

When IKE over TCP is enabled on the Security Gateway, the Security Gateway continues to support IKE over UDP as well. For remote clients, IKE over TCP is supported only for as long as the client works with a *profile that enables* IKE over TCP.

Configuring Small IKE phase II Proposals

Small phase II IKE proposals always include AES-256, but not AES-128. Suppose you want to include AES-128 in the small proposals:

1. Open the command line database editing tool **DBedit**. There are two properties that control whether small proposals are used or not, one for *pre-NG with Application Intelligence*, the other for *NG with Application Intelligence*.
 - **phase2_proposal** - determines whether an old client (*pre-NG with Application Intelligence*) will try small proposals - default "false".
 - **phase2_proposal_size** - determines whether a new client (for *NG with Application Intelligence*) will try small proposals - default "true".
2. In **Global Properties > Remote Access** page > **VPN -Advanced** subpage > **User Encryption Properties** section, select **AES-128**. This configures remote users to offer AES-128 as a small proposal.

Configuring NAT Traversal (UDP Encapsulation)

On the Security Gateway network object, enable UDP encapsulation, and decide on a port to handle UDP encapsulation:

1. **General Properties > Remote Access** page > **NAT Traversal** section, select **Support NAT traversal mechanism (UDP encapsulation)**.
2. From the **Allocated port** drop-down box, select a port. **VPN1_IPSec_encapsulation** is the default.
3. IKE phase II proposals are offered both with and without UDP encapsulation when dealing with remote access. (There is no UDP encapsulation between Security Gateways). There is no need to enable UDP on the client unless you want to shorten the existing small IKE phase II proposals. Enable UDP encapsulation in a connection profile; the remote user works in connect mode to automatically receive the profile. To configure:

- a) From the file menu, **Manage > Remote Access > Connection profiles...** the **Connection Profiles** window opens. Click **New...**
- b) **Connection Profile Properties** window opens. On the **Advanced** tab, select **Force UDP Encapsulation**.

If the user is not working in connect mode, the user has to manually enable UDP Encapsulation on the client. On the client's file menu, **Tools > Advanced IKE Settings**, select **Force UDP Encapsulation**.

Selecting UDP encapsulation on the Security Gateway means that the Security Gateway supports both encapsulated VPN traffic and traffic that is not encapsulated.

Configuring Visitor Mode

Visitor Mode requires the configuration of both the Server and the Client. See also: Visitor Mode and MEP (on page 235).

Server Configuration

To enable the TCP tunneling feature on the Security Gateways:

On the Security Gateway object running the Visitor Mode Server, **IPsec VPN > Remote Access > Visitor Mode Configuration** section, select **Support Visitor Mode**.

- If port 443 is the assigned port for TCPT server, do not change the **tcp https** default in the **Allocated Port** section.
- If a customized port (other than the default port) is agreed upon, from the drop-down menu select the service that corresponds to this port. If the chosen port is not represented by a pre-defined service in SmartDashboard, create this service. If Mobile Access is enabled on the gateway, this setting cannot be changed.
- In **Allocated IP Address** the default is **All IPs**. To avoid port conflicts, select the appropriate routable valid IP for the Visitor Mode server. If the server has **Dynamic Interface Resolving Configuration...** enabled (on the **VPN - Advanced** page) it is recommended to allocate a specific address for visitor mode instead of **All IPs**. If Mobile Access is enabled on the gateway, this setting cannot be changed



Note - When Visitor Mode is activated on the gateway, the RDP interface discovery mechanism does not work. A Visitor Mode handshake is used instead.

These settings configure a Visitor Mode server to run on the Security Gateway.

Visitor Mode and Gateway Clusters

Cluster support is limited. The high availability and Load Sharing solutions must provide "stickiness". That is, the visitor mode connection must always go through the same cluster member.

Failover from cluster member to cluster member in a High Availability scenario is not supported.

Enabling Visitor Mode Using a Connection Profile

Create a customized connection profile for Visitor Mode users. This profile enables the Visitor Mode feature on the Client side.

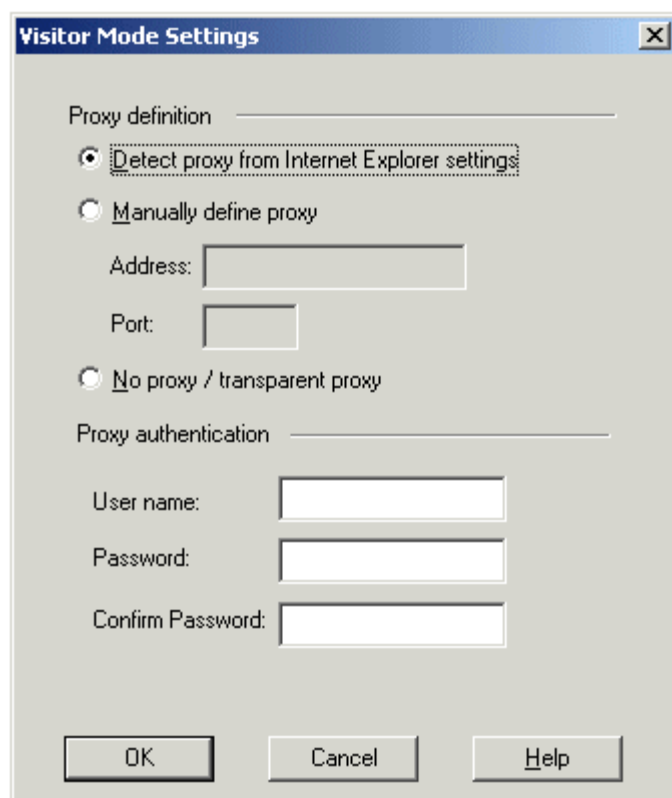
To create the profile:

1. In SmartDashboard, **Manage > Remote Access > Connection profiles...** the **Connection Profiles** window opens.
2. Click **New...** to create a new connection profile or **Edit...** to alter an existing profile. The **Connection Profile Properties** window opens.
3. On the **Advanced** tab, select **Visitor Mode**.

On the remote client, configure the user to work in connect mode.

