NetScreen Concepts & Examples
ScreenOS Reference Guide

Volume 5: VPNs

ScreenOS 5.0.0

P/N 093-0928-000

Rev. B

Copyright Notice

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089
www.netscreen.com

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

Contents

Preface v
Conventions vi
CLI Conventions vi
WebUI Conventions vii
Illustration Conventions ix
Naming Conventions and Character Types x
NetScreen Documentation xi
Chapter 1 IPSec 1
Introduction to VPNs 2
IPSec Concepts 3
Modes 4
Transport Mode 4
Tunnel Mode 5
Protocols 7
AH 7
ESP 8
Key Management 9
Manual Key 9
AutoKey IKE 9
Security Association 10
Tunnel Negotiation 11
Phase 1 11
Main Mode and Aggressive Mode 12
The Diffie-Hellman Exchange 13
Phase 2 13
Perfect Forward Secrecy 14
Replay Protection 14
Chapter 2 Public Key Cryptography 15
Introduction to Public Key Cryptography 16
PKI 18
Certificates and CRLs 21
Obtaining a Certificate Manually 22
Example: Requesting a Certificate Manually 23
Example: Loading Certificates and CRLs 26
Example: Configuring CRL Settings for a CA Certificate 28
Obtaining a Local Certificate Automatically 30
Example: Requesting a Local Certificate Automatically 31
Automatic Certificate Renewal 34
Key Pair Generation 35
Checking for Revocation Using OCSP 36
Configuring for OCSP 37
Specifying either CRL or OCSP for Revocation Checking 37
Displaying Certificate Revocation Status Attributes 37
Specifying the URL of an OCSP Responder for a Certificate 38
Removing Certificate Revocation Check Attributes 38
Chapter 3 VPN Guidelines 39
Cryptographic Options 40
Site-to-Site Cryptographic Options 41
Dialup VPN Options 50

Route- and Policy-Based Tunnels....58

Packet Flow: Site-to-Site VPN....60

Tunnel Configuration Tips 67

Chapter 4 Site-to-Site VPNs 69

Site-to-Site VPN Configurations 70

Site-to-Site Tunnel Configuration Steps....71

Example: Route-Based Site-to-Site VPN, AutoKey IKE....77

Example: Policy-Based Site-to-Site VPN, AutoKey IKE....91

Example: Route-Based Site-to-Site VPN, Dynamic Peer....102

Example: Policy-Based Site-to-Site VPN, Dynamic Peer....117

Example: Route-Based Site-to-Site VPN, Manual Key 131

Example: Policy-Based Site-to-Site VPN, Manual Key 142

FQDN for Dynamic IKE Gateways 151

Aliases....152

Example: AutoKey IKE Peer with FQDN....153

VPN Sites with Overlapping Addresses....168

Example: Tunnel Interface with NAT-Src and NAT-Dst 171

Transparent Mode VPN 186

Example: Transparent Mode, Policy-Based AutoKey IKE VPN 187

Chapter 5 Dialup VPNs 199

Dialup VPNs 200

Example: Policy-Based Dialup VPN, AutoKey IKE....201

Example: Route-Based Dialup VPN, Dynamic Peer 209

Example: Policy-Based Dialup VPN, Dynamic Peer 220

Bidirectional Policies for Dialup VPN Users 229

Example: Bidirectional Dialup VPN Policies 230

Group IKE ID 237

Group IKE ID with Certificates 238

Wildcard and Container ASN1-DN IKE ID Types 240

Example: Group IKE ID (Certificates) 243

Group IKE ID with Preshared Keys 250

Example: Group IKE ID (Preshared Keys) 252

Shared IKE IDs....259

Example: Shared IKE ID (Preshared Keys).... 260

Chapter 6 L2TP....269

Introduction to L2TP 270

Packet Encapsulation and Decapsulation....274

Encapsulation 274

Decapsulation.... 275

L2TP Parameters....276

Example: Configuring an IP Pool and L2TP Default Settings 277

L2TP and L2TP-over-IPSec....279

Example: Configuring L2TP.... 280

Example: Configuring L2TP-over-IPSec.... 286

Chapter 7 Advanced VPN Features....299

IPSec NAT Traversal 301

Traversing a NAT Device.... 302

UDP Checksum.... 303

The Keepalive Frequency Value 303

IPSec NAT-Traversal and Initiator/Responder Symmetry 304

Example: Enabling NAT-Traversal..............................305

VPN Monitoring 307

Rekey and Optimization Options 307

Source Interface and Destination Address 308

Policy Considerations 310

Configuring the VPN Monitoring Feature..............................310

Example: Specifying Source and Destination Addresses for VPN Monitoring 312

Security Consideration for a Route-Based VPN Design 323

SNMP VPN Monitoring Objects and Traps..............................325

Multiple Tunnels per Tunnel Interface 326

Route-to-Tunnel Mapping 327

Remote Peers' Addresses..............................328

Manual and Automatic Table Entries..............................330

Manual Table Entries 330

Automatic Table Entries.............................. 331

Example: Multiple VPNs on One Tunnel Interface to Overlapping Subnets.............................. 333

Example: Automatic Route and NHTB Table Entries.............................. 364

Redundant VPN Gateways 382

VPN Groups 383

Monitoring Mechanisms 384

IKE Heartbeats.............................. 384

IKE Recovery Procedure.............................. 385

TCP SYN-Flag Checking.............................. 388

Example: Redundant VPN Gateways.............................. 389

Back-to-Back VPNs..............................401

Example: Back-to-Back VPNs 402

Hub-and-Spoke VPNs..............................412

Example: Hub-and-Spoke VPNs 413

Index.............................. IX-I

Preface

A virtual private network (VPN) is a cost-effective and secure way for corporations to provide users dialup access to the corporate network and for remote networks to communicate with each other across the Internet. Secure private connections over the Internet are more cost-effective than dedicated private lines. NetScreen devices provide full VPN functions for secure site-to-site and dialup VPN applications.

Volume 5, “VPNs” describes the following VPN concepts and features that are available on NetScreen devices:

- Internet Protocol Security (IPsec) elements
- Certificates and certificate revocation lists (CRLs) within the context of Public Key Infrastructure (PKI)
- Site-to-site VPNs
- Dialup VPNs
- Layer 2 Tunneling Protocol (L2TP) and L2TP-over-IPSec
- Advanced VPN features such as binding multiple VPN tunnels to a single tunnel interface and redundant IKE gateways.

This volume also includes extensive examples for all the above features.

Conventions

This document contains several types of conventions, which are introduced in the following sections:

- "CLI Conventions"
- "WebUI Conventions" on page vii
- "Illustration Conventions" on page ix
- "Naming Conventions and Character Types" on page x

CLI Conventions

The following conventions are used when presenting the syntax of a command line interface (CLI) command:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example,

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  means "set the management options for the ethernet1, ethernet2, or ethernet3 interface".
- Variables appear in *italic.* For example:

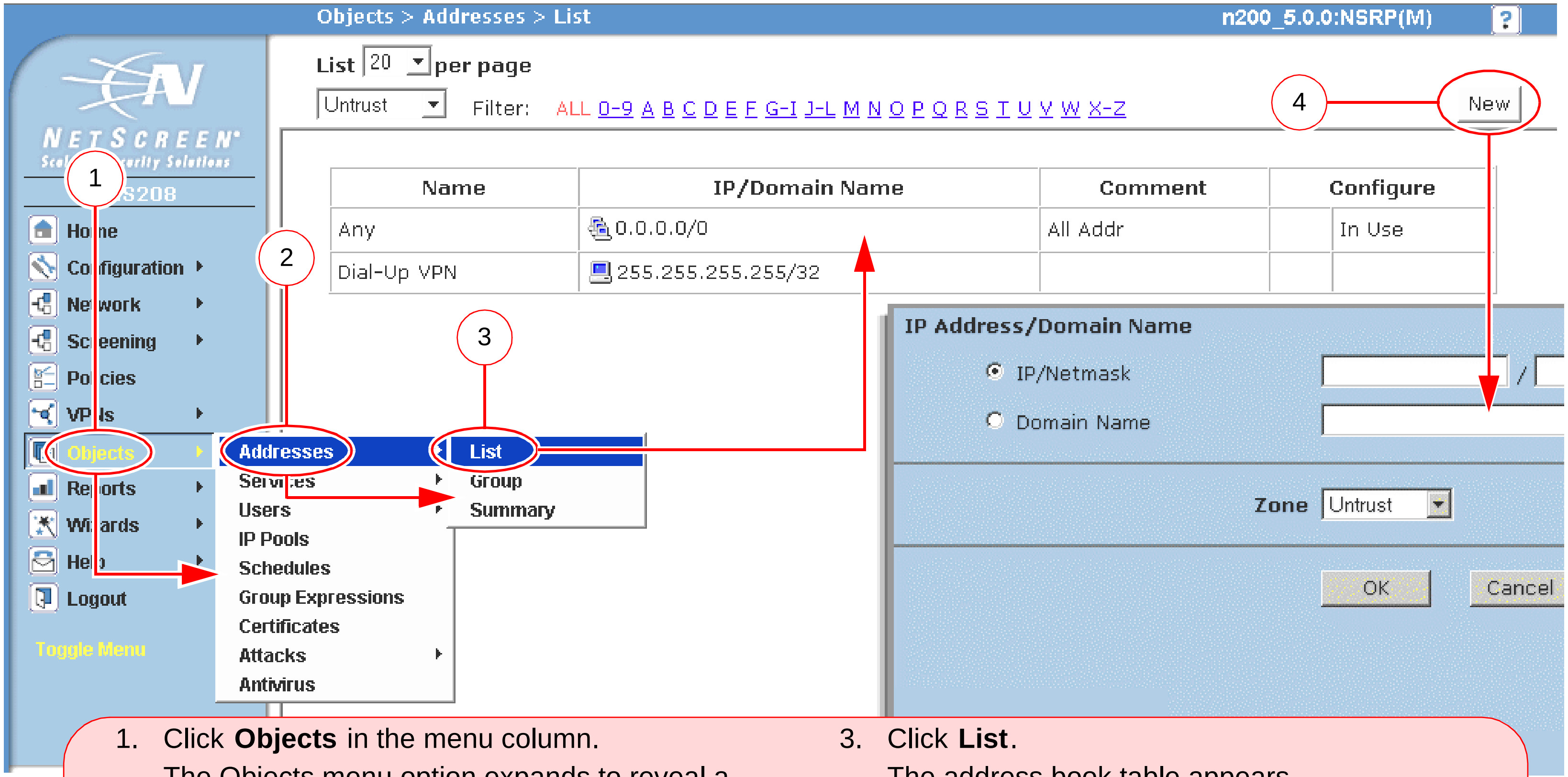
  ```
  set admin user name password
  ```

When a CLI command appears within the context of a sentence, it is in **bold** (except for variables, which are always in *italic*). For example: "Use the **get system** command to display the serial number of a NetScreen device."

> ***Note:*** *When typing a keyword, you only have to type enough letters to identify the word uniquely. For example, typing* ***set adm u joe j12fmt54*** *is enough to enter the command* ***set admin user joe j12fmt54****. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.*

WebUI Conventions

Throughout this book, a chevron (>) is used to indicate navigation through the WebUI by clicking menu options and links. For example, the path to the address configuration dialog box is presented as **Objects > Addresses > List > New**. This navigational sequence is shown below.



Name	IP/Domain Name	Comment	Configure
Any	0.0.0.0/0	All Addr	In Use
Dial-Up VPN	255.255.255.255/32		

1. Click **Objects** in the menu column.

   The Objects menu option expands to reveal a subset of options for Objects.

2. (Applet menu) Hover the mouse over **Addresses**.

   (DHTML menu) Click **Addresses**.

   The Addresses option expands to reveal a subset of options for Addresses.

3. Click **List**.

   The address book table appears.

4. Click the **New** link.

   The new address configuration dialog box appears.

To perform a task with the WebUI, you must first navigate to the appropriate dialog box where you can then define objects and set parameters. The set of instructions for each task is divided into two parts: a navigational path and configuration details. For example, the following set of instructions includes the path to the address configuration dialog box and the settings for you to configure:

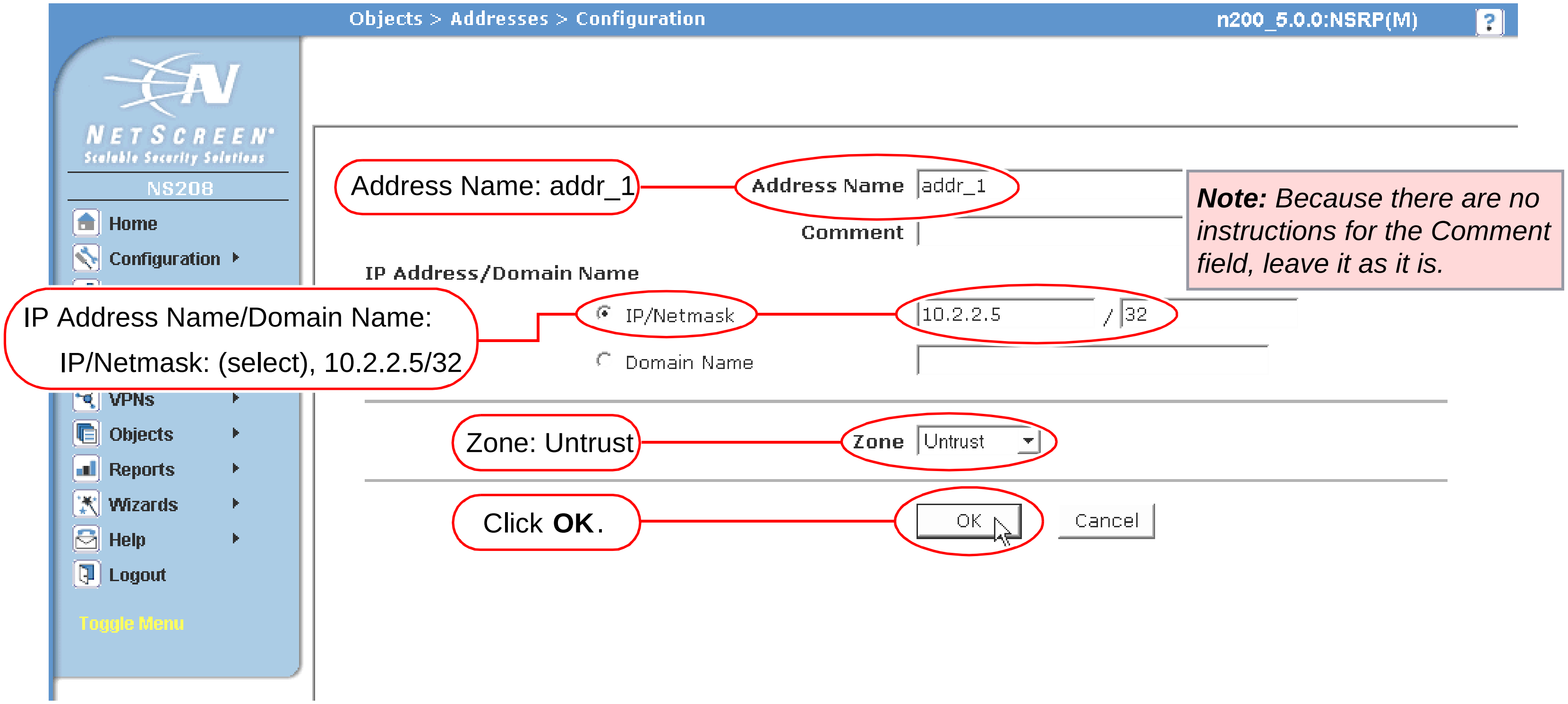
Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.5/32

Zone: Untrust



Objects > Addresses > Configuration n200_5.0.0:NSRP(M)

Address Name: addr_1

Address Name: addr_1

Comment:

IP Address/Domain Name

● IP/Netmask: 10.2.2.5 / 32

○ Domain Name

Zone: Untrust

IP Address Name/Domain Name:

IP/Netmask: (select), 10.2.2.5/32

Zone: Untrust

Click **OK**.

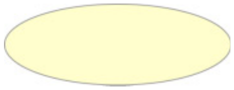
***Note:** Because there are no instructions for the Comment field, leave it as it is.*

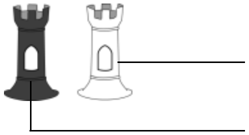
Illustration Conventions

The following graphics make up the basic set of images used in illustrations throughout this book:

Generic NetScreen Device

Virtual Routing Domain


Security Zone


Security Zone Interfaces

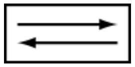
White = Protected Zone Interface
(example: Trust Zone)

Black = Outside Zone Interface
(example: Untrust Zone)

Tunnel Interface

VPN Tunnel

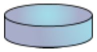
Router Icon


Switch Icon

Local Area Network (LAN)
with a Single Subnet

(example: 10.1.1.0/24)

Internet


Dynamic IP (DIP) Pool

Desktop Computer

Laptop Computer

Generic Network Device

(examples: NAT server,
Access Concentrator)

Server

Naming Conventions and Character Types

ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations.

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes (“); for example, **set address trust “local LAN” 10.1.1.0/24**.
- NetScreen trims any spaces leading or trailing text within a set of double quotes; for example, **“ local LAN ”** becomes **“local LAN”**.
- NetScreen treats multiple consecutive spaces as a single space.
- Name strings are case sensitive, although many CLI key words are case insensitive. For example, **“local LAN”** is different from **“local lan”**.

ScreenOS supports the following character types:

- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.

  Note: *A console connection only supports SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your Web browser supports.*

- ASCII characters from 32 (0x20 in hexidecimals) to 255 (0xff), except double quotes (“), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

NetScreen Documentation

To obtain technical documentation for any NetScreen product, visit www.netscreen.com/resources/manuals/.

To obtain the latest software version, visit www.netscreen.com/services/download_soft. Select a category of software product from the dropdown list, then follow the displayed instructions. (You must be a registered user to download NetScreen software.)

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

techpubs@netscreen.com

1

IPSec

This chapter introduces the various elements of Internet Protocol Security (IPSec) and how they relate to virtual private network (VPN) tunneling. Following an “Introduction to VPNs” on page 2, the remainder of the chapter covers the following elements of IPSec:

- “IPSec Concepts” on page 3
  - “Modes” on page 4
  - “Protocols” on page 7
  - “Key Management” on page 9
  - “Security Association” on page 10
- “Tunnel Negotiation” on page 11
  - “Phase 1” on page 11
  - “Phase 2” on page 13

Introduction to VPNs

A virtual private network (VPN) provides a means for securely communicating between remote computers across a public wide area network (WAN), such as the Internet.

A VPN connection can link two local area networks (LANs) or a remote dialup user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches, and other network equipment that make up the public WAN. To secure VPN communication while passing through the WAN, the two participants create an IP Security (IPSec) tunnel[1].

An IPSec tunnel consists of a pair of unidirectional Security Associations (SAs)—one at each end of the tunnel—that specify the security parameter index (SPI), destination IP address, and security protocol (Authentication Header or Encapsulating Security Payload) employed.

Note: *For more information on SPIs, see "Security Association" on page 10. For more about the IPSec security protocols, see "Protocols" on page 7.*

Through the SA, an IPSec tunnel can provide the following security functions:

- Privacy (via encryption)
- Content integrity (via data authentication)
- Sender authentication and—if using certificates—nonrepudiation (via data origin authentication)

The security functions you employ depend on your needs. If you only need to authenticate the IP packet source and content integrity, you can authenticate the packet without applying any encryption. On the other hand, if you are only concerned with preserving privacy, you can encrypt the packet without applying any authentication mechanisms. Optionally, you can both encrypt and authenticate the packet. Most network security designers choose to encrypt, authenticate, and replay-protect their VPN traffic.

NetScreen supports IPSec technology for creating VPN tunnels with two kinds of key creation mechanisms:

- Manual Key
- AutoKey IKE with a preshared key or a certificate

[1] The term "tunnel" does not denote either transport or tunnel mode (see "Modes" on page 4). It simply refers to the IPSec connection.

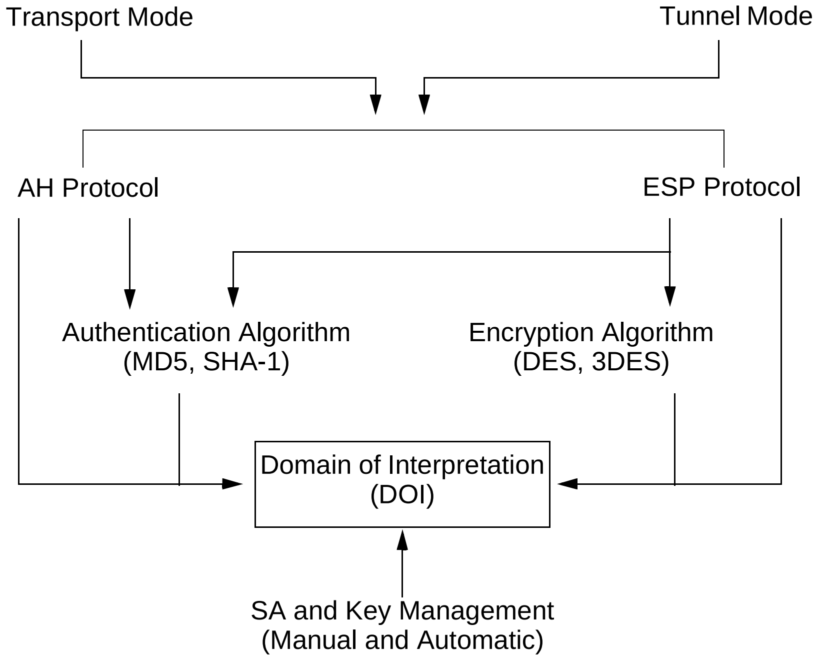
IPSec Concepts

IP Security (IPSec) is a suite of related protocols for cryptographically securing communications at the IP packet layer. IPSec consists of two modes and two main protocols:

- Transport and tunnel modes
- The Authentication Header (AH) protocol for authentication and the Encapsulating Security Payload (ESP) protocol for encryption (and authentication)

IPSec also provides methods for the manual and automatic negotiation of Security Associations (SAs) and key distribution, all the attributes for which are gathered in a Domain of Interpretation (DOI). See RFC 2407 and 2408.

IPSec Architecture



Note: NetScreen does not support Transport Mode with AH.

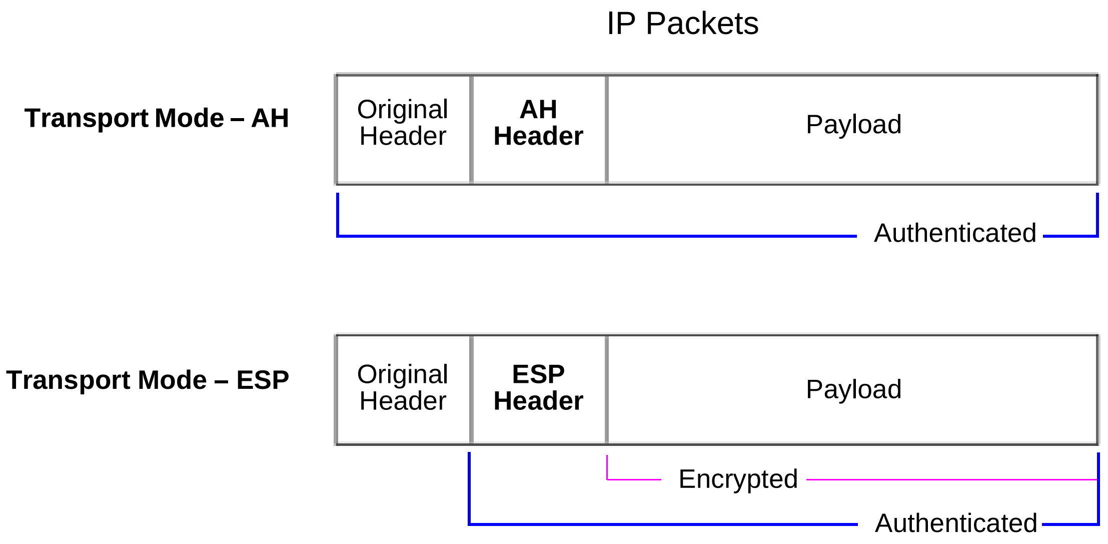
Note: *The IPSec Domain of Interpretation (DOI) is a document containing definitions for all the security parameters required for the successful negotiation of a VPN tunnel—essentially, all the attributes required for SA and IKE negotiations.*

Modes

IPSec operates in one of two modes: transport and tunnel. When both ends of the tunnel are hosts, you can use transport mode or tunnel mode. When at least one of the endpoints of a tunnel is a security gateway, such as a router or firewall, you must use tunnel mode. NetScreen devices always operate in tunnel mode for IPSec tunnels and transport mode for L2TP-over-IPSec tunnels.

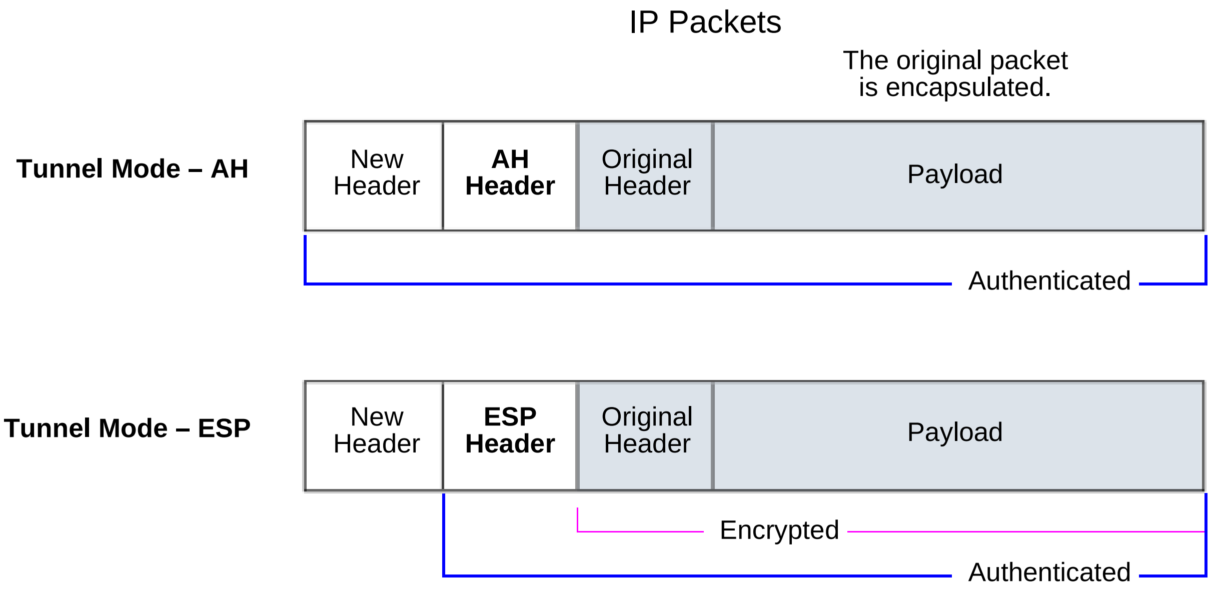
Transport Mode

The original IP packet is not encapsulated within another IP packet. The entire packet can be authenticated (with AH), the payload can be encrypted (with ESP), and the original header remains in plaintext as it is sent across the WAN.

