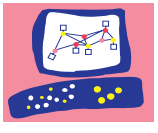
# Check Point™ Virtual Private Networks

*Check Point 2000*

Part No.: 700057
January 2000

CHECK POINT™
Software Technologies Ltd.



*We Secure the Internet.*

---

**Check Point Software Technologies Ltd.**

**International Headquarters:**
3A Jabotinsky Street
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256

e-mail: info@CheckPoint.com

**U.S. Headquarters:**
Three Lagoon Drive, Suite 400
Redwood City, CA 94065
Tel: 800-429-4391 ; (650) 628-2000
Fax: (650) 654-4233

http://www.checkpoint.com

February 2, 2000

Please direct all comments regarding this publication to **techwriters@checkpoint.com.**

# Contents

# Figures

# Tables

# Preface

## Scope

The VPN-1/FireWall-1 User Guide describes CheckPoint VPN-1/FireWall-1, and consists of the following books:

*Getting Started with VPN-1/FireWall-1*

This book introduces VPN-1/FireWall-1 and describes the VPN-1/FireWall-1 installation process.

*VPN-1/FireWall-1 Administration Guide*

This book is the technical reference to VPN-1/FireWall-1 features, including authentication and address translation. In addition, chapters on troubleshooting and Frequently Asked Questions (FAQ) are included.

*Check Point Virtual Private Networks*

This book describes how to implement the Virtual Private Network features in Check Point VPN-1/FireWall-1.

*VPN-1/FireWall-1 Reference Guide*

This book describes INSPECT, the command line interface and other reference subjects, and includes a glossary.

*Account Management Client*

This book describes how to install and use the Check Point Account Management Client.

## Who Should Use this User Guide

This User Guide is written for system administrators who are responsible for maintaining network security. It assumes you have a basic understanding and a working knowledge of:

- system administration
- the Unix or Windows operating system
- the Windows GUI
- Internet protocols (IP, TCP, UDP *etc*.)

## Summary of Contents

Chapter 1, “Introduction,” is an introduction to the subject of encryption, and describes how encryption is implemented in VPN-1/FireWall-1.

Chapter 2, “Encryption Schemes,” decribes the encryption and authentication schemes implemented by VPN-1/FireWall-1.

Chapter 3, “Certificate Authorities,” describes how to define Certificate Authorities and how to create and use certificates in VPN-1/FireWall-1.

Chapter 4, “Implementing IKE Encryption,” decribes how to implement IKE encryption using VPN-1/FireWall-1.

Chapter 5, “Implementing FWZ Encryption,” decribes how to implement FWZ encryption using VPN-1/FireWall-1.

Chapter 6, “Implementing Manual IPSec Encryption,” decribes how to implement Manual IPSec encryption using VPN-1/FireWall-1.

Chapter 7, “Implementing SKIP Encryption,” decribes how to implement SKIP encryption using VPN-1/FireWall-1.

Chapter 8, “Encryption Properties,” describes the VPN-1/FireWall-1 Graphical User Interface (GUI), with which encryption properties are defined.

Chapter 9, “SecuRemote Server,” describes the VPN-1/FireWall-1 SecuRemote Server.

Chapter 10, “SecuRemote Client,” describes the VPN-1/FireWall-1 SecuRemote Client.

Chapter 11, “VPN-1 SecureClient,” describes how to implement LAN security using VPN-1/FireWall-1 SecureClient.

Chapter 12, “High Availability for Encrypted Connections,” describes how Check Point implements high availabilty features for encrypted connections.

Chapter 13, “FWZ Encryption Protocol,” describes the FWZ encryption protocol.

Chapter 14, “Troubleshooting,” describes common problems and their solutions.

## What Typographic Changes Mean

The following table describes the typographic changes used in this book.

**TABLE P-1** Typographic Conventions

| Typeface or Symbol | Meaning | Example |
|---|---|---|
| `AaBbCc123` | The names of commands, files, and directories; on-screen computer output | Edit your `.login` file.<br>Use `ls -a` to list all files.<br>`machine_name% You have mail.` |
| **`AaBbCc123`** | What you type, when contrasted with on-screen computer output | `machine_name% u`<br>`Password:` |
| *AaBbCc123* | Command-line placeholder: replace with a real name or value | To delete a file, type `rm` *filename*. |
| *AaBbCc123* | Book titles, new words or terms, or words to be emphasized | Read Chapter 6 in *User's Guide*.<br>These are called *class* options.<br>You *must* be root to do this. |
| **Save** | Text that appears on an object in a window | Click on the **Save** button. |

**Note –** This note draws the reader's attention to important information.

**Warning –** This warning cautions the reader about an important point.

**Tip –** This is a helpful suggestion.

## Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, Korn shell and DOS.

**TABLE P-2** Shell Prompts

| Shell | Prompt |
|---|---|
| C shell prompt | *machine_name*% |
| C shell superuser prompt | *machine_name*# |
| Bourne shell and Korn shell prompt | $ |
| Bourne shell and Korn shell superuser prompt | # |
| DOS | *current-directory*> |

## Network Topology Examples

Network topology examples usually show a gateway's name as a city name (for example, Paris or London) and the names of hosts behind each gateway as names of popular sites in those cities (for example, Eiffel and BigBen).

CHAPTER 1

# Introduction

## In This Chapter



## Overview

### The Problem

When Bob sends Alice a message over a public network such as the Internet, the message passes through many computers, routers, switches and similar equipment before it arrives at Alice's computer. Charlie has many opportunities to intercept the message along the way and even to alter it, so that the message that Alice receives may be quite different from the one that Bob sent. In fact, Charlie might even send Alice a false message, disguised to appear as though it was sent by Bob.

Alice and Bob want to ensure:

- **Privacy** — that no one can listen to their communication.

  Bob wants to be sure that only Alice can read the message he sends her. Privacy can be achieved by using encryption.

- **Integrity** — that no one is tampering with their communication.

  Bob wants to be sure that the message that Alice will receive is exactly the same message that he sent, that is, that message was not tampered with in transit. Integrity can be achieved through the use of hashing.

- **Authenticity** — that no one is sending false messages.

  Alice wants to be sure that the message she received from Bob really did come from Bob, and not from someone else. Authenticity can be achieved through the use of digital signatures.

## The Check Point VPN-1/FireWall-1 Solution

VPN-1/FireWall-1's optional VPN (Virtual Private Network) module protects communications on the Internet and enables an enterprise to build its own easy-to-maintain Virtual Private Network (VPN) using private and public network segments.

VPN-1/FireWall-1 provides the ideal platform for enterprise VPN deployments, enabling encrypted communications and guaranteeing data privacy, integrity and authenticity. In addition to site-to-site VPN capability, VPN-1/FireWall-1 Gateway deployments provide access to remote users when used with Check Point's VPN-1 SecuRemote Client software. For more information on the SecuRemote Client, see "SecuRemote" on page 10.

Check Point's VPN-1 products support industry-standard algorithms and protocols, such as DES, 3DES, and IPSec/IKE. Digital certificate support is included for organizations with Public Key Infrastructure (PKI) deployments.

## Some Definitions

### Encryption

Encrypting a message modifies ("encrypts") its text ("plaintext" or "cleartext") so that the encrypted text ("ciphertext") can only be read ("decrypted") with the aid of some additional information ("key") known only to the sender and the intended recipient.

### Encryption Algorithm

The detailed sequence of mathematical operations by which the cleartext and key are combined to produce the encrypted text. Examples of encryption algorithms are DES (Data Encryption Standard) and CAST.

### Key Strength

A measure of the difficulty of decrypting text when the encryption algorithm is known and only the key is unknown. The key strength is usually a function of the key length.

### Hashing

A hash is a computation performed on a message whose result can be used to uniquely identify the message, because (a) even a small change in the message leads to a vastly different hash result, and (b) it is computationally unfeasible to compute a message that yields a given hash result.

### Digital Signature

A digital signature is some text that can only have been created by someone who knows a specified secret. Encrypting an agreed-upon text can serve as a digital signature (because decryption produces the agreed-upon text) provided that only the "signer" knows the encryption key.

# Secrecy

## Secret Key Encryption

The simplest way to encrypt a message is by using a secret key, known only to the sender and recipient. Because a secret key is used to both encrypt and decrypt a message, it is also known as a symmetric key. Ensuring the key's secrecy is critical, since anyone who knows the key can decrypt and read the message.

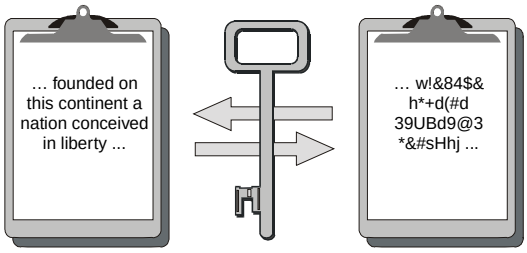



**FIGURE 1-1** Encrypting and then decrypting with a secret key

### Sharing a Secret Key

Secret key encryption is simple and fast, but it has two disadvantages:

- A secure channel is required by which the correspondents can agree on a key before their first encrypted communication.

  This is a serious drawback, because if such a channel existed, there might be no need for encryption. Agreeing on a secret key by direct face-to-face negotiation may be impractical or unfeasible, and the correspondents may have to agree on a key by mail or telephone or some other relatively insecure means.

- The number of keys required can quickly become unmanageable, since there must be a different key for each pair of possible correspondents.

  For example, the number of keys that must be managed for 10,000 entities (people or computing devices) is about 50 million!

## Public Key Encryption

Public key systems, where each correspondent has a pair of keys, can solve both these problems.

A key-pair is composed of two mathematically related keys: a public key known to everyone, and a private key known only to its owner. A message encrypted with one of the keys in a key-pair can only be decrypted with the other key in the pair.[1] Because different keys are used for encryption and decryption, they are known as asymmetric keys.

1. This section describes the RSA public key scheme, where the public and private keys are used to encrypt and decrypt messages. In contrast, the Diffie-Hellman public key scheme is used to exchange secret keys without communicating secret information. VPN-1/FireWall-1 uses both RSA and Diffie-Hellman keys.

If Bob wants to send Alice a message, he encrypts the message with Alice's public key before sending it to her. Because the message was encrypted with Alice's public key, it can only be decrypted with Alice's private key. The only person who knows Alice's private key is Alice herself, so only Alice can read the message. If Charlie were to somehow intercept the message, he would be unable to read it because he doesn't know Alice's private key.

## Integrity

Bob wants to be sure that the message that Alice receives is the same message that he sent, in other words, that no one tampers with the message while it is in transit on the network. To ensure the message's integrity, Bob computes a hash of the message.

A hash is a mathematical computation ("hash function") performed on the text of the message. The hash function is designed so that changing even one bit in the message results in a completely different hash result, and there is no practical way to reverse the computation, that is, to compute a message from a given hash result. So the hash result uniquely identifies the message.

When Alice receives the message, she decrypts it, applies the same hash function and compares her hash result to Bob's hash result.

If they are the same, then Alice can be sure that the message was not tampered with, because the hash she calculated is the same one that Bob calculated.

## Authenticity

Bob also wants Alice to be able to verify that the message actually came from him and not from an impostor, so Bob attaches his digital signature to the message. A digital signature acts as proof of the sender's identity and the message's integrity.

One widely-used technique for creating digital signatures is for Bob to encrypt some pre-agreed text (for example, the hash result) with his private key (which only he knows). Alice can then decrypt the digital signature with Bob's public key and compare it to the hash result she calculated. If they are the same, she knows that the message can only have come from Bob.

## Summary

To summarize, here is a step-by-step description of one way that Bob can send Alice a message so that they can both be sure that only Alice can read the message, and Alice can be sure that the message she receives was sent by Bob and was not tampered with:

1. First, Bob computes a hash of the message.
2. Bob encrypts the hash with his own private key — this is the digital signature.

   Only Bob can do this, because only he knows his private key.
3. Bob encrypts the message with Alice's public key.
4. He then sends Alice both the encrypted hash and the encrypted message.

When she receives the message, Alice can confirm that it was sent by Bob and also that it was not tampered with, as follows:

***5*** First, she decrypts the message using her private key.

Only Alice can do this, because only she knows her private key.

***6*** Next, she decrypts the digital signature using Bob's public key.

***7*** Alice calculates the hash value of the unencrypted message (this is the same calculation that Bob performed) and compares it to the hash value received from Bob.

If they are the same, then Alice can be sure that:

- The message was sent by Bob, because Bob is the only person who knows Bob's private key and thus the only person who could have encrypted the hash value.
- The message was not tampered with, because the hash value Alice calculated is the same one that Bob calculated.

**Note –** In this scenario, the hash value serves two purposes: it confirms the message's integrity and is also the pre-agreed text of the digital signature. It is possible to use some other pre-agreed text, but the hash value is convenient because it is different for each message and doesn't actually have to be agreed on in advance.

## Public Key vs. Private Key Technology

Public key encryption requires significantly more computation effort than private key encryption, and so is much slower. In practice, encrypted communication sessions are often divided into two phases:

- a preliminary, relatively short key negotiation (exchange) phase, secured by inefficient public key encryption, in which a private key is negotiated (exchanged) for encrypting the actual message (communication)

  IKE (Internet Key Exchange, formerly known as ISAKMP/OAKLEY) and SKIP (Simple Key-Management for Internet Protocols) are examples of commonly-used key exchange mechanisms.

- the message encryption phase, in which the message is encrypted using the efficient private key negotiated in the first phase

  DES (Data Encryption Standard) and CAST are examples of commonly-used encryption algorithms.

# Certificates

## Verifying Public Keys

### Trusting a Public Key

Since public keys are the basis for secure encryption, there needs to be a reliable way of obtaining public keys. For example, if Bob and Alice obtain each others' public keys over an insecure channel such as the Internet, they must be certain that the keys are genuine. Alice cannot simply ask Bob for his public key, because there is the danger that Charlie might intercept Alice's request and send Alice his own key instead. Charlie would then be able to read all of Alice's encrypted messages to Bob (and Bob would not be able to read them).

### What is a Certificate Authority?

A Certificate Authority (CA) is a trusted third party from whom public keys (and possibly other information) can be reliably obtained, even over an insecure channel.

### What is a Certificate?

A certificate is issued by a trusted Certificate Authority and identifies the bearer (which may be a person or computer) and contains some information about the bearer. For example, a CA might send Bob's certificate to Alice. If Alice trusts the CA, then she by implication trusts the information in the certificate. This information might be:

- Bob's unique identifier (for example, his LDAP Distinguished Name)
- Bob's public key
- the CA's unique identifier, so that anyone examining a certificate can know who issued it
- a digital signature, signed with the CA's private key

Alternatively, Bob can send Alice his certificate directly. In either case, Alice can verify the certificate (this is equivalent to verifying Bob's public key) by the procedure described earlier. To do this, she needs the CA's public key, which must be reliably available from an out-of-band source, such as a printed directory.

To prove his identity to Alice, Bob sends her a message consisting of:

- a digital signature, encrypted with his private key
- his certificate (if Alice doesn't already have it) which includes his unique identifier (for example, his LDAP Distinguished Name and IP address)

Alice verifies the digital signature using Bob's public key (from the certificate), proving that the message could only have been encrypted by Bob and that the information it contains (specifically, Bob's unique identifier, which is in both the certificate and the message) is genuine. In this way, Bob can prove who he is and what his IP address is, and Alice can be confident that she is communicating with Bob and not with someone else who is pretending to be Bob.

After Alice and Bob prove their identities in this way, they can use each other's public keys with confidence, because they are certified by certificates from a trusted CA. Usually, the public keys are used to negotiate a secret key for encrypting the actual message.

**Note –** In a Virtual Private Network, certificates are also used by encrypting entities (for example, gateways) to identify themselves and supply their public keys to their peers.

To summarize, a certificate is like a passport. It identifies the bearer and contains some important information about him or her.

### Passports

A passport is issued by a government, and presented by the bearer to anyone who needs to verify the bearer's identity.

A passport consists of the following elements:

1. Proof that the passport belongs to the bearer: the bearer's photograph.
2. Some important information about the bearer: for example, the bearer's name.
3. An expiration date.
4. Proof that the passport is genuine and that it has not been tampered with: the issuer's seal and the special paper on which the passport is printed are intact.

For example, Alice Smith might present her US passport to Donna, an airport immigration official, to prove her identity. Donna believes that Alice is who she claims to be (that is, that she is a US citizen named Alice Smith) because:

1. The passport belongs to Alice and not to someone else (the picture is Alice's picture).
2. Donna can see that Alice's passport has not been tampered with.
3. Donna trusts the issuer (that is, she trusts the US State Department to issue passports in a reliable way).
4. Alice's passport has not yet expired (the expiration date printed in the passport has not passed)

If Bob tries to use Alice's passport, he will be found out because Alice's photograph doesn't match his face. If Bob tries to replace Alice's photograph with his own, the tampering will be immediately noticeable.

## Certificates

A certificate is issued by a trusted Certificate Authority and identifies the bearer (which may be a person or computer). A certificate is often embedded in a token, which is either an encrypted disk file or a hardware device, such as a smart card. The token has a password, or PIN. Only someone who physically has the token (the file or device) in his or her possession and knows its PIN can use the token.

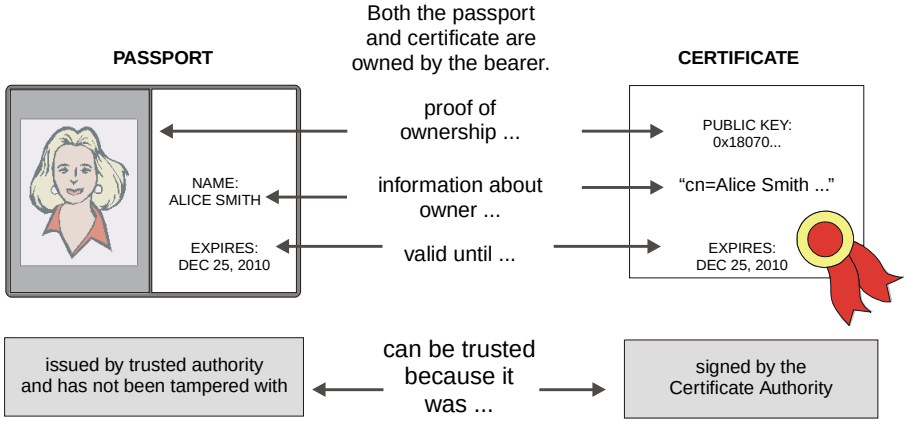



**FIGURE 1-2** Passports and Certificates

**Note –** In one popular model, the information in the token is called a profile. In addition to the certificate, the profile includes the Certificate Authority's public and private keys (used for validating information signed by the Certificate Authority, such as a CRL). The profile is kept either on a hardware device or is saved as a file on a diskette, limiting physical access and minimizing the possibilities of misuse.

The certificate contains some important information about the bearer.

1. Proof that the certificate belongs to the bearer: for example, the bearer's public key.

   The public key is considered proof, because the signature can be verified with it.

2. Some important information about the bearer: for example, the bearer's DN (Distinguished Name).

3. An expiration date.

4. Proof that the certificate is genuine and has not been tampered with: a digital signature.

   The entire certificate, including its hash, is signed by the Certificate Authority, proving that the certificate could only have been created by the Certificate Authority.

Bob cannot use Alice's certificate for two reasons:

1. Bob doesn't have Alice's private key.

   The private key is on a hardware token (a physical device) which is in Alice's possession, and which she carefully guards. With some physical devices, the private key is physically protected and cannot be read out.

2. Even if Bob had the certificate (for example, if he has stolen the hardware token), he still doesn't know the access password (PIN).

   Only Alice knows the access password. Without the password, the certificate cannot be used.

The certificate's security is based on these factors:

- the difficulty of obtaining (and reading) the physical device on which the certificate is stored
- the secrecy of the access password (PIN).

## Creating Certificates

A user's certificate is created by a Certificate Authority. There are several different ways in which the user acquires the certificate, depending on the PKI vendor:

1. A file (sometimes called a "profile") is created, either by the user or by the Certificate Authority.
   - One method is for the user to create the profile on his or her own computer, using special client software (for example, the Check Point SecuRemote Client). The user can then store the profile file on a diskette or on a hardware token, minimizing the possibility of its unauthorized copying and misuse. Some hardware tokens can generate the key pairs on the device, providing enhanced security for the user's private key. The profile file is further protected by the access password, known only to the user.
   - A second method is for the Certificate Authority to create the profile file (preferably on a hardware token) and then give it to the user. This method centralizes the creation of profile files, but may be impractical in a geographically dispersed organization.
2. The user registers to the Certificate Authority using a Web browser, and can then export the certificate and private key for the use of other applications.
3. The user creates a certificate registration request in a file, and transfers the file (via mail, ftp, *etc*.) to the Certificate Authority. The Certificate Authority approves the request and generates the certificate on a file, which is transferred back to the user (again using mail, ftp, etc).

### Certificate Revocation Lists

When a user leaves an organization, or when a key is compromised (for example, when a token is stolen), the user's certificate must be revoked. The Certificate Authority does this by issuing and distributing a Certificate Revocation List (CRL), a list of certificates that are no longer valid.

Certificate Revocation Lists are issued periodically, at fixed intervals, by a Certificate Authority, but they can be issued at any time if required. Before accepting a certificate, the CRL should be examined to confirm that the certificate has not been revoked. The CRL's distribution point — the address from which an up-to-date CRL can be obtained — usually an LDAP or HTTP-based Web Server — is usually specified in the certificate.

### Certificate Authorities

#### IKE

In the IKE encryption scheme, an encrypting gateway's CA is specified in the **Certificates** tab of the **Workstation Properties** window. The CA itself is defined in the **CA Properties** window. See also Chapter 3, "Certificate Authorities" of *Check Point Virtual Private Networks* for more information.

#### FWZ and SKIP

In the FWZ and SKIP encryption schemes, FireWalled Management Modules function as Certificate Authorities for the encrypting gateways.

## VPN-1 Accelerator Card

In addition to the standard software implementation, Check Point VPN-1 IKE encryption can be implemented in a hardware accelerator card, significantly increasing the throughput and reducing CPU utilization.

VPN-1 Accelerator Card is installed on the encrypting gateway. Its installation is completely transparent, and no changes to the Rule Base or configuration files are required.

**Note** – The VPN-1 Accelerator Card supports IKE encryption only.

## SecuRemote

### Overview

Check Point VPN-1 SecuRemote enables PC users to securely communicate sensitive and private information to networks and individual servers. Check Point VPN-1 SecuRemote extends the VPN to Windows 9x and Windows NT workstations and desktops, using both dial-up and LAN connections.

Typical uses for SecuRemote are:

- Specific employees can be granted encrypted access to sensitive corporate data.
- A server can be set up to provide encrypted information to paying customers only. Because the communication is encrypted, eavesdropping is impossible.
- Users at a remote office can conduct encrypted communications with the FireWalled enterprise network without installing VPN-1/FireWall-1 at the remote office.
- General network access (email, intranet Web, *etc*.) can be provided for remote employees such as telecommuters and business travelers.
- A group of workers dealing with sensitive information can create private workgroups over internal, shared-access networks such as Ethernets by using VPN-1 SecuRemote and encryption-enabled application servers.

VPN-1 SecuRemote is based on a technology called Client Encryption. Because SecuRemote encrypts data before it leaves the laptop, it offers a completely secure solution for remote connections.

VPN-1 SecuRemote can transparently encrypt any TCP/IP communication. There is no need to change any of the existing network applications on the user's PC. SecuRemote can interface with any existing adapter and TCP/IP stack. A PC on which SecuRemote is running can be connected to several different VPN-1/FireWall-1 sites.

A VPN-1/FireWall-1 security manager can enable access for SecuRemote users with the standard VPN-1/FireWall-1 Rule Base editor. After a SecuRemote user is authenticated, a completely transparent secured connection is established and the user is treated just as any user in the Virtual Private Network. The network administrator can enforce VPN-1/FireWall-1 security features, including authentication servers, logging and alerts, on SecuRemote connections (just as with any other connection).

The configuration below depicts a Virtual Private Network with a nomadic SecuRemote user securely connected to the Enterprise network through the Internet.

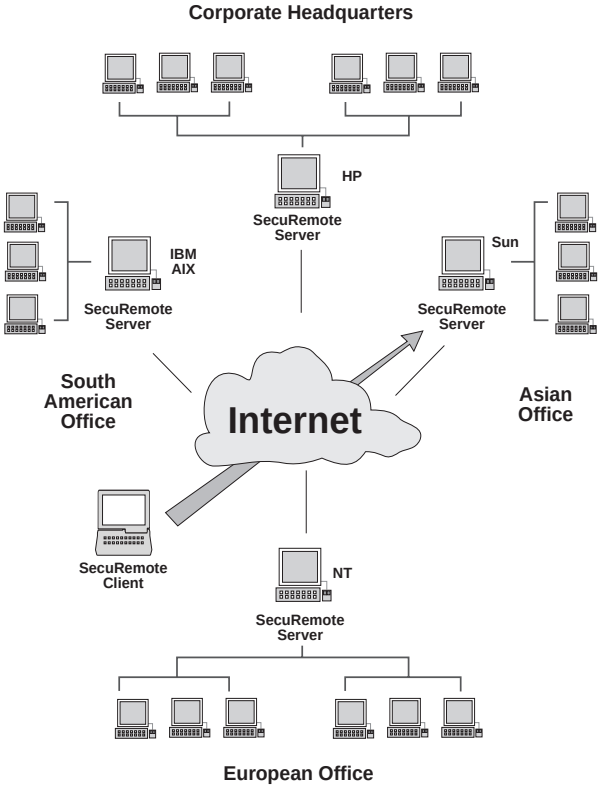



**FIGURE 1-3** Virtual Private Network with a nomadic SecuRemote Client

SecuRemote includes support for dynamic IP addressing, which is necessary for dial-up communication. SecuRemote can also be used from stationary PC's with fixed IP addresses.

SecuRemote supports IKE key exchange, as well as the proprietary FWZ protocol. Strong user authentication is supported by means of Entrust certificates, as well as a number of other authentication schemes (RADIUS, S/Key, password *etc*). Encryption schemes include (in accordance with export restrictions):

- IKE using DES, triple DES or 40 bit encryption
- FWZ (a Check Point proprietary scheme) using DES or FWZ1

## Additional Information

For information about configuring the SecuRemote Server (VPN/FireWall Module), see Chapter 9, “SecuRemote Server” of *Check Point Virtual Private Networks*.

For information about the SecuRemote Client software, see Chapter 10, “SecuRemote Client” of *Check Point Virtual Private Networks*.

CHAPTER 2

# Encryption Schemes

## In This Chapter



## Encryption Schemes

### Elements of an Encryption Scheme

An encryption scheme consists of the following elements:

- **a key management protocol** — for generating and exchanging keys
- **an encryption algorithm** — for encrypting messages
- **an authentication algorithm** — for ensuring integrity, that is, that messages have not been tampered with

# Encryption Schemes Supported by VPN-1/FireWall-1

VPN-1/FireWall-1 supports the following encryption schemes (TABLE 2-1).

**TABLE 2-1** Encryption Schemes

| encryption scheme | authentication algorithm | encryption algorithm | encryption is ... |
|---|---|---|---|
| Manual IPSec — Manual IPSec is an industry-standard fixed key encryption and authentication scheme. | MD5, SHA-1, CBC-DES MAC | DES, RC2 | encapsulated |
| IKE — IKE (formerly known as ISAKMP/OAKLEY) adds key management features to Manual IPSec. | HMAC-MD5, HMAC-SHA-1 | DES (triple DES for key encryption), CAST | encapsulated; the traffic encryption is IPSec |
| SKIP — Like IKE, SKIP (Simple Key-Management for Internet Protocols) adds key management features to Manual IPSec. | MD5, SHA-1, CBC-DES MAC | DES (triple DES for key encryption) | encapsulated; the traffic encryption is IPSec |
| FWZ — FWZ is a proprietary FireWall-1 encryption scheme. | MD5 | DES, FWZ1 | in-place |

DES, FWZ1, CAST, RC2, and RC4 are all encryption algorithms used to encrypt the data portion of a packet.

# Manual IPSec Encryption Scheme

Manual IPSec is an encryption and authentication scheme. A Security Association (SA) is associated with each packet, consisting of:

- functionality — indicates whether the packet is encrypted, authenticated, or both
- algorithms — specifies the encryption algorithm (for example, DES) and the authentication algorithm (for example, MD5) used in the packet
- keys used in the above algorithms
- additional data, for example, initialization vector (IV)

A 32-bit number, known as the Security Parameters Index (SPI), identifies a specific SA. An SPI is simply an identifier, assigned by the correspondents themselves in a particular context, and has no meaning outside that context.

## Encryption

IP packets are encrypted in accordance with the Encapsulating Security Payload (ESP) standard (RFC 1825, 1827 and 1829). As its name implies, the ESP standard specifies that the original packet is encrypted and then encapsulated into a new, longer packet.

There are two modes of performing this encapsulation:

- Tunnel Mode
- Transport Mode (not supported by VPN-1/FireWall-1)

### Tunnel Mode

In the tunnel mode, the entire packet (including the IP header) is encrypted in accordance with the SA previously decided upon by the correspondents. An ESP header containing the SPI and other data is added to the start of the packet, and a new IP header is constructed.

The new packet (which is of course larger than the original packet) consists of:

- the new IP header
- the ESP header
- the encrypted original packet

The new packet is then sent on its way. An advantage of this mode is that the destination specified in the new IP header may be different from the one in the original IP header. It is thus possible to send the packet to a host which performs decryption on behalf of a number of other hosts; the decrypting host decrypts the packet, strips the ESP and IP headers added by the encrypting host, and then sends the original packet to its destination. Tunnel mode closely corresponds to the VPN-1/FireWall-1 encryption model, where gateways encrypt and decrypt on behalf of other hosts.

### Transport Mode (not supported by VPN-1/FireWall-1)

In the transport mode, the IP header is not encrypted. An ESP header is inserted between the IP header and the transport layer header. The transport layer header and everything following is encrypted.

This mode does not increase the length of the packet as much as the Tunnel Mode does (no additional IP header is added). The encrypted packet must be sent to its original destination.

Transport mode is not supported by VPN-1/FireWall-1, because it is designed for end-to-end encryption, and does not allow for the case where gateways encrypt and decrypt on behalf of other hosts.

### Authentication

If authentication is specified by the SA, then an Authentication Header (AH) is added to the packet, in addition to the ESP header (and to the second IP header in Tunnel Mode).

VPN-1/FireWall-1 conforms to the Authentication standards described by RFC 1825, 1826, 1828 and 1852.

### Shortcomings

Manual IPSec has two shortcomings:

- the keys are fixed for the connection's duration
- there is no mechanism for exchanging keys

Both IKE and SKIP address these shortcomings.

# IKE Encryption Scheme

IKE is a standard for negotiating Security Associations (SAs) between two hosts that will be using IPSec, and is the key management scheme that was chosen for IP Version 6. In IP Version 4, IKE is optional. IKE offers improved authentication (HMAC) and Perfect Forward Secrecy (PFS).

The VPN-1/FireWall-1 implementation of IKE supports the Entrust PKI (Public Key Infrastructure).

IKE key exchange is divided into two phases:

### IKE Phase One (Main/Aggressive Mode)

In this phase, the peers negotiate an IKE Security Association that will be used for encrypting and authenticating Phase Two exchanges. Phase One involves long and CPU-intensive computations, and so is executed infrequently. A cookie exchange mechanism precedes the computations in order to prevent denial-of-service attacks.

The negotiated SA includes the encryption method, authentication method and keys. This SA is used in the Phase Two negotiation.

VPN-1/FireWall-1 supports two modes for Phase One:

- aggressive mode (the default), in which three packets are exchanged
- main mode, in which six packets are exchanged

### IKE Phase Two (Quick Mode)

Using the SA negotiated in Phase One, the peers negotiate an SA for encrypting the IPSec traffic. Keys can be modified as often as required during a connection's lifetime by performing Phase Two.

# SKIP Encryption Scheme

SKIP, developed by Sun Microsystems, adds two features to Manual IPSec:

- improved keys

  Manual IPSec uses fixed keys. In contrast, SKIP uses a hierarchy of constantly changing keys.

- key management

  Manual IPSec does not provide a mechanism by which users can exchange keys. SKIP implements a key management protocol for Manual IPSec.

SKIP provides a hierarchy of keys that change over time, which are used to encrypt the connection as well as to implement a key management protocol. SKIP also includes ESP and AH, and adds its own header to the packet.

The Encryption Key and the Authentication Key are derived from the Session Key, which changes at fixed intervals, or when the amount of data encrypted exceeds a given threshold. The newly changed Session Key is communicated by encrypting it with the Kijn key, which changes once every hour. The Kijn key is derived from the Diffie-Hellman shared secret Kij key, using a cryptographic hash function (see “Public Key Schemes” on page 20). Each correspondent obtains the public part of the other correspondent’s Diffie-Hellman key from a Certificate Authority, which signs the transmission with its own RSA key.

SKIP includes a protocol (Certificate Discovery Protocol) for this exchange of public keys. However, this protocol is not supported by VPN-1/FireWall-1, which uses instead a proprietary protocol for key exchange. VPN-1/FireWall-1 also supports manual key exchange.

## FWZ (VPN-1/FireWall-1) Encryption Scheme

Under the VPN-1/FireWall-1 encryption scheme (FWZ), a message is encrypted with a secret key derived in a secure manner from the correspondents’ Diffie-Hellman keys (see “Public Key Schemes” on page 20). The Diffie-Hellman keys are authenticated by a Certificate Authority.

TABLE 13-1 on page 253 lists the keys used in the FWZ encryption scheme.

Under this scheme, the number of keys that must be managed is proportional to the number of correspondents. This is in contrast to some other schemes, in which the number of keys to be managed is proportional to the square of the number of correspondents.

The TCP/IP packet headers are not encrypted, to ensure that the protocol software will correctly handle and deliver the packets. The cleartext TCP/IP header is combined with the session key (derived from the Basic Session Key; see TABLE 2-2 on page 20 for details) to encrypt the data portion of each packet, so that no two packets are encrypted with the same key. A cryptographic checksum is embedded in each packet (utilizing otherwise unused bits in the header) to ensure its data integrity.

Encryption is in–place. A packet’s length remains unchanged, so the MTU remains valid and efficiency is not compromised.

# Comparison of Encryption Schemes

TABLE 2-2 presents a high-level comparison of the encryption schemes supported by VPN-1/FireWall-1.

**TABLE 2-2** Comparison of Encryption Schemes

| feature | Manual IPSec | IKE | SKIP | FWZ |
|---|---|---|---|---|
| portability | standard | standard | standard supported by Sun and other vendors | CheckPoint proprietary |
| key management | manual | automatic; external PKI | automatic | automatic |
| Session Keys | fixed | keys change at configurable times during connection's lifetime | keys change over time or as amount of data exceeds threshold | each TCP or UDP session has a new key |
| number of keys is proportional to the … | square of the number of correspondents | square of the number of correspondents | number of correspondents | number of correspondents |
| packet size | increased | increased | increased | unchanged |
| PFS (Perfect Forward Secrecy) | | yes | | |
| Replay Protection | | yes | | |
| Certificate Authority | | specified in the **Certificates** tab of the gateway's **Workstation Properties** window | | a local or remote VPN-1/ FireWall-1 Management Station |

# Public Key Schemes

VPN-1/FireWall-1 supports two types of public keys:

- Diffie-Hellman

  A Diffie-Hellman public-private key pair is used for calculating a secret key, which is in turn used for encrypting and decrypting messages. No secret information is communicated during the key exchange, so it does not require a secure channel.

- RSA Public Keys (Certificates)

  In contrast to a Diffie-Hellman public-private key pair, an RSA public-private key pair is used for encrypting and decrypting messages. A message encrypted with the public key can only be decrypted with the private key, and *vice versa*. The key exchange involves the communication of secret information, so it must be protected by using certificates (see "Certificates" on page 6).

## Diffie-Hellman Scheme

In the Diffie-Hellman scheme, no secret information is communicated during the key exchange, so a secure channel is not required. Only one key pair needs to be managed for each correspondent (instead of one key for each pair of correspondents). The correspondents compute a shared secret key, which they use to encrypt and decrypt messages between them.

FIGURE 2-1 illustrates this computation, using the private and public parts of Alice's and Bob's Diffie-Hellman keys. The process is as follows:

1. Bob gets Alice's public key and performs a calculation involving his own private key and Alice's public key.

2. Alice gets Bob's public key and performs a calculation involving her own private key and Bob's public key.

The results of both calculations are the same, and this result is the secret key. No secret information is communicated, so there is no opportunity for an eavesdropper to determine the secret key.

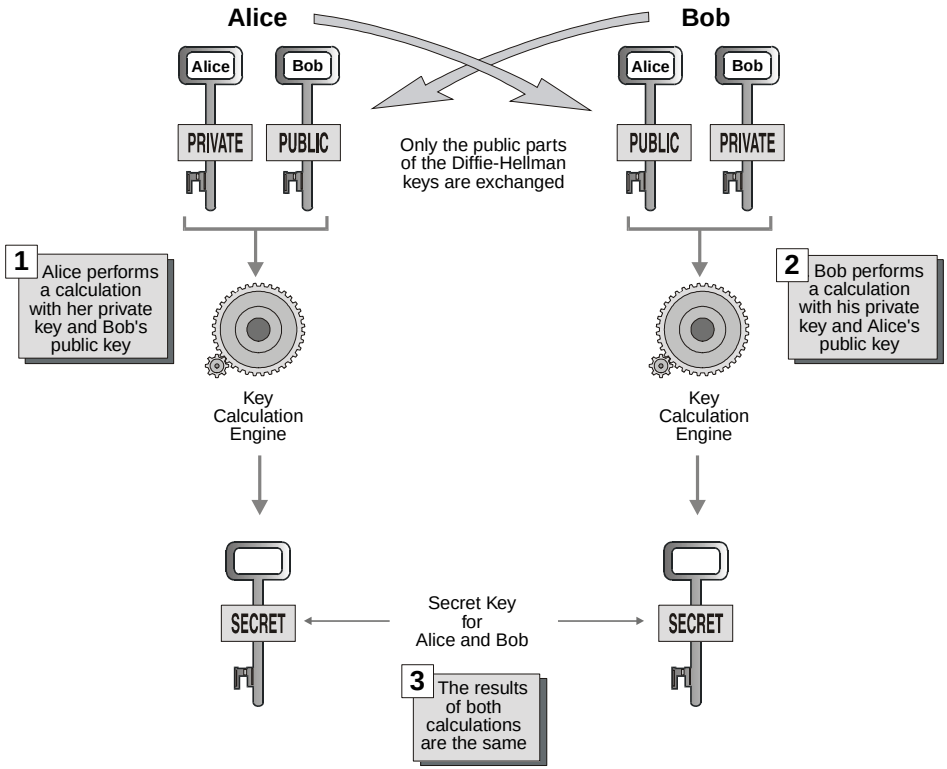



**FIGURE 2-1** Agreeing on a Secret Key by exchanging the public parts of Diffie-Hellman keys

# Intel RNG

VPN-1/FireWall-1 and SecuRemote use the  Intel RNG (random number generator) hardware (when installed) as a seed for generating cryptographic random numbers.

A special Intel hardware component must be present on the motherboard. Supported Operating Systems are: Windows NT 4.0, Windows 98, Windows 95 (OSR2 or later or Windows 95 with IE 3.02 or later). Please refer to Intel's web site for more details.

To determine whether the Intel RNG is active, use the `fw intelrng` command (on the VPN/FireWall Module) or see **Help➤About** in SecuRemote.

You should install Intel's Security driver from the VPN-1/FireWall-1 installation CD (under 3rd party) or from Intel's web site. If the Security driver installation is taken from Intel's web site, only the full installation — which installs both the driver and the CAPI (Microsoft Cryptographic API) CSP (Cryptographic Service Provider) — should be used.

## fw intelrng

`fw intelrng` displays the status of the Intel RNG. This command is a Windows NT only command.

Syntax

```
fw intelrng
```

Examples

```
#fw intelrng
Using Intel(R) Security Driver.
```

```
#fw intelrng
Intel(R) Security Driver not detected.
```

CHAPTER 3

# Certificate Authorities

## In This Chapter



## Overview

### Using Certificates

A Certificate Authority (CA) issues certificates to entities (users or computers) which the entities later use to identify themselves and provide verifiable information about themselves. For example, a certificate includes an entity's DN (Distinguished Name — the identifying information) and public key (information about itself) and possibly its IP address. After two entities exchange and validate each others' certificates, they can begin encrypting communications between them using the public keys in the certificates.

There are two kinds of entities that can identify themselves using certificates:

- encrypting gateways (workstations), when encrypting with other (peer) encrypting gateways or with SecuRemote Clients
- people (using SecuRemote Clients) — the SecuRemote Client and the site confirm each others' identities with certificates

Certificates are used in gateway-to-gateway (peer-to-peer) encryption when both gateways have **Public Key Signatures** enabled in their **IKE Properties** windows (FIGURE 8-5 on page 108).

Certificates are used in SecuRemote Client-to-site encryption when the gateway has **Public Key Signatures** enabled in the **IKE Properties** window (FIGURE 8-5 on page 108) and the user has **Public Keys** enabled in the **IKE Properties** tab of the **User Properties** window (FIGURE 9-9 on page 137).

## Multiple Certificate Authorities

In a small network, a single Certificate Authority may be sufficient, but as networks change, requirements change as well. For example, a company might wish to authenticate and encrypt communications with its suppliers or customers, or with newly-acquired subsidiaries, who may have Certificate Authorities of their own.

In such cases, a VPN must be able to:

- acquire and recognize different kinds of certificates (for example, Entrust and OPSEC PKI)
- trust more than one CA (that is, validate certificates issued by more than one CA, including processing Certificate Revocation Lists)
- acquire more than one certificate for an entity (but note that an entity can only have one certificate from each CA)

This chapter describes how to implement this functionality in Check Point VPN-1/FireWall-1.

## Trusting Certificates

A certificate can be trusted if it is possible to validate that:

- the certificate was issued by a trusted Certificate Authority, *and*
- it has not been revoked, that is, it does not appear in a Certificate Revocation List (CRL).

For a detailed description of certificates and why they can be trusted, see “Certificates” on page 6.

VPN-1/FireWall-1 trusts all the CAs defined in its database (see “Defining Certificate Authorities” on page 25).

## Enabling the Use of Certificates in VPN-1/FireWall-1

To use certificates in VPN-1/FireWall-1, proceed as follows:

1. Make the necessary arrangements with the Certificate Authority.

   These arrangements may require that you install special software at your site.

2. Define the CA to VPN-1/FireWall-1 (see “Defining Certificate Authorities” on page 25).

3. Generate the certificates.

   The details of this step depend on the type of the CA.

The VPN-1/FireWall-1 IKE implementation supports X.509 digital certificates supplied by the following Public Key Infrastructure (PKI) implementations:

- Check Point VPN-1 Certificate Manager
- OPSEC PKI vendors
- Entrust Technologies

# Defining Certificate Authorities

**Warning** – Each CA defined to VPN-1/FireWall-1 must have a unique DN (within the name space of all the CA's known to VPN-1/FireWall-1). A CA's DN is defined when the CA is created (not when it is defined to VPN-1/FireWall-1).

To define a Certificate Authority, proceed as follows:

1. Open the **Server Objects** window (FIGURE 3-1) by:
   - choosing **Servers** from the **Manage** menu, *or*
   - selecting  from the toolbar.

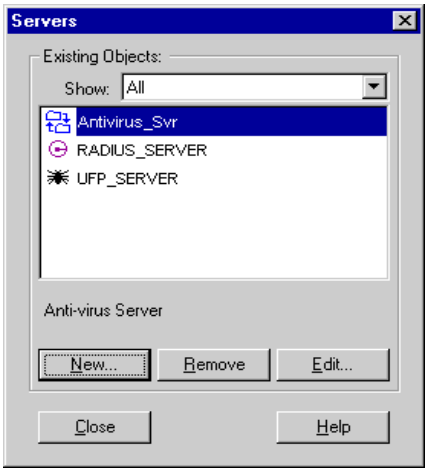



**FIGURE 3-1** Servers window

**2** Click on **New**.

A menu appears (FIGURE 3-2), listing the types of servers you can create.

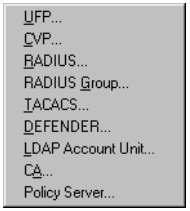



**FIGURE 3-2** Add Server menu

**3** Choose **CA** from the menu and click on **OK**.

The **General** tab of the **CA Properties** window (FIGURE 3-3 on page 26) is displayed.

The next steps in this procedure depend on the type of CA being defined (see TABLE 3-1).

**TABLE 3-1** Defining a CA — the next steps

| If you are defining a CA of type ... | ... see ... |
|---|---|
| Entrust or VPN-1 Certificate Manager | "Entrust Certificate Authority (Entrust or VPN-1 Certificate Manager)" on page 26 |
| OPSEC PKI | "OPSEC PKI Certificate Authority" on page 28 |

## Entrust Certificate Authority (Entrust or VPN-1 Certificate Manager)

After completing step 1 through step 3 above, continue as follows:

**1** Define the CA and specify its type (Entrust or VPN-1 Certificate Manager) in the **General** tab of the **CA Properties** window (FIGURE 3-3).

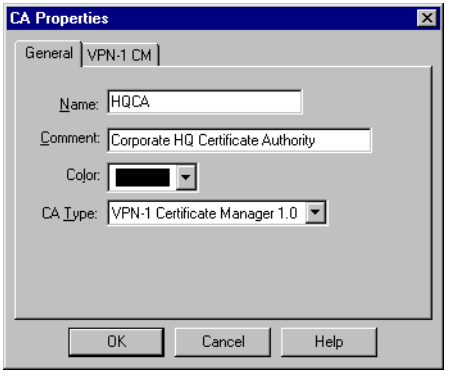



**FIGURE 3-3** CA Properties window — General tab

**2** In the **Entrust PKI** tab or the **VPN-1 CM** tab of the **CA Properties** window (FIGURE 3-4 on page 27 — these tabs are functionally identical despite their different names), configure the Entrust CA.

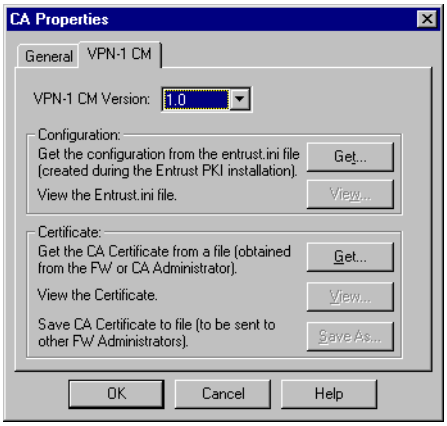



**FIGURE 3-4** CA Properties window — VPN-1 CM tab

**Entrust PKI Version** — Specifies the version of the Entrust PKI on which the VPN-1 Certificate Manager is based.

**Configuration** — The `entrust.ini` file (provided by your Entrust CA administrator) specifies the location and other parameters of an Entrust CA. Click on one of the following (under **Configuration**):

- **Get** — Get the CA's configuration from the `entrust.ini` file.

  You can browse for the `entrust.ini` file.
- **View** — View the `entrust.ini` file.

**Certificate** — Before you can validate certificates issued by the CA you have just defined, you must obtain the CA's own certificate.

- If a Management Station will be generating certificates on this CA (see "Generating Entrust Certificates" on page 30), then the CA sends the Management Station its own certificate together with the workstation's certificate. In this case, there is no need to explicitly obtain the CA's own certificate — it is obtained as a by-product of generating other certificates.
- If a Management Station will *not* be generating certificates on the CA but only validating them, then you must explicitly obtain the CA's own certificate by clicking on **Get** (see below).
  - **Get** — Get the CA's certificate from a file that contains the CA's certificate.

    The CA's certificate can be provided by another VPN-1/FireWall-1 administrator (who has already generated a certificate from the CA) using the **Save As** button (see below).

**View** — View the CA's certificate.

**Save As** — Save the CA's certificate to a file, which can be read by another Management Station using the **Get** button.

## OPSEC PKI Certificate Authority

After completing step 1 through step 3 above, continue as follows:

1. Define the CA and specify its type (OPSEC PKI), using the **CA Properties** window (FIGURE 3-3 on page 26).

2. In the **OPSEC PKI** tab of the **CA Properties** window (FIGURE 3-5), specify how CRLs are obtained under **Retrieve CRL From**.


**FIGURE 3-5** CA Properties window — OPSEC PKI tab

3. If you select **LDAP Servers** (under **Retrieve CRL From**), then define the LDAP Server as a VPN-1/FireWall-1 Account Unit (see "VPN-1/FireWall-1 LDAP Account Management" on page 174 of *VPN-1/FireWall-1 Administration Guide*).

**Warning –** If you fail to define the LDAP Server as a VPN-1/FireWall-1 Account Unit, certificates issued by the CA will be considered invalid because the CRL cannot be obtained. **CRL Retrieval** must be checked under **LDAP Usage** in the **LDAP Account Unit Properties** window (FIGURE 10-17 on page 335 of *VPN-1/FireWall-1 Administration Guide*).

Before you can validate certificates issued by the CA you have just defined, you must obtain the CA's own certificate out-of-band from the CA administrator.

**Certificate** — Before you can validate certificates issued by the CA you have just defined, you must obtain the CA's own certificate from the CA administrator.

Click on (under **Certificate**):

- **Get** — Get the CA's certificate from a file that contains the CA's certificate.
- **View** — View the CA's certificate.

- **Save As** — Save the CA's certificate to a file, which can be read by another Management Station using the **Get** button.

# Generating Certificates

Before you can generate a certificate on a CA, you must define the CA to VPN-1/FireWall-1 (see "Defining Certificate Authorities" on page 25).

## Check Point VPN-1 Certificate Manager and Entrust Certificates

An Entrust Certificate is created in a two-step process (see "Generating Entrust Certificates" on page 30 for a step-by-step description of this procedure):

1. Preparation:

   A VPN-1/FireWall-1 administrator asks an Entrust administrator to issue a Reference Number and Authorization Code that will be used at some later time to generate a certificate.

2. Generation:

   An Entrust-enabled client (for example, Check Point VPN-1/FireWall-1) requests that the Entrust CA generate a certificate based on the Reference Number and Authorization Code the Entrust administrator issued in the previous step.

   VPN-1/FireWall-1 saves the certificate on the Management Station and downloads the certificate to the workstation when the Security Policy or the User Database is installed (see "Database Installation" on page 167 of *VPN-1/FireWall-1 Administration Guide*).

   For information about how to create Entrust certificates, see "Generating Entrust Certificates" on page 30.

## OPSEC PKI Certificates

**Note –** For a list of OPSEC PKI-compliant CA vendors, see http://www.checkpoint.com.

An OPSEC PKI Certificate is created in a four-step process (see "Generating OPSEC PKI Certificates" on page 32 for a step-by-step description of this procedure):

1. A VPN-1/FireWall-1 administrator generates a PKCS #10 certificate request using VPN-1/FireWall-1 (see FIGURE 3-9 on page 32).

2. The VPN-1/FireWall-1 administrator contacts the CA and requests the certificate.

   This is usually done using a Web browser and HTTPS.

3 At some later time, the CA sends the certificate to the VPN-1/FireWall-1 administrator.

The CA administrator can provide information about how long you can expect to wait before receiving the certificate.

4 The VPN-1/FireWall-1 administrator enters the certificate in the VPN-1/FireWall-1 database (see FIGURE 3-6 on page 30).

## Generating Entrust Certificates

1 Define the workstation for which the CA will generate a certificate.

See Chapter 4, “Network Objects” of *VPN-1/FireWall-1 Administration Guide* for information on how to define workstations.

2 Obtain a Reference Number and Authorization Code for the workstation’s certificate from the CA, using an Entrust-enabled client (for example, Check Point VPN-1 Certificate Manager or Entrust/Admin).

3 Open the **Certificates** tab of the workstation’s **Workstation Properties** window (FIGURE 3-6 on page 30).


**FIGURE 3-6** Workstation Properties Window — Certificates tab

If the **Certificates** tab is not visible, click on  to scroll the tabs until the **Certificates** tab becomes visible.

**4** Click on **Add** to open the **Certificate Properties** window (FIGURE 3-7).

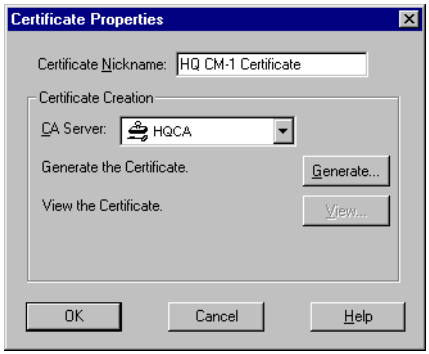



**FIGURE 3-7** Certificate Properties window (Entrust)

**5** Select the Entrust CA that will issue the certificate.

**6** Specify a nickname for the certificate.

You must specify a nickname for each certificate because a workstation can have more than one certificate.

**7** Click on **Generate**.

**8** In the **Generate Keys and Get Entrust Certificate** window (FIGURE 3-8), enter:

- **Generation Mode** — Select **Initialize** to generate a new certificate.

  **Recover** is used to create a new certificate when a certificate has been compromised. **Refresh** is used to "refresh" a certificate when its expiration date is near.

- **Reference Number** and **Authorization Code** — These values (generated by the Certificate Authority) were given to you by your system administrator.

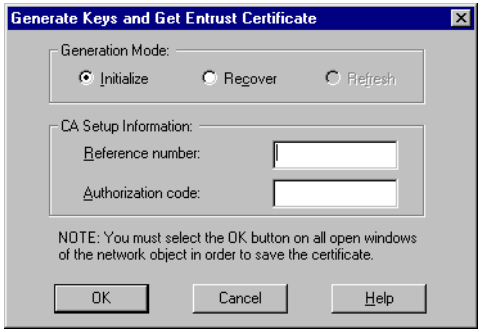



**FIGURE 3-8** Generate Keys and Get Entrust Certificate window

**9** Click on **OK**.

The workstation's certificate is generated and saved in the Management Station's database. The certificate can be viewed by clicking on **View** in the **Certificate Properties** window (FIGURE 3-7 on page 31).

In addition, the CA's own certificate is retrieved and can be viewed by clicking on **View** in the **VPN-1 CM** or **Entrust PKI** tab (FIGURE 3-3 on page 26 — these tabs are functionally identical despite their different names) of the **CA Properties** window.

When you generate an Entrust certificate, the following sequence of events takes place:

- An RSA key pair is generated.
- The public part of the key is sent to the Entrust Certificate Authority.
- The Entrust Certificate Authority computes a certificate and signs it.
- The Entrust Certificate Authority sends the certificate (as well as its own certificate) to the VPN-1/FireWall-1 Management Server.
- The Management Server stores the certificate (as well as the CA's own certificate) in the VPN-1/FireWall-1 database.

## Generating OPSEC PKI Certificates

1. Define the workstation for which the CA will generate a certificate.

   See Chapter 4, "Network Objects" of *VPN-1/FireWall-1 Administration Guide* for information on how to define workstations.

2. Open the **Certificates** tab of the workstation's **Workstation Properties** window (FIGURE 3-6 on page 30).

3. Click on **Add** to open the **Certificate Properties** window (FIGURE 3-9).

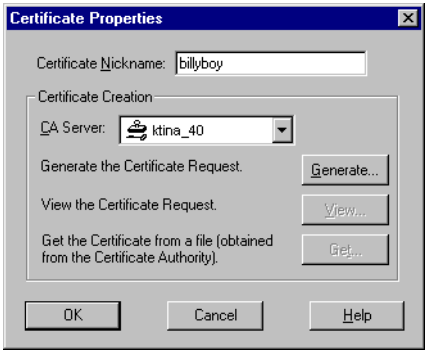



**FIGURE 3-9** Certificate Properties window (OPSEC PKI)

4. Select the OPSEC PKI CA that will issue the certificate.

5. Specify a nickname for the certificate.

   You must specify a nickname for each certificate because a workstation can have more than one certificate.

**6** Click on **Generate** to generate the PKCS #10 certificate request.

You will be asked to specify the file that contains the CA's certificate.

**7** In the **Generate Certificate Request** window, specify the CA's full DN.

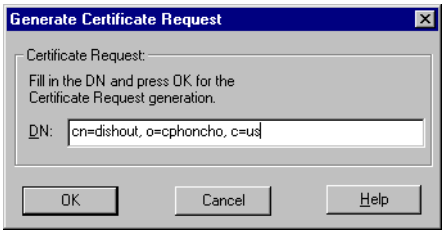



**FIGURE 3-10** Generate Certificate Request window (OPSEC PKI)

**8** Click on **OK**.

**9** Click on **View** to display the **Certificate Request View** window (FIGURE 3-11).


**FIGURE 3-11** Certificate Request View window (OPSEC PKI)

**10** Select the text in the window and copy it to the clipboard.

**11** Contact the CA and request the certificate.

This is usually done using a Web browser and HTTPS.