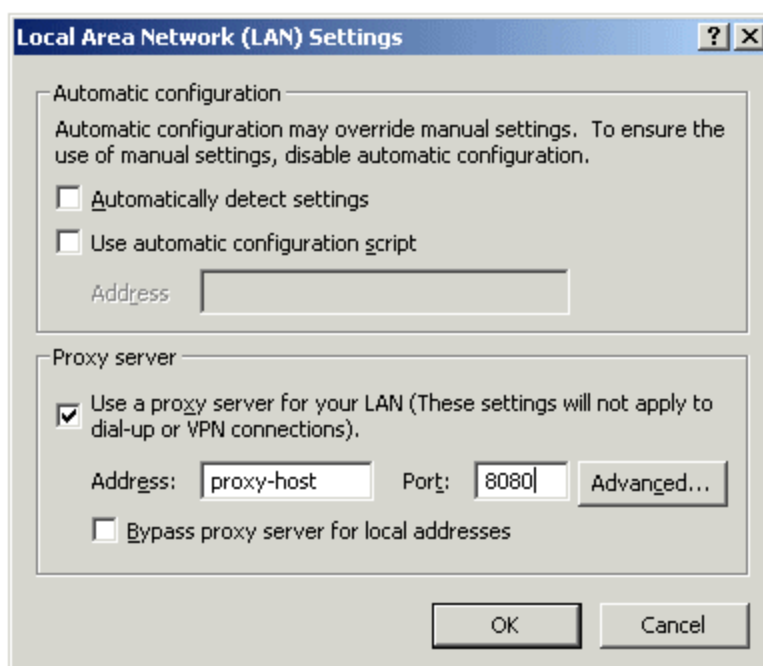
Configuring Remote Clients to Work with Proxy Servers

1. In SecureClient, select **Detect Proxy from Internet Explorer Settings**



In previous versions, the proxy had to be manually defined.

2. Enter a username and password for proxy authentication. This information is later transferred with the "connect" command to the proxy server.



Now Secure Client can read any of the Visitor Mode settings, but only if:

- SecureClient is connected to a LAN or WLAN (not dial-up)
- Secure Domain Logon (SDL) is *not* enabled.

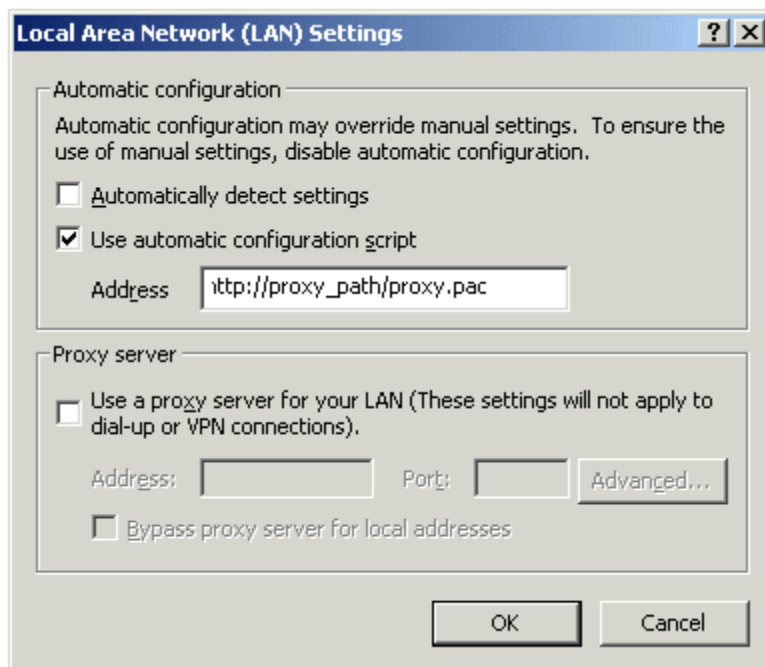


Note - Visitor mode attempts to connect to the proxy server without authenticating. If a user name and password is required by the proxy, the error message "proxy requires authentication appears".

Windows Proxy Replacement

If SecureClient is on a LAN/WLAN and a proxy server is configured on the LAN, SecureClient replaces the proxy settings so that new connections are not sent to the VPN domain via the proxy but go directly to the LAN/WLAN's Security Gateway. This feature works with and without Visitor Mode. SecureClient must be on a WAN/WLAN and not using a dial-up connection.

When SC replaces the proxy file, it generates a similar plain script PAC file containing the entire VPN domain IP ranges and DNS names (to be returned as "DIRECT"). This file is stored locally, since the windows OS must receive this information as a plain script PAC file. This file replaces the automatic configuration script as defined in Internet Explorer:



Special Considerations for Windows Proxy Replacement

Sensitive information regarding the site's IP Address and DNS settings are contained in SecureClient's **userc.C** file. For this reason, the file is obfuscated by an algorithm that hides the real content (but does not encrypt it). When the proxy replacement feature is used, the same information is written to the plain text PAC file. For this reason, administrators should be aware that the Windows Proxy Replacement feature exposes the VPN domain by writing Site IP addresses and DNS settings as Java Script code in this plain text PAC file, which can be viewed by any end user.