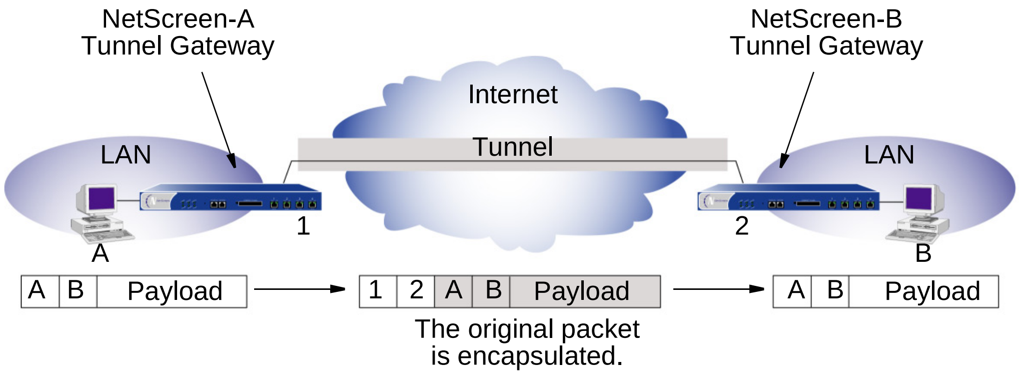


Tunnel Mode

The entire original IP packet—payload and header—is encapsulated within another IP payload and a new header appended to it. The entire original packet can be encrypted, authenticated, or both. With AH, the AH and new headers are also authenticated. With ESP, the ESP header can also be authenticated.

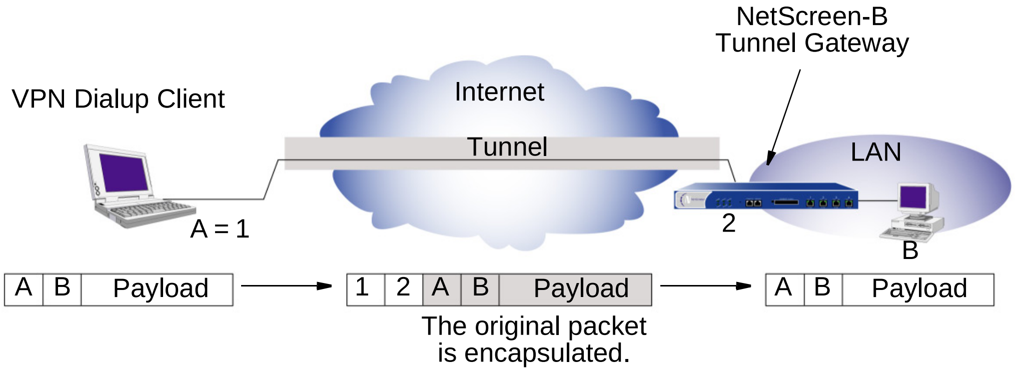


In a site-to-site VPN, the source and destination addresses used in the new header are the IP addresses of the outgoing interface (in NAT or Route mode) or the VLAN1 IP address (in Transparent mode); the source and destination addresses of the encapsulated packets are the addresses of the ultimate endpoints of the connection.



Site-to-Site VPN in Tunnel Mode

In a dialup VPN, there is no tunnel gateway on the VPN dialup client end of the tunnel; the tunnel extends directly to the client itself. In this case, on packets sent from the dialup client, both the new header and the encapsulated original header have the same IP address: that of the client's computer[2].



Dialup VPN in Tunnel Mode

[2] Some VPN clients such as the NetScreen-Remote allow you to define a virtual inner IP address. In such cases, the virtual inner IP address is the source IP address in the original packet header of traffic originating from the client, and the IP address that the ISP dynamically assigns the dialup client is the source IP address in the outer header.

Protocols

IPSec uses two protocols to secure communications at the IP layer:

- Authentication Header (AH)—A security protocol for authenticating the source of an IP packet and verifying the integrity of its content
- Encapsulating Security Payload (ESP)—A security protocol for encrypting the entire IP packet (and authenticating its content)

AH

The Authentication Header (AH) protocol provides a means to verify the authenticity/integrity of the content and origin of a packet. You can authenticate the packet by the checksum calculated via a hash-based message authentication code (HMAC) using a secret key and either MD5 or SHA-1 hash functions.

Message Digest version 5 (MD5)—An algorithm that produces a 128-bit hash (also called a digital signature or message digest) from a message of arbitrary length and a 16-byte key. The resulting hash is used, like a fingerprint of the input, to verify content and source authenticity and integrity.

Secure Hash Algorithm-1 (SHA-1)—An algorithm that produces a 160-bit hash from a message of arbitrary length and a 20-byte key. It is generally regarded as more secure than MD5 because of the larger hashes it produces. Because the computational processing is done in the NetScreen ASIC, the performance cost is negligible.

Note: *For more information on MD5 and SHA-1 hashing algorithms, see the following RFCs: (MD5) 1321, 2403; (SHA-1) 2404. For information on HMAC, see RFC 2104.*

ESP

The Encapsulating Security Payload (ESP) protocol provides a means to ensure privacy (encryption), and source authentication and content integrity (authentication). ESP in tunnel mode encapsulates the entire IP packet (header and payload), and then appends a new IP header to the now encrypted packet. This new IP header contains the destination address needed to route the protected data through the network.

With ESP, you can encrypt and authenticate, encrypt only, or authenticate only. For encryption, you can choose either of the following encryption algorithms:

Data Encryption Standard (DES)—A cryptographic block algorithm with a 56-bit key.

Triple DES (3DES)—A more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key. DES provides a significant performance savings but is considered unacceptable for many classified or sensitive material transfers.

Advanced Encryption Standard (AES)—An emerging encryption standard which, when adopted by Internet infrastructures worldwide, will offer greater interoperability with other network security devices. NetScreen supports AES with 128-, 192-, and 256-bit keys.

For authentication, you can use either MD5 or SHA-1 algorithms.

For either the encryption or authentication algorithm you can select **NULL**; however, you cannot select **NULL** for both simultaneously.

Key Management

The distribution and management of keys are critical to successfully using VPNs. IPSec supports both manual and automatic key distribution methods.

Manual Key

With Manual Keys, administrators at both ends of a tunnel configure all the security parameters. This is a viable technique for small, static networks where the distribution, maintenance, and tracking of keys are not difficult. However, safely distributing Manual Key configurations across great distances poses security issues. Aside from passing the keys face-to-face, you cannot be completely sure that the keys have not been compromised while in transit. Also, whenever you want to change the key, you are faced with the same security issues as when you initially distributed it.

AutoKey IKE

When you need to create and manage numerous tunnels, you need a method that does not require you to configure every element manually. IPSec supports the automated generation and negotiation of keys and security associations using the Internet Key Exchange (IKE) protocol. NetScreen refers to such automated tunnel negotiation as AutoKey IKE and supports AutoKey IKE with preshared keys and AutoKey IKE with certificates.

AutoKey IKE with Preshared Keys

With AutoKey IKE using preshared keys to authenticate the participants in an IKE session, each side must configure and securely exchange the preshared key[3] in advance. In this regard, the issue of secure key distribution is the same as that with Manual Keys. However, once distributed, an AutoKey, unlike a Manual Key, can automatically change its keys at predetermined intervals using the IKE protocol. Frequently changing keys greatly improves security, and automatically doing so greatly reduces key-management responsibilities. However, changing keys increases traffic overhead; therefore, doing so too often can reduce data transmission efficiency.

[3] A preshared key is a key for both encryption and decryption that both participants must have before initiating communication.

AutoKey IKE with Certificates

When using certificates to authenticate the participants during an AutoKey IKE negotiation, each side generates a public/private key pair (see Chapter 2, "Public Key Cryptography" on page 15) and acquires a certificate (see "Certificates and CRLs" on page 21). As long as the issuing certificate authority (CA) is trusted by both sides, the participants can retrieve the peer's public key and verify the peer's signature. There is no need to keep track of the keys and SAs; IKE does it automatically.

Note: *For examples of both Manual Key and AutoKey IKE tunnels, see Chapter 4, "Site-to-Site VPNs" on page 69.*

Security Association

A security association (SA) is a unidirectional agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel. Full bidirectional communication requires at least two SAs, one for each direction.

An SA groups together the following components for securing communications:

– Security algorithms and keys
– Protocol mode (transport or tunnel)
– Key management method (Manual Key or AutoKey IKE)
– SA lifetime

For outbound VPN traffic, the policy invokes the SA associated with the VPN tunnel. For inbound traffic, the NetScreen device looks up the SA by using the following triplet: destination IP, security protocol (AH or ESP), and security parameter index (SPI) value.

Tunnel Negotiation

For a Manual Key IPSec tunnel, because all of the security association (SA) parameters have been previously defined, there is no need to negotiate which SAs to use. In essence, the tunnel has already been established. When traffic matches a policy using that Manual Key tunnel or when a route involves the tunnel, the NetScreen device simply encrypts and authenticates the data, as you determined, and forwards it to the destination gateway.

To establish an AutoKey IKE IPSec tunnel, two phases of negotiation are required:

- In Phase 1, the participants establish a secure channel in which to negotiate the IPSec SAs.
- In Phase 2, the participants negotiate the IPSec SAs for encrypting and authenticating the ensuing exchanges of user data.

Phase 1

Phase 1 of an AutoKey IKE tunnel negotiation consists of the exchange of proposals for how to authenticate and secure the channel. The exchange can be in one of two modes: Aggressive mode or Main mode (see below). Using either mode, the participants exchange proposals for acceptable security services such as:

- Encryption algorithms (DES and 3DES) and authentication algorithms (MD5 and SHA-1). For more information about these algorithms, see “Protocols” on page 7.
- A Diffie-Hellman Group (See “The Diffie-Hellman Exchange” on page 13.)
- Preshared Key or RSA/DSA certificates (see “AutoKey IKE” on page 9)

A successful Phase 1 negotiation concludes when both ends of the tunnel agree to accept at least one set of the Phase 1 security parameters proposed, and then process them. NetScreen devices support up to four proposals for Phase 1 negotiations, allowing you to define how restrictive a range of security parameters for key negotiation you will accept.

The predefined Phase 1 proposals that NetScreen provides are as follows:

- **Standard:** pre-g2-aes128-sha and pre-g2-3des-sha
- **Compatible:** pre-g2-3des-sha, pre-g2-3des-md5, pre-g2-des-sha, and pre-g2-des-md5
- **Basic:** pre-g1-des-sha and pre-g1-des-md5

You can also define custom Phase 1 proposals.

Main Mode and Aggressive Mode

Phase 1 can take place in either Main mode or Aggressive mode. The two modes are described below.

Main Mode: The initiator and recipient send three two-way exchanges (six messages total) to accomplish the following services:

- First exchange, (messages 1 and 2): Propose and accept the encryption and authentication algorithms.
- Second exchange, (messages 3 and 4): Execute a Diffie-Hellman exchange, and the initiator and recipient each provide a nonce (randomly generated number).
- Third exchange, (messages 5 and 6): Send and verify their identities.

The information transmitted in the third exchange of messages is protected by the encryption algorithm established in the first two exchanges. Thus, the participants' identities are not transmitted in the clear.

Aggressive Mode: The initiator and recipient accomplish the same objectives, but only in two exchanges, and a total of three messages:

- First message: The initiator proposes the SA, initiates a Diffie-Hellman exchange, and sends a nonce and its IKE identity.
- Second message: The recipient accepts the SA, authenticates the initiator, and sends a nonce, its IKE identity, and, if using certificates, the recipient's certificate.
- Third message: The initiator authenticates the recipient, confirms the exchange, and, if using certificates, sends the initiator's certificate.

Because the participants' identities are exchanged in the clear (in the first two messages), Aggressive mode does not provide identity protection.

Note: *When a dialup VPN user negotiates an AutoKey IKE tunnel with a preshared key, Aggressive mode must be used. Note also that a dialup VPN user can use an e-mail address, a fully qualified domain name (FQDN), or an IP address as its IKE ID. A dynamic peer can use either an e-mail address or FQDN, but not an IP address.*

The Diffie-Hellman Exchange

A Diffie-Hellman exchange allows the participants to produce a shared secret value. The strength of the technique is that it allows the participants to create the secret value over an unsecured medium without passing the secret value through the wire. There are five Diffie-Hellman (DH) groups (NetScreen supports groups 1, 2, and 5). The size of the prime modulus used in each group's calculation differs as follows:

- DH Group 1: 768-bit modulus[4]
- DH Group 2: 1024-bit modulus
- DH Group 5: 1536-bit modulus

The larger the modulus, the more secure the generated key is considered to be; however, the larger the modulus, the longer the key-generation process takes. Because the modulus for each DH group is a different size, the participants must agree to use the same group[5].

Phase 2

After the participants have established a secure and authenticated channel, they proceed through Phase 2, in which they negotiate the SAs to secure the data to be transmitted through the IPSec tunnel.

Like the process for Phase 1, the participants exchange proposals to determine which security parameters to employ in the SA. A Phase 2 proposal also includes a security protocol—either Encapsulating Security Payload (ESP) or Authentication Header (AH), and selected encryption and authentication algorithms. The proposal can also specify a Diffie-Hellman group, if Perfect Forward Secrecy (PFS) is desired.

Note: *For more about Diffie-Hellman groups, see "The Diffie-Hellman Exchange" above. For more about PFS, see "Perfect Forward Secrecy" on page 14.*

Regardless of the mode used in Phase 1, Phase 2 always operates in Quick mode and involves the exchange of three messages[5].

[4] The strength of DH Group 1 security has depreciated, and NetScreen does not recommend its use.

[5] If you configure multiple (up to four) proposals for Phase 1 negotiations, use the same Diffie-Hellman group in all proposals. The same guideline applies to multiple proposals for Phase 2 negotiations.

NetScreen devices support up to four proposals for Phase 2 negotiations, allowing you to define how restrictive a range of tunnel parameters you will accept. NetScreen also provides a replay protection feature. Use of this feature does not require negotiation because packets are always sent with sequence numbers. You simply have the option of checking the sequence numbers or not. (For more information about replay protection, see below.)

The predefined Phase 2 proposals that NetScreen provides are as follows:

- **Standard:** g2-esp-3des-sha and g2-esp-aes128-sha
- **Compatible:** nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, and nopfs-esp-des-md5
- **Basic:** nopfs-esp-des-sha and nopfs-esp-des-md5

You can also define custom Phase 2 proposals.

In Phase 2, the peers also exchange proxy IDs. A proxy ID is a three-part tuple consisting of local IP address–remote IP address–service. The proxy ID for both peers must match, which means that the service specified in the proxy ID for both peers must be the same, and the local IP address specified for one peer must be the same as the remote IP address specified for the other peer.

Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) is a method for deriving Phase 2 keys independent from and unrelated to the preceding keys. Alternatively, the Phase 1 proposal creates the key (the SKEYID_d key) from which all Phase 2 keys are derived. The SKEYID_d key can generate Phase 2 keys with a minimum of CPU processing. Unfortunately, if an unauthorized party gains access to the SKEYID_d key, all your encryption keys are compromised.

PFS addresses this security risk by forcing a new Diffie-Hellman key exchange to occur for each Phase 2 tunnel. Using PFS is thus more secure, although the rekeying procedure in Phase 2 might take slightly longer with PFS enabled.

Replay Protection

A replay attack occurs when somebody intercepts a series of packets and uses them later either to flood the system, causing a denial-of-service (DoS), or to gain entry to the trusted network. The replay protection feature enables NetScreen devices to check every IPSec packet to see if it has been received before. If packets arrive outside a specified sequence range, the NetScreen device rejects them.

2

Public Key Cryptography

This chapter provides an introduction to public key cryptography and the use of certificates and certificate revocation lists (CRLs) within the context of Public Key Infrastructure (PKI). The material is organized into the following sections:

- "Introduction to Public Key Cryptography" on page 16
- "PKI" on page 18
- "Certificates and CRLs" on page 21
  - "Obtaining a Certificate Manually" on page 22
  - "Obtaining a Local Certificate Automatically" on page 30
  - "Automatic Certificate Renewal" on page 34
- "Checking for Revocation Using OCSP" on page 36
  - "Configuring for OCSP" on page 37

Introduction to Public Key Cryptography

In public key cryptography, a public/private key pair is used to encrypt and decrypt data. Data encrypted with a public key, which the owner makes available to the public, can only be decrypted with the corresponding private key, which the owner keeps secret and protected. For example, if Alice wants to send Bob an encrypted message, Alice can encrypt it with Bob's public key and send it to him. Bob then decrypts the message with his private key.

The reverse is also useful; that is, encrypting data with a private key and decrypting it with the corresponding public key. This is known as creating a digital signature. For example, if Alice wants to present her identity as the sender of a message, she can encrypt the message with her private key and send the message to Bob. Bob then decrypts the message with Alice's public key, thus verifying that Alice is indeed the sender.

Public/private key pairs also play an important role in the use of digital certificates. The procedure for signing a certificate (by a CA) and then verifying the signature works as follows (by the recipient):

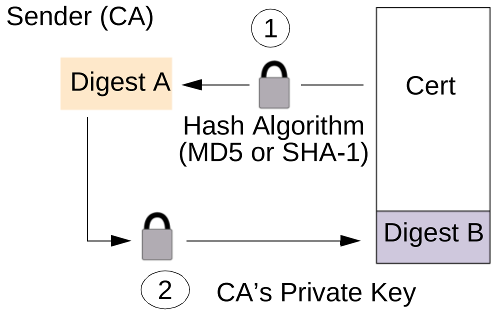
Signing a Certificate

1. The Certificate Authority (CA) that issues a certificate hashes the certificate by using a hash algorithm (MD5 or SHA-1) to generate a digest.
2. The CA then “signs” the certificate by encrypting the digest with its private key. The result is a digital signature.
3. The CA then sends the digitally signed certificate to the person who requested it.

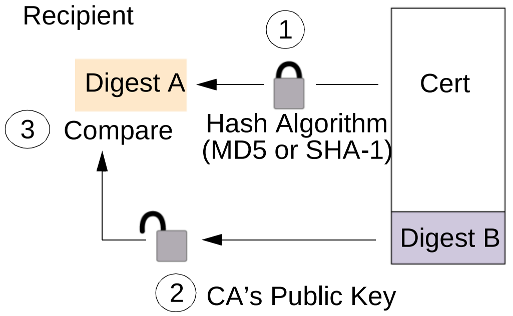
Verifying a Digital Signature

1. When the recipient gets the certificate, he or she also generates another digest by applying the same hash algorithm (MD5 or SHA-1) on the certificate file.
2. The recipient uses the CA's public key to decrypt the digital signature.
3. The recipient compares the decrypted digest with the digest he or she just generated. If the two digests match, the recipient can confirm the integrity of the CA's signature and, by extension, the integrity of the accompanying certificate.

1. Using either the MD5 or SHA-1 hash algorithm, the CA makes digest A from the certificate.
2. Using the its private key, the CA encrypts digest A. The result is digest B, the digital signature.
3. The CA sends the digitally signed certificate to the person who requested it.



1. Using either MD5 or SHA-1, the recipient makes digest A from the certificate.
2. Using the CA’s public key, the recipient decrypts digest B.
3. The recipient compares digest A with digest B. If they match, the recipient knows that the certificate has not been tampered with.

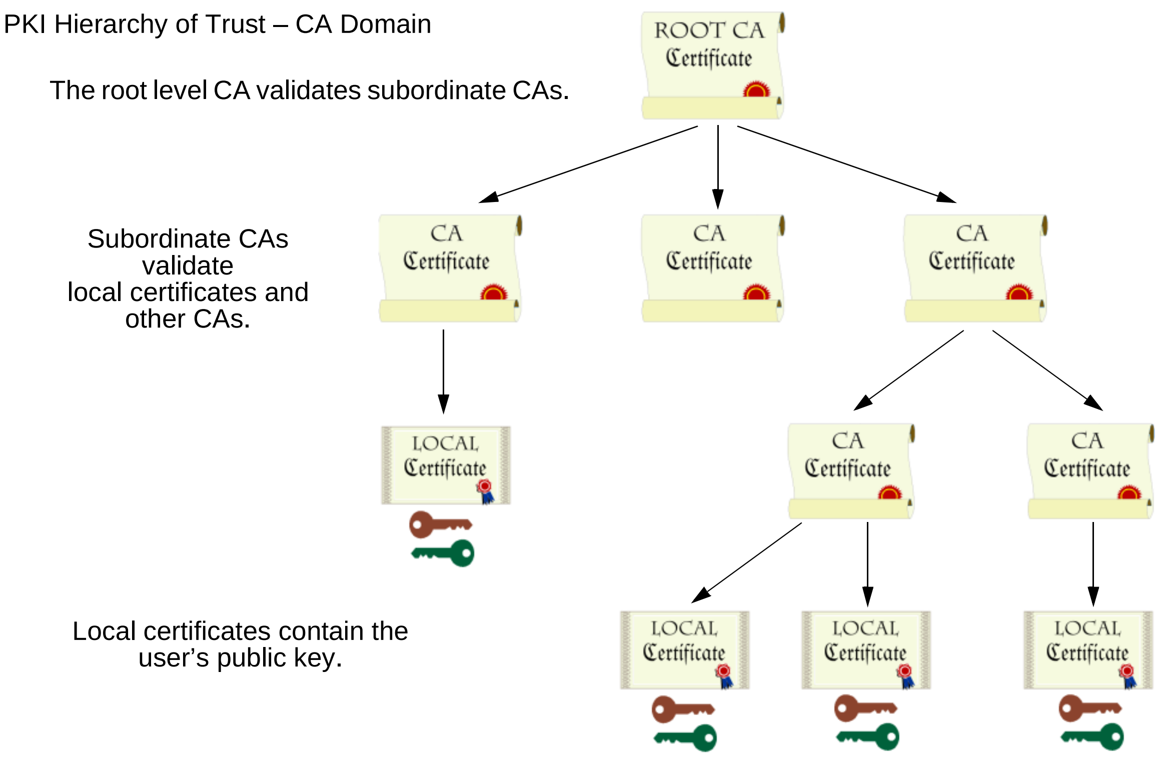


The procedure for digitally signing messages sent between two participants in an IKE session works very similarly, with the following differences:

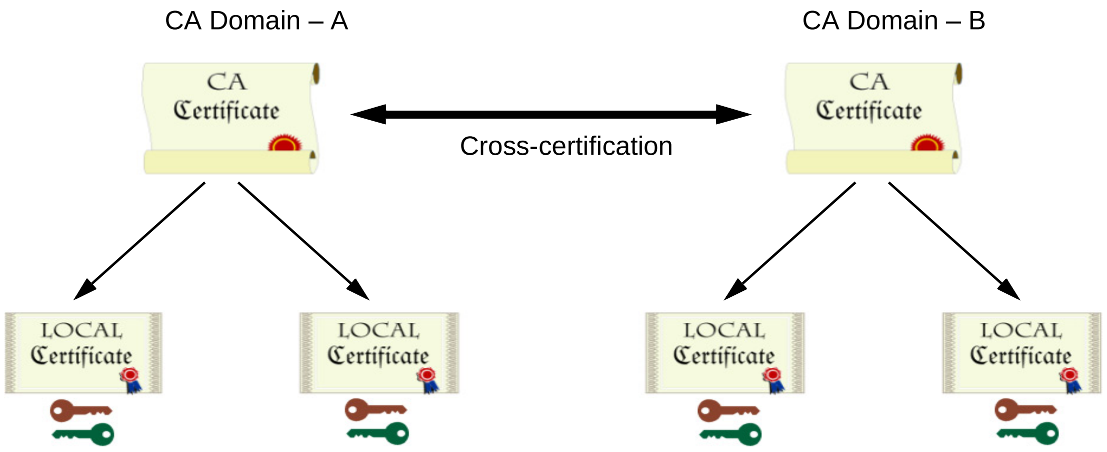
- Instead of making a digest from the CA certificate, the sender makes it from the data in the IP packet payload.
- Instead of using the CA’s public/private key pair, the participants use the sender’s public/private key pair.

PKI

The term Public Key Infrastructure (PKI) refers to the hierarchical structure of trust required for the successful implementation of public key cryptography. To verify the trustworthiness of a certificate, you must be able to track a path of certified CAs from the one issuing your local certificate back to a root authority of a CA domain.


PKI Hierarchy of Trust – CA Domain
The root level CA validates subordinate CAs.
ROOT CA Certificate
Subordinate CAs validate local certificates and other CAs.
CA Certificate
CA Certificate
CA Certificate
LOCAL Certificate
CA Certificate
CA Certificate
Local certificates contain the user’s public key.
LOCAL Certificate
LOCAL Certificate
LOCAL Certificate

If certificates are used solely within an organization, that organization can have its own CA domain within which a company CA issues and validates certificates among its employees. If that organization later wants its employees to be able to exchange their certificates with those from another CA domain (for example, with employees at another organization that also has its own CA domain), the two CAs can develop cross-certification; that is, they can agree to trust the authority of each other. In this case, the PKI structure does not extend vertically but horizontally.



Users in CA domain A can use their certificates and key pairs with users in CA domain B because the CAs have cross-certified each other.

For convenience and practicality, PKI must be transparently managed and implemented. Toward this goal, the NetScreen ScreenOS does the following:

1. Generates a public/private key pair when you create a certificate request.
2. Supplies that public key as part of the certificate request in the form of a text file for transmission to a Certificate Authority (CA) for certificate enrollment (PKCS10 file).

3. Supports loading the local certificate, the CA certificate, and the certificate revocation list (CRL)[1] into the unit.

   You can also specify an interval for refreshing the CRL online. For more information on CRLs, see "Certificates and CRLs" on page 21.

4. Provides certificate delivery when establishing an IPSec tunnel.
5. Supports certificate path validation upward through eight levels of CA authorities in the PKI hierarchy.
6. Supports the PKCS #7 cryptographic standard, which means the NetScreen device can accept X.509 certificates and CRLs packaged within a PKCS #7 envelope[2]. PKCS #7 support allows you to submit multiple X.509 certificates within a single PKI request. You can now configure PKI to validate all the submitted certificates from the issuing CA at one time.
7. Supports online CRL retrieval via LDAP or HTTP.