You may be asked to paste the text you copied in the previous step into the PKCS #10 certificate request field in the browser.

**Warning –** Do not click on **Cancel** in the **Certificate Properties** window (FIGURE 3-9 on page 32). If you do click on **Cancel**, the key information will be lost and the certificate you obtain afterwards (step 15 on page 34) will not be accepted.

**12** Close the **Certificate Request View** window (FIGURE 3-11).

13 When the CA sends the certificate to the administrator, save the certificate as a file.

**Note** – The CA administrator can provide information about how long you can expect to wait before receiving the certificate.

14 Return to this certificate's **Certificate Properties** window (FIGURE 3-9 on page 32).

15 Click on **Get** and specify the name of the file that contains the certificate you received from the CA.

16 Click on **OK.**

# Rule Base

## VPN-1 Certificate Manager and Entrust

In order to enable the Management Station to create certificates, the following rules must be added to the Rule Base:

- A rule that allows connections between the Management Station and the CA for the Entrust-CA group of services.
- A rule that enables LDAP connections (the ldap or ldap-ssl service) between Management Station and the LDAP Server.

# Advanced Topics

## Multiple CAs

If Enterprise A wants to conduct IKE encryption with Enterprise B using certificates, then Enterprise A and Enterprise B must trust each others CAs. See "External Gateways" on page 51 for information on how to configure this capability.

## SecuRemote

When a SecuRemote user and a site authenticate each other using certificates, the SecuRemote Client trusts only the CA that signed the user's certificate. If the site's certificate is signed by a different CA (even if the gateway's CA is in the same hierarchy as the user's CA — see FIGURE 3-12 on page 35), the authentication will fail.

## CA Hierarchy

In a CA hierarchy (where a CA's certificate is issued by another CA), only the highest level trusted CA must be defined (even if there are other CA's higher up in the hierarchy). Certificates issued by a CA subordinate to a defined (trusted) CA are also trusted.

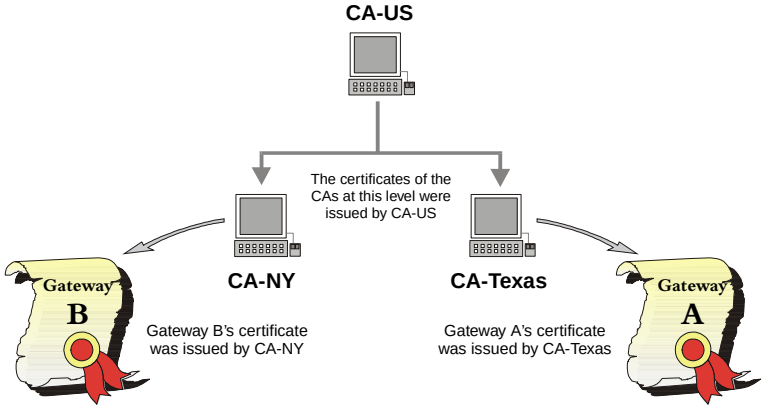



**FIGURE 3-12** CA hierarchy

For example, suppose both Gateway A and Gateway B (FIGURE 3-12) trust CA-US (that is, they have both defined CA-US as a Certificate Authority), and CA-NY's and CA-Texas' own certificates were both issued by CA-US. Then Gateway A and Gateway B will also trust both CA-NY and CA-Texas.

So if Gateway A has a certificate issued by CA-Texas and Gateway B has a certificate issued by CA-NY, then Gateway A and Gateway B will accept each others certificates.

## Deployment Scenarios

This section describes some typical environments containing VPN-1/FireWall-1 and PKI components.

## CA Service over the Internet

FIGURE 3-13 depicts a configuration in which the CA and HTTP are accessed over the Internet.

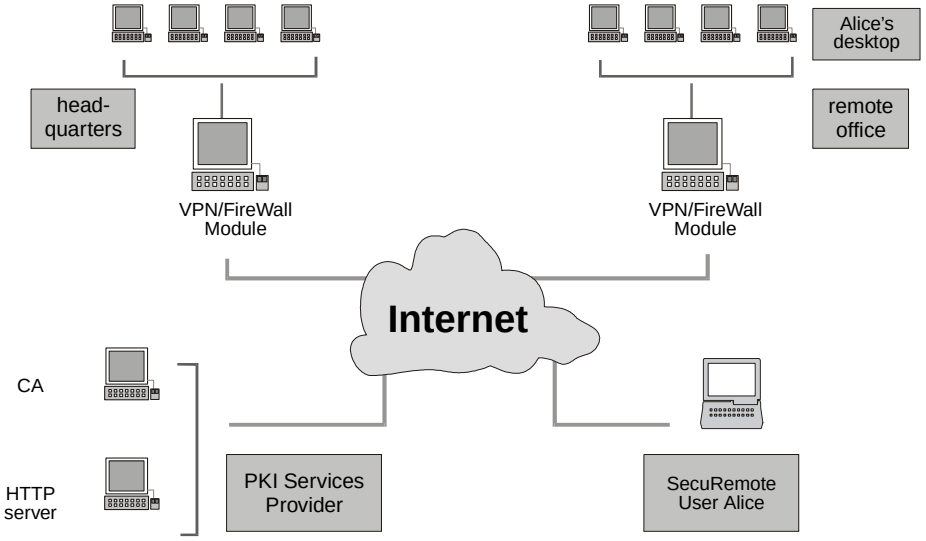



**FIGURE 3-13** CA Service over the Internet

The scenario in FIGURE 3-13 describes a PKI where the CA and the CRL repository are active servers that can be reached using the Internet. In this model, all Check Point VPN-1/FireWall-1 components are assumed to have access to the CRL repository, using HTTP.

The VPN-1/FireWall-1 Management Station manages keys and certificates on behalf of the VPN/FireWall Modules. The certification process involves interaction between the VPN-1/FireWall-1 Management Station and the CA. In FIGURE 3-13, the two VPN/FireWall Modules can create a VPN between them using their keys and certificates to authenticate one another. The SecuRemote User Alice can generate a key pair on her own and contact the CA to receive a certificate. She can then use her key and certificate to establish a VPN between her mobile or home PC and any of the offices (in FIGURE 3-13, Headquarters for POP3 or Remote Office to access her desktop).

## Local CA

FIGURE 3-14 depicts a configuration in which the CA and HTTP are accessed locally.

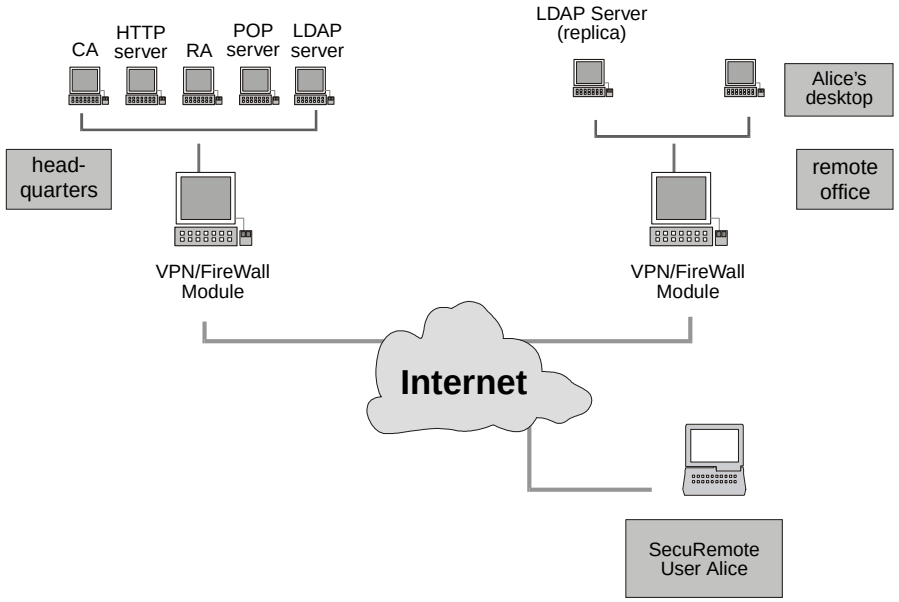



**FIGURE 3-14** Local CA

The scenario in FIGURE 3-14 describes a PKI where the CA and the CRL repository are local servers managed by the security administrator in the Headquarters. SecuRemote users are not assumed to have access to the LDAP servers (and thus, they cannot download CRLs). The VPN/FireWall Module in the Remote Office can access a local replica of the LDAP server. The Remote Office VPN/FireWall Module is assumed to have access to an LDAP server containing the CRLs.

The VPN-1/FireWall-1 Management station manages keys and certificates on behalf of the VPN/FireWall Modules. The certification process involves interaction between the VPN-1/FireWall-1 Management Station and the CA.

In FIGURE 3-14, the two VPN/FireWall Modules can create a VPN between them using their keys and certificates to authenticate one another. The SecuRemote User Alice can generate a key pair on her own and contact the CA to receive a certificate. She can then use her key and certificate to establish a VPN between her mobile or home PC and any of the offices (in FIGURE 3-14, Headquarters for POP3 or Remote Office for access to her desktop). The SecuRemote software mandates that the CRL be sent to it, and fails IKE negotiations if a valid CRL is not sent to it as part of the IKE negotiation.

CHAPTER 4

# Implementing IKE Encryption

## In This Chapter



## Overview

This chapter presents a step-by-step description of how to implement IKE encryption in VPN-1/FireWall-1.

FIGURE 4-1 on page 40 shows a corporate internetwork where three private networks (HQ-net, London-net and DMZ-net) are connected to the Internet through FireWalled gateways. HQ is the Management Station for itself and London. The private networks are protected by the FireWalled gateways, but the public part of the network — the Internet — must be considered insecure.

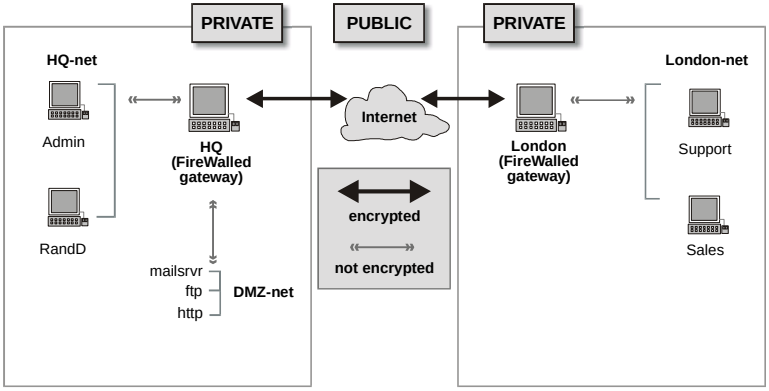



**FIGURE 4-1** Two Gateway Network Configuration

## Specifying Encryption

To specify encryption between London-net and HQ-net, you must answer the following questions:

***1*** Who will encrypt?

Define:

- the encrypting gateways (in the **Workstation Properties** window — see FIGURE 4-2 on page 42)
- their encryption domains (in the **VPN** tab of the **Workstation Properties** window — see FIGURE 4-3 on page 43)

***2*** What are the encryption keys?

The connection itself is encrypted using IPSec. However, before the encrypted connection can begin, the IKE key negotiation takes place. During IKE key negotiation, the encrypting gateways identify themselves to each other and then negotiate an encryption key for encrypting the IPSec connection.

The gateways identify themselves to each other by presenting their credentials. These are defined for each gateway in the **IKE Properties** window (FIGURE 4-4 on page 43). There are two kinds of credentials:

- pre-shared secret (defined for a pair of gateways)

  Each gateway proves that it knows a pre-shared secret (sometimes known as a “password”). This pre-shared secret is defined in the **Shared Secret** window (FIGURE 4-6 on page 45).

- certificates

  Each gateway presents a certificate, which contains identifying information and the identity of the Certificate Authority that issued the certificate. For information about certificates, see “Certificates” on page 6.

***3*** What connections will be encrypted, and how?

Add a rule (or rules) to the Rule Base specifying encryption — see “Example — Adding an Encryption Rule to a Rule Base” on page 48.

Since the gateways support several different encryption and authentication algorithms, you must specify each rule’s encryption parameters in the rule’s **IKE Properties** window (see FIGURE 4-11 on page 47). The parameters must be supported by both gateways.

**Note –** The parameters defining the IKE key negotiation are defined in the gateway’s **IKE Properties** window (FIGURE 4-4 on page 43). The parameters defining the encrypted connection itself are defined the rule’s **IKE Properties** window (FIGURE 4-11 on page 47).

## Encryption Domains

A gateway performs encryption on behalf of its encryption domain: the local area network (LAN) or group of networks that the gateway protects. Behind the gateway, in the internal networks, packets are not encrypted.

For example, if the system administrator has specified that communications between HQ and London are to be encrypted, VPN-1/FireWall-1 encrypts packets traveling between them on the Internet. A packet traveling from Sales to Admin is encrypted on the London-HQ segment of its trip, but not encrypted on the Sales-London and HQ-Admin segments.

# A Two Gateway Configuration

## Both Gateways FireWalled

To encrypt communications between HQ's encryption domain and London's encryption domain (FIGURE 4-1 on page 40) using the IKE encryption scheme, proceed as follows on HQ, their Management Station:

1 Define HQ and London, the gateways that will perform the encryption.

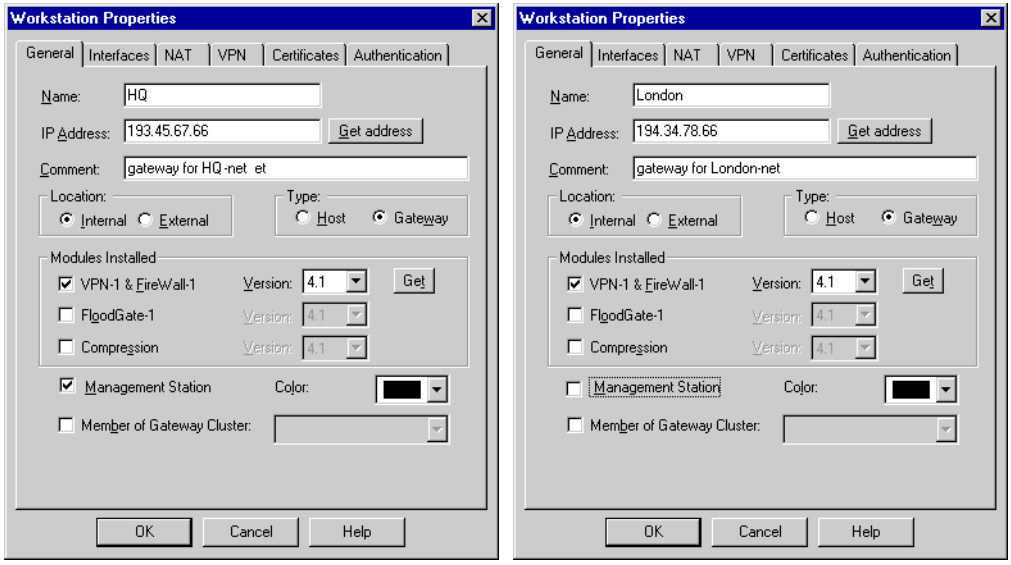



**FIGURE 4-2** Encrypting Gateways (HQ and London)

2 Define HQ-net, London-net and DMZ-net as networks.

See "Network Properties" on page 115 of *VPN-1/FireWall-1 Administration Guide* for information about defining networks.

**3** Open the **VPN** tab of HQ's **Workstation Properties** window (FIGURE 4-3).

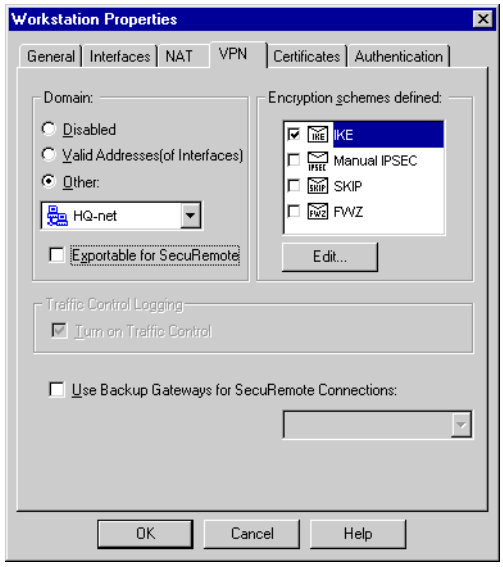



**FIGURE 4-3** HQ's Workstation Properties — VPN tab

For information about the fields in this window, see "Workstation Encryption Properties" on page 105.

**4** In **Domain**, click on **Other** and choose **HQ-net** from the drop-down list.

**5** In **Encryption schemes defined**, check **IKE** and click on **Edit**.

The **IKE Properties** window (FIGURE 4-4) is displayed.

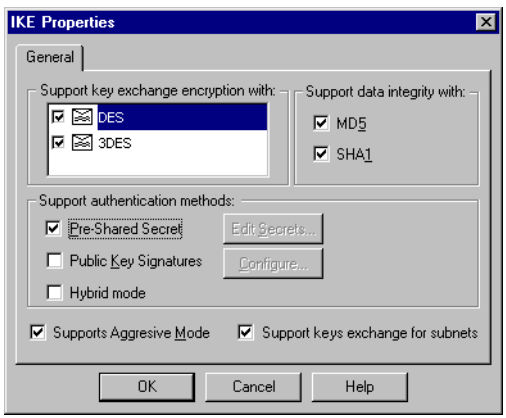



**FIGURE 4-4** IKE Properties window — General tab

For information about the fields in this window, see "IKE Properties" on page 108.

6 In **Key Negotiation Encryption Method(s)**, check one or more encryption method.

These will be used to secure parts of the IKE key negotiation.

7 Check one or more **Hash Method**.

8 Check **Pre-shared Secrets**.

**Note –** This example describes pre-shared secret credentials. For information about using certificates, see "Using Certificates" on page 50.

At this point, you must define London's encryption properties, so that you will be able to define the pre-shared secret between HQ and London.

9 Open the **VPN** tab of London's **Workstation Properties** window (FIGURE 4-5).

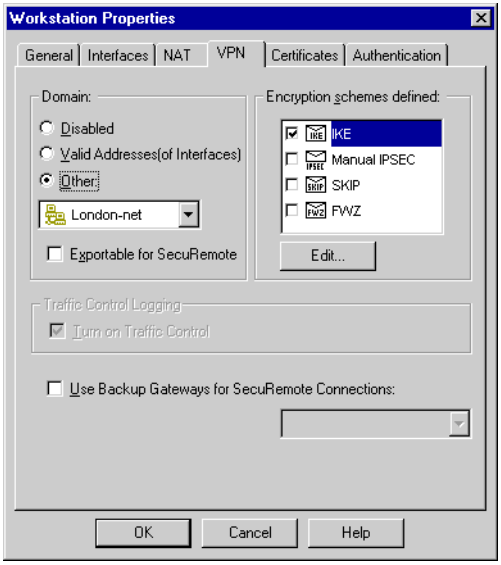



**FIGURE 4-5** Workstation Properties — VPN tab

10 In **Domain**, click on **Other** and choose **London-net** from the drop-down list.

11 In **Encryption schemes defined**, check **IKE** and click on **Edit**.

The **IKE Properties** window (FIGURE 4-4 on page 43) is displayed.

12 In **Key Negotiation Encryption Method(s)**, check one or more encryption method.

13 Check one or more **Hash Method**.

14 Check **Pre-shared Secrets**.

15 Click on **Edit Secrets**.

The **Shared Secret** window (FIGURE 4-6) is displayed.

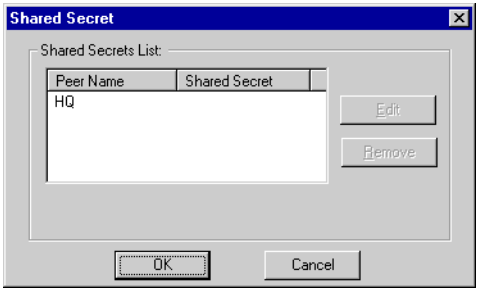



**FIGURE 4-6** Shared Secret window

***16*** Select HQ (highlight it) and click on **Edit**.

**Note –** If HQ is not listed, then you probably skipped step 8 on page 44.

An edit box appears (FIGURE 4-7), in which you should enter the shared secret.

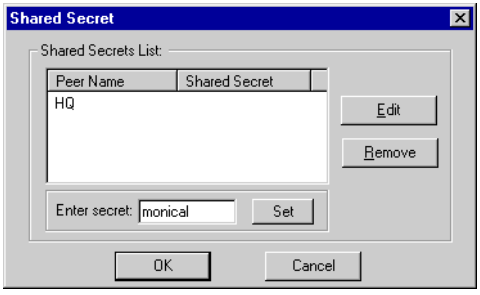



**FIGURE 4-7** Shared Secret window with newly-entered secret

***17*** Enter the shared secret and click on **Set**.

A pre-shared secret is defined per gateway-pair.

The **Shared Secret** window now shows the pre-shared secret (as a string of asterisks) next to HQ's name.

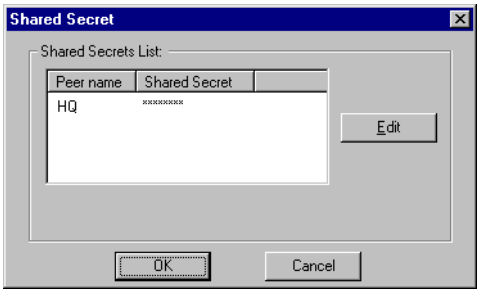



**FIGURE 4-8** London's Shared Secrets window showing the London-HQ shared secret

***18*** Define a network object group (for example, "Enterprise") consisting of all the networks that will participate in the encryption (HQ-net and London-net).

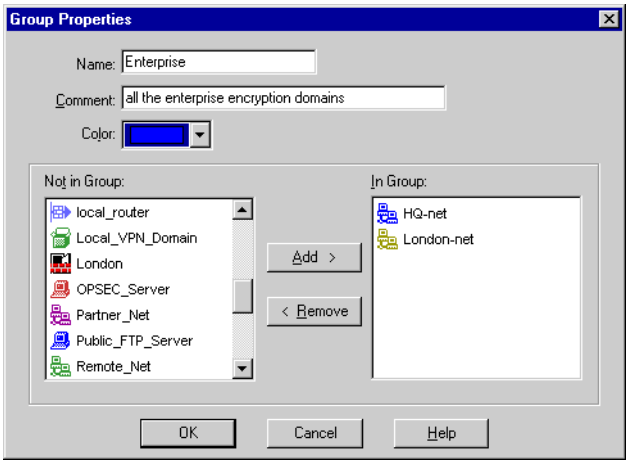



**FIGURE 4-9** Enterprise group definition

***19*** Define a rule in the Rule Base that specifies **Encrypt** as the **Action** for communications between members of the Enterprise group.

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| Enterprise | Enterprise | Any | Encrypt | Long Log | Gateways |

The **Encrypt** action means:

- encrypt outgoing packets
- decrypt incoming encrypted packets and accept them

**Note –** You can also add encryption to an Authentication rule (User, Client or Session) by right-clicking on the Action and selecting **Add Encryption** from the menu.

***20*** In the rule, double-click on **Encrypt** in the rule's **Action** column to display the **General** tab of the **Encryption Properties** window (FIGURE 4-10).

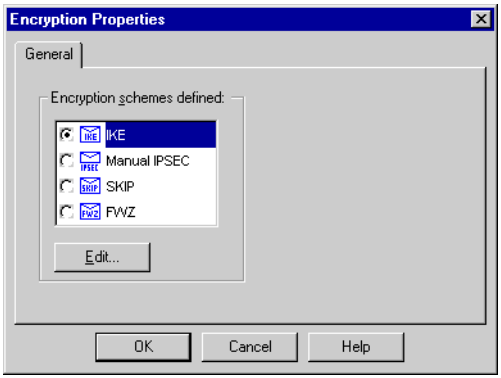



**FIGURE 4-10** Encryption Properties window — General tab

***21*** Click on **IKE**.

***22*** Click on **Edit** to display the **IKE Properties** window (FIGURE 4-11).

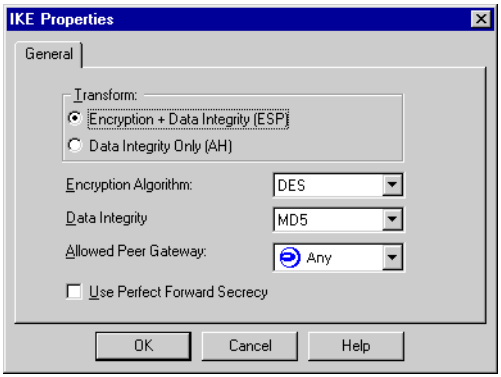



**FIGURE 4-11** IKE Properties window

This window defines the IPSec methods that will be used to encrypt connections to which this rule applies. In contrast, the **VPN** tab of the **Workstation Properties** window (FIGURE 4-3 on page 43) defines the methods used during the IKE key exchange that precedes the encrypted connection.

For information about the fields in this window, see “IKE Encryption Properties” on page 118.

***23*** Install the Security Policy on the gateways (HQ and London).

## Example — Adding an Encryption Rule to a Rule Base

TABLE 4-1 shows a simple Rule Base for the network configuration shown in FIGURE 4-1 on page 40.

**TABLE 4-1** Rule Base without Encryption

| | Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | DMZ-net | Enterprise | Any | Reject | Long Log | Gateways |
| 2 | Enterprise | Any | Any | Accept | Short Log | Gateways |
| 3 | Any | DMZ-net | ftp, http, smtp | Accept | Short Log | Gateways |
| 4 | AllUsers@Any | Any | telnet | UserAuth | Long Log | Gateways |
| 5 | Any | Any | Any | Reject | Long Log | Gateways |

**Note** – The simplified Rule Base shown here is for illustration only, and should not be viewed as a recommendation.

The Rule Base is explained in TABLE 4-2.

**TABLE 4-2** Explanation of Rule Base

| Rule No. | Explanation |
|---|---|
| 1 | prevents DMZ-net from initiating traffic to the internal networks |
| 2 | allows all internal hosts to go out to the Internet |
| 3 | allows unrestricted access to FTP, HTTP and SMTP on DMZ-net |
| 4 | specifies User Authentication for incoming telnet to internal hosts |
| 5 | rejects and logs all other communications |

The encryption rule should be inserted before the second rule in the Rule Base. In this way, mail between Enterprise hosts will be encrypted, but mail from an Enterprise host to other hosts will not be encrypted.

TABLE 4-3 on page 49 shows the Rule Base after the encryption rule has been added before the original second rule, which has now become the third rule.

**TABLE 4-3** Rule Base with Encryption Rule Added

| | Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | DMZ-net | Enterprise | Any | Reject | Long Log | Gateways |
| 2 | Enterprise | Enterprise | Any | Encrypt | Long Log | Gateways |
| 3 | Enterprise | Any | Any | Accept | Short Log | Gateways |
| 4 | Any | DMZ-net | ftp, http, smtp | Accept | Short Log | Gateways |
| 5 | AllUsers@Any | Any | telnet | UserAuth | Long Log | Gateways |
| 6 | Any | Any | Any | Reject | Long Log | Gateways |

## Only One Gateway FireWalled (Extranet)

VPN-1/FireWall-1 is interoperable with other software that implements IKE and IPSec standards. You can also encrypt connections between VPN-1/FireWall-1 sites and these sites.

If only one of the gateways has VPN-1/FireWall-1 installed and the other does not (for example, if HQ has VPN-1/FireWall-1 installed and Madrid does not), proceed as follows:

1. Define the other gateway (Madrid) as an external object in the **General** tab of its **Workstation Properties** window (FIGURE 4-12 on page 50).

2. Coordinate the IKE and IPsec parameters with Madrid's system manager.

   For example, you must coordinate the key negotiation methods (see FIGURE 4-4 on page 43), including shared secrets or certificates, and the IPSec encryption parameters (see FIGURE 4-11 on page 47).

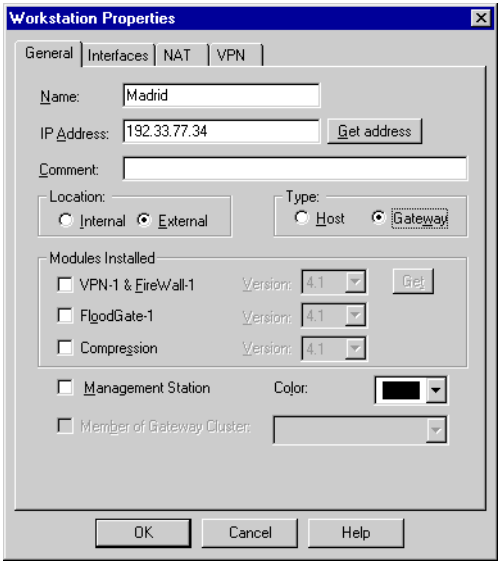



**FIGURE 4-12** Workstation Properties window (Madrid)

## Using Certificates

To configure IKE key negotiation between HQ and London to use certificates rather than pre-shared secrets, proceed as follows:

1. Define the Certificate Authorities that your site (that is, your Management Station and all the gateways it manages) will trust.

   For information on how to define a CA, see “Defining Certificate Authorities” on page 25.

2. Generate certificates for HQ and London.

   For information on how to generate certificates, see “Generating Certificates” on page 29.

3. In the **IKE Properties** window for HQ and London (FIGURE 4-4 on page 43), check **Public Key Signatures**.

**Note –** A pre-shared secret is an attribute of a pair of entities, but a certificate is an attribute of a single entity. If a pre-shared secret is defined for a pair of gateways, and each of the gateways has a certificate as well, then IKE key negotiation between the gateways will use the pre-shared secret rather than the certificates.

**4** Click on **Configure** to display the **Public Key Matching Criteria** window (FIGURE 4-13) to define the matching criteria.

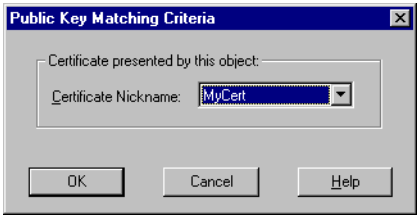



**FIGURE 4-13** Public Key Matching Criteria window (internal workstation)

**5** In **Certificate Nickname**, select the certificate from the list. The available certificates are listed in the **Certificates** tab of the **Workstation Properties** window (FIGURE 3-6 on page 30).

For more information about the **Public Key Matching Criteria** window, see "Public Key Configuration" on page 111.

## External Gateways

VPN-1/FireWall-1 can also accept certificates from external gateways, if the Management Station trusts the CA that issued the certificate. For example, if Madrid (see FIGURE 4-12 on page 50) is an external gateway and Madrid's CA is defined to HQ, then HQ trusts Madrid's certificate if the matching criteria are met, as defined in the **Public Key Matching Criteria** window (FIGURE 4-15).

**1** Define Madrid's CA (see "Defining Certificate Authorities" on page 25).

**2** Obtain Madrid's CA's own certificate.

- If Madrid's CA is an Entrust and VPN-1 Certificate Manager CA, see "Entrust Certificate Authority (Entrust or VPN-1 Certificate Manager)" on page 26 for information on how to obtain its certificate.
- If Madrid's CA is an OPSEC PKI CA, see "OPSEC PKI Certificate Authority" on page 28 for information on how to obtain its certificate.

**3** If Madrid's CA provides its CRLs via LDAP, define an Account Unit for the LDAP Server (see "VPN-1/FireWall-1 LDAP Account Management" on page 174 of *VPN-1/FireWall-1 Administration Guide*).

Entrust and VPN-1 Certificate Manager CAs provides their CRLs via LDAP, but in this case it is not necessary to define an Account Unit. OPSEC PKI CAs can provide CRLs either via LDAP or HTTP (see FIGURE 3-5 on page 28).

**4** Click on **Configure** in Madrid's **IKE Properties** window (FIGURE 4-14).

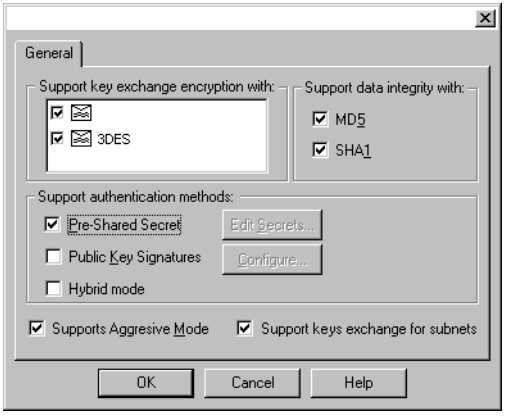



**FIGURE 4-14** IKE Properties window (Madrid)

The **Public Key Matching Criteria** window for external gateways (FIGURE 4-15) will be displayed.


**FIGURE 4-15** Public Key Matching Criteria window (external workstations)

In **Public Key Matching Criteria** window, specify the criteria for matching the certificate to the gateway, in other words, for confirming that the certificate belongs to the gateway presenting it. The options are ORed, in other words, if there is a match on any of them, the certificate is accepted, even if some or all of the others do not match.

## Examples

- If the **DN** is checked, and the DN in the certificate matches the external gateway's DN, the certificate is accepted.
- If **IP Address/DNS** is checked, and either the IP address or the DNS name (for example, "ourfriendlysupplier.com") in the certificate matches the external gateway's IP address or DNS name, the certificate is accepted.

For more information, see Chapter 3, "Certificate Authorities."

# A Three Gateway Configuration

FIGURE 4-16 on page 53 depicts the network configuration shown in FIGURE 4-1 on page 40 after a third gateway (Paris) has been added.

To include Paris and its hosts (Louvre and Eiffel) in the encryption, proceed as follows:

1. Define Paris as a gateway (FIGURE 4-16).
2. Define Paris-net as a network.

   See “Network Properties” on page 115 of *VPN-1/FireWall-1 Administration Guide* for information about defining networks.
3. Add Paris-net to the Enterprise group (see FIGURE 4-9 on page 46).

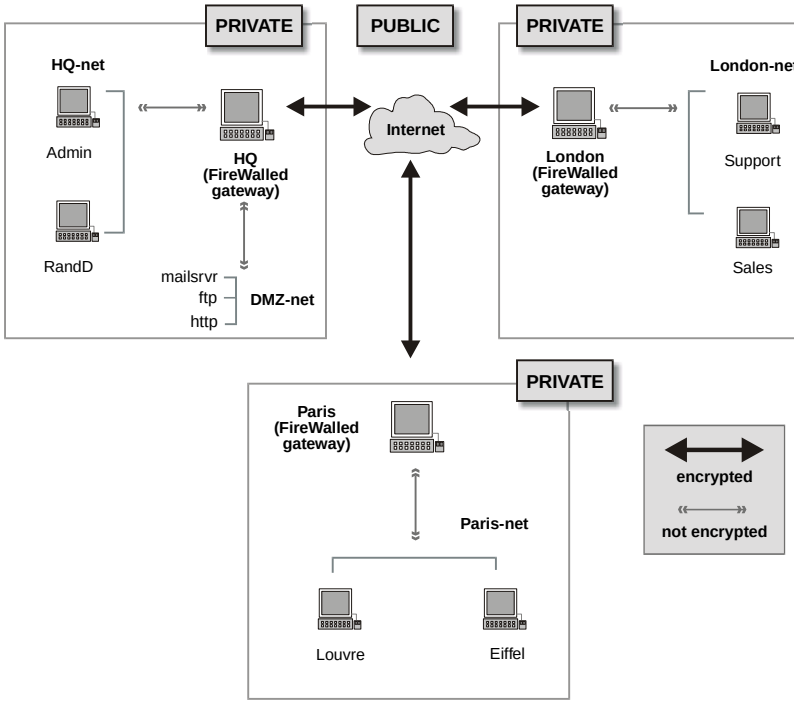



**FIGURE 4-16** Three Gateway Network Configuration

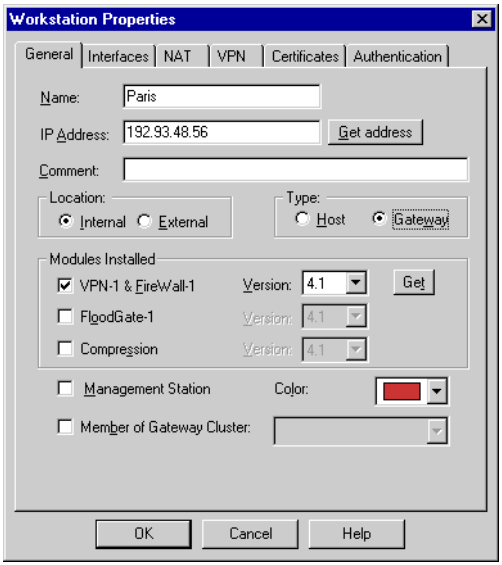



**FIGURE 4-17** Encrypting Gateways (Paris)

***4*** Open the **VPN** tab of Paris' **Workstation Properties** window (FIGURE 4-18).

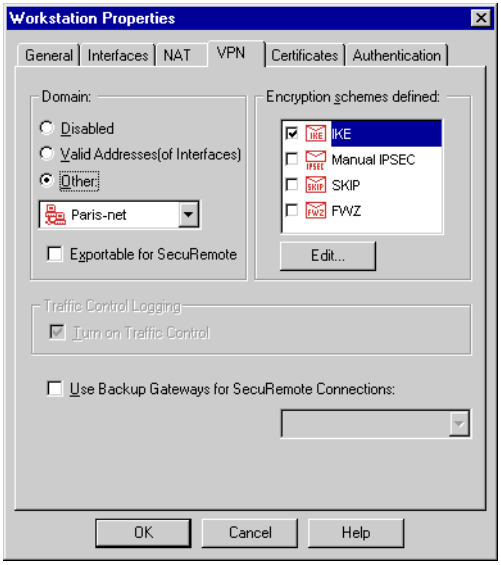



**FIGURE 4-18** Encrypting Gateway (Paris)

***5*** In **Domain**, click on **Other** and choose **Paris-net** from the drop-down list

***6*** In **Encryption schemes defined**, check **IKE** and click on **Edit**.

The **IKE Properties** window (FIGURE 4-4 on page 43) is displayed.

7 In **Key Negotiation Encryption Method(s)**, check one or more encryption method.

8 Check one or more **Hash Method**.

9 Check **Pre-shared Secrets**.

10 Check **Edit Secrets**.

11 In the **Shared Secret** window, select HQ (highlight it) and click on **Edit**.

12 In the edit box, enter the pre-shared secret (between Paris and HQ) and click on **Set**.

13 In the **Shared Secret** window, select London (highlight it) and click on **Edit**.

14 In the edit box, enter the pre-shared secret (between Paris and London) and click on **Set**.

**Note –** The pre-shared secret between London and HQ was defined earlier (in step 16 on page 45).

15 Install the Security Policy on the gateways (HQ, London and Paris).

No changes to the Rule Base are necessary, because there is no change in what is being encrypted.

CHAPTER 5

# Implementing FWZ Encryption

## In This Chapter



## Overview

This chapter presents a step-by-step description of how to implement FWZ encryption in VPN-1/FireWall-1.

FIGURE 5-1 shows a corporate internetwork where three private networks (HQ-net, London-net and DMZ-net) are connected to the Internet through FireWalled gateways. HQ is the Management Station for itself and London. The private networks are protected by the FireWalled gateways, but the public part of the network — the Internet — must be considered insecure.

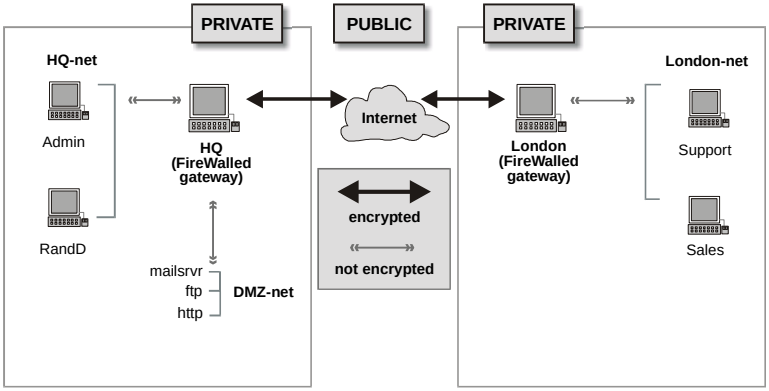



**FIGURE 5-1** Two Gateway Network Configuration

## Specifying Encryption

To specify encryption, you must answer the following questions:

***1*** Who will encrypt?

Define:

- the encrypting gateways (in the **Workstation Properties** window — see FIGURE 5-2 on page 59)
- their encryption domains (in the **VPN** tab of the **Workstation Properties** window — see FIGURE 5-3 on page 60)

***2*** What are the encryption keys?

On the Management Station, generate the Diffie-Hellman keys for the encrypting gateway and its CA (in the **FWZ Properties** window — see FIGURE 5-4 on page 60), or obtain the certified keys from the remote gateways or Certificate Authorities.

***3*** What will be encrypted?

Add a rule (or rules) to the Rule Base specifying encryption.

***4*** Which encryption scheme will be used?

Specify the encryption scheme in the rule. The scheme must be one that both parties to the encryption can implement.

## Encryption Domains

A gateway performs encryption on behalf of its encryption domain: the local area network (LAN) or group of networks that the gateway protects. Behind the gateway, in the internal networks, packets are not encrypted.

For example, if the system administrator has specified that communications between HQ and London are to be encrypted, VPN-1/FireWall-1 encrypts packets traveling between them on the Internet. A packet traveling from Sales to Admin is encrypted on the London-HQ segment of its trip, but not encrypted on the Sales-London and HQ-Admin segments.

## A Two Gateway Configuration

To encrypt communications between HQ's encryption domain and London's encryption domain (FIGURE 5-1 on page 58) using the FWZ encryption scheme, proceed as follows on HQ, their Management Station:

***1*** Define HQ and London, the gateways that will perform the encryption.

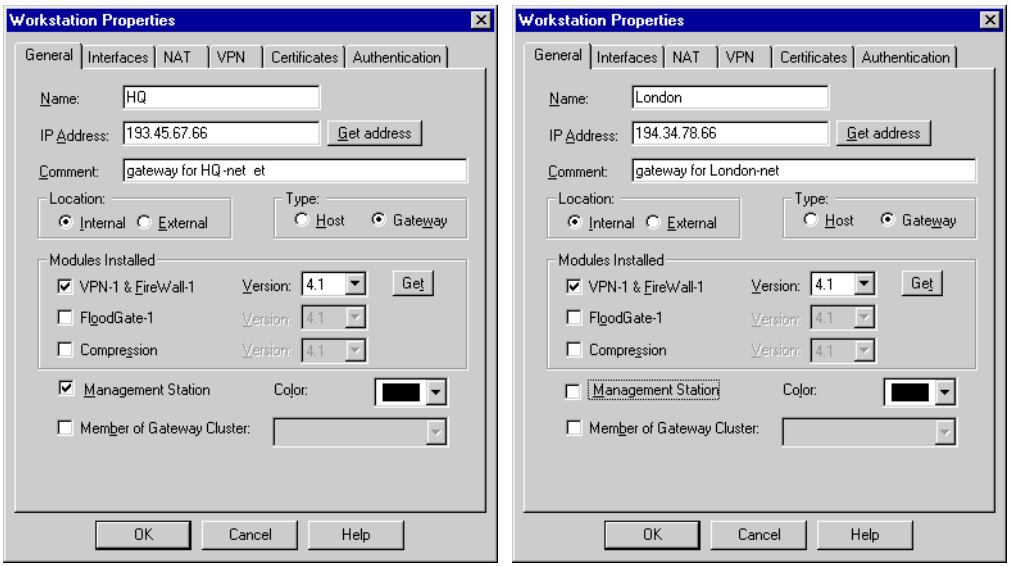



**FIGURE 5-2** Encrypting Gateways (HQ and London)

***2*** Define HQ-net, London-net and DMZ-net as networks.

See "Network Properties" on page 115 of *VPN-1/FireWall-1 Administration Guide* for information about defining networks.

**3** Open the **VPN** tab of HQ's **Workstation Properties** window (FIGURE 5-3).

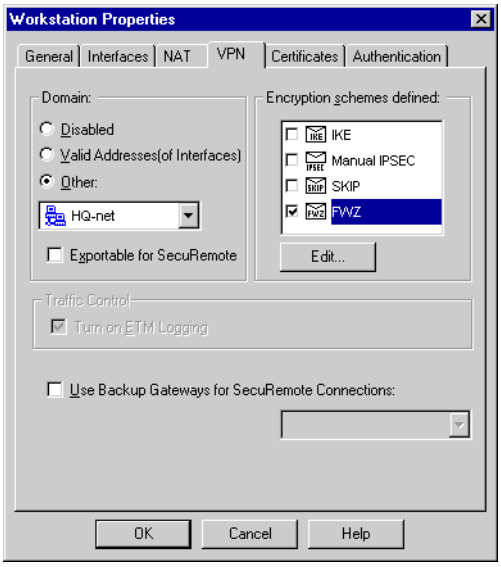



**FIGURE 5-3** HQ's Workstation Properties — VPN tab

For information about the fields in this window, see "Workstation Encryption Properties" on page 105.

**4** In **Domain**, click on **Other** and choose **HQ-net** from the drop-down list.

**5** In **Encryption schemes defined**, check **FWZ** and click on **Edit**.

The **FWZ Properties** window (FIGURE 5-4) is displayed.

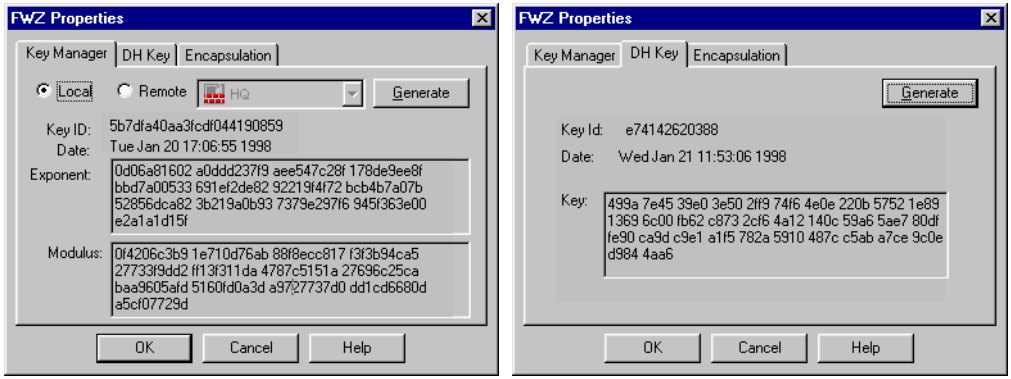



**FIGURE 5-4** FWZ Properties window — after a key has been generated (HQ)

For information about the fields in this window, see "FWZ Properties" on page 114.

6 In the **Key Manager** tab, check **Local** (the default), because HQ is managed by the Management Station you are now working with (HQ).

HQ is its own Management Station.

7 Click on **Generate** to generate an RSA key pair for HQ.

This key is used by HQ to identify itself as a CA.

8 In the **DH Key** tab (FIGURE 5-4 on page 60), the key that was generated when you installed VPN-1/FireWall-1 is displayed.

**Note –** If there is no key displayed in the **DH Key** tab, then click on **Generate** to generate a Diffie-Hellman key pair for HQ.

9 This key is used by HQ for generating a secret (symmetric) key for encrypted sessions (see "Public Key Schemes" on page 20).

10 Open the **VPN** tab of London's **Workstation Properties** window (FIGURE 5-5).

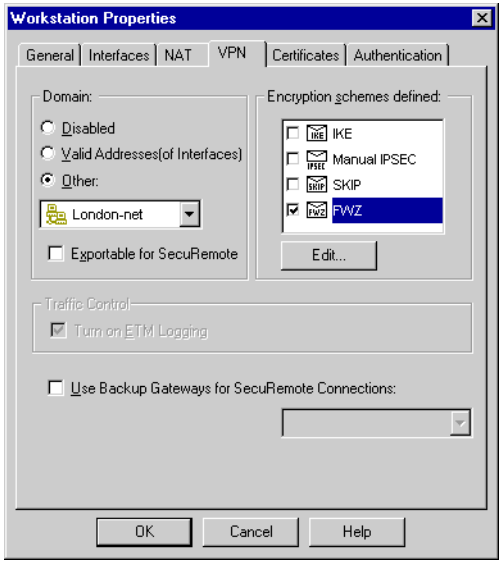



**FIGURE 5-5** Workstation Properties window — VPN tab (London)

11 In **Domain**, click on **Other** and choose **London-net** from the drop-down list.

12 In **Encryption schemes defined**, check **FWZ** and click on **Edit**.

The **FWZ Properties** window (FIGURE 5-4 on page 60) is displayed.

**13** In the **Key Manager** tab, check **Local** (the default), because London is managed by the Management Station you are now working with (HQ). In other words, London's **Location** is **Internal** in the **General** tab of its **Workstation Properties** window (FIGURE 5-2 on page 59).

**14** In the **DH Key** tab (FIGURE 5-4 on page 60), the key that was generated when you installed VPN-1/FireWall-1 is displayed.

**Note –** If there is no key displayed in the **DH Key** tab, then click on **Generate** to generate a Diffie-Hellman key pair for London.

This key is used by London for generating a secret (symmetric) key for encrypted sessions (see "Public Key Schemes" on page 20).

**15** Define a network object group (for example, "Enterprise") consisting of all the networks that will participate in the encryption (HQ-net and London-net).

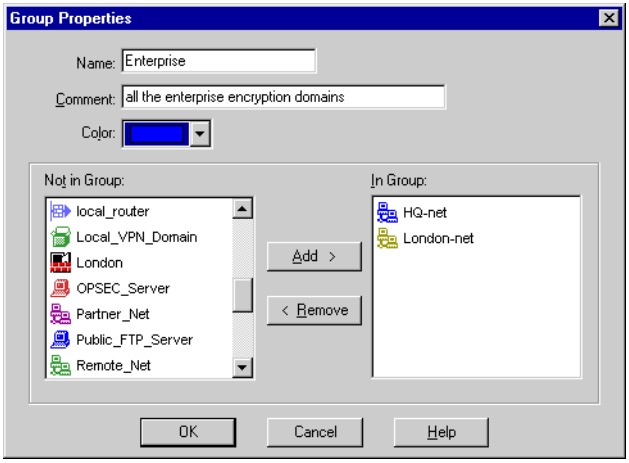



**FIGURE 5-6** Enterprise group definition

**16** Define a rule in the Rule Base that specifies **Encrypt** as the **Action** for communications between members of the Enterprise group.

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| Enterprise | Enterprise | Any | Encrypt | Long Log | Gateways |

The **Encrypt** action means:

- encrypt outgoing packets

- decrypt incoming encrypted packets and accept them

**Note –** You can also add encryption to an Authentication rule (User, Client or Session) by right-clicking on the Action and selecting **Add Encryption** from the menu.

**17** In the rule, double-click on **Encrypt** in the **Action** column to open the **Encryption Properties** window (FIGURE 5-7).

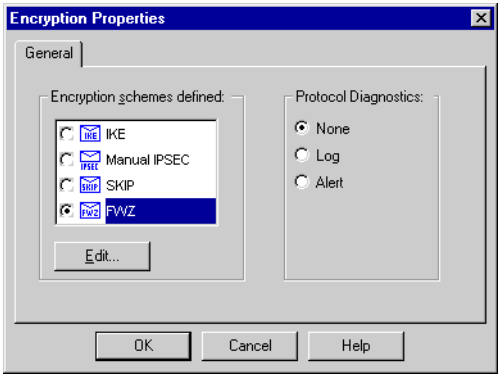



**FIGURE 5-7** Encryption Properties window (FWZ rule)

**18** Click on **FWZ**.

**19** Click on **Edit** to display the **FWZ Properties** window (FIGURE 5-8).

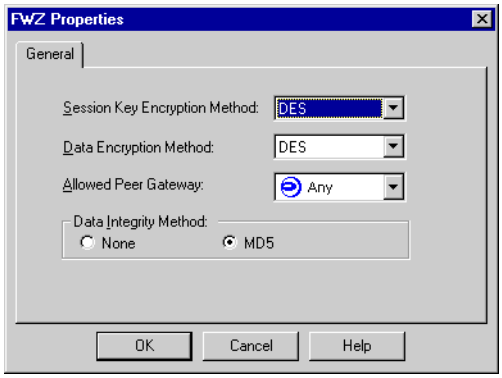



**FIGURE 5-8** FWZ Encryption Properties window

For information about the fields in this window, see “FWZ Encryption Properties” on page 123.

**20** Install the Security Policy on the gateways (HQ and London).

## Example — Adding an Encryption Rule to a Rule Base

TABLE 5-1 shows a simple Rule Base for the network configuration shown in FIGURE 5-1 on page 58.

**TABLE 5-1** Rule Base without Encryption

| | Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | DMZ-net | Enterprise | Any | Reject | Long Log | Gateways |
| 2 | Enterprise | Any | Any | Accept | Short Log | Gateways |
| 3 | Any | DMZ-net | ftp, http, smtp | Accept | Short Log | Gateways |
| 4 | AllUsers@Any | Any | telnet | UserAuth | Long Log | Gateways |
| 5 | Any | Any | Any | Reject | Long Log | Gateways |

**Note –** The simplified Rule Base shown here is for illustration only, and should not be viewed as a recommendation.

The Rule Base is explained in TABLE 5-2.

**TABLE 5-2** Explanation of Rule Base

| Rule No. | Explanation |
|---|---|
| 1 | prevents DMZ-net from initiating traffic to the internal networks |
| 2 | allows all internal hosts to go out to the Internet |
| 3 | allows unrestricted access to FTP, HTTP and SMTP on DMZ-net |
| 4 | specifies User Authentication for incoming telnet to internal hosts |
| 5 | rejects and logs all other communications |

The encryption rule should be inserted before the second rule in the Rule Base. In this way, mail between Enterprise hosts will be encrypted, but mail from an Enterprise host to other hosts will not be encrypted.

TABLE 5-3 on page 65 shows the Rule Base after the encryption rule has been added before the original second rule, which has now become the third rule.

**TABLE 5-3** Rule Base with Encryption Rule Added

| | Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | DMZ-net | Enterprise | Any | Reject | Long Log | Gateways |
| 2 | Enterprise | Enterprise | Any | Encrypt | Long Log | Gateways |
| 3 | Enterprise | Any | Any | Accept | Short Log | Gateways |
| 4 | Any | DMZ-net | ftp, http, smtp | Accept | Short Log | Gateways |
| 5 | AllUsers@Any | Any | telnet | UserAuth | Long Log | Gateways |
| 6 | Any | Any | Any | Reject | Long Log | Gateways |

# A Three Gateway Configuration

FIGURE 5-10 on page 66 depicts the network configuration shown in FIGURE 5-1 on page 58 after a third gateway (Paris) has been added.

To include Paris and its hosts (Louvre and Eiffel) in the encryption, proceed as follows:

***1*** Define Paris as a gateway.

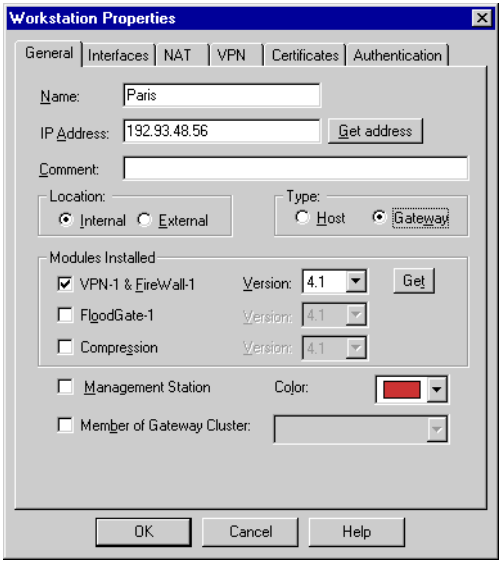



**FIGURE 5-9** Encrypting Gateways (Paris)

**2** Define Paris-net as a network

See “Network Properties” on page 115 of *VPN-1/FireWall-1 Administration Guide* for information about defining networks.