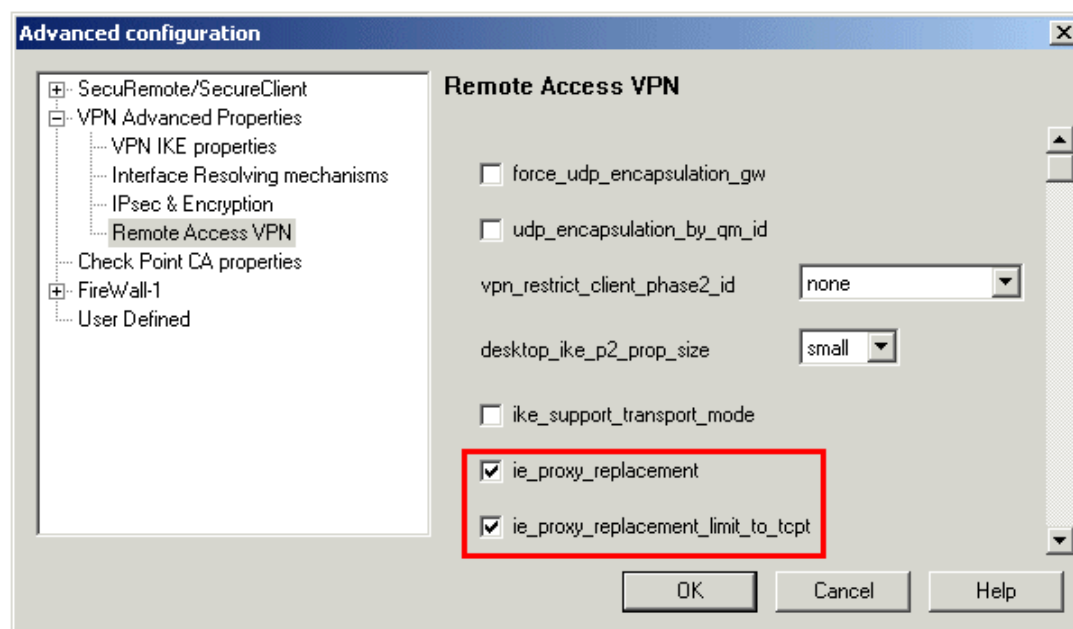
Configuring windows Proxy Replacement

Windows proxy replacement is configured either on the Security Gateway or on the SecureClient client.

On the Security Gateway:

1. **Global Properties > SmartDashboard Customization**
2. Click **Configure**

The **Advanced Configuration** window opens:



3. Select either:

- **ie_proxy_replacement.** If option is selected, windows proxy replacement is always performed, even if visitor mode is not enabled.
- **ie_proxy_replacement_limit_to_tcpt.** If this option is selected, then proxy replacement takes place *only* when visitor mode is enabled.

When SecureClient performs an update, the policy regarding windows proxy replacement is downloaded and put into effect.

On SecureClient

Alternatively, these two properties can be set in the `userc.C` file on the remote client:

```
:ie_proxy_replacement (true)
:ie_proxy_replacement_limit_to_tcpt (true)
```

Appendices

Appendix A

VPN Command Line Interface

In This Appendix

| | |
|-------------------------|-----|
| VPN Commands | 285 |
| SecureClient Commands | 286 |
| Desktop Policy Commands | 287 |

VPN Commands

The following command lines relate to VPN and are also documented in the *R75.40 Command Line Interface Reference Guide* (<http://supportcontent.checkpoint.com/solutions?id=sk67581>).

VPN Command Line interface

| Command | Description |
|-----------------------|--|
| VPN | This command and subcommands are used for working with various aspects of VPN. VPN commands executed on the command line generate status information regarding VPN processes, or are used to stop and start specific VPN services. |
| vpn accel | This command performs operations on accelerator cards (encryption only cards, not the full SecureXL cards). |
| vpn compreset | This command resets the compression/decompression statistics to zero. |
| vpn compstat | This command displays compression/decompression statistics. |
| vpn crl_zap | This command is used to erase all Certificate Revocation Lists (CRLs) from the cache. |
| vpn crlview | This command retrieves the Certificate Revocation List (CRL) from various distribution points and displays it for the user. |
| vpn debug | This command instructs the VPN daemon to write debug messages to the log file: \$FWDIR/log/vpnd.elg . |
| vpn drv | This command installs the VPN kernel (vpnk) and connects it to the FireWall kernel (fwk), attaching the VPN driver to the FireWall driver. |
| vpn export_p12 | This command exports information contained in the network objects database and writes it in the PKCS#12 format to a file with the p12 extension. |
| vpn macutil | This command is related to Remote Access VPN, specifically Office mode, generating a MAC address per remote user. This command is relevant only when allocating IP addresses via DHCP. |

| Command | Description |
|---------------------------|--|
| vpn mep_refresh | This command causes all MEP tunnels to fail-back to the best available gateway, providing that backup stickiness has been configured. |
| vpn nssm_topology | This command generates and uploads a topology (in NSSM format) to a IPSO NSSM server for use by IPSO clients. |
| vpn overlap_encdom | <p>This command displays all overlapping VPN domains. Some IP addresses might belong to two or more VPN domains. The command alerts for overlapping encryption domains if one or both of the following conditions exist:</p> <ul style="list-style-type: none"> • The same VPN domain is defined for both Security Gateways • If the gateway has multiple interfaces, and one or more of the interfaces has the same IP address and netmask. |
| vpn sw_topology | This command downloads the topology for a SofaWare Security Gateway. |
| vpn ver | This command displays the VPN major version number and build number. |
| vpn tu | This command launches the TunnelUtil tool which is used to control VPN tunnels. |

SecureClient Commands

The following commands relate to SecureClient.

SecureClient command line interface

| Command | Explanation |
|--------------------------|---|
| SCC | VPN commands executed on SecureClient are used to generate status information, stop and start services, or connect to defines sites using specific user profiles. |
| scc connect | This command connects to the site using the specified profile, and waits for the connection to be established. In other words, the OS does not put this command into the background and executes the next command in the queue. |
| scc connectnowait | This command connects asynchronously to the site using the specified profile. This means, the OS moves onto the next command in the queue and this command is run in the background. |
| scc disconnect | This command disconnects from the site using a specific profile. |
| scc erasecreds | This command unsets authorization credentials. |
| scc listprofiles | This command lists all profiles. |
| scc numprofiles | This command displays the number of profiles. |

| | |
|---------------------------------|--|
| scc restartsc | This command restarts SecureClient services. |
| scc passcert | This command sets the user's authentication credentials when authentication is performed using certificates. |
| scc setmode <mode> | This command switches the SecuRemote/SecureClient mode. |
| scc setpolicy | This command enables or disables the current default security policy. |
| scc sp | This command displays the current default security policy. |
| scc startsc | This command starts SecureClient services. |
| scc status | This is command displays the connection status. |
| scc stopsc | This command stops SecureClient services. |
| scc suppressdialogs | This command enables or suppresses dialog popups. By default, suppressdialogs is off. |
| scc userpass | This commands sets the user's authentication credentials -- username, and password. |
| scc ver | This command displays the current SecureClient version. |
| scc icacertenroll | This command enrolls a certificate with the internal CA, and currently receives 4 parameters - site, registration key, filename and password. Currently the command only supports the creation of p12 files. |
| scc sethotspotreg | This command line interface now includes HotSpot/Hotel registration support. |

Desktop Policy Commands

The following command lines relate to the Desktop Policy.