[1] The Certificate Authority usually provides a CRL. Although you can load a CRL into the NetScreen device, you cannot view it once loaded.

[2] NetScreen supports a PKCS #7 file size of up to 7 Kilobytes.

Certificates and CRLs

A digital certificate is an electronic means for verifying your identity through the word of a trusted third party, known as a Certificate Authority (CA). The CA server you use can be owned and operated by an independent CA[3], or by your own organization, in which case you become your own CA. If you use an independent CA, you must contact them for the addresses of their CA and CRL servers (for obtaining certificates and certificate revocation lists), and for the information they require when submitting personal certificate requests. When you are your own CA, you determine this information yourself.

Note: *ScreenOS contains a CA certificate for authenticating downloads from the antivirus (AV) pattern file server and the Deep Inspection (DI) attack object database server. For more information about the AV pattern file server, see "Enabling Internal AV Scanning" on page* ***4*** *-81. For more information about the DI attack object database server, see "Attack Object Database Server" on page* ***4*** *-128.*

To use a digital certificate to authenticate your identity when establishing a secure VPN connection, you must first do the following:

- Generate a key in the NetScreen device, send it to a CA to obtain a personal certificate (also known as a *local* certificate), and load the certificate in the NetScreen device.
- Obtain a CA certificate for the CA that issued the personal certificate (basically verifying the identity of the CA verifying you), and load the CA certificate in the NetScreen device. You can perform this task manually, or automatically using Simple Certificate Enrollment Protocol (SCEP).
- If the certificate does not contain a certificate distribution point (CDP) extension, and you cannot automatically retrieve the CRL via LDAP or HTTP, you can retrieve a CRL manually and load that in the NetScreen device.

During the course of business, there are several events that make it necessary to revoke a certificate. You might wish to revoke a certificate if you suspect that it has been compromised or when a certificate holder leaves a company. Managing certificate revocations and validation can be accomplished locally (which is a limited solution) or by referencing a CA's CRL, which you can automatically access online at daily, weekly, or monthly intervals, or at the default interval set by the CA.

[3] NetScreen supports the following CAs: Baltimore, Entrust, Microsoft, Netscape, RSA Keon, and Verisign.

Obtaining a Certificate Manually

To obtain a signed digital certificate using the manual method, you must complete several tasks in the following order:

1. Generate a public/private key pair.
2. Fill out the Certificate Request.
3. Submit your request to your CA of choice.
4. After you receive your signed certificate, you must load it into the NetScreen device along with the CA certificate.

You now have the following items for the following uses:

- A local certificate for the NetScreen device, to authenticate your identity with each tunnel connection
- A CA Certificate (their public key), to be used to verify the peer's certificate
- If the Certificate Revocation List (CRL) was included with the CA certificate[4], a CRL to identify invalid certificates

When you receive these files (the certificate files typically have the extension .cer, and the CRL typically has the extension .crl), load them into your NetScreen using the procedure described in the following section.

Note: *If you are planning to use e-mail to submit a PKCS10 file to obtain your certificates, you must properly configure your NetScreen settings so that you can send e-mail to your system administrator. You have to set your primary and secondary DNS servers and specify the SMTP server and e-mail address settings.*

[4] A CRL might accompany a CA certificate and be stored in the NetScreen database. Alternatively, the CA certificate might contain the CRL URL (either LDAP or HTTP) for a CRL that is stored in the CA's database. If the CRL is unobtainable by either method, you can manually enter the default server settings for the CRL URL in the NetScreen device, as explained in "Example: Configuring CRL Settings for a CA Certificate" on page 28.

Example: Requesting a Certificate Manually

When you request a certificate, the NetScreen device generates a key pair. The public key becomes incorporated in the request itself and, eventually, in the digitally signed local certificate you receive from the CA.

In the following example, the security administrator is making a certificate request for Michael Zhang in the Development department at NetScreen Technologies in Santa Clara, California. The certificate is going to be used for a NetScreen device at IP address 10.10.5.44. The administrator instructs the NetScreen device to send the request via e-mail to the security administrator at *admin@netscreen.com.* The security administrator then copies and pastes the request in the certificate request text field at the CA's certificate enrollment site. After the enrollment process is complete, the CA usually sends the certificates via e-mail back to the security administrator.

Note: *Before generating a certificate request, make sure that you have set the system clock and assigned a host name and domain name to the NetScreen device. (If the NetScreen device is in an NSRP cluster, replace the host name with a cluster name. For more information, see "Cluster Name" on page* ***8*** *-17.)*

WebUI

1. Certificate Generation

Objects > Certificates > New: Enter the following, and then click **Generate**:

Name: Michael Zhang

Phone: 408-730-6000

Unit/Department: Development

Organization: NetScreen Technologies

County/Locality: Santa Clara

State: CA

Country: US

E-mail: mzhang@netscreen.com[5]

IP Address: 10.10.5.44

Write to file: (select)

RSA: (select)

Create new key pair of *1024*[6] length: (select)

The NetScreen generates a PKCS #10 file and prompts you to send the file via e-mail, save the file to disk, or automatically enroll via the Simple Certificate Enrollment Protocol (SCEP).

Select the **E-mail to** option, type **admin@netscreen.com**, and then click **OK**[7].

2. Certificate Request

The security administrator opens the file, and copies its contents, taking care to copy the entire text but not any blank spaces before or after the text. (Start at “-----BEGIN CERTIFICATE REQUEST-----”, and end at “-----END CERTIFICATE REQUEST-----”.)

The security administrator then follows the certificate request directions at the CA’s Web site, pasting the PKCS #10 file in the appropriate field when required.

3. Certificate Retrieval

When the security administrator receives the certificate from the CA via e-mail, he forwards it to you. Copy it to a text file, and save it to your workstation (to be loaded to the NetScreen device later through the WebUI) or to a TFTP server (to be loaded later through the CLI).

[5] Some CAs do not support an e-mail address in a certificate. If you do not include an e-mail address in the local certificate request, you cannot use an e-mail address as the local IKE ID when configuring the NetScreen device as a dynamic peer. Instead, you can use a fully-qualified domain name (if it is in the local certificate), or you can leave the local ID field empty. By default the NetScreen device sends its hostname.domainname. If you do not specify a local ID for a dynamic peer, enter the hostname.domainname of that peer on the device at the other end of the IPSec tunnel in the peer ID field.

[6] The value 1024 indicates the bit length of the key pair. If you are using the certificate for SSL (see “Secure Sockets Layer” on page **3**-7), be sure to use a bit length that your Web browser also supports.

[7] Using the e-mail address assumes that you have already configured the IP address for your SMTP server: **set admin mail server-name** { *ip_addr* **|** *dom_name* }.

CLI

1. Certificate Generation

```
set pki x509 dn country-name US
set pki x509 dn email mzhang@netscreen.com
set pki x509 dn ip 10.10.5.44
set pki x509 dn local-name “Santa Clara”
set pki x509 dn name “Michael Zhang”
set pki x509 dn org-name “NetScreen Technologies”
set pki x509 dn org-unit-name Development
set pki x509 phone 408-730-6000
set pki x509 dn state-name CA
set pki x509 default send-to admin@netscreen.com[8]
exec pki rsa new-key 1024
```

The certificate request is sent via e-mail to admin@netscreen.com.

2. Certificate Request

The security administrator opens the file, and copies its contents, taking care to copy the entire text but not any blank spaces before or after the text. (Start at “-----BEGIN CERTIFICATE REQUEST-----”, and end at “-----END CERTIFICATE REQUEST-----”.)

The security administrator then follows the certificate request directions at the CA’s Web site, pasting the PKCS #10 file in the appropriate field when required.

3. Certificate Retrieval

When the security administrator receives the certificate from the CA via e-mail, he forwards it to you. Copy it to a text file, and save it to your workstation (to be loaded to the NetScreen device later through the WebUI) or to a TFTP server (to be loaded later through the CLI).

[8] Using the e-mail address assumes that you have already configured the IP address for your SMTP server: **set admin mail server-name** { *ip_addr* **|** *dom_name* }.

Example: Loading Certificates and CRLs

The CA returns the following three files to you for loading onto the NetScreen device:

- A CA certificate, which contains the CA's public key
- A local certificate that identifies your local machine (your public key)
- A CRL, which lists any certificates revoked by the CA

For the WebUI example, you have downloaded the files to a directory named C:\certs\ns on the administrator's workstation. For the CLI example, you have downloaded the TFTP root directory on a TFTP server with IP address 198.168.1.5.

> ***Note:*** *NetScreen devices, including virtual systems, configured with ScreenOS 2.5 or later support loading multiple local certificates from different CAs.*

This example illustrates how to load two certificate files named auth.cer (CA certificate) and local.cer (your public key), and the CRL file named distrust.crl.

WebUI

1. Objects > Certificates: Select **Load Cert**, and then click **Browse**.
2. Navigate to the C:\certs directory, select **auth.cer**, and then click **Open**.

   The directory path and file name (C:\certs\ns\auth.cer) appear in the File Browse field.
3. Click **Load**.

   The auth.cer certificate file loads.
4. Objects > Certificates: Select **Load Cert**, and then click **Browse**.
5. Navigate to the C:\certs directory, select **local.cer**, and then click **Open**.

   The directory path and file name (C:\certs\ns\local.cer) appear in the File Browse field.

6. Click **Load**.

   The auth.cer certificate file loads.

7. Objects > Certificates: Select **Load CRL**, and then click **Browse**.
8. Navigate to the C:\certs directory, select **distrust.crl**, and then click **Open**.
9. Click **Load**.

   The distrust.crl CRL file loads.

CLI

```
exec pki x509 tftp 198.168.1.5 cert-name auth.cer
exec pki x509 tftp 198.168.1.5 cert-name local.cer
exec pki x509 tftp 198.168.1.5 crl-name distrust.crl
```

Example: Configuring CRL Settings for a CA Certificate

In Phase 1 negotiations, participants check the CRL list to see if certificates received during an IKE exchange are still valid. If a CRL did not accompany a CA certificate and is not loaded in the NetScreen database, the NetScreen device tries to retrieve the CRL through the LDAP or HTTP[9] CRL location defined within the CA certificate itself. If there is no URL address defined in the CA certificate, the NetScreen device uses the URL of the server that you define for that CA certificate. If you do not define a CRL URL for a particular CA certificate, the NetScreen device refers to the CRL server at the default CRL URL address.

Note: *With ScreenOS 2.5 and later, you can disable the checking of a CRL's digital signature when you load the CRL. However, disabling CRL certificate checking compromises the security of your NetScreen device.*

In this example, you first configure the Entrust CA server to check the CRL daily by connecting to the LDAP server at 2.2.2.121 and locating the CRL file. You then configure default certificate validation settings to use the company's LDAP server at 10.1.1.200, also checking the CRL on a daily basis.

Note: *The index (IDX) number for the Entrust CA certificate is 1. To view a list of the IDX numbers for all the CA certificates loaded on a NetScreen device, use the following CLI command:* ***get pki x509 list ca-cert****.*

WebUI

Objects > Certificates (Show: CA) > Server Settings (for NetScreen): Enter the following, and the click **OK**:

X509 Cert_Path Validation Level: Full

CRL Settings:

URL Address: ldap:///CN=Entrust,CN=en2001,CN=PublicKeyServices, CN=Services,CN=Configuration,DC=EN2001,DC=com?CertificateRevocationList?base?objectclass=CRLDistributionPoint

LDAP Server: 2.2.2.121

Refresh Frequency: Daily

[9] The CRL distribution point extension (.cdp) in an X509 certificate can be either an HTTP URL or an LDAP URL.

Objects > Certificates > Default Cert Validation Settings: Enter the following, and then click **OK**:

X509 Certificate Path Validation Level: Full

Certificate Revocation Settings:

Check Method: CRL

URL Address: ldap:///CN=NetScreen,CN=safecert,CN=PublicKeyServices, CN=Services,CN=Configuration,DC=SAFECERT,DC=com?CertificateRevocationList?base?objectclass=CRLDistributionPoint

LDAP Server: 10.1.1.200

CLI

```
set pki authority 1 cert-path full
set pki authority 1 cert-status crl url “ldap:///CN=Entrust,CN=en2001,
    CN=PublicKeyServices,CN=Services,CN=Configuration,DC=EN2000,DC=com?Certific
    ateRevocationList?base?objectclass=CRLDistributionPoint”
set pki authority 1 cert-status crl server-name 2.2.2.121
set pki authority 1 cert-status crl refresh daily
set pki authority default cert-path full
set pki authority default cert-status crl url “ldap:///CN=NetScreen,
    CN=safecert,CN=PublicKeyServices,CN=Services,CN=Configuration,DC=SAFECERT,
    DC=com?CertificateRevocationList?base?objectclass=CRLDistributionPoint”
set pki authority default cert-status crl server-name 10.1.1.200
set pki authority default cert-status crl refresh daily
save
```

Obtaining a Local Certificate Automatically

To use a digital certificate to authenticate your identity when establishing a secure VPN connection, you must first do the following:

- Obtain a certificate authority (CA) certificate from which you intend to obtain a personal certificate, and then load the CA certificate in the NetScreen device.
- Obtain a local certificate (also known as a personal certificate) from the CA whose CA certificate you have previously loaded, and then load the local certificate in the NetScreen device. You can perform this task manually, or automatically using Simple Certificate Enrollment Protocol (SCEP).

Because the manual method of requesting local certificates has steps requiring you to copy information from one certificate to another, it can be a somewhat lengthy process. To bypass these steps, you can use the automatic method.

Note: *Before using SCEP, you must perform the following tasks:*

- *Configure and enable DNS (see “Domain Name System Support” on page **2** -495).*
- *Set the system clock (see “System Clock” on page **2** -541).*
- *Assign a host name and domain name to the NetScreen device. (If the NetScreen device is in an NSRP cluster, replace the host name with a cluster name. For more information, see “Cluster Name” on page **8** -17.)*

Example: Requesting a Local Certificate Automatically

In this example, you use the automatic method to request a certificate using SCEP from the Verisign CA. You set the following CA settings:

- Full certificate path validation
- RA CGI: http://ipsec.verisign.com/cgi-bin/pkiclient.exe[10]
- CA CGI: http://ipsec.verisign.com/cgi-bin/pkiclient.exe
- Automatic integrity confirmation of CA certificates
- CA ID, which identifies a SCEP server, where Verisign SCEP server uses a domain name, such as netscreen.com or a domain set up by Verisign for your company
- Challenge password
- Automatic certificate polling every 30 minutes (the default is no polling)

You then generate an RSA key pair, specifying a key length of 1024 bits, and initiate the SCEP operation to request a local certificate from the Verisign CA with the above CA settings.

When using the WebUI, you refer to CA certificates by name. When using the CLI, you refer to CA certificates by index (IDX) number. In this example, the IDX number for the Verisign CA is “1”. To see the IDX numbers for CA certificates, use the following command: **get pki x509 list ca-cert**. The output displays an IDX number and an ID number for each certificate. Note the IDX number and use that when referencing the CA certificate in commands.

[10] The Common Gateway Interface (CGI) is a standard way for a web server to pass a user request to an application program, and to receive data back. CGI is part of the Hypertext Transfer Protocol (HTTP). You must specify an RA CGI path even if the RA does not exist. If the RA does not exist, use the value specified for the CA CGI.

WebUI

1. CA Server Settings

Objects > Certificates > Show CA > Server Settings (for Verisign): Enter the following, and then click **OK**:

X509 certificate path validation level: Full

SCEP Settings:

RA CGI: http://ipsec.verisigncom/cgi-bin/pkiclient.exe

CA CGI: http://ipsec.verisigncom/cgi-bin/pkiclient.exe

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic CA Server Settings configuration page:

Polling Interval: 30

Certificate Authentication: Auto

Certificate Renew: 14

2. Local Certificate Request

Objects > Certificates > New: Enter the following, and then click **Generate**:

Name: Michael Zhang

Phone: 408-730-6000

Unit/Department: Development

Organization: NetScreen Technologies

County/Locality: Santa Clara

State: CA

Country: US

Email: mzhang@netscreen.com

IP Address: 10.10.5.44

Create new key pair of *1024*[11] length: (select)

Issue the **get pki x509 pkcs** CLI command to have the NetScreen device generate a PKCS #10 file and then, do one of the following:

- Send the PKCS #10 certificate request file to an e-mail address
- Save it to disk
- Automatically enroll by sending the file to a CA that supports the Simple Certificate Enrollment Protocol (SCEP)

3. Automatic Enrollment

Select the **Automatically enroll to** option, select the **Existing CA server settings** option, and then select **Verisign** from the drop-down list.

Contact Verisign to inform them of your certificate request. They must authorize the certificate request before you can download the certificate.

CLI

1. CA Server Settings

```
set pki authority 1 cert-path full
set pki authority 1 scep ca-cgi “http://ipsec.verisign.com/cgi-bin
    /pkiclient.exe”[12]
set pki authority 1 scep ra-cgi “http://ipsec.verisign.com/cgi-bin
    /pkiclient.exe”[13]
set pki authority 1 scep polling-int 30
set pki authority 1 scep renew-start 14
```

[11] The value 1024 indicates the bit length of the key pair. If you are using the certificate for SSL, be sure to use a bit length that your Web browser also supports.

[12] The Common Gateway Interface (CGI) is a standard way for a web server to pass a user request to an application program, and to receive data back. CGI is part of the Hypertext Transfer Protocol (HTTP).

[13] You must specify an RA CGI path even if the RA does not exist. If the RA does not exist, use the value specified for the CA CGI.

2. Local Certificate Request

```
set pki x509 dn country-name US
set pki x509 dn email mzhang@netscreen.com
set pki x509 dn ip 10.10.5.44
set pki x509 dn local-name “Santa Clara”
set pki x509 dn name “Michael Zhang”
set pki x509 dn org-name “NetScreen Technologies”
set pki x509 dn org-unit-name Development
set pki x509 phone 408-730-6000
set pki x509 dn state-name CA
exec pki rsa new 1024
```

3. Automatic Enrollment

```
exec pki x509 scep 1
```

If this is the first certificate request from this CA, a prompt appears presenting a fingerprint value for the CA certificate. You must contact the CA to confirm that this is the correct CA certificate.

Contact Verisign to inform them of your certificate request. They must authorize the certificate request before you can download the certificate.

Automatic Certificate Renewal

You can enable the NetScreen device to automatically renew certificates it acquired through SCEP (Simple Certificate Enrollment Protocol). This feature saves you from having to remember to renew certificates on the NetScreen device before they expire, and by the same token, helps maintain valid certificates at all times.

This feature is disabled by default. You can configure the NetScreen device to automatically send out a request to renew a certificate before it expires. You can set the time when you want the NetScreen device to send out the certificate renewal request in number of days and minutes before the expiration date. By setting different times for each certificate, you prevent the NetScreen device from having to renew all certificates at the same time.

For this feature to work, the NetScreen device must be able to reach the SCEP server, and the certificate must be present on the NetScreen device during the renewal process. Furthermore, for this feature to work, you must also ensure that the CA issuing the certificate can do the following:

- Support automatic approval of certificate requests.
- Return the same DN (Domain Name). In other words, the CA cannot modify the subject name and SubjectAltName extension in the new certificate.

You can enable and disable the automatic SCEP certificate renewal feature for all SCEP certificates or on a per-certificate basis.

Key Pair Generation

A NetScreen device holds pre-generated keys in memory. The number of pre-generated keys depends on the device model. During normal operation, the NetScreen device can manage to have enough keys available to renew certificates by generating a new key every time it uses one. The process of generating a key usually goes unnoticed as the device has time to generate a new key before one is needed. In the event that the NetScreen device renews a great number of certificates at once, thus using up keys rapidly, it might run out of pre-generated keys and have to generate them promptly for each new request. In this case, the generation of keys might affect the performance of the NetScreen device. Especially in a HA (High Availability) environment where the performance of the NetScreen device might slow down for a number of minutes.

The number of pre-generated key pairs on a NetScreen device depends on the model. For more information, refer to the specification sheet for your NetScreen product.

Checking for Revocation Using OCSP

When a NetScreen device performs an operation that uses a certificate, it may be necessary to check the certificate for premature revocation. The default way to check the revocation status of a digital certificate is to use CRL.

Online Certificate Status Protocol (OCSP) is an alternative way to check the status of a digital certificate. OCSP may provide additional information about the certificate. It may also provide the certificate status in a more timely manner.

When a NetScreen device uses OCSP, it is referred to as the *OCSP client* (or *requester*). This client sends a verification request to a server device called the *OCSP responder*. ScreenOS supports Verisign and Valicert as OCSP responders. The client's request contains the identity of the certificate to check. Before the NetScreen device can perform any OCSP operation, you must configure it to recognize the location of the OCSP responder.

After receiving the request, the OCSP responder confirms that the status information for the certificate is available, then returns the current status to the NetScreen device. The response of the OCSP responder contains the certificate's revocation status, the name of the responder, and the validity interval of the response. Unless the response is an error message, the responder signs the response using the responder's private key. The NetScreen device verifies the validity of the responder's signature by using the certificate of the responder. The certificate of the responder may either be embedded in the OCSP response, or stored locally and specified in the OCSP configuration. If the certificate is stored locally, use the following command to specify the locally stored certificate:

```
set pki authority id_num1 cert-status ocsp cert-verify id id_num2
```

id_num1 identifies the CA certificate that issued the certificate being verified, and *id_num2* identifies the locally stored certificate the device uses to verify the signature on the OCSP response.

If the certificate of the responder is not embedded in the OCSP response or stored locally, then the NetScreen device verifies the signature by using the CA certificate that issued the certificate in question.

Configuring for OCSP

You can use CLI commands to configure a NetScreen device to support OCSP operation. Most of these commands use an identification number to associate the revocation reference URL with the CA certificate. You can obtain this ID number using the following CLI command:

```
get pki x509 list ca-cert
```

Note: *The NetScreen device dynamically assigns the ID number to the CA certificate when you list the CA certificates. This number might change after you modify the certificate store.*

Specifying either CRL or OCSP for Revocation Checking

To specify the revocation check method (CRL, OCSP, or none) for a certificate of a particular CA, use the following CLI syntax:

```
set pki authority id_num cert-status revocation-check { CRL | OCSP | none }
```

where *id_num* is the identification number for the certificate.

The following example specifies OCSP revocation checking.

```
set pki authority 3 cert-status revocation-check ocsp
```

The ID number 3 identifies the certificate of the CA.

Displaying Certificate Revocation Status Attributes

To display the revocation check attributes for a particular CA, use the following CLI syntax:

```
get pki authority id_num cert-status
```

where *id_num* is the identification number for the certificate issued by the CA.

To display the revocation status attributes for the CA that issued certificate 7:

```
get pki authority 7 cert-status
```

Specifying the URL of an OCSP Responder for a Certificate

To specify the URL string of an OCSP responder for a particular certificate, use the following CLI syntax:

```
set pki authority id_num cert-status ocsp url url_str
```

To specify the URL string of an OCSP responder (http:\\192.168.10.10) for the CA with certificate at index 5, use the following CLI syntax:

```
set pki authority 5 cert-status ocsp url http:\\192.168.10.10
```

To remove the URL (http:\\192.168.2.1) of a CRL server for a certificate 5:

```
unset pki authority 5 cert-status ocsp url http:\\192.168.2.1
```

Removing Certificate Revocation Check Attributes

To remove all attributes related to a certificate revocation check for a CA that issued a particular certificate, use the following syntax:

```
unset pki authority id_num cert-status
```

To remove all revocation attributes related to certificate 1:

```
unset pki authority 1 cert-status
```

3

VPN Guidelines

NetScreen offers a variety of cryptographic options when you configure a VPN tunnel. Even when configuring a simple tunnel, you must make choices. The goal of the first half of this chapter is to summarize all the choices for a basic site-to-site VPN and a basic dialup VPN, and to present one or more reasons for choosing one option or another.

In the second half of the chapter, we explore the difference between policy-based and route-based VPN tunnels. We then examine the packet flow for a route-based and policy-based site-to-site AutoKey IKE VPN tunnel to see the outbound and inbound processing stages that a packet undergoes. The chapter concludes with some useful VPN configuration tips to keep in mind when configuring a tunnel.

The chapter is organized as follows:

- "Cryptographic Options" on page 40
  - "Site-to-Site Cryptographic Options" on page 41
  - "Dialup VPN Options" on page 50
- "Route- and Policy-Based Tunnels" on page 58
- "Packet Flow: Site-to-Site VPN" on page 60
- "Tunnel Configuration Tips" on page 67

Cryptographic Options

When configuring a VPN, you must make many decisions about the cryptography you want to use. Questions arise about which Diffie-Hellman group is the right one to choose, which encryption algorithm provides the best balance between security and performance, and so on. This section presents all the cryptographic options required to configure a basic site-to-site VPN tunnel and a basic dialup VPN tunnel, and explains one or more benefits about each one to help you make your decisions.