**3** Add Paris-net to the Enterprise group (see FIGURE 5-6 on page 62).

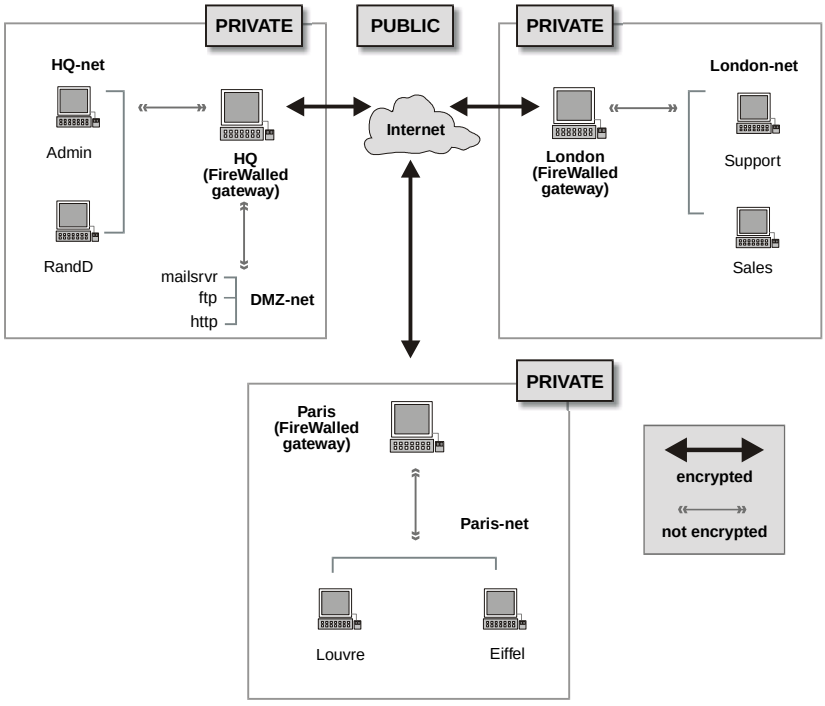



**FIGURE 5-10** Three Gateway Network Configuration

**4** Open the **VPN** tab of London's **Workstation Properties** window (FIGURE 5-11).

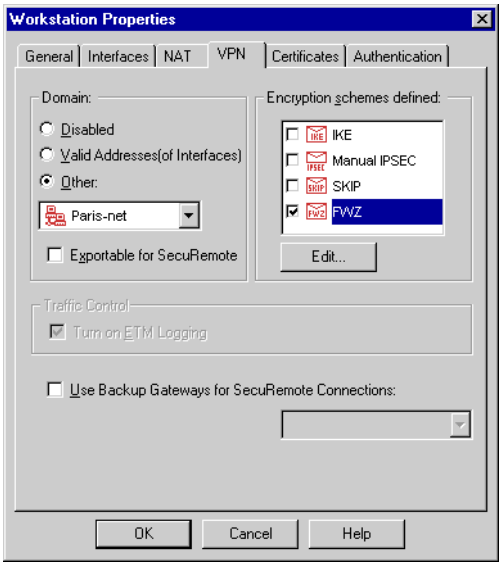



**FIGURE 5-11** Encrypting Gateway (Paris)

**5** In **Domain**, click on **Other** and choose **Paris-net** from the drop-down list

**6** In **Encryption schemes defined**, check **FWZ** and click on **Edit**.

The **FWZ Properties** window (FIGURE 5-4 on page 60) is displayed.

**7** In the **Key Manager** tab, check **Local**, because Paris is managed by the Management Station you are now working with (HQ). In other words, Paris' **Location** is **Internal** in the **General** tab of its **Workstation Properties** window (FIGURE 5-2 on page 59).

**8** In the **DH Key** tab (FIGURE 5-4 on page 60), click on **Generate** to generate a Diffie-Hellman key pair for Paris.

This key is used by Paris for generating a private key for encrypted sessions (see "Public Key Schemes" on page 20). Paris' public key is generated and displayed in the **DH Key** tab.

**9** Install the Security Policy on the gateways (HQ, London and Paris).

No changes to the Rule Base are necessary, because there is no change in what is being encrypted.

## Encrypting Communications with External Networks

The examples described above assume the encrypting gateways are controlled from the same Management Station. Encryption can also be implemented between gateways that are controlled from different Management Stations.

FIGURE 5-12 depicts a configuration similar to the one shown in FIGURE 5-10 on page 66, but with an external gateway (Reseller) added. Reseller-net's HTTP server is Chile, and its Management Station is Reseller, while the other gateways (HQ, London and Paris) are all managed by HQ.

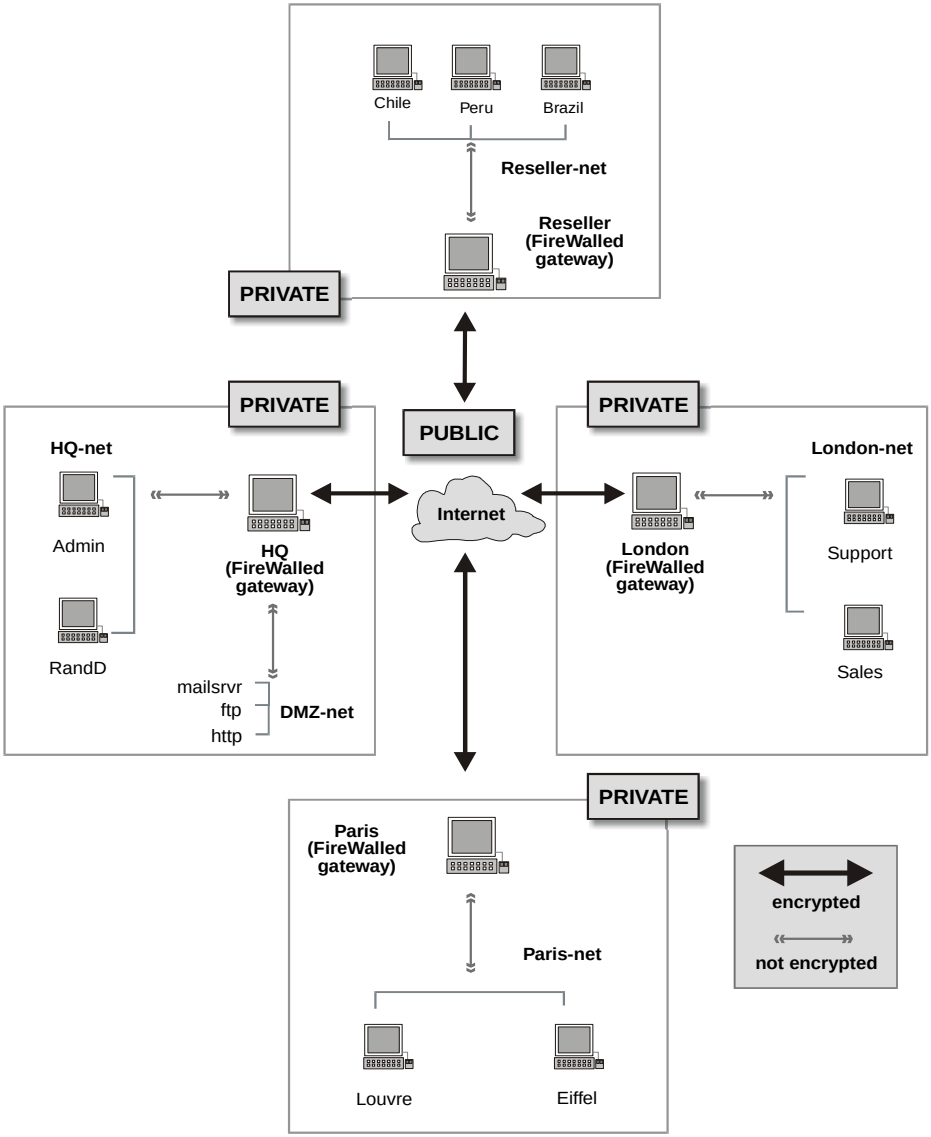



**FIGURE 5-12** Network Configuration with External Encrypting Gateway

## Configuring the “Local” Network

In order to encrypt HTTP between Enterprise and Reseller, Enterprise’s system administrator must proceed as follows on HQ:

1. Define Reseller as an external gateway (select **External** in the **Location** field in the **General** tab of its **Workstation Properties** window — FIGURE 5-13).

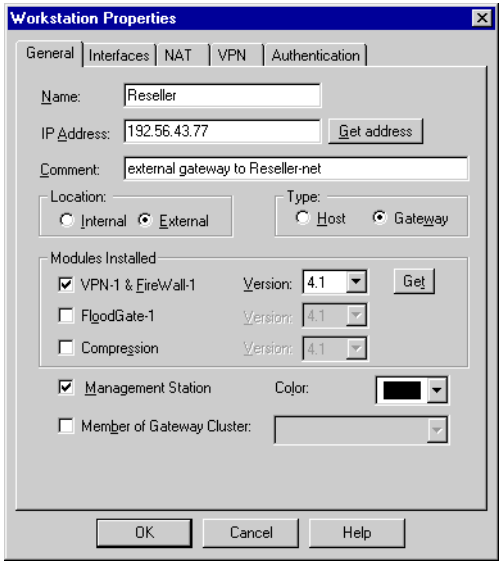



**FIGURE 5-13** Encrypting gateway (Reseller)

2. Define Reseller-net as a network.

   See “Network Properties” on page 115 of *VPN-1/FireWall-1 Administration Guide* for information about defining networks.

3. Open the **VPN** tab of Reseller’s **Workstation Properties** window (FIGURE 5-14 on page 70).

4. In **Domain**, click on **Other** and choose **Reseller-net** from the drop-down list.

5. In **Encryption schemes defined**, check **FWZ** and click on **Edit**.

   The **FWZ Properties** window (FIGURE 5-4 on page 60) is displayed.

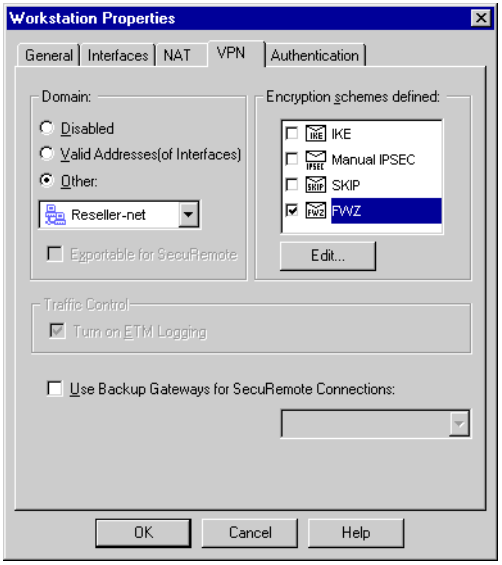



**FIGURE 5-14** Encrypting Gateway (Reseller)

***6*** In the **Key Manager** tab, check **Remote**, because Reseller's Management Station (which in the FWZ scheme functions as the CA) is Reseller, whose **Location** is **External** in the **General** tab of its **Workstation Properties** window (FIGURE 5-13 on page 69).

***7*** Select Reseller from the **Certificate Authority** menu.

This specifies that Reseller itself manages and authenticates Reseller's keys.

***8*** Click on **Get** to get Reseller's RSA key pair.

This key is used by Reseller to identify itself as a CA.

**Warning –** The first time you contact Reseller, its CA public key will be automatically fetched. However, since this transaction cannot be authenticated, you will get a warning message. It is advisable that you verify the key just obtained over the network by some other non-network means, such as by fax or telephone.

***9*** In the **DH Key** tab (FIGURE 5-4 on page 60), click on **Get** to get Reseller's Diffie-Hellman key pair.

This key is used by Reseller for generating a private key for encrypted sessions (see "Public Key Schemes" on page 20). Paris' public key is generated and displayed in the **DH Key** tab.

10 In the Rule Base, define a rule for encrypting HTTP.

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| Enterprise | Reseller-net | http | Encrypt | Short Log | Gateways |

The rule should be placed before any rules accepting HTTP in the Rule Base (see TABLE 5-3 on page 65).

11 In the new rule, double-click on **Encrypt** and specify the rule’s encryption properties in the **Encryption Properties** window (FIGURE 5-8 on page 63).

12 Install the Security Policy on the gateways.

### Configuring the “Remote” Network

Reseller’s system administrator, working on Brazil, must configure Reseller’s Security Policy as well, performing the same tasks as Enterprise’s system administrator.

## When Keys Change

When an internal gateway’s public Diffie-Hellman key changes, the VPN-1/FireWall-1 daemon on the peer gateway become aware of the new key when the Security Policy is reinstalled.

When an external gateway’s RSA key changes, you must get it explicitly (see step 8 on page 70). When an external gateway’s Diffie-Hellman key changes, VPN-1/FireWall-1 automatically re-fetches the changed key before computing the session key.

VPN-1/FireWall-1 gets keys using secure protocols that ensure their authenticity and prevent “man in the middle” attacks.

## Internal Encryption

The examples described above assume that the internal networks can be regarded as secure. This assumption may not always be appropriate. Even within a single organization, some communications may demand a higher level of security than others.

VPN-1/FireWall-1 easily accommodates this requirement. For example, encryption can be implemented for FTP sessions between specific hosts, even if the hosts (which must have a VPN/FireWall Module installed on them) are all on the same sub-network protected by the same FireWalled gateway.

CHAPTER 6

# Implementing Manual IPSec Encryption

## In This Chapter



## FireWall-1 Encryption — Overview

This chapter presents a step-by-step description of how to implement Manual IPSec encryption in VPN-1/FireWall-1.

FIGURE 6-1 shows a corporate internetwork where three private networks (HQ-net, London-net and DMZ-net) are connected to the Internet through FireWalled gateways. HQ is the Management Station for itself and London. The private networks are protected by the FireWalled gateways, but the public part of the network — the Internet — must be considered insecure.

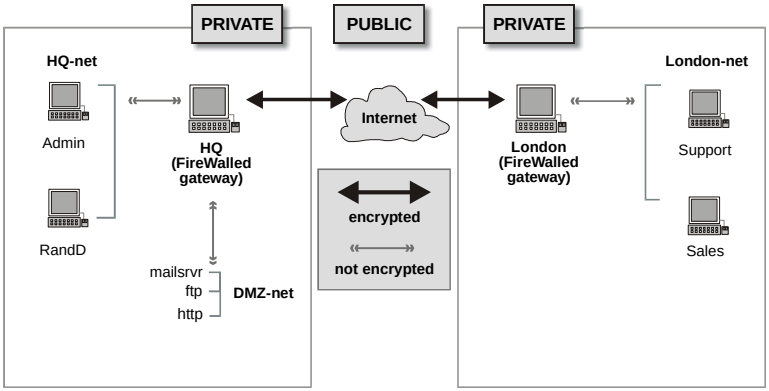



**FIGURE 6-1** Two Gateway Network Configuration

## Specifying Encryption

To specify encryption, you must answer the following questions:

***1*** Who will encrypt?

Define:

- the encrypting gateways (in the **Workstation Properties** window — see FIGURE 6-2 on page 75)
- their encryption domains (in the **VPN** tab of the **Workstation Properties** window — see FIGURE 6-4 on page 77)

***2*** What are the encryption keys?

Create an SA that defines the encryption parameters (see FIGURE 6-5 on page 77).

***3*** What will be encrypted?

Add a rule (or rules) to the Rule Base specifying encryption.

***4*** Which encryption scheme will be used?

Specify the SPI in the rule (FIGURE 6-10 on page 80).

## Encryption Domains

A gateway performs encryption on behalf of its encryption domain: the local area network (LAN) or group of networks that the gateway protects. Behind the gateway, in the internal networks, packets are not encrypted.

For example, if the system administrator has specified that communications between HQ and London are to be encrypted, VPN-1/FireWall-1 encrypts packets traveling between them on the Internet. A packet traveling from Sales to Admin is encrypted on the London-HQ segment of its trip, but not encrypted on the Sales-London and HQ-Admin segments.

# A Two Gateway Configuration

## Both Gateways FireWalled

To encrypt communications between HQ's encryption domain and London's encryption domain (FIGURE 6-1 on page 74) using the Manual IPSec encryption scheme, proceed as follows on HQ, their Management Station:

***1*** Define HQ and London, the gateways that will perform the encryption.

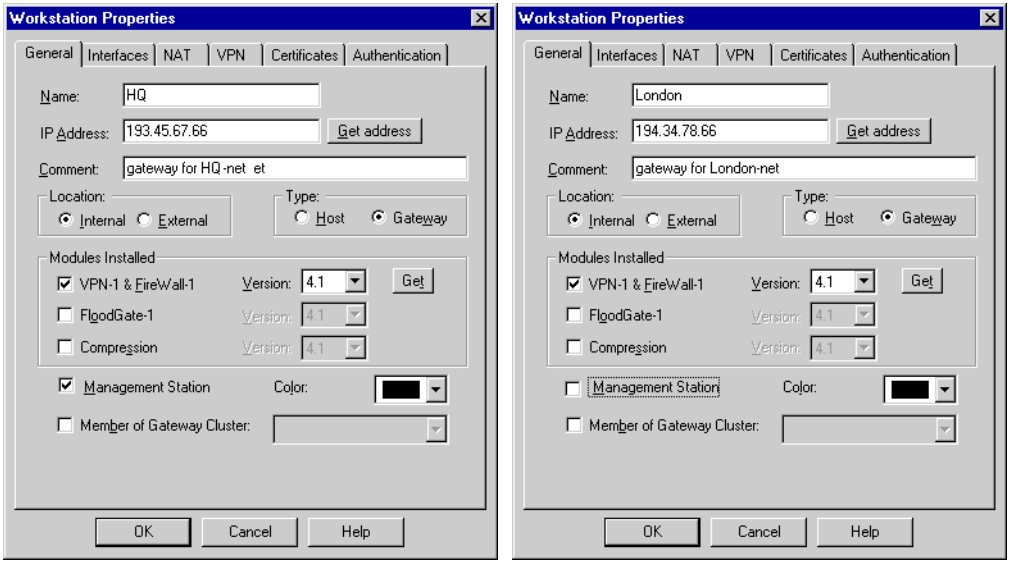



**FIGURE 6-2** Encrypting Gateways (HQ and London)

***2*** Define HQ-net, London-net and DMZ-net as networks.

See "Network Properties" on page 115 of *VPN-1/FireWall-1 Administration Guide* for information about defining networks.

**3** Open the **VPN** tab of HQ's **Workstation Properties** window (FIGURE 6-3)..

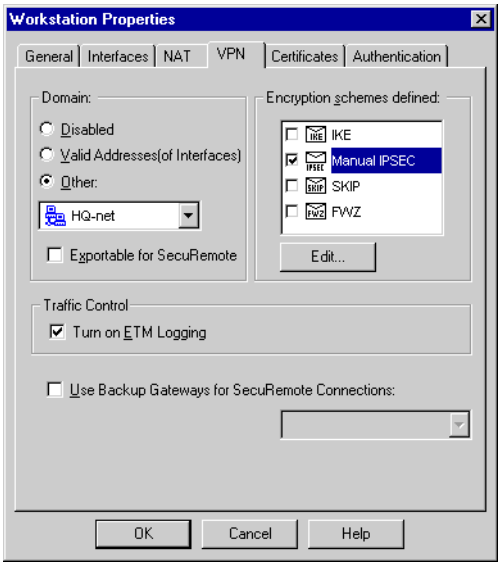



**FIGURE 6-3** Workstation Properties — VPN tab (HQ)

For information about the fields in this window, see "Workstation Encryption Properties" on page 105.

**4** In **Domain**, click on **Other** and choose **HQ-net** from the drop-down list.

**5** In **Encryption schemes defined**, check **Manual IPSEC**.

In the Manual IPSec scheme, gateways do not have encryption properties. Instead:

- Encryption properties are defined individually for each rule.
- SPIs are defined in the **SPI** tab of the **Manual IPSec** window (FIGURE 6-6 on page 78).

  To display the **SPI** tab of the **Manual IPSec** window, select **Keys** from the **Manage** menu. For more information, see "Defining an SPI" on page 121.

**6** Open the **VPN** tab of London's **Workstation Properties** window (FIGURE 6-4).

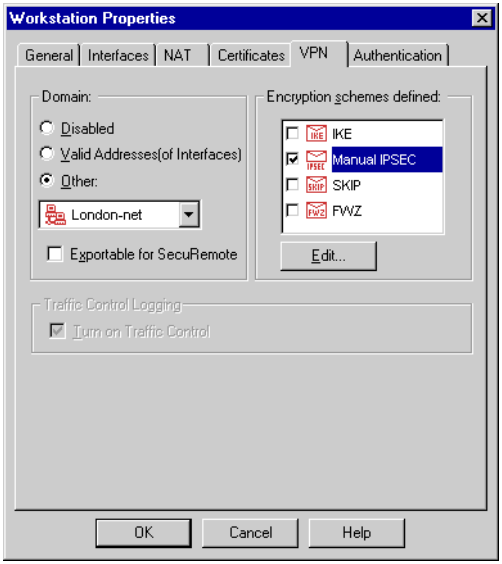



**FIGURE 6-4** Workstation Properties — VPN tab (London)

***7*** In **Domain**, click on **Other** and choose **London-net** from the drop-down list.

***8*** In **Encryption schemes defined**, check **Manual IPSEC**.

Next, create a Security Association (SA) that defines the encryption parameters. A numeric identifier, known as a Security Parameters Index (SPI), identifies the SA.

***9*** Select **Keys** from the **Manage** menu.

The **Encryption Keys** window (FIGURE 6-5) is displayed.

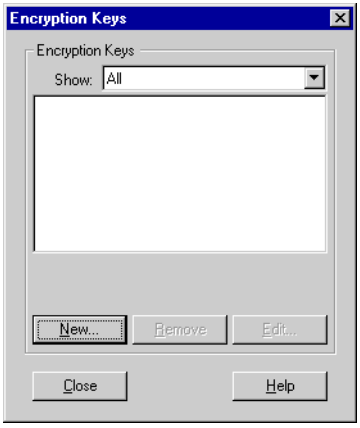



**FIGURE 6-5** Encryption Keys window (empty)

***10*** Click on **New** and select **SPI** from the menu.

The **Manual IPSec** window (FIGURE 6-6) is displayed.

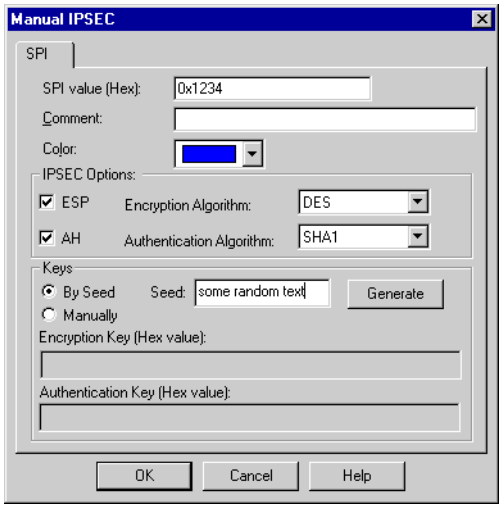



**FIGURE 6-6** Manual IPSec window

For information about the fields in this window, see FIGURE 8-22 on page 122.

***11*** In **SPI value**, enter a unique identifying key.

This is a hexadecimal number (enter leading 0x) and must be greater than 0x100. The value must be in the range defined in **SPI Allocation Range** in the **Encryption** tab of the **Properties Setup** window (see FIGURE 8-1 on page 102).

***12*** In **IPSec Options**, check **ESP** and **AH**.

***13*** Enter a value for **Seed** and click on **Generate**.

An encryption key is generated and displayed in **Encryption Key**, and an authentication key is generated and displayed in **Authentication Key**.

***14*** Click on **OK**.

The **Encryption Keys** window (FIGURE 6-7) now lists the SPI you have just created.


**FIGURE 6-7** Encryption Keys window (showing the newly defined SPI)

***15*** Define a network object group (for example, “Enterprise”) consisting of all the networks that will participate in the encryption (HQ-net and London-net).

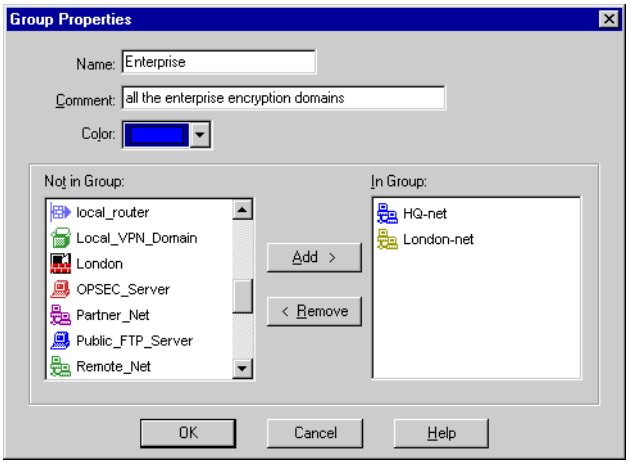



**FIGURE 6-8** Enterprise group definition

***16*** Define a rule in the Rule Base that specifies **Encrypt** as the **Action** for communications between members of the Enterprise group.

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| Enterprise | Enterprise | Any | Encrypt | Long Log | Gateways |

The **Encrypt** action means:

- encrypt outgoing packets
- decrypt incoming encrypted packets and accept them

**Note** – You can also add encryption to an Authentication rule (User, Client or Session) by right-clicking on the Action and selecting **Add Encryption** from the menu.

***17*** In the rule, double-click on **Encrypt** in the **Action** column to display the **Encryption Properties** window (FIGURE 6-9).

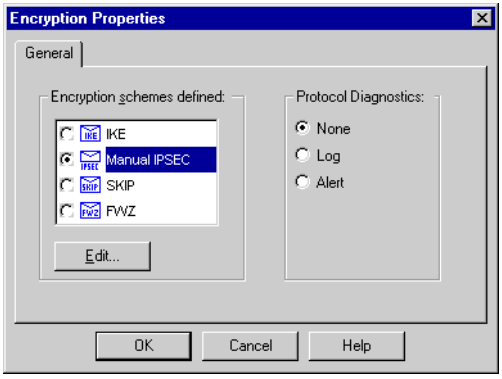



**FIGURE 6-9** Encryption Properties window (Manual IPSec rule)

***18*** Click on **Manual IPSEC**.

***19*** Click on **Edit** to display the **Manual IPSEC Properties** window (FIGURE 6-10).

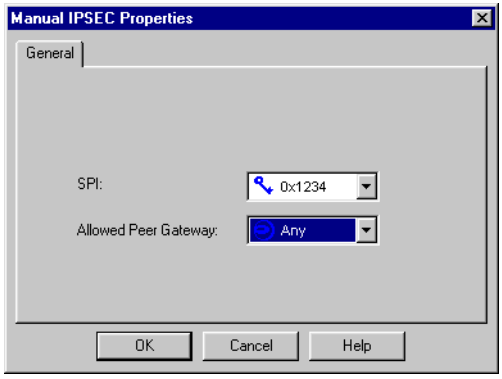



**FIGURE 6-10** Manual IPSec Properties window

For information about the fields in this window, see “Manual IPSec Encryption Properties” on page 120.

**20** In **SPI**, specify the SPI you defined in the **Manual IPSEC** window (FIGURE 6-6 on page 78).

## Only One Gateway FireWalled (Extranet)

VPN-1/FireWall-1 is interoperable with other software that implements IPSec standards. You can encrypt connections between VPN-1/FireWall-1 sites and these sites.

If only one of the gateways has VPN-1/FireWall-1 installed and the other does not (for example, if HQ has VPN-1/FireWall-1 installed and Madrid does not), proceed as follows:

**1** Define the other gateway (Madrid) as an external object (in the **General** tab of its **Workstation Properties** window).

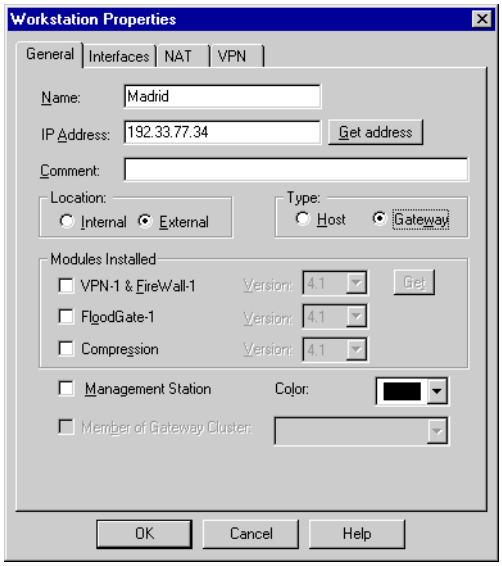



**FIGURE 6-11** Workstation Properties window (Madrid)

**2** Coordinate the IPsec parameters with Madrid's system manager.

For example, you must coordinate the SA (FIGURE 6-7 on page 79) and the SPI (FIGURE 6-6 on page 78).

## Example — Adding an Encryption Rule to a Rule Base

TABLE 6-1 shows a simple Rule Base for the network configuration shown in FIGURE 6-1 on page 74.

**TABLE 6-1** Rule Base without Encryption

| | Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | DMZ-net | Enterprise | Any | Reject | Long Log | Gateways |
| 2 | Enterprise | Any | Any | Accept | Short Log | Gateways |
| 3 | Any | DMZ-net | ftp, http, smtp | Accept | Short Log | Gateways |
| 4 | AllUsers@Any | Any | telnet | UserAuth | Long Log | Gateways |
| 5 | Any | Any | Any | Reject | Long Log | Gateways |

**Note –** The simplified Rule Base shown here is for illustration only, and should not be viewed as a recommendation.

The Rule Base is explained in TABLE 6-2.

**TABLE 6-2** Explanation of Rule Base

| Rule No. | Explanation |
|---|---|
| 1 | prevents DMZ-net from initiating traffic to the internal networks |
| 2 | allows all internal hosts to go out to the Internet |
| 3 | allows unrestricted access to FTP, HTTP and SMTP on DMZ-net |
| 4 | specifies User Authentication for incoming telnet to internal hosts |
| 5 | rejects and logs all other communications |

The encryption rule should be inserted before the second rule in the Rule Base. In this way, mail between Enterprise hosts will be encrypted, but mail from an Enterprise host to other hosts will not be encrypted.

TABLE 6-3 on page 83 shows the Rule Base after the encryption rule has been added before the original second rule, which has now become the third rule.

**TABLE 6-3** Rule Base with Encryption Rule Added

| | Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | DMZ-net | Enterprise | Any | Reject | Long Log | Gateways |
| 2 | Enterprise | Enterprise | Any | Encrypt | Long Log | Gateways |
| 3 | Enterprise | Any | Any | Accept | Short Log | Gateways |
| 4 | Any | DMZ-net | ftp, http, smtp | Accept | Short Log | Gateways |
| 5 | AllUsers@Any | Any | telnet | UserAuth | Long Log | Gateways |
| 6 | Any | Any | Any | Reject | Long Log | Gateways |

# A Three Gateway Configuration

FIGURE 6-13 on page 84 depicts the network configuration shown in FIGURE 6-1 on page 74 after a third gateway (Paris) has been added.

To include Paris and its hosts (Louvre and Eiffel) in the encryption, proceed as follows:

***1*** Define Paris as a gateway.

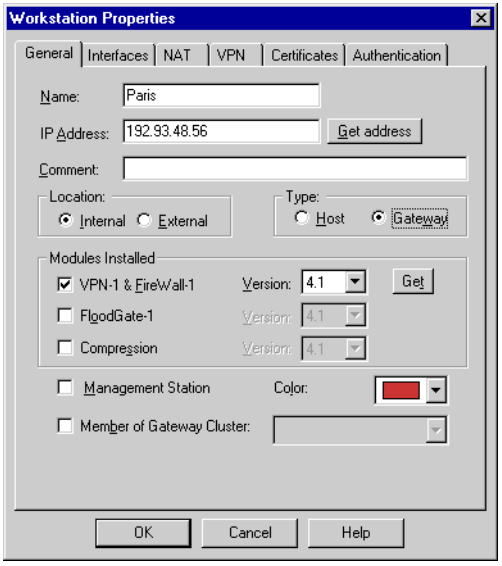



**FIGURE 6-12** Encrypting Gateways (Paris)

2 Define Paris-net as a network.

See “Network Properties” on page 115 of *VPN-1/FireWall-1 Administration Guide* for information about defining networks.

3 In the **VPN** tab of Paris’ **Workstation Properties** window, specify its **Encryption Domain** as Paris-net.

4 In **Encryption schemes defined**, check **Manual IPSEC**.

5 Add Paris-net to the Enterprise group (see FIGURE 6-8 on page 79).

6 Install the Security Policy on the gateways (HQ, London and Paris).

7 In the **VPN** tab of Paris’ **Workstation Properties** window, specify its **Encryption Domain** as Paris-net.

8 In **Encryption schemes defined**, check **Manual IPSEC**.

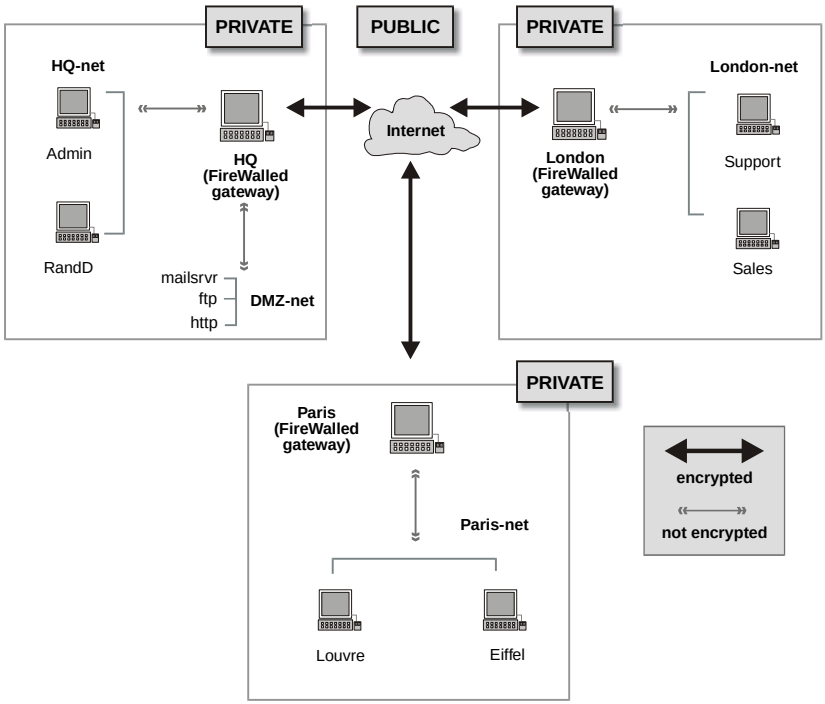



**FIGURE 6-13** Three Gateway Network Configuration

9 In the **VPN** tab of Paris’ **Workstation Properties** window, specify its **Encryption Domain** as Paris-net.

10 In **Encryption schemes defined**, check **Manual IPSEC**.

11 Add Paris-net to the Enterprise group (see FIGURE 6-8 on page 79).

***12*** Install the Security Policy on the gateways (HQ, London and Paris).

No changes to the Rule Base are necessary, because there is no change in what is being encrypted.

CHAPTER 7

# Implementing SKIP Encryption

## In This Chapter



## FireWall-1 Encryption — Overview

This chapter presents a step-by-step description of how to implement SKIP encryption in VPN-1/FireWall-1.

FIGURE 7-1 shows a corporate internetwork where three private networks (HQ-net, London-net and DMZ-net) are connected to the Internet through FireWalled gateways. HQ is the Management Station for itself and London. The private networks are protected by the FireWalled gateways, but the public part of the network — the Internet — must be considered insecure.

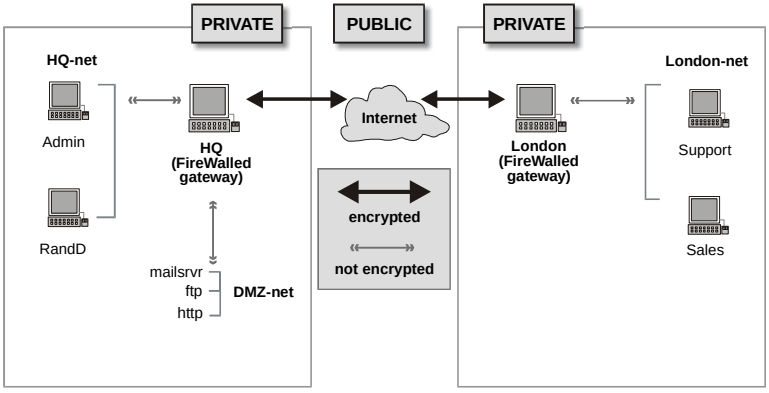



**FIGURE 7-1** Two Gateway Network Configuration

## Specifying Encryption

To specify encryption, you must answer the following questions:

1. Who will encrypt?

   Define:

   - the encrypting gateways (in the **Workstation Properties** window — see FIGURE 7-2 on page 89)
   - their encryption domains (in the **VPN** tab of the **Workstation Properties** window — see FIGURE 7-3 on page 90)

2. What are the encryption keys?

3. What will be encrypted?

   Add a rule (or rules) to the Rule Base specifying encryption.

4. Which encryption scheme will be used?

## Encryption Domains

A gateway performs encryption on behalf of its encryption domain: the local area network (LAN) or group of networks that the gateway protects. Behind the gateway, in the internal networks, packets are not encrypted.

For example, if the system administrator has specified that communications between HQ and London are to be encrypted, VPN-1/FireWall-1 encrypts packets traveling between them on the Internet. A packet traveling from Sales to Admin is encrypted on the London-HQ segment of its trip, but not encrypted on the Sales-London and HQ-Admin segments.

# A Two Gateway Configuration

## Both Gateways FireWalled

To encrypt communications between HQ's encryption domain and London's encryption domain (FIGURE 7-1 on page 88) using the SKIP encryption scheme, proceed as follows on HQ, their Management Station:

***1*** Define HQ and London, the gateways that will perform the encryption.

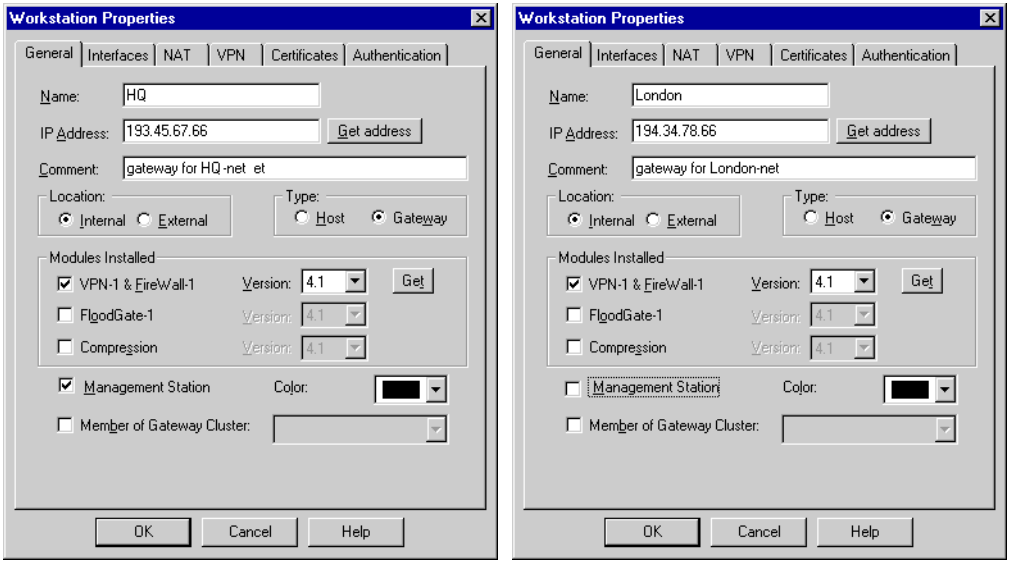



**FIGURE 7-2** Encrypting Gateways (HQ and London)

***2*** Define HQ-net, London-net and DMZ-net as networks.

See "Network Properties" on page 115 of *VPN-1/FireWall-1 Administration Guide* for information about defining networks.

**3** Open the **VPN** tab of HQ's **Workstation Properties** window (FIGURE 7-3)..

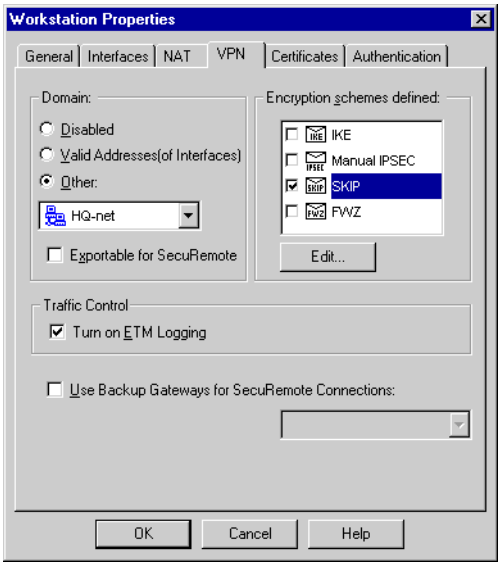



**FIGURE 7-3** Workstation Properties — VPN tab (HQ)

For information about the fields in this window, see "Workstation Encryption Properties" on page 105.

**4** In **Domain**, click on **Other** and choose **HQ-net** from the drop-down list.

**5** In **Encryption schemes defined**, check **SKIP** and click on **Edit**.

The **SKIP Properties** window (FIGURE 7-4) is displayed.

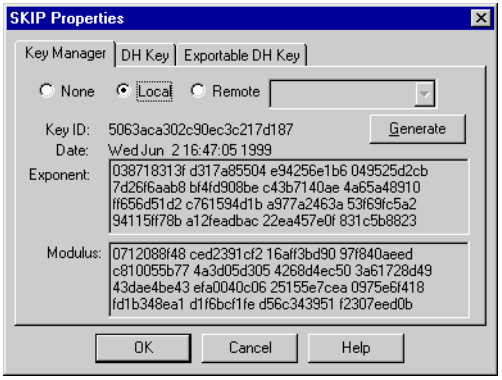



**FIGURE 7-4** SKIP Properties window - Key Manager tab

For information about the fields in this window, see "SKIP Properties" on page 112.

6 In the **Key Manager** tab, check **Local** (the default), because HQ's Key Manager (similar to a Certificate Authority) is HQ, whose **Location** is **Internal** in the **General** tab of its **Workstation Properties** window (FIGURE 7-2 on page 89).

7 Click on **Generate** to generate a RSA key pair for HQ.

This key is used by HQ to identify itself as a Key Manager.

8 In the **DH Key** tab (FIGURE 7-5), the key that was generated when you installed VPN-1/FireWall-1 is displayed.

**Note –** If there is no key displayed in the **DH Key** tab, then click on Generate to generate a Diffie-Hellman key pair for HQ.

This key is used by HQ for generating a secret (symmetric) key for encrypted sessions (see "Public Key Schemes" on page 20)

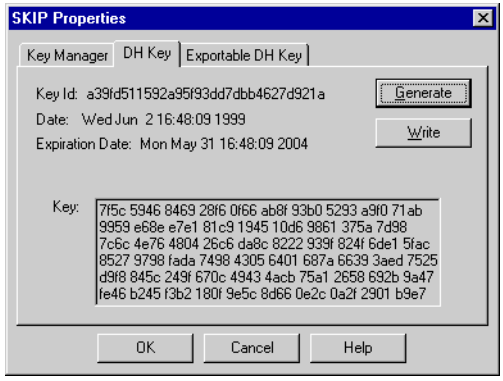



**FIGURE 7-5** SKIP Properties window - DH Key tab

**9** Open the **VPN** tab of London's **Workstation Properties** window (FIGURE 7-6).

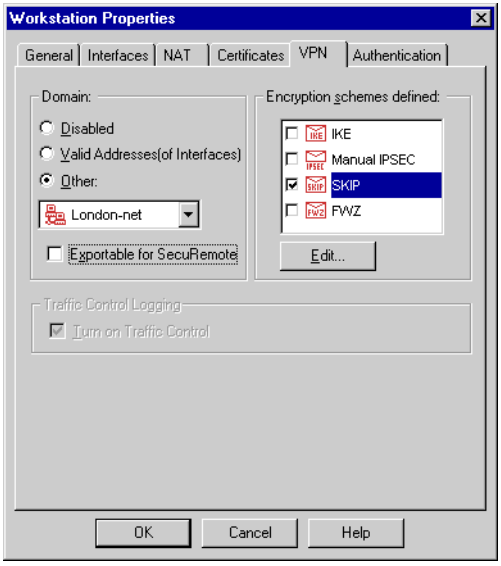



**FIGURE 7-6** Workstation Properties — VPN tab

**10** In **Domain**, click on **Other** and choose **London-net** from the drop-down list.

**11** In **Encryption schemes defined**, check **SKIP** and click on **Edit**.

The **SKIP Properties** window (FIGURE 7-4 on page 90) is displayed.

**12** In the **Key Manager** tab, check **Local** (the default), because London's Key Manager is HQ, whose **Location** is **Internal** in the **General** tab of its **Workstation Properties** window (FIGURE 7-2 on page 89).

**13** In the **DH Key** tab (FIGURE 7-5 on page 91), the key that was generated when you installed VPN-1/FireWall-1 is displayed.

**Note** – If there is no key displayed in the **DH Key** tab, then click on Generate to generate a Diffie-Hellman key pair for London.

This key is used by London for generating a secret (symmetric) key for encrypted sessions (see "Public Key Schemes" on page 20).

**14** Define a network object group (for example, “Enterprise”) consisting of all the networks that will participate in the encryption (HQ-net and London-net).

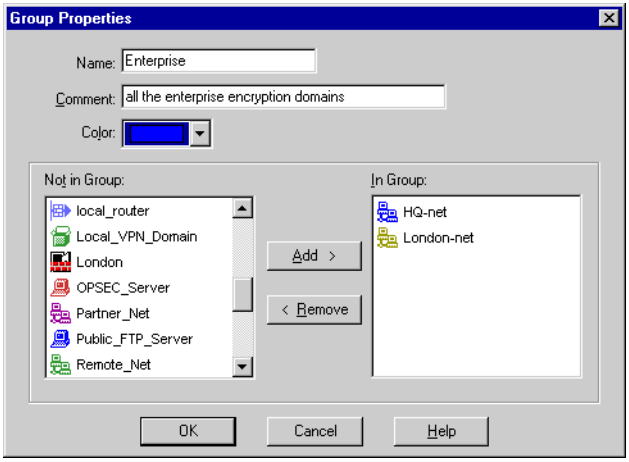



**FIGURE 7-7** Enterprise group definition

**15** Define a rule in the Rule Base that specifies **Encrypt** as the **Action** for communications between members of the Enterprise group.

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| Enterprise | Enterprise | Any | Encrypt | Long Log | Gateways |

The **Encrypt** action means:

- encrypt outgoing packets
- decrypt incoming encrypted packets and accept them

**Note –** You can also add encryption to an Authentication rule (User, Client or Session) by right-clicking on the Action and selecting **Add Encryption** from the menu.

**16** Double-click on **Encrypt** to display the **Encryption Properties** window (FIGURE 7-8).

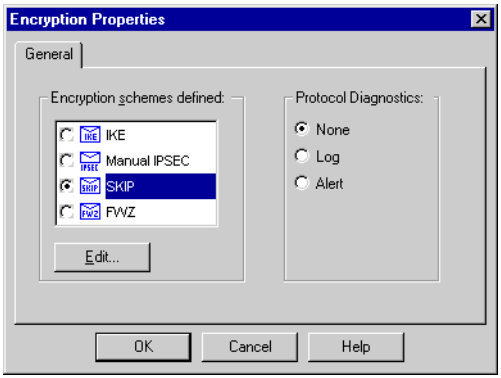



**FIGURE 7-8** Encryption Properties window — General tab

**17** Select **SKIP**.

**18** Click on **Edit** to display the **SKIP Properties** window (FIGURE 7-9).

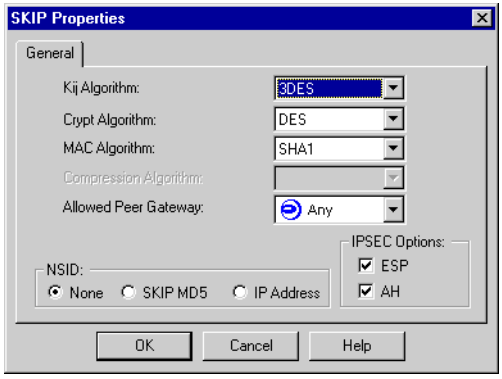



**FIGURE 7-9** SKIP Properties window

For information about the fields in this window, see “SKIP Encryption Properties” on page 119.

**19** Install the Security Policy on the gateways (HQ and London).

## Example — Adding an Encryption Rule to a Rule Base

TABLE 7-1 shows a simple Rule Base for the network configuration shown in FIGURE 7-1 on page 88.

**TABLE 7-1** Rule Base without Encryption

| | Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | DMZ-net | Enterprise | Any | Reject | Long Log | Gateways |
| 2 | Enterprise | Any | Any | Accept | Short Log | Gateways |
| 3 | Any | DMZ-net | ftp, http, smtp | Accept | Short Log | Gateways |
| 4 | AllUsers@Any | Any | telnet | UserAuth | Long Log | Gateways |
| 5 | Any | Any | Any | Reject | Long Log | Gateways |

**Note –** The simplified Rule Base shown here is for illustration only, and should not be viewed as a recommendation.

The Rule Base is explained in TABLE 7-2.

**TABLE 7-2** Explanation of Rule Base

| Rule No. | Explanation |
|---|---|
| 1 | prevents DMZ-net from initiating traffic to the internal networks |
| 2 | allows all internal hosts to go out to the Internet |
| 3 | allows unrestricted access to FTP, HTTP and SMTP on DMZ-net |
| 4 | specifies User Authentication for incoming telnet to internal hosts |
| 5 | rejects and logs all other communications |

The encryption rule should be inserted before the second rule in the Rule Base. In this way, mail between Enterprise hosts will be encrypted, but mail from an Enterprise host to other hosts will not be encrypted.

TABLE 7-3 on page 96 shows the Rule Base after the encryption rule has been added before the original second rule, which has now become the third rule.

**TABLE 7-3** Rule Base with Encryption Rule Added

| | Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | DMZ-net | Enterprise | Any | Reject | Long Log | Gateways |
| 2 | Enterprise | Enterprise | Any | Encrypt | Long Log | Gateways |
| 3 | Enterprise | Any | Any | Accept | Short Log | Gateways |
| 4 | Any | DMZ-net | ftp, http, smtp | Accept | Short Log | Gateways |
| 5 | AllUsers@Any | Any | telnet | UserAuth | Long Log | Gateways |
| 6 | Any | Any | Any | Reject | Long Log | Gateways |

## Only One Gateway FireWalled (Extranet)

VPN-1/FireWall-1 is interoperable with other software that implements SKIP standards. You can also encrypt connections between VPN-1/FireWall-1 sites and these sites.

If only one of the gateways has VPN-1/FireWall-1 installed and the other does not (for example, if HQ has VPN-1/FireWall-1 installed and Madrid does not), proceed as follows:

1. Define the other gateway (Madrid) as an external object (in the **General** tab of its **Workstation Properties** window).
2. Coordinate the SKIP parameters with Madrid's system manager.

   You will have to exchange keys manually using an intermediate file. See "SKIP Properties" on page 112 for more information.

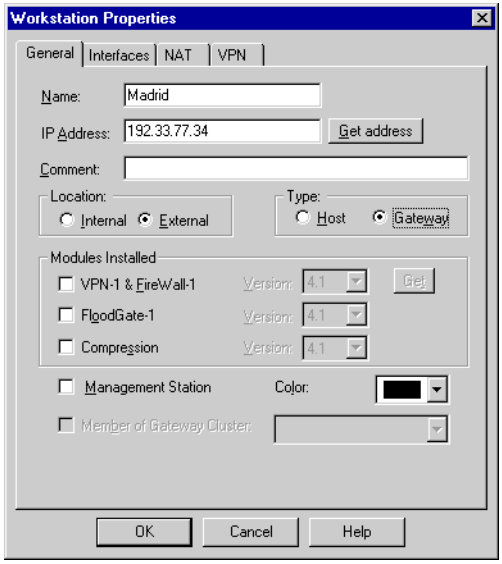



**FIGURE 7-10** Workstation Properties window (Madrid)

# A Three Gateway Configuration

FIGURE 7-12 on page 98 depicts the network configuration shown in FIGURE 7-1 on page 88 after a third gateway (Paris) has been added.

To include Paris and its hosts (Louvre and Eiffel) in the encryption, proceed as follows:

1. Define Paris as a gateway
2. Define Paris-net as a network.

   See “Network Properties” on page 115 of *VPN-1/FireWall-1 Administration Guide* for information about defining networks.

**3** Add Paris-net to the Enterprise group (see FIGURE 7-7 on page 93)..

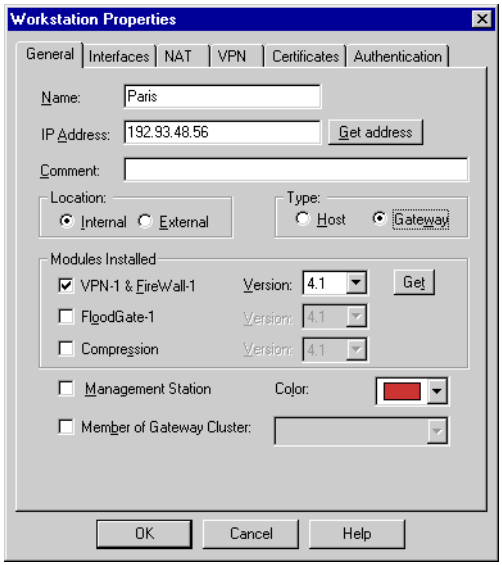



**FIGURE 7-11** Encrypting Gateways (Paris)

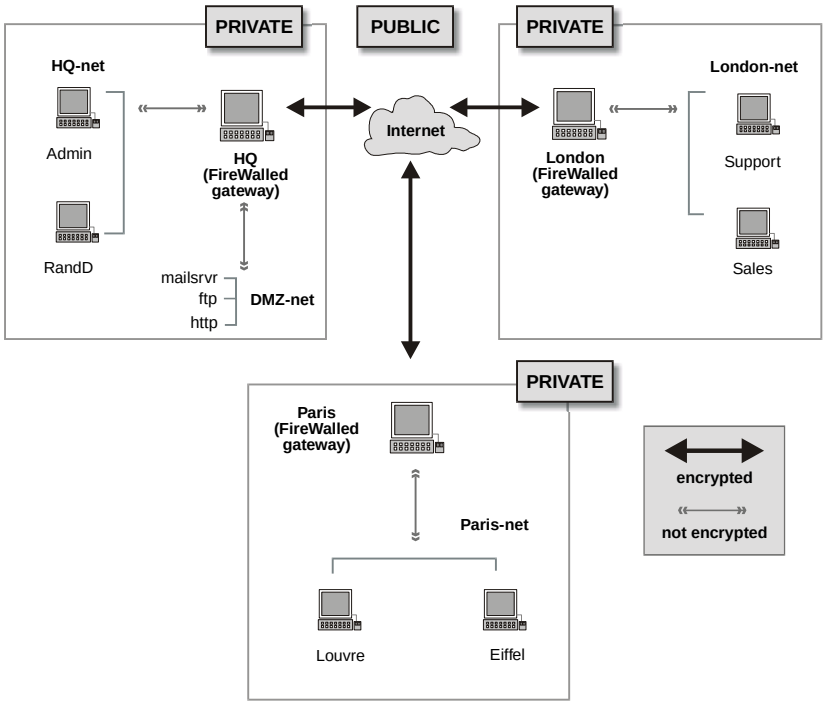



**FIGURE 7-12** Three Gateway Network Configuration

**4** Open the **VPN** tab of Paris' **Workstation Properties** window (FIGURE 7-13).

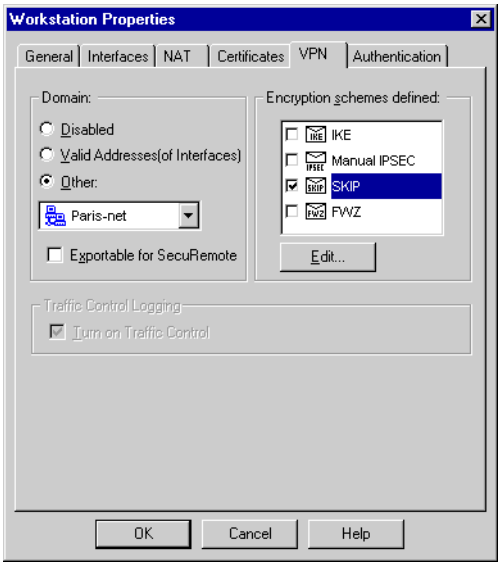



**FIGURE 7-13** Encrypting Gateway (Paris)

**5** In **Domain**, click on **Other** and choose **Paris-net** from the drop-down list

**6** In **Encryption schemes defined**, check **SKIP** and click on **Edit**.

The **SKIP Properties** window (FIGURE 7-4 on page 90) is displayed.