Desktop Policy command line interface

| Command | Description |
|--|---|
| dtps ver | This command displays the policy server version. |
| dtps debug [on off] | This command starts or stops the debug printouts to \$FWDIR/log/dtps.elg |
| fwm psload <path to desktop policy file> <target> | <p>This command loads the desktop policy onto the module. The target is the name of the module where the desktop policy is being loaded and should be entered as it appears in SmartDashboard. This command should be run from the management.</p> <p>For example: fwm psload \$FWDIR/conf/Standard.S Server_1</p> |

| Command | Description |
|--|---|
| fwm sdsload <path to SDS objects file> <target> | <p>This command loads the SDS database onto the module. The target is the name of the module where the SDS objects file is being loaded and should be entered as it appears in SmartDashboard. This command should be run from the management.</p> <p>For example: fwm sdsload \$FWDIR/conf/SDS_objects.C Server_1</p> |

Appendix B

VPN Shell

In This Appendix

[Configuring a Virtual Interface Using the VPN Shell](#)

289

Configuring a Virtual Interface Using the VPN Shell

The VPN Shell, used for creating Virtual VPN Tunnel Interfaces, is composed of menus and commands. The shell can be used interactively or as a single command line. Invoking the command - **vpn shell** - without any other arguments starts the interactive shell. Adding arguments after **vpn shell** is interpreted as a direct command and executed.

VPN shell — starts the interactive mode

- The basic format of the command is: **[path/path/path arguments]**, for example **interface/add** takes you directly to the menu for adding numbered interfaces.
- Within the VPN shell, command line completion is available, for example **i/a/n** is completed to **interface/add/numbered** and executed provided there are not two commands starting with the same letter.
- Use Control-D to exit the VPN shell/end of line (when including vpn shell commands in a script)

Expressions and meanings for the VPN shell are shown in the following table:

VPN Shell Commands/Arguments

| Expression | Meaning |
|-------------------------------|--|
| ? | Shows available commands |
| / | Returns to the top of the main menu |
| .. (two dots) | Moves up one menu level |
| /quit | Exits the VPN shell |
| show/interface/summary | Shows summary of all interfaces or of a specific interface |
| show/interface/detailed | Shows summary of all interfaces or of a specific interface with greater detail |
| interface/add/numbered | Adds a numbered interface (Local IP, remote IP, peer name and interface name required) |
| interface/add/unnumbered | Adds an unnumbered interface (Peer name and interface name required) |
| interface/modify/peer/mtu | Modify the MTU of an interface by peer name |
| interface/modify/peer/netmask | Modify the netmask of an interface by peer name |
| interface/modify/ifname/mtu | Modify the MTU of an interface by given interface name |

| Expression | Meaning |
|--------------------------------|--|
| interface/modify/iface/netmask | Modify the netmask of an interface by given interface name |
| interface/delete/peer | Delete interface by given peer name |
| interface/delete/iface | Delete interface by given interface name |
| interface/show/summary | Shows summary of all interfaces or of a specific interface |
| interface/show/detailed | Shows summary of all interfaces or of a specific interface with greater detail |
| tunnels/show/IKE/all | Displays all valid SA's |
| tunnels/show/IKE/peer | Displays valid SA for a specific peer (gateway IP address required) |
| tunnels/show/IPSec/all | Displays all IPSec tunnels |
| tunnels/show/IPSec/peer | Displays IPSec tunnels for a specific peer |
| tunnels/delete/IKE/peer | Deletes valid SA's for a specific peer (Security Gateway IP address required) |
| tunnels/delete/IKE/user | Deletes valid SA's for a specific user (internal IP address and user name required) |
| tunnels/delete/IKE/all | Deletes all valid SA's |
| tunnels/delete/IPSec/peer | Deletes IPSec tunnels for a specific peer (gateway IP address required) |
| tunnels/delete/IPSec/user | Deletes IPSec tunnels for a specific user (internal IP address and user name required) |
| tunnels/delete/IPSec/all | Deletes all IPSec tunnels |
| tunnels/delete/all | Deletes all SA's and IPSec tunnels |

Index

A

- A Closer Look • 167
- A Complete Example of a local.scv File • 203
- About ActiveX Controls • 260
- Accepting all Encrypted Traffic • 33
- Access Control and VPN Communities • 32
- Access Control for Remote Access Community • 152
- Active IPsec PMTU • 275
- Add and Remove Files in Package • 183
- Add Rules Allowing Communication Inside the VPN Domain • 142
- Adding a Language • 258
- Adding Matching Criteria to the Validation Process • 50
- Adding Scripts to a Package • 182
- Additional Considerations • 231
- Additional Script Elements • 198
- Advanced Features • 154
- Advanced IKE Dos Attack Protection Settings • 21
- Advanced Permanent Tunnel Configuration • 80
- Advanced Settings • 122
- After Running the Wizard • 142
- Allocating Customized Ports • 277
- Allowing Clients to Route all Traffic Through a Security Gateway • 220
- Allowing Firewall Control Connections Inside a VPN • 39
- Alternatives to SecuRemote/SecureClient • 154
- Anti Spoofing • 169
- Assigning IP Addresses • 168
- Auth+Encrypt Rules • 142
- Authenticating the Client Machine During IKE • 190
- Authenticating the User • 190
- Authentication • 24
- Authentication Between Community Members • 26
- Authentication Methods • 189
- Authentication of Users and Client Machines • 189
- Authentication Timeout and Password Caching • 231
- Authentication Timeout Interval • 229
- Auto Topology Update (Connect Mode only) • 233
- Automatic Enrollment with the Certificate Authority • 45
- Automatic RIM • 82
- Automatically Renewing a Users' Certificate • 163
- Avoiding Double Authentication for Policy Server • 185

B

- Back Connections (Server to Client) • 232
- Behavior of an L2TP Connection • 188
- By VPN Domain • 120