The first decision that you must make is whether the tunnel is for a site-to-site VPN tunnel (between two NetScreen devices) or whether it is for a dialup VPN (from the NetScreen-Remote VPN client to a NetScreen device). Although this is a networking decision, the distinction between the two types of tunnels affects some cryptographic options. Therefore, the options are presented in two different decision trees:

- “Site-to-Site Cryptographic Options” on page 41
- “Dialup VPN Options” on page 50

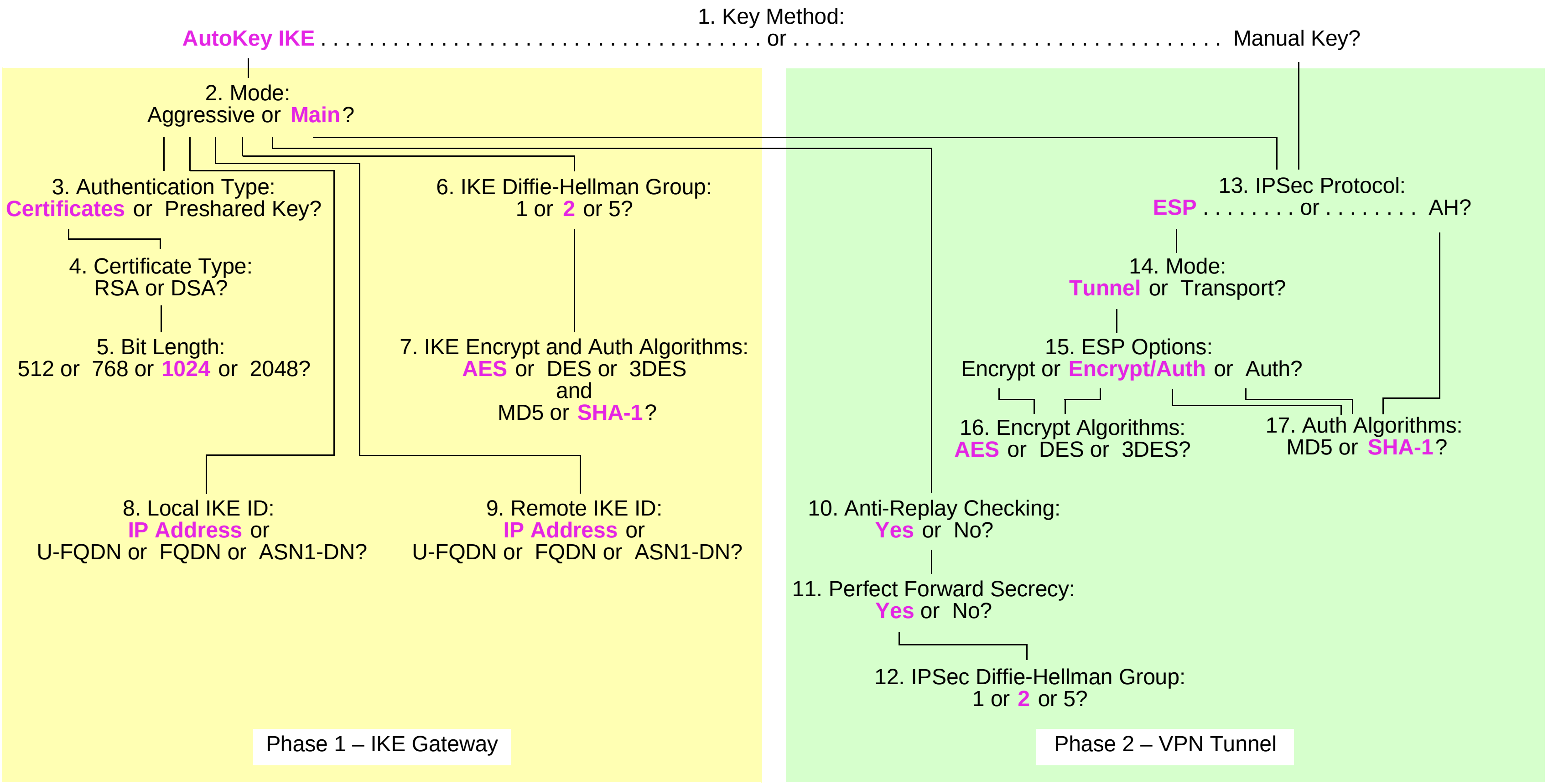
After you decide whether you are going to configure a site-to-site tunnel or a dialup tunnel, you can refer to the appropriate decision tree for guidance. Each tree presents the cryptographic choices that you must make while configuring the tunnel. Following each tree are reasons for choosing each option that appears in the tree.

Note: *Examples for configuring both kinds of tunnels are in Chapter 4, “Site-to-Site VPNs” and Chapter 5, “Dialup VPNs”.*

Site-to-Site Cryptographic Options

When configuring a basic site-to-site VPN tunnel, you must choose among the cryptographic options in the decision tree below. Advantages for each option follow.

***Note:** Options highlighted in **purple** indicate NetScreen-recommended options. For background information about the different IPSec options, see Chapter 1, "IPSec".*



1. Key Method: Manual Key of AutoKey IKE?

AutoKey IKE

- Provides automatic key renewal and key freshness, thereby increasing security

Manual Key

- Useful for debugging IKE problems
- Eliminates IKE negotiation delays when establishing a tunnel

2. Mode: Aggressive or Main?

Aggressive

- Required when the IP address of one of the IPSec peers is dynamically assigned and a preshared key is used

Main

- Provides identity protection
- Can be used when the dialup user has a static IP address or if certificates are used for authentication

3. Authentication Type: Preshared Key or Certificates?

Certificates

- Greater security than provided by preshared keys because you can validate certificates with a certificate authority (CA). (For more information, see Chapter 2, “Public Key Cryptography”.)

Preshared Key

- Easier to use and faster to set up because it does not require a Public Key Infrastructure (PKI)

4. Certificate Type: RSA or DSA?

This depends on the CA from whom you get your certificates. There is no advantage of one certificate type over the other.

5. Bit Length: 512 or 768 or 1024 or 2048?

512

- Incurs the least processing overhead

768

- Provides more security than 512 bits
- Incurs less processing overhead than 1024 and 2048 bits

1024

- Provides more security than 512 and 768 bits
- Incurs less processing overhead than 2048 bits

2048

- Provides the most security

6. IKE Diffie-Hellman Group: 1 or 2 or 5?

Diffie-Hellman Group 1

- Incurs less processing overhead than Diffie-Hellman Groups 2 and 5
- Processing acceleration provided in NetScreen hardware

Diffie-Hellman Group 2

- Incurs less processing overhead than Diffie-Hellman Group 5
- Provides more security than Diffie-Hellman Group 1
- Processing acceleration provided in NetScreen hardware

Diffie-Hellman Group 5

- Provides the most security

7. IKE Encrypt and Auth Algorithms: AES or DES or 3DES and MD5 or SHA-1?

AES

- Cryptographically stronger than DES and 3DES if key lengths are all equal
- Processing acceleration provided in NetScreen hardware
- Approved encryption algorithm for Federal Information Processing Standards (FIPS) and Common Criteria EAL4 standards

DES

- Incurs less processing overhead than 3DES and AES
- Useful when the remote peer does not support AES

3DES

- Provides more cryptographic security than DES
- Processing acceleration provided in NetScreen hardware

MD5

- Incurs less processing overhead than SHA-1

SHA-1

- Provides more cryptographic security than MD5
- The only authentication algorithm that FIPS accepts

8. Local IKE ID: IP Address (Default) or U-FQDN or FQDN or ASN1-DN?

IP Address

- Can only be used if the local NetScreen device has a static IP address
- Default IKE ID when using a preshared key for authentication
- Can be used with a a certificate if the IP address appears in the SubjectAltName field

U-FQDN

- User-Fully Qualified Domain Name (U-FQDN—an e-mail address): Can be used with a preshared key or a certificate if the U-FQDN appears in the SubjectAltName field

FQDN

- Fully Qualified Domain Name (FQDN): Can be used with a preshared key or a certificate if the FQDN appears in the SubjectAltName field
- Useful for VPN gateways that have dynamic IP addresses
- Default IKE ID when using RSA or DSA certificates for authentication

ASN1-DN

- Can be used only with certificates
- Useful if the CA does not support the SubjectAltName field in the certificates it issues

9. Remote IKE ID: IP Address (Default) or U-FQDN or FQDN or ASN1-DN?

IP Address

- Does not require you to enter a remote IKE ID for a peer at a static IP address when using preshared keys for authentication and the peer is a NetScreen device
- Can be used for a device with a static IP address
- Can be used with a preshared key or a certificate if the IP address appears in the SubjectAltName field

U-FQDN

- User-Fully Qualified Domain Name (U-FQDN—an e-mail address): Can be used with a preshared key or a certificate if the U-FQDN appears in the SubjectAltName field

FQDN

- Fully Qualified Domain Name (FQDN): Can be used with a preshared key or a certificate if the FQDN appears in the SubjectAltName field
- Useful for VPN gateways that have dynamic IP addresses
- Does not require you to enter a remote IKE ID when using certificates for authentication and the peer is a NetScreen device

ASN1-DN

- Can be used only with certificates
- Useful if the CA does not support the SubjectAltName field in the certificates it issues

10. Anti-Replay Checking:

No or Yes?

Yes

- Enables the recipient to check sequence numbers in packet headers to prevent Denial-of-Service (DoS) attacks caused when a malefactor resends intercepted IPSec packets

No

- Disabling this might resolve compatibility issues with third-party peers

11. Perfect Forward Secrecy: No of Yes?

Yes

- Perfect Forward Secrecy (PFS): Provides increased security because the peers perform a second Diffie-Hellman exchange to produce the key used for IPSec encryption/decryption

No

- Provides faster tunnel setup
- Incurs less processing during Phase 2 IPSec negotiations

12. IPSec Diffie-Hellman Group: 1 or 2 or 5?

Diffie-Hellman Group 1

- Incurs less processing overhead than Diffie-Hellman Groups 2 and 5
- Processing acceleration provided in NetScreen hardware

Diffie-Hellman Group 2

- Incurs less processing overhead than Diffie-Hellman Group 5
- Provides more security than Diffie-Hellman Group 1
- Processing acceleration provided in NetScreen hardware

Diffie-Hellman Group 5

- Provides the most security

13. IPSec Protocol:

ESP or AH?

ESP

- Encapsulating Security Payload (ESP): Can provide both confidentiality through encryption and encapsulation of the original IP packet and integrity through authentication
- Can provide either encryption alone or authentication alone

AH

- Authentication Header (AH): Provides authentication of the entire IP packet, including the IPSec header and outer IP header

14. Mode: Tunnel or Transport?

Tunnel

- Conceals the original IP header, thereby increasing privacy

Transport

- Required for L2TP-over-IPSec tunnel support

15. ESP Options: Encrypt or Encrypt/Auth or Auth?

Encrypt

- Provides faster performance and incurs less processing overhead than using encrypt/auth
- Useful when you require confidentiality but do not require authentication

Encrypt/Auth

- Useful when you want confidentiality and authentication

Auth

- Useful when you want authentication but do not require confidentiality. Perhaps when the information is not secret, but it is important to establish that the information truly comes from the person who claims to send it and that nobody tampered with the content while in transit.

16. Encrypt Algorithms: AES or DES or 3DES?

AES

- Cryptographically stronger than DES and 3DES if key lengths are all equal
- Processing acceleration provided in NetScreen hardware
- Approved encryption algorithm for FIPS and Common Criteria EAL4 standards

DES

- Incurs less processing overhead than 3DES and AES
- Useful when the remote peer does not support AES

3DES

- Provides more cryptographic security than DES
- Processing acceleration provided in NetScreen hardware

17. Auth Algorithms: MD5 or SHA-1?

MD5

– Incurs less processing overhead than SHA-1

SHA-1

– Provides more cryptographic security than MD5

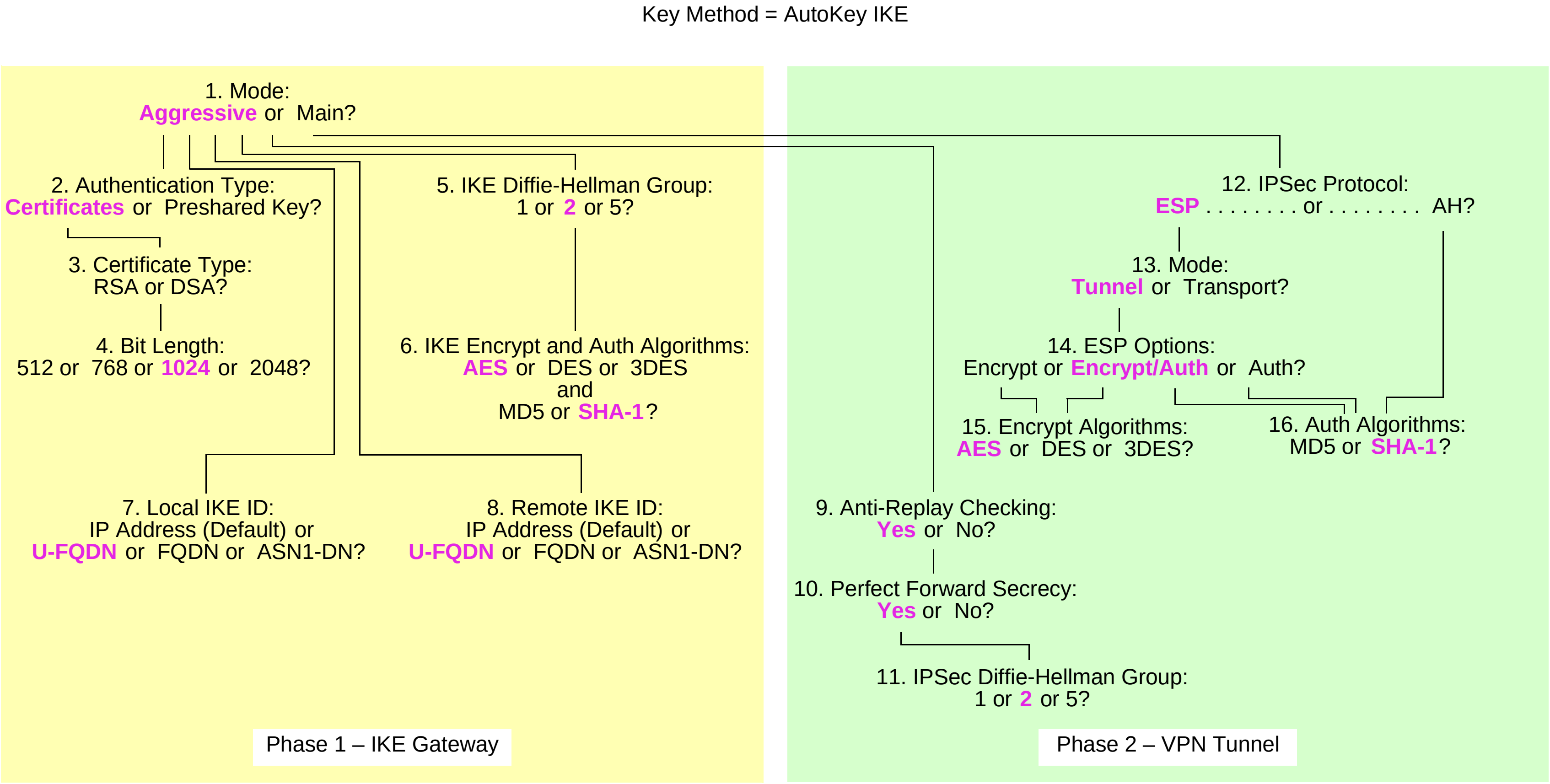
Using the recommended options from the above list, a generic site-to-site VPN configuration between two NetScreen devices with static IP addresses would consist of the following components:

- AutoKey IKE
- Main mode
- 1024-bit certificates (RSA or DSA)
- Phase 1 Diffie-Hellman Group 2
- Encryption = AES
- Authentication = SHA-1
- IKE ID = IP address (default)
- Anti-replay protection = yes
- Perfect Forward Secrecy (PFS) = yes
- Phase 2 Diffie-Hellman Group 2
- Encapsulating Security Payload (ESP)
- Tunnel mode
- Encryption/Authentication
- Encryption = AES
- Authentication = SHA-1

Dialup VPN Options

When configuring a basic dialup VPN tunnel, you must choose among the cryptographic options in the decision tree below. Advantages for each option follow.

Note: *Options highlighted in **purple** indicate NetScreen-recommended options. For background information about the different IPSec options, see Chapter 1, “IPSec”.*



1. Mode: Aggressive or Main?

Aggressive

- Required when the IP address of one of the IPSec peers is dynamically assigned and a preshared key is used
- Can be used with either certificates or preshared keys for authentication

Main

- Provides identity protection

2. Authentication Type: Preshared Key or Certificates?

Certificates

- Greater security than provided by preshared keys because you can validate certificates with a certificate authority (CA). (For more information, see Chapter 2, “Public Key Cryptography”.)

Preshared Key

- Easier to use and faster to set up because it does not require a Public Key Infrastructure (PKI)

3. Certificate Type: RSA or DSA?

This depends on the CA from whom you get your certificates. There is no advantage of one certificate type over the other.

4. Bit Length: 512 or 768 or 1024 or 2048?

512

- Incurs the least processing overhead

768

- Provides more security than 512 bits
- Incurs less processing overhead than 1024 and 2048 bits

1024

- Provides more security than 512 and 768 bits
- Incurs less processing overhead than 2048 bits

2048

- Provides the most security

5. IKE Diffie-Hellman Group: 1 or 2 or 5?

Diffie-Hellman Group 1

- Incurs less processing overhead than Diffie-Hellman Groups 2 and 5
- Processing acceleration provided in NetScreen hardware

Diffie-Hellman Group 2

- Incurs less processing overhead than Diffie-Hellman Group 5
- Provides more security than Diffie-Hellman Group 1
- Processing acceleration provided in NetScreen hardware

Diffie-Hellman Group 5

- Provides the most security

6. IKE Encrypt and Auth Algorithms: AES or DES or 3DES and MD5 or SHA-1?

AES

- Cryptographically stronger than DES and 3DES if key lengths are all equal
- Processing acceleration provided in NetScreen hardware
- Approved encryption algorithm for FIPS and Common Criteria EAL4 standards

DES

- Incurs less processing overhead than 3DES and AES
- Useful when the remote peer does not support AES

3DES

- Provides more cryptographic security than DES
- Processing acceleration provided in NetScreen hardware

MD5

- Incurs less processing overhead than SHA-1

SHA-1

- Provides more cryptographic security than MD5

7. Local IKE ID: IP Address (Default) or U-FQDN or FQDN or ASN1-DN?

IP Address (Default)

- Does not require you to enter an IKE ID for a device with a static IP address
- Can be used for a device with a static IP address
- Can be used with a preshared key or a certificate if the IP address appears in the SubjectAltName field

U-FQDN

- User-Fully Qualified Domain Name (U-FQDN—an e-mail address): Can be used with a preshared key or a certificate if the U-FQDN appears in the SubjectAltName field

FQDN

- Fully Qualified Domain Name (FQDN): Can be used with a preshared key or a certificate if the FQDN appears in the SubjectAltName field
- Useful for VPN gateways that have dynamic IP addresses

ASN1-DN

- Can be used only with certificates
- Useful if the CA does not support the SubjectAltName field in the certificates it issues

8. Remote IKE ID: IP Address (Default) or U-FQDN or FQDN or ASN1-DN?

IP Address (Default)

- Does not require you to enter an IKE ID for a device with a static IP address
- Can be used for a device with a static IP address
- Can be used with a preshared key or a certificate if the IP address appears in the SubjectAltName field

U-FQDN

- User-Fully Qualified Domain Name (U-FQDN—an e-mail address): Can be used with a preshared key or a certificate if the U-FQDN appears in the SubjectAltName field

FQDN

- Fully Qualified Domain Name (FQDN): Can be used with a preshared key or a certificate if the FQDN appears in the SubjectAltName field
- Useful for VPN gateways that have dynamic IP addresses

ASN1-DN

- Can be used only with certificates
- Useful if the CA does not support the SubjectAltName field in the certificates it issues

9. Anti-Replay Checking: No or Yes?

Yes

- Enables the recipient to check sequence numbers in packet headers to prevent Denial-of-Service (DoS) attacks caused when a malefactor resends intercepted IPSec packets

No

- Disabling this might resolve compatibility issues with third-party peers

10. Perfect Forward Secrecy: No of Yes?

Yes

- Perfect Forward Secrecy (PFS): Provides increased security because the peers perform a second Diffie-Hellman exchange to produce the key used for IPSec encryption/decryption

No

- Provides faster tunnel setup
- Incurs less processing during Phase 2 IPSec negotiations

11. IPSec Diffie-Hellman Group: 1 or 2 or 5?

Diffie-Hellman Group 1

- Incurs less processing overhead than Diffie-Hellman Groups 2 and 5
- Processing acceleration provided in NetScreen hardware

Diffie-Hellman Group 2

- Incurs less processing overhead than Diffie-Hellman Group 5
- Provides more security than Diffie-Hellman Group 1
- Processing acceleration provided in NetScreen hardware

Diffie-Hellman Group 5

- Provides the most security

12. IPSec Protocol: ESP or AH?

ESP

- Encapsulating Security Payload (ESP): Can provide both confidentiality through encryption and encapsulation of the original IP packet and integrity through authentication
- Can provide either encryption alone or authentication alone

AH

- Authentication Header (AH): Provides authentication of the entire IP packet, including the IPSec header and outer IP header

13. Mode: Tunnel or Transport?

Tunnel

- Conceals the original IP header, thereby increasing privacy

Transport

- Required for L2TP-over-IPSec tunnel support

14. ESP Options: Encrypt or Encrypt/Auth or Auth?

Encrypt

- Provides faster performance and incurs less processing overhead than using encrypt/auth
- Useful when you require confidentiality but do not require authentication

Encrypt/Auth

- Useful when you want confidentiality and authentication

Auth

- Useful when you want authentication but do not require confidentiality. Perhaps when the information is not secret, but it is important to establish that the information truly comes from the person who claims to send it and that nobody tampered with the content while in transit.

15. Encrypt Algorithms: AES or DES or 3DES?

AES

- Cryptographically stronger than DES and 3DES if key lengths are all equal
- Processing acceleration provided in NetScreen hardware
- Approved encryption algorithm for FIPS and Common Criteria EAL4 standards

DES

- Incurs less processing overhead than 3DES and AES
- Useful when the remote peer does not support AES

3DES

- Provides more cryptographic security than DES
- Processing acceleration provided in NetScreen hardware

16. Auth Algorithms: MD5 or SHA-1?

MD5

- Incurs less processing overhead than SHA-1

SHA-1

- Provides more cryptographic security than MD5

Using the recommended options from the above list, a generic dialup VPN configuration between two NetScreen devices with static IP addresses would consist of the following components:

- Aggressive mode
- 1024-bit certificates (RSA or DSA)
- Phase 1 Diffie-Hellman Group 2
- Encryption = AES
- Authentication = SHA-1
- IKE ID = U-FQDN (e-mail address)
- Anti-replay protection = yes
- Perfect Forward Secrecy (PFS) = yes
- Phase 2 Diffie-Hellman Group 2
- Encapsulating Security Payload (ESP)
- Tunnel mode
- Encryption/Authentication
- Encryption = AES
- Authentication = SHA-1

Route- and Policy-Based Tunnels

The configuration of a NetScreen device for VPN support is particularly flexible. You can create route-based and policy-based VPN tunnels. Additionally, each type of tunnel can use Manual Key or AutoKey IKE to manage the keys used for encryption and authentication.

With policy-based VPN tunnels, a tunnel is treated as an object (or a building block) that together with source, destination, service, and action, comprises a policy that permits VPN traffic. (Actually, the VPN policy action is *tunnel*, but the action *permit* is implied, if unstated). In a policy-based VPN configuration, a policy specifically references a VPN tunnel by name.

With route-based VPNs, the policy does not specifically reference a VPN tunnel. Instead, the policy references a destination address. When the NetScreen device does a route lookup to find the interface through which it must send traffic to reach that address, it finds a route via a tunnel interface, which is bound to a specific VPN tunnel[1].

Thus, with a policy-based VPN tunnel, you can consider a tunnel as an element in the construction of a policy. With a route-based VPN tunnel, you can consider a tunnel as a means for delivering traffic, and the policy as a method for either permitting or denying the delivery of that traffic.

The number of policy-based VPN tunnels that you can create is limited by the number of policies that the device supports. The number of route-based VPN tunnels that you create is limited by the number of route entries or the number of tunnel interfaces that the device supports—whichever number is lower.

A route-based VPN tunnel configuration is a good choice when you want to conserve tunnel resources while setting granular restrictions on VPN traffic. Although you can create numerous policies referencing the same VPN tunnel, each policy creates an individual IPSec security association (SA) with the remote peer, each of which counts as an individual VPN tunnel. With a route-based approach to VPNs, the regulation of traffic is not coupled to the means of its delivery. You can configure dozens of policies to regulate traffic flowing through a single VPN tunnel between two sites, and there is just one IPSec SA at work. Also, a route-based VPN configuration allows you to create policies referencing a destination reached through a VPN tunnel in which the action is *deny*, unlike a policy-based VPN configuration, in which—as stated earlier—the action must be *tunnel*, implying *permit*.

[1] Typically, a tunnel interface is bound to a single tunnel. You can also bind a tunnel interface to multiple tunnels. For more information, see “Multiple Tunnels per Tunnel Interface” on page 326.

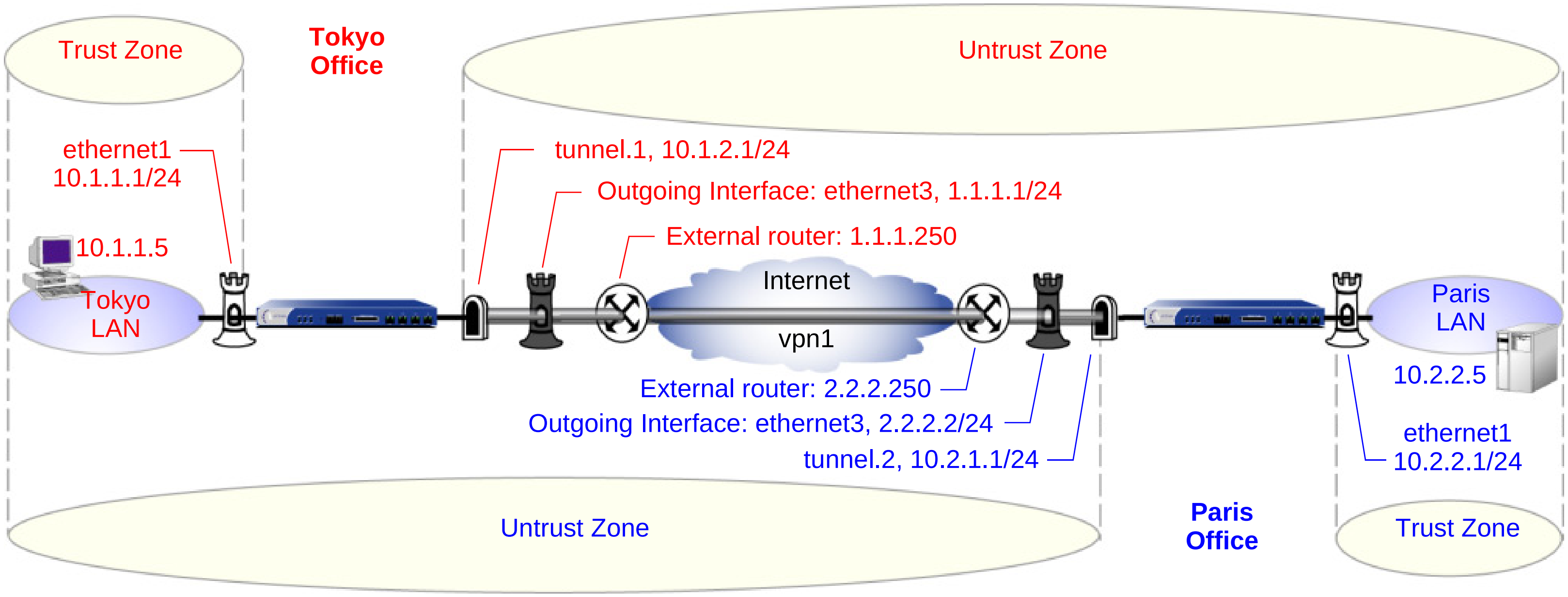
Another advantage that route-based VPNs offer is the exchange of dynamic routing information through VPN tunnels. You can enable an instance of a dynamic routing protocol, such as Border Gateway Protocol (BGP), on a tunnel interface that is bound to a VPN tunnel. The local routing instance exchanges routing information through the tunnel with a neighbor enabled on a tunnel interface bound to the other end.