**7** In the **Key Manager** tab, check **Local** (the default), because Paris' Key Manager is HQ, whose **Location** is **Internal** in the **General** tab of its **Workstation Properties** window (FIGURE 7-2 on page 89).

**8** In the **DH Key** tab (FIGURE 7-5 on page 91), the key that was generated when you installed VPN-1/FireWall-1 is displayed.

**Note –** If there is no key displayed in the **DH Key** tab, then click on Generate to generate a Diffie-Hellman key pair for Paris.

This key is used by Paris for generating a secret (symmetric) key for encrypted sessions (see "Public Key Schemes" on page 20)..

**9** Install the Security Policy on the gateways (HQ, London and Paris).

No changes to the Rule Base are necessary, because there is no change in what is being encrypted.

CHAPTER 8

# Encryption Properties

## In This Chapter



## Encryption Properties

Encryption properties (the encryption and data integrity methods to be used when encrypting a connection) are defined for:

**workstations** — A workstation's encryption properties include all the encryption schemes the workstation can use when encrypting connections to and from its encryption domain.

**users** — A user's encryption properties include all the encryption schemes the user can use for SecuRemote connections (Client Encryption). See "Defining SecuRemote Users" on page 133 for information on specifying a user's encryption properties.

**rules** — A rule's encryption properties specify the specific encryption scheme that the rule implements. For example, a gateway might be defined as able to use both FWZ and SKIP. The scheme used for a specific connection is specified by the rule that applies to the connection.

In addition, some system-wide encryption properties (that apply to all VPN-1-enabled gateways managed by this Management Station) are defined in the **VPN** and **Desktop Security** tabs of the **Properties Setup** window. IKE logging options are defined in the **Log and Alert** tab of the **Properties Setup** window.

# Properties Setup - Encryption

This window (FIGURE 8-1) defines system-wide encryption properties.

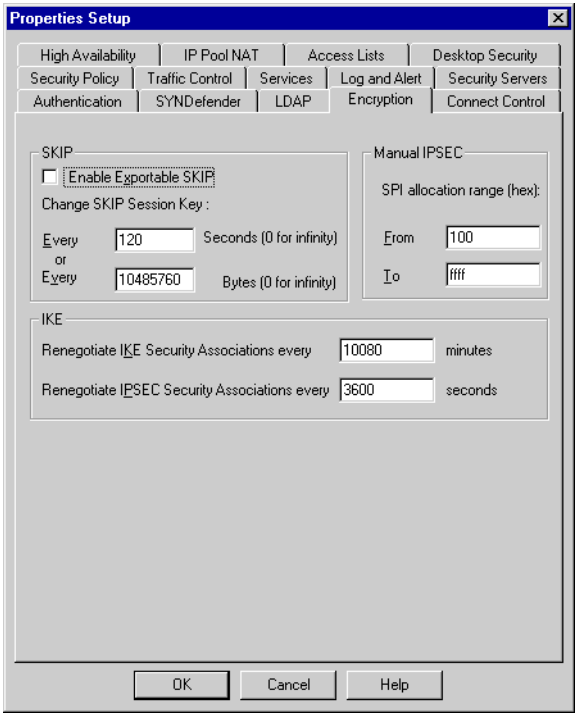



**FIGURE 8-1** Properties Setup window — Encryption tab

## SKIP

**Enable Exportable SKIP** — If checked, then FireWall Modules will generate keys for exportable SKIP (in addition to non-exportable SKIP keys) and conduct SKIP encryption with other hosts that are enabled only for exportable SKIP. The **Exportable DH Key** tab of the **SKIP Properties** window (FIGURE 8-12 on page 113) is available only if this option is checked.

**Change SKIP key every ... seconds (0 for infinity)** — the number of seconds after which the SKIP session key expires

**Change SKIP key every ... bytes (0 for infinity)** — the number of bytes transferred after which the SKIP session key expires

SKIP session keys expire either after **Change SKIP key every ... seconds** seconds or after bytes **Change SKIP key every ... bytes** bytes have been transferred in the encrypted session, whichever occurs sooner.

## Manual IPSec

**SPI Allocation Range** — Enter **From** and **To**.

The range is reserved for allocations of Manual IPSec SPIs. When you define an SPI in **SPI value** in the **Manual IPSec** window (see FIGURE 8-22 on page 122), it must be in this range. IKE will allocate SPIs from outside this range.

## IKE

**Renegotiate IKE Security Associations every ... minutes —** the number of minutes after which IKE Security Associations expire

See "IKE Encryption Scheme" on page 18 for more information.

**Renegotiate IPSEC Security Associations every ... seconds —** the number of seconds after which IPSec Security Associations expire

See "Manual IPSec Encryption Scheme" on page 16 for more information.

When an IPSec or IKE Security Association expires during an encryption session, VPN-1/FireWall-1 renegotiates the SA with the peer and continues the encryption session with the new SA. This process is transparent to the user.

# Properties Setup - Log and Alert

This window (FIGURE 8-2) defines system-wide logging properties. The encryption logging options are under **Track**.

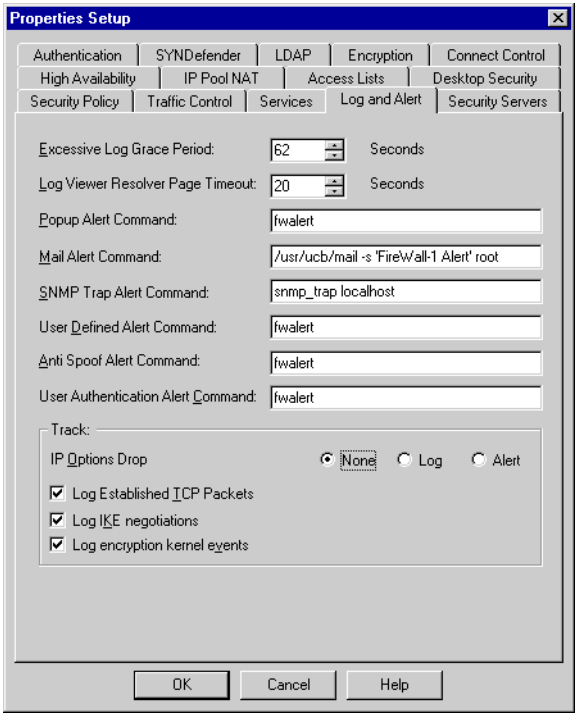



**FIGURE 8-2** Properties Setup window — Log and Alert tab

**Log IKE Negotiations** — This option controls logging IKE negotiation events.

If enabled, the following events are logged:

- start of IKE daemon
- beginning and end of Phase One IKE negotiation
- beginning of IKE Phase Two negotiation
- sending and receiving IKE notification (error) messages

  The **Info** field in the log contains information about the error.
- sending and receiving IKE SA delete messages

  In Phase Two, the SA's SPI appears in the text.
- IKE negotiation errors

**Log encryption kernel events** — This option controls logging encryption kernel events.

These events are usually errors, for example, scheme or method mismatch, checksum errors, clock synchronization mismatch, or rekey policy mismatch (SKIP).

# Properties Setup - Desktop Security

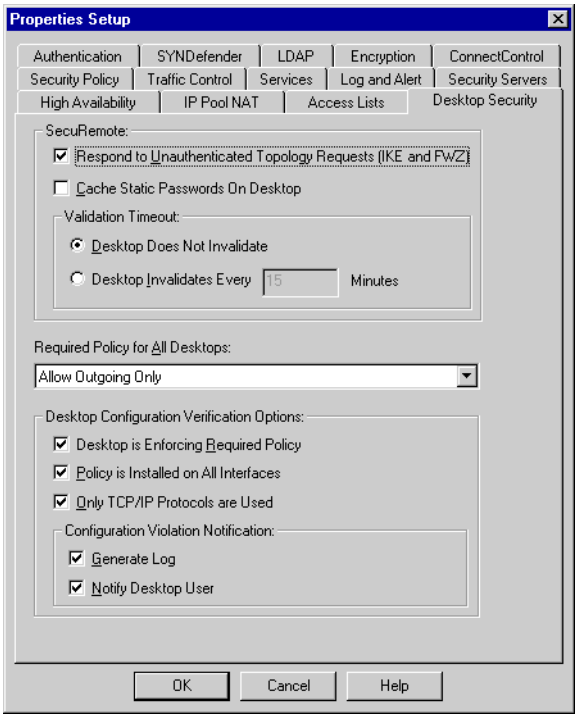



**FIGURE 8-3** Properties Setup — Desktop Security tab

This window (FIGURE 8-3) defines properties related to SecuRemote and SecureClient.

- For information about SecuRemote, see “Desktop Security” on page 132.
- For information about SecureClient, see Chapter 11, “VPN-1 SecureClient”.

# Workstation Encryption Properties

In order for a gateway to perform VPN functions, its encryption domain and encryption schemes must be defined. Multiple encryption schemes may be defined for a gateway, and the properties of each scheme must be defined.

**Note** – An encryption domain is the set of network objects on whose behalf the VPN/FireWall Module encrypts and decrypts.

These parameters are specified in the **VPN** tab of the **Workstation Properties** window (FIGURE 8-4 on page 106).

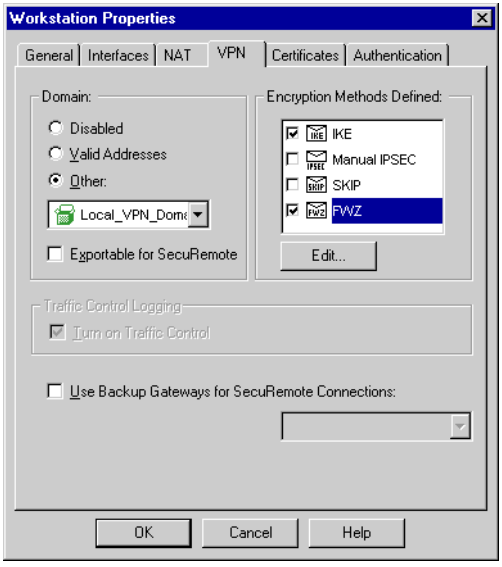



**FIGURE 8-4** Workstation Properties window — VPN tab

**Getting Here –** To display this window, choose **Manage➤Network Objects** in the menu, select the network object in the **Network Objects** window (FIGURE 4-1 on page 98 of *VPN-1/FireWall-1 Administration Guide*, click on **Edit** and then click on the **VPN** tab.

If the **VPN** tab is not visible, click on  to scroll the tabs until the **VPN** tab becomes visible.

**Domain** — the network object (usually a network or group) on whose behalf the VPN/FireWall Module encrypts and decrypts

> **Domain** is enabled only if **Gateway** is selected in **Type** in the **General** tab of the **Workstation Properties** window (FIGURE 4-5 on page 102 of *VPN-1/FireWall-1 Administration Guide*).
>
> If all the gateway's interfaces have been defined in the **Interfaces** tab of the gateway's **Workstation Properties window**, then **Valid Addresses** can be selected in **Domain**. In this case, the encryption domain is defined as the union of all the network objects defined in those **Valid Addresses** fields not specified as **Any**, **Others**, or **Open**.

**Encryption Methods Defined** — Check those encryption methods (schemes) defined for this machine.

> To define the properties of a workstation's encryption method, proceed as follows:

1. In **Encryption Methods Defined**, check the encryption method.
2. Select the encryption method (highlight it).
3. Click on **Edit**.

The appropriate window will be displayed, as follows:

- **IKE** — FIGURE 8-5 on page 108
- **Manual IPSEC** — No window will be displayed, because the Manual IPSec properties are properties of a rule, not properties of a workstation.
- **SKIP** — FIGURE 8-10 on page 112
- **FWZ** — FIGURE 8-13 on page 114

**Exportable for SecuRemote** — Specifies whether information about this object can be made available to SecuRemote Clients.

For information about SecuRemote, see Chapter 9, "SecuRemote Server," of *Check Point Virtual Private Networks*.

This field is relevant only for objects whose **Location** (in the **General** tab of the **Workstation Properties** window — FIGURE 4-5 on page 102 of *VPN-1/FireWall-1 Administration Guide* — is **Internal**.

**Turn on ETM Logging** — Specifies whether ETM products (FloodGate-1 and Compression) generate log entries in the VPN-1/FireWall-1 log.

ETM products use the OPSEC ELA proxy to generate log entries in the VPN-1/FireWall-1 log.

**Use Backup Gateways for SecuRemote Connections** — See "Properties Setup" on page 246 for information about this parameter.

# Encryption Method Properties

## IKE Properties

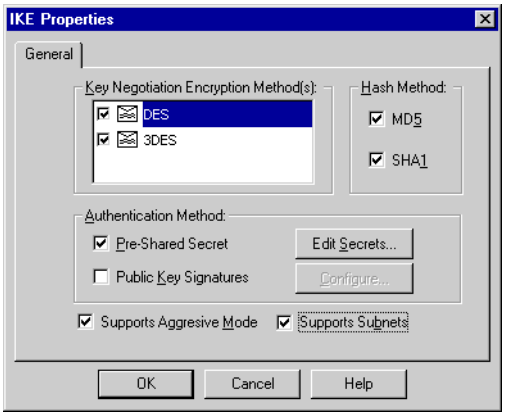



**FIGURE 8-5** IKE Properties window

The parameters in the **IKE Properties** window define the methods supported by the workstation for IKE key negotiations. The methods used to encrypt a specific session are defined in the **Rule Encryption Properties** windows (see “Rule Encryption Properties” on page 117).

**Key Negotiation Encryption Method(s)** — Check at least one of the methods.

**Hash Method** — Check at least one of the methods.

**Authentication Method** — Select at least one of the methods:

- **Pre-Shared Secret** — This workstation can authenticate itself and others (workstations and users) using pre-shared secrets.

  A pre-shared secret is sometimes called a “password.” If you check **Pre-Shared Secrets**, then click on **Edit Secrets** to display the **Shared Secrets** window (FIGURE 8-6 on page 109) in which you can define or modify the pre-shared secret.

- **Public Key Signatures** — This workstation can authenticate itself by a public key signature.

  If you check **Public Key Signatures**, then click on **Configure** to display the **Public Key Matching Criteria** window (FIGURE 8-9 on page 111) to define the matching criteria.

**Note –** A pre-shared secret is an attribute of a pair of entities, but a certificate is an attribute of a single entity. If a pre-shared secret is defined for a pair of gateways, and each of the gateways has a certificate as well, then IKE key negotiation between the gateways will use the pre-shared secret rather than the certificates.

**Supports Aggressive Mode** — If checked, the standard six packet IKE Phase 1 exchange is replaced by a three packet exchange (see “IKE Phase One (Main/Aggressive Mode)” on page 18).

**Supports Subnets** — If checked, IKE Phase 2 negotiates encryption keys for subnets rather than for individual hosts.

## Shared Secrets

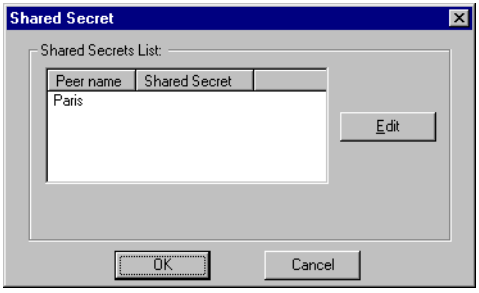



**FIGURE 8-6** IKE Shared Secrets window

In this window, you define the shared secret between this workstation and other workstations. The menu lists all other workstations listed for which IKE is enabled, except for this workstation (that is, the workstation whose properties you are defining now).

To define a pre-shared secret between this workstation and one of those in the list, proceed as follows:

1. Select that workstation.
2. Click on **Edit**.

   A text box is displayed below the list in which to enter the pre-shared secret.

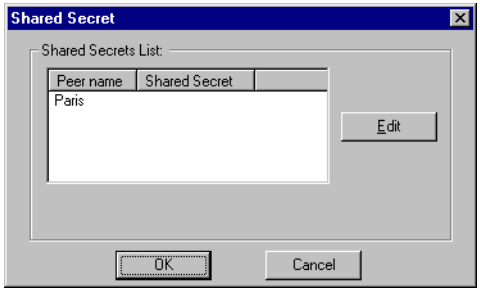



**FIGURE 8-7** Entering a Pre-Shared Secret

3. Enter the pre-shared secret and click on **Set**.

The **Shared Secrets** window now shows the pre-shared secret next to the workstation's name.

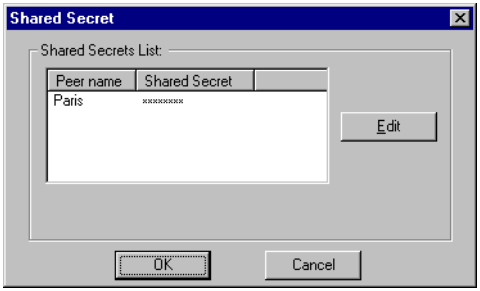



**FIGURE 8-8** Shared Secrets window showing a pre-shared secret

4 Click on **OK** to close the **Pre-Shared Secrets** window.

5 Click on **OK** to close the **IKE Properties** window.

If both workstations in a pair are managed by the same Management Module (that is, if **Internal** is selected for both of them under **Location** in the **General** tabs of their **Workstation Properties** windows — see FIGURE 4-5 on page 102 of *VPN-1/FireWall-1 Administration Guide*), then the shared secrets are updated for both workstations when you close the **IKE Properties** window. If they are managed by different Management Modules, you must repeat this procedure on each Management Module.

## Public Key Infrastructure

The VPN-1/FireWall-1 IKE implementation supports X.509 digital certificates supplied by the following Public Key Infrastructure (PKI) implementations:

- Check Point VPN-1 Certificate Manager
- OPSEC PKI vendors
- Entrust Technologies

For information about certificates, see Chapter 3, "Certificate Authorities."

## Public Key Configuration

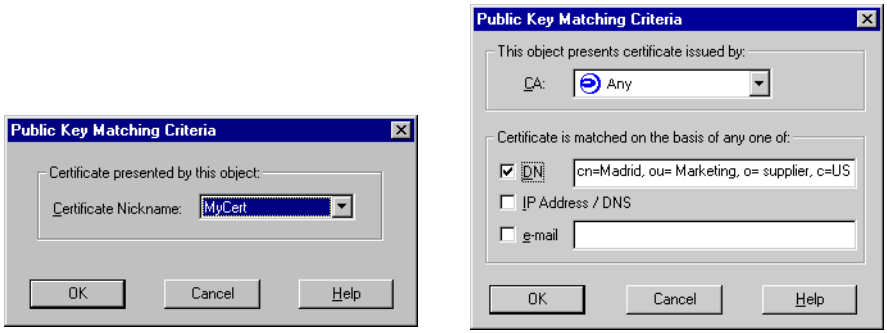



**FIGURE 8-9** Public Key Matching Criteria window (internal and external workstations)

The **Public Key Matching Criteria** window defines:

- for an internal workstation, the certificate with which the workstation will identify itself to other workstations
- for an external workstation, the CA that issued the workstation's certificate and the matching criteria

### Internal Workstations

An internal workstation is one where **Internal** is selected under **Location** in the **General** tab of its **Workstation Properties** window (see FIGURE 4-5 on page 102 of *VPN-1/FireWall-1 Administration Guide*).

In the **Public Key Matching Criteria** window (FIGURE 8-9), select a **Certificate** which this workstation will use to identify itself.

> The names in the list are those assigned to the workstation's certificates in the **Certificate Properties** window (see FIGURE 3-7 on page 31).

### External Workstations

An external workstation is one where **External** is selected under **Location** in the **General** tab of its **Workstation Properties** window (see FIGURE 4-5 on page 102 of *VPN-1/FireWall-1 Administration Guide*).

In the **Public Key Matching Criteria** window (FIGURE 8-9), select the **CA** that generated the external workstation's certificate, and then optionally check one or more of the certificate matching criteria (**DN**, **IP address / DNS** and **e-mail**).

**Warning –** The certificate is accepted if at least one of the selected criteria matches, even if some or all of the others do not match.

If you check **DN** or **e-mail**, you must also specify a value.

# SKIP Properties

## Key Manager Tab

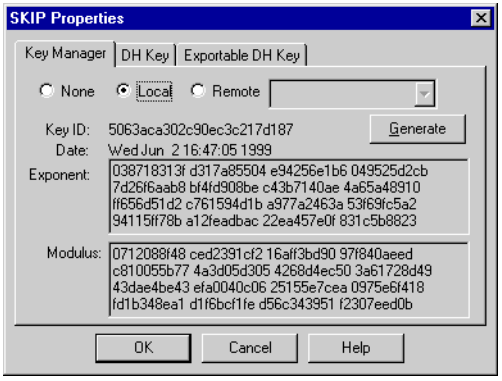



**FIGURE 8-10** SKIP Properties window - Key Manager tab

**Local**, **Remote** or **None** — Specifies the workstation's Certificate Authority.

- If you select **Local**, then this workstation's Certificate Authority is the Management Module with which you are currently working.
- If you select **Remote**, choose the workstation's Certificate Authority from the menu. The items in the menu are all the workstations on which VPN-1/ FireWall-1 is installed (as specified under **Modules Installed** in the **General** tab of their **Workstation Properties** windows), except this workstation's Management Station.
- If you select **None**, then there is no Certificate Authority and the keys will be read from a file with the **Read** button.

**Generate** — Generate the Certificate Authority's key or replace its existing key (available when **Certificate Authority** is **Local**).

**Get** — Get the Certificate Authority's key (available when **Certificate Authority** is **Remote**).

**Warning –** The first time you contact a Certificate Authority, its CA public key will be automatically fetched. However, since this transaction cannot be authenticated, you will get a warning message. It is recommended that you verify the key just obtained over the network by some non-network means, such as by fax or telephone.

**KeyID** — a unique ID (a cryptographic hash function of the public key value) identifying this object's key

**Date** — the date and time the key was generated

**Exponent** and **Modulus** —These read-only fields comprise the public key.

## DH Key Tab

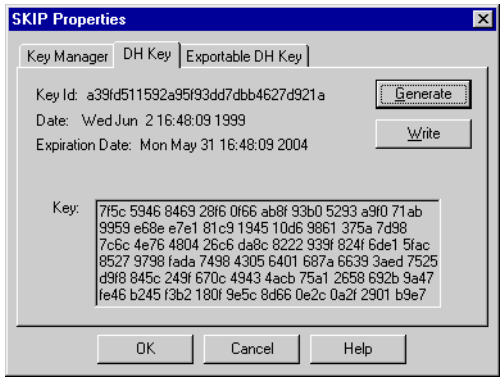



**FIGURE 8-11** SKIP Properties window - DH Key tab

**Generate** — Generate this workstation's Diffie-Hellman key or replace its existing key (available when **Certificate Authority** is **Local**).

**Get** — Get this workstation's Diffie-Hellman key from its Certificate Authority (available when **Certificate Authority** is **Remote**).

**Read** — Click on **Read** to read this workstation's key from a file (available when **Certificate Authority** is **None**).

**KeyID** — A unique ID (a cryptographic hash function of the public key value) identifying this workstation's key.

**Date** — The date and time the key was generated.

**Expiration Date** — The date the key expires.

**Key** — This read-only field is the public key.

## Exportable DH Key Tab

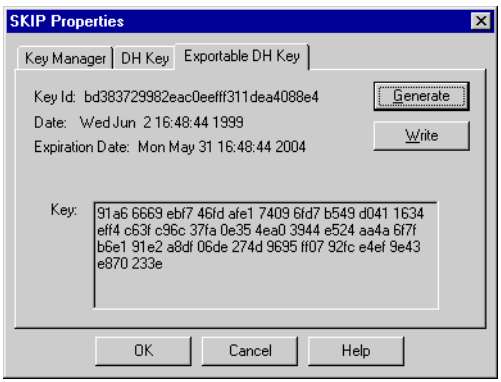



**FIGURE 8-12** SKIP Properties window - Exportable DH Key tab

The **Exportable DH Key** tab is available only if **Enable Exportable SKIP** is checked in the **Encryption** tab of the **Properties Setup** window (FIGURE 8-1 on page 102).

The fields in the **Exportable DH Key** tab are the same as those in the **DH Key** tab. The difference between the tabs is the strength of the generated key.

### Additional SKIP Properties

Additional properties relating to SKIP are defined in the **Encryption** tab of the **Properties Setup** window (FIGURE 8-1 on page 102).

## Manual IPSec Properties

There are no object–specific parameters for Manual IPSec encryption. All IPSec encryption parameters are rule–specific. See "Manual IPSec Encryption Properties" on page 120 for information on rule–specific Manual IPSec encryption parameters.

## FWZ Properties

### Key Manager Tab

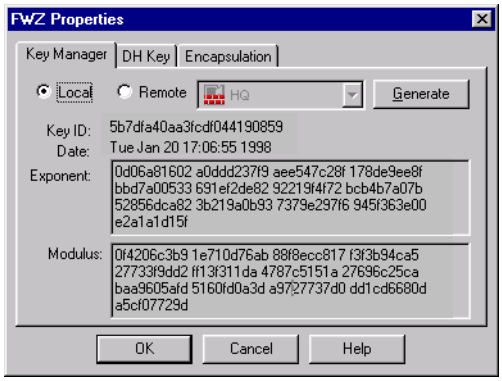



**FIGURE 8-13** FWZ Properties — Key Manager tab

**Local**, **Remote** or **None** — Specifies the workstation's Certificate Authority.

- If you select **Local**, then this workstation's Certificate Authority is the Management Module with which you are currently working.
- If you select **Remote**, choose the workstation's Certificate Authority from the menu. The items in the menu are all the workstations on which VPN-1/FireWall-1 is installed (as specified under **Modules Installed** in the **General** tab of their **Workstation Properties** windows), except this workstation's Management Station.

**Generate** — Generate the Certificate Authority's key or replace its existing key (available when **Certificate Authority** is **Local**).

**Get** — Get the Certificate Authority's key (available when **Certificate Authority** is **Remote**).

You cannot get the key of a gateway you have just defined. You must first install a Security Policy on that gateway and then click on **Get** to get its key.

**Warning –** The first time you contact a Certificate Authority, its CA public key will be automatically fetched. However, since this transaction cannot be authenticated, you will get a warning message. It is recommended that you verify the key just obtained over the network by some non-network means, such as by fax or telephone.

**KeyID** — a unique ID (a cryptographic hash function of the public key value) identifying this object's key

**Date** — the date and time the key was generated

**Exponent** and **Modulus** —These read-only fields comprise the actual key.

## DH Key Tab

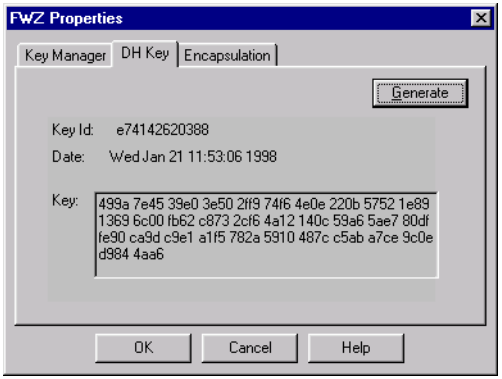



**FIGURE 8-14** FWZ Properties — DH Key tab

**Generate** — Generate this object's Diffie-Hellman key or replace its existing key (available when **Certificate Authority** is **Local**).

**Get** — Get this object's Diffie-Hellman key from its Certificate Authority (available when **Certificate Authority** is **Remote**).

**KeyID** — a unique ID (a cryptographic hash function of the public key value) identifying this object's key

**Date** — the date and time the key was generated

**Key** — This read-only field is the actual key.

### Encapsulation Tab

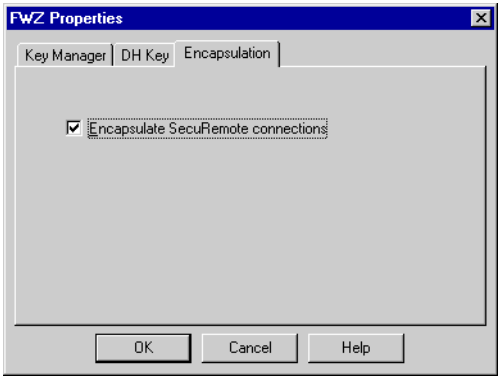



**FIGURE 8-15** FWZ Properties — Encapsulation tab

**Encapsulate SecuRemote connections** — Encapsulate SecuRemote packets inside packets with the encrypting gateway's IP address as the destination.

> This option enables a SecuRemote Client to connect to otherwise unreachable hosts inside the site's encryption domain. For more information, see "FWZ Encapsulation" on page 151.

## Key Info (FWZ and SKIP)

To display the **Key Info** window (FIGURE 8-16), click on **View** in the **VPN** tab of the **Workstation Properties** window (FIGURE 8-4 on page 106).

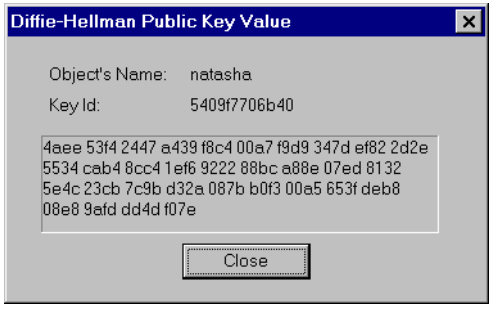



**FIGURE 8-16** A gateway's public key

This window displays information about a key, but does not allow modification of this information, which can be performed only from the **VPN** tab of the **Workstation Properties** window (FIGURE 8-4 on page 106).

**Object Name** — the name of the object

**KeyID** — a unique ID (a cryptographic hash function of the public key value) identifying this key

# Rule Encryption Properties

After adding an encryption rule to the Rule Base, the rule's encryption scheme and associated parameters must be defined in its **Encryption Properties** window.

**Note –** Keep in mind that:

- A rule can only have one encryption scheme, but multiple encryption rules for encrypting traffic between two sites can be defined. For example, one rule might specify that HTTP communications between the sites is encrypted with IKE and 3DES/SHA1, while another rule specifies that SMTP and POP communications between the sites is encrypted with SKIP and DES/MD5.
- Some services, for example, FTP and RSH, open back connections on another port. These back connections are automatically encrypted, and there is no need to define a rule for this purpose.

To display a rule's **Encryption Properties** window, proceed as follows:

1. Double click on a rule's **Encrypt** action in the Rule Base Editor.

   The **General** tab of the **Encryption Properties** window (FIGURE 8-17) is displayed.

2. Select an encryption scheme for the rule from the list and click on **Edit**.

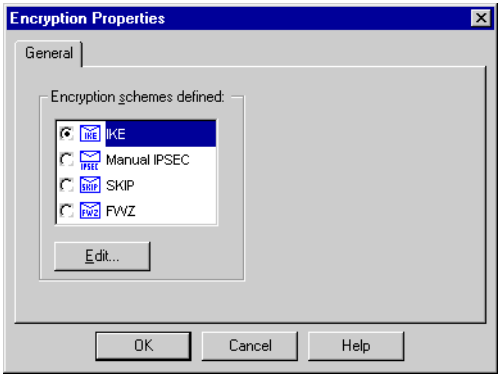



**FIGURE 8-17** Encryption Properties window — General tab

The appropriate window will be opened, depending on the scheme you selected.

## IKE Encryption Properties

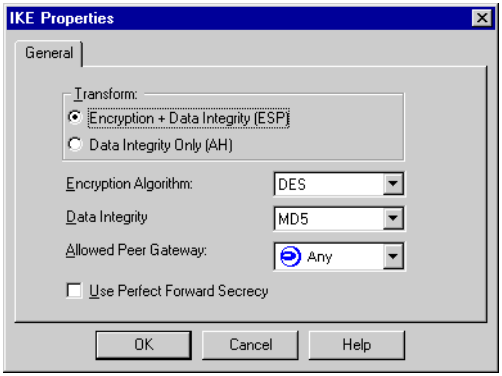



**FIGURE 8-18** IKE Properties window

The IKE properties in this window define how packets are encrypted. The IKE properties in the **VPN** tab of the **Workstation Properties** window (FIGURE 8-4 on page 106) define how the IKE key exchange is encrypted.

In **Transform**, check one of the following:

- **Encryption + Data Integrity (ESP)** — The Security Association will include both encryption and data integrity (authentication).
- **Data Integrity Only (AH)** — The Security Association will include only data integrity (authentication).

**Encryption Algorithm** — Specifies the encryption algorithm for the traffic.

The available choices depend on the encryption algorithms installed.

**Data Integrity** — Specifies the cryptographic checksum method to be used for ensuring data integrity.

**Peer Gateway** — Specifies the gateways with which a gateway encrypting under this rule is prepared to conduct an encrypted session.

This field can be set to the following values:

- **Any** — each gateway is prepared to conduct encrypted sessions with all other gateways
- *gateway or host name* — each gateway is prepared to conduct encrypted sessions only with the named gateway or host

In both cases, a gateway is prepared to conduct encrypted sessions with another gateway only if the packet's source IP address (for decryption) or destination IP address (for encryption) is in the other gateway's encryption domain.

**Use Perfect Forward Secrecy** — This feature ensures that an eavesdropper who uncovers a long-term encryption key will be unable to use it to decrypt traffic sent in the past.

### Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) is optional only in Phase 2 (Quick Mode) exchanges. Phase 1 (Aggressive or Main Mode) always involves the exchange of Diffie-Hellman (DH) keys. Turning on PFS means that DH keys will be exchanged in Phase 2 as well, reducing performance, but enhancing security.

Suppose you are not using PFS, and an intruder somehow manages to find out your Phase 1 keys. The intruder will now be able to decrypt all the Phase 2 exchanges, and derive the IPSEC keys from these exchanges.

However, if you are using PFS, an intruder who discovers your Phase 1 keys will still have to discover the DH shared secrets in order to discover the IPSEC keys. So every time another Phase 2 exchange takes place, the intruder will have to break yet another DH key even though he already knows the Phase 1 keys.

The name “Perfect Forward Secrecy" is derived from the fact that if an intruder breaks your system at a given point of time, and gains access to your entire state (all current Phase 1 and Phase 2 keys), he will not be able to decrypt future communications after the next Phase 2 exchange takes place.

## SKIP Encryption Properties

The **SKIP Encryption Properties** window defines the encryption properties of a SKIP encryption rule.

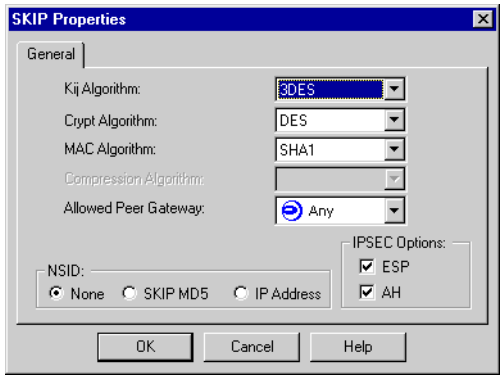



**FIGURE 8-19** SKIP Encryption Properties window

**Kij Algorithm** — the algorithm used to encrypt the keys used for data encryption and data authentication

**Crypt Algorithm** — the data encryption algorithm

**MAC Algorithm** — the data authentication algorithm

**Peer Gateway** — Specifies the gateways with which a gateway encrypting under this rule is prepared to conduct an encrypted session.

This field can be set to the following values:

- **Any** — VPN-1/FireWall-1 will attempt to find a suitable gateway based on the defined encryption domains.
- *gateway or host name* — each gateway is prepared to conduct encrypted sessions only with the named gateway or host

In both cases, a gateway is prepared to conduct encrypted sessions with another gateway only if the packet's source IP address (for decryption) or destination IP address (for encryption) is in the other gateway's encryption domain.

If both gateways are FireWalled (VPN-1/FireWall-1 is installed on them both), then there must be two rules — each specifying encryption in one direction — and only one rule must be installed on each of the gateways.

**SKIP Diagnostics Track** — Select one of the following:

- **None** — no logging or alerting
- **Log** — log the event
- **Alert** — issue an alert

**NSID** — Name Space ID, the domain from which Key IDs in the SKIP header are taken

- **None** — No Key IDs appear in the header.
- **SKIP MD5** — The KeyIDs are an MD5 hash of the Diffie-Hellman public keys.
- **IP Address** — The KeyIDs are the IP address of the gateway.

**IPSec Options** — At least one option must be checked.

- **ESP** — encrypt
- **AH** — authenticate

## Manual IPSec Encryption Properties

The **Manual IPSec Encryption Properties** window defines the encryption properties of a Manual IPSec encryption rule.

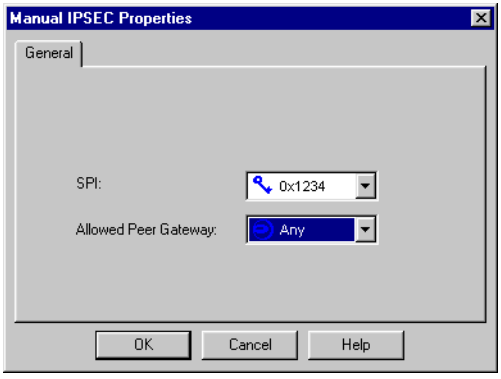



**FIGURE 8-20** Manual IPSec Encryption Properties window

**SPI** — Security Parameters Index — a number which uniquely identifies a group of security parameter definitions

Select an SPI from the drop-down list.

The SPIs are defined in the **SPI** tab of the **Manual IPSec** window (FIGURE 8-22 on page 122). For more information, see “Defining an SPI” on page 121.

**Peer Gateway** — Specifies the decrypting gateway. This gateway will be the destination in the new IP header.

This field can be set to the following values:

- **Any** — VPN-1/FireWall-1 will attempt to find a suitable gateway based on the defined encryption domains.
- *gateway name* — VPN-1/FireWall-1 will conduct encrypted sessions only with the named gateway.

In both cases, a gateway is prepared to conduct encrypted sessions with another gateway only if the packet’s source IP address (for decryption) or destination IP address (for encryption) is in the other gateway’s encryption domain.

If both gateways are FireWalled (VPN-1/FireWall-1 is installed on them both), then there must be two rules — each one specifying encryption in one direction — and only one rule must be installed on each of the gateways.

## Defining an SPI

To define an SPI, select **Keys** from the **Manage** menu. The **Encryption Keys** window (FIGURE 8-21) is displayed.

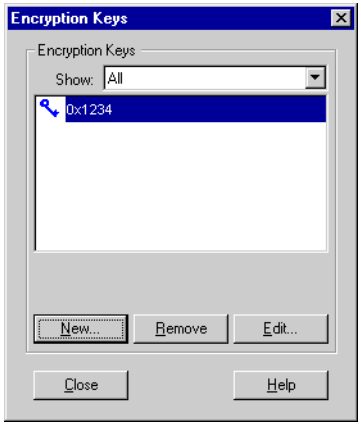



**FIGURE 8-21** Encryption Keys window

### Creating a New Key

To create a new key, click on **New** and select **SPI** from the menu.

The **Manual IPSec** window (FIGURE 8-22) is displayed.

## Deleting a Key

To delete a key, select the object and click on **Remove**.

## Modifying a Key

To modify a key, select the key and click on **Edit**, or double-click on the key.

The **Manual IPSec** window (FIGURE 8-22) is displayed.

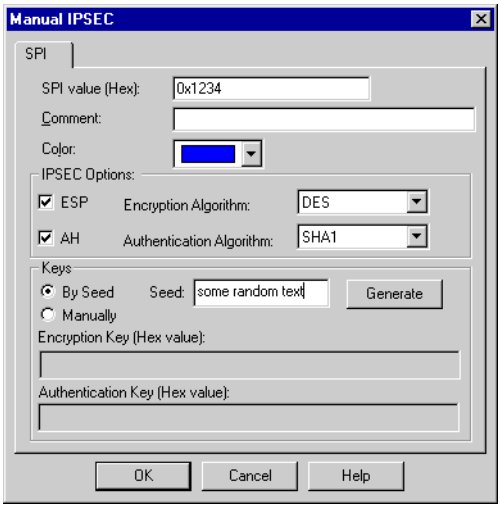



**FIGURE 8-22** Manual IPSec window

**SPI value** — a unique identifying key

This is a hexadecimal number (enter leading 0x) and must be greater than 0x100. The value must be in the range defined in **SPI Allocation Range** in the **Encryption** tab of the **Properties Setup** window (see FIGURE 8-1 on page 102).

**Comment** — descriptive text

This text is displayed on the bottom of the **Keys** window when this key is selected.

**Color** — the color of the key's icon

Select the desired color from the drop-down list.

**IPSec Options** — At least one option must be checked.

- **ESP** — If encryption is defined for this SPI, check **ESP** and choose an **Encryption Algorithm** from the drop-down list.
- **AH** — If authentication is defined for this SPI, check **AH** and choose an **Authentication Algorithm** from the drop-down list.

**Keys** — You can choose to generate a key from a seed, or enter a key manually.

### ▼ To generate a key from a seed

Enter a value for **Seed** and click on **Generate**.

- If **ESP** is checked under **IPSec Options**, an encryption key is generated and displayed in **Encryption Key**.
- If **AH** is checked under **IPSec Options**, an authentication key is generated and displayed in **Authentication Key**.

### ▼ To generate a key manually

Enter the key(s) manually.

- If **ESP** is checked under **IPSec Options**, enter an encryption key in **Encryption Key**.
- If **AH** is checked under **IPSec Options**, enter an authentication key in **Authentication Key**.

**Encryption Key (Hex value)** — read-only, unless key was manually generated

**Authentication Key (Hex value)** — read-only, unless key was manually generated

## FWZ Encryption Properties

The **FWZ Properties** window defines the encryption properties of an FWZ encryption rule.

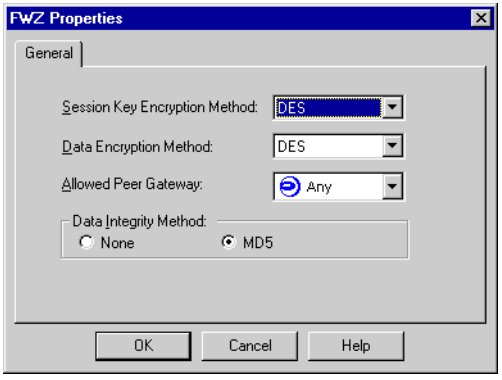



**FIGURE 8-23** FWZ Encryption Properties window

**Session Key Encryption Method** — Specifies the encryption algorithm for session keys.

**Data Encryption Method** — Specifies the encryption algorithm for communications packets.

The available choices depend on the encryption algorithms installed.

You can also choose **Clear** (meaning no encryption) or **Any** (meaning the data encryption method is chosen by the other party).

**Data Integrity Method** — Specifies the cryptographic checksum method to be used for ensuring data integrity.

**Peer Gateway** — Specifies the gateways with which a gateway encrypting under this rule is prepared to conduct an encrypted session.

This field can be set to the following values:

- **Any** — each gateway is prepared to conduct encrypted sessions with all other gateways
- *gateway or host name* — each gateway is prepared to conduct encrypted sessions only with the named gateway or host

In both cases, a gateway is prepared to conduct encrypted sessions with another gateway only if the packet's source IP address (for decryption) or destination IP address (for encryption) is in the other gateway's encryption domain.

**Protocol Diagnostics** and **Diagnostics Track** — Specifies the action to be taken if protocol errors are detected.

# Certificate Authority (FWZ Encryption)

## Overview

To display the **Certificate Authority Keys** window (FIGURE 8-24), click on **Edit** in the **Encryption Setup** window. The **Certificate Authority Keys** window displays information about a Certificate Authority's public key. The information cannot be directly modified or edited in this window, but a new key can be generated or fetched from the Certificate Authority.

The data displayed in this window are all public data. No private data are displayed.

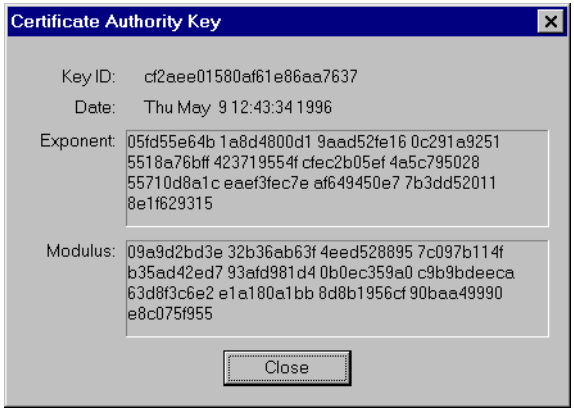



**FIGURE 8-24** Certificate Authority Key window

**Object Name** — the name of the object

**Scheme** — the encryption scheme for the object

**Generation Date** — the date and time the key was generated

**KeyID** — a unique ID identifying this object's key

This is a cryptographic hash (using MD5) of the public key value, and suffices to verify the public key when out of band verification is required

**Exponent** — the exponent part of the CA's RSA key

**Modulus** — the modulus part of the CA's RSA key

### New Keys

You can generate or fetch a Certificate Authority's public key as follows:

- If the CA is the local Management Station, click on **Generate** to generate a new key for the CA.
- If the CA is external, click on **Get** to fetch the CA's public key.

**Warning –** The first time you fetch the key, it is recommended that you authenticate it by some other non-network means, such as by fax or telephone.
The local CA key is generated automatically during the VPN-1/FireWall-1 installation. There is seldom any compelling reason to change it by generating a new key. Moreover, changing the key requires coordination with remote FireWalls to ensure that they re-fetch the local key and reload their gateways.

## Encrypting Services That Open Back Connections

Some services, for example, FTP and RSH, open back connections on another port. These back connections are automatically encrypted, and there is no need to define a rule for this purpose.

CHAPTER 9

# SecuRemote Server

## In This Chapter



## SecuRemote Implementation

### Overview

Check Point SecuRemote provides client-to-site VPN services, where a site can be an enterprise network, a specific LAN segment or an individual server. It consists of a client component (SecuRemote Client) and one or more VPN-enabled VPN/FireWall Modules and Management Stations.

- For an overview of SecuRemote deployment and usage, see “SecuRemote” on page 10.
- For information about the SecuRemote Client software, see Chapter 10, “SecuRemote Client.”

SecuRemote is implemented in the framework of a Check Point Virtual Private Network. The system administrator must first configure a VPN and implement the VPN Encryption feature, and then extend encryption facilities to nomadic users with the SecuRemote feature.

To configure SecuRemote, you must:

1. Configure and implement Check Point VPN Encryption on the enterprise network.

   If your enterprise network consists of one site only, then configure and implement Check Point VPN Encryption at that site.

2. Define the users that will be allowed access, and specify their means of authentication.

   For information on how to define a SecuRemote user's means of authentication, see "Defining SecuRemote Users" on page 133.

   Every authentication scheme you select for a user must be enabled on the SecuRemote Server.

   - For FWZ authentication, enable the authentication scheme in the **Authentication** tab of the **Workstation Properties** window (see FIGURE 4-10 on page 110 of *VPN-1/FireWall-1 Administration Guide*).
   - For IKE authentication, define the authentication parameters in the **Authentication** and **Encryption** tabs of the user's **IKE Properties** window (FIGURE 9-9 on page 137).

3. Install the SecuRemote Client on users' computers.

   For information on installing and configuring a SecuRemote Client, see "Installing the SecuRemote Client" on page 181.

4. Define rules in the Rule Base that enable SecuRemote users to connect to the enterprise network.

   As in any other case, in order for SecuRemote users to gain access to the network, there must be a rule in the Rule Base that allows them access. It is not necessary that there be a specific rule for SecuRemote users. A SecuRemote user can be allowed access as part of a group of users, some of whom are SecuRemote users and some of whom are not.

   A SecuRemote user's connection is encrypted when the user makes the connection using SecuRemote, but is not encrypted when the user makes the connection without using SecuRemote, as do the other users in the group.

# Example

## Before SecuRemote is Installed

Suppose that in the network configuration depicted in FIGURE 9-1, Kings is Bob's PC and Backs is Alice's PC.

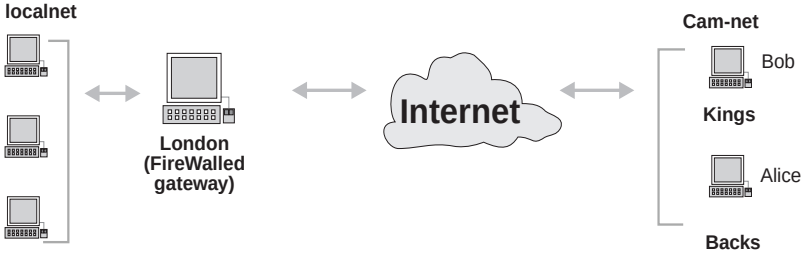



**FIGURE 9-1** SecuRemote Example Configuration

Suppose also that a group Dons has been defined, consisting of Alice and Bob, and that the following rules in London's Rule Base allow Alice and Bob access to localnet:

| | Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | Cam_net | localnet | telnet | Accept | Short Log | Gateways |
| 2 | Dons@Cam_net | localnet | ftp | UserAuth | Short Log | Gateways |

These rules specify that Alice and Bob can freely use TELNET on localnet, but they can use FTP only after User Authentication. It doesn't matter from which PC each user connects. Bob can connect from Alice's PC and *vice versa*, provided they use their own names for the authentication process.

## After SecuRemote is Installed

Suppose that Bob installs the SecuRemote Client on his PC (Kings) and defines London as a site. This has the effect of encrypting connections between Kings and the defined sites (because SecuRemote is an attribute of a PC, not of a user). Bob can continue to use FTP and TELNET on localnet from Kings under the same rules, but the connection will be encrypted, provided *all* the following conditions are met (see FIGURE 9-2):

***1*** London's encryption domain includes localnet.

This is defined on London's Management Module.

***2*** London's encryption domain is exportable.

This is defined on London's Management Module.

***3*** On Kings, London is defined as a site.

This is defined on King's SecuRemote Client.

If any of these conditions is not true, then the connection will not be encrypted.

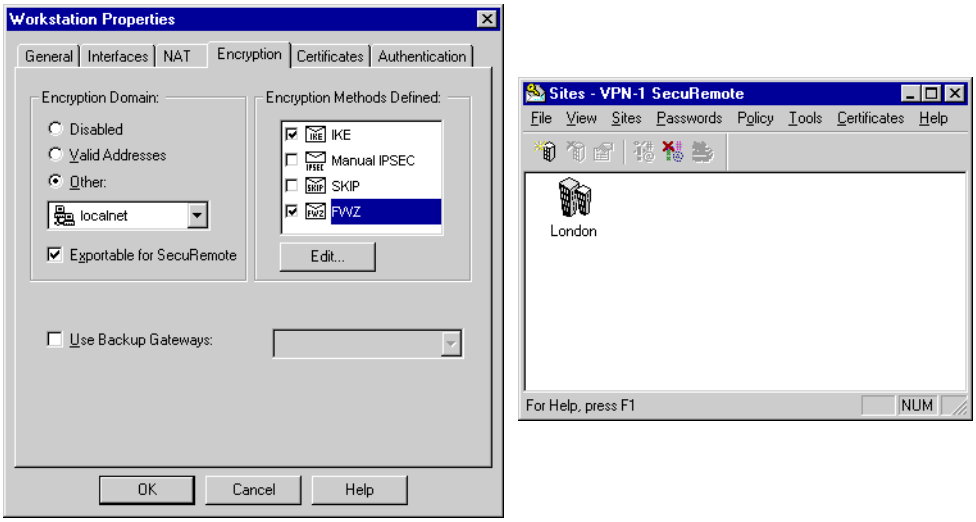



**FIGURE 9-2** London VPN parameters and SecuRemote Site

When Bob attempts to use FTP on localnet from Kings, he will be authenticated twice: the first time by SecuRemote on Kings (the SecuRemote Client on the PC asks Bob to authenticate himself, but it is the SecuRemote Server that verifies his credentials) and the second time by the SecuRemote Server on London (as the Rule Base specifies).

Bob can also connect from Alice's PC (Backs), but in this case the connection will not be encrypted, because SecuRemote is not installed on Backs. The same situation applies to Alice — if she connects from Kings, the session will be encrypted, but if she connects from Backs it will not.

Next, suppose London's system administrator changes the **Action** in the second rule to **Client Encrypt**, as follows:

| | Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | Cam_net | localnet | telnet | Accept | Short Log | Gateways |
| 2 | Dons@Cam_net | localnet | ftp | Client Encrypt | Short Log | Gateways |

TABLE 9-1 summarizes how Alice and Bob use TELNET and FTP on localnet.

**TABLE 9-1** How Alice and Bob connect

| user | computer | TELNET connects under ... | and FTP ... |
|---|---|---|---|
| **Bob** | Kings (SecuRemote installed) | the first rule, and the session is encrypted | connects under the second rule, and the session must be encrypted |
| **Bob** | Backs | the first rule, and the session is *not* encrypted because there is no SecuRemote on Backs | cannot connect, because the session *must* be encrypted but there is no SecuRemote on Backs |
| **Alice** | Kings (SecuRemote installed) | the first rule, and the session is encrypted | connects under the second rule, and the session must be encrypted |
| **Alice** | Backs | the first rule, and the session is *not* encrypted because there is no SecuRemote on Backs | cannot connect, because the session *must* be encrypted but there is no SecuRemote on Backs |

The effect of the Client Encryption rule is to force the connection from Kings to be encrypted. Without the Client Encryption rule, the connection would not be encrypted if one of the required conditions were not true (see “After SecuRemote is Installed” on page 129).

# Properties Setup

## Desktop Security

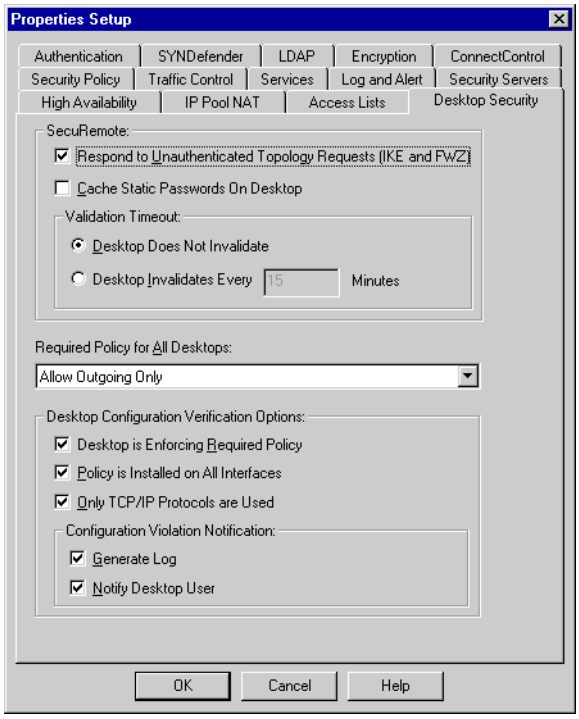



**FIGURE 9-3** Properties Setup — Desktop Security tab

### SecuRemote

**Respond to Unauthenticated Topology Requests (IKE and FWZ)** — If checked, the site will respond to topology requests from SecuRemote Clients even if the request is not encrypted.

This feature enables backwards-compatibility with earlier versions of the SecuRemote Client.

If this option is not checked, then the SecuRemote user must have IKE defined as one of the **Client Encryption** methods in the **Encryption** tab of his or her **User Properties** window (see FIGURE 9-5 on page 134).

**Cache Static Passwords on Desktop** — If checked, static passwords (OS and VPN-1/FireWall-1) will be cached on the desktop, and the SecuRemote Client user will not be required to reauthenticate if he or she is using OS or VPN-1/FireWall-1 passwords.

**Validation Timeout** — Check one of:

**Desktop Does Not Invalidate** — If checked, SecuRemote passwords never expire (that is, that they are valid until the next time the PC is turned off or re-booted).

**Desktop Invalidates Every ... Minutes** — If checked, SecuRemote passwords become invalid after the specified time period and the user must re-authenticate.

If multiple sites are defined on a SecuRemote Client, the timeout for all sites will be the minimum of all the sites' timeouts.

# Defining SecuRemote Users

**Note –** This section describes how to configure users with the Check Point GUI. See *Check Point Account Management Client* for information on configuring users on an LDAP Server.

## User Properties

To define a SecuRemote user's authentication and encryption properties, proceed as follows:

1. Open the **Users** window (FIGURE 9-4 on page 133) by:
   - choosing **Users** from the **Manage** menu, *or*
   - clicking on  in the toolbar.


**FIGURE 9-4** Users window

**2** Open the **User Properties** window (FIGURE 9-5) for the user by:

- double-clicking on the user, *or*
- selecting the user and clicking on **Edit**.