C

- CA Certificate Rollover • 49
- CA Certificate Rollover CLI • 50
- CA Located on the LAN • 42
- CA of An External Security Management Server • 41
- CA Services Over the Internet • 42
- Cached Information • 232
- Certificate Recovery and Renewal • 49
- Certificate Revocation (All CA Types) • 49
- Certificates • 189
- Check Point GO • 148
- Check Point Mobile for Android • 148
- Check Point Mobile for iPhone and iPad • 148
- Check Point Mobile for Windows • 147
- Check Point Remote Access Solutions • 144
- Check Point SCV Checks • 197
- Check Point Solution for Connectivity Issues • 271
- Check Point Solution for Greater Connectivity and Security • 219
- Checking the Syntax • 177
- Choosing a Topology • 29
- Choosing the Authentication Method • 132
- Choosing the Certificate Authority • 132
- Client Properties • 22
- Client Side Configuration • 186, 199
- Client to Client via Multiple Hubs Using Hub Mode • 223
- Client-Based vs. Clientless • 144
- Client-Security Gateway Authentication Schemes • 152
- Client-side Pre-Requisites • 251
- Command Line • 267
- Common Attributes • 209
- Commonly Used Concepts • 250
- Completing the Configuration • 59
- Confidentiality • 24
- Configurable Objects in a Direction • 94
- Configuration File Attributes • 268
- Configuration of Client to Client Routing by Including the Office Mode Range of Addresses in the VPN Domain of the Security Gateway • 223
- Configuration of PKI Operations • 47
- Configuration via Editing the VPN Configuration File • 54
- Configuring a Loopback Interface • 74
- Configuring a Meshed Community Between Internally Managed Gateways • 34
- Configuring a Remote Access Environment • 191
- Configuring a Star VPN Community • 35
- Configuring a Virtual Interface Using the VPN Shell • 289
- Configuring a VPN using a Pre-Shared Secret • 135
- Configuring a VPN with External Security Gateways Using a Pre-Shared Secret • 37
- Configuring a VPN with External Security Gateways Using PKI • 35
- Configuring Advanced IKE Properties • 22
- Configuring an SCV Policy on the Security Management server • 196
- Configuring Anti-Spoofing on VTIs • 74

Configuring Authentication • 153
 Configuring Authentication for NT groups and RADIUS Classes • 161
 Configuring Certificates Using Third Party PKI • 160
 Configuring CRL Grace Period • 51
 Configuring Desktop Security • 186
 Configuring Directional VPN Between Communities • 96
 Configuring Directional VPN with Remote Access Communities • 226
 Configuring Directional VPN Within a Community • 95
 Configuring Domain Based VPN • 54
 Configuring ESOD Policies • 256
 Configuring Explicit MEP • 126
 Configuring IKE Over TCP • 279
 Configuring Implicit First to Respond • 127
 Configuring Implicit Load Distribution • 128
 Configuring Implicit MEP • 127
 Configuring Implicit Primary-Backup • 127
 Configuring IP Assignment Based on Source IP Address • 175
 Configuring IP pool NAT • 237
 Configuring IP Pool NAT • 129
 Configuring IP Selection by Remote Peer • 97
 Configuring Link Selection for Remote Access Only • 224
 Configuring MEP • 126, 236
 Configuring Microsoft Internet Explorer • 259
 Configuring MSI Packaging • 182
 Configuring Multiple Hubs • 56
 Configuring NAT Traversal (UDP Encapsulation) • 279
 Configuring Numbered VTIs • 63
 Configuring OCSP • 51
 Configuring Office Mode • 174
 Configuring Office Mode and L2TP Support • 191
 Configuring On Demand Links • 113
 Configuring Outgoing Route Selection • 99
 Configuring Preferred Backup Security Gateway • 237
 Configuring Remote Access Connectivity • 279
 Configuring Remote Access for Microsoft IPsec/L2TP Clients • 191
 Configuring Remote Access VPN • 157
 Configuring Remote Clients to Work with Proxy Servers • 281
 Configuring Return Packets • 237
 Configuring RIM • 85
 Configuring RIM in a Meshed Community: • 86
 Configuring RIM in a Star Community: • 85
 Configuring RIM on Gaia • 87
 Configuring SCV • 198
 Configuring SDL Timeout • 231
 Configuring Secure Domain Logon • 232
 Configuring Service Based Link Selection • 106
 Configuring Site to Site VPNs • 33
 Configuring Small IKE phase II Proposals • 279
 Configuring Source IP Address Settings • 101
 Configuring the 'Accept VPN Traffic Rule' • 55
 Configuring the Gateway to Support the SSL Network Extender • 254
 Configuring the Languages Option • 258
 Configuring the SecuRemote DNS Server • 230
 Configuring the Security Gateway as a Member of the Remote Access Community • 253
 Configuring the Server • 253
 Configuring the Skins Option • 257
 Configuring the SSL Network Extender • 253, 254
 Configuring Traditional Mode VPNs • 132
 Configuring Trusted Links • 110
 Configuring Tunnel Features • 79
 Configuring Unnumbered VTIs • 74
 Configuring User Certificate Purposes • 193
 Configuring Visitor Mode • 280
 Configuring VPN Between Internal Gateways using ICA Certificates • 133
 Configuring VPN Routing and Access Control on Security Management server A • 56
 Configuring VPN Routing and Access Control on Security Management server B • 56
 Configuring VPN Routing for Remote Access VPN • 222
 Configuring VPN Routing for Security Gateways through SmartDashboard • 54
 Configuring VPN with Externally Managed Gateways Using Certificates • 134
 Configuring VTIs in a Clustered Environment • 65
 Configuring windows Proxy Replacement • 282
 Configuring Wire Mode • 91
 Confirming a VPN Tunnel Successfully Opens • 35
 Connection Mode • 151
 Connectivity Features • 150
 Considerations for Choosing Microsoft IPsec/L2TP Clients • 190
 Considerations for VPN Creation • 132
 Considerations regarding SCV • 198
 Conversion of Auth+Encrypt Rules • 141
 Conversion of Client Encrypt Rules • 141
 Conversion of Encrypt Rule • 139
 Converting a Traditional Policy to a Community Based Policy • 137
 Creating a New Package Profile • 181
 Creating a P12 Certificate File • 159
 Creating a Preconfigured Package • 181
 Creating a Skin • 257
 Creating and Configuring the Security Gateway • 160
 Creating Certificate Registration Key • 159
 Creating Remote Access VPN Certificates for Users • 158
 CRL • 46
 CRL Cache Usage • 51
 CRL Grace Period • 47
 CRL Prefetch-Cache • 46
 Custom Scripts • 83
 Customizing the SSL Network Extender Portal • 257
D
 Debug • 183
 Defense Against IKE DoS Attacks • 20
 Defining a User Group • 162