When a tunnel does not connect large networks running dynamic routing protocols and you do not need to conserve tunnels or define various policies to filter traffic through the tunnel, a policy-based tunnel makes sense. Also, because there is no network beyond a dialup VPN client, policy-based VPN tunnels are good choices for dialup VPN configurations.

Packet Flow: Site-to-Site VPN

To better understand how the various components comprising the creation of an IPSec tunnel work in relation to each other, this section looks at the processing of a packet flow through a tunnel—both when a NetScreen device sends outbound VPN traffic and when it receives inbound VPN traffic. The processing for a route-based VPN is presented, followed by an addendum noting the two places in the flow that differ for a policy-based VPN.

A company based in Tokyo has just opened a branch office in Paris and needs to connect the two sites through an IPSec tunnel. The tunnel uses AutoKey IKE, the ESP protocol, AES for encryption, SHA-1 for authentication using a preshared key, and has anti-replay checking enabled. The NetScreen devices protecting each site are in NAT mode, and all the zones are in the trust-vr routing domain. The addresses are as follows:



The path of a packet coming from 10.1.1.5/32 in the Tokyo LAN and going to 10.2.2.5/32 in the Paris LAN through an IPSec tunnel proceeds as described in the following subsections.

Tokyo (Initiator)

1. The host at 10.1.1.5 sends a packet destined for 10.2.2.5 to 10.1.1.1, which is the IP address ethernet1 and is the default gateway configured in the TCP/IP settings of host.
2. The packet arrives at ethernet1, which is bound to the Trust zone.
3. If you have enabled SCREEN options such as IP spoof detection for the Trust zone, the NetScreen device activates the SCREEN module at this point. SCREEN checking can produce one of the following three results:
   - If a SCREEN mechanism detects anomalous behavior for which it is configured to block the packet, the NetScreen device drops the packet and makes an entry in the event log.
   - If a SCREEN mechanism detects anomalous behavior for which it is configured to record the event but not block the packet, the NetScreen device records the event in the SCREEN counters list for ethernet1 and proceeds to the next step.
   - If the SCREEN mechanisms detect no anomalous behavior, the NetScreen device proceeds to the next step.

   If you have not enabled any SCREEN options for the Trust zone, the NetScreen device immediately proceeds to the next step.
4. The session module performs a session lookup, attempting to match the packet with an existing session.

   If the packet does not match an existing session, the NetScreen device performs First Packet Processing, a procedure involving the remaining steps.

   If the packet matches an existing session, the NetScreen device performs Fast Processing, using the information available from the existing session entry to process the packet. Fast Processing bypasses the route and policy lookups because the information generated by the bypassed steps has already been obtained during the processing of the first packet in the session.
5. The address-mapping module checks if a mapped IP (MIP) configuration uses the destination IP address 10.2.2.5. Because 10.2.2.5 is not used in a MIP configuration, the NetScreen device proceeds to the next step. (For information about packet processing when MIPs, VIPs, or destination address translation [NAT-dst] is involved, see “Packet Flow for Destination Translation” on page **2** -278.)

6. To determine the destination zone, the route module does a route lookup for 10.2.2.5. (The route module uses the ingress interface to determine which virtual router to use for the route lookup.) It finds a route entry directing traffic to 10.2.2.5 through the tunnel.1 interface bound to a VPN tunnel named “vpn1”. The tunnel interface is in the Untrust zone. By determining the ingress and egress interfaces, the NetScreen device has thereby determined the source and destination zones and can now do a policy lookup.
7. The policy engine does a policy lookup between the Trust and Untrust zones (as determined by the corresponding ingress and egress interfaces). The action specified in the policy matching the source address and zone, destination address and zone, and service is permit.
8. The IPSec module checks if an active Phase 2 security association (SA) exists with the remote peer. The Phase 2 SA check can produce either of the following results:
   - If the IPSec module discovers an active Phase 2 SA with that peer, it proceeds to step 10.
   - If the IPSec module does not discover an active Phase 2 SA with that peer, it drops the packet and triggers the IKE module.
9. The IKE module checks if an active Phase 1 SA exists with the remote peer. The Phase 1 SA check can produce either of the following results:
   - If the IKE module discovers an active Phase 1 SA with the peer, it uses this SA to negotiate a Phase 2 SA.
   - If the IKE module does not discover an active Phase 1 SA with that peer, it begins Phase 1 negotiations in Main mode, and then Phase 2 negotiations.
10. The IPSec module puts an ESP header and then an outer IP header on the packet. Using the address specified as the outgoing interface, it puts 1.1.1.1 as the source IP address in the outer header. Using the address specified for remote gateway, it puts 2.2.2.2 as the destination IP address in the outer header. Next, it encrypts the packet from the payload to the next header field in the original IP header. Then, it authenticates the packet from the ESP trailer to the ESP header.
11. The NetScreen device sends the encrypted and authenticated packet destined for 2.2.2.2 through the outgoing interface (ethernet3) to the external router at 1.1.1.250.

Paris (Recipient)

1. The packet arrives at 2.2.2.2, which is the IP address of ethernet3, an interface bound to the Untrust zone.
2. Using the SPI, destination IP address, and IPSec protocol contained in the outer packet header, the IPSec module attempts to locate an active Phase 2 SA with the initiating peer along with the keys to authenticate and decrypt the packet. The Phase 2 SA check can produce one of the following three results:
   - If the IPSec module discovers an active Phase 2 SA with the peer, it proceeds to step 4.
   - If the IPSec module does not discover an active Phase 2 SA with the peer but it can match an inactive Phase 2 SA using the source IP address but not the SPI, it drops the packet, makes an event log entry, and sends a notification that it received a bad SPI to the initiating peer.
   - If the IPSec module does not discover an active Phase 2 SA with that peer, it drops the packet and triggers the IKE module.
3. The IKE module checks if an active Phase 1 SA exists with the remote peer. The Phase 1 SA check can produce either of the following results:
   - If the IKE module discovers an active Phase 1 SA with the peer, it uses this SA to negotiate a Phase 2 SA.
   - If the IKE module does not discover an active Phase 1 SA with that peer, it begins Phase 1 negotiations in Main mode, and then Phase 2 negotiations.
4. The IPSec module performs an anti-replay check. This check can produce one of two results:
   - If the packet fails the anti-replay check, because it detects a sequence number that the NetScreen device has already received, the NetScreen device drops the packet.
   - If the packet passes the anti-replay check, the NetScreen device proceeds to the next step.
5. The IPSec module attempts to authenticate the packet. The authentication check can produce one of two results:
   - If the packet fails the authentication check, the NetScreen device drops the packet.
   - If the packet passes the authentication check, the NetScreen device proceeds to the next step.
6. Using the Phase 2 SA and keys, the IPSec module decrypts the packet, uncovering its original source address (10.1.1.5) and its ultimate destination (10.2.2.5). It learns that the packet came through vpn1, which is bound to tunnel.1. From this point forward, the NetScreen device treats the packet as if its ingress interface is tunnel.1 instead of ethernet3. It also adjusts the anti-replay sliding window at this point.

7. If you have enabled SCREEN options for the Untrust zone, the NetScreen device activates the SCREEN module at this point. SCREEN checking can produce one of the following three results:
   - If a SCREEN mechanism detects anomalous behavior for which it is configured to block the packet, the NetScreen device drops the packet and makes an entry in the event log.
   - If a SCREEN mechanism detects anomalous behavior for which it is configured to record the event but not block the packet, the NetScreen device records the event in the SCREEN counters list for ethernet3 and proceeds to the next step.
   - If the SCREEN mechanisms detect no anomalous behavior, the NetScreen device proceeds to the next step.
8. The session module performs a session lookup, attempting to match the packet with an existing session. It then either performs First Packet Processing or Fast Processing.

   If the packet matches an existing session, the NetScreen device performs Fast Processing, using the information available from the existing session entry to process the packet. Fast Processing bypasses all but the last two steps (encrypting the packet and forwarding it) because the information generated by the bypassed steps has already been obtained during the processing of the first packet in the session.
9. The address-mapping module checks if a mapped IP (MIP) or virtual IP (VIP) configuration uses the destination IP address 10.2.2.5. Because 10.2.2.5 is not used in a MIP or VIP configuration, the NetScreen device proceeds to the next step.
10. The route module first uses the ingress interface to determine the virtual router to use for the route lookup; in this case, the trust-vr. It then performs a route lookup for 10.2.2.5 in the trust-vr and discovers that it is accessed through ethernet1. By determining the ingress interface (tunnel.1) and the egress interface (ethernet1), the NetScreen device can thereby determine the source and destination zones. The tunnel.1 interface is bound to the Untrust zone, and ethernet1 is bound to the Trust zone. The NetScreen device can now do a policy lookup.
11. The policy engine checks its policy list from the Untrust zone to the Trust zone and finds a policy that grants access.
12. The NetScreen device forwards the packet through ethernet1 to its destination at 10.2.2.5.

Addendum: Policy-Based VPN

The packet flow for a policy-based VPN configuration differs from that of a route-based VPN configuration at two points: the route lookup and the policy lookup.

Tokyo (Initiator)

The first stages of the outbound packet flow are the same for both route-based and policy-based VPN configurations until the route lookup and subsequent policy lookup occur:

Route Lookup: To determine the destination zone, the route module does a route lookup for 10.2.2.5. Not finding an entry for that specific address, the route module resolves it to a route through ethernet3, which is bound to the Untrust zone. By determining the ingress and egress interfaces, the NetScreen device has thereby determined the source and destination zones, and can now perform a policy lookup.

Policy Lookup: The policy engine does a policy lookup between the Trust and Untrust zones. The lookup matches the source address and zone, destination address and zone, and service and finds a policy that references a VPN tunnel named vpn1.

The NetScreen device then forwards the packet through ethernet1 to its destination at 10.2.2.5.

Paris (Recipient)

Most stages of the inbound packet flow on the recipient's end are the same for both route-based and policy-based VPN configurations except that the tunnel is not bound to a tunnel interface, but to a tunnel zone. The NetScreen device learns that the packet came through vpn1, which is bound to the Untrust-Tun tunnel zone, whose carrier zone is the Untrust zone. Unlike route-based VPNs, the NetScreen device considers ethernet3 to be the ingress interface of the decrypted packet—not tunnel.1.

The flow changes after packet decryption is complete. At this point, the route and policy lookups differ:

Route Lookup: The route module performs a route lookup for 10.2.2.5 and discovers that it is accessed through ethernet1, which is bound to the Trust zone. By learning that the Untrust zone is the source zone (because vpn1 is bound to the Untrust-Tun tunnel zone, whose carrier zone is the Untrust zone) and by determining the destination zone based on the egress interface (ethernet1 is bound to the Trust zone), the NetScreen device can now check for a policy from the Untrust to the Trust zones that references vpn1.

Policy Lookup: The policy engine checks its policy list from the Untrust zone to the Trust zone and finds a policy that references a VPN tunnel named vpn1 and that grants access to 10.2.2.5.

The NetScreen device then forwards the packet to its destination.

Tunnel Configuration Tips

This section offers some guidelines, or tips, to keep in mind when configuring VPN tunnels. When configuring an IPSec VPN tunnel, keep the following points in mind:

- NetScreen supports up to four proposals for Phase 1 negotiations and up to four proposals for Phase 2 negotiations. A peer must be configured to accept at least one Phase 1 proposal and one Phase 2 proposal proffered by the other peer. For information about Phase 1 and Phase 2 IKE negotiations, see "Tunnel Negotiation" on page 11.
- If you want to use certificates for authentication and there is more than one local certificate loaded on the NetScreen device, you must specify which certificate you want each VPN tunnel configuration to use. For more information about certificates, see Chapter 2, "Public Key Cryptography" on page 15.
- For a basic policy-based VPN:
  - Use user-defined addresses in the policy, not the pre-defined address "Any".
  - The addresses and service specified in policies configured at both ends of the VPN must match.
  - Use symmetric policies for bidirectional VPN traffic.
- The proxy ID for both peers must match, which means that the service specified in the proxy ID for both peers is the same, and the local IP address specified for one peer is the same as the remote IP address specified for the other peer[2].
  - For a route-based VPN configuration, the proxy ID is user configurable.
  - For a policy-based VPN configuration, the NetScreen device—by default—derives the proxy ID from the source address, destination address, and service specified in the policy that references that VPN tunnel in the policy list. You can also define a proxy ID for a policy-based VPN that supersedes the derived proxy ID.

  The simplest way to ensure that the proxy IDs match is to use 0.0.0.0/0 for the local address, 0.0.0.0/0 for the remote address, and "any" for the service. Instead of using the proxy ID for access control, you use policies to control the traffic to and from the VPN. For examples of VPN configurations with user-configurable proxy IDs, see the route-based VPN examples in Chapter 4, "Site-to-Site VPNs".

[2] The proxy ID is a three-part tuple consisting of local IP address-remote IP address-service.

- As long as the peers' proxy ID settings match, it does not matter if one peer defines a route-based VPN and the other defines a policy-based VPN. If peer-1 uses a policy-based VPN configuration and peer-2 uses a route-based VPN configuration, then peer-2 must define a proxy ID that matches the proxy ID derived from peer-1's policy[3]. If peer-1 performs source network address translation (NAT-src) using a DIP pool, use the address and netmask for the DIP pool as the remote address in peer-2's proxy ID. For example:

When the DIP pool is:	Use this in the proxy ID:
1.1.1.8 – 1.1.1.8	1.1.1.8/32
1.1.1.20 – 1.1.1.50	1.1.1.20/26
1.1.1.100 – 1.1.1.200	1.1.1.100/25
1.1.1.0 – 1.1.1.255	1.1.1.0/24

  For more information about proxy IDs when used with NAT-src and NAT-dst, see "VPN Sites with Overlapping Addresses" on page 168.

- Because proxy IDs support either a single service or all services, the service in a proxy ID derived from a policy-based VPN referencing a service group is considered as "any".
- When both peers have static IP addresses, they can each use the default IKE ID, which is their IP addresses. When a peer or dialup user has a dynamically assigned IP address, that peer or user must use another type of IKE ID. An FQDN is a good choice for a dynamic peer and a U-FQDN (e-mail address) is a good choice for a dialup user. You can use both FQDN and U-FQDN IKE ID types with preshared keys and certificates (if the FQDN or U-FQDN appears in the SubjectAltName field in the certificate). If you use certificates, the dynamic peer or dialup user can also use all or part of the ASN1-DN as the IKE ID.

[3] Peer-1 can also define a proxy ID that matches peer-2's proxy ID. Peer-1's user-defined proxy ID supersedes the proxy ID that the NetScreen device derives from the policy components.

4

Site-to-Site VPNs

This chapter explains how to configure a site-to-site virtual private network (VPN) tunnel between two NetScreen devices. It examines route-based and policy-based VPN tunnels, presents the various elements that you must consider when setting up a tunnel, and offers several examples.

- “Site-to-Site VPN Configurations” on page 70
  - “Site-to-Site Tunnel Configuration Steps” on page 71
  - “Example: Route-Based Site-to-Site VPN, AutoKey IKE” on page 77
  - “Example: Policy-Based Site-to-Site VPN, AutoKey IKE” on page 91
  - “Example: Route-Based Site-to-Site VPN, Dynamic Peer” on page 102
  - “Example: Policy-Based Site-to-Site VPN, Dynamic Peer” on page 117
  - “Example: Route-Based Site-to-Site VPN, Manual Key” on page 131
  - “Example: Policy-Based Site-to-Site VPN, Manual Key” on page 142
- “FQDN for Dynamic IKE Gateways” on page 151
  - “Example: AutoKey IKE Peer with FQDN” on page 153
- “VPN Sites with Overlapping Addresses” on page 168
  - “Example: Tunnel Interface with NAT-Src and NAT-Dst” on page 171
- “Transparent Mode VPN” on page 186
  - “Example: Transparent Mode, Policy-Based AutoKey IKE VPN” on page 187

SITE-TO-SITE VPN CONFIGURATIONS

An IPSec VPN tunnel exists between two gateways, and each gateway needs an IP address. When both gateways have static IP addresses, you can configure the following kinds of tunnels:

- Site-to-Site VPN, AutoKey IKE tunnel (with a preshared key or certificates)
- Site-to-Site VPN, Manual Key tunnel

When one gateway has a static address and the other has a dynamically assigned address, you can configure the following kind of tunnel:

- Dynamic Peer Site-to-Site VPN, AutoKey IKE tunnel (with a preshared key or certificates)

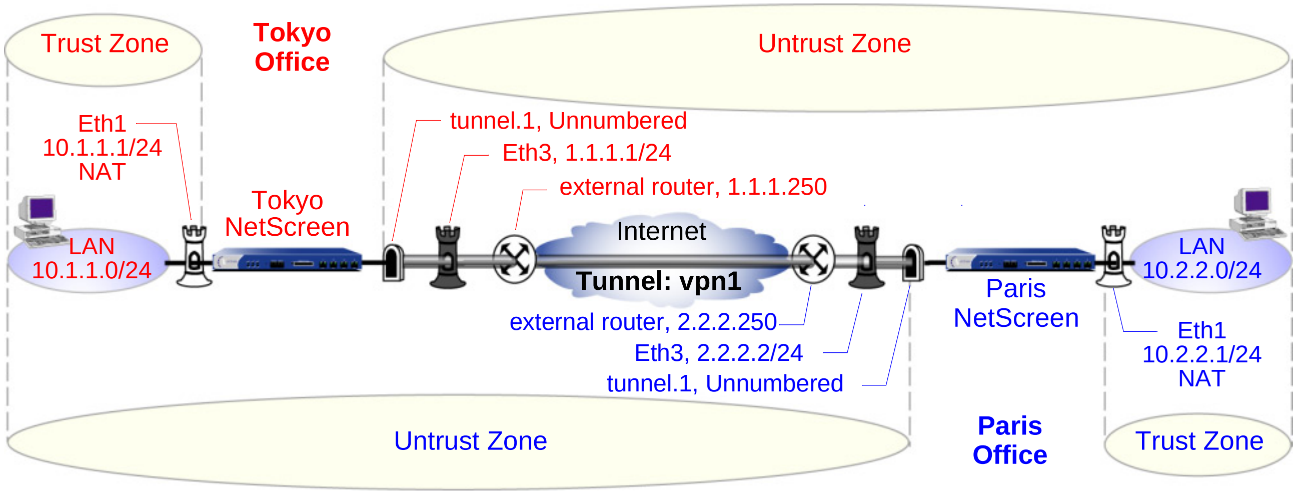
As used here, a static site-to-site VPN involves an IPSec tunnel connecting two sites, each with a NetScreen device operating as a secure gateway. The physical interface or subinterface used as the outgoing interface on both devices has a fixed IP address, and the internal hosts also have static IP addresses. If the NetScreen device is in Transparent mode, it uses the VLAN1 address as the IP address for the outgoing interface. With a static site-to-site VPN, hosts at either end of the tunnel can initiate the VPN tunnel setup because the IP address of the remote gateway remains constant and thus reachable.

If the outgoing interface of one of the NetScreen devices has a dynamically assigned IP address, that device is termed a dynamic peer and the VPN is configured differently. With a dynamic peer site-to-site VPN, only hosts behind the dynamic peer can initiate the VPN tunnel setup because only their remote gateway has a fixed IP address and is thus reachable from their local gateway. However, after a tunnel is established between a dynamic peer and a static peer, hosts behind either gateway can initiate VPN traffic if the destination hosts have fixed IP addresses.

Note: *For background information about the available VPN options, see Chapter 1, “IPSec”. For guidance when choosing among the various options, see Chapter 3, “VPN Guidelines”.*

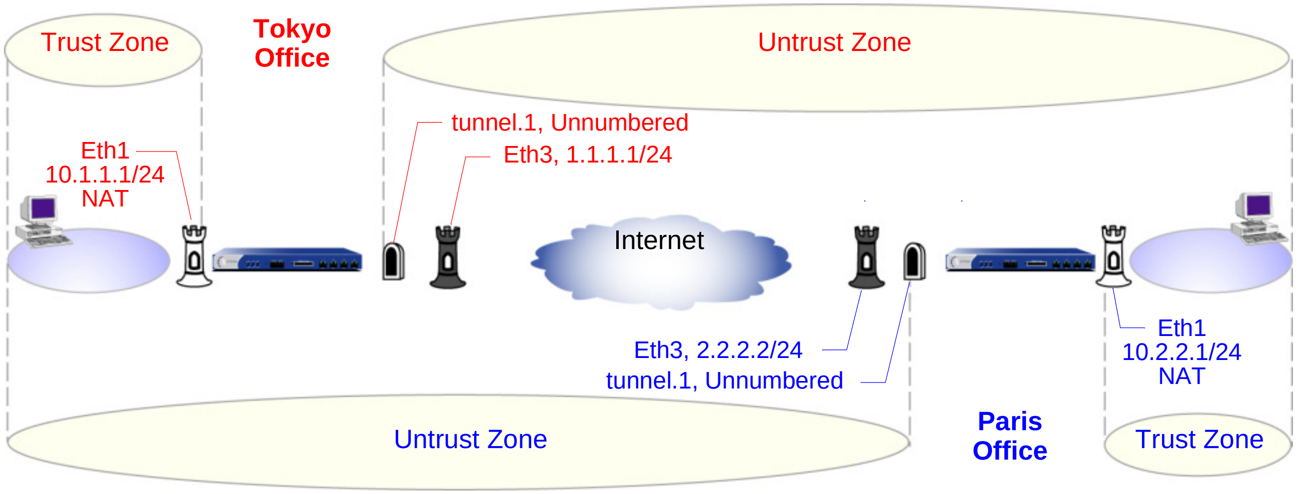
Site-to-Site Tunnel Configuration Steps

The configuration of a site-to-site VPN tunnel requires the coordination of the tunnel configuration with that of other settings—interfaces, addresses, routes, and policies. The three example VPN configurations in this section are set in the following context: an office in Tokyo wants to communicate securely with an office in Paris through an IPSec VPN tunnel.



The administrators in both offices configure the following settings:

- Interfaces – Security Zones and Tunnel
- Addresses
- VPN (one of the following)
  - AutoKey IKE
  - Dynamic Peer
  - Manual Key
- Routes
- Policies



1. Interfaces – Security Zones and Tunnel

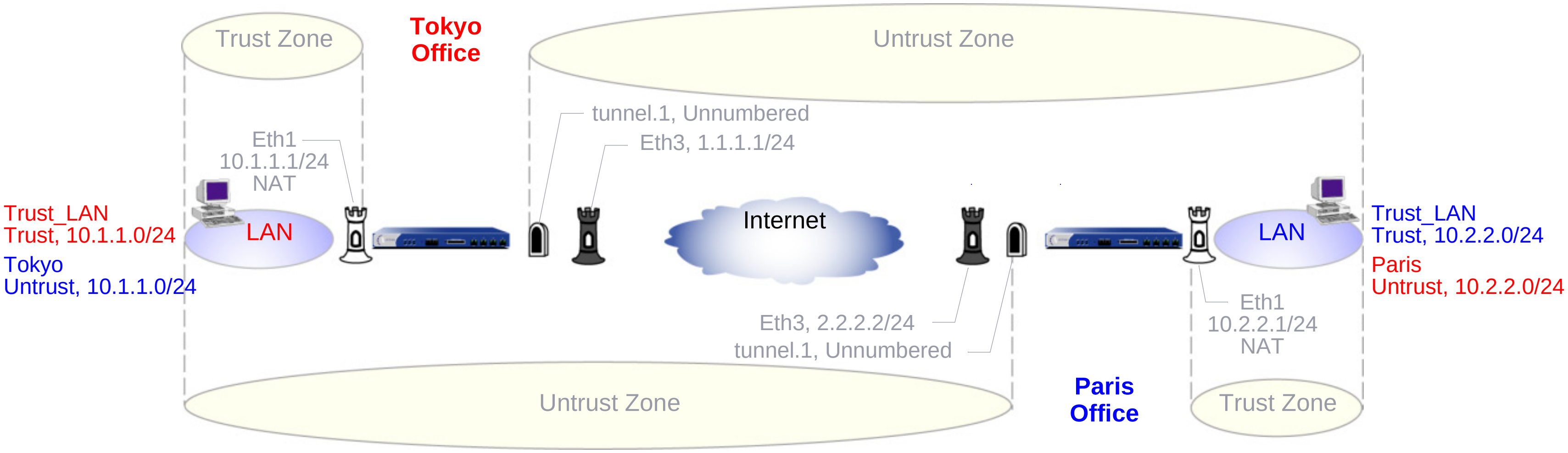
The admin at the Tokyo office configures the security zone and tunnel interfaces with the settings that appear in red in the above illustration. The admin at the Paris office does likewise with the settings that appear in blue.

Ethernet3 is going to be the outgoing interface for VPN traffic and the remote gateway for VPN traffic sent from the other end of the tunnel.

Ethernet1 is in NAT mode so each admin can assign IP addresses to all the internal hosts, yet when traffic passes from the Trust zone to the Untrust zone, the NetScreen device translates the source IP address in the packet headers to the address of the Untrust zone interface, ethernet3—1.1.1.1 for Tokyo, and 2.2.2.2 for Paris.

For a route-based VPN, each admin binds the tunnel interface tunnel.1 to the VPN tunnel vpn1. By defining a route to the address space of the remote office LAN, the NetScreen device can direct all traffic bound for that LAN to the tunnel.1 interface and thus through the tunnel to which tunnel.1 is bound.

Because policy-based NAT services are not needed, a route-based VPN configuration does not require tunnel.1 to have an IP address/netmask, and a policy-based VPN configuration does not even require a tunnel interface.