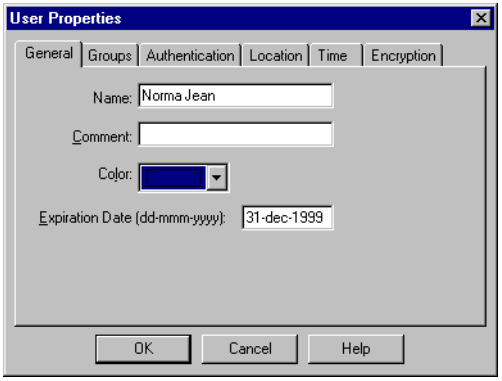



**FIGURE 9-5** User Properties window — General tab

**Note –** For FWZ encryption, a user's authentication method is defined in the **Authentication** tab (FIGURE 9-6). For IKE encryption, the user's authentication method is defined in the **Encryption** tab (FIGURE 9-7 on page 135). Encryption properties for both FWZ and IKE encryption are defined in the **Encryption** tab.
A user can have both FWZ and IKE encryption defined.

**3** If the user's encryption scheme will only be IKE, proceed to "IKE Properties" on page 137.

## FWZ Authentication Properties

**4** Display the user's **Authentication** tab (FIGURE 9-6).

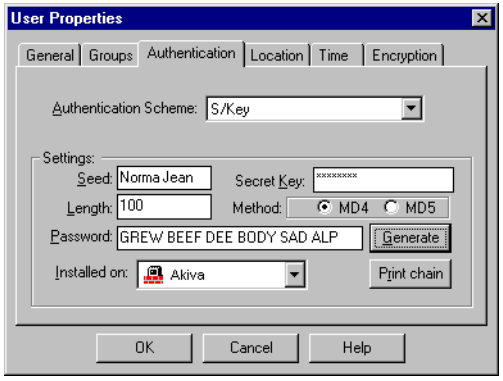



**FIGURE 9-6** User Properties window — Authentication tab showing S/key Authentication

**5** Choose an **Authentication Scheme** for the user.

After defining how the user will be authenticated for FWZ, you must next define the encryption properties of the user's SecuRemote connections.

## Client Encryption Properties

**6** Display the user's **Encryption** tab (FIGURE 9-6).


**FIGURE 9-7** User Properties window — Encryption tab

**7** Under **Successful Authentication Track**, specify a logging option for encryption attempts.

For Client Encryption, **Successful Authentication Track** is specified in the **Encryption** tab of the **User Properties** window, because successful authentication and key exchange are possible even if there are no Client Encryption rules.

**8** To enable an encryption method for the user, check the box next to the encryption scheme's name under **Client Encryption Methods**.

**Note –** If **IKE** is not selected, then **Respond to Unauthenticated Topology Requests (IKE and FWZ)** must be checked in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 9-3 on page 132).

**9** To define this user's encryption method properties, double-click on the icon next to the encryption method's name. The appropriate **Encryption Properties** window (FIGURE 9-8 or FIGURE 9-9) is displayed.

## FWZ Properties

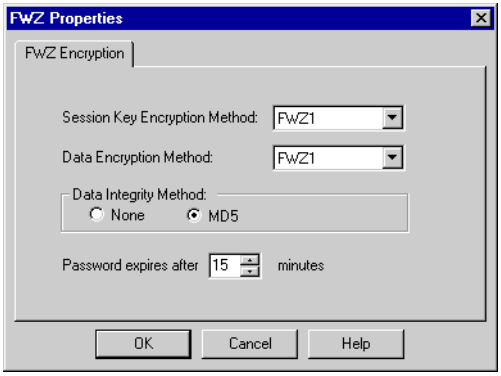



**FIGURE 9-8** FWZ Properties window

**Session Key Encryption Method** — the encryption algorithm for session keys

The available choices depend on the encryption algorithms installed.

You can also choose **Clear** (meaning no encryption) or **Any** (meaning the session key encryption method is chosen by the other party).

**Data Encryption Method** — the encryption algorithm for communications packets

The available choices depend on the encryption algorithms installed.

You can also choose **Clear** (meaning no encryption) or **Any** (meaning the data encryption method is chosen by the other party).

**Data Integrity Method** — the cryptographic checksum method to be used for ensuring data integrity

**Password Expires After ... Minutes** — the number of minutes (not less than 15) after which the user will be asked to re-authenticate by entering the password again

For multiple user passwords, the user enters the same password as before. For one-time passwords, the user must enter the currently valid password.

## IKE Properties

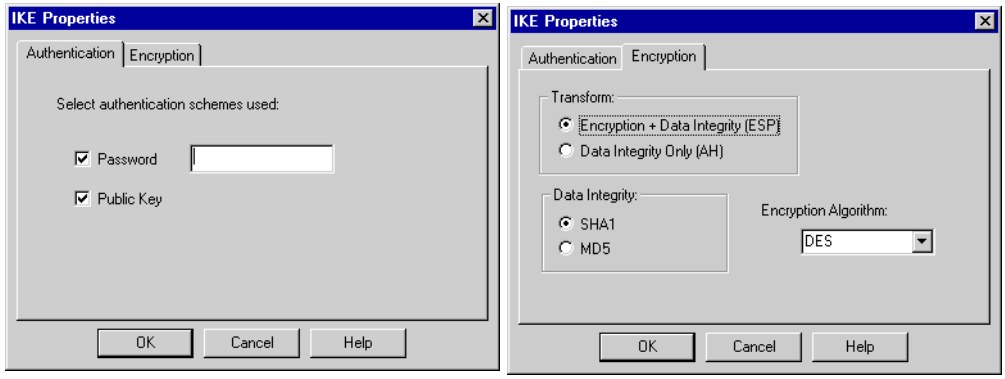



**FIGURE 9-9** IKE Properties windows

### Authentication Tab

Check the authentication schemes to be used to authenticate this user for SecuRemote connections:

- **Password** — The user will be authenticated by a password (pre-shared secret).

  If **Password** is checked, enter the password.

- **Public Key** — the user will be authenticated by a public key certificate (PKI).

### Encryption Tab

In **Transform**, check one of the following:

- **Encryption + Data Integrity (ESP)** — The Security Association will include both encryption and data integrity (authentication).
- **Data Integrity Only (AH)** — The Security Association will include only data integrity (authentication).

**Data Integrity** — the cryptographic checksum method to be used for ensuring data integrity

Choose **SHA1** or **MD5**.

**Encryption Algorithm** — the encryption algorithm to be used

Choose one of the available algorithms. You should choose one of the algorithms available to the SecuRemote Client. If you choose an algorithm stronger than any of those available to the SecuRemote Client, the connection will fail.

- The algorithms available on the SecuRemote Server depend on the VPN-1/ FireWall-1 software version and license.

- The algorithms available on the SecuRemote Client depend on the SecuRemote Client software version. To see which versions are available on the SecuRemote Client, select **About** from the SecuRemote Client's **Help** menu.

  TABLE 9-2 lists the available methods on the SecuRemote Client.

**TABLE 9-2** Client About SecuRemote window text and encryption methods

| text in About box | available encryption algorithms |
|---|---|
| Export | 40 bit algorithms (CAST-40 and DES-40CP) |
| DES | DES (in addition to those listed under Export) |
| Strong | 3DES (in addition to those listed under DES and Export) |

# Structure of a SecuRemote Connection

## Topology

Before a SecuRemote connection can take place, the SecuRemote Client must obtain information (including the topology) about the sites to which it will connect. There are two ways the Client can obtain the site information:

- A user can define a site and download the site information.

  See "Defining Sites" on page 187 for information on how to define sites on the SecuRemote Client.

- The System Administrator can prepare a standard `userc.c` file on the installation media for SecuRemote users, pre-defining sites for them. In this way users do not have to download the topologies of the sites to which they will be connecting.

The SecuRemote Client stores the topologies it knows about in the `userc.c` file. It is only necessary for a SecuRemote Client to download the site information when it changes.

### Site Information (Topology) Download

Starting with Versions 4.0 of the SecuRemote Client and Server, site information may be downloaded by a SecuRemote Client in encrypted format. Earlier versions did not encrypt the site information download.

#### Pre-Version 4.0 SecuRemote Clients

If you are using a pre-Version 4.0 SecuRemote Client with a Version 4.0 or higher SecuRemote Server, check **Respond to Unauthenticated Topology Requests (IKE and FWZ)** in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 9-3 on page 132). The SecuRemote Server will then download site information in unencrypted format to all SecuRemote Clients.

If **Respond to Unauthenticated Topology Requests (IKE and FWZ)** is not checked, then:

- Users of Version 4.0 SecuRemote Clients must have IKE Client Encryption defined as one of the **Client Encryption** methods in the **Encryption** tab of their **User Properties** window (see FIGURE 9-7 on page 135).
- Pre-Version 4.0 SecuRemote Clients will be unable to obtain the site information.

The site information also indicates whether a gateway supports FWZ or IKE or both. For gateways that support both FWZ and IKE, the method used depends on the settings in the **Options** window of the SecuRemote Client (see TABLE 9-4 on page 141).

**Note –** System administrators can ensure that all company personnel have the same site configuration for SecuRemote by copying a standard `userc.c` file to the installation diskette set. It is also possible to supply FWZ and IKE users with different `userc.c` files.

## Pre-Version 4.1 SecuRemote Clients

Pre-Version 4.1 SecuRemote Clients download site information through the SecuRemote Server port 256. Starting with Version 4.1, site information is downloaded through port 264.

If you are using pre-Version 4.1 SecuRemote Clients with a Version 4.1 or higher SecuRemote Server, you must specify a rule that enables the SecuRemote Server to download site information through TCP port 256.

FIGURE 9-10 shows an example of such a rule.

- **Source** is set to **Any** because the SecuRemote Client's IP address is not known in advance.
- **Destination** must include all the SecuRemote Servers from which pre-Version 4.1 SecuRemote Clients will download site information.
- **Install On** should be the same as **Destination**.
- Even though the **Action** is **Accept**, the connection will be authenticated unless **Respond to Unauthenticated Topology Requests (IKE and FWZ)** is checked in the **Desktop Security** tab of the **Properties Setup** window.


**FIGURE 9-10** Rule for Module- Use Port 256

## Pre-Version 4.1 SecuRemote Servers

If you are using Version 4.1 SecuRemote Client(s) with a pre-Version 4.1 SecuRemote Server, the SecuRemote Client will experience a delay of 30 seconds (in addition to normal network delays) while it attempts to download the SecuRemote Server's site information. This happens because the pre-Version 4.1 Server expects to download site

information through port 256 while Version 4.1 Clients open a connection to SecuRemote Server port 264. The Version 4.1 Clients wait 30 seconds and then try to open a connection through SecuRemote Server port 256.

There are two different methods to prevent the 30 second timeout:

***1*** Add a rule similar to the one shown in FIGURE 9-11:


**FIGURE 9-11** Rule to Reject Topology Download on Port 264

- **Destination** should be the SecuRemote Servers.
- **Service** should be FW1_topo (the VPN-1/FireWall-1 topology service).
- **Action** should be **reject** to cause the SecuRemote Client to immediately re-try by connecting to SecuRemote Server port 256 instead of waiting 30 seconds and then timing out.
- **Install On** should be the same as **Destination**.

If the FW1_topo service is not defined (this may happen if your Management Module is pre-Version 4.1), define it using the **TCP Service Properties** window (FIGURE 9-12) as follows:

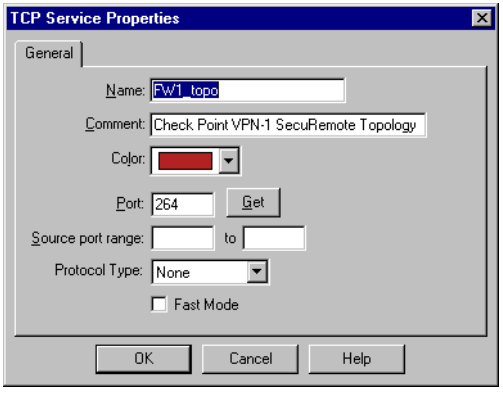



**FIGURE 9-12** SecuRemote Topology Service Port 264

***2*** Add the following line to the `options` section of the `userc.C` files of Version 4.1 SecuRemote Clients:

```
:gettopo_port (256)
```

This method is not recommended, because the change will be overwritten if you upgrade or reinstall SecuRemote.

## Authentication

The first time a SecuRemote Client initiates a connection to a site (and also whenever a password expires), the user must first authenticate himself or herself to the FireWall/VPN Module. The authentication method used depends on the encryption method used for the connection.

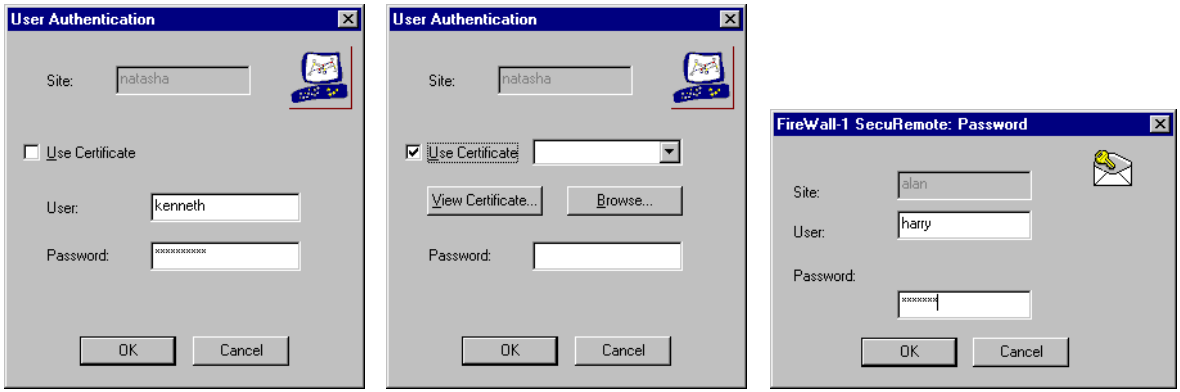



**FIGURE 9-13** SecuRemote Client User Authentication and Password windows

### Encryption Method

The encryption method used depends on the encryption methods supported by the SecuRemote Client and VPN/FireWall Module.

**TABLE 9-3** Encryption Method Supported by SecuRemote

| SecuRemote | version | supports ... |
|---|---|---|
| FireWall/VPN Module | 4.0 and higher | IKE, FWZ |
| | pre-4.0 | FWZ only |
| Client | 4.0 and higher | IKE, FWZ |
| | pre-4.0 | FWZ only |

TABLE 9-4 lists which encryption method is used for a given connection.

**TABLE 9-4** Encryption Method Used for a Given Connection by SecuRemote

| If the FireWall/VPN Module supports ... | then the encryption method used is ... |
|---|---|
| FWZ and IKE | ■ SecuRemote Client Version 4.0 and higher — the method specified in the SecuRemote Client's **Default Key Scheme** window (**Tools➤Key Scheme**)<br>■ SecuRemote Client pre-Version 4.0 — FWZ |
| FWZ only | FWZ |
| IKE only | IKE (SecuRemote Client Version 4.0 and higher) |

### Authentication Methods

There are several possible authentication methods:

#### FWZ

- FWZ — any of the authentication schemes supported on the VPN/FireWall Module: password, S/Key, RADIUS etc.

  In the **Password** window, the user enters his or her user name and the password, in accordance with the **Authentication Scheme** specified in the **Authentication** tab of the **User Properties** window.

  If the password is not entered, the user will be prompted for it.

  If the encryption method is FWZ, the authentication is encrypted using Diffie-Hellman keys.

#### IKE

- pre-shared secret

  The SecuRemote Client and VPN/FireWall Module authenticate each other by verifying that the other party knows the pre-shared secret, which is the user's password (as defined in the **Authentication** tab of the user's **IKE Properties** in window). The user enters his or her user name in **User** and the pre-shared secret in **Password**.

- certificates

  The user checks **Use Certificate**, enters an Entrust profile file name and a **Password** to access the certificate.

  The SecuRemote Client authenticates itself to the VPN/FireWall Module by using its certificate. The VPN/FireWall Module verifies the certificate against a certificate revocation list (CRL). The VPN/FireWall Module authenticates itself by sending the SecuRemote Client its certificate and a copy of a valid CRL signed by the Certificate Authority.

### Key Exchange

Once the user has been authenticated, the SecuRemote Client and SecuRemote Server exchange encryption keys, in preparation for encrypting the actual connection. The method of key exchange depends on the encryption scheme used: FWZ or IKE.

### Connection

After encryption keys have been exchanged, the connection begins. The connection is encrypted according to the encryption scheme used: FWZ or IPSec (for IKE).

## Routing Considerations

The default routing must ensure that reply packets (returning to the SecuRemote client) are routed through the same encrypting gateway through which the original packets were routed.

If this is not the case, then one way to force reply packets back through the gateway is to perform Address Translation on the gateway, hiding all outside addresses (those addresses not in the internal network) behind the gateway. The internal hosts will see the packet as having originated on the gateway, and will direct the reply packets to the gateway.

This solution is most suitable when a single gateway is dedicated to handling SecuRemote sessions.

**Warning –** The IP address of a gateway's external interface must never be hidden.

Another way of solving this problem is to use IP Pools (see "IP Pools" on page 249).

# Step by Step Example

## Configuring the Network

To implement SecuRemote, proceed as follows:

1. Configure and implement a VPN.
2. For each SecuRemote Server:
   - Check the **Exportable** checkbox in the **VPN** tab of its **Workstation Properties** window (FIGURE 8-4 on page 106).

     This indicates that the information about the SecuRemote Server (including its encryption domain) is to be made available to any SecuRemote Client that requests the information.
   - Specify the FWZ or IKE method in the **VPN** tab of the **Workstation Properties** window.

     See "Workstation Encryption Properties" on page 105 for information on these windows.
   - Specify the properties for each scheme in the **FWZ Properties** and **IKE Properties** windows.

     See "Workstation Encryption Properties" on page 105 for information on these windows.
   - For FWZ authentication, enable the authentication scheme in the **Authentication** tab of the **Workstation Properties** window (see FIGURE 4-10 on page 110 of *VPN-1/FireWall-1 Administration Guide*).
   - For IKE authentication, define the authentication parameters in the **Authentication** and **Encryption** tabs of the user's **IKE Properties** window (see FIGURE 8-5 on page 108).

## Defining Users

***3*** Define the users who will be using the SecuRemote Client. You can define users either with the Check Point GUI or with the VPN-1/FireWall-1 Account Management Client.

- For example, suppose Alice and Bob (whose user names are alice and bob respectively) will be SecuRemote users, then define a user group called SR_users and add them to the group.
- If you are defining the user with the Check Point GUI, then for certificate users, the user name must be the "commonname" (cn) in the certificate. Embedded spaces are significant.

  For example, if the user's DN is "cn=Barbara Jensen, o=University of Michigan, c=US", then the user name is "Barbara Jensen".
- For each user, specify the authentication method(s) and encryption properties.

See "Defining SecuRemote Users" on page 133 for information on defining SecuRemote users.

**Note –** For Client Encryption, the encryption properties are defined per user. In contrast, for Encryption, the encryption properties are defined per rule.

## Rule Base

***4*** If you wish to force SecuRemote users to always use SecuRemote when they connect to the enterprise network, then you must define a rule whose **Action** is **Client Encrypt**, for example:

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| SR_users@Any | localnet | telnet | Client Encrypt | Short Log | Gateways |

This rule indicates that when users sr_alice and sr_bob attempt a TELNET session with localnet, then the **Action** is **Client Encryption**.

- **Source** is the user group defined above.
- **Destination** is (an object) in the encryption domain of the rule's **Installed On** object.
- In the rule above, localnet is in SR_GW's encryption domain.

If you double-click on a Client Encryption rule's **Action**, the **User Encryption Action Properties** window (FIGURE 9-14) is displayed.

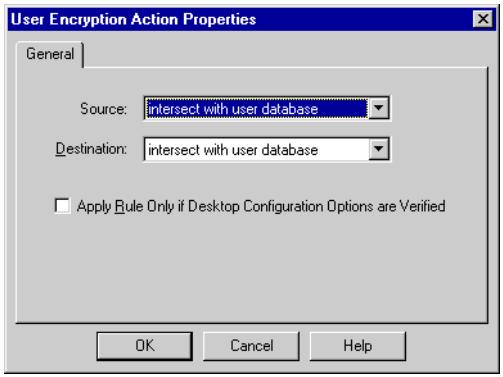



**FIGURE 9-14** User Encryption Action Properties window

In this window, the fields have the same meaning as in the **Rule Authentication Properties** window for a User Authentication rule.

**Source** — reconcile **Source** in the rule with **Allowed Sources** in the **User Properties** window.

The **Allowed Sources** field in the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access from the source address, while the rule may allow access. This field indicates how to resolve this conflict.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Source** specified in the rule.

**Destination** — reconcile **Destination** in the rule with **Allowed Destinations** in the **User Properties** window.

The **Allowed Destinations** field in the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access to the destination address, while the rule may allow access. This field indicates how to resolve this conflict.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.

- Choose **Ignore User Database** to allow access according to the **Destination** specified in the rule.

**Note** – Even if the selections under a rule's **Source** or **Destination** deny access, it is still possible that another rule allows access.

**Apply Rule Only if Desktop Configuration Options are Verified** — Apply this rule to a connection from a SecureClient (a SecuRemote Client configured with the Desktop Security option) only if the SecureClient passes all the verification criteria, including Desktop Policy.

Specifying **Client Encrypt** as the action means that only SecuRemote Clients can communicate under the rule, and that the authentication is handled automatically by the SecuRemote Client and Server transparently to the user. Client Encryption provides a higher level of security than User Authentication.

5. Install the Security Policy.
6. Install Check Point SecuRemote on each PC that will be using SecuRemote to communicate with the enterprise network.
7. Configure each SecuRemote PC (see Chapter 10, "SecuRemote Client" for information on how to do this).

## Destination

A Client Encryption rule applies to packets whose destination is in both:

- the object(s) appearing under **Destination** in the rule
- the encryption domain of the FireWall through which the connection is made (which is one of the FireWalls listed under **Install On** in the rule)

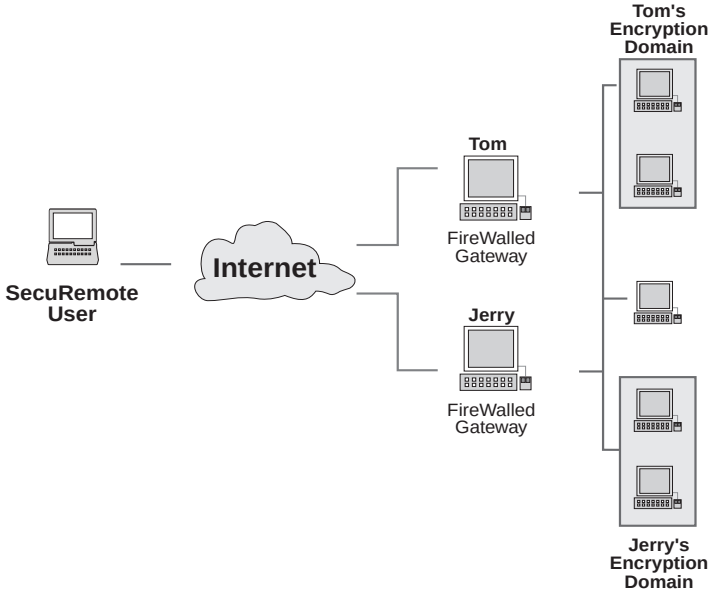



**FIGURE 9-15** Two FireWalls and Encryption Domains

Consider the following rule:

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| SR_users@Any | localnet | Any | Client Encrypt | Short Log | Tom, Jerry |

This rule applies to sessions with computers in Tom's encryption domain if the connection is through Tom, and to sessions with computers in Jerry's encryption domain if the connection is through Jerry. This is true even though the encryption domains are part of the same network. However, if the connection is through Tom to one of the computers in Jerry's encryption domain, then the rule does not apply. This means that the session will not be allowed unless there is another rule in the Rule Base that allows it.

# Other FireWalls

## Services

If there are other firewalls along the path connecting the SecuRemote Client (that performs the encryption) and the SecuRemote Server (the FireWall that performs the decryption), you should configure the other firewalls to allow FW-1 services to pass from the SecuRemote Client to the SecuRemote Server. You should allow the following services:

- FWZ
  - RDP (UDP on port 259)
- IKE
  - IPSEC and IKE (UDP on port 500)
  - IPSEC ESP (IP type 50)
  - IPSEC AH (IP type 51)

## Address Translation

When a SecuRemote Client's address is translated using NAT by a device other than the SecuRemote Server (for example, by another VPN/FireWall Module), there are some potential problems. HIDE mode cannot be used at all, because:

- FWZ — All SecuRemote Clients whose addresses are being hidden behind the same IP address will overwrite each other's keys on the SecuRemote Server.
- IKE — IPSec cannot use HIDE mode because there is no port information available for distinguishing between different translated hosts.

If STATIC mode is used, the SecuRemote Server must still be directed to map the illegal addresses it sees in the key exchange packets to the legal addresses it sees in the encrypted packets of the connection.

The SecuRemote Server will perform this mapping only if the appropriate property is set in `$FWDIR/conf/objects.C`, as follows:

```
:props (
    ...
    :userc_NAT (true)         for FWZ,  or
    :userc_IKE_NAT (true)     for IKE (ISAKMP)
    ...
)
```

To change these values, edit `$FWDIR/conf/objects.C` and confirm that the changes appear in both `$FWDIR/conf/objects.C` and `$FWDIR/database/objects.C`.

# Current Restrictions

Version 4.1 of Check Point SecuRemote imposes certain restrictions, which will be removed in future versions of VPN-1/FireWall-1.

## VPN Configuration

- If there is more than one VPN/FireWall Module along the path from a SecuRemote Client to its destination, then only one of the VPN/FireWall Modules can be a SecuRemote Server for the connection.
- Any overlapping encryption domains must conform to the restrictions given in "Overlapping Encryption Domains" on page 156.

Violations of these restrictions are reported by the SecuRemote Clients that encounter them.

## Properties Setup

Some services provided by a server inside an encryption domain must be specially configured for SecuRemote users in the **Services** tab of the **Properties Setup** window (FIGURE 7-2 on page 242 of *VPN-1/FireWall-1 Administration Guide*) as follows:

Enable the following options:

- **Enable FTP PORT Data Connections**
- **Enable FTP PASV Connections**

## RPC

If the server is inside an encryption domain, then the only way to allow a SecuRemote user to access an RPC service under a rule whose **Action** is **Client Encrypt** is to specify **Any** under **Services** in the rule. For example, the following rule will allow SecuRemote access to NFS services:

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| All_users@Any | NFS-Server | Any | Client Encrypt | Short Log | SR_GW |

This rule, on the other hand, will not allow SecuRemote access to NFS services, though all other users will be allowed access:

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| Any | NFS-Server | NFS-group | Client Encrypt | Short Log | SR_GW |

To allow access, either define a rule as shown above, or disable the SecuRemote Client.

This anomaly will be corrected in a future version of VPN-1/FireWall-1.

## Other Services

- The following services must be explicitly enabled under **Services** in the Client Encrypt rule.
  - RealAudio
  - VDOLive

- For the following services, the Client Encrypt rule must specify **Any** (or **tcp-high-ports** or **udp-high-ports**, as appropriate) under **Services**:

  - SQLNet
  - H323
  - NetShow
  - RTSP
  - FreeTel
  - BackWeb
  - DCE-RPC

# Known Restrictions

## Timeout

The first time the user connects to a site, it may happen that the delay introduced by entering a user name and password may cause the application (for example, TELNET) to timeout. In this case, the user should simply restart the application.

## Data Not Encrypted

The following data are not encrypted:

- The connection between the PC and a SecuRemote Server in which a key is exchanged (FWZ).

  However, the information is signed and the password and the session key are encrypted.
- DNS information (but see "DNS" on page 153 for information on how to encrypt DNS)
- In FTP, RealAudio, and VDOLive connections, some packets are not encrypted.

  These packets contain the information needed to open a back connection from the SecuRemote Server to the PC.
- Local connections are not encrypted.

  A connection is "local" if both the IP Address of the PC (Client) and the IP Address of the destination (server) are both inside the same Encryption Domain of the same SecuRemote Server.

## TCP Stacks

The following TCP/IP stacks are supported:

- MS TCP (Microsoft)

## VPN/FireWall-1 User Password

If the authentication scheme is VPN/FireWall-1 Password, the user password is limited to 8 characters.

### VPN-1/FireWall-1 Adapters (Windows 9x)

Only one FW-1 Adapter can be added or removed in one session of the Control Panel Network applet (Windows 9x only).

# Advanced Configurations

## FWZ Encapsulation

This section describes encapsulation between a SecuRemote Client and a FireWall-1 SecuRemote Server when FWZ encryption is used.

**Note –** In the IKE (IPsec) encryption scheme, packets are always encapsulated.

### How FWZ Encapsulation Works

The figure below shows a SecuRemote user (Alice) connecting to a host inside London's encryption domain.

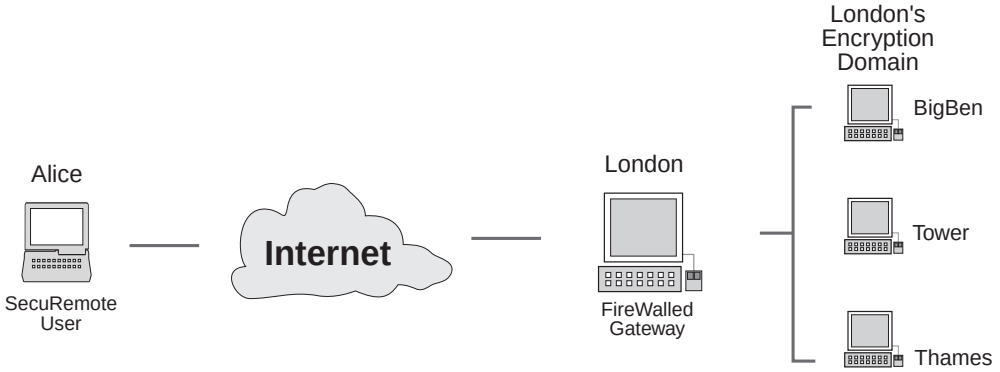



**FIGURE 9-16** SecuRemote user connecting to a host inside a site's encryption domain

The connection begins when, for example, the user at Alice types:

```
telnet Thames
```

or:

```
telnet IPaddress
```

This initiates a key exchange with London (the gateway), after which the first TELNET packet is sent to Thames.

However, if Thames is not reachable from Alice (perhaps because Thames has an invalid IP address[1]) then it is still possible for Alice to conduct a SecuRemote session with Thames using encapsulation.

Suppose Alice attempts to initiate a TELNET session with Thames.

1. Although Alice does not know how to contact Thames, Alice does know that Thames is in London's encryption domain, so Alice initiates a key exchange session with London.

   If necessary, Alice first asks the user to authenticate himself or herself in the usual way.

2. If **Encapsulate SecuRemote connections** (in the **Encapsulation** tab of London's **FWZ Properties** window — see FIGURE 8-15 on page 116) is checked, London instructs Alice to encapsulate all packets it sends to hosts in London's encryption domain.

3. Alice encapsulates the initial TELNET packet inside another packet (with destination IP address London) and sends the encapsulated packet to London.

   The encapsulation consists of replacing the IP address and appending the original IP address at the end of the packet, increasing its length by 5 bytes (the appended IP address is not in cleartext).

4. London extracts the original packet from the encapsulated packet and sends it to Thames.

5. Thames sends a reply packet (with source IP address of Thames and destination IP address of Alice).

6. London intercepts the reply packet, encapsulates it inside another packet (with source IP address London and destination IP address Alice), and sends it on.

7. Alice receives the encapsulated reply packet and extracts the original reply packet.

The communication continues in this way, with Alice and London encapsulating and de-encapsulating packets. As they pass through the Internet, these packets appear to be part of a communication between Alice and London, but the communication is actually between Alice and Thames.

**Note** – Encapsulation is supported by VPN-1/FireWall-1 Version 3.0a and higher, and by SecuRemote Version 3.0 and higher.

1. If the problem is an invalid IP address, then another solution might be FireWall-1's Network Address Translation feature. See Chapter 14, "Network Address Translation," of *FireWall Administration Guide* for more information.

## Implementing Encapsulation

To implement encapsulation, check the **Encapsulate SecuRemote connections** in the **Encapsulation** tab of the encapsulating gateway's **FWZ Encryption Properties** window.

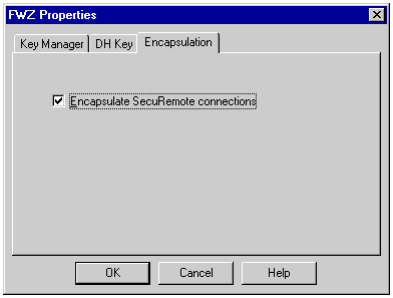



**FIGURE 9-17** FWZ Encryption Properties — Encapsulation tab

TABLE 9-5 lists what happens for various combinations of the **Encapsulate SecuRemote connections** option and the SecuRemote version.

**TABLE 9-5** Combinations of the Encapsulate SecuRemote connections Option and the SecuRemote Version

| Encapsulate SecuRemote connections | SecuRemote Version 3.0 and higher | SecuRemote Version pre-Version 3.0 |
|---|---|---|
| checked | The communication will be encapsulated. | The key exchange session will time out on the SecuRemote client, and there will be an error indication on the gateway. |
| not checked | The communication will not be encapsulated, and if the host is unreachable, connections will time out. | The communication will not be encapsulated, and if the host is unreachable, connections will time out. |

## DNS

The scenario under which encapsulation takes place leaves the following question unanswered: if the destination machine has an unregistered IP address, who resolves its name?

The best solution is to configure the SecuRemote Client's primary DNS as an internal DNS server that can resolve internal names with unregistered (for example, RFC 1918-style) IP addresses. It's best to encrypt the DNS resolution of these internal names, but you will probably not want all DNS traffic to be encrypted, because this would mean that every DNS resolution would require authentication.

**Note –** This scenario can also arise when a SecuRemote user accesses a server whose name is not defined in the enterprise DNS service.

To solve this problem, proceed as follows:

1. Modify the `$FWDIR/conf/dnsinfo.C` file on the Management Station to redirect DNS by providing the following information.
   - the internal DNS server's IP address
   - the domain for which it resolves names
   - the maximum number of labels to resolve (for example, 3 for `xxx.hello.com`)

     Suppose the SecuRemote Client's domain is `.hello.com` and it fails to resolve `yyy.goodbye.com`. By default, Windows will then try to resolve `yyy.goodbye.com.hello.com`, and you will probably not want this query to be encrypted.
   - the network addresses for which it resolves (for reverse DNS)
2. In `$FWDIR/conf/dnsinfo.C`, set `:encrypt_dns (true)` under `:dnsinfo`.
3. Instruct the gateway to encrypt DNS by changing the definition of `USERC_DECRYPT_SRC` in `crypt.def`.
4. Reinstall the Security Policy on the gateway so that these changes take effect.
5. On the SecuRemote Client, set `:dns_encrypt (true)` under `:options` in `database\userc.C`.

**Note –** `:dns_encrypt (true)` is the default in VPN-1/FireWall-1 Version 4.1 and higher.

### Example

`$FWDIR/conf/dnsinfo.C` file on the Management Station

```
:dns_servers (
(
    : (bigben.london
            :obj (
                    : (192.204.75.192)
            )
            :topology (
                    : (
                            :ipaddr (192.204.75.0)
                            :ipmask (255.255.255.0)
                    )
            )
            :domain (
                    : (
                            :dns_label_count (3)
                            :domain (.hello.com)
                    )
            )
    )
)
:encrypt_dns (true)
)
```

`$FWDIR/lib/crypt.def` file on the Management Station

```
#define ENCDNS
define USERC_DECRYPT_SRC {
    (
#ifndef ENCDNS
           not(dport = SERV_domain, (udp or tcp)),
#endif
           not(dport = FWD_SVC_PORT, tcp),
        not(dport = FWM_SVC_PORT, tcp),
           not(dport = ISAKMPD_DPORT, sport = ISAKMPD_SPORT, udp)
    )
};
```

`$FWDIR\database\userc.C` on the SecuRemote Client

```
(
    :options (
                    :dns_xlate (true)
                    :dns_encrypt (true)
    )
)
```

## Overlapping Encryption Domains

Beginning with VPN-1/FireWall-1 Version 4.1, overlapping encryption domains within a single site are supported, subject to the restrictions described below.

### Full Overlap

In FIGURE 9-18, the encryption domains of Gateway A and Gateway B fully overlap, in other words, they are identical.

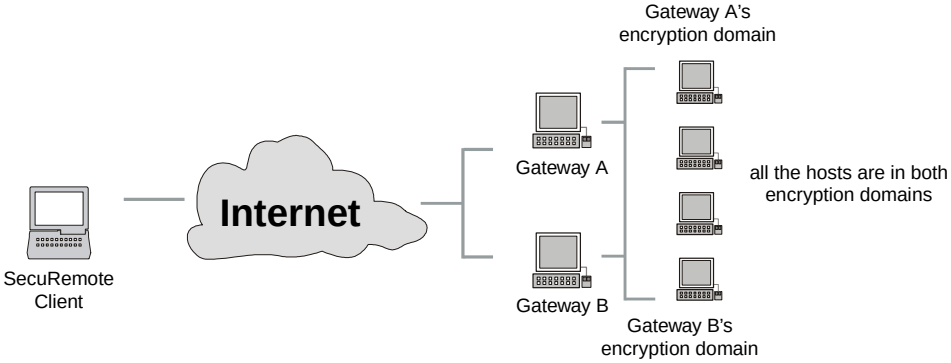



**FIGURE 9-18** Fully Overlapping Encryption Domains

VPN-1/FireWall-1 supports fully overlapping encryption domains.

**Note –** A gateway's encryption domain consists of the network object defined in the **VPN** tab of the gateway's **Workstation Properties** window and also the gateway itself. To implement fully overlapping encryption domains (as in FIGURE 9-18), define a group that includes both gateways *and* all the networks they protect. Then specify that group as the encryption domain for both gateways.

When the SecuRemote Client attempts to establish an encrypted connection with one of the hosts in the encryption domain, it tries to connect to both gateways using the RDP protocol. The encrypted connection is established through the first gateway that replies to the SecuRemote Client, as are all connections initiated to the encryption domain for a specified period of time (currently one minute). This period of time is not currently configurable.

### Reply Packets and Back Connections

A potential problem is asymmetric routing for reply packets and back connections. Suppose a SecuRemote Client connects to a host through Gateway A, but the host's reply packet is routed through Gateway B, which does not encrypt the packet.

There are two solutions to this problem:

1. Use Network Address Translation to hide all connections passing through Gateway A behind Gateway A.

   On the host, the hiding address (the address behind which the SecuRemote Client is hidden) must be routable to Gateway A.

   For information on Network Address Translation, see Chapter 14, "Network Address Translation" of *VPN-1/FireWall-1 Administration Guide*.

2. Use IP Pools.

   For information on IP Pools, see "IP Pools" on page 249.

   On the host, the IP Pool addresses must be routable to Gateway A.

### FWZ Encryption

In FWZ encryption, the key exchange takes place between the SecuRemote Client and the gateway, but the encrypted session takes place between the SecuRemote Client and the host. Suppose the SecuRemote Client negotiates a key exchange with Gateway A, but when the encrypted session begins, the packets are routed to the host through Gateway B. Gateway B has no knowledge of the encryption parameters, and the connection will fail.

The solution to this problem is to use FWZ encapsulation. For information about FWZ encapsulation, see "FWZ Encapsulation" on page 151.

## Partial Overlap

In FIGURE 9-19 on page 158, there is a partial overlap between the encryption domains of Gateway A and Gateway B: there is one host that is in both encryption domains, but the other hosts are not in both encryption domains.

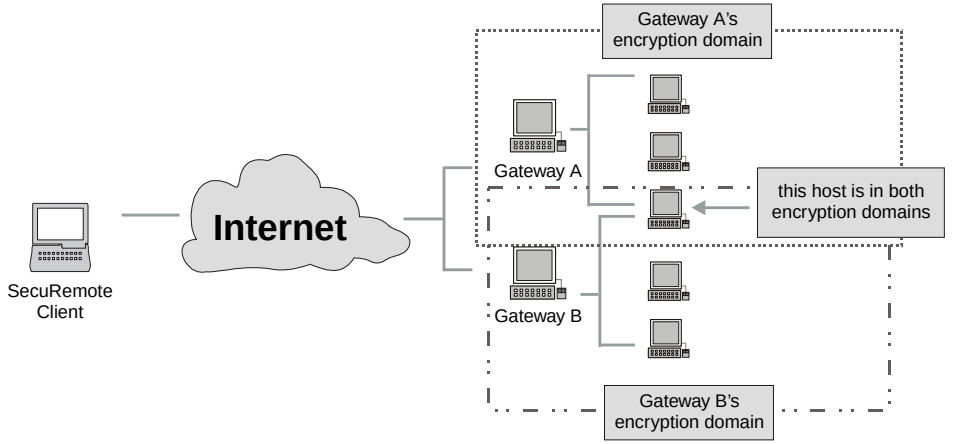



**FIGURE 9-19** Partially Overlapping Encryption Domains

VPN-1/FireWall-1 does **not** support partially overlapping encryption domains.

## Proper Subset

In FIGURE 9-20 on page 158, Gateway B's encryption domain is a proper subset of Gateway A's encryption domain, that is, Gateway B's encryption domain is fully contained in Gateway A's encryption domain.

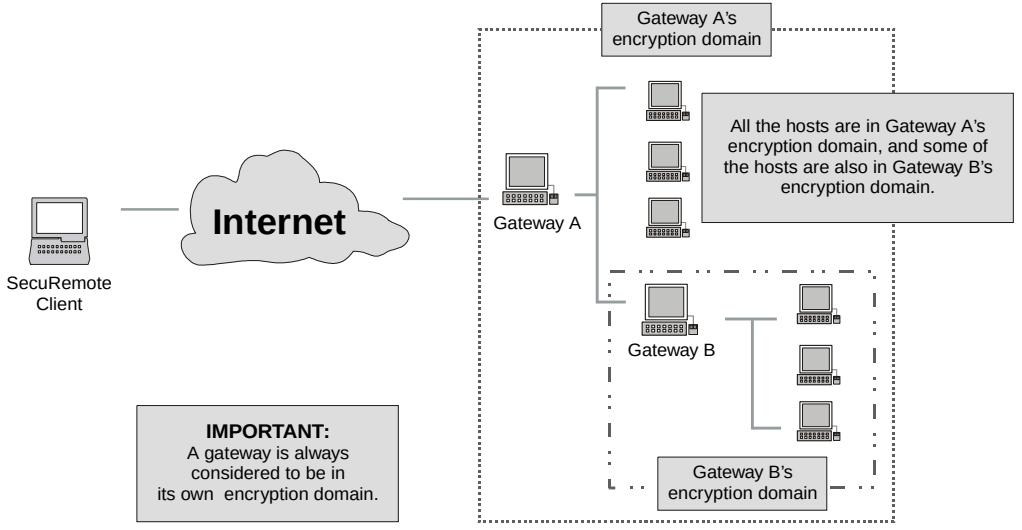



**FIGURE 9-20** "Proper Subset" Overlapping Encryption Domains (2 levels)

VPN-1/FireWall-1 supports overlapping encryption domains of this type. The SecuRemote Client encrypts with the gateway closest to the host (the "innermost" gateway). In the configuration shown in FIGURE 9-20, the SecuRemote Client would encrypt with Gateway B for hosts in Gateway B's encryption domain and with Gateway A for all other hosts.

When the SecuRemote Client encrypts with the inner gateway (Gateway B), the Rule Base must allow the connection through the outer gateway (Gateway A), as listed in TABLE 9-6.

**TABLE 9-6** Services that must be allowed through outer gateway

| | **services to allow in outer gateway (key negotiation)** | **services to allow in outer gateway (encrypted traffic)** |
|---|---|---|
| IKE | IKE | ESP or AH, as needed |
| FWZ | RDP | a rule that allows the encrypted service (FTP, HTTP *etc*.) |
| FWZ (encapsulated) | RDP | FW1_Encapsulation and RDP |

The rules can specify the inner gateway as the **Source** and **Destination**.

In FIGURE 9-21, three encryption domains are nested inside each other.

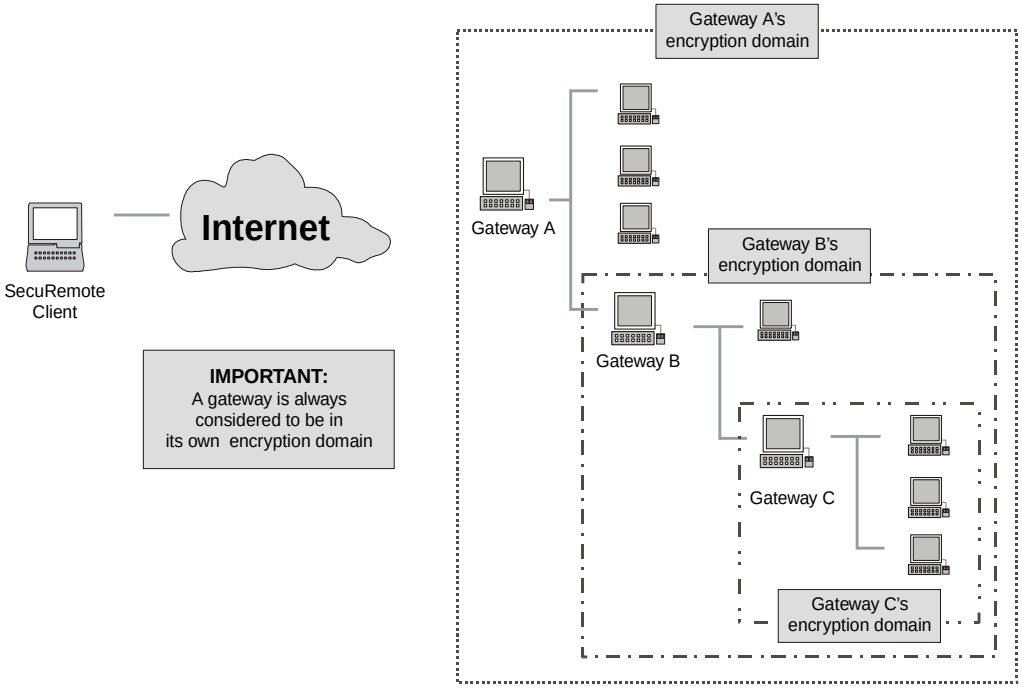



**FIGURE 9-21** "Proper Subset" Overlapping Encryption Domains (3 levels)

This configuration is an extension of the configuration shown in FIGURE 9-20 on page 158, and the same considerations are in effect. The SecuRemote Client encrypts as follows:

**TABLE 9-7** Hosts and Their Encrypting Gateways

| for ... | ... the SecuRemote Client encrypts with ... |
|---|---|
| hosts in Gateway C's encryption domain | Gateway C |
| hosts *only* in Gateway B's encryption domain (and not in any other encryption domain) | Gateway B |
| all other hosts | Gateway A |

When the SecuRemote Client encrypts with the one of the inner gateways (Gateway B or Gateway C), the Rule Base must allow the connection through the outer gateways (Gateway A and Gateway B) as described in TABLE 9-6 on page 159.

## Backup Gateways

### No Overlapping Encryption Domains

FIGURE 9-22 shows two geographically separated internal networks (each of which is connected to the Internet through its own gateway) that are connected to each other via a dedicated link. The encryption domains of Gateway A and Gateway B do not overlap, but Gateway B is defined as a backup for Gateway A (in the **VPN** tab of Gateway A's **Workstation Properties** window).

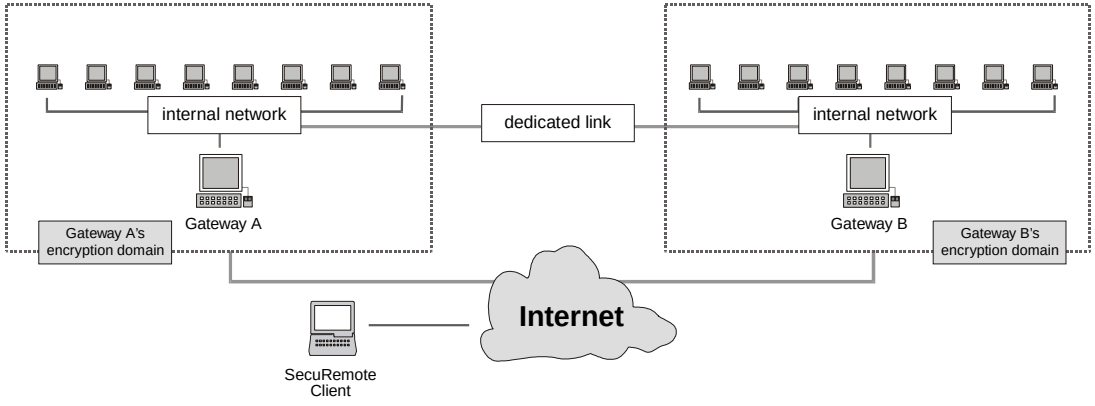



**FIGURE 9-22** Backup Gateways with No Overlapping Encryption Domains

When the SecuRemote Client attempts to establish an encrypted connection with one of the hosts in Gateway A's encryption domain, it will first attempt to connect through Gateway A. If Gateway A is unavailable, the SecuRemote Client will then attempt to connect through Gateway B.

**Note –** VPN-1/FireWall-1 does not support configurations in which the encryption domains partially overlap (see "Partial Overlap" on page 157).
This configuration is subject to the problems described under "Reply Packets and Back Connections" and "FWZ Encryption" on page 157.

## Fully Overlapping Encryption Domains

Like FIGURE 9-22 on page 160, FIGURE 9-23 shows two geographically separated internal networks that are connected to each other via a dedicated link, but in FIGURE 9-23, two gateways (Gateway A and Gateway B) protect the leftmost internal network. The encryption domains of Gateway A and Gateway B are identical (that is, they fully overlap), and Gateway C is defined as a backup for Gateway A and Gateway B.

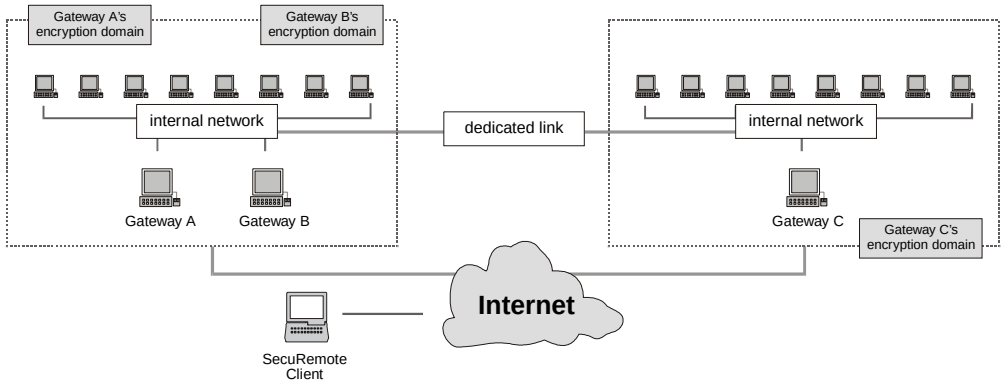



**FIGURE 9-23** Backup Gateways with Fully Overlapping Encryption Domains

The left side of the diagram (Gateway A, Gateway B and the network they protect) is similar to the configuration depicted in FIGURE 9-18 on page 156. FIGURE 9-23 adds a backup gateway (Gateway C) to that configuration.

When the SecuRemote Client attempts to establish an encrypted connection with one of the hosts in the encryption domain, it tries to connect to all the gateways (including Gateway C) using the RDP protocol. The encrypted connection is established through the first gateway that replies to the SecuRemote Client, as are all connections initiated to the encryption domain for a specified period of time (currently one minute). This period of time is not currently configurable.

**Note –** VPN-1/FireWall-1 does not support configurations in which the encryption domains partially overlap (see "Partial Overlap" on page 157).
This configuration is subject to the problems described under "Reply Packets and Back Connections" and "FWZ Encryption" on page 157.

# Secure Domain Logon

## Overview

The Secure Domain Logon feature enables Windows NT/9x SecuRemote Clients to securely logon to a domain controller, protected by VPN-1/FireWall-1, using both LAN and dial-up connections. If the feature is enabled, SecuRemote is activated before the domain controller authenticates a domain logon. The next time you restart your computer and attempt to login to a domain controller, a **SecuRemote Client User Authentication** window (FIGURE 9-13 on page 141) will be displayed after you have entered the operating system credentials. Therefore, the exchange of user's credentials (user name and password) and user profile between the workstation and domain controller respectively is encrypted.

If the Single SignOn option is enabled, the encrypted user name and password are automatically retrieved from the Windows registry and the **User Authentication** window is not displayed.

For more information on Single SignOn, see "Single SignOn" on page 205.

## Windows NT

### Enabling and Disabling Secure Domain Logon

The Secure Domain Logon can be enabled only if the machine is configured as part of a domain.

To enable the Secure Domain Logon:

1. Select **Enable SDL** from the **Passwords** menu.
2. Reboot the computer.

**Warning –** Do not change the machine domain configuration when the Secure Domain Logon is enabled!

To disable the Secure Domain Logon, select **Disable SDL** from the **Passwords** menu.

### Name Resolution

To find and connect to an NT domain controller protected by VPN-1/FireWall-1 or/and residing on a different LAN, a SecuRemote Client maps the name of the NT domain controller to the corresponding IP address using one of the two name resolution services: LMHOSTS or WINS (Windows Internet Name Service).

LMHOSTS

The LMHOSTS name resolution service is applicable both for LAN and dial-up configurations.

To use the LMHOSTS file for name resolution, put the file dnsinfo.C under the directory $FWDIR/conf.

Syntax

```
(
      :LMData(
             :(
                    :ipaddr (<IP address>)
                    :name (<host name>)
                    :domain (<domain name>)
             )
             :(
                    :ipaddr (<IP address>)
                    :name (<host name>)
                    :domain (<domain name>)
             )
      )
)
```

When a SecuRemote client updates the topology, the name resolution data will be automatically transferred to the dnsinfo entry of the SecuRemote client's userc.C file and then to the LMHOSTS file.

WINS

The WINS name resolution service is applicable for dial-up configurations only.

To use the WINS name resolution:

1. Specify the primary and, optionally, the secondary WINS servers protected by VPN-1/FireWall-1.
2. Reboot the computer.

## Configuring SDL Timeout

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.C. The default timeout is 45 sec.

**Note** – This feature is not applicable if the Single SignOn option is enabled.

### Using Cached Information

When a SecuRemote Client succesfully logs on to a domain controller, the user's profile is saved in cache. If the SecuRemote Client fails to log on to the domain controller at any subsequent attempt, the cached information will be used.

To configure this option:

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 the LMHOSTS or WINS name resolution service to resolve the name of the domain controller.
2. Configure SDL timeout.
3. Define the site where the domain controller resides and download/update the topology.
4. Configure the machine as a domain member.
5. Enable Single SignOn (optional).
6. Enable the Secure Domain Logon.
7. Reboot the computer.

### Using Secure Domain Logon

After you have rebooted the computer:

1. When the Windows NT **Logon** window is displayed, enter the operating system credentials.

   The SecuRemote **Logon** window is displayed.
2. Enter the SecuRemote credentials in the defined time (see "Configuring SDL Timeout" on page 163).

If you fail to logon and no cached information is used, wait one minute and try again.

## Windows 9x

### Enabling and Disabling Secure Domain Logon

To enable the Secure Domain Logon, select **Enable SDL** from the **Passwords** menu.

To disable the Secure Domain Logon, select **Disable SDL** from the **Passwords** menu.

### Name Resolution

See “Name Resolution” on page 162.

### Configuring Secure Domain Logon

1. Configure the SecuRemote Client to use the LMHOSTS name resolution service to resolve the name of the domain controller.
2. Define the site where the domain controller resides and download/update the topology.
3. Configure the machine as a domain member.
4. Reboot and logon.

### Using Secure Domain Logon

After you have rebooted the computer, proceed as follows:

1. When the Windows **Logon** window is displayed, enter the operating system’s credentials.

   The SecuRemote **Logon** window is displayed.

If you fail to logon, an informative message is displayed. Click on **Cancel** and try again. Reboot the computer before any subsequent domain logon attempt.