- Defining a VPN Community and its Participants • 162
- Defining Access Control Rules • 162
- Defining an LDAP User Group • 162
- Defining the CAs • 134
- Defining the Client Machines and their Certificates • 191
- Defining the Encrypt Rule • 133, 134, 135, 136
- Defining the Externally Managed Security Gateways • 134
- Defining the Internally Managed Security Gateways • 134
- Defining the Security Gateways • 133, 135
- Defining User and Authentication Methods in LDAP • 160
- Defining User Authentication Methods in Hybrid Mode • 161
- Defining VPN Properties • 132
- Desktop Policy Commands • 287
- Desktop Security • 185
- Desktop Security Considerations • 185
- DHCP Server • 168, 171
- Diffie Hellman Groups • 16
- Digital Certificates • 152
- Directional Enforcement between Communities • 95
- Directional Enforcement within a Community • 93
- Directional VPN Enforcement • 93
- Directional VPN in RA Communities • 225
- Disabling a Language • 258
- Disabling a Skin • 257
- Disabling MEP • 236, 237
- Discovering Which Services are Used for Control Connections • 39
- Distributed Key Management and Storage • 47
- Domain Based VPN • 33, 53
- Domain Controller Name Resolution • 229
- Downloading and Connecting the Client • 260
- Downloading the SCV Policy to the Client • 196
- During IKE phase I • 272
- During IKE phase II • 273
- During IPSec • 273
- Dynamically Assigned IP Security Gateways • 28

E

- Editing a Traditional Mode Policy • 132
- Enabling a User Certificate • 159
- Enabling and Disabling Secure Domain Logon • 229
- Enabling Dynamic Routing Protocols on VTIs • 71
- Enabling Hub Mode for Remote Access clients • 222
- Enabling Hybrid Mode and Methods of Authentication • 161
- Enabling IP Address per User • 171
- Enabling Route Based VPN • 63
- Enabling the RIM_inject_peer_interfaces flag • 86
- Enabling Visitor Mode Using a Connection Profile • 280

- Enabling Wire Mode on a Specific Security Gateway • 92
- Enabling Wire Mode on a VPN Community • 91
- Encrypted Back Connections • 244
- Encryption • 241
- Endpoint Security on Demand • 250
- Endpoint Security Suite • 148
- Endpoint Security VPN • 147
- Enhancing SecuRemote with SecureClient Extensions • 149
- Enrolling a Managed Entity • 43
- Enrolling through a Subordinate CA • 45
- Enrolling User Certificates - ICA Management Tool • 160
- Enrolling with a Certificate Authority • 44
- ESOD Issues • 270
- ESOD Policy per User Group • 250
- Establishing a Connection Between a Remote User and a Security Gateway • 150
- Establishing a VPN between a Microsoft IPSec/L2TP Client and a Check Point Gateway • 188
- Example • 257, 258
- Excluded Services • 33
- Explicit MEP • 118
- Expressions • 200
- Expressions and Labels with Special Meanings • 201

F

- Features • 252
- Fetching the xml Configuration File • 255
- First to Respond • 119, 124, 236
- For internally managed Users • 163
- For More Information • 193
- For Users Managed in LDAP • 163

G

- Gateway with a Single External Interface • 102
- Gateway with an Interface Behind a Static NAT Device • 103
- Gateway with Several IP Addresses Used by Different Parties • 102
- General Configuration Procedure • 191
- Generating a Package • 181

H

- HotSpot Registration • 241
- How an Encrypt Rule Works in Traditional Mode • 138
- How Does Packaging Tool Work? • 180
- How does SCV work? • 196
- How it Works • 25
- How Office Mode Works • 167
- How the Converter Handles Disabled Rules • 142
- How the Gateway Searches for Users • 153
- How the SSL Network Extender Works • 250
- How to Authorize Firewall Control Connections in VPN Communities • 38
- How to Manually Edit Userc.C • 239
- How to Work with non-Check Point Firewalls • 233

How Traditional VPN Mode Differs from a Simplified VPN Mode • 137
How Userc.C Is Automatically Updated • 239
Hub Mode (VPN Routing for Remote Clients) • 220

I

Identifying Elements of the Network to the Remote Client • 151
IKE DoS Attacks • 20
IKE DoS Protection • 19
IKE Over TCP • 273
IKE Phase I • 13
IKE Phase II (Quick mode or IPSec Phase) • 15
ike_dos_max_puzzle_time_daip • 21
ike_dos_max_puzzle_time_gw • 21
ike_dos_max_puzzle_time_sr • 21
ike_dos_puzzle_level_identified_initiator • 21
ike_dos_puzzle_level_unidentified_initiator • 21
ike_dos_supported_protection_sr • 22
ike_dos_threshold • 21
IKEv1 and IKEv2 • 16
Implementation • 117
Implicit MEP • 123
Important Information • 3
Injecting Peer Security Gateway Interfaces • 85
Installation Command Line Options • 183
Installation for Users without Administrator Privileges • 259
Installing SCV Plugins on the Client • 196
Installing the Policy • 162
Instructions for End Users • 160
Integrity • 24
Interface Resolution • 279
Internal User Database vs. External User Database • 155
Internally and Externally Managed Security Gateways • 132
Introducing Secure Configuration Verification • 195
Introduction
 The Need to Simplify Remote Client Installations • 180
Introduction to Converting to Simplified VPN Mode • 137
Introduction to L2TP Clients • 187
Introduction to Site to Site VPN • 24
Introduction to the SSL Network Extender • 249
Introduction to Traditional Mode VPNs • 130
Introduction to Userc.C and Product.ini • 238
IP Address Lease duration • 169
IP Assignment Based on Source IP Address • 168
IP Compression • 18
IP Pool • 168
IP Pool NAT • 236
IP Pool Network Address Translation (NAT) • 125
IP pool Versus DHCP • 174
ipassignment.conf File • 172
IPSEC & IKE • 13
IPSec Path Maximum Transmission Units • 274