2. Addresses

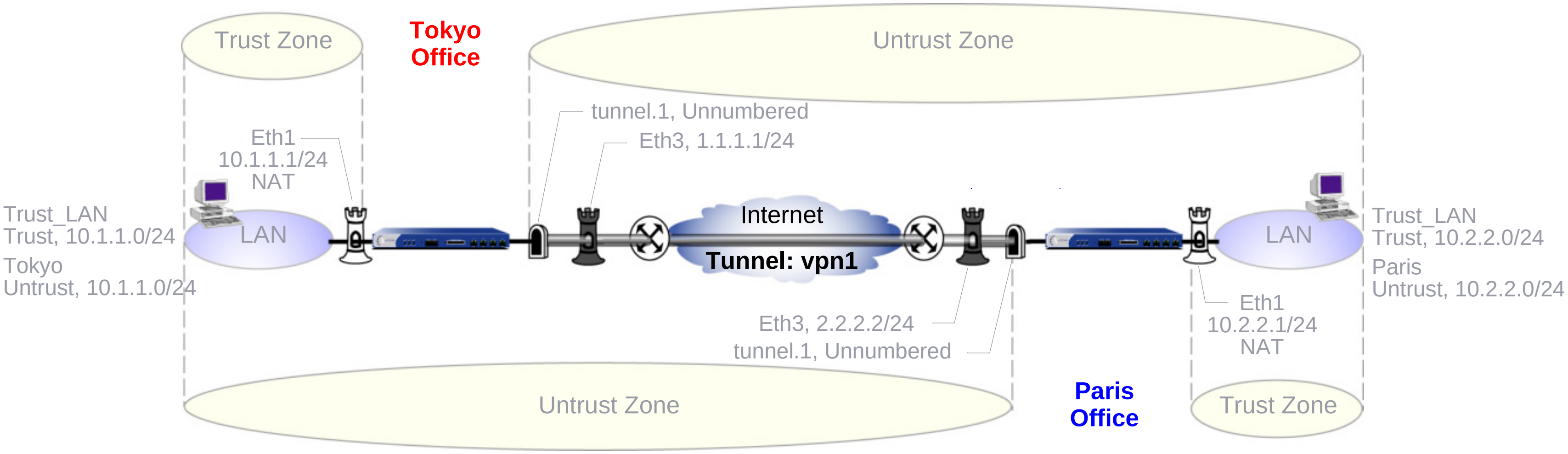
The admins define addresses for later use in inbound and outbound policies. The admin at the Tokyo office defines the addresses that appear in red in the above illustration. The admin at the Paris office does likewise with the addresses that appear in blue.

For policy-based VPNs, the NetScreen device derives proxy IDs from policies[1]. Because the proxy IDs used by the NetScreen devices at both ends of the VPN tunnel must match perfectly, you cannot use the predefined address “ANY”, whose IP address is 0.0.0.0/0, at one end of the tunnel if you use a more specific address at the other end. For example,

If the proxy ID in Tokyo is …		and the proxy ID in Paris is …	then the proxy IDs do not
From: 0.0.0.0/0	✗	To: 10.1.1.0/24	match and IKE
To: 10.2.2.0/24	✓	From: 10.2.2.0/24	negotiations will fail.
Service: ANY	✓	Service: ANY	

For route-based VPNs, you can use “0.0.0.0/0–0.0.0.0/0–any” to define the local and remote IP addresses and service type for a proxy ID. You can then use more restrictive policies to filter the inbound and outbound VPN traffic by source address, destination address, and service type.

[1] In ScreenOS 5.0.0, you can also define proxy IDs for VPN tunnels referenced in policy-based VPN configurations.



3. VPN

You can configure one of the following three VPNs:

– AutoKey IKE

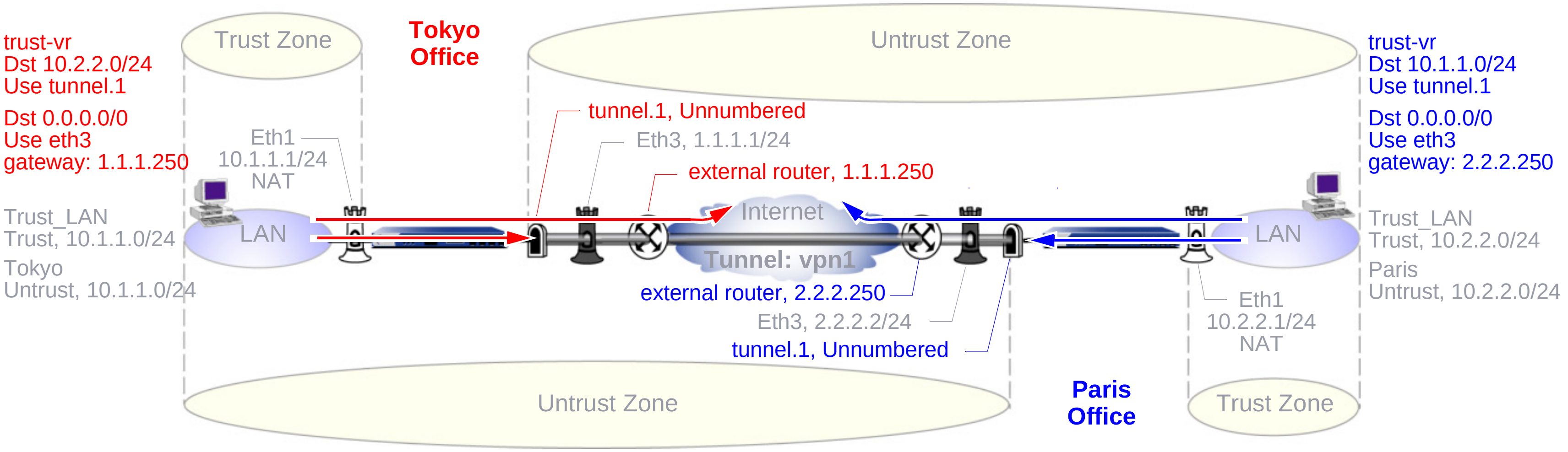
The AutoKey IKE method uses a preshared key or a certificate to refresh—that is, change—the encryption and authentication keys automatically at user-defined intervals (known as key lifetimes). Essentially, frequently updating these keys strengthens security, although excessively short lifetimes might reduce overall performance.

– Dynamic Peer

A dynamic peer is a remote gateway that has a dynamically assigned IP address. Because the IP address of the remote peer might be different each time IKE negotiations begin, hosts behind the peer must initiate VPN traffic. Also—if using a preshared key for authentication—the peer must send an IKE ID during the first message of Phase 1 negotiations in aggressive mode to identify itself.

– Manual Key

The Manual Key method requires you to set and update the encryption and authentication keys manually. This method is a viable option for a small set of VPN tunnels.

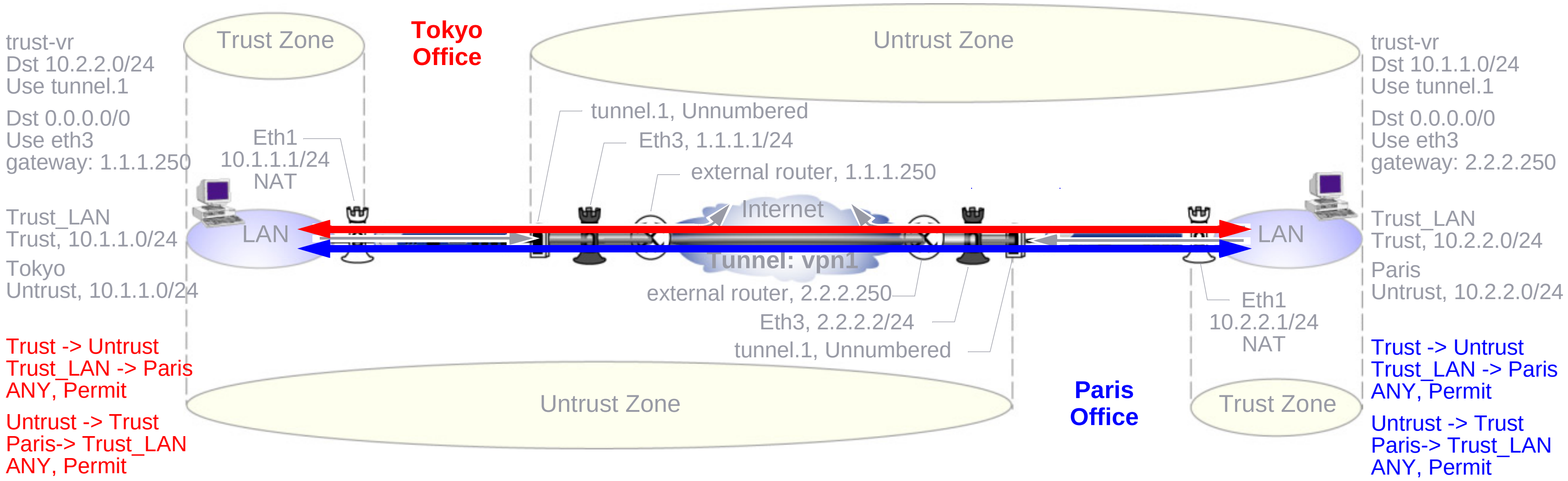


4. Routes

The admins at each site must configure at least the following two routes:

- A route for traffic to reach an address on the remote LAN to use tunnel.1
- A default route for all other traffic, including the outer VPN tunnel traffic, to reach the internet via ethernet3 and then the external router beyond it—1.1.1.250 for the Tokyo office and 2.2.2.250 for Paris[2]. The external router is the default gateway to which the NetScreen device forwards any traffic for which it does not have a specific route in its routing table.

[2] If the NetScreen device at the Tokyo office receives its external IP address dynamically from its ISP (that is, from the point of view of the Paris office, the NetScreen device at the Tokyo office is its dynamic peer), then the ISP automatically provides the Tokyo NetScreen with its default gateway IP address.



5. Policies

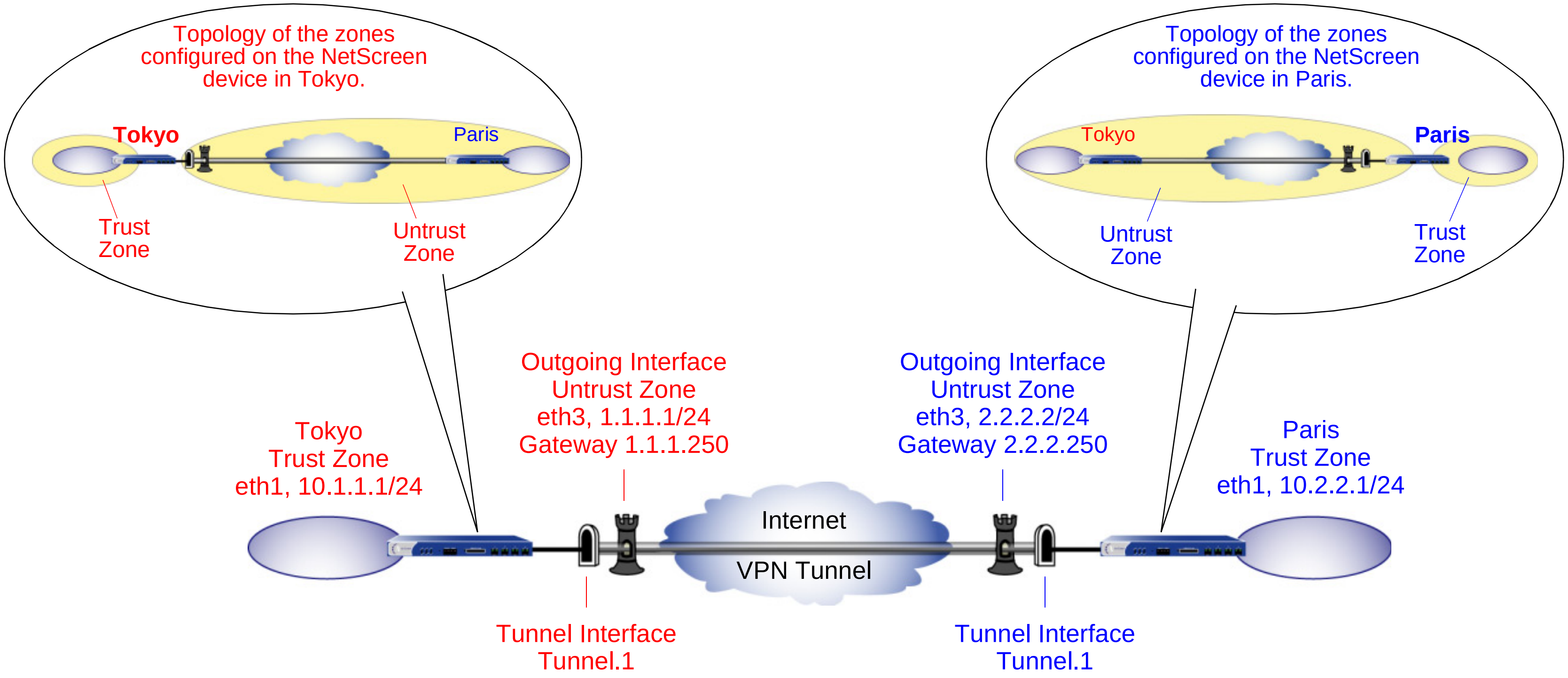
The admins at each site define policies to permit traffic between the two offices:

- A policy permitting any kind of traffic from “Trust_LAN” in the Trust zone to “Paris” or “Tokyo” in the Untrust zone
- A policy permitting any kind of traffic from “Paris” or “Tokyo” in the Untrust zone to “Trust_LAN” in the Trust zone

Because the route to the remote site specifies tunnel.1, which is bound to the VPN tunnel vpn1, the policy does not need to reference the VPN tunnel.

Example: Route-Based Site-to-Site VPN, AutoKey IKE

In this example, an AutoKey IKE tunnel using either a preshared secret or a pair of certificates (one at each end of the tunnel) provides the secure connection between the Tokyo and Paris offices. For the Phase 1 and 2 security levels, you specify one Phase 1 proposal—either pre-g2-3des-sha for the preshared key method or rsa-g2-3des-sha for certificates—and select the predefined “Compatible” set of proposals for Phase 2. All zones are in the trust-vr.


Topology of the zones configured on the NetScreen device in Tokyo.
Tokyo
Paris
Trust Zone
Untrust Zone
Topology of the zones configured on the NetScreen device in Paris.
Tokyo
Paris
Untrust Zone
Trust Zone
Outgoing Interface Untrust Zone eth3, 1.1.1.1/24 Gateway 1.1.1.250
Outgoing Interface Untrust Zone eth3, 2.2.2.2/24 Gateway 2.2.2.250
Tokyo Trust Zone eth1, 10.1.1.1/24
Paris Trust Zone eth1, 10.2.2.1/24
Internet
VPN Tunnel
Tunnel Interface Tunnel.1
Tunnel Interface Tunnel.1

Setting up a route-based AutoKey IKE tunnel using either a preshared secret or certificates involves the following steps:

1. Assign IP addresses to the physical interfaces bound to the security zones and to the tunnel interface.
2. Configure the VPN tunnel, designate its outgoing interface in the Untrust zone, bind it to the tunnel interface, and configure its proxy-ID.

3. Enter the IP addresses for the local and remote endpoints in the address books for the Trust and Untrust zones.
4. Enter a default route to the external router in the trust-vr, and a route to the destination via the tunnel interface.
5. Set up policies for VPN traffic to pass between each site.

In the following examples, the preshared key is h1p8A24nG5. It is assumed that both participants already have RSA certificates and are using Entrust as the certificate authority (CA). (For information about obtaining and loading certificates, see “Certificates and CRLs” on page 21.)

WebUI (Tokyo)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: ethernet3 (trust-vr)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Paris_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Paris

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 2.2.2.2

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Tokyo_Paris

Security Level: Compatible

Remote Gateway:

Predefined: (select), To_Paris

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Security Level: Compatible

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 10.1.1.0/24

Remote IP / Netmask: 10.2.2.0/24

Service: ANY

4. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.2.2.0/24

Gateway: (select)

Interface: Tunnel.1

Gateway IP Address: 0.0.0.0

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To Paris

Source Address: Trust_LAN

Destination Address: Paris_Office

Service: ANY

Action: Permit

Position at Top: (select)

Policies > (From: Untrust, To: Trust) > New: Enter the following, and then click **OK**:

Name: From Paris

Source Address: Paris_Office

Destination Address: Trust_LAN

Service: ANY

Action: Permit

Position at Top: (select)

WebUI (Paris)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.2.2.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: ethernet3 (trust-vr)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN
IP Address/Domain Name:
IP/Netmask: (select), 10.2.2.0/24
Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Tokyo

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 1.1.1.1

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level):
pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

Name: Paris_Tokyo

Security Level: Custom

Remote Gateway:

Predefined: (select), To_Tokyo

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Security Level: Compatible

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 10.2.2.0/24

Remote IP / Netmask: 10.1.1.0/24

Service: ANY

4. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.1.1.0/24

Gateway: (select)

Interface: Tunnel.1

Gateway IP Address: 0.0.0.0

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To Tokyo

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Tokyo_Office

Service: ANY

Action: Permit

Position at Top: (select)

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Name: From Tokyo

Source Address:

Address Book Entry: (select), Tokyo_Office

Destination Address:

Address Book Entry: (select), Trust_LAN

Service: ANY

Action: Permit

Position at Top: (select)

CLI (Tokyo)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. Addresses

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Paris_Office 10.2.2.0/24
```

3. VPN

Preshared Key

```
set ike gateway To_Paris address 2.2.2.2 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Tokyo_Paris gateway To_Paris sec-level compatible
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

(or)

Certificate

```
set ike gateway To_Paris address 2.2.2.2 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway To_Paris cert peer-ca 1[3]
set ike gateway To_Paris cert peer-cert-type x509-sig
set vpn Tokyo_Paris gateway To_Paris sec-level compatible
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

4. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
```

5. Policies

```
set policy top name “To Paris” from trust to untrust Trust_LAN Paris_Office any
    permit
set policy top name “From Paris” from untrust to trust Paris_Office Trust_LAN
    any permit
save
```

[3] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get ike ca**.

CLI (Paris)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. Addresses

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust Tokyo_Office 10.1.1.0/24
```

3. VPN

Preshared Key

```
set ike gateway To_Tokyo address 1.1.1.1 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Paris_Tokyo gateway To_Tokyo sec-level compatible
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

(or)

Certificate

```
set ike gateway To_Tokyo address 1.1.1.1 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway To_Tokyo cert peer-ca 1
set ike gateway To_Tokyo cert peer-cert-type x509-sig
set vpn Paris_Tokyo gateway To_Tokyo sec-level compatible
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

4. Routes

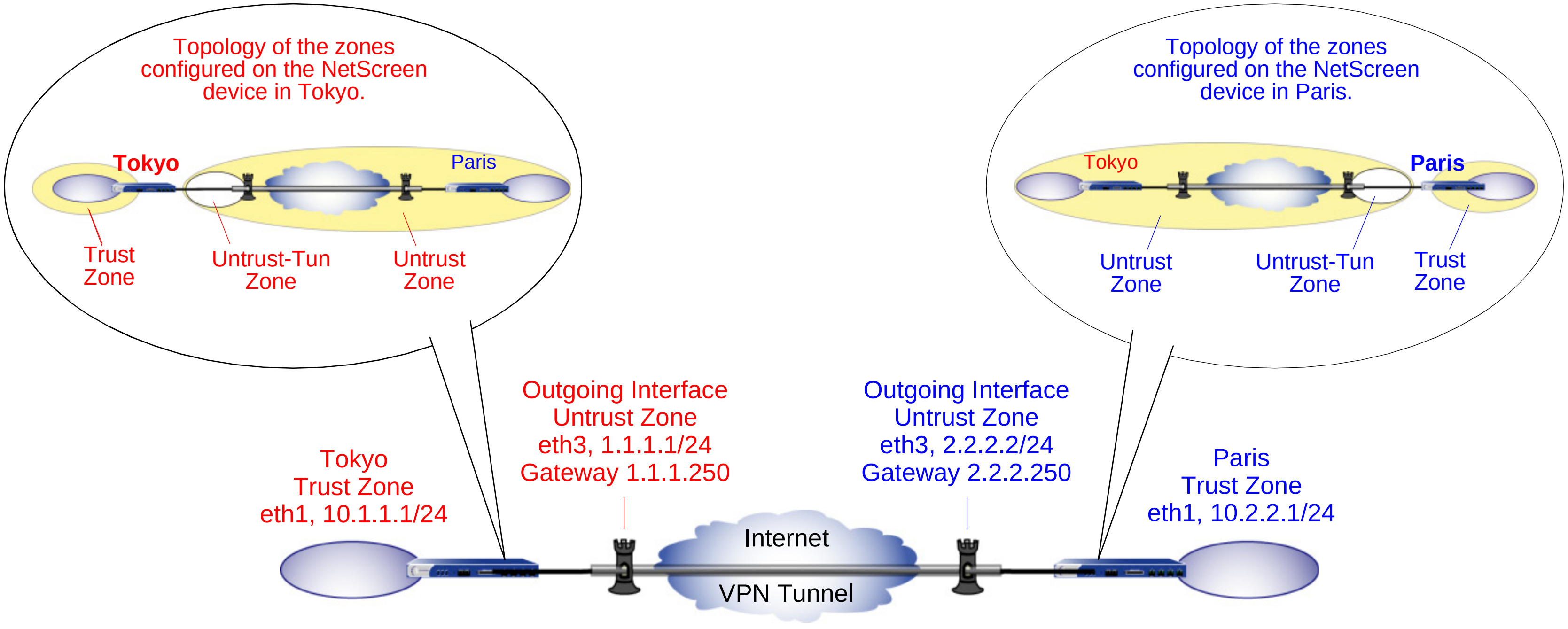
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
```

5. Policies

```
set policy top name “To Tokyo” from trust to untrust Trust_LAN Tokyo_Office any
    permit
set policy top name “From Tokyo” from untrust to trust Tokyo_Office Trust_LAN
    any permit
save
```

Example: Policy-Based Site-to-Site VPN, AutoKey IKE

In this example, an AutoKey IKE tunnel using either a preshared secret or a pair of certificates (one at each end of the tunnel) provides the secure connection between the Tokyo and Paris offices. For the Phase 1 and 2 security levels, you specify one Phase 1 proposal—either pre-g2-3des-sha for the preshared key method or rsa-g2-3des-sha for certificates—and select the predefined “Compatible” set of proposals for Phase 2. All zones are in the trust-vr.


Topology of the zones configured on the NetScreen device in Tokyo.
Tokyo
Paris
Trust Zone
Untrust-Tun Zone
Untrust Zone
Topology of the zones configured on the NetScreen device in Paris.
Tokyo
Paris
Untrust Zone
Untrust-Tun Zone
Trust Zone
Outgoing Interface Untrust Zone eth3, 1.1.1.1/24 Gateway 1.1.1.250
Outgoing Interface Untrust Zone eth3, 2.2.2.2/24 Gateway 2.2.2.250
Tokyo Trust Zone eth1, 10.1.1.1/24
Paris Trust Zone eth1, 10.2.2.1/24
Internet
VPN Tunnel

Setting up the AutoKey IKE tunnel using AutoKey IKE with either a preshared secret or certificates involves the following steps:

1. Define security zone interface IP addresses.
2. Make address book entries for the local and remote end entities.

3. Define the remote gateway and key exchange mode, and specify either a preshared secret or a certificate.
4. Create the Autokey IKE VPN.
5. Set a default route to the external router.
6. Configure policies.

In the following examples, the preshared key is h1p8A24nG5. It is assumed that both participants already have RSA certificates and are using Entrust as the certificate authority (CA). (For information about obtaining and loading certificates, see “Certificates and CRLs” on page 21.)