## Automatic Topology Update

The system administrator can configure SecuRemote Clients to automatically update a site’s topology either when starting SecuRemote or just before the key exchange. To enable this feature, set the appropriate properties in `$FWDIR/conf/objects.C` as follows:

```
:props (
...
:desktop_update_at_start (true)
:desktop_update_frequency (n)
...
)
```

In addition, the following parameters in the `options` section of the `objects.C` file on the SecuRemote Client affect the automatic topology update feature:

| property | description |
|---|---|
| `desktop_update_at_start` | If true, the user will be prompted to update this site's topology when the SecuRemote Client starts. The user can choose not to update the topology; this is useful when the user is not connected to the network when the SecuRemote Client starts. If the user chooses not to update the topology at startup, the topology will be automatically updated before the next key exchange with the site (see the next parameter). |
| `desktop_update_frequency` | The site's topology will be updated before the next key exchange if `n` seconds have passed since the last time the topology was updated. The user will not be prompted before the update. |
| `partial_topo` | If true, the site's topology will be automatically downloaded the first time the SecuRemote Client connects to the site, regardless of the values of any other parameters. This parameter is useful when SecuRemote users download their SecuRemote installations from a publicly accessible site and enables the system administrator to include minimal site topology information (only the site's IP address) in the downloadable `userc.C` file. The first time the user connects to the site, the site's topology is downloaded automatically (after the user is authenticated). |

In addition, the following parameters in the options section of the `userc.C` file on the SecuRemote Client affect the automatic topology update feature:

```
:options (
...
:update_topo_at_start (true)
:partial_topo (true)
...
)
```

| property | description |
|---|---|
| update_topo_at_start | If true, the user will be prompted to update the topologies of all defined sites when the SecuRemote Client starts. |
| partial_topo | If true, the site's topology will be automatically downloaded the first time the SecuRemote Client connects to the site, regardless of the values of any other parameters. This parameter is deleted from the userc.C file after the topology download (see the explanation of this parameter in the objects.C file above). |

## Automatic Version Update

The system administrator can configure SecuRemote Clients to automatically check the availability of a newer version of SecuRemote Client software before connecting to a site. To enable this feature, set the appropriate properties in objects.C as follows:

```
:props (
:...
:desktop_build_number ( version_number)
:desktop_sw_url_path (" URL")
:...
)
```

| property | description |
|---|---|
| desktop_build_number | If the SecuRemote Client version number is less than version_number, the user will be prompted to obtain the SecuRemote Client Version version_number from the specified URL (see next parameter). |
| desktop_sw_url_path | The URL from which the user can obtain the correct version of the SecuRemote Client. The URL is displayed in the prompt and the user can connect to the URL to obtain the correct SecuRemote Client version. |

Example

```
:props (
:...
:desktop_build_number (4.1)
:desktop_sw_url_path ("http://www.bigcorp.com")
:...
)
```

## Authentication by IP Address

VPN-1/FireWall-1 can “remember” a user either by user name only (the default), or by a combination of user name and IP address. The combination of user name and IP address has the advantage that when a user connects from an IP address that is different from the one he or she connected from the last time, the user will be re-authenticated.

**Note –** The same user can connect simultaneously from more than one IP address. This feature only requires the user to re-authenticate in this case.

To implement this feature (user name-IP address combination), proceed as follows:

1. Stop VPN-1/FireWall-1.
   - On Windows, NT stop the FW-1 service.
   - On Unix run `fwstop`.
2. In the file `$FWDIR/conf/objects.C`, add the line:

```
        :userc_bind_user_to_IP (true)
```

   after the line:

```
:props (
```

3. Start VPN-1/FireWall-1.
   - On Windows NT, restart the FW-1 service.
   - On Unix, run `fwstart`.
   - Reinstall the Security Policy.

## Partial Topology

SecuRemote Clients can be pre-configured with a partial site topology to reduce exposure of sensitive network information. The first time the SecuRemote Client connects to a site, the user will be given the opportunity to download the complete topology over the secure connection (if authentication is required for topology download).

To enable this feature, configure the `userc.c` file (see “userc.c File” on page 170) in the installation package as follows:

```
(
    :gws ()
    :managers (
           : (Site-name
                  :partial_topo (true)
                  :obj (
                         :type (node)
                         : (n.n.n.n)
                  )
           )
    )
)
```

`n.n.n.n` is the accessible IP address of the Management Station from which the full topology can be downloaded.

## Thin Client

A smaller SecuRemote Client installation file set (with limited certificate functionality) is available. A Thin Client cannot import PKCS #12 certificates or use the Offline Certificate Utility, but it can use the Entrust PKI and other PKI’s if the end user is provided by the administrator with a certificate in `EPF` format.

To configure a Thin Client installation package, proceed as follows:

1. Unzip the installation package (if it is zipped).
2. Delete the following files:
   - `r_certut.exe`
   - `r_entpm.dll`
3. Edit the `product.ini` file and set “`IncludeEntrustCertUtil=0`”.

## Certificate Revocation List Validity

**CRL validity** — A SecuRemote Client and a site must have their date, time of day and (on NT) daylight savings time policy synchronized to avoid a situation where a Certificate Revocation List (CRL) has expired on one but not on the other. A default grace period of 15 minutes is defined, during which a CRL can be used both before and after its period of validity. Two properties in `objects.C` are relevant:

- `crl_start_grace` — the number of seconds before the CRL’s validity period during which the CRL will be regarded as valid
- `crl_end_grace` — the number of seconds after the CRL’s validity period during which the CRL will be regarded as valid

These properties should be added to `objects.C` near the `crlcache_timeout` property. The VPN/FireWall Module must be stopped (`fwstop`) and restarted (`fwstart`) for the settings to take effect. The settings take effect on the SecuRemote Client after the next topology download.

# userc.c File

## userc.c parameters

The `userc.c` file (located on the SecuRemote Client) contains information about the SecuRemote configuration, including site topology. The parameters listed in TABLE 9-8 are defined in the `options` section.

**Warning –** The SecuRemote Client performs minimal syntax checking for the `userc.c` file. If a parameter is entered incorrectly, the site to which it belongs is deleted. No error messages are displayed.

**TABLE 9-8** userc.c parameters

| parameter (default value in parentheses) | meaning |
|---|---|
| `keep_alive (false)` | Specifies whether the VPN/FireWall Modules will maintain session key information for the Client. |
| `keep_alive_interval (`*n*`)` | When `keep_alive` is true, the Client will ping the VPN/FireWall Module every *n* seconds. `keep_alive_interval` is relevant for IKE only. For FWZ, the Client will ping every 800 seconds if `keep_alive` is `true`. |
| `dns_xlate (true)` | Enable split DNS feature (see “DNS” on page 153) — server must be configured appropriately. |
| `dns_encrypt(true)` | Enable DNS encryption — server must be configured appropriately. |
| `fwm_encrypt (false)` | Enable SecuRemote encryption for GUI Client-Server communication — server must be configured appropriately. |
| `gettopo_port (264)` | Specifies the port for topology download. If unsuccessful after 30 seconds, the Client will try again on port 256. |
| `encrypt_db (false)` | Obscure topology information in local database. |

**TABLE 9-8** userc.c parameters (continued)

| parameter (default value in parentheses) | meaning |
|---|---|
| **Note –** The following parameters apply to overlapping encryption domains and MEP (see "Multiple Entry Point (MEP) Example Configuration" on page 244). | |
| `active_resolver(true)` | If `true`, the SecuRemote Client will automatically initiate an RDP status query with a gateway to check if it is still alive.<br>If `false`, the SecuRemote Client will postpone sending the query until that information is actually needed (in which case the user may experience some delay). |
| `resolver_session_interval(60)` | The interval (in seconds) between RDP status queries. |
| `resolver_ttl(10)` | The number of seconds the SecuRemote Client will wait for a reply on an RDP status query before concluding that the gateway is unavailable. |

# Troubleshooting SecuRemote

## Installation

You may receive the following message when you install the SecuRemote Client:

```
Setup program has found that a previous installation was removed
without rebooting the computer. Please reboot your computer before
re-installation.
```

This usually means that you uninstalled SecuRemote and then re-installed it before first rebooting you machine. Reboot and try again to re-install. If the problem persists, then delete the file `sruninst.exe` from your Windows directory and re-install.

## Routing

It may happen that your first attempt to use the SecuRemote Client will expose preexisting routing problems of which your system administrator was previously unaware if this is the first time someone is accessing the server from outside the local network. In this event, you can trace the routing by using `tracert` from the PC. Your system administrator can provide you with instructions on how to use `tracert`.

## No SecuRemote Server Along Route

If there is no SecuRemote Server along the route between the PC and the host with which it is communicating, then communication is not possible (there is no one to decrypt what SecuRemote is encrypting). This can happen, for example, when a

portable computer is moved from home to office and the computer's IP address at the office is not in the same Encryption Domain as the destination. (If it is in the same Encryption Domain, then no encryption will take place.)

In this case, the only solution is to disable SecuRemote (and thus communicate without encryption), either by killing the SecuRemote Client or by removing the VPN-1/FireWall-1 adapter from the interface. For example, if the VPN-1/FireWall-1 adapter is installed on the dial-up interface but not on the Ethernet interface, then SecuRemote will encrypt when the user is working at home but not encrypt when the user is working at the office. See also "Data Not Encrypted" on page 150.

## Password Dialog Box

If something goes wrong, you will need to determine whether the problem is on the SecuRemote Client side (on the PC) or on the SecuRemote Server side. In general, if the SecuRemote Client displays the password dialog box, then it is functioning correctly and whatever problems you are experiencing are on the SecuRemote Server side of the connection.

If you don't see the password dialog box, then one of the following is probably true:

- The SecuRemote software was not correctly installed on the PC.
- The site with which you are trying to communicate was not defined on the PC.
- The information received from the Management Station when the site was defined is incorrect.

  This can happen if the site information on the PC is old and it should be updated, or if the SecuRemote Server's encryption domain is not properly defined.

You can verify the information on the PC by browsing through the file `userc.c` in the `database` directory under the directory on which you installed SecuRemote.The default path is `C:\Program Files\CheckPoint\SecuRemote\database\userc.c`.

In this file there should be several fields of the form:

```
(
   gws(
    :topology (
       : (
         ....
         :ipaddr ( xxx.xxx.xxx.xxx)
         :ipmask ( yyy.yyy.yyy.yyy)
    ...
   )
   ...
)
```

One of these `ipaddr-ipmask` pairs should match your destination. If none does, then proceed as follows:

1. Exit any editor that you may have opened on `userc.c`.
2. Update the site with which you want to encrypt.
3. Check the `userc.c` file again.

If the problem has not been solved, contact your system administrator for assistance.

You can make a backup copy of `userc.c` when experimenting, but there is no point in manually editing it since SecuRemote updates it automatically.

## Service Cannot be Accessed

If you cannot access a service, disable SecuRemote (choose **Kill** from the **File** menu) and try again.

**If you cannot access the service even when not using SecuRemote** — It is the Security Policy that is denying you access, and you should contact your system administrator for assistance.

**If you can access the service when not using SecuRemote** — There is a problem with the way SecuRemote is configured on your PC.

## Data Not Encrypted

If data is being transmitted in the clear (that is, data is not being encrypted) and no authentication is taking place (that is, you don't see the **User Authentication** or **Password** windows), then examine the following possibilities:

- SecuRemote is not properly installed (Windows 9x).

  **Course of Action** — Open the **Network** dialog box and verify that **FW1 Adapter/Protocol** is between the TCP/IP and the adapter through which you expect the data to pass. For example, if you have both Dial-up and Ethernet adapters, and FW1 is bound to the Dial-up adapter, then stop the Ethernet adapter.

  Make sure that the SecuRemote Daemon is running after the PC completes its boot.

- The SecuRemote Client on the PC does not know that it must encrypt the data.

  **Course of Action** — Encryption takes place only if the destination is in the FireWall's encryption domain (which must be exportable to the PC using the **Update** or **Make New Site** operations), and the source is not in the FireWall's encryption domain.

- The information received by the SecuRemote about which IP address should be used with encryption may be incorrect.

You can verify this information by examining the file `userc.c` in the `database` directory under the directory on which you installed SecuRemote. The default path is given in TABLE 9-9.

**TABLE 9-9** Default path for `userc.c`

| OS | default path for userc.c |
|---|---|
| Windows 95 | `C:\Program Files\CheckPoint\SecuRemote\database\userc.c` |
| Windows NT | `WINDIR\fw\database\userc.c` |

This file contains a set whose first entry should be of the form:

```
(
    gws (
        .....
    )
    ....
)
```

Make sure that the IP Address with which you want to encrypt is within the `topology` attribute of the `gws` set (one of these `ipaddr-ipmask` pairs should match your destination).

If this is not so, for example if the `gws` set is empty (that is, `gws ()`), then proceed as follows:

1. Exit any editor that you may have opened on `userc.c`.
2. Update the site.
3. Check the `userc.c` file again.

   If the file is still empty, then the gateway's encryption domain is probably not exportable.

- The FireWall instructed the SecuRemote to send the data in the clear.

  **Course of Action —** In the Log Viewer, you should see an entry with an envelope in which the user name and the key-id appear.

  If this is not the case, then the SecuRemote user was defined to work in the clear.

  Open the user's **User Properties** window and click on **Encryption**. Verify that the data encryption method is correct. If this is not the problem, proceed to the next item in this procedure.

  Open the **Workstation Properties** window of the FireWall that should be doing the decryption.

Verify that:

- **Encryption Domain** is valid
- **Exportable** is checked

In the SecuRemote user's **User Properties** window, verify that:

- The user's name is identical to the user name as specified in the **Password** window on the SecuRemote Client.
- **Data Encryption Method** is not set to **Clear**.

### Long Connections

When using FWZ encryption with MD5, connections (especially long ones, for example FTP downloads) may hang. To resolve this problem, edit `objects.C` as follows:

1. Stop the VPN/FireWall Module (`fwstop`).
2. Change the `:icmpcryptver (n)` property as follows:
   - If `n` is 0, change it to 2.
   - If `n` is 1, change it to 3.
3. Start the VPN/FireWall Module (`fwstart`).
4. Make the same change to the `:icmpcryptver (n)` property on the SecuRemote Client, in the `state\userc.set` file.

After making these changes, the VPN/FireWall Module will be incompatible with VPN/FireWall Modules that have not been changed, and with SecuRemote Clients up to and including build 4005.

# SecuRemote Error Messages

## SecuRemote Client

**TABLE 9-10** SecuRemote Client Errors

| Error Message | Meaning | Course of Action |
|---|---|---|
| "Internal problem" | SecuRemote encountered an unexpected problem. | Make a copy of the entire message and pass it on to your system administrator. |
| "No answer received from a FireWall ... at site ..." | SecuRemote is unable to make a connection to the indicated FireWall. | Verify that you are using the correct user name and password and then try to reconnect. |
| "Communication with site ... has failed" | SecuRemote is unable to make a connection to the indicated site. | Try to ping the site. If this fails, confirm that the Internet connection to the site is functioning. If the problem persists, notify your system administrator. |
| "Site ... has failed to sign its message" | There is a problem with the site's signature. | Notify your system administrator. |

**TABLE 9-10** SecuRemote Client Errors (continued)

| Error Message | Meaning | Course of Action |
|---|---|---|
| "Site... says that it is not a Certificate Authority" | The site does not identify itself as an FWZ Certificate Authority. | Verify that you have the correct IP address for the site, and confirm with the site's system administrator that the site is indeed a VPN-1/FireWall-1 Management Station.<br>If the site does not support FWZ, then uncheck **Respond to Unauthenticated Topology Requests (IKE and FWZ)** in the **Desktop Security** tab of the **Properties Setup** window. |
| "Site ...has failed on error ..." | SecuRemote encountered an unexpected problem. | Notify your system administrator. |
| "Site ... has changed" | The SecuRemote Client's information about the site is out-of-date. | Update the site. |
| "The IP address (...) of site ... is the same as the IP address of site ..." | Two sites have the same IP address. | Delete the incorrect one. |
| "Site ... has at least two gateways with an overlapping Encryption Domain" | There is an error in the configuration. | Notify your system administrator. |
| "Driver not found" | The driver could not be found. | Check your network configuration and reinstall SecuRemote.<br>If this message persists, uninstall SecuRemote and contact your system administrator for further assistance. |
| "Database was corrupted" | The SecuRemote Client's site database has been corrupted and is no longer usable. | Delete the `userc.c` file and redefine all your sites. |

## SecuRemote Server

**TABLE 9-11** SecuRemote Server Errors

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| FWZ,IKE, topology download | "User Alice unknown / User unknown" | The user was not found in the local VPN-1/FireWall-1 database or in an LDAP Server. | Make sure that a user with that name exists on either the local database or an LDAP Server connected to the FireWall. |
| IKE | "No pre-shared secret defined for user." | There is no pre-shared secret (password) defined for the user in the database. | Define a password for the user. |
| IKE | "The scheme IKE is not defined for user / User cannot use IKE." | The user is not configured to use IKE. | Define IKE properties for the user. |
| IKE, FWZ | "Login expired" | The user is not allowed to login on the current date. | Edit the user's properties in the **Time** tab of the **User Properties** window. |
| IKE, FWZ | "Day of Week Limitation" | The user is not allowed to login on the current day of the week. | Edit the user's properties in the **Time** tab of the **User Properties** window. |
| IKE, FWZ | "Time Limitation" | The user is not allowed to login at this time of day. | Edit the user's properties in the **Time** tab of the **User Properties** window. |
| IKE | "Firewall does not support IKE." | The VPN/FireWall Module (gateway) does not support IKE. | Define IKE properties for the VPN/FireWall Module. |
| IKE | "Could not find a common encryption method for both user and Firewall." | The VPN/FireWall Module and the SecuRemote client could not agree on a key encryption method. | In the IKE Properties of the VPN/FireWall Module, define DES or 3DES. |
| IKE | "Could not find a common hash method for both user and Firewall." | The VPN/FireWall Module and the SecuRemote Client could not agree on a hash method for the key exchange. | In the IKE Properties of the VPN/FireWall Module, define MD5 or SHA1. |
| IKE | "No common authentication method with Firewall / Could not agree on common methods." | There is no common authentication method between the authentication schemes supported by the VPN/FireWall Module, the allowed authentication method for the user and the authentication method the user tried to use. | Verify that the authentication method the user is using is defined on both the VPN/FireWall Module and on the user object in the local database/LDAP. |

**TABLE 9-11** SecuRemote Server Errors (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| FWZ | "Gateway specifies encapsulation but client does not support it" | The VPN/FireWall Module is configured to use FWZ encapsulation but the SecuRemote Client does not support FWZ encapsulation. | Upgrade the SecuRemote Client to a newer version that does support FWZ encapsulation. |
| topology download | "Refused Topology request. User not defined properly" | The most likely cause is that there is no authentication scheme defined for the user. | Define at least one IKE authentication scheme (certificates or password). |
| topology download | "Refused Topology request. Authentication scheme not allowed for user." | The user tried to use an authentication scheme which is not defined for the user. | Confirm that the authentication scheme the user tried to use (certificates or password) is defined for the user (in the **IKE Properties** tab of the **User Properties** window). |
| topology download | "Failed to retrieve gateway's CRL" | The gateway failed to retrieve a CRL from the LDAP Server. | Confirm that:<br>■ The CA is up and running.<br>■ The SecuRemote Server has connectivity to the LDAP Server that has the CRL.<br>■ The SecuRemote Server and the CA clocks are synchronized. |
| topology download | "No user password specified" | No password is defined for the user. | Define a password for the user in the **IKE Properties** tab of the **User Properties** window. |
| topology download | "Refused Topology request. Wrong Password" | The user entered an incorrect password. | Try again. If the attempt fails, define a new password. |

CHAPTER 10

# SecuRemote Client

## In This Chapter



## SecuRemote Client

The SecuRemote Client consists of a kernel module and a daemon.

### SecuRemote Kernel Module

The SecuRemote kernel module is an NDIS3.1 driver, installed between the TCP/IP stack and adapter already in use, which filters all TCP/IP communication passing through the PC. The module behaves as both an “adapter” and a “transport” connected back-to-back. Using the NDIS3.1 standard makes it possible to interface to the Microsoft TCP/IP stack or adapter using the same standard.

Initially, the TCP/IP stack (transport) is bound to a “real” adapter, for example, a dial-up or Ethernet adapter. The SecuRemote kernel module is installed by first unbinding the TCP/IP stack from the real adapter and then binding the TCP/IP stack to the adapter side of the SecuRemote kernel module and at the same time binding the

transport side of the SecuRemote kernel module to the real adapter. This is done automatically by the installation program, but it can be manually reconfigured (on Windows 9x only).

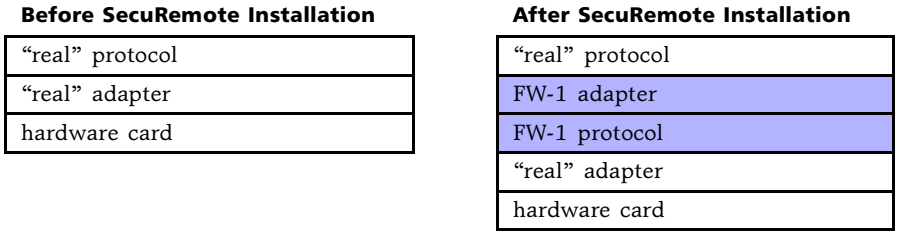



**FIGURE 10-1** Network configuration before and after SecuRemote installation

The SecuRemote kernel can determine if an outgoing or incoming packet is going to or coming from an encryption domain and so should be encrypted or decrypted.

The SecuRemote kernel also knows with which VPN/FireWall Module the encryption will take place, and invokes the daemon in order to exchange keys with the VPN/FireWall Module.

## SecuRemote Daemon

The SecuRemote daemon is a Win32 application that is run when Windows starts up and until the user logs out. The SecuRemote daemon performs the following functions:

1. Loads the SecuRemote kernel with information about all VPN/FireWall Modules and their encryption domains.
2. Provides a Graphic User Interface (GUI) by which the user can add, update, enable/disable and remove sites.

   This is done by communicating with the site's Management Module. The communication is signed with an RSA key.
3. Maintains the site list and assigns authentication credentials to each site.
4. Exchanges a session key with a VPN/FireWall Module.

   The key exchange is initiated by the SecuRemote kernel module. If necessary, the SecuRemote daemon involves the user in the authentication process. If the authentication is successful, the SecuRemote daemon exchanges a session key with the VPN/FireWall Module and loads the key into the SecuRemote kernel.

## When the SecuRemote Kernel Module Starts

When Windows is loaded, the SecuRemote kernel module is loaded and bound between the TCP/IP stack and the adapter, and its internal tables are initialized.

### When the SecuRemote Daemon Starts

When the daemon starts, it loads a list of addresses with which it should conduct encrypted sessions (the encryption domains of all the VPN/FireWall Modules in the defined sites) into SecuRemote kernel.

### As the User Works

The user can then freely use the Internet. However, when the user connects to one of the sites in the database (or a host in one of the encryption domains), the kernel module "wakes up" the daemon. Next, the daemon:

- Holds the first packet without transmitting it.
- Examines the packet and determines the relevant site, and the VPN/FireWall Module in the site.
- Challenges the user to authenticate himself or herself.
- Initiates a key exchange protocol with the VPN/FireWall Module.
- Encrypts the first packet and transmits it.

After this happens, everything the PC sends to the VPN/FireWall Module's encryption domain is encrypted.

For more information, see "Encryption Method Properties" on page 108.

# Installing the SecuRemote Client

## Minimum Installation Requirements

TABLE 10-1 lists the minimum hardware and operating system requirements for the Check Point SecuRemote Client.

**TABLE 10-1** Minimum Requirements (SecuRemote Client)

| | |
|---|---|
| **Platforms** | Windows 9x, Windows NT (Intel only) |
| **Disk space** | 6 Mbytes |
| **Memory** | Windows 9x — 16 Mbytes<br>Windows NT — 32 Mbytes |

## Installation Procedure

**Note –** If you are downgrading to a previous version of SecuRemote Client, uninstall the currently installed version before proceeding. If you are upgrading to a newer version of the SecuRemote Client, it is not necessary to uninstall the currently installed version.

***1*** Confirm that TCP/IP is working properly.

You can do this by pinging a host you know is accessible from your PC. If the ping is successful, then TCP/IP is working properly.

2 If you have the original Check Point SecuRemote Client media, insert it in the drive.

If you have downloaded the SecuRemote executable, copy it to a temporary directory and execute it. The file will self-extract.

**Note –** System administrators can ensure that all company personnel have the same site configuration for their SecuRemote Clients by copying a standard `userc.c` file to the installation diskette set. The `userc.c` file is not compressed on the diskette, and the default file contains no topology information.

3 Open the **Start** Menu and choose **Settings**.

4 Choose **Control Panel** from the **Settings** menu.

5 Double click on **Add/Remove Programs** and follow the instructions.

Alternatively, you can open the **Start** Menu and choose **Run**, and then run the `SETUP` application on the disk.

6 If Check Point SecuRemote Client is already installed on your computer, you will be asked whether you wish to overwrite the existing configuration or update it (FIGURE 10-2).

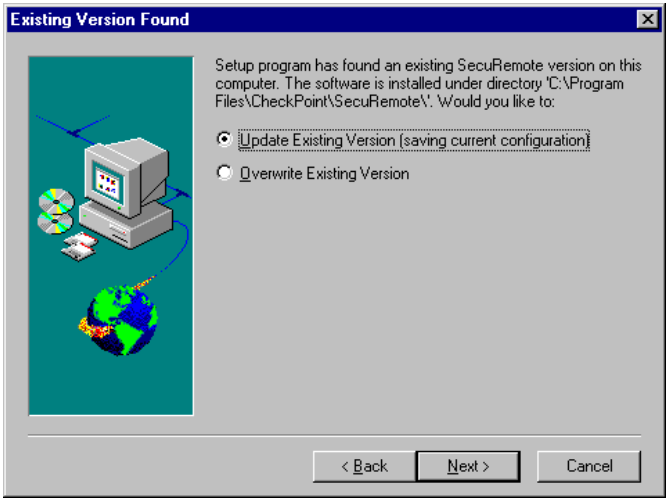



**FIGURE 10-2** Existing Version Found window

**7** The **Choose Destination Location** window (FIGURE 10-3) allows you to specify a directory in which Check Point SecuRemote Client will be installed by selecting **Browse**.

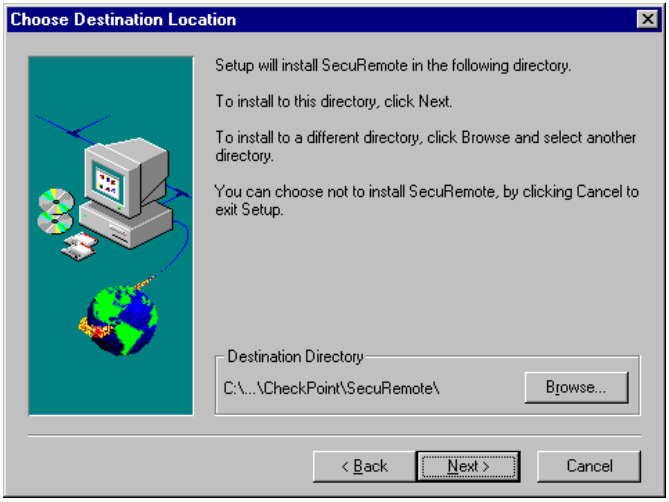



**FIGURE 10-3** Choose Destination Location window

If you do not choose a directory, then Check Point SecuRemote Client will be installed in the default directory, indicated under **Destination Directory**.

**8** Specify whether to install Desktop Security support (see Chapter 11, "VPN-1 SecureClient).

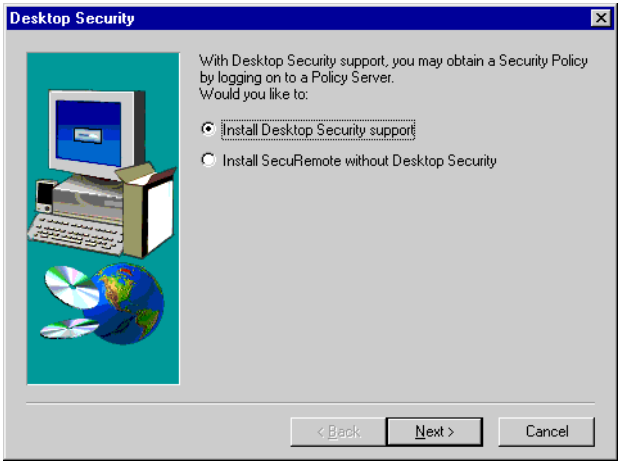



**FIGURE 10-4** Desktop Security window

**9** If you choose not to install Desktop Security support, you will be asked on which adapters to install SecuRemote.


**FIGURE 10-5** SecuRemote Bindings window

You would typically install SecuRemote only on dial-up adapters, unless your system administrator instructs you otherwise.

**Note** – You can change this setting after installation by choosing **Rebind Adapters** from the SecuRemote Client's **Tools** menu.

**10** When the installation completes, you will be asked whether you wish to restart the computer.

The new configuration will take effect only after you restart the computer.

**11** At this point, you can delete all the files from the temporary directory.

After you have restarted your computer, your first step should be to define at least one site so that you can begin to use SecuRemote to encrypt your communications. For information on how to define sites, see "Using the SecuRemote Client" on page 187.

# Uninstalling the SecuRemote Client

To uninstall the SecuRemote Client, proceed as follows:

**1** Open the Windows **Start** menu and choose **Control Panel**.

**2** Double-click on **Add/Remove Programs**.

3 Select Check Point **SecuRemote** (FIGURE 10-6).

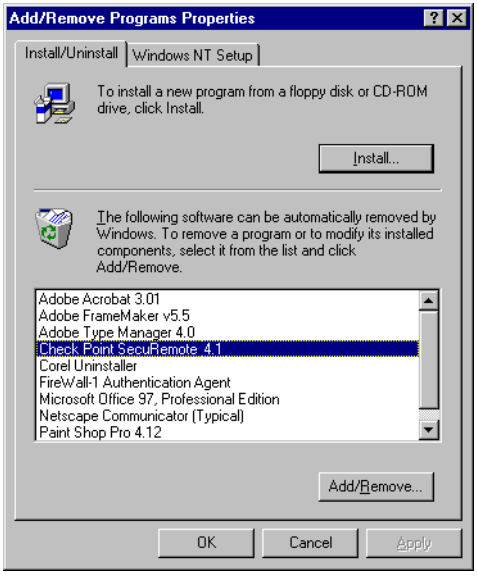



**FIGURE 10-6** Uninstalling SecuRemote

4 Click on **Add/Remove**.

5 Click on **OK**.

# After Installing

## Removing or Moving the SecuRemote Files

Do not remove or move the SecuRemote files manually. If you wish to remove the files, uninstall SecuRemote (see “Uninstalling the SecuRemote Client” on page 184). If you wish to move the files to another directory, reinstall SecuRemote with the Update option.

## Modifying the Network Configuration

On Windows 9x, if you modify your computer’s network configuration after installing the SecuRemote Client, you will have to re-install the SecuRemote Client.

## Multiple Adapters

If you have more than one adapter, the FW-1 adapter is bound to all of them. In Windows 9x, the binding is static and takes place when SecuRemote is installed. On Windows NT, the binding takes place at boot time.

For example, in FIGURE 10-7, the Check Point Protocol (FW1) is bound to both the dial-Up adapter and to the Intel EtherExpress adapter.

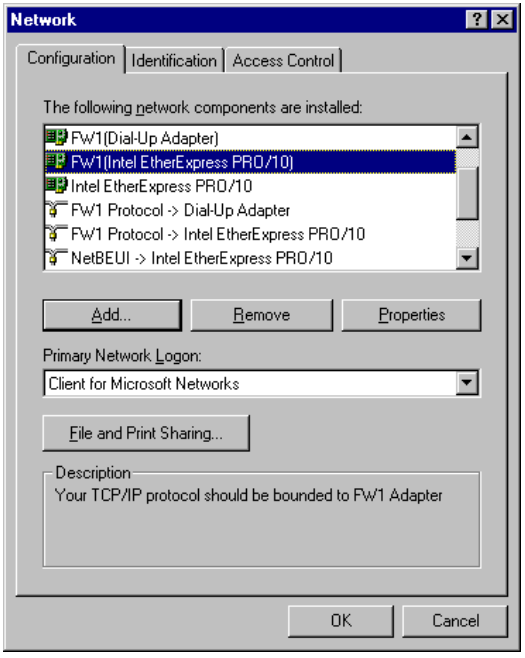



**FIGURE 10-7** Network showing two FW-1 adapters (Windows 9x only)

## Removing the FW-1 Adapter

If you are using both a dial-up and Ethernet connection, then in Windows 9x, you may find that you want to remove FW-1 adapter from the Ethernet adapter. There are three ways to do this:

1. When installing SecuRemote, install it on only on the dial-up adapter.

   Select this option during the installation process.

2. Remove the FW-1 adapter from the Ethernet adapter.

   See “To Remove the FW-1 Adapters” below.

3. Rebind by selecting **Rebind Adapters** from the **Tools** menu.

In Windows NT the need to remove the FW-1 adapter does not arise because the binding is dynamic. When you remove the FW-1 Ethernet adapter and re-boot, SecuRemote binds only to the dial-up adapter.

### To Remove the FW-1 Adapters

1. Open the Windows 9x **Start** menu and choose **Control Panel**.
2. Choose the **Network** applet.

3 In the **Configuration** tab of the **Network** window, select the FW-1 adapter you wish to remove.

For example, in FIGURE 10-7, the FW-1 adapter (positioned between the Intel EtherExpress PRO/10 adapter and the TCP/IP protocol) is selected.

If you have more than one adapter, make sure you select the one to which the SecuRemote Client is attached.

4 Click on **Remove**.

5 Click on **OK**.

6 Reboot the computer.

### Removing More than One Adapter

If you have more than one adapter, you can selectively remove SecuRemote from some of them by removing the corresponding FW-1 adapters. In most cases, there is no need to remove a FW-1 adapter.

If you wish to remove all the FW-1 adapters, uninstall the SecuRemote Client (see "Uninstalling the SecuRemote Client" on page 184).

If you wish to remove more than one FW-1 adapter (but not all of them), then you must select and remove each of the FW-1 adapters individually (see "Removing the FW-1 Adapter" on page 186), that is, you must click on **OK** to close the **Network** window and reopen it for each deletion.

# Using the SecuRemote Client

## Defining Sites

Before you can communicate using the SecuRemote daemon, you must define the sites with which you wish to communicate.

**Note –** System administrators can ensure that all company personnel have the same site configuration for SecuRemote by copying a standard `userc.c` file to the installation diskette set.

Site information can be obtained from either:

- a Management Station that manages one or more VPN/FireWall Modules*, or*
- one of the VPN/FireWall Modules (only if **Respond to Unathenticated Cleartext Topology Requests** is *not* checked in the **Desktop Security** tab of the **Properties Setup** window — see FIGURE 9-3 on page 132)

Once you define a site, you can use SecuRemote to communicate with any of the hosts in the site's encryption domain(s).

For example, in the enterprise network configured in FIGURE 10-8 on page 188, the Management Station (Mango) in the Corporate Headquarters network manages all the enterprise VPN/FireWall Modules..

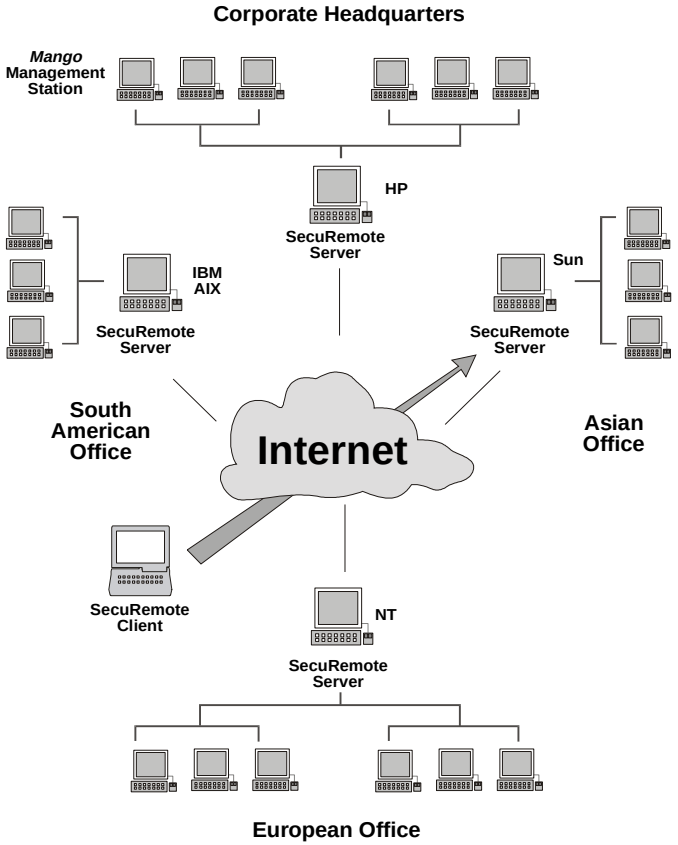



**FIGURE 10-8** Enterprise Network Configuration

If you click on the SecuRemote daemon's icon (the  icon in the taskbar's system tray), the **Sites** window (FIGURE 10-9 on page 189) is displayed. The first time you run the SecuRemote daemon, no sites are defined (unless your system administrator has provided you with pre-defined sites as part of your installation package).

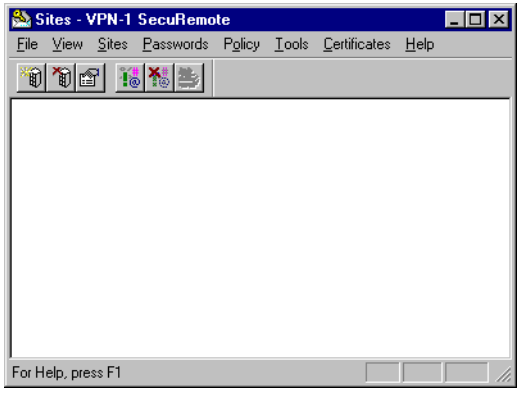



**FIGURE 10-9** Sites window

## Adding a Site

### ▼ To add a new site

1. Confirm that you are connected to the network.
2. Open the **Sites** menu and select **Make New Site** or click on  in the toolbar. The **Site** window (FIGURE 10-9) is displayed.


**FIGURE 10-10** Site window

**3** In **Name**, enter the site's name.

There are possibilities for **Name**:

- Enter a descriptive name, for example, "HQ USA" or "London". Then enter a resolvable name or IP address in **IP Address** and click on **OK**.
- Enter a resolvable name and then click on **Get**. After the IP Address is retrieved, click on **OK**.

Your system administrator will provide you with the information to enter in **IP Address**.

If the site has more than one IP address or name, use the externally known name. If this is not resolvable, try the other names one after the other until you are successful.

**4** Authenticate yourself (see "Authentication Methods" on page 126) if you are asked to do so.

If authentication is successful, the site's topology and other information are then downloaded from the site and stored locally on disk. The information is encrypted if the `encrypt_db` is set to `true` in `userc.c` (see "userc.c File" on page 170).

If authentication is unsuccessful, an error message window (FIGURE 10-11) is displayed.


**FIGURE 10-11** "Unknown User Name" message window

This message indicates that the user is unknown to the site, or that the password is incorrect. Verify that the user is defined on the site (see Chapter 5, "Managing Users" of *VPN-1/FireWall-1 Administration Guide*) before trying again to define the site.

Another possible cause is that the Single SignOn feature (see "Single SignOn" on page 205) is enabled and you are attempting to define more than one site. In this case you should disable Single SignOn and erase the passwords (see "Erasing Passwords" on page 200) before trying again to define the site.

If you attempt to a add new site whose encryption domain overlaps that of an existing site, a warning message window (FIGURE 10-12) is displayed.


**FIGURE 10-12** Overlapping Sites Warning

If you click on **Cancel**, the new site is not defined. If you click on **OK**, the new site is defined and all sites overlapping this site are disabled.

**5** If the site definition is successful, you will be reminded to verify that the information in the **Site** window (FIGURE 10-14 on page 191) is correct, in order to confirm that you have indeed communicated with the site and not with an impostor.

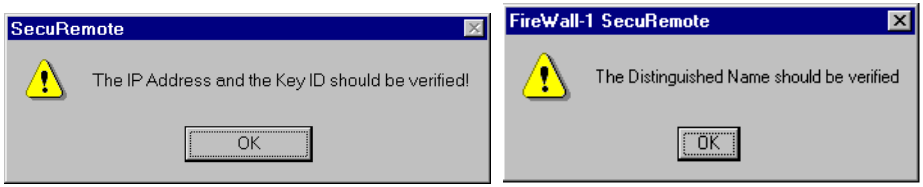



**FIGURE 10-13** Verify Site reminder (FWZ and IKE)

- For FWZ authentication, the IP Address and Key ID should be verified.
- For IKE authentication, the site's DN should be verified.

**Warning** – It is very important that you verify the information by contacting the site's system administrator by telephone or other means. For security reasons, you should not use the Internet to verify the information.

**6** Click on **OK**.

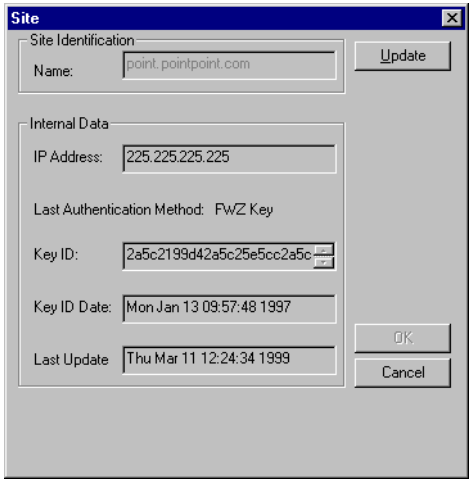



**FIGURE 10-14** Site window

After you add a site, its icon will be displayed in the **Sites** window (FIGURE 10-15).

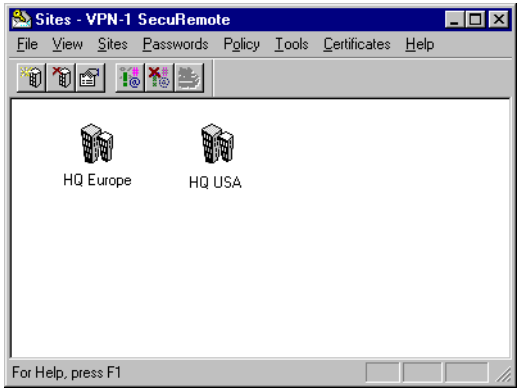



**FIGURE 10-15** Sites window showing two sites

If a site became disabled because its encryption domain overlapped that of a newly-defined site (FIGURE 10-17 on page 194), you can enable the previously-defined site (see “Enabling a Disabled Site” on page 194). If you do this, the newly-defined site becomes disabled. Two sites with overlapping encryption domains cannot be simultaneously enabled.

## Viewing Sites

You can view sites either as icons (as in FIGURE 10-15 on page 192) or as a list (FIGURE 10-16). To view the sites as a list, where the properties are displayed as well, select **Details** from the **View** menu.

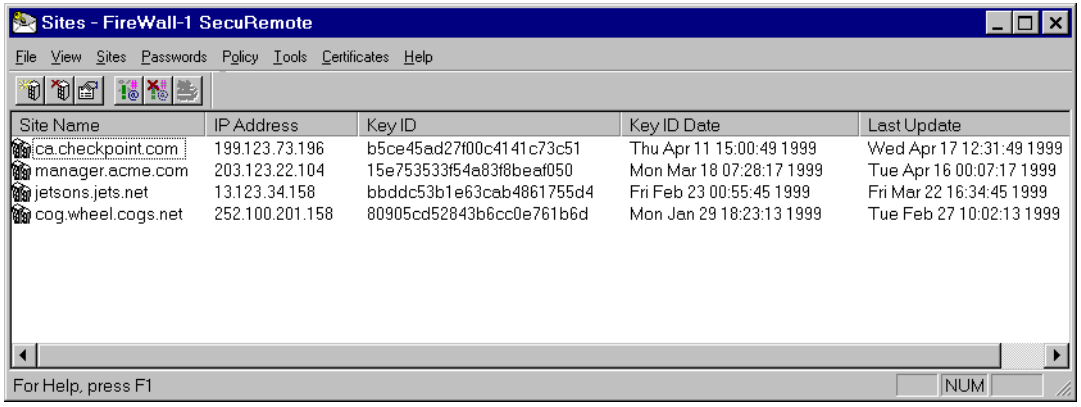



**FIGURE 10-16** Site List

## Updating a Site

You must update a site whenever its Encryption Domain changes.

### ▼ To update a site

1. Select the site by clicking on it.
2. Select **Properties** from the **Sites** menu.

   The **Site** window (FIGURE 10-18 on page 195) is displayed.

   Alternatively, you can double-click on the icon, or right-click on the icon to open the **Properties** menu (see "Properties" on page 204) and then select **Properties** from the menu.
3. Click on **Update**.

   The site information is updated. Note that the field **Last Update** has changed.

## Deleting a Site

### ▼ To delete a site

1. Select the site by clicking on it.
2. Select **Delete** from the **Sites** menu or click on  in the toolbar.

## Enabling and Disabling Sites

### Disabling a Site

1. Select the site by clicking on it.
2. Select **Disable** from the **Sites** menu.

   Alternatively, you can double-click on the icon, or right-click on the icon to open the **Properties** menu (see "Properties" on page 204) and then select **Disable** from the menu.

The SecuRemote Client will not encrypt and decrypt communications with a disabled site.

**Note –** The Security Policy may allow some services to the site to be unencrypted, for example, ICMP. If the SecuRemote Client has exchanged a session key with a VPN/FireWall Module, then if you disable the site, communication will not be possible for up to 15 minutes, because the VPN/FireWall Module still remembers the session key and expects communications to be encrypted. The solution is to wait 15 minutes and try again.

A disabled site is indicated in the **Sites** window by a large “X” over its icon (FIGURE 10-17).


**FIGURE 10-17** Site window showing a disabled site

### Enabling a Disabled Site

1. Select the disabled site by clicking on it.
2. Select **Enable** from the **Sites** menu.

   Alternatively, you can double-click on the icon, or right-click on the icon to open the **Properties** menu (see “Properties” on page 204) and then select **Enable** from the menu.

The SecuRemote Client will once again encrypt and decrypt communications with the site.

## Properties

### Viewing a Site’s Properties

1. Select the site by clicking on it.
2. Select **Properties** from the **Sites** menu or click on  in the toolbar.

   Alternatively, you can double-click on the icon, or right-click on the icon to open the **Properties** menu (see “Properties” on page 204).

The **Site** window (FIGURE 10-18) is displayed.

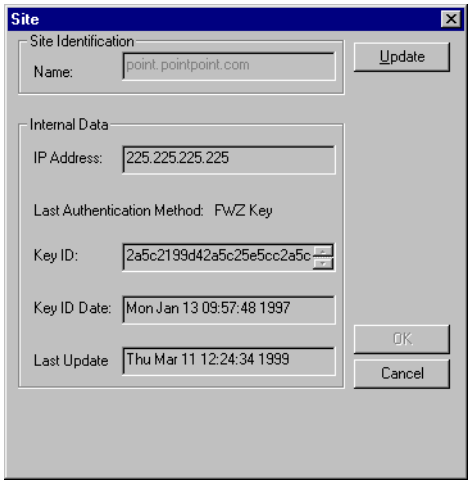



**FIGURE 10-18** Site window

You can update the site's properties, that is, retrieve them from the site, by pressing **Update**. You cannot directly modify any of the data in the window.

## Authentication

The first time a SecuRemote Client initiates a connection to a site (and also whenever a password expires), the user must first authenticate himself or herself to the FireWall/VPN Module. The authentication method used depends on the encryption method used for the connection.

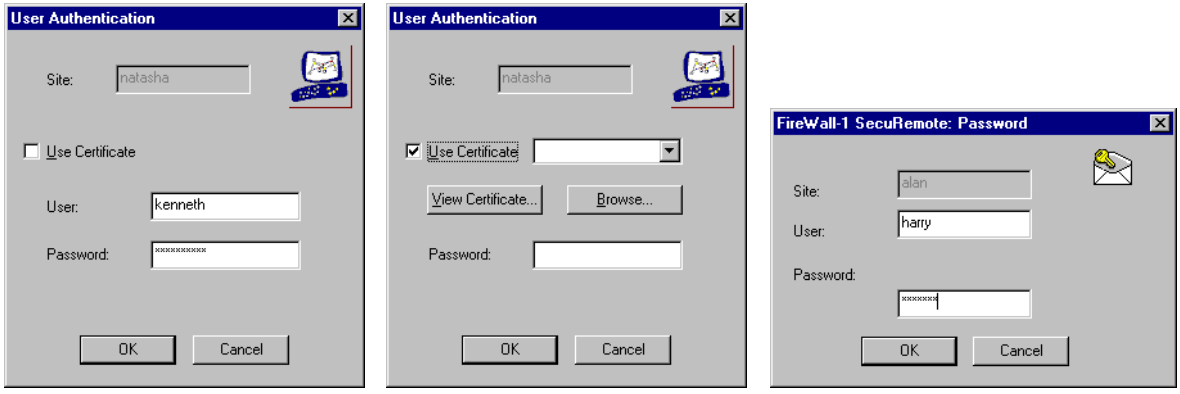



**FIGURE 10-19** SecuRemote Client User Authentication and Password windows

## Encryption Method

The encryption method used depends on the encryption methods supported by the SecuRemote Client and VPN/FireWall Module.

**TABLE 10-2** Encryption Method Supported by SecuRemote

| SecuRemote | version | supports ... |
|---|---|---|
| FireWall/VPN Module | 4.0 and higher | IKE, FWZ |
| | pre-4.0 | FWZ only |
| Client | 4.0 and higher | IKE, FWZ |
| | pre-4.0 | FWZ only |

TABLE 10-3 lists which encryption method is used for a given connection.

**TABLE 10-3** Encryption Method Used for a Given Connection by SecuRemote

| If the FireWall/VPN Module supports ... | then the encryption method used is ... |
|---|---|
| FWZ and IKE | ■ SecuRemote Client Version 4.0 and higher — the method specified in the SecuRemote Client's **Default Key Scheme** window (**Tools➤Key Scheme**)<br>■ SecuRemote Client pre-Version 4.0 — FWZ |
| FWZ only | FWZ |
| IKE only | IKE (SecuRemote Client Version 4.0 and higher) |

## Authentication Methods

There are several possible authentication methods:

### FWZ

■ FWZ — any of the authentication schemes supported on the VPN/FireWall Module: password, S/Key, RADIUS etc.

In the **Password** window, the user enters his or her user name and the password, in accordance with the **Authentication Scheme** specified in the **Authentication** tab of the **User Properties** window.

If the password is not entered, the user will be prompted for it.

If the encryption method is FWZ, the authentication is encrypted using Diffie-Hellman keys.

### IKE

- pre-shared secret

  The SecuRemote Client and VPN/FireWall Module authenticate each other by verifying that the other party knows the pre-shared secret, which is the user's password (as defined in the **Authentication** tab of the user's **IKE Properties** in window). The user enters his or her user name in **User** and the pre-shared secret in **Password**.

- certificates

  The user checks **Use Certificate**, enters an Entrust profile file name and a **Password** to access the certificate.

  The SecuRemote Client authenticates itself to the VPN/FireWall Module by using its certificate. The VPN/FireWall Module verifies the certificate against a certificate revocation list (CRL). The VPN/FireWall Module authenticates itself by sending the SecuRemote Client its certificate and a copy of a valid CRL signed by the Certificate Authority.

## FWZ Authentication

On the user's first attempt to connect to a site using FWZ encryption, the **Password** window (FIGURE 10-20) will appear. The type of password depends on the authentication scheme defined for the user in the **Authentication** tab of the **User Properties** window (FIGURE 15-2 on page 483 of *VPN-1/FireWall-1 Administration Guide*).

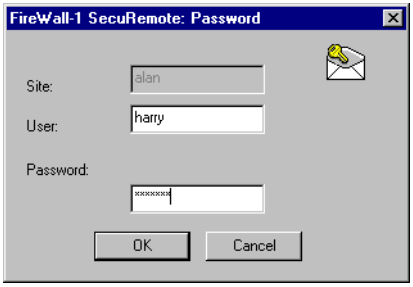



**FIGURE 10-20** Password window

Enter a user name and a password.

**Note –** You may find that it is best to enter only a user name. The site will then request the password in a separate step, and will indicate what kind of password to enter. In this way, the user will not have to remember what kind of authentication scheme he or she is using.

Passwords may be stored in the SecuRemote daemon if so configured (by checking **Cache Static FWZ Passwords on Desktop** in the **Desktop Security** tab of the **Properties Setup** window — see FIGURE 9-3 on page 132), but are not written to disk (so they are "forgotten" when the user re-boots).

**Note** – Passwords are verified by the site, not by the SecuRemote daemon. When you change a password, the new password is verified only when it is first used.

## IKE Authentication

The **User Authentication** window is displayed on a user's first attempt to connect to a site, or whenever the password expires (see "Default Key Scheme Window" on page 199).

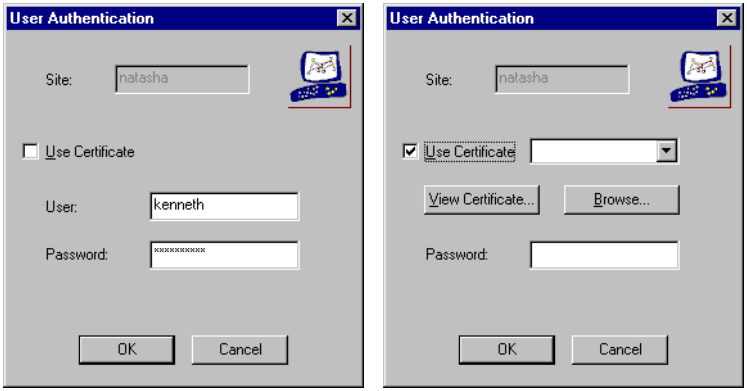



**FIGURE 10-21** SecuRemote Client User Authentication window

**Site** — the site's name

This is a read-only field.

**Use Certificate** — If checked, then specify an Entrust profile file (.EPF file) or select a hardware token from the drop-down list.

You can click on **Browse** to locate a profile.

**Warning** – When the SecuRemote user and a site authenticate each other using certificates, the SecuRemote Client trusts only the CA that signed the user's certificate. If the site's certificate is signed by a different CA (even if the gateway's CA is in the same hierarchy as the user's CA), the authentication will fail.

You can view the certificate by clicking on **View Certificate**. The **Certificate** window is displayed.

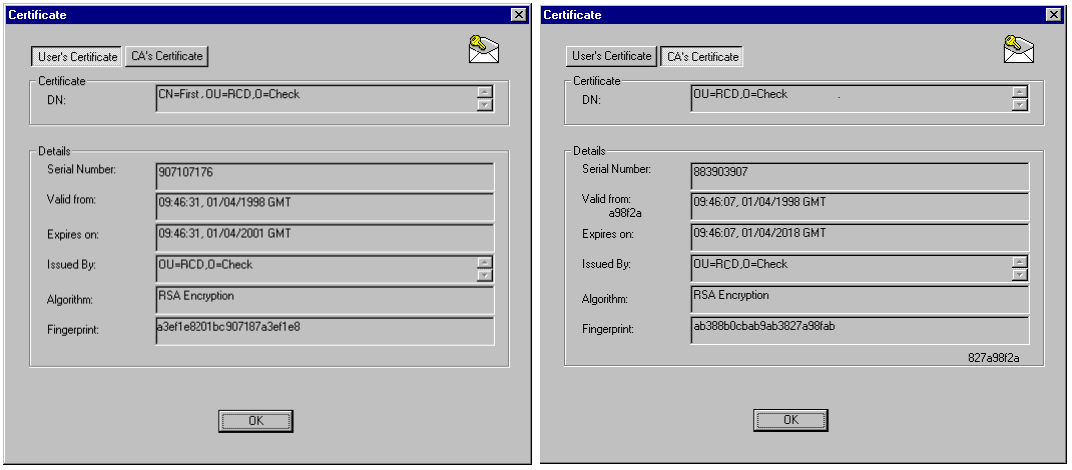



**FIGURE 10-22** Certificate window (User and CA tabs)

**Note –** You cannot modify the information in the Certificate window.

**User** — Enter the user's name.

**Password** — Enter the password.

If **Use Certificate** is checked, then this is the password for accessing the profile.

# Key Scheme

## Default Key Scheme Window

To display the **Default Key Scheme** window, select **Key Scheme** from the **Tools** menu.

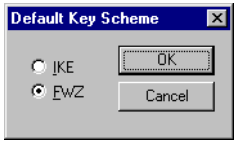



**FIGURE 10-23** Default Key Scheme window

Choose a **Default Key Scheme**. This is the encryption method that will be used when the VPN/FireWall Module supports more than one method (see TABLE 6-2 on page 125). You can choose either FWZ or IKE.