J

Java • 266

L

L2TP Global Configuration • 189
Last Known Available Peer IP Address • 99
Layer Two Tunneling Protocol (L2TP) Clients • 187
Link Selection • 97
Link Selection and ISP Redundancy • 113
Link Selection for Remote Access Clients • 224
Link Selection Overview • 97
Link Selection Scenarios • 101
Link Selection with non-Check Point Devices • 115
LMHOSTS • 229
Load Distribution • 125, 237
Load Sharing Cluster Support • 256
Logical Sections • 201

M

Making the L2TP Connection • 193
Making the Organizational Security Policy SCV-Aware • 196
Management Features • 150
Management of Internal CA Certificates • 254
Managing a CA Certificate Rollover • 50
Manual Enrollment with OPSEC Certified PKI • 44
Manually Set Priority List • 121
MEP Selection Methods • 119
Meshed VPN Community • 27
Methods of Encryption and Integrity • 16
Migrating from Traditional Mode to Simplified Mode • 34
Miscellaneous • 245
Mobile Access Web Portal • 146
Modifying a Language • 259
Modifying Encryption Properties for Remote Access VPN • 163
Modifying the CRL Pre-Fetch Cache • 51
Multiple Certificates per User • 155
Multiple Entry Point • 243
Multiple Entry Point for Remote Access VPNs • 234
Multiple Entry Point VPNs • 117

N

NAT and Load Sharing Clusters • 276
NAT Traversal (UDP Encapsulation for Firewalls and Proxies) • 273
Need for Integration with Different PKI Solutions • 40
Need for Remote Access VPN • 154
Non-Private Client IP Addresses • 227
NT Domain Support • 244
NT Group/RADIUS Class Authentication Feature • 156
Number of Users • 277
Numbered VTI • 63
Numbered VTIs • 63

O

- Obtain Information from the Peer Administrator
 - 134, 135
- OCSF • 46
- Office Mode • 166, 250
- Office Mode — DHCP Configuration • 177
- Office Mode — IP Pool Configuration • 174
- Office Mode - Using a RADIUS Server • 178
- Office Mode and Static Routes in a Non-flat Network • 169
- Office Mode Configuration on SecureClient • 178
- Office Mode Considerations • 174
- Office Mode IP assignment file • 162
- Office Mode per Site • 179
- Office Mode Per Site • 170
- Office Mode through the ipassignment.conf File • 176
- On Demand Links (ODL) • 112
- On SecureClient • 283
- On the Gateway Network Object • 23
- On the Security Gateway: • 282
- On the VPN Community Network Object • 23
- Other Authentication Methods Available via Hybrid Mode • 153
- Other Connectivity Issues • 271
- Outgoing Link Tracking • 101
- Overcoming NAT Related Issues • 271
- Overcoming Restricted Internet Access • 276
- Overview • 13, 180, 224
- Overview of Directional VPN • 93
- Overview of Domain-based VPN • 53
- Overview of MEP • 117
- Overview of Route Injection • 82
- Overview of Route-based VPN • 61
- Overview of Tunnel Management • 77
- Overview of Wire Mode • 88

P

- Packaging SecureClient • 180
- Passive IPSec PMTU • 275
- Password Caching • 229
- Perfect Forward Secrecy • 17
- Permanent Tunnels • 77, 79
- Permanent Tunnels in a MEP Environment • 77
- Phase I modes • 17
- PKI and Remote Access Users • 41
- PKI Deployments and VPN • 41
- Placing the Client Certificate in the Machine Certificate Store • 191
- Placing the Security Gateways into the Communities • 139
- Placing the User Certificate in the User Certificate Store • 192
- Planning the SCV Policy • 198
- Policy Definition for Remote Access • 155
- Preferred Backup Security Gateway • 235
- Preparation • 182
- Preparing the Client Machines • 191
- Pre-Requisites • 251
- Pre-Shared Secret • 152
- Preventing a Client Inside the Encryption Domain from Encrypting • 228
- Primary-Backup • 236

- Primary-Backup Security Gateways • 125
- Principles of the Conversion to Simplified Mode
 - 139
- Product.ini Parameters • 246
- Protection After Successful Authentication • 22
- Providing Secure Remote Access • 144
- Public Key Infrastructure • 40

R

- RADIUS Server • 169
- Random Selection • 120
- Recovery and Renewal with Internal CA • 49
- Remote Access Advanced Configuration • 227
- Remote Access Community • 26, 151, 250
- Remote Access Solution Comparison • 145
- Remote Access VPN • 11, 250
- Remote Access VPN Overview • 149
- Remote Access VPN Workflow • 158
- Remote Client to Client Communication • 221
- Removing an Imported Certificate • 269
- Renegotiating IKE & IPSec Lifetimes • 17
- Resolving Connectivity Issues • 271
- Resolving Internal Names with the SecuRemote DNS Server • 233
- Revocation Checking • 44
- Revoking Certificates • 163
- RIM • 126
- Route Based VPN • 33, 61
- Route Injection Mechanism • 82
- Routing all Traffic through the Security Gateway • 221
- Routing Multicast Packets Through VPN Tunnels • 75
- Routing Return Packets • 125, 236
- Routing Table Modifications • 174
- Routing Traffic within a VPN Community • 33
- Runtime SCV Checks • 196

S

- Sample • 204
- Sample ipassignment.conf File • 173
- Screened Software Types • 251
- SCV Checks • 197, 209
- SCV Policy Syntax • 199
- SCVGlobalParams • 203
- SCVNames • 202
- SCVPolicy • 203
- Secure Configuration Verification • 195
- Secure Connectivity and Endpoint Security • 145
- Secure Domain Logon (SDL) • 231
- SecureClient • 239
- SecureClient Commands • 286
- SecureClient Connect Profiles and MEP • 234
- SecureClient Remote Access Solution • 149
- SecuRemote • 147
- SecurID Authentication Devices • 164
- Security Features • 150
- Security Gateway Requirements for IPSec/L2TP • 189
- Sending Keep-Alive Packets to the Server • 232
- Server Configuration • 280
- Server Side Configuration • 186, 199
- Server-Side Configuration • 253