WebUI (Tokyo)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Paris_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Paris

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 2.2.2.2

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **OK** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **OK** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Main (ID Protection)

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Tokyo_Paris

Security Level: Compatible

Remote Gateway: Predefined: (select), To_Paris

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To/From Paris

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Paris_Office

Service: ANY

Action: Tunnel

Tunnel VPN: Tokyo_Paris

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

WebUI (Paris)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.2.2.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.2/24

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Tokyo

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 1.1.1.1

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Main (ID Protection)

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Paris_Tokyo

Security Level: Compatible

Remote Gateway: Predefined: (select), To_Tokyo

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To/From Tokyo

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Tokyo_Office

Service: ANY

Action: Tunnel

Tunnel VPN: Paris_Tokyo

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

CLI (Tokyo)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Addresses

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust paris_office 10.2.2.0/24
```

3. VPN

Preshared Key

```
set ike gateway to_paris address 2.2.2.2 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn tokyo_paris gateway to_paris sec-level compatible
```

(or)

Certificates

```
set ike gateway to_paris address 2.2.2.2 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway to_paris cert peer-ca 1[4]
set ike gateway to_paris cert peer-cert-type x509-sig
set vpn tokyo_paris gateway to_paris sec-level compatible
```

[4] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get ike ca**.

4. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. Policies

```
set policy top name “To/From Paris” from trust to untrust Trust_LAN
    paris_office any tunnel vpn tokyo_paris
set policy top name “To/From Paris” from untrust to trust paris_office
    Trust_LAN any tunnel vpn tokyo_paris
save
```

CLI (Paris)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
```

2. Addresses

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust tokyo_office 10.1.1.0/24
```

3. VPN

Preshared Key

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn paris_tokyo gateway to_tokyo sec-level compatible
```

(or)

Certificates

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway to_tokyo cert peer-ca 1
set ike gateway to_tokyo cert peer-cert-type x509-sig
set vpn paris_tokyo gateway to_tokyo tunnel proposal nopfs-esp-3des-sha
```

4. Route

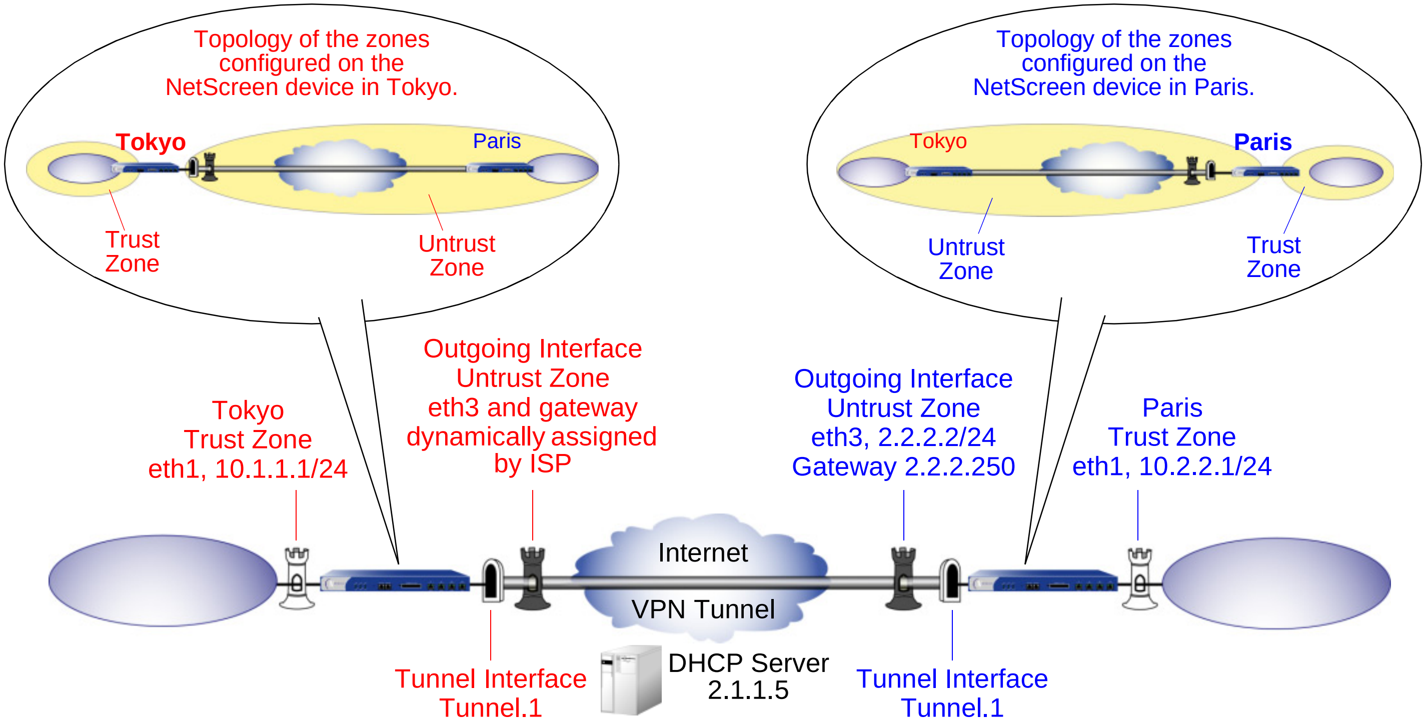
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

5. Policies

```
set policy top name “To/From Tokyo” from trust to untrust Trust_LAN
    tokyo_office any tunnel vpn paris_tokyo
set policy top name “To/From Tokyo” from untrust to trust tokyo_office
    Trust_LAN any tunnel vpn paris_tokyo
save
```

Example: Route-Based Site-to-Site VPN, Dynamic Peer

In this example, an AutoKey IKE VPN tunnel using either a preshared key or a pair of certificates (one at each end of the tunnel) provides a secure connection between NetScreen devices protecting the Tokyo and Paris offices. The Untrust zone interface for the NetScreen device at the Paris office has a static IP address. The ISP serving the Tokyo office assigns the IP address for the Untrust zone interface dynamically via DHCP. Because only the Paris NetScreen device has a fixed address for its Untrust zone, VPN traffic must originate from hosts in the Tokyo office. After a tunnel has been established, traffic through the tunnel can originate from either end. All security and tunnel zones are in the trust-vr.


Topology of the zones configured on the NetScreen device in Tokyo.
Tokyo
Paris
Trust Zone
Untrust Zone
Topology of the zones configured on the NetScreen device in Paris.
Tokyo
Paris
Untrust Zone
Trust Zone
Tokyo Trust Zone eth1, 10.1.1.1/24
Outgoing Interface Untrust Zone eth3 and gateway dynamically assigned by ISP
Outgoing Interface Untrust Zone eth3, 2.2.2.2/24 Gateway 2.2.2.250
Paris Trust Zone eth1, 10.2.2.1/24
Internet
VPN Tunnel
Tunnel Interface Tunnel.1
DHCP Server 2.1.1.5
Tunnel Interface Tunnel.1

The preshared key is h1p8A24nG5. It is assumed that both participants already have RSA certificates from the certificate authority (CA) Verisign, and that the e-mail address *pmason@abc.com* appears in the local certificate on NetScreen-A. (For information about obtaining and loading certificates, see "Certificates and CRLs" on page 21.) For the Phase 1 and 2 security levels, you specify one Phase 1 proposal—either pre-g2-3des-sha for the preshared key method or rsa-g2-3des-sha for certificates—and select the "Compatible" set of proposals for Phase 2.

WebUI (Tokyo)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **Apply**:

Zone Name: Untrust

Enter the following, and then click **OK**:

Obtain IP using DHCP: (select)[5]

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: ethernet3 (trust-vr)

[5] You cannot specify the IP address of the DHCP server through the WebUI; however, you can do so through the CLI.

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Paris_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Paris

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 2.2.2.2

Preshared Key

Preshared Key: h1p8A24nG5

Local ID: pmason@abc.com

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(or)

Certificates

Local ID: pmason@abc.com[6]

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

[6] The U-FQDN “pmason@abc.com” must appear in the SubjectAltName field in the certificate.

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Tokyo_Paris

Security Level: Compatible

Remote Gateway:

Predefined: (select), To_Paris

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface: (select), tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 10.1.1.0/24

Remote IP / Netmask: 10.2.2.0/24

Service: ANY

4. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 0.0.0.0[7]

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.2.2.0/24

Gateway: (select)

Interface: Tunnel.1

Gateway IP Address: 0.0.0.0

[7] The ISP provides the gateway IP address dynamically through DHCP.

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Paris_Office

Service: Any

Action: Permit

Position at Top: (select)

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Paris_Office

Destination Address:

Address Book Entry: (select), Trust_LAN

Service: Any

Action: Permit

Position at Top: (select)

WebUI (Paris)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.2.2.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: ethernet3 (trust-vr)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Tokyo

Security Level: Custom

Remote Gateway Type:

Dynamic IP Address: (select), Peer ID: pmason@abc.com

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Paris_Tokyo

Security Level: Compatible

Remote Gateway:

Predefined: (select), To_Tokyo

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface: (select), tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 10.2.2.0/24

Remote IP / Netmask: 10.1.1.0/24

Service: ANY

4. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: (select), 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.1.1.0/24

Gateway: (select)

Interface: Tunnel.1

Gateway IP Address: 0.0.0.0

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Tokyo_Office

Service: Any

Action: Permit

Position at Top: (select)

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Tokyo_Office

Destination Address:

Address Book Entry: (select), Trust_LAN

Service: Any

Action: Permit

Position at Top: (select)

CLI (Tokyo)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 dhcp client
set interface ethernet3 dhcp client settings server 1.1.1.5

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. Addresses

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Paris_Office 10.2.2.0/24
```

3. VPN

Preshared Key

```
set ike gateway To_Paris address 2.2.2.2 aggressive local-id pmason@abc.com
    outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Tokyo_Paris gateway To_Paris tunnel proposal nopfs-esp-3des-sha
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

(or)

Certificates

```
set ike gateway To_Paris address 2.2.2.2 aggressive local-id pmason@abc.com[8]
    outgoing-interface ethernet3 proposal rsa-g2-3des-sha
set ike gateway To_Paris cert peer-ca 1[9]
set ike gateway To_Paris cert peer-cert-type x509-sig
set vpn Tokyo_Paris gateway To_Paris tunnel proposal nopfs-esp-3des-sha
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

4. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3[10]
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
```

5. Policies

```
set policy top from trust to untrust Trust_LAN Paris_Office any permit
set policy top from untrust to trust Paris_Office Trust_LAN any permit
save
```

[8] The U-FQDN “pmason@abc.com” must appear in the SubjectAltName field in the certificate.

[9] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get ike ca**.

[10] The ISP provides the gateway IP address dynamically through DHCP, so you cannot specify it here.

CLI (Paris)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. Addresses

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust Tokyo_Office 10.1.1.0/24
```

3. VPN

Preshared Key

```
set ike gateway To_Tokyo dynamic pmason@abc.com aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Paris_Tokyo gateway To_Tokyo tunnel proposal nopfs-esp-3des-sha
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

(or)

Certificates

```
set ike gateway To_Tokyo dynamic pmason@abc.com aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway To_Tokyo cert peer-ca 1[11]
set ike gateway To_Tokyo cert peer-cert-type x509-sig
set vpn Paris_Tokyo gateway To_Tokyo tunnel proposal nopfs-esp-3des-sha
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

4. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
```

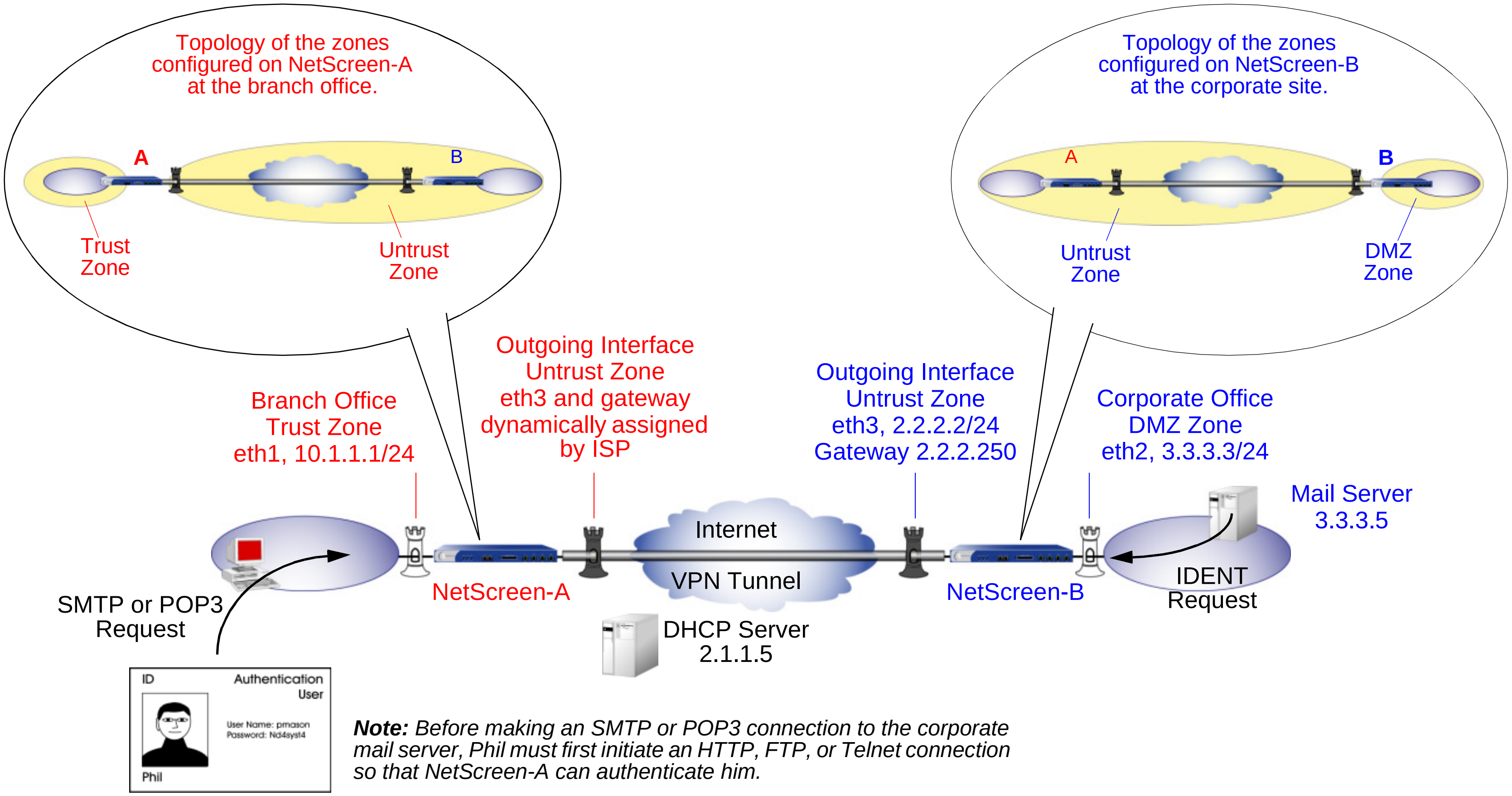
5. Policies

```
set policy top from trust to untrust Trust_LAN Tokyo_Office any permit
set policy top from untrust to trust Tokyo_Office Trust_LAN any permit
save
```

[11] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get ike ca**.

Example: Policy-Based Site-to-Site VPN, Dynamic Peer

In this example, a VPN tunnel securely connects the users in the Trust zone behind NetScreen-A to the mail server in the corporate DMZ zone, protected by NetScreen-B. The Untrust zone interface for NetScreen-B has a static IP address. The ISP serving NetScreen-A assigns the IP address for its Untrust zone interface dynamically via DHCP. Because only NetScreen-B has a fixed address for its Untrust zone, VPN traffic must originate from hosts behind NetScreen-A. After NetScreen-A has established the tunnel, traffic through the tunnel can originate from either end. All zones are in the trust-vr routing domain.



Note: *Before making an SMTP or POP3 connection to the corporate mail server, Phil must first initiate an HTTP, FTP, or Telnet connection so that NetScreen-A can authenticate him.*

In this example, the local auth user Phil (login name: pmason; password: Nd4syst4) wants to get his e-mail from the mail server at the corporate site. When he attempts to do so, he is authenticated twice: first, NetScreen-A authenticates him locally before allowing traffic from him through the tunnel[12]; second, the mail server program authenticates him, sending the IDENT request through the tunnel.

Note: *The mail server can send the IDENT request through the tunnel only if the NetScreen-A and B administrators add a custom service for it (TCP, port 113) and set up policies allowing that traffic through the tunnel to the 10.10.10.0/24 subnet.*

The preshared key is h1p8A24nG5. It is assumed that both participants already have RSA certificates from the certificate authority (CA) Verisign, and that the e-mail address *pmason@abc.com* appears in the local certificate on NetScreen-A. (For information about obtaining and loading certificates, see "Certificates and CRLs" on page 21.) For the Phase 1 and 2 security levels, you specify one Phase 1 proposal—either pre-g2-3des-sha for the preshared key method or rsa-g2-3des-sha for certificates—and select the predefined "Compatible" set of proposals for Phase 2.

WebUI (NetScreen-A)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

[12] Because Phil is an authentication user, before he can make an SMTP of POP3 request, he must first initiate an HTTP, FTP, or Telnet connection so that NetScreen-A can respond with a firewall user/login prompt to authenticate him. After NetScreen-A authenticates him, he has permission to contact the corporate mail server via the VPN tunnel.

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Obtain IP using DHCP: (select)[13]

2. User

Objects > Users > Local > New: Enter the following, and then click **OK**:

User Name: pmason

Status: Enable

Authentication User: (select)

User Password: Nd4syst4

Confirm Password: Nd4syst4

3. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trusted network

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Mail Server

IP Address/Domain Name:

IP/Netmask: (select), 3.3.3.5/32

Zone: Untrust

[13] You cannot specify the IP address of the DHCP server through the WebUI; however, you can do so through the CLI.

4. Services

Objects > Services > Custom > New: Enter the following, and then click **OK**:

Service Name: Ident

Service Timeout:

Use protocol default: (select)

Transport Protocol: TCP (select)

Source Port: Low 0, High 65535

Destination Port: Low 113, High 113

Objects > Services > Group > New: Enter the following, move the following services, and then click **OK**:

Group Name: Remote_Mail

Group Members << Available Members:

HTTP
FTP
Telnet
Ident
MAIL
POP3

5. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Mail

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 2.2.2.2

Preshared Key

Preshared Key: h1p8A24nG5

Local ID: pmason@abc.com

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(or)

Certificates

Local ID: pmason@abc.com

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

Name: branch_corp

Security Level: Compatible

Remote Gateway Tunnel: To_Mail

6. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 0.0.0.0[14]

7. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Trusted network

Destination Address:

Address Book Entry: (select), Mail Server

Service: Remote_Mail

Action: Tunnel

VPN Tunnel: branch_corp

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

[14] The ISP provides the gateway IP address dynamically through DHCP.

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

Authentication: (select)

Auth Server: Local

User: (select), Local Auth User - pmason

WebUI (NetScreen-B)

1. Interfaces

Network > Interfaces > Edit (for ethernet2): Enter the following, and then click **OK**:

Zone Name: DMZ

Static IP: (select this option when present)

IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.2/24

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Mail Server

IP Address/Domain Name:

IP/Netmask: (select), 3.3.3.5/32

Zone: DMZ

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: branch office

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Untrust

3. Services

Objects > Services > Custom > New: Enter the following, and then click **OK**:

Service Name: Ident

Service Timeout:

Use protocol default: (select)

Transport Protocol: TCP (select)

Source Port: Low 0, High 65535

Destination Port: Low 113, High 113

Objects > Services > Group > New: Enter the following, move the following services, and then click **OK**:

Group Name: Remote_Mail

Group Members << Available Members:

Ident

MAIL

POP3

4. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_branch

Security Level: Custom

Remote Gateway Type:

Dynamic IP Address: (select), Peer ID: pmason@abc.com

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: corp_branch

Security Level: Compatible

Remote Gateway:

Predefined: (select), To_branch

5. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

6. Policies

Policies > (From: DMZ, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Mail Server

Destination Address:

Address Book Entry: (select), branch office

Service: Remote_Mail

Action: Tunnel

VPN Tunnel: corp_branch

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

CLI (NetScreen-A)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 dhcp client
set interface ethernet3 dhcp client settings server 1.1.1.5
```

2. User

```
set user pmason password Nd4syst4
```

3. Addresses

```
set address trust “trusted network” 10.1.1.0/24
set address untrust “mail server” 3.3.3.5/32
```

4. Services

```
set service ident protocol tcp src-port 0-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add http
set group service remote_mail add ftp
set group service remote_mail add telnet
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

5. VPN

Preshared Key

```
set ike gateway to_mail address 2.2.2.2 aggressive local-id pmason@abc.com
    outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn branch_corp gateway to_mail sec-level compatible
```

(or)

Certificates

```
set ike gateway to_mail address 2.2.2.2 aggressive local-id pmason@abc.com[15]
    outgoing-interface ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_mail cert peer-ca 1[16]
set ike gateway to_mail cert peer-cert-type x509-sig
set vpn branch_corp gateway to_mail sec-level compatible
```

6. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3[17]
```

7. Policies

```
set policy top from trust to untrust “trusted network” “mail server”
    remote_mail tunnel vpn branch_corp auth server Local user pmason
set policy top from untrust to trust “mail server” “trusted network”
    remote_mail tunnel vpn branch_corp
save
```

[15] The U-FQDN “pmason@abc.com” must appear in the SubjectAltName field in the certificate.

[16] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get ike ca**.

[17] The ISP provides the gateway IP address dynamically through DHCP.

CLI (NetScreen-B)

1. **Interfaces**

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 3.3.3.3/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
```

2. **Addresses**

```
set address dmz “mail server” 3.3.3.5/32
set address untrust “branch office” 10.1.1.0/24
```

3. **Services**

```
set service ident protocol tcp src-port 0-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

4. **VPN**

Preshared Key

```
set ike gateway to_branch dynamic pmason@abc.com aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn corp_branch gateway to_branch tunnel sec-level compatible
```

(or)

Certificates

```
set ike gateway to_branch dynamic pmason@abc.com aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_branch cert peer-ca 1[18]
set ike gateway to_branch cert peer-cert-type x509-sig
set vpn corp_branch gateway to_branch sec-level compatible
```

5. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

6. Policies

```
set policy top from dmz to untrust “mail server” “branch office” remote_mail
    tunnel vpn corp_branch
set policy top from untrust to dmz “branch office” “mail server” remote_mail
    tunnel vpn corp_branch
save
```

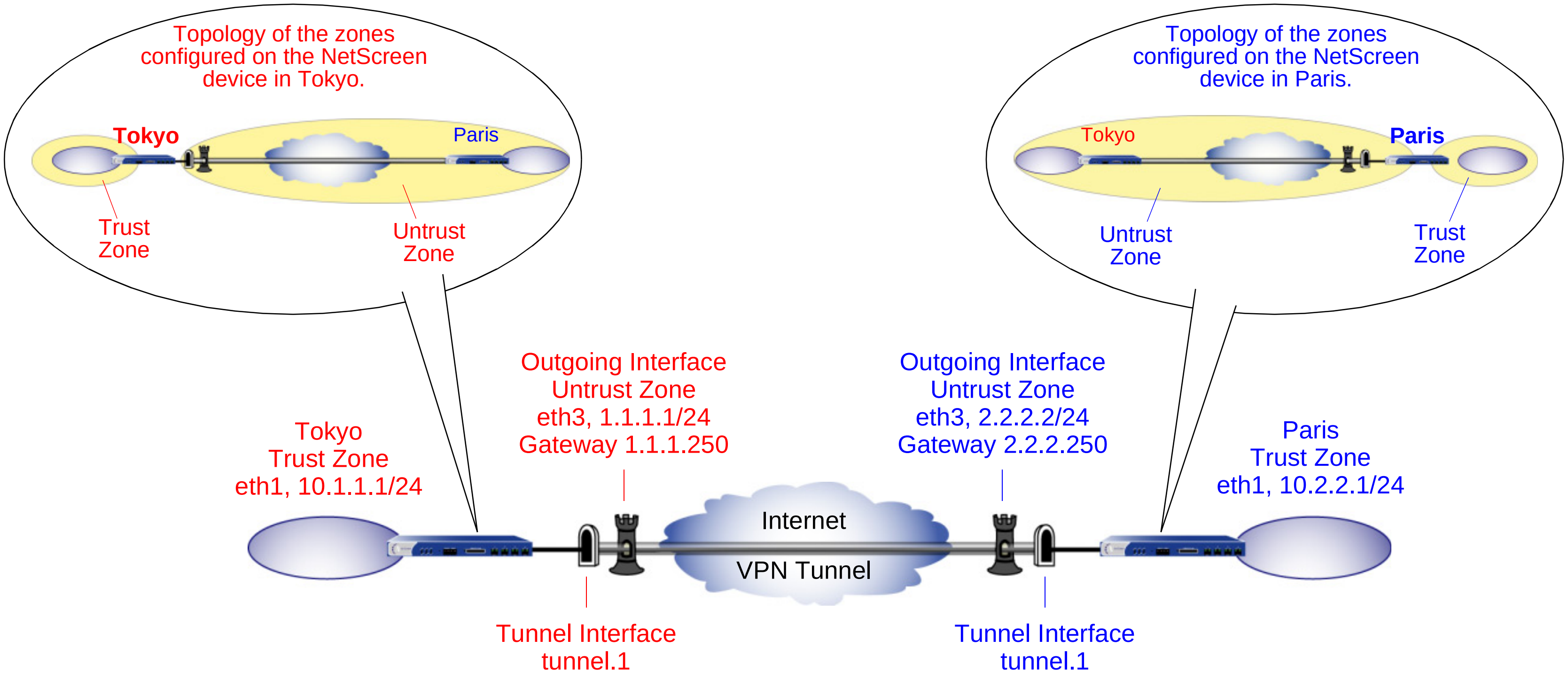
[18] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get ike ca**.

Example: Route-Based Site-to-Site VPN, Manual Key

In this example, a Manual Key tunnel provides a secure communication channel between offices in Tokyo and Paris. The Trust zones at each site are in NAT mode. The addresses are as follows:

- Tokyo:
  - Trust zone interface (ethernet1): 10.1.1.1/24
  - Untrust zone interface (ethernet3): 1.1.1.1/24
- Paris:
  - Trust zone interface (ethernet1): 10.2.2.1/24
  - Untrust zone interface (ethernet3): 2.2.2.2/24

The Trust and Untrust security zones and the Untrust-Tun tunnel zone are all in the trust-vr routing domain. The Untrust zone interface (ethernet3) serves as the outgoing interface for the VPN tunnel.



To set up the tunnel, perform the following steps on the NetScreen devices at both ends of the tunnel:

1. Assign IP addresses to the physical interfaces bound to the security zones and to the tunnel interface.
2. Configure the VPN tunnel, designate its outgoing interface in the Untrust zone, and bind it to the tunnel interface.
3. Enter the IP addresses for the local and remote endpoints in the address books for the Trust and Untrust zones.
4. Enter a default route to the external router in the trust-vr, and a route to the destination via the tunnel interface.
5. Set up policies for VPN traffic to pass between each site.