**Note –** The FWZ encryption method supports all the authentication schemes supported on the VPN/FireWall Module.

## Erasing Passwords

You can erase all the passwords (for all the defined sites) in the SecuRemote daemon by selecting **Erase Passwords** from the **Passwords** menu. This forces the SecuRemote daemon to "forget" the passwords. Open connections are not broken.

Alternatively, you can click on  in the toolbar.

Passwords are also forgotten when the Graphical User Interface (GUI) application terminates or when the computer is re-booted.

## Password Expiration

The encryption key for SecuRemote remains valid for about 15 minutes. After this time, another key exchange session between the SecuRemote Client and the site takes place, and a new key may be calculated.

If the SecuRemote Client has "forgotten" its password because the user erased it (see "Erasing Passwords" above) or if the authentication has timed out on the gateway, the user will be re-authenticated.

This re-authentication will not involve the user if *all* the following conditions are true:

1. The password has not been erased.
2. The **Password Expires After** timer in the user's **User Encryption Properties** window (FIGURE 9-8 on page 136 — FWZ only) has not expired.
3. The **Desktop Invalidates Every ... Minutes** timer in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 9-3 on page 132) has not expired.

## Entering a Password Before the Connection Begins

You can optionally enter a password even before you attempt a connection by selecting a site and then choosing **Set Password** from the **Passwords** menu. This option is useful if you find that your first attempt times out because it takes too long to enter the password.

Alternatively, open the **Properties** menu (see "Properties" on page 204) by right-clicking on a site's icon and then choose **Set Password**.

# Certificates

If the encryption method is IKE (see TABLE 10-2 on page 196), you may be asked to present a Certificate obtained from an Entrust Certificate Authority in the **User Authentication** window (FIGURE 10-21 on page 198) when you are asked to authenticate yourself.

Presenting an Entrust Certificate means specifying the location of an appropriate `.EPF` file. SecuRemote defaults to the last `.EPF` file used, but you can specify another file by clicking on **Browse**. All available hardware profiles are shown in the **User Authentication** window, below the **Use Certificate** checkbox.

**Warning –** The times on the SecuRemote Client Client and the SecuRemote Server must be accurately synchronized (including identical specification of Daylight Savings Time). If they are are not, a situation can arise where a CRL is considered valid on one side and expired onthe other.

## ENTRUST.INI File

The file `entrust.ini`, which may contain information about the Entrust and LDAP Servers, must be accessible to SecuRemote. Usually, this file is in the `WINDOWS` directory, but you can specify an alternate location for it by selecting **Select INI file** from the **Certificates menu**.

To configure an Entrust `.INI` file, choose **Configure INI** from the **Certificates menu**. The **Configure Entrust.INI** window (FIGURE 10-24) is displayed.

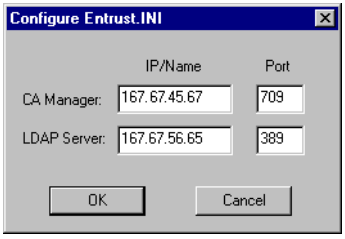



**FIGURE 10-24** Configure Entrust.INI window

**CA Manager** — Enter the IP address or resolvable name of the CA Manager and the port number.

**LDAP Server** — Enter the IP address or resolvable name of the LDAP Server and the port number.

# Entrust Users

If a user forgets his or her profile or if a profile is corrupted, the system administrator will arrange for the Certificate Authority to either create a new user or recover the existing user.

## Creating a Certificate

To create an Entrust certificate, choose **Create** from the **Certificates** menu. The **Create User** window (FIGURE 10-25) is displayed.

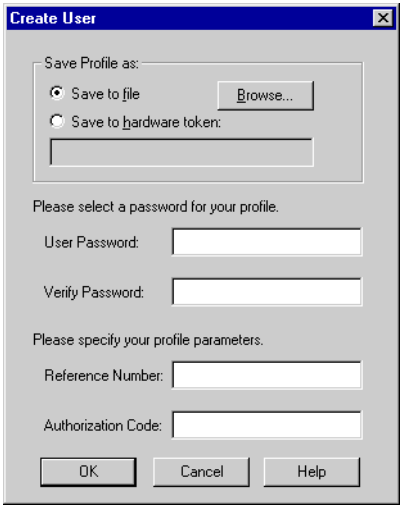



**FIGURE 10-25** Create User window

**Save to file** — Click on **Browse** and specify the full path name of the file (for example, `c:\EPF\alicejones.EPF`) to which the profile will be saved.

**Save to hardware token** — Specify a name for the profile.

**User Password** — Choose a password.

**Verify Password** — Enter the password a second time to ensure it is entered correctly.

**Reference Number** and **Authorization Code** — These values (generated by the Certificate Authority) were given to you by your system administrator.

## Recovering a Certificate

**Warning** – Consult with your system administrator before recovering a certificate.

To recover an Entrust certificate, choose **Recover** from the **Certificates** menu. The **Recover User** window (FIGURE 10-26) is displayed.

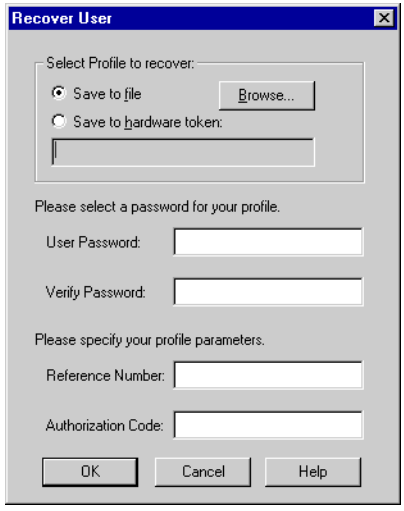



**FIGURE 10-26** Recover User window

The fields in the **Recover User** window are the same as those in the **Create User** window (FIGURE 10-25 on page 202).

### Offline Certificate Registration

To create a certificate using the Entrust Certificate Utility, select **Offline Registration Utility** from the **Certificates** menu.

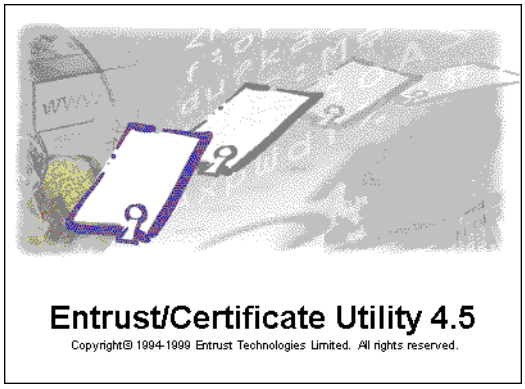



**FIGURE 10-27** Entrust Certificate Utility window

### Importing PKCS#12 Certificates

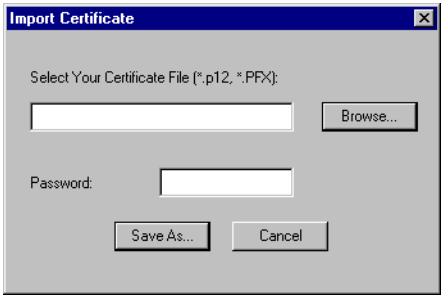



**FIGURE 10-28** Import Certificate window

PKCS #12 type certificates are usually files with a P12 or PFX suffix, and are obtained using a Web browser.

## Properties

If you right-click on a site icon, the **Properties** menu is displayed.

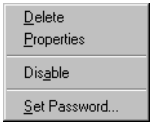



**FIGURE 10-29** Properties menu

The **Properties** menu items are shortcuts for menu commands (see TABLE 10-4).

**TABLE 10-4** Properties menu items and their corresponding menu commands

| Menu Item | Menu Command | See ... |
|---|---|---|
| **Delete** | **Sites➤Delete** | "Deleting a Site" on page 193 |
| **Properties** | **Sites➤Properties** | "Properties" on page 194 |
| **Disable** | **Sites➤Disable** | "Enabling and Disabling Sites" on page 193 |
| **Enable** | **Sites➤Enable** | "Enabling and Disabling Sites" on page 193 |
| **Set Password** | **Passwords➤Set Password ...** | "Entering a Password Before the Connection Begins" on page 200 |

# Closing the SecuRemote Daemon

To close the SecuRemote daemon window, select **Exit** from the **File** menu. The SecuRemote daemon remains active, but its window is closed. To open it again, click on its icon.

You can deactivate the SecuRemote daemon by selecting **Kill** from the **File** menu. The SecuRemote kernel remains in the stack, but it does nothing. When you reboot the computer or restart the SecuRemote Client from the **Start** menu, it becomes active again.

You can also restart the SecuRemote daemon by selecting it from the SecuRemote folder in the **Start** menu.

# Entrust Entelligence

If Entrust Entelligence is running, then it will be used for all certificate-related operations instead of SecuRemote. In other words, the user will work in the Entrust Entelligence windows instead of in the SecuRemote windows.

You can ensable (or disable) Entrust Entelligence by choosing **Enable/Disable Entrust Entelligence** from the **Certificates** menu. However, Entrust Entelligence will be used to create certificates even it is disabled in the SecuRemote Client, in order to ensure that SecuRemote certificates are compatible with Entelligence in terms of encryption key strength.

# Single SignOn

## Overview

The Single SignOn option allows you to save your SecuRemote user name and password so they do not have to be entered manually in the future. Single SignOn is available for password authentication only, and is suitable for SecuRemote Clients with only one site defined.

## Configuring Single SignOn

1 Select **Configure SSO** from the **Passwords** menu.

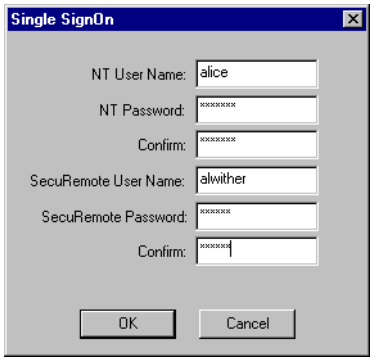



**FIGURE 10-30** Single SignOn window

2 In the **Single SignOn** window (FIGURE 10-30), enter your NT and SecuRemote user names and passwords.

3 To enable Single SignOn, select **Enable SSO** from the **Passwords** menu.

Your SecuRemote user name and password (your "credentials") are then encrypted in the Windows NT registry. The next time you restart your computer, Single Signon will be in effect. On future boots you will not be prompted for this information.

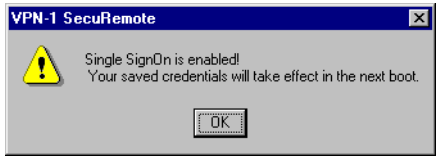



**FIGURE 10-31** Single SignOn Enabled window

If your NT password changes, you must reconfigure your Single SignOn passwords.

## Disabling Single SignOn

To disable Single SignOn, select **Disable SSO** from the **Passwords** menu.

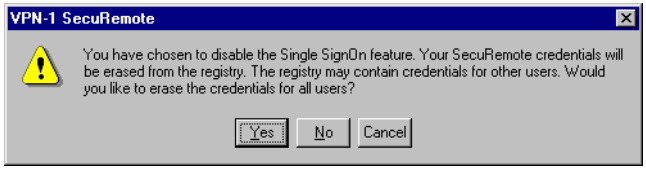



**FIGURE 10-32** Disabling Single SignOn window

# SecuRemote Client Menus

## File Menu

**TABLE 10-5** File Menu Commands

| Menu Entry | Toolbar Button | Description | See |
|---|---|---|---|
| **Exit** | none | | |
| **Kill** | none | | |

## View Menu

**TABLE 10-6** View Menu Commands

| Menu Entry | Toolbar Button | Description | See |
|---|---|---|---|
| **Toolbar** | none | Toggle the display of the SecuRemote Client toolbar. | "SecuRemote Client Toolbar" on page 210 |
| **Status Bar** | none | Toggle the display of the SecuRemote Client Status Bar. | |
| **Large Icons** | none | Display sites as large icons. | "Viewing Sites" on page 192 |
| **Small Icons** | none | Display sites as small icons. | "Viewing Sites" on page 192 |
| **List** | none | Display sites as a list. | "Viewing Sites" on page 192 |
| **Details** | none | Display sites as a list showing details. | "Viewing Sites" on page 192 |

The SecuRemote Client toolbar is displayed below the menu. The SecuRemote Client Status Bar is displayed at the bottom of the SecuRemote Client window.

## Sites Menu

**TABLE 10-7** Sites Menu Commands

| Menu Entry | Toolbar Button | Description | See |
|---|---|---|---|
| **Make New** |  | Make a new site. | "Adding a Site" on page 189 |
| **Delete** |  | Delete a site. | "Deleting a Site" on page 193 |
| **Disable** | none | Disable a site. | |
| **Properties** |  | Display a site's properties. | "Properties" on page 194 |

## Passwords Menu

**TABLE 10-8** Passwords Menu Commands

| Menu Entry | Toolbar Button | Description | See |
|---|---|---|---|
| **Set Password** |  | Enter a new password to be used for the next authentication. | "Entering a Password Before the Connection Begins" on page 200 |
| **Erase Passwords** |  | Erase all the password's from the SecuRemote daemon's memory | "Erasing Passwords" on page 200 |
| **Configure SSO** | none | Configure your SecuRemote credentials. | "Single SignOn" on page 205 |
| **Enable SSO** | none | Enable the Single SignOn option. | "Single SignOn" on page 205 |
| **Disable SSO** | none | Disable the Single SignOn option. | "Single SignOn" on page 205 |
| **Configure SDL Timeout** | none | Define the Secure Domain Logon timeout. | "Secure Domain Logon" on page 162 |
| **Enable SDomain Logon** | none | Enable the Secure Domain Logon option. | "Secure Domain Logon" on page 162 |
| **Disable SDomain Logon** | none | Disable the Secure Domain Logon option. | "Secure Domain Logon" on page 162 |

## Policy Menu

**TABLE 10-9** Policy Menu Commands

| Menu Entry | Toolbar Button | Description | See |
|---|---|---|---|
| **Disable Policy** | none | Disable the Desktop Policy. | Chapter 11, "VPN-1 SecureClient" |
| **Allow All** | none | No Desktop Policy is installed on the SecureClient. This option is equivalent to the standard VPN-1 SecuRemote Client. | |
| **Allow Outgoing and Encrypted** | none | Only outbound connections (from the SecureClient) are allowed, except for the following (which are also allowed):<br>■ ICMP return packets<br>■ Session Authentication Agent protocol (port 261) | |
| **Allow Outgoing Only** | none | Only VPN (encrypted) connections are allowed (inbound and outbound) | |
| **Allow Encrypted Only** | none | Connections allowed by **Allow Outgoing Only** and **Allow Encrypted Only** are allowed. | |
| **Block All** | none | Block all connections to the SecuRemote Client machine. | |
| **Login to Policy Server** |  | Download a Desktop Policy from a Policy Server. | |

## Tools Menu

**TABLE 10-10** Tools Menu Commands

| Menu Entry | Toolbar Button | Description | See |
|---|---|---|---|
| **Key Scheme** | none | Display the **Default Key Scheme** window. | "Default Key Scheme Window" on page 199 |
| **Rebind Adapters** | none | Reconfigure the adapters to which SecuRemote is bound. | |

## Certificates Menu

**TABLE 10-11** Certificates Menu Commands

| Menu Entry | Toolbar Button | Description | See |
|---|---|---|---|
| **Create** | none | Create an Entrust user (profile). | "Creating a Certificate" on page 202 |
| **Recover** | none | Recover an Entrust profile. | "Recovering a Certificate" on page 203 |
| **Import** | none | | "Importing PKCS#12 Certificates" on page 204 |
| **Offline Registration Utility** | none | Start the Entrust certificate generation procedure. | |
| **Select INI File** | none | Specify an INI file to be used. | "ENTRUST.INI File" on page 201 |
| **Configure INI File** | none | Configure INI file parameters. | "ENTRUST.INI File" on page 201 |
| **Enable/Disable Entrust Entelligence** | none | Enable or Disable Entrust Entelligence | "Entrust Entelligence" on page 205 |

## Help Menu

**TABLE 10-12** Help Menu Commands

| Menu Entry | Toolbar Button | Description | See |
|---|---|---|---|
| **Index** | none | Display Help. | |
| **Using Help** | none | Display instructions for using Help. | |
| **About SecuRemote** | none | Display the "About SecuRemote" window. | |

# SecuRemote Client Toolbar

**FIGURE 10-33** SecuRemote Client Toolbar

The toolbar buttons are shortcuts for menu commands (see TABLE 10-13).

**TABLE 10-13** Toolbar buttons and their corresponding menu commands

| Toolbar Button | Menu Command |
|---|---|
|  | **Sites➤Make New** |
|  | **Sites➤Delete** |
|  | **Sites➤Properties** |
|  | **Passwords➤Set Password** |
|  | **Passwords➤Erase Passwords** |
|  | **Policy➤Login to Policy Server** |

CHAPTER 11

# VPN-1 SecureClient

## In This Chapter



## Overview

### What is Check Point VPN-1 SecureClient?

Check Point VPN-1 SecureClient extends security to the desktop by enabling administrators to enforce a Security Policy on desktops — both inside the LAN and connecting from the Internet — and prevent unauthorized users from taking control of authorized connections ("hijacking" them). In addition, the configuration of SecureClient machines can be verified and access denied to misconfigured SecureClient machines.

Check Point VPN-1 SecureClient consists of:

- VPN-1 SecuRemote Client software with the Desktop Security feature installed
- A Policy Server from which the VPN-1 SecuRemote Client obtains its Desktop Policy

## Examples

FIGURE 11-1 on page 214 shows how an intruder can take advantage of an existing valid SecuRemote connection to penetrate the internal enterprise network. This kind of attack can be prevented by enforcing — on the VPN-1 SecuRemote Client — a Desktop Policy that does not allow incoming connections to the VPN-1 SecuRemote Client.

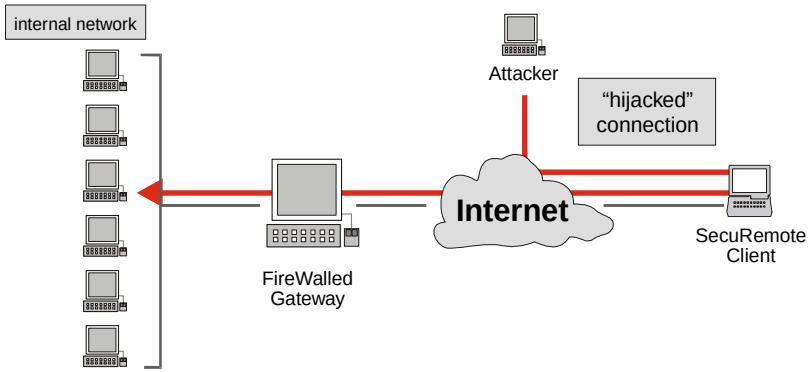



**FIGURE 11-1** Taking unauthorized control of ("hijacking") a SecuRemote connection

In FIGURE 11-2, the servers in FinanceNet are protected by an internal VPN/FireWall Module on Tower. The Security Policy allows Bob on BigBen to connect to FinanceNet, but users on Tate are not allowed to do so.

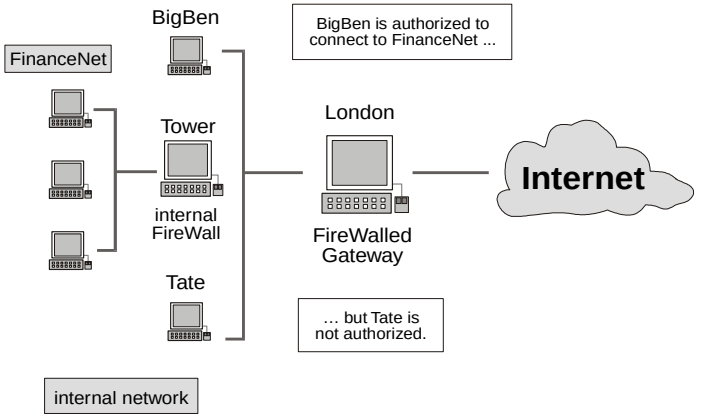



**FIGURE 11-2** Securing an internal subnetwork

By installing SecureClient on BigBen, this high degree of security can be enhanced to:

- Prevent Tate (and anyone else) from taking control of the connection between BigBen and FinanceNet.

  This is configured by installing a Desktop Policy on BigBen in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 11-4 on page 219).

- Encrypt connections between BigBen and FinanceNet.

  This is configured (in the **VPN** tab of Tower's **Workstation Properties** window) by:

  - defining FinanceNet to be in Tower's encryption domain
  - checking **Exportable to SecuRemote**

- Verify that BigBen is properly configured.

  The proper configuration is defined in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 11-4 on page 219). The configuration is verified by defining a Client Encrypt rule for the connection and checking **Apply Rule only if Desktop Configuration Options are Verified** in the rule's **User Encryption Action Properties** window (FIGURE 11-5 on page 221).

# Example Configuration

## Network Configuration

FIGURE 11-3 depicts a configuration in which SecureClient provides security both inside and outside the LAN.

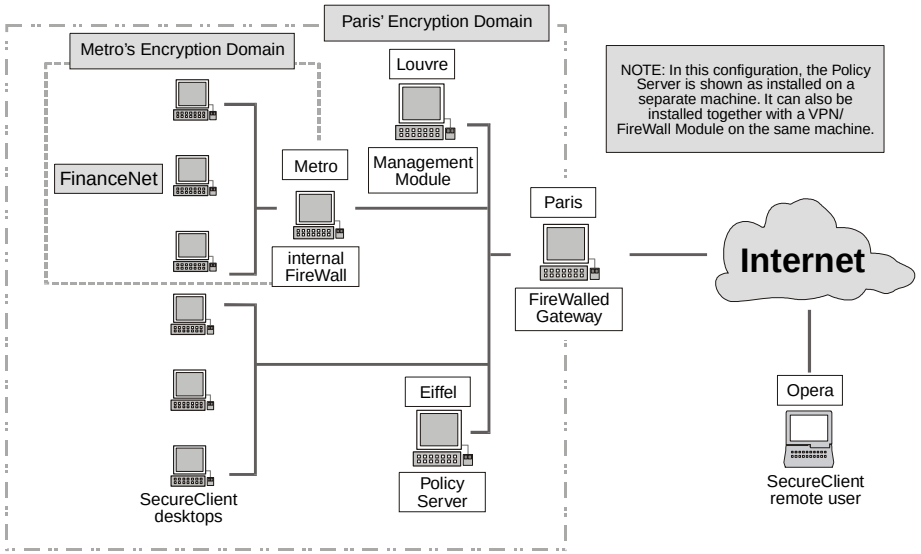



**FIGURE 11-3** Securing a LAN with VPN-1 SecureClient

The configuration consists of:

- a Management Module (Louvre), on which the Security Policy is defined
- a FireWalled gateway (Paris), which enforces the Security Policy
- a Policy Server (Eiffel), from which the Desktop Policy is downloaded to the SecureClients
- an internal VPN/FireWall Module (Metro), which protects the Finance subnet by encrypting connections

An internal VPN/FireWall Module is required to protect a network (as in this configuration), but if only the host itself must be protected, then a VPN-1 SecureServer Module is adequate.

- a number of internal SecureClient desktops
- a remote SecureClient (Opera)

**Note –** The Policy Server can be installed either on a separate machine, or together with a VPN/FireWall Module on the same machine. So for example, in FIGURE 11-3, the Policy Server can be either on Eiffel or on Paris.

## Installed Software Modules

TABLE 11-1 lists the VPN-1/FireWall-1 software installed on each of the machines in FIGURE 11-3.

**TABLE 11-1** Installed Software Modules

| machine | installed VPN-1/FireWall-1 software module |
|---|---|
| Louvre | Management Module |
| Paris | VPN/FireWall Module |
| Eiffel | VPN/FireWall Module with SecureClient license |
| Metro | VPN/FireWall Module |
| desktops | SecureClient (SecuRemote with Desktop Security enabled) |
| Opera | SecureClient (SecuRemote with Desktop Security enabled) |

Desktop Security can be enabled in the VPN-1 SecuRemote Client when it is installed.

# Configuring SecureClient

To configure SecureClient (referring to the example configuration in FIGURE 11-3), proceed as follows:

***1*** Install the appropriate VPN-1/FireWall-1 software and licenses on each machine (see TABLE 11-1).

2 Define the network objects (see Chapter 4, “Network Objects” of *VPN-1/FireWall-1 Administration Guide* for information) and configure them as described in TABLE 11-4.

**TABLE 11-2** Network Objects Configuration

| network object | configuration |
|---|---|
| Louvre | In the **General** tab of Louvre’s **Workstation Properties** window, check **Management Station**. |
| Paris | In Paris’ **Workstation Properties** window:<br>■ In the **General** tab, check **VPN-1 & FireWall-1 Modules Installed**.<br>■ In the **VPN** tab, specify Paris’ encryption domain.<br>■ In the **VPN** tab, check **Exportable to SecuRemote**. |
| Eiffel | In Eiffel’s **Workstation Properties** window:<br>■ In the **General** tab, check **VPN-1 & FireWall-1 Modules Installed**.<br>■ In the **VPN** tab, check **Exportable to SecuRemote**.<br>■ In the **Policy Server Properties** window (FIGURE 11-7), define Eiffel as a Policy Server. |
| Metro | In Metro’s **Workstation Properties** window:<br>■ In the **General** tab, check **VPN-1 & FireWall-1 Modules Installed**.<br>■ In the **VPN** tab, specify Metro’s encryption domain.<br>■ In the **VPN** tab, check **Exportable to SecuRemote**. |

3 Configure the SecuRemote and Desktop Security options in the **Desktop Security** tab of the **Properties Setup** window (see FIGURE 11-4 on page 219).

4 Define the users and user groups who will be allowed access to the protected networks (see Chapter 5, “Managing Users” of *VPN-1/FireWall-1 Administration Guide* for information).

5 Define the Policy Server and assign a user group (see FIGURE 11-7 on page 223).

6 Define the appropriate rules to allow authorized users to access the protected networks (see Chapter 8, “Security Policy Rule Base” of *VPN-1/FireWall-1 Administration Guide* for information).

In the example, the required rule is similar to:

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| FinanceUser@Any | FinanceNet | Any | Client Encrypt | None | Gateways |

7. If the configuration includes overlapping encryption domains (as in FIGURE 11-3 on page 215), then define a rule allowing access through the "outer" VPN/FireWall Module as described in "Overlapping Encryption Domains" on page 224.

8. Define a rule on the Policy Server that allows the (pre-defined) FW1_pslogon service between the SecureClient and the Policy Server.

9. If there is a VPN/FireWall Module between the Policy Server and the SecureClient, you must allow the fw1_encapsulation and RDP services for FWZ and the IPSec service for IKE.

10. Install the Security Policy.

    This will also download the Desktop Policy to the Policy Server.

11. SecureClient users then download the Desktop Policy.

    To download a Desktop Policy, the SecureClient user should do one of the following:

    - Choose **Policy➤Login to Policy Server** select a Policy Server, *or*
    - Right-click on the SecureClient icon in the taskbar and choose **Login**, *or*
    - Click on  in the toolbar.

    The user then is challenged to authenticate himself or herself. If the user is not a member of the group specified in the **Policy Server Properties** window (FIGURE 11-7 on page 223), the Desktop Policy is not downloaded.

The SecuRemote Client's taskbar icon changes when a Desktop Policy has been successfully downloaded.

-  indicates that a Desktop Policy is being enforced.

  The lock is either green (packet allowed) or red (packet dropped).

-  indicates that a Desktop Policy is being enforced, and that the SecureClient's configuration has been verified by the Policy Server.

  The lock is either green (packet allowed) or red (packet dropped).

-  indicates that no Desktop Policy is being enforced.

# Properties Setup — Desktop Security Tab

The Desktop Policy is defined in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 11-4 on page 219) and is downloaded from the Management Module (Louvre) to the Policy Server (Eiffel) when the Security Policy is installed.

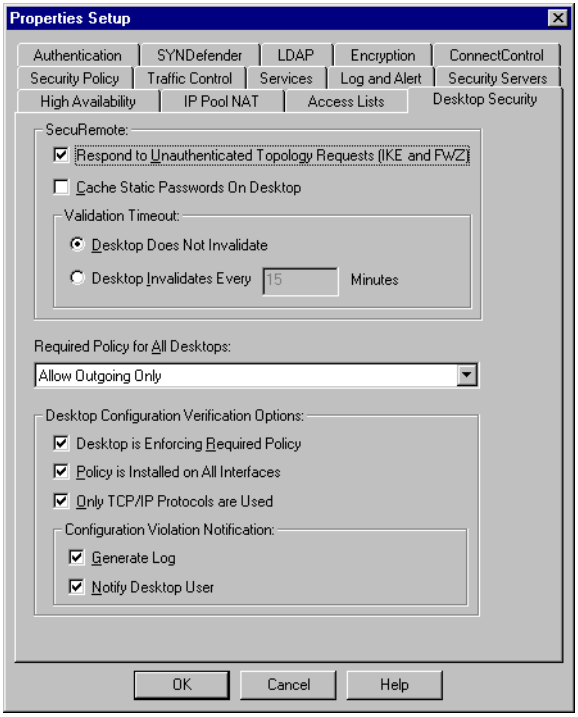



**FIGURE 11-4** Properties Setup — Desktop Security tab

**Required Policy for All Desktops** specifies the Desktop Policy that will be downloaded to all Policy Servers (and from there to SecureClients). These Desktop Security Policies are described in TABLE 11-3:

**TABLE 11-3** Desktop Policy options

| Desktop Policy | meaning (inbound and outbound refer to the desktop) |
|---|---|
| **Allow All** | No Desktop Policy is installed on the SecureClient. This option is equivalent to the standard VPN-1 SecuRemote Client. |
| **Allow Outgoing Only** | Only outbound connections (from the SecureClient) are allowed, except for the following (which are also allowed):<br>■ ICMP return packets<br>■ Session Authentication Agent protocol (port 261) |
| **Allow Encrypted Only** | Only VPN (encrypted) connections are allowed (inbound and outbound) |
| **Allow Outgoing and Encrypted** | Connections allowed by **Allow Outgoing Only** and **Allow Encrypted Only** are allowed. |

## Desktop Configuration Verification

**Desktop Configuration Verification Options** specifies the components of the desktop configuration that the Policy Server verifies when an encrypted connection is negotiated (during the key exchange procedure). If the Desktop Policy does not conform, the action specified under **Configuration Violation Notification** is taken.

**TABLE 11-4** Configuration Verification options

| Option | means that the Policy Server verifies that ... |
|---|---|
| **Desktop is Enforcing Required Policy** | ... the desktop is enforcing the Security Policy defined for it in **Required Policy for All Desktops**. |
| **Policy is Installed on all Interfaces** | ... the Desktop Policy is installed on all of the desktop's interfaces. |
| **Only TCP/IP Protocols are Used** | ... only TCP/IP is enabled on the desktop (and not, for example, IPX). |

After the Desktop Policy has been downloaded, the Policy Server maintains an open connection to the SecureClient. If Policy Server is notified whenever the SecureClient's Desktop Policy is modified.

You can verify that the SecureClient is properly configured before applying a rule whose action is either Client Encrypt or Session Authentication. A misconfigured SecureClient is denied access under the rule. The configuration components verified are the components checked in the **Desktop Security** tab of the **Properties Setup** window.

The result of a configuration verification is cached for the time period (in seconds) specified by the `timeout` parameter in the `$FWDIR/database/fwdtmquery.C` file.

```
(
    :cache_params (
           :timeout (15)
    )
)
```

If this file does not exist, the timeout period defaults to 15 seconds. If `timeout` is set to zero, there is no caching and the configuration is verified for each connection.

Client Encrypt

In the Client Encrypt rule's **User Encryption Action Properties** window (FIGURE 11-5), check **Apply Rule Only if Desktop Configuration Options are Verified**.

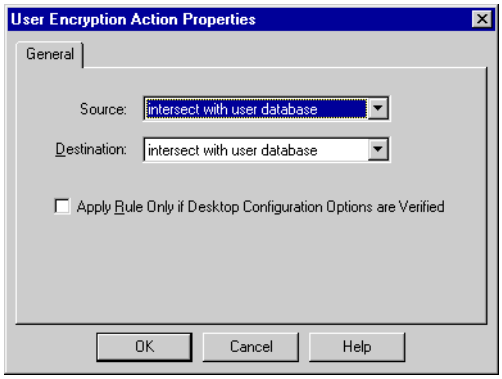



**FIGURE 11-5** User Encryption Action Properties window

**Getting Here** – To display the **User Encryption Action Properties** window, double-click on the Client Encrypt action in the rule.

Session Authentication

In the Session Authentication rule's **Session Authentication Action Properties** window (FIGURE 11-6), check **Verify secure configuration with Policy Server** and select a Policy Server from the drop-down list.

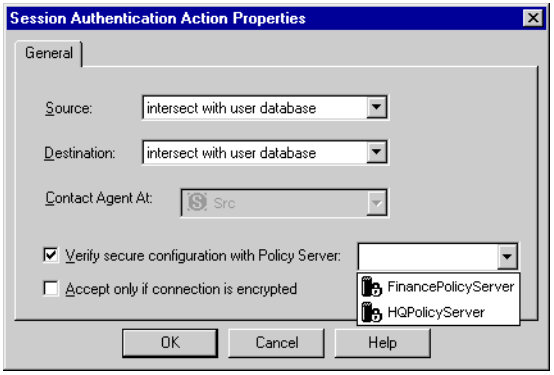



**FIGURE 11-6** Session Authentication Action Properties window

**Getting Here** – To display the **Session Authentication Action Properties** window, double-click on the Session Authentication action in the rule.

The VPN/FireWall Module enforcing the rule will confirm with the specified Policy Server that the SecureClient is properly configured.

**Note** – The first time you install a Security Policy that includes a Session Authentication rule with **Verify secure configuration with Policy Server** checked, you must stop and restart the VPN/FireWall Module before the setting takes effect.

## Policy Server Properties Window

Policy Servers are defined in the **Policy Server Properties** window (FIGURE 11-7).

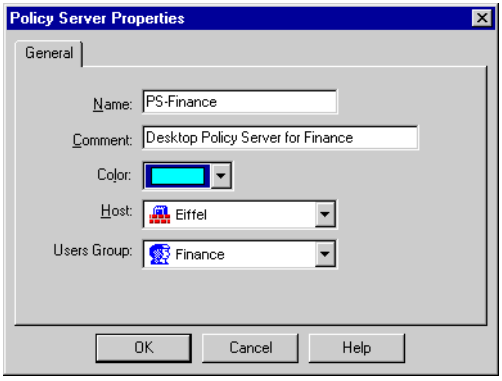



**FIGURE 11-7** Policy Server Properties window

**Getting Here** – To display this window, choose **Manage➤Servers** in the menu, and in the **Server Objects** window (FIGURE 10-1 on page 319 of *VPN-1/FireWall-1 Administration Guide*):

- To define a new Policy Server, click on **New** and then on **Policy Server**.
- To edit the properties of an existing Policy Server, select the Policy Server and click on **Edit**.

**Host** must be a workstation for which:

- **VPN-1 & FireWall-1** is checked and Version set to **4.1** or higher in **Modules Installed** in the **General** tab of its **Workstation Properties** window
- **Exportable to SecuRemote** is checked in the **VPN** tab of its **Workstation Properties** window

**Users Group** specifies the users who will be downloading their Desktop Security Policies from the Policy Server. The user group can be a FireWall-1 group or a group defined on an LDAP Server. The Policy Server counts the users to verify that the software license is not violated.

When a Security Policy is installed, the Desktop Policy defined in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 11-4 on page 219) is downloaded to all the Policy Servers.

### Overlapping Encryption Domains

When the remote SecureClient (Opera in the example configuration depicted in FIGURE 11-3 on page 215) connects to a host in the Finance subnet, it encrypts with Metro. The site's topology information specifies that Metro's encryption domain is contained in Paris' encryption domain, so there must be a rule that allows encrypted communications to pass through Paris without being decrypted, as follows:

| Source | Destination | Services | Action | Track | Install On |
|---|---|---|---|---|---|
| Any | FinanceNet | Encrypted_Services | Accept | None | Paris |

"Encrypted_Services" is a pre-defined service. There must also be an appropriate Client Encrypt rule on Metro to decrypt the connection (see step 6 on page 217 for an example).

**Warning –** FWZ encryption without encapsulation is not supported for overlapping encryption domains.

# Installing Desktop Policies

When the Security Policy is installed on the VPN/FireWall Modules, the Policy Servers receive the Desktop Policy that they will later install on the SecureClients. The Policy Servers install the Desktop Policy on the SecureClients when the users login to the Policy Server, explicitly or implicitly (see "Downloading a Desktop Policy" on page 227).

## Specifying the Desktop Policy

The Desktop Policy to be downloaded to SecureClients is specified in **Required Policy for All Desktops** in the **Desktop Security** tab of the **Properties Setup** window (FIGURE 11-8 on page 225). See TABLE 11-3 on page 220 for an explanation of the available options.

## Desktop Policy Verification

In the **Desktop Security** tab of the **Properties Setup** window (FIGURE 11-8 on page 225), the system administrator can specify that the Desktop configuration be verified, and the action to take if the configuration is incorrect. See TABLE 11-3 on page 220 for an explanation of the available options.

The Desktop configuration is verified when the SecureClient user downloads a Desktop Policy from the Policy Server, and whenever the desktop performs a key exchange with a Version 4.1 or higher VPN/FireWall Module.

If the configuration is incorrect, the action specified in **Configuration Violation Notification** is taken. The options are:

**Generate Log** — Generate a log entry to the VPN-1/FireWall-1 Log.

The log entry's action is "Deauthorize" and the reason is the text given in TABLE 11-5 on page 226.

**Notify Desktop User** — Display an error message window (for example, FIGURE 11-10 on page 228) on the SecureClient machine.

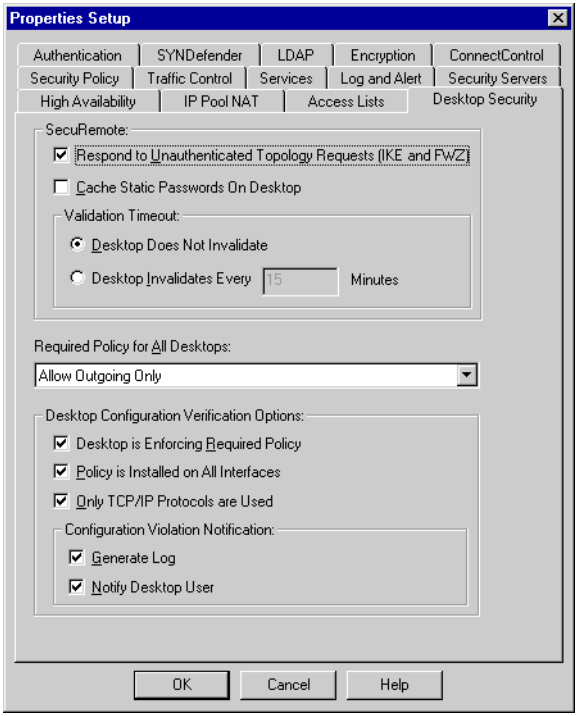



**FIGURE 11-8** Properties Setup — Desktop Security tab

TABLE 11-5 lists the error messages displayed in the VPN-1/FireWall-1 log or on the desktop when the desktop is incorrectly configured.

**TABLE 11-5** Desktop Configuration Errors

| Log text | Desktop error message text | meaning |
|---|---|---|
| "Old SecuRemote" | There is no message on the desktop. | An obsolete version of SecuRemote, which does not support Desktop Security, is installed on the desktop. |
| "Lost policy" | "You are not authorized to have a policy!" | The user has been removed from the group of users authorized to receive a Desktop Policy from the Policy Server. This error occurs only if the desktop tries to download a policy from the same Policy Server from which it last downloaded a policy. |
| "No policy" | "The security policy on your computer has been removed." | The desktop has no Desktop Policy. |
| "Wrong Policy" | "You are using an inappropriate policy. Load a new policy from your Policy Server." | The Desktop Policy on the desktop is different from the Desktop Policy specified in **Required Policy for All Desktops**. |
| "Not all network adapters are protected and you are using non-IP protocol which is not protected." | "Not all network adapters are protected and you are using a non-IP protocol which is not protected." | The SecuRemote Client is not bound to all the network adapters, and is using a non-IP protocol. |
| "Not all network adapters are protected." | "Not all network adapters are protected." | The SecuRemote Client is not bound to all the network adapters. |
| "non-IP protocol in use." | "You are using NetBEUI or another non-IP network protocol which is not protected." | The SecuRemote Client is using a non-IP protocol. |

## Enforcing the Desktop Policy

There are several ways in which the system administrator can restrict access to SecureClients.

- Rule Base

  Define a rule with Client Encrypt as the **Action**.

- **Client Encryption Properties** window (FIGURE 11-5 on page 221)

  Select **Apply Rule only if Desktop Configuration Options are Verified**. This feature has no effect on pre-Version 4.1 VPN/FireWall Modules.

In addition, the system administrator can deny a user access by removing the user from the user group.

# SecureClient on the Desktop

## Downloading a Desktop Policy

A Desktop Policy is downloaded to the SecureClient when the SecureClient logs in to the Policy Server, either explicitly or implicitly.

### Explicit Login

The SecureClient user is asked whether to download a Desktop Policy whenever the user adds or updates a site.

#### Adding or Updating Sites

When a user adds or updates a site, the **Download Policy** window (FIGURE 11-9) is displayed.

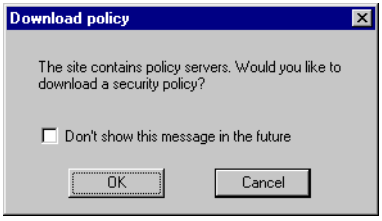



**FIGURE 11-9** Download Policy window

The window is also displayed when the SecuRemote Client is restarted.

Click on **OK** to download a Desktop Policy. The user will be asked to authenticate himself or herself. If the authentication is successful and the user is authorized to download a policy from the Policy Server (that is, the user is a member of the user group specified in the **Policy Server Properties** window — see “Policy Server Properties window” on page 223), a Desktop Policy will be downloaded. If the newly-downloaded Desktop Policy is different from the one currently installed, a message will be displayed (FIGURE 11-10).

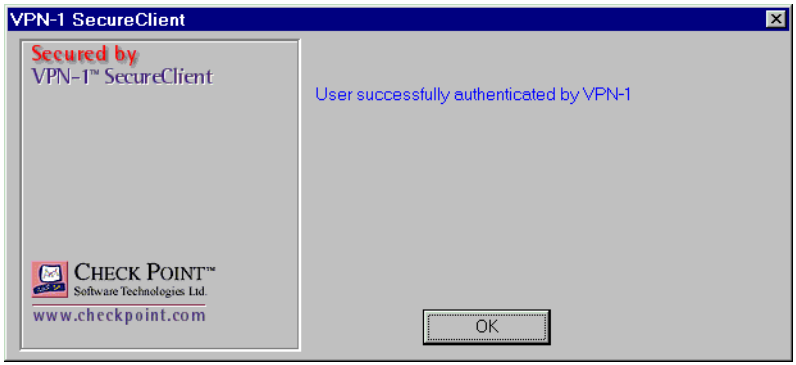



**FIGURE 11-10** SecureClient message

Possible messages (displayed in red) are:

- "The security policy on your computer has been removed."
- "The security policy on your computer has changed."
- "You are not authorized to have a policy."

## Logging in to a Policy Server

When a user selects **Login to Policy Server** from the **Policy** menu, a sub-menu is displayed from which a Policy Server must be selected. The Policy Servers listed (in the format *site*:*PolicyServer*) are those defined for the current site. You cannot login to a Policy Server if its site is disabled in the SecuRemote Client.

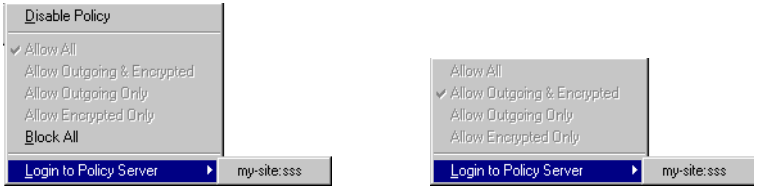



**FIGURE 11-11** Policy menus

The Desktop Policy currently being enforced is marked by a check (✔).

**Note –** Alternatively, right-click on the SecuRemote icon in the Windows system tray and select **Login**, or double-click on the SecuRemote icon.

Choose one of the following from the **Policy** menu:

**Note** – The Desktop Policy currently being enforced is marked by a check (✔).

- **Disable Policy**

  Disable the Desktop Policy, or if it is already disabled, enable it. You will be asked to confirm your action.


**FIGURE 11-12** Warning when you choose Disable Policy

  If you choose **Disable Policy** while there are active encrypted connections, the connections will continue and the change will take effect only after you restart SecuRemote.

  If you later download a Desktop Policy from a Policy Server, the newly-downloaded policy is enabled.

- **Allow All**

  No Desktop Policy is installed on the SecureClient. This option is equivalent to the standard VPN-1 SecuRemote Client.

  This option is always disabled because it cannot be modified by the SecureClient.

- **Allow Outgoing Only**

  Only outbound connections (from the SecureClient) are allowed, except for the following (which are also allowed):

  - ICMP return packets
  - Session Authentication Agent protocol (port 261)

  This option is always disabled because it cannot be modified by the SecureClient.

- **Allow Encrypted Only**

  Only VPN (encrypted) connections are allowed (inbound and outbound).

  If the SecureClient is inside an encryption domain, it is limited to communication with peers inside an internal encryption domain. For example, in FIGURE 11-2 on page 214, BigBen would be able to communicate with FinanceNet but not with Tate.

  This option is always disabled because it cannot be modified by the SecureClient.

- **Allow Outgoing & Encrypted**

  Connections allowed by **Allow Outgoing Only** and **Allow Encrypted Only** are allowed.

  This option is always disabled because it cannot be modified by the SecureClient.

- **Block All**

  Block all connections to the SecuRemote Client machine.

  The Policy Server never installs this policy on the SecuRemote Client machine. You will be asked to confirm your action.

- **Login to Policy Server**

  Select the Policy Server from the sub-menu.

  Select the Policy Server from the list, which includes all the Policy Servers defined for the selected site.

  The policy that you receive or change will remain in effect even if you reboot your computer.

**Note –** A Desktop Policy is installed only on those interfaces on which SecuRemote is also installed and only affects the TCP/IP protocol. Your system administrator may decide to configure the VPN/FireWall Modules to warn you and to limit your access if you have unprotected interfaces and/or protocols.

### Implicit Login

A Desktop Policy is installed automatically when the SecureClient initiates a connection to a site and the user is asked to authenticate himself or herself to a VPN/FireWall Module which is also a Policy Server.

## Boot Policy

When a SecureClient machine on which a Desktop Policy is being enforced boots up, a boot policy allowing only outgoing connections is enforced until the SecureClient Desktop Policy is loaded.

## Logging

SecureClient logs, if any are generated, are written to a text file named `c:\SR.log`, if one exists. The contents of `c:\SR.log` are erased each time the SecuRemote Client is started. You can create an empty `SR.log` file using a text editor.

## IP Forwarding

When the user logs in to the OS, SecureClient checks if IP Forwarding is enabled. If it is enabled, a warning is displayed and SecureClient-specific features are disabled, that is, the SecureClient functions as a SecuRemote Client.

## SecuRemote Icons

TABLE 11-6 shows the SecuRemote icons displayed in the system tray.

**TABLE 11-6** SecureClient System Tray Icons

| Icon | meaning |
|---|---|
|  | standard SecuRemote icon |
|  | Allow out-going and/or encrypted communication. The lock is green. |
|  | **Block All** policy is in effect, but no packet has been dropped recently. |
|  | A packet was dropped while non-trivial policy (**Allow Encrypted Only**, **Allow Out-going Only**, and **Allow Outgoing & Encrypted Only**) is in effect. Information about dropped packets is logged to the local log file (see "Logging" on page 230). The lock is red for about half a second. |
|  | A Desktop Policy is being enforced, and the security of the SecureClient's configuration has been verified by the Policy Server. |
|  | A packet was dropped while in **Block All** policy is in effect. The lock is red for about half a second. |

# userc.c File

## userc.c parameters

The `userc.c` file (located on the Secure Client) contains information about the Secure Client configuration, including site topology. The parameters listed in TABLE 11-7 are defined in the `options` section.

**Warning** – The SecuRemote Client performs minimal syntax checking for the `userc.c` file. If a parameter is entered incorrectly, the site to which it belongs is deleted. No error messages are displayed.

**TABLE 11-7** userc.c parameters

| parameter (default value in parentheses) | meaning |
|---|---|
| `default_ps` | If specified, the IP address (in dot format) of a Policy Server to which the SecureClient will automatically logon upon launch. |

CHAPTER 12

# High Availability for Encrypted Connections

## In This Chapter



## Overview

### The Problem

As enterprises have become more dependent on the Internet for their core applications, uninterrupted connectivity has become more crucial to their success. Beginning with VPN-1/FireWall-1 Version 4.1, encrypted connections are supported in High Availability configurations and can survive failure of a VPN-1/FireWall-1 gateway.

**Note –** For information about High Availability for non-encrypted connections, see "FireWall State Synchronization" on page 557 of *VPN-1/FireWall-1 Administration Guide*.

This chapter describes two example High Availability configurations:

1. Single Entry Point (SEP) — see FIGURE 12-1 on page 235

   In this example configuration, there is a single entry point from the Internet to the internal network, at which two or more gateways are situated.

2 Multiple Entry Points (MEP) — see FIGURE 12-13 on page 244

In this example configuration, there are multiple geographically-separated entry points from the Internet to the internal networks, with a gateway at each entry point. In some cases asymmetric routing issues must be resolved as well.

### The Solution

VPN-1/FireWall-1 High Availability solutions consist of three key elements:

1 A mechanism for detecting gateway failure and redirecting traffic around the failed gateway to a backup gateway.

**Note** – This capability is provided by a third-party solution. For more information about approved third-party solutions, see http://www.checkpoint.com/opsec/guides/ha/index.html.

2 State synchronization between two gateways, so that the backup gateway is able to continue connections that were originally handled by the failed gateway (Single Entry Point configuration only).

3 IP Pools, ranges of IP addresses that a gateway substitutes for the source IP address to ensure correct routing of reply packets (Multiple Entry Points configuration only).

## Single Entry Point (SEP) Example Configuration

### Network Configuration

In this example configuration (FIGURE 12-1 on page 235), the internal VPN-1/ FireWall-1 tables on two or more gateways are synchronized. The gateways are defined as members of a gateway cluster — a group of gateways with many properties in common. If one of the gateway fails, the other gateways takes over the failed gateway's connections.

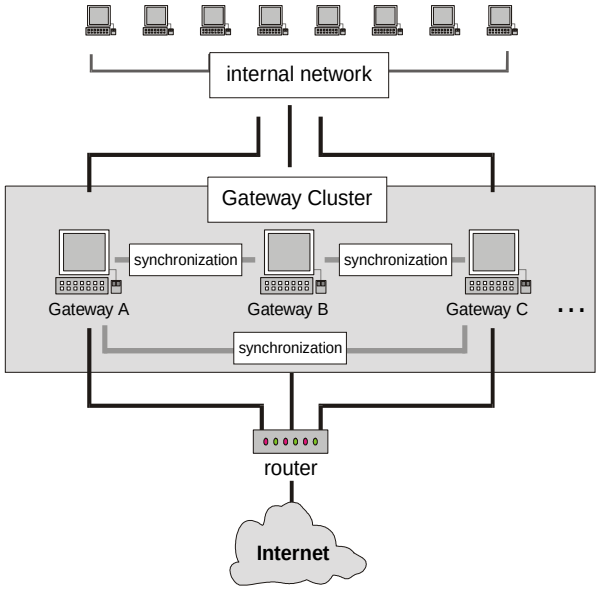



**FIGURE 12-1** Single Entry Point Configuration

## VPN-1/FireWall-1 Configuration (SEP)

To implement a Single Entry Point (SEP) Solution configuration, proceed as follows:

**Warning –** All the gateways in a cluster must have the same OS and the same versions (Version 4.1 or higher) of the same VPN-1/FireWall-1 software modules installed.

### Properties Setup

*1* In the **High Availability** tab of the **Properties Setup** window (FIGURE 12-2 on page 236), check **Enable Gateway Clusters**.

When **Enable Gateway Clusters** is checked, then **Gateway Cluster** becomes available as a menu choice when you click on **New** in the **Network Objects** window (FIGURE 12-3 on page 237).

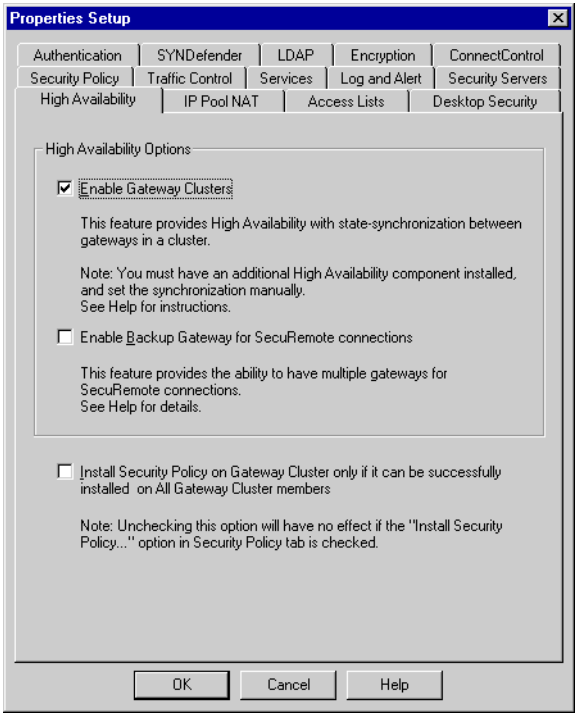



**FIGURE 12-2** Properties Setup — High Availability tab

**2** Check **Install Security Policy on Gateway Cluster only if it can be successfully installed on all Gateway Cluster members** to enforce collective installation of the Security Policy on all the members of a gateway cluster.

Because all the gateways in a cluster must at all times be enforcing the same Security Policy, you have the option of specifying that when a Security Policy is installed on a gateway cluster, then it is either successfully installed on all the gateways in the cluster or it is installed on none of them.

## Gateway Cluster Network Object

***3*** Open the **Network Objects** window (FIGURE 12-3) by:

- choosing **Network Objects** from the **Manage** menu, *or*
- selecting  from the toolbar.

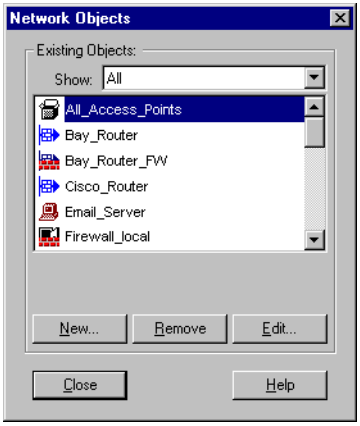



**FIGURE 12-3** Network Objects window

***4*** Click on **New** and select **Gateway Cluster** from the menu.


**FIGURE 12-4** Add Network Object menu

If **Gateway Cluster** is not one of the menu choices in the **Add Network Object** menu, then return to the first step.

The **Gateway Cluster Properties** window (FIGURE 12-5 on page 238) is now displayed.

A gateway is defined as a member of a gateway cluster in the **General** tab of gateway's **Workstation Properties** window (FIGURE 12-10 on page 242) — the "bottom-up" method. In other words, first define the gateway cluster and then assign gateways to the cluster.

The gateways that you will define to be members of this cluster will inherit all the properties defined for the cluster. When you assign a gateway to a gateway cluster, any properties you may have defined for that gateway in the past are overwritten by the properties inherited from the gateway cluster.

### Gateway Cluster Properties Window — General Tab

***5*** In this window, assign a name and an IP address to the cluster.

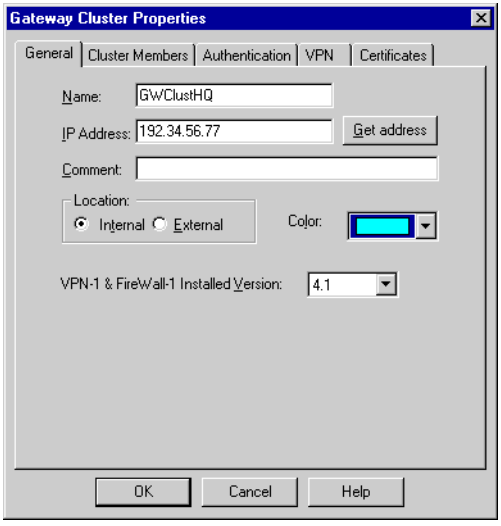



**FIGURE 12-5** Gateway Cluster Properties window — General tab

Assign an IP address to the gateway cluster object in accordance with the instructions provided with the third-party solution.