- Server-Side Pre-Requisites • 252
- Service Based Link Selection • 105
- Service Based Link Selection Scenarios • 106
- Sets and Sub-sets • 199
- Setting up the Microsoft IPsec/L2TP Client Connection Profile • 192
- Simple Deployment – Internal CA • 41
- Site to Site VPN • 10
- Small IKE Phase II Proposals • 273
- SmartDashboard IKE DoS Attack Protection Settings • 21
- SoftID and SecureClient • 165
- Solution - Working with L2TP Clients • 187
- Solving Remote Access Issues • 227
- Special Condition for VPN Security Gateways • 31
- Special Considerations • 126
- Special Considerations for PKI • 47
- Special Considerations for Planning a VPN Topology • 33
- Special Considerations for the CRL Pre-fetch Mechanism • 46
- Special Considerations for the SSL Network Extender • 251
- Special Considerations for Windows Proxy Replacement • 282
- Special Considerations for Wire Mode • 91
- Split Installation • 181, 183
- SSL Network Extender • 147, 249
- SSL Network Extender Command Attributes • 267
- SSL Network Extender Issues • 269
- SSL Network Extender User Experience • 259
- Star VPN Community • 28
- Stateless Protection Against IKE DoS Attacks • 20
- Structure of Userc.C • 238
- Subnet masks and Office Mode Addresses • 177
- Subnets and Security Associations • 18
- Subordinate Certificate Authorities • 43
- Summary of Remote Access Options • 146
- Supporting a Wide Variety of PKI Solutions • 40

T

- Take out Unneeded Drop Rules • 142
- Terminating Permanent Tunnels • 80
- The Check Point Solution - SecureClient Packaging Tool • 180
- The Check Point Solution for Multiple Entry Points • 234
- The Check Point VPN Solution • 9
- The Difference between SCVNames and SCVPolicy • 203
- The local.scv Sets • 202
- The MSI Packaging Solution • 181
- The Need for Connectivity Resolution Features • 271
- The Need for Desktop Security • 185
- The Need for Multiple Entry Point Security Gateways • 234
- The Need for Remote Clients to be Part of the LAN • 166
- The Need for Supporting L2TP Clients • 187

- The Need for Virtual Private Networks • 24
- The Need for VPN Routing • 219
- The Need to Verify Remote Client's Security Status • 195
- The Problem • 228, 231, 233
- The Product.ini file • 239
- The Secure Configuration Verification Solution • 195
- The Solution • 171, 228, 231, 233
- The Userc.C File • 238
- Third Party SCV Checks • 198
- To configure the CA to Issue Certificates with Purposes • 193
- To Configure the Microsoft IPsec/L2TP Clients so they do not Check for the • 193
- To use a third-party PKI solution: • 161
- Topology • 244
- Topology and Encryption Issues • 29
- Tracing the Status of User's Certificate • 163
- Tracking • 123
- Tracking Options • 80, 87
- Traditional Mode VPNs • 130
- Troubleshooting SSL Network Extender • 269
- Trusted Links • 109
- Trusted Links Scenarios • 111
- Trusted Sites Configuration • 260
- Trusting a CA – Step-By-Step • 47
- Trusting An External CA • 43
- Trusting an Externally Managed CA • 47
- Trusting an ICA • 47
- Trusting an OPSEC Certified CA • 48
- Tunnel Management • 77
- Tunnel Testing for Permanent Tunnels • 78
- Types of Solutions • 144

U

- Understanding DoS Attacks • 19
- Understanding the Terminology • 9
- Uninstall on Disconnect • 265
- Unique SA Per Pair of Peers • 19
- Unnumbered VTI • 63
- Upgrading ESOD • 255
- User Certificate Creation Methods when Using the ICA • 155
- User Certificate Management • 163
- User Certificate Purposes • 190
- User Groups as the Destination in RA communities • 225
- User Privileges • 198
- User Profiles • 151
- Userc.C and Product.ini Configuration Files • 238
- Userc.C File Parameters • 239
- Using a Pre-Shared Secret • 162
- Using Directional VPN for Remote Access • 225
- Using Dynamic Routing Protocols • 63
- Using Name Resolution - WINS and DNS • 169
- Using Office Mode with Multiple External Interfaces • 170
- Using Puzzles to Protect Against IKE DoS Attacks • 20
- Using Route Based Probing • 100
- Using Secure Domain Logon • 232
- Using SmartDashboard • 58

- Using SSL Network Extender on Linux / Mac Operating Systems • 266
- Using the CLI • 59
- Using the Internal CA vs. Deploying a Third Party CA • 47
- Using the Multiple External Interfaces Feature • 174
- Using Trusted Links with Service Based Link Selection • 112
- Utilizing Load Sharing • 103

V

- Validation of a Certificate • 44
- Verifying the SCV Policy • 196
- Visitor Mode • 250, 276
- Visitor Mode and Gateway Clusters • 280
- Visitor Mode and MEP • 235
- Visitor Mode and Proxy Servers • 278
- Visitor Mode in a MEPed Environment • 278
- Visitor Mode When the Port 443 is Occupied By an HTTPS Server • 278
- Visitor Mode with SecurePlatform/IPSO • 278
- VPN Between Internal Gateways Using Third Party CA Certificates • 133
- VPN Command Line Interface • 285
- VPN Commands • 285
- VPN Communities • 10, 25
- VPN Components • 9
- VPN Domains and Encryption Rules • 131
- VPN for a SmartLSM Profile • 57
- VPN for Remote Access Considerations • 155
- VPN High Availability Using MEP or Clustering • 117
- VPN Routing - Remote Access • 219
- VPN Routing and Access Control • 53
- VPN Shell • 289
- VPN Topologies • 27
- VPN Tunnel Interface (VTI) • 62
- VPN Tunnel Sharing • 79, 80
- VPN with One or More LSM Profiles • 57
- VTIs in a Clustered Environment • 65

W

- When Responding to a Remotely Initiated Tunnel • 99
- When the Client Has a Private Address • 228
- When the Converted Rule Base is too Restrictive • 140
- Why Turning off FireWall Implied Rules Blocks Control Connections • 39
- Windows Proxy Replacement • 282
- WINS (Connect Mode Only) • 230
- Wire Mode • 88
- Wire Mode Between Two VPN Communities • 91
- Wire Mode in a MEP Configuration • 89
- Wire Mode Scenarios • 88
- Wire Mode with Route Based VPN • 90
- Working in Connect Mode While Not Connected • 228
- Working with RSA Hard and Soft Tokens • 164

Z

- Zone Labs Endpoint Security Client • 183