***6*** Specify **Location**, **Color** and the number of the **VPN-1/FireWall-1 Installed Version**.

### Gateway Cluster Properties Window — Cluster Members Tab

***7*** Click on **Cluster Members** to display the Cluster Members tab (FIGURE 12-6 on page 239).

The **Cluster Members** tab lists the gateways in the cluster. Because you have not yet defined any gateways as members of the cluster, there are at this point no gateways in the list.

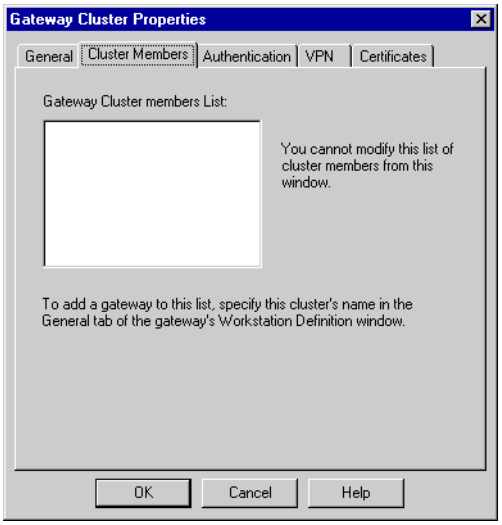



**FIGURE 12-6** Workstation Properties window — empty Cluster Members tab

## Gateway Cluster Properties Window — Authentication Tab

***8*** In the **Authentication** tab (FIGURE 12-7), check the authentication schemes that will be supported on all the gateways in the cluster.

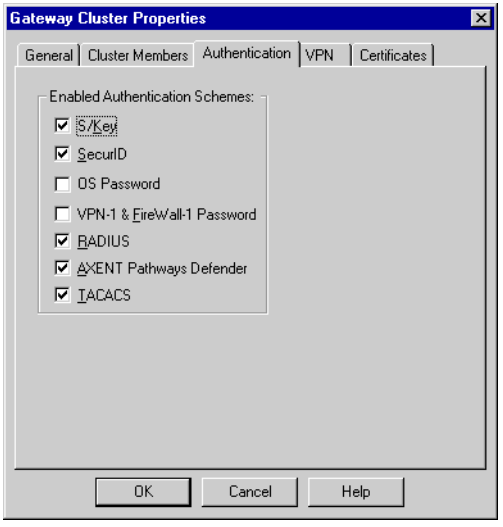



**FIGURE 12-7** Gateway Cluster Properties window — Authentication tab

For information abut authentication schemes, see “Defining the Gateway’s Authentication Schemes” on page 489 of *VPN-1/FireWall-1 Administration Guide*.

## Gateway Cluster Properties Window — VPN Tab

***9*** In the **VPN** tab (FIGURE 12-8) and in the **Encryption Properties** windows you open by clicking on **Edit**, define the encryption methods that will be supported on all the gateways in the cluster. For information about these windows, see “Workstation Encryption Properties” on page 105.

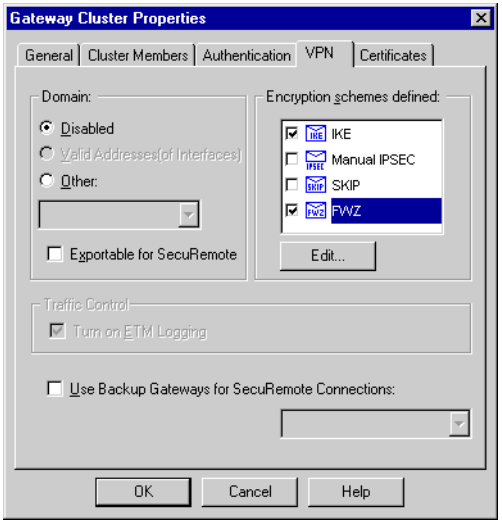



**FIGURE 12-8** Gateway Cluster Properties window — VPN tab

## Workstation Properties Window — Certificates Tab

***10*** In this window (FIGURE 12-9 on page 241), define the gateway cluster’s certificates.

In a SEP configuration, certificates belong to the gateway cluster (that is, to all the gateways in the cluster use the same certificates).

For information about the **Certificates tab** of the **Gateway Cluster Properties** window, see “Generating Certificates” on page 29.

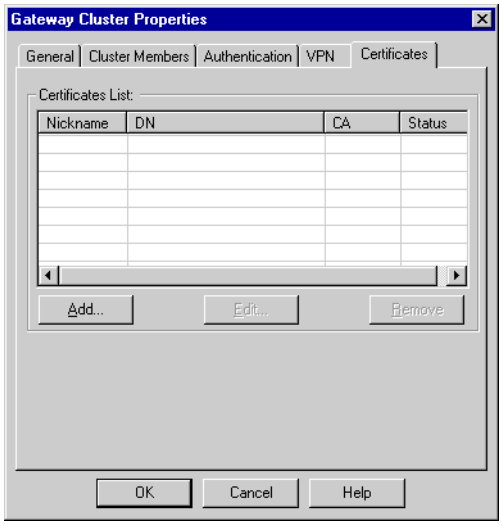



**FIGURE 12-9** Gateway Cluster Properties window — Certificates tab

## Assigning a Gateway to a Cluster

***11*** Now that you have defined the gateway cluster, you can add gateways to the cluster.

**Note –** A FireWall-1 Management Station cannot be a member of a gateway cluster.

***12*** For each cluster member, open the **General** tab of its **Workstation Properties** window (FIGURE 12-10 on page 242).

***13*** Assign an **IP address** to the gateway in accordance with the instructions provided with the third-party solution.

***14*** Select **Gateway** under **Type**.

***15*** Select **VPN-1 & FireWall-1** under **Modules Installed**.

***16*** In **Version**, select Version 4.1 or higher.

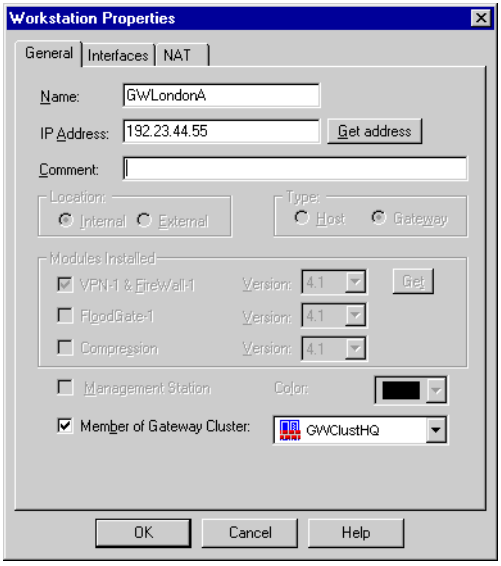



**FIGURE 12-10** Workstation Properties window — General tab of cluster member

**Member of Gateway Cluster** is now enabled.

***17*** Check **Member of Gateway Cluster**.

When **Member of Gateway Cluster** is checked, **Location**, **Type** and **Modules Installed** are disabled. The values in these fields are taken from the **General** tab of the **Gateway Cluster Properties** window (FIGURE 12-5 on page 238).

***18*** Select a gateway cluster object from the drop-down list.

**19** In the **NAT** tab of the gateway's **Workstation Properties** window (FIGURE 12-11), specify whether to implement Network Address Translation for the gateway.

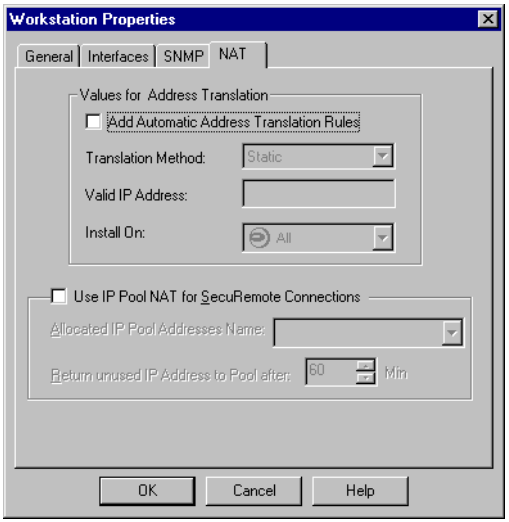



**FIGURE 12-11** Workstation Properties window — NAT tab of cluster member

**20** The **Cluster Members** tab of the **Gateway Cluster Properties** window (FIGURE 12-12) now lists the gateways in the cluster.

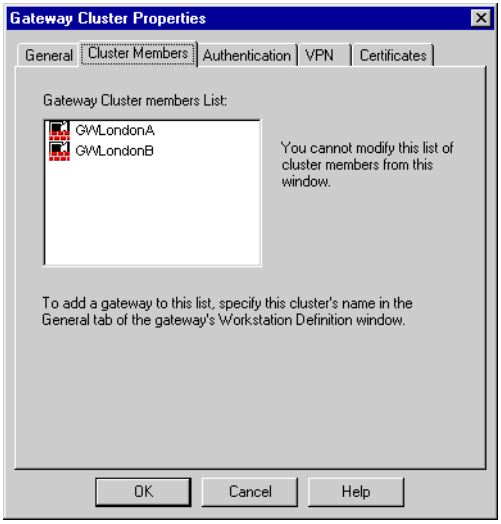



**FIGURE 12-12** Gateway Cluster Properties window — Cluster Members tab

**21** Configure state synchronization between the gateways in the cluster.

See "FireWall State Synchronization" on page 557 of *VPN-1/FireWall-1 Administration Guide* for more information.

# Multiple Entry Point (MEP) Example Configuration

**Warning –** In this release of VPN-1/FireWall-1, the MEP configuration is supported only for SecuRemote connections.

FIGURE 12-13 shows two geographically separated internal networks (each of which is connected to the Internet through its own gateway) that are connected to each other via a dedicated link.

In this configuration, the gateways are too far apart for their states to be synchronized.

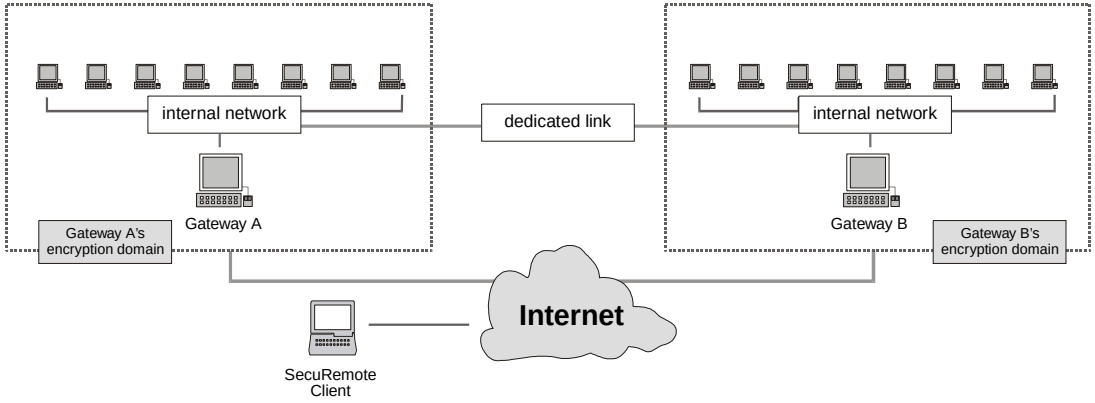



**FIGURE 12-13** Multiple Entry Points Configuration

If Gateway B is defined as a backup for Gateway A (see FIGURE 12-17 on page 249), then when the SecuRemote Client attempts to establish an encrypted connection with one of the hosts in Gateway A's encryption domain, it will first attempt to connect through Gateway A. If Gateway A is unavailable, the SecuRemote Client will then attempt to connect through Gateway B.

**Note –** VPN-1/FireWall-1 does not support configurations in which the encryption domains partially overlap (see "Partial Overlap" on page 157).
This configuration is subject to the problems described under "Reply Packets and Back Connections" and "FWZ Encryption" on page 157.

Two problems can arise in this configuration:

- asymmetric routing

  If a SecuRemote connection is established to a host in Gateway A's internal network through Gateway A, then the reply packets must be routed through Gateway A. If the possibility exists that the reply packets will be routed to the Internet through Gateway B, then IP Pools can be used to ensure that this does not happen.

An IP Pool is a range of (usually illegal) IP addresses from which Gateway A chooses IP addresses to substitute for the SecuRemote Client's source address. The IP Pool addresses are routable to Gateway A, so that reply packets from the host return to Gateway A, which restores the SecuRemote Client's source address. Once an IP Pool address has been assigned to a SecuRemote Client, all subsequent connections to that SecuRemote Client will use the same IP Pool address.

You should define IP Pools for both Gateway A and Gateway B. There should be no overlap in the IP addresses of the IP Pools.

- High Availability

  If Gateway A fails, its open connections SecuRemote connections fail. After a short delay, new SecuRemote connections (with SecuRemote Version 4.1 and higher Clients) are routed through Gateway B.

# VPN-1/FireWall-1 Configuration (MEP)

To implement VPN-1/FireWall-1 for the Multiple Entry Point (MEP) Solution configuration, proceed as follows:

## Properties Setup

1 In the **High Availability** tab of the **Properties Setup** window (FIGURE 12-14), check **Enable Backup Gateway for SecuRemote Connections**.

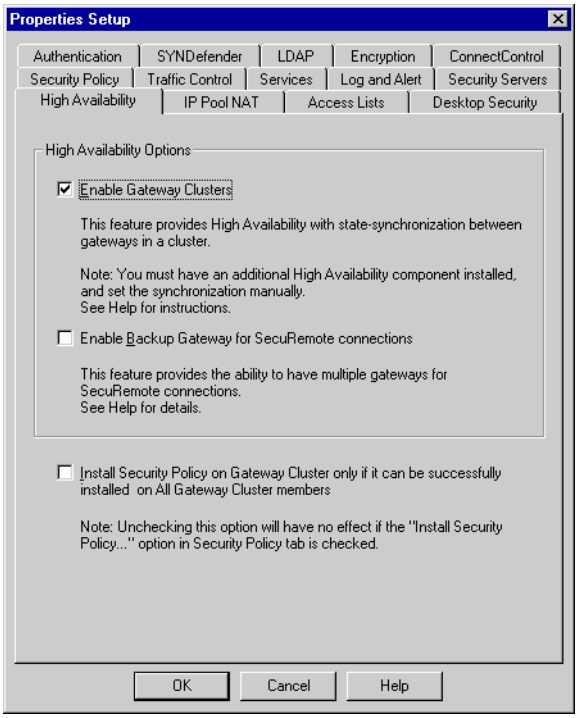



**FIGURE 12-14** Properties Setup — High Availability tab

2 If you will be using IP Pools, then open the **IP Pool NAT** tab of the **Properties Setup** window (FIGURE 12-15 on page 247).

If you will not be using IP Pools, then proceed to step 4 on page 248.

**3** Check **Enable IP Pool NAT for SecuRemote Connections**.

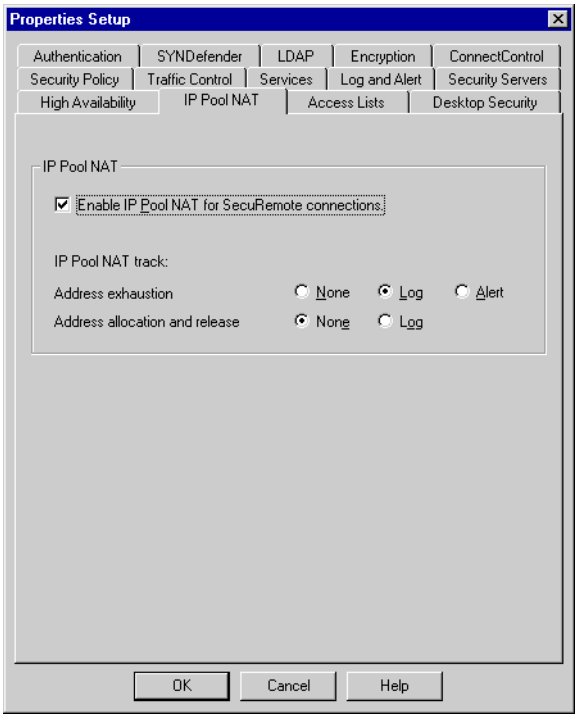



**FIGURE 12-15** Properties Setup — IP Pool NAT tab

The IP Pool NAT Track options will now be enabled. See “IP Pools” on page 249 for information about IP Pools.

**Address Exhaustion** — Specify the action to take if the IP Pool is exhausted.

**Address Allocation and Resource** — Specify whether to log each allocation and release of an IP address from the IP Pool.

## Workstation Properties

**4** In the **NAT** tab of the gateway's **Workstation Properties** window, check **Use IP Pool for SecuRemote Connections**.

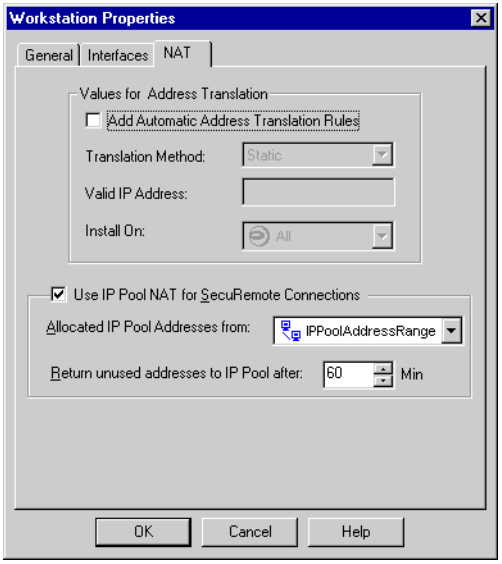



**FIGURE 12-16** Workstation Properties window — NAT tab

**5** In **Allocated IP Pool Addresses from**, select the network object (an Address Range, network or a group of one of these objects) whose IP addresses will serve as the IP Pool's IP addresses.

**6** In **Return unused IP addresses to Pool after**, set the time period during which an IP Pool address will remain assigned to a SecuRemote Client even after all open connections have ended.

7 If you wish to implement MEP High Availability, then in the **VPN** tab of Gateway A's **Workstation Properties** window (FIGURE 12-17), define Gateway B as Gateway A's backup gateway.

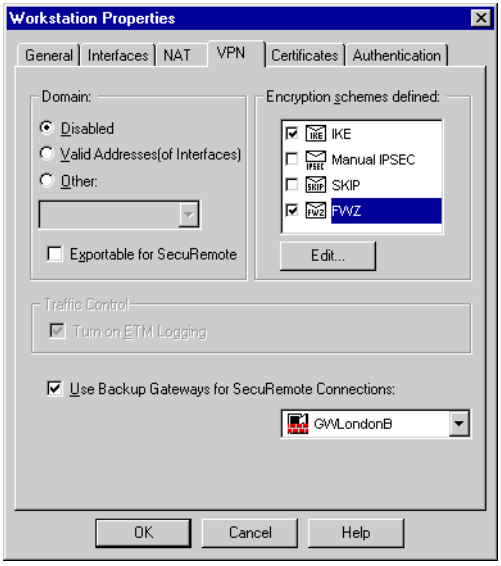



**FIGURE 12-17** Workstation Properties window — Encryption tab showing backup gateway

To specify more than one backup gateway, use group objects.

# IP Pools

An IP Pool is a range of IP addresses (an Address Range, a network or a group of one of these objects) routable to the gateway. When a connection is opened to a host, the gateway substitutes an IP address from the IP Pool for the source IP address. The IP Pool addresses must be routable to the gateway, so that reply packets from the host return to the gateway, which restores the original source IP address and forwards the packets to the source.

The IP addresses in an IP Pool are usually illegal. If the IP addresses are legal addresses in the local network, you must use the proxy ARP method to configure the routing so that reply packets are routed back to the gateway. For information on the proxy ARP method, see "Ensuring That the Packet Reaches the Gateway" on page 435 of *VPN-1/FireWall-1 Administration Guide*.

## Enabling IP Pools

To enable the IP Pool option, check **Enable Backup Gateway for SecuRemote Connections** in the **IP Pool NAT** tab of the **Properties Setup** window (FIGURE 12-15 on page 247), and set the IP Pool parameters (see step 2 on page 246).

## Associating an IP Pool with a Gateway

To associate an IP Pool with a gateway, open the **NAT** tab of the gateway's **Workstation Properties** window (FIGURE 12-16 on page 248), check **Use IP Pool NAT for SecuRemote Connections** and set the parameters (see "Workstation Properties" on page 248).

You can now use IP Pools for SecuRemote connections.

## Load Balancing or High Availability

You can also use IP Pools in a VPN to prevent asymmetric routing in a Load Balancing or High Availability configuration, as follows:

1. Enable IP Pools (see "Enabling IP Pools" on page 249).
2. Associate an IP Pool with the gateway (see "Associating an IP Pool with a Gateway" above).
3. In the `objects.C` file, add the property `:ip_pool_vpn (true)` to the gateway.

IP Pools will also be enabled for SecuRemote connections (see step 4 on page 248).

CHAPTER 13

# FWZ Encryption Protocol

## In This Chapter



## Virtual Encryption Session (FWZ)

Following is a detailed description of the FWZ encryption scheme, based on FIGURE 13-1.

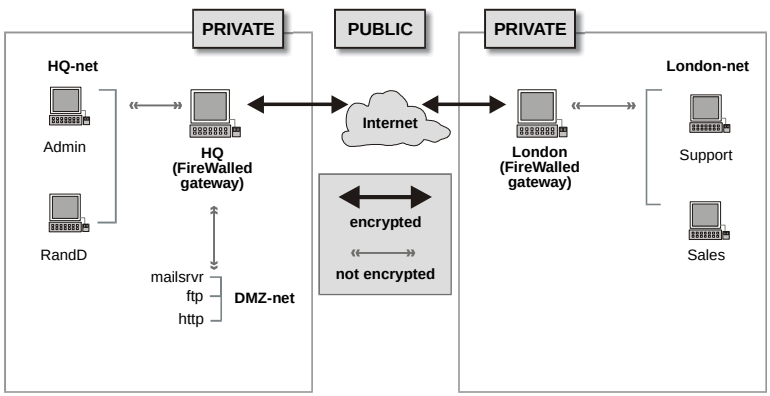



**FIGURE 13-1** Two Gateway Network Configuration

Suppose Admin (one of the hosts in HQ's encryption domain) initiates an SMTP session with Support (one of the hosts in London's encryption domain).

1. When the first SMTP packet reaches HQ, HQ inspects its Rule Base and determines that the session must be encrypted, and that the source address (Admin) is in its own encryption domain.
2. HQ searches the VPN-1/FireWall-1 network objects database and finds that the destination address (Support) is in London's encryption domain.
3. HQ notifies London that an encrypted session is to take place between them.
4. HQ and London compute a secret Basic Session Key (BSK) using the scheme described above (see "Public Key Schemes" on page 20).
5. HQ and London conduct a secured key exchange protocol during which they agree on a randomly generated session key (a DES or FWZ1 key, depending on the relevant rule's properties) for the encrypted SMTP session, which then begins.

The TCP/IP packet headers are not encrypted, to ensure that the protocol software will correctly handle and deliver the packets. The cleartext TCP/IP header is combined with the session key to encrypt the data portion of each packet, so that no two packets are encrypted with the same key. A cryptographic checksum is embedded in each packet (utilizing otherwise unused bits in the header) to ensure its data integrity.

Encryption is in–place. A packet's length remains unchanged, so the MTU remains valid and efficiency is not compromised. Key management and encryption are secure, completely integrated, and transparent to the user.

## FWZ Key Hierarchy

TABLE 13-1 shows the hierarchy of FWZ encryption keys. The system administrator configures the first two keys (Certificate Authority and Encryption). The other keys are automatically generated by VPN-1/FireWall-1 for each Virtual Encryption Session.

The Basic Session Key is derived from the Diffie-Hellman key when the Virtual Encryption Session begins, using the mechanism depicted in FIGURE 2-1 on page 21. The Session Key is randomly generated and encrypted using the Basic Session Key in

accordance with the encryption method — DES or FWZ1 — specified for the rule. The Packet Key is derived by combining the Session Key with some bytes of the TCP/IP header, so that no two packets are encrypted with the same key.

**TABLE 13-1** FWZ Key Hierarchy

| key | managed by | type | associated with | comments |
|---|---|---|---|---|
| Certificate Authority (CA) key | CA | RSA public key (512 bits) | Management Station or external CA | used to authenticate the communication of a gateway's public encryption key |
| Encryption key | user | Diffie-Hellman public key (512 bits) | gateway | used to generate the Basic Session Key |
| Basic Session Key (BSK) | automatically generated when the session begins | shared Diffie-Hellman secret key (512 bits) | gateway pair | used to encrypt the Session Key |
| Session Key (SK) | automatically generated | depends on the encryption algorithm | session | randomly generated, encrypted using the BSK |
| Packet Key | automatically generated | depends on the encryption algorithm | packet | combination of the Session Key and IP header |

# Examples

In the examples that follow, the gateways are named Alice and Bob.

After an encryption connection has been established, both gateways encrypt outgoing packets and decrypt incoming packets, so the distinction between the encrypting gateway (Alice) and the decrypting gateway (Bob) is relevant to the direction of the first packet only. It may be more accurate to speak of the "initiating" and "receiving" gateways, but for the sake of simplicity the terms "encrypting" and "decrypting" will be used throughout this discussion.

The encryption protocol takes place between two peer gateways whenever a new connection that the Rule Base indicates must be encrypted is established. The encryption protocol itself consists of the usual two packets: a request for encryption sent by Alice and the reply returned by Bob. However, if either of the gateways has an out-of-date version of the other gateway's key, then an automatic update protocol may take place as part of the encryption protocol. In this case, the encryption protocol would include as many as four (4) packets in all.

# Basic Encryption (Session Key Exchange) Protocol

## Actions Performed by Alice

1. The protocol is initiated by Alice when VPN-1/FireWall-1 receives the first packet of a connection that the Rule Base indicates must be encrypted. Alice holds this packet and initiates the encryption protocol for the connection.

2. The protocol software on Alice examines the source and destination addresses to see if they are in its encryption domain.

   The usual case is that the source address is in Alice's encryption domain but the destination address is not.

3. Alice then searches the VPN-1/FireWall-1 network objects database for a gateway which has the destination address in its encryption domain.

   In this example, Alice finds that Bob is that gateway.

4. Alice then retrieves Bob's public key from the database and sends Bob a normal encryption request RDP packet.

**Note –** RDP (Reliable Data Protocol) is an internal VPN-1/FireWall-1 protocol.

The RDP request packet contains:

- a suggestion for Alice's public key
- possible suggestions for Bob's public key
- suggestions for the session key encryption method
- suggestions for the data encryption method

5. The RDP request packet is sent to the original destination address, on the assumption that Bob is along the route to that address and will intercept the packet.

   The RDP request packet is not sent directly to Bob because there may be more than one gateway with the destination in its encryption domain.

## Actions Performed by Bob

1. VPN-1/FireWall-1 on Bob intercepts the RDP request packet sent by Alice, which contains the parameters of the original connection packet.

   Bob examines the destination address to check whether it is in Bob's encryption domain. If it is not in Bob's encryption domain, then Bob simply ignores the packet and passes it on.

2. Bob checks its Rule Base to see whether the connection must be encrypted.

3. Bob examines the source address to see if it is in Alice's encryption domain.

4 Bob compares Alice's key suggestion for itself to Bob's version of Alice's key, and Alice's key suggestion for Bob to Bob's version of its own key.

If they match, then Bob generates a random session key and encrypts it using the common Basic Session Key obtained from the Diffie-Hellman computation (see "Public Key Schemes" on page 20), or from a cache, if it was computed previously.

5 Bob sends the session key to Alice in Bob's RDP reply.

This step ends the RDP protocol, from Bob's point of view.

### Actions Performed by Alice on Receipt of Bob's Reply

1 VPN-1/FireWall-1 on Alice receives and verifies Bob's reply.

The verification consists of decrypting and checking the session key.

2 If the verification is successful, then Alice installs the session key for the connection.

3 Alice encrypts the original first packet and sends it to its destination.

## Extended Encryption Protocol (Automatic Key Update)

In the extended protocol, one gateway (Alice or Bob, or even both) may discover that it does not have a key for the peer, or that the key is out-of-date. In this event, the gateway will try to obtain a new key from the peer, provided that it has a key for the peer's Certificate Authority.

For example, suppose that Alice discovers — while preparing the RDP packet — that it does not have a key for Bob. If Alice has the public key of Bob's CA, Alice will ask Bob for its (possibly new) key, signed by Bob's CA.

Since all VPN-1/FireWall-1 gateways have (or can obtain) this signature, Bob can supply his signed key to Alice. Alice then verifies the signature and installs Bob's key.

CHAPTER 14

# Troubleshooting

## In This Chapter



# General Troubleshooting Procedures

## Preventing Common Problems

### IPSec and IKE

It is crucial that the computer's host name correspond to the IP address of its external interface's IP address. If this is not so, IPSec packets will carry the internal interface's non-routable IP address, and reply packets will not be routed back to the computer.

You can find out the IP address that corresponds to the hostname as follows:

#### Unix

The IP address is given in the response to the `hostname` command.

#### NT

1. From the Control Panel, double-click on **Network**.
2. In the **Network** window, click on the **Protocols** tab.
3. Select **TCP/IP** and click on **Properties**.
4. In the **Microsoft TCP/IP Properties** window, click on **DNS**.
   The computer's name is in **Host Name**.
5. From a command window, `ping` the name in **Host Name**.
   The response to the `ping` command should show a resolvable legal IP address.

### SKIP

SKIP requires that clocks be synchronized to a difference of no more than 1 hour.

## Examining the Log

Whenever there is a problem in the encryption protocol, the result is that the connection will either hang, or be dropped or rejected by one of the gateways.

The first step in troubleshooting should be to examine the log. Of course, the log will show information about the connection only if logging is specified for the encryption rule in the Rule Base.

If an encrypted connection is successfully established, the log shows an **Encrypt** entry for Alice and a **Decrypt** entry for Bob.

If the encryption protocol fails, then the log shows a **Reject** action for Alice. The **Info** field then has an error message of the form:

```
Encryption Failure : <error diagnostic>
```

In addition, the encryption scheme and the methods are given.

There is usually also a similar entry for Bob, with the **Info** field showing an error message of the form:

```
Decryption Failure : <error diagnostic>
```

## Configuration

In the examples that follow, the encryption is of a TELNET session between the hosts Arthur and Betty, configured as shown in FIGURE 14-1.

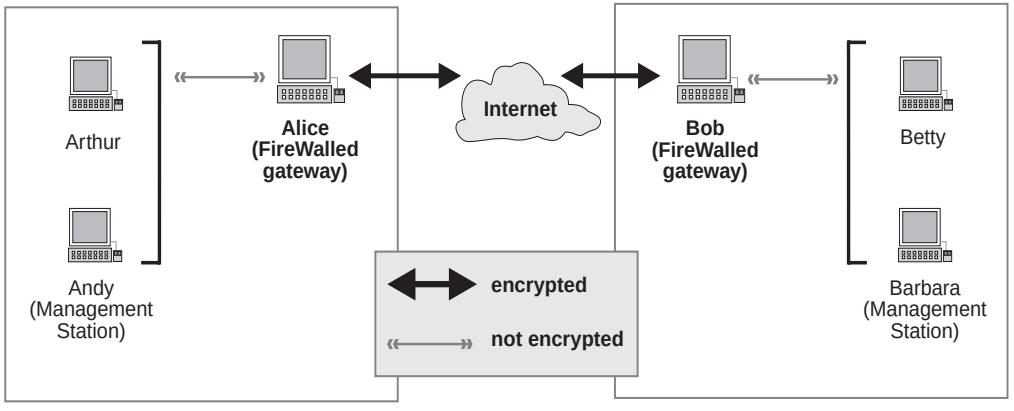



**FIGURE 14-1** Network Configuration for Troubleshooting Examples

# Encryption Error Messages

## Basic Encryption Protocol

### Errors Reported by Alice (Encrypting Gateway)

The messages in this group are reported by Alice (the encrypting gateway), and the problems and their solution are to be found in Alice's database.

The solution usually consists of correcting a configuration error on Alice's Management Station (Andy in this example) and downloading the corrected Security Policy to Alice. It is sometimes sufficient to download just the database.

**TABLE 14-1** Errors reported by Alice (Encrypting Gateway)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| All | There is no encryption error message, but there is some other log entry for the connection. | Alice did not try to encrypt the connection. | Check the rule number in the log and determine which rule was applied instead of the encryption rule, and why. |
| All | "Neither source nor destination is in my domain" | A rule specifies encryption, but the gateway is responsible for neither source nor destination. | Correct the Rule Base and/or the gateway's Encryption Domain. |
| All | "Gateway connected to both endpoints" | A rule specifies encryption, but the same gateway is responsible for both source nor destination. | Correct the Rule Base and/or the gateway's Encryption Domain. |
| All | "I (Alice) don't have a network object" | Alice is not defined in the database. | Correct Alice's database |
| All | "Rule peer gateway *gateway name* does not match destination" | The gateway defined in the rule as **Peer Gateway** does not include the destination in its Encryption Domain. | Correct Alice's database. |
| All | "No peer gateway found for the destination" | Alice did not identify Bob as the gateway responsible for the connection to Betty. In other words, in Alice's database, Bob's Encryption Domain is incorrectly defined. | Correct Alice's database. |
| All | "unknown scheme" | VPN-1/FireWall-1 does not support this scheme. | Contact your VPN-1/FireWall-1 support representative. |
| IKE | "Peer does not support IKE" | Bob does not support IKE. | Correct Bob's configuration. |
| IKE | "I don't support IKE" | Alice does not support IKE. | Correct Alice's configuration. |

**TABLE 14-1** Errors reported by Alice (Encrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| IKE | "No matching encryption/hash methods between myself and peer" | There are no encryption or hash methods supported by both Alice and Bob. | Correct Alice's and/or Bob's configuration. |
| IKE | "Certificate's Subject ID does not match peer's ID *id*" | The Subject ID in Bob's certificate is different from Bob's ID.<br>*id* is the subject ID in Bob's certificate. | Confirm that the match certificate criteria (in the **Public Key Configuration** window) are correct. If they are, the certificate may be forged. |
| IKE | "Peer's certificate invalid: *text*" | Bob's certificate is invalid.<br>*text* is the reason that the certificate is invalid. | Bob must obtain a valid certificate. The certificate Bob presented may have been tampered with or used by an eavesdropper. |
| IKE | "No response from peer: scheme IKE" | Bob did not respond to Alice's IKE negotiation messages. | Confirm that `fwd` and `isakmpd` are running on Bob (both are started by `fwstart`). |
| IKE | "IKE daemon: no 'encryption', 'des', or 'IKE' license" | The IKE daemon (`isakmpd`) cannot execute because of a license problem. | Obtain and install a valid license. |
| IKE | "Cannot read the methods from the rule" | The relevant rule's Rule Encryption Properties have not been defined. | Define the rule's Rule Encryption Properties and set the methods. |
| IKE | "Cannot communicate with the IKE daemon" | The FireWall daemon (`fwd`) is unable to communicate with the IKE daemon (`isakmpd`). | The IKE daemon may not be running, or there may be another process listening on UDP port 500. Run `fwstop`, kill the other process, and run `fwstart`. |
| IKE | "Error: IKE signing key cannot be found" | VPN-1/FireWall-1 did not find the RSA signing key in its database. | Generate a signing key for Alice in the **IKE Public Key Configuration** window. |
| IKE | "Error: IKE certificate cannot be found" | VPN-1/FireWall-1 did not find the IKE signing key certificate in its database. | Obtain a certificate for Alice in the **IKE Public Key Configuration** window. |
| IKE | "Error: IKE CA's certificate cannot be found" | VPN-1/FireWall-1 did not find the IKE signing key certificate in its database. | Generate a signing key for Alice in the **IKE Public Key Configuration** window. |

**TABLE 14-1** Errors reported by Alice (Encrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| IKE | "Error: IKE certificate not valid: *text*" | The certificate in the database is invalid. Future IKE negotiations using signature authentication mode will fail. *text* specifies the reason. | Generate a new certificate for Bob in the **Public Key Configuration** window. |
| IKE | "Warning: IKE certificate not valid: *text*" | Failed to check the validity of Bob's certificate in the database. Future IKE negotiations using signature authentication mode may use the certificate. *text* specifies the reason. | Confirm that the cms daemon and your PKI are running. Confirm that VPN-1/FireWall-1 can communicate with the PKI. |
| IKE | Received Notification from Peer: *text* | Bob sent Alice an IKE notification. *Text* is the content of the message. | The different *text* messages are detailed below. |
| IKE | Received Notification from Peer: no proposal chosen | Bob's IKE configuration differs from Alice's, which is why Bob rejects Alice's proposal. Bob may also not support the parameters offered by Alice. This can only happen if Alice and Bob have different policies installed (for example, belong to different vendors, or controlled by different management stations). | Confirm that the IKE properties configured for Alice and Bob match (Encryption Method, Hash Method, Authentication Method, Aggressive Support Mode). Confirm that the IKE parameters in the matching rule are supported by Bob. |
| IKE | Received Notification from Peer: invalid exchange type | IKE interoperability problem. This may also be a synchronization problem. | Restarting the negotiation may solve the problem. If not, contact your VPN-1/FireWall-1 support representative. |
| IKE | Received Notification from Peer: invalid cert encoding | IKE interoperability problem. Bob does not accept the format of the certificate/CRL sent by Alice in the negotiation. | Contact your VPN-1/FireWall-1 support representative. |

**TABLE 14-1** Errors reported by Alice (Encrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| IKE | Received Notification from Peer: Invalid certificate | Bob cannot validate Alice's certificate | Check which certificate is sent to Bob (appears in `IKE.elg` or `fwd.elg`); check the validity time of this certificate; check if Bob is assumed to accept this certificate (that is, that he trusts the CA of the certificate sent); check if the CRL repository is up and running; check that the repository is accessible from Bob's machine (for example, by ping) and that it can be accessed according to Bob's Security Policy. |
| IKE | Received Notification from Peer: Bad certificate request syntax | IKE Interoperability problem. | Examine the format of the certificate request sent by Bob (in `IKE.elg`). Contact your VPN-1/FireWall-1 support representative. |
| IKE | Received Notification from Peer: authentication failed | Bob could not authenticate the identity of Alice. | Confirm that Bob and Alice have the same IKE pre-shared secret configured (when used). |
| IKE | Received Notification from Peer: notify sa lifetime | Bob notifies Alice that he is using a different life time for the IKE Security Association. | This is not a problem. |
| IKE | Received Notification from Peer: invalid id information | This is either an IKE interoperability problem, or Alice offered Bob subnets as ID's in an IKE negotiation while Bob is configured not to support subnets. | To Confirm that this is a subnet support problem you may consult the log produced by Bob. Either check **Support Subnet** in Bob's IKE Properties window, or change Alice's configuration so as not to support subnets. If this is not a subnet support problem, contact your VPN-1/FireWall-1 support representative. |

**TABLE 14-1** Errors reported by Alice (Encrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| IKE | Received Notification from Peer: payload malformed | May be an IKE interoperability problem. Typically this message appears when using a wrong IKE pre-shared secret. This can also happen if an IKE packet did not arrive properly. | If pre-shared secret is the authentication method being used, confirm that Alice and Bob are configured for the same IKE pre-shared secret. If not, and this message appears often, contact your VPN-1/FireWall-1 support representative. |
| IKE | Received Notification from Peer: invalid payload type/ DOI not supported/ situation not supported/ invalid cookie/ invalid major version/ invalid minor version / invalid flags/ invalid message id/ invalid protocol id/ invalid spi/ invalid transform id/ attributes not supported/ bad proposal syntax / invalid key information/ invalid hash information / invalid signature / unsupported exchange type/ unequal payload lengths/ invalid cert authority/ certificate unavailable | IKE interoperability problem. The two vendors are apparently not compatible, and cannot communicate using IKE. | Contact your VPN-1/FireWall-1 support representative. |
| IKE | decryption error | Alice could not decrypt an encrypted IKE packet. The packet may have been sent by a malicious adversary or this may be an IKE interoperability problem. | If this happens often, contact your VPN-1/FireWall-1 support representative. |
| IKE | Sent Notification: *text* | Alice sent Bob an IKE notification. *text* is the content of the message. | The different *text* messages are detailed below. |

**TABLE 14-1** Errors reported by Alice (Encrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| IKE | Sent Notification: no proposal chosen | Bob's IKE configuration differs from Alice's, which is why Alice rejects Bob's proposal. Alternately, Bob may have offered proposals with parameters not supported by the VPN/FireWall Module. This can only happen if Alice and Bob have different policies installed (for example, belong to different vendors, or controlled by different management stations). | Confirm that the IKE properties configured for Alice and Bob match (Encryption Method, Hash Method, Authentication Method, Aggressive Support Mode). |
| IKE | Sent Notification: invalid payload type/ DOI not supported/ situation not supported/ invalid cookie/ invalid major version/ invalid minor version/ invalid flags/ invalid message id/ invalid protocol id/ invalid spi/ invalid transform id/ attributes not supported/ bad proposal syntax / invalid key information/ invalid id information/ invalid hash information/ invalid signature/ notify sa lifetime/ unsupported exchange type/ unequal payload lengths | Interoperability problem. The two vendors are apparently not compatible, and cannot communicate using IKE. | Contact your VPN-1/FireWall-1 support representative. |
| IKE | Sent Notification: invalid exchange type/ payload malformed | IKE Interoperability problem. This may also be a synchronization problem | Restarting the negotiation may solve the problem. If not, contact your VPN-1/FireWall-1 support representative. |
| IKE | Sent Notification: invalid cert encoding/ invalid certificate/ bad cert request syntax/ invalid cert authority/ certificate unavailable | Alice had a problem with what Bob sent as certificate information. | This message is accompanied by a more detailed message describing the problem. |

**TABLE 14-1** Errors reported by Alice (Encrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| IKE | Sent Notification: no subnet support in ike negotiations | Bob offered Alice subnets as ID's in an IKE negotiation. Alice is configured not to support subnets. (The real notification sent is "invalid id information") | Either check **Support Subnet** in Alice's **IKE Properties** window, or change Bob so as not to support subnets. |
| IKE | Sent Notification: authentication failed | Alice could not authenticate the identity of Bob. | Confirm that Alice and Bob have the same IKE pre-shared secret configured (when used). |
| IKE | Sent Notification: Client Encrypt Notification | A SecuRemote user was notified of a problem using IKE. | The SecuRemote user is informed of the problem, and of a suggested course of action. |
| IKE | Sent Notification: payload malformed - possibly a mismatch in pre-shared keys | The decryption of the first encrypted IKE packet failed. This can be an interoperability problem, but is also typical for a mismatch in pre-shared secret (since this is the first place the shared secret is used). | Confirm that Alice and Bob are configured for the same IKE pre-shared secret. |
| IKE | Send Delete SA to Peer | This happens when Alice receives an IPSEC packet, which is encrypted using a Security Association that doesn't exist for Alice. It can happen when Alice and Bob are out of synchronization. Normally, Bob will receive this notification and stop using the old Security Association. | This is not a problem. |

**TABLE 14-1** Errors reported by Alice (Encrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| IKE | Received Delete SA from Peer | This happens when Bob receives an IPSEC packet, which is encrypted using a Security Association that doesn't exist for Bob. Bob may send this notification also as an informatory message, just to let Alice know that a Security Association has expired. It can happen when Alice and Bob are out of synchronization, or when Bob has an IKE implementation which sends this message every time a Security Association expires. Normally, Alice will receive this notification and stop using the old Security Association. | This is not a problem. |
| IKE | FW-1 IKE daemon: failed opening socket, exiting. | The IKE daemon on Alice failed to open a connection to other IKE implementations, probably due to insufficient system resources. | In some cases rebooting the machine might solve the problem. Contact a system administrator or your VPN-1/FireWall-1 support representative. |
| IKE | FW-1 IKE daemon: failed binding IKE socket | The IKE daemon on Alice failed to use the IKE socket address. There may not be enough resources or the right permissions to complete this operation. | In some cases rebooting the machine might solve the problem. Contact a system administrator or your VPN-1/FireWall-1 support representative. |
| IKE | no shared secret for myself and peer (Bob) | No pre-shared secret is configured on Alice for Alice and Bob. | Correct the configuration on Alice. |
| IKE | no common authentication methods between myself and peer (Bob) | Alice and Bob are configured to use different authentication methods. | Correct the configuration on Alice. |
| FWZ, SKIP | "Peer (Bob) has neither CA nor key" | There is no key information for Bob defined in Alice's database. | Correct Alice's database. Obtain a key for Bob. |
| FWZ, SKIP | "I (Alice) have no private key" | Alice has no private key defined. | Generate a key for Alice. |

**TABLE 14-1** Errors reported by Alice (Encrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| FWZ | "Peer (Bob) failed to reply" | Bob did not reply to Alice's encryption request. | There are several possible causes for this failure:<br>■ Check if VPN-1/FireWall-1 is running on Bob.<br>■ Check Bob's log for errors. If Bob is managed by a remote organization, this step may require coordination with Bob's system administrator. |
| FWZ | "Illegal peer reply" *or* "Peer (Bob) failed to authenticate its reply" | This should never happen. The message indicates that Bob's reply is not in the correct format, or that its cryptographic signature is incorrect. | Bob's reply may have been tampered with. |
| FWZ | "Failed to generate shared key" *or* "Session key installation failed" | Internal VPN-1/FireWall-1 error. | Contact your VPN-1/FireWall-1 support representative. |
| FWZ | *"CA name* has no CA key." | | Correct the database. |
| IKE, SKIP, Manual IPSec | "No encryption license" | You are attempting to use encryption without a license | Obtain and install a valid license. |
| IKE, SKIP, Manual IPSec | "No scheme license" | You are attempting to use an encryption scheme for which you have no license. | Obtain and install a valid license. |
| SKIP | "Failed to compute a shared secret" | A key for one of the sides is either missing or has expired. | Check that both keys are defined and valid. |
| Manual IPSec | "Source/Destination is not a manual key manager" | One of the sides is not defined as a manager of manual keys. | Check **Manual IPSec** in the **Encryption** tab of the **Workstation Properties** window (FIGURE 8-1 on page 102). |

## Errors Reported by Bob (Decrypting Gateway)

The messages in this group are reported by Bob (the decrypting gateway), and the problems and their solution are to be found in Bob's database.

The solution usually consists of correcting a configuration error on Bob's Management Station (Barbara in this example) and downloading the corrected Security Policy to Bob. It is sometimes sufficient to download just the database.

**TABLE 14-2** Errors reported by Bob (Decrypting Gateway)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| IKE, SKIP, Manual IPSec | "No encryption license" | You are attempting to use encryption without a license | Obtain and install a valid license. |
| IKE, SKIP, Manual IPSec | "No scheme license" | You are attempting to use an encryption scheme for which you have no license. | Obtain and install a valid license. |
| IKE | "Peer uses wrong methods" | Alice has sent an encrypted packet with the wrong IKE methods. | Correct Alice's configuration. |
| SKIP | "Failed to compute a shared secret" | A key for one of the sides is either missing or has expired. | Check that both keys are defined and valid. |
| Manual IPSec | "Source/Destination is not a manual key manager" | One of the sides is not defined as a manager of manual keys. | Check **Manual IPSec** in the the **Encryption** tab of the **Workstation Properties** window (FIGURE 8-1 on page 102). |
| SKIP | "Rule NSID differs from packet NSID" | There is a mismatch in NSID types. | Correct the Rule Base so that the NSID matches on both sides of the connection. |
| SKIP | "Mismatch between rule and packet Kij/Crypt/Auth methods". | There is a mismatch in methods. | Correct the Rule Base so that the methods match on both sides of the connection. |
| SKIP | "Source/Destination object not in database" | A SKIP packet has been received from an unknown SKIP gateway. | If required, define the unknown SKIP gateway in the database. |
| SKIP | "Cannot find Source/Destination key hash in database" | Cannot locate the SKIP DH key. | Define the key. |
| SKIP | "Packet Source KeyID (*keyid*) does not match database KeyID" | The peer is using a SKIP key different from the one in the database. | Update the peer's SKIP key. |
| SKIP | "Packet Destination KeyID (*keyid*) does not match database KeyID" | Peer does not have Bob's correct key. | Inform peer of Bob's correct key. |

**TABLE 14-2** Errors reported by Bob (Decrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| SKIP | "NSID 1 source address mismatch" | The NSID 1 KeyID (IP address) does not match the peer's IP address. | Inform the peer. |
| SKIP | "NSID 1 destination address is not mine" | The peer is using an incorrect IP address for the NSID 1 key. | Inform the peer. |
| Manual IPSec | "Couldn't get SPI data" | Bob received a packet with an unknown SPI. | Define the SPI that the peer is using. |
| FWZ | "Matching rule is not FWZ" | The rule that matches the RDP request specifies a non-FWZ encryption scheme. | Correct the database. |
| FWZ | "Mismatching/Illegal encryption method" | The RDP request asks for an unsupported encryption scheme, or does not match the methods in the relevant rule. | Correct the Rule Base. |
| FWZ | "Matching rule does not encrypt" | The relevant (matching) rule does not allow encryption. | Correct the Rule Base. |
| FWZ | There are no log entries. | Bob thinks that Betty is not in Bob's **Encryption Domain**, and ignored Alice's RDP request packet, assuming that there is another gateway behind Bob that will handle the request. | Correct Bob's database. |
| FWZ | "No matching decryption rule found" | here is no encryption rule on Bob that corresponds to Alice's encryption connection request. | Correct Bob's Rule Base. |
| FWZ | "Illegal peer request" | This should never happen. The message indicates that Alice's encryption connection request is not in the correct format. | It may be that Alice's encryption connection request has been tampered with. |

**TABLE 14-2** Errors reported by Bob (Decrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| FWZ | "Illegal encryption method" | Alice has requested an encryption method that Bob does not support for this connection. | Agree on the encryption methods to be used for the connection, and define the methods in the **Encryption Properties** window of the relevant rule in the Rule Bases of both Alice and Bob. |
| FWZ | "Cannot find peer's (*Alice's IP address*) object" | Alice is not defined in Bob's database. | Define Alice (including its key and **Encryption Domain**) in Bob's database. |
| FWZ | "Peer (Alice) is not responsible for src" | In Bob's database, Alice's **Encryption Domain** does not include Arthur (the source of the connection). | Correct Bob's database. |
| FWZ | "Peer did not send my key" | Bob is not included among Alice's suggestions for an encrypting gateway. There are several possible causes for this failure: Alice's database has the wrong IP address for Bob, or, in Alice's database, Betty is not in Bob's **Encryption Domain**, but in the **Encryption Domain** of some other gateway. | Correct Alice's database (from Alice's Management Station). |
| FWZ | "Peer (Alice) has neither CA nor key" | In Bob's database, there is no public key for Alice. | Correct Bob's database by fetching a key for Alice. |

**TABLE 14-2** Errors reported by Bob (Decrypting Gateway) (continued)

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| FWZ | "Peer claims to have more updated version of my key" | Alice has a more up-to-date version of Bob's key than Bob has. This can happen if Alice got Bob's key from Barbara (Bob's Management Station) but Bob has not yet received the key from Barbara. | Download Bob from Barbara. |
| FWZ | "Peer (Alice) claims to have older version of its key" | This is the reverse of the previous problem. This can happen if Alice has not yet fetched its own key from Andy (Alice's Management Station) but Bob has fetched Alice's key from Andy. | Download Alice from Andy. |
| FWZ | "Failed to generate shared key" or "Session key installation failed" | Internal VPN-1/FireWall-1 error. | Contact your VPN-1/FireWall-1 support representative. |

## Extended Encryption Protocol (FWZ only)

The errors in this section can occur when a gateway asks a peer for its certified key (signed by the CA).

**TABLE 14-3** Extended Encryption Protocol — Key Update Protocol Errors

| Scheme | Error Message | Meaning | Course of Action |
|---|---|---|---|
| FWZ | "Barbara (Bob's CA) has no CA key" | Alice's database does not have Barbara's CA key, and will not accept Bob's key. | Fetch Barbara's CA key to Alice's database, using the **Certificate Authority Key** window, and then verify the key out-of-band. |
| FWZ | "Barbara (Bob's CA) has probably changed its key" | Alice's database has a different CA key for Barbara, and will not accept Bob's key. | Fetch Barbara's CA key to Alice's database, using the **Certificate Authority Key** window. |
| FWZ | "Peer has not got my correct CA key" | Alice's received a request from Bob for Alice's key, but Bob does not have the correct CA key for Andy (Alice's CA). | On Barbara (Bob's Management Station), fetch Andy's CA key to Bob's database, using the **Certificate Authority Key** window. |
| FWZ | "Bad signature of CA Barbara for Bob's key" | Barbara's signature is incorrect. | It may be that the protocol packet has been tampered with. |
| FWZ | "Peer failed to reply to key request" | Alice did not receive a reply to its request (to Bob) for Bob's encryption key. This can happen if Alice has a bad CA key for Barbara (Bob's CA). | Check Bob's log for relevant error messages. |

The same error messages can appear in Bob's log, with the roles reversed.

## Fetching Keys from a Remote Certificate Authority

When you click on **Get** or **Apply** in the **Key Management** window of a remotely managed gateway, VPN-1/FireWall-1 attempts to fetch the gateway's public key from its Certificate Authority. If this attempt fails, an error message is displayed in a pop-up window. Following is a list of these error messages and explanations of what they mean, as well as suggestions for solving the problems they indicate.

The problem can often be solved by downloading the corrected Security Policy. It is sometimes sufficient to download just the database.

In the examples that follow, the remote gateway's name is Floyd and the CA's name is Oscar.

**TABLE 14-4** Fetching Keys from a remote Certificate Authority Errors

| Error Message | Meaning | Course of Action |
|---|---|---|
| "Communication with Floyd's Certificate Authority (Oscar) failed" or "Cannot connect to Certificate Authority (Oscar)" | These messages indicate that the local computer is unable to communicate with the remote CA (Oscar). | Confirm that you have the correct IP address for the remote CA.<br>Ping the CA to confirm that you are able to communicate with it.<br>Contact the CA's system administrator to confirm that the VPN-1/FireWall-1 daemon on the CA is indeed running, and that it has no configuration problems. |
| "Oscar says that it is not a Certificate Authority" | Though Oscar is a VPN/FireWall Module and the VPN-1/FireWall-1 daemon is running, there is no CA key defined for it. | Contact the CA's system administrator to confirm that there are no configuration problems. |
| "Certificate Authority (Oscar) claims to have a different certificate public key" | This message usually indicates that the Certificate Authority has changed its RSA certificate public key since the last time it was fetched by the local computer. This can happen only after the key was fetched once. | In the CA's Certificate Authority Key window, re-fetch the key by clicking on **Get**. |
| "Certificate Authority (Oscar) denies knowledge of Floyd" | This message indicates that the gateway is not controlled by the CA (which is always a VPN/FireWall Module machine). | Confirm that you have the correct IP address for the gateway. Contact the CA's system administrator and verify that the gateway is one for which the CA is responsible. |
| "Certificate Authority (Oscar) does not have key defined for Floyd" | This message is similar to the previous one, and indicates that the gateway is defined in the CA's VPN-1/FireWall-1 database, but not as a gateway that performs encryption. | Contact the CA's system administrator and verify that the gateway is one for which the CA is responsible. |

**TABLE 14-4** Fetching Keys from a remote Certificate Authority Errors (continued)

| Error Message | Meaning | Course of Action |
|---|---|---|
| "WARNING: Getting Oscar's management key WITHOUT AUTHENTICATION. Verify the transaction MANUALLY" | This message does not indicate an error, but is a warning which is issued the first time a computer fetches a CA's public key without authentication. | As a precaution against tampering, it is recommended that you contact the CA's system administrator by some non-network means (such as telephone or fax) and verify that you received the CA's public key correctly.<br>The key can be verified by the **KeyID** field (a 24 hex character MD5 cryptographic hash of the actual key value) displayed in the **Certificate Authority Key** window. |
| "Certificate Authority's (Oscar) signature for Floyd is bad" | This message indicates that the RSA signature the CA sent for the key for the gateway has been tampered with. This should never happen under normal circumstances. | |
| "Certificate Authority's (Oscar) response for Floyd is outdated" | This message indicates that the key the CA sent for the gateway is outdated, that is, its generation date precedes the generation date in hand for the gateway's key. It is likely that the system administrator at the CA reverted to an old key database. | If you wish to use the outdated key, delete the current key by unchecking FWZ in the gateway's **Key Management** window and pressing **Apply**. Next, open the window again and re-fetch the key. |

# Index

## E



## F



## G



## H



## I

## T



## U



## V



## W



## X