WebUI (Tokyo)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK** :

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: ethernet3 (trust-vr)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Paris_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Untrust

3. VPN

VPNs > Manual Key > New: Enter the following, and then click **OK**:

VPN Tunnel Name: Tokyo_Paris

Gateway IP: 2.2.2.2

Security Index: 3020 (Local), 3030 (Remote)

Outgoing Interface: ethernet3

ESP-CBC: (select)

Encryption Algorithm: 3DES-CBC

Generate Key by Password: asdlk24234

Authentication Algorithm: SHA-1

Generate Key by Password: PNas134a

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Manual Key tunnel configuration page:

Bind to: Tunnel Interface, tunnel.1

4. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.2.2.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To Paris

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Paris_Office

Service: ANY

Action: Permit

Position at Top: (select)

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Name: From Paris

Source Address:

Address Book Entry: (select), Paris_Office

Destination Address:

Address Book Entry: (select), Trust_LAN

Service: ANY

Action: Permit

Position at Top: (select)

WebUI (Paris)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.2.2.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: ethernet3 (trust-vr)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Untrust

3. VPN

VPNs > Manual Key > New: Enter the following, and then click **OK**:

VPN Tunnel Name: Paris_Tokyo

Gateway IP: 1.1.1.1

Security Index: 3030 (Local), 3020 (Remote)

Outgoing Interface: ethernet3

ESP-CBC: (select)

Encryption Algorithm: 3DES-CBC

Generate Key by Password: asdlk24234

Authentication Algorithm: SHA-1

Generate Key by Password: PNas134a

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Manual Key tunnel configuration page:

Bind to: Tunnel Interface, tunnel.1

4. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.1.1.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To Tokyo

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Tokyo_Office

Service: ANY

Action: Permit

Position at Top: (select)

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Name: From Tokyo

Source Address:

Address Book Entry: (select), Tokyo_Office

Destination Address:

Address Book Entry: (select), Trust_LAN

Service: ANY

Action: Permit

Position at Top: (select)

CLI (Tokyo)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. Addresses

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Paris_Office 10.2.2.0/24
```

3. VPN

```
set vpn Tokyo_Paris manual 3020 3030 gateway 2.2.2.2 outgoing-interface
    ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
set vpn Tokyo_Paris bind interface tunnel.1
```

4. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
```

5. Policies

```
set policy top name “To Paris” from trust to untrust Trust_LAN Paris_Office any
    permit
set policy top name “From Paris” from untrust to trust Paris_Office Trust_LAN
    any permit
save
```

CLI (Paris)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. Addresses

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust Tokyo_Office 10.1.1.0/24
```

3. VPN

```
set vpn Paris_Tokyo manual 3030 3020 gateway 1.1.1.1 outgoing-interface
    ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
set vpn Paris_Tokyo bind interface tunnel.1
```

4. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
```

5. Policies

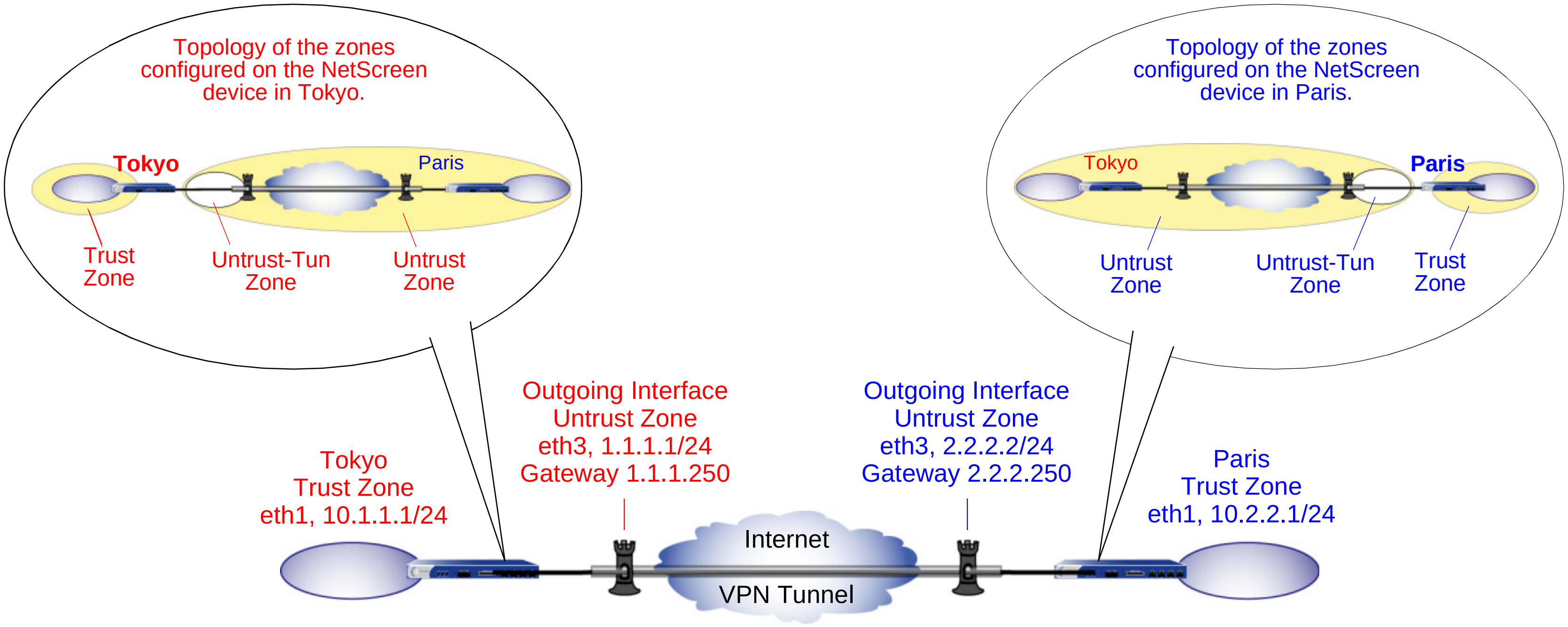
```
set policy top name “To Tokyo” from trust to untrust Trust_LAN Tokyo_Office any
    permit
set policy top name “From Tokyo” from untrust to trust Tokyo_Office Trust_LAN
    any permit
save
```

Example: Policy-Based Site-to-Site VPN, Manual Key

In this example, a Manual Key tunnel provides a secure communication channel between offices in Tokyo and Paris, using ESP with 3DES encryption and SHA-1 authentication. The Trust zones at each site are in NAT mode. The addresses are as follows:

- Tokyo:
  - Trust interface (ethernet1): 10.1.1.1/24
  - Untrust interface (ethernet3): 1.1.1.1/24
- Paris:
  - Trust interface (ethernet1): 10.2.2.1/24
  - Untrust interface (ethernet3): 2.2.2.2/24

The Trust and Untrust security zones and the Untrust-Tun tunnel zone are in the trust-vr routing domain. The Untrust zone interface (ethernet3) serves as the outgoing interface for the VPN tunnel.


Topology of the zones configured on the NetScreen device in Tokyo.
Tokyo
Paris
Trust Zone
Untrust-Tun Zone
Untrust Zone
Topology of the zones configured on the NetScreen device in Paris.
Tokyo
Paris
Untrust Zone
Untrust-Tun Zone
Trust Zone
Outgoing Interface Untrust Zone eth3, 1.1.1.1/24 Gateway 1.1.1.250
Outgoing Interface Untrust Zone eth3, 2.2.2.2/24 Gateway 2.2.2.250
Tokyo Trust Zone eth1, 10.1.1.1/24
Paris Trust Zone eth1, 10.2.2.1/24
Internet
VPN Tunnel

To set up the tunnel, perform the following five steps on the NetScreen devices at both ends of the tunnel:

1. Assign IP addresses to the physical interfaces bound to the security zones.
2. Configure the VPN tunnel, and designate its outgoing interface in the Untrust zone.
3. Enter the IP addresses for the local and remote endpoints in the Trust and Untrust address books.
4. Enter a default route to the external router.
5. Set up policies for VPN traffic to pass bidirectionally through the tunnel.

WebUI (Tokyo)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Paris_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Untrust

3. VPN

VPNs > Manual Key > New: Enter the following, and then click **OK**:

VPN Tunnel Name: Tokyo_Paris

Gateway IP: 2.2.2.2

Security Index: 3020 (Local), 3030 (Remote)

Outgoing Interface: ethernet3

ESP-CBC: (select)

Encryption Algorithm: 3DES-CBC

Generate Key by Password: asdlk24234

Authentication Algorithm: SHA-1

Generate Key by Password: PNas134a

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Manual Key tunnel configuration page:

Bind to: Tunnel Zone, Untrust-Tun

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To/From Paris

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Paris_Office

Service: ANY

Action: Tunnel

Tunnel VPN: Tokyo_Paris

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

WebUI (Paris)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.2.2.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.2/24

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Untrust

3. VPN

VPNs > Manual Key > New: Enter the following, and then click **OK**:

VPN Tunnel Name: Paris_Tokyo

Gateway IP: 1.1.1.1

Security Index (HEX Number): 3030 (Local), 3020 (Remote)

Outgoing Interface: ethernet3

ESP-CBC: (select)

Encryption Algorithm: 3DES-CBC

Generate Key by Password: asdlk24234

Authentication Algorithm: SHA-1

Generate Key by Password: PNas134a

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Manual Key tunnel configuration page:

Bind to: Tunnel Zone, Untrust-Tun

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To/From Tokyo

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Tokyo_Office

Service: ANY

Action: Tunnel

Tunnel VPN: Paris_Tokyo

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

CLI (Tokyo)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Addresses

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust paris_office 10.2.2.0/24
```

3. VPN

```
set vpn tokyo_paris manual 3020 3030 gateway 2.2.2.2 outgoing-interface
    ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
set vpn tokyo_paris bind zone untrust-tun
```

4. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. Policies

```
set policy top name “To/From Paris” from trust to untrust Trust_LAN
    paris_office any tunnel vpn tokyo_paris
set policy top name “To/From Paris” from untrust to trust paris_office
    Trust_LAN any tunnel vpn tokyo_paris
save
```

CLI (Paris)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
```

2. Addresses

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust tokyo_office 10.1.1.0/24
```

3. VPN

```
set vpn paris_tokyo manual 3030 3020 gateway 1.1.1.1 outgoing-interface
    ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
set vpn paris_tokyo bind zone untrust-tun
```

4. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

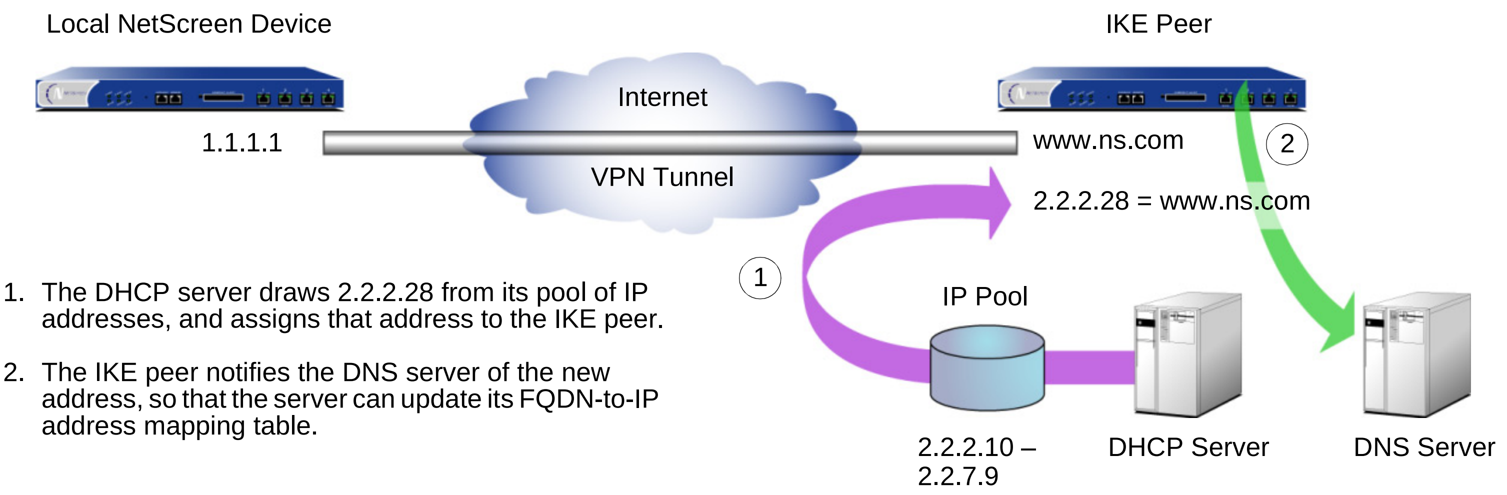
5. Policies

```
set policy top name “To/From Tokyo” from trust to untrust Trust_LAN
    tokyo_office any tunnel vpn paris_tokyo
set policy top name “To/From Tokyo” from untrust to trust tokyo_office
    Trust_LAN any tunnel vpn paris_tokyo
save
```

FQDN FOR DYNAMIC IKE GATEWAYS

For an IKE peer that has a static fully qualified domain name (FQDN) but a dynamically assigned IP address, you can specify the FQDN in the local configuration for the remote gateway. For example, an Internet service provider (ISP) might assign IP addresses via DHCP to its customers. The ISP draws addresses from a pool of about 2000 addresses and assigns them when its customers come online. Although the IKE peer has a static FQDN, it has an unpredictably changing IP address. The IKE peer has three methods available for maintaining a Domain Name Service (DNS) mapping of its static FQDN to its dynamically assigned IP address (a process known as dynamic DNS).

- If the remote IKE peer is a NetScreen device, the admin can manually notify the DNS server to update its FQDN-to-IP address mapping each time the NetScreen device receives a new IP address from its ISP.
- If the remote IKE peer is another kind of VPN termination device that has dynamic DNS software running on it, that software can automatically notify the DNS server of its address changes so the server can update its FQDN-to-IP address mapping table.
- If the remote IKE peer is a NetScreen device or any other kind of VPN termination device, a host behind it can run an FQDN-to-IP address automatic update program that alerts the DNS server of address changes.

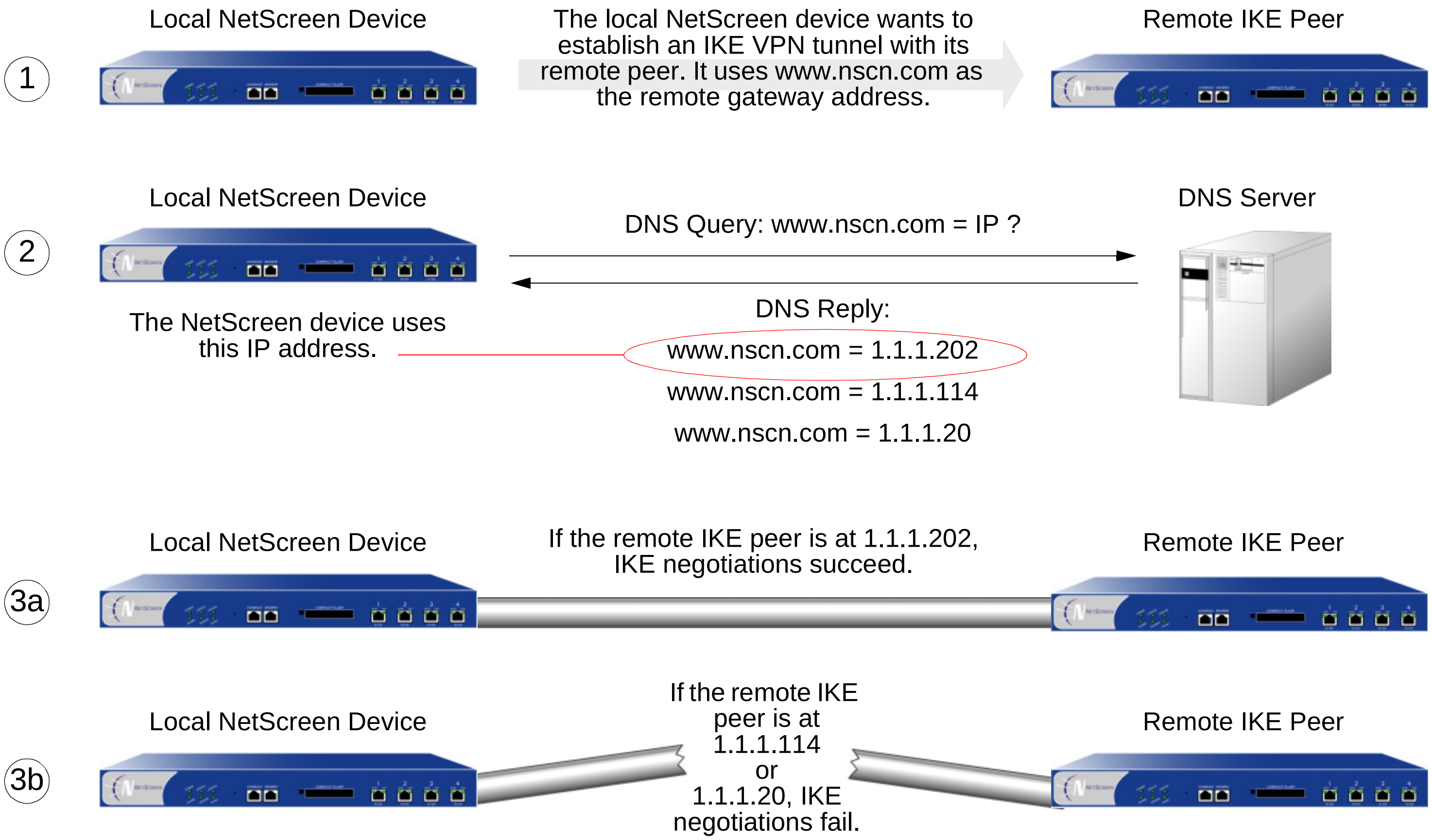


1. The DHCP server draws 2.2.2.28 from its pool of IP addresses, and assigns that address to the IKE peer.
2. The IKE peer notifies the DNS server of the new address, so that the server can update its FQDN-to-IP address mapping table.

Without needing to know the current IP address of a remote IKE peer, you can now configure an AutoKey IKE VPN tunnel to that peer using its FQDN instead of an IP address.

Aliases

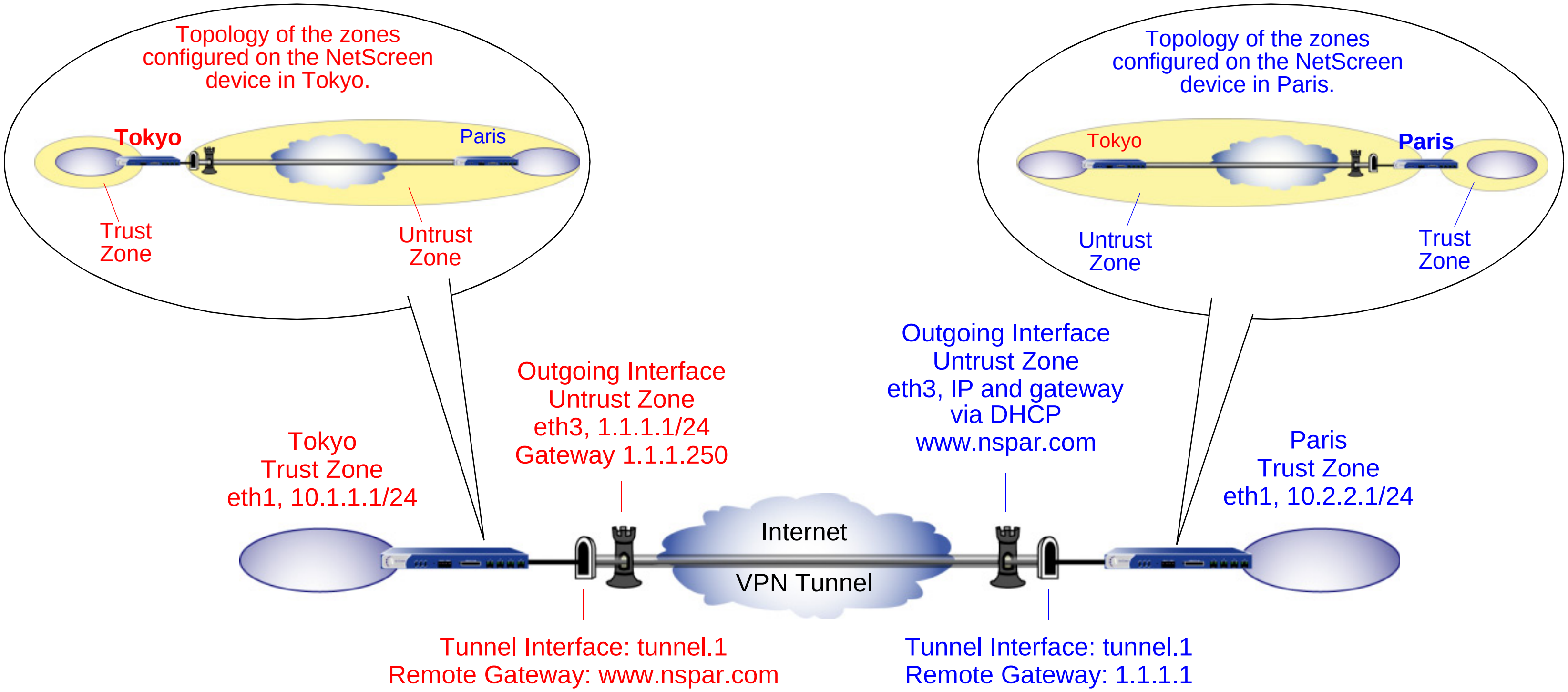
You can also use an alias for the FQDN of the remote IKE peer if the DNS server that the local NetScreen device queries returns only one IP address. If the DNS server returns several IP addresses, the local device uses the first one it receives. Because there is no guarantee for the order of the addresses in the response from the DNS server, the local NetScreen device might use the wrong IP address and IKE negotiations might fail.


1
Local NetScreen Device
The local NetScreen device wants to establish an IKE VPN tunnel with its remote peer. It uses www.nscn.com as the remote gateway address.
Remote IKE Peer
2
Local NetScreen Device
DNS Query: www.nscn.com = IP ?
DNS Server
The NetScreen device uses this IP address.
DNS Reply:
www.nscn.com = 1.1.1.202
www.nscn.com = 1.1.1.114
www.nscn.com = 1.1.1.20
3a
Local NetScreen Device
If the remote IKE peer is at 1.1.1.202, IKE negotiations succeed.
Remote IKE Peer
3b
Local NetScreen Device
If the remote IKE peer is at 1.1.1.114 or 1.1.1.20, IKE negotiations fail.
Remote IKE Peer

Example: AutoKey IKE Peer with FQDN

In this example, an AutoKey IKE VPN tunnel using either a preshared secret or a pair of certificates (one at each end of the tunnel) provides a secure connection between two offices in Tokyo and Paris. The Paris office has a dynamically assigned IP address, so the Tokyo office uses the remote peer's FQDN (www.nspar.com) as the address of the remote gateway in its VPN tunnel configuration.

The following configuration is for a route-based VPN tunnel. For the Phase 1 and 2 security levels, you specify one Phase 1 proposal—either pre-g2-3des-sha for the preshared key method or rsa-g2-3des-sha for certificates—and select the predefined “Compatible” set of proposals for Phase 2. All zones are in the trust-vr.



Setting up a route-based AutoKey IKE tunnel using either a preshared secret or certificates involves the following steps:

1. Assign IP addresses to the physical interfaces bound to the security zones and to the tunnel interface.
2. Define the remote gateway and key exchange mode, and specify either a preshared secret or a certificate
3. Configure the VPN tunnel, designate its outgoing interface in the Untrust zone, bind it to the tunnel interface, and configure its proxy-ID.
4. Enter the IP addresses for the local and remote endpoints in the Trust and Untrust address books.
5. Enter a default route to the external router in the trust-vr, and a route to the destination via the tunnel interface.
6. Set up policies for traffic to pass between each site.

In the following examples, the preshared key is h1p8A24nG5. It is assumed that both participants already have RSA certificates and are using Entrust as the certificate authority (CA). (For information about obtaining and loading certificates, see *NetScreen Concepts & Examples ScreenOS Reference Guide, Volume 4, VPNs*.)

WebUI (Tokyo)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK** :

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: ethernet3 (trust-vr)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Paris_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Paris

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: www.nspar.com

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Tokyo_Paris

Security Level: Compatible

Remote Gateway:

Predefined: (select), To_Paris

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Security Level: Compatible

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 10.1.1.0/24

Remote IP / Netmask: 10.2.2.0/24

Service: ANY

4. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 0.0.0.0[19]

[19] The ISP provides the gateway IP address dynamically through DHCP.

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.2.2.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To Paris

Source Address: Trust_LAN

Destination Address: Paris_Office

Service: ANY

Action: Permit

Position at Top: (select)

Policies > Policy (From: Untrust, To: Trust) > New Policy: Enter the following, and then click **OK**:

Name: From Paris

Source Address: Paris_Office

Destination Address: Trust_LAN

Service: ANY

Action: Permit

Position at Top: (select)

WebUI (Paris)

1. Host Name and Domain Name

Network > DNS: Enter the following, and then click **Apply**:

Host Name: www

Domain Name: nspar.com

2. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.2.2.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Obtain IP using DHCP: (select)

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: ethernet3 (trust-vr)

3. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Untrust

4. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Tokyo

Security Level: Custom

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 1.1.1.1

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level):
pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

Name: Paris_Tokyo

Security Level: Custom

Remote Gateway:

Predefined: (select), To_Tokyo

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Security Level: Compatible

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 10.2.2.0/24

Remote IP / Netmask: 10.1.1.0/24

Service: ANY

5. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.1.1.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

6. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Name: To Tokyo

Source Address: Trust_LAN

Destination Address: Tokyo_Office

Service: ANY

Action: Permit

Position at Top: (select)

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Name: From Tokyo

Source Address: Tokyo_Office

Destination Address: Trust_LAN

Service: ANY

Action: Permit

Position at Top: (select)

CLI (Tokyo)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. Addresses

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust paris_office 10.2.2.0/24
```

3. VPN

Preshared Key

```
set ike gateway to_paris address www.nspar.com main outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn tokyo_paris gateway to_paris sec-level compatible
set vpn tokyo_paris bind interface tunnel.1
set vpn tokyo_paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

(or)

Certificate

```
set ike gateway to_paris address www.nspar.com main outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_paris cert peer-ca 1[20]
set ike gateway to_paris cert peer-cert-type x509-sig
set vpn tokyo_paris gateway to_paris sec-level compatible
set vpn tokyo_paris bind interface tunnel.1
set vpn tokyo_paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

4. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
```

5. Policies

```
set policy top name “To Paris” from trust to untrust Trust_LAN paris_office any
    permit
set policy top name “From Paris” from untrust to trust paris_office Trust_LAN
    any permit
save
```

[20] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get ike ca**.

CLI (Paris)

1. Host Name and Domain Name

```
set hostname www
set domain nspar.com
```

2. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip dhcp-client enable

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

3. Addresses

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust tokyo_office 10.1.1.0/24
```

4. VPN

Preshared Key

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn paris_tokyo gateway to_tokyo sec-level compatible
set vpn paris_tokyo bind interface tunnel.1
set vpn paris_tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

(or)

Certificate

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway to_tokyo cert peer-ca 1[3]
set ike gateway to_tokyo cert peer-cert-type x509-sig
set vpn paris_tokyo gateway to_tokyo sec-level compatible
set vpn paris_tokyo bind interface tunnel.1
set vpn paris_tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

5. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
```

6. Policies

```
set policy top name “To Tokyo” from trust to untrust Trust_LAN tokyo_office any
    permit
set policy top name “From Tokyo” from untrust to trust tokyo_office Trust_LAN
    any permit
save
```

VPN Sites with Overlapping Addresses

Because the range of private IP addresses is relatively small, there is a good chance that the addresses of protected networks of two VPN peers overlap[21]. For bidirectional VPN traffic between two end entities with overlapping addresses, the NetScreen devices at both ends of the tunnel must apply source and destination network address translation (NAT-src and NAT-dst) to the VPN traffic passing between them.

For NAT-src, the interfaces at both ends of the tunnel must have IP addresses in mutually unique subnets, with a dynamic IP (DIP) pool in each of those subnets [22]. The policies regulating outbound VPN traffic can then apply NAT-src using DIP pool addresses to translate original source addresses to those in a neutral address space.

To provide NAT-dst on inbound VPN traffic, there are two options:

- Policy-based NAT-dst: A policy can apply NAT-dst to translate inbound VPN traffic to an address that is either in the same subnet as the tunnel interface—but not in the same range as the local DIP pool used for outbound VPN traffic—or to an address in another subnet to which the NetScreen device has an entry in its route table. (For information about routing considerations when configuring NAT-dst, see “Routing for Destination Translation” on page **2** -282.)
- Mapped IP (MIP): A policy can reference a MIP as the destination address. The MIP uses an address in the same subnet as the tunnel interface—but not in the same range as the local DIP pool used for outbound VPN traffic. (For information about MIPs, see “Mapped IP Addresses” on page **2** -331.)

VPN traffic between sites with overlapping addresses requires address translation in both directions. Because the source address on outbound traffic cannot be the same as the destination address on inbound traffic—the NAT-dst address or MIP cannot be in the DIP pool—the addresses referenced in the inbound and outbound policies cannot be symmetrical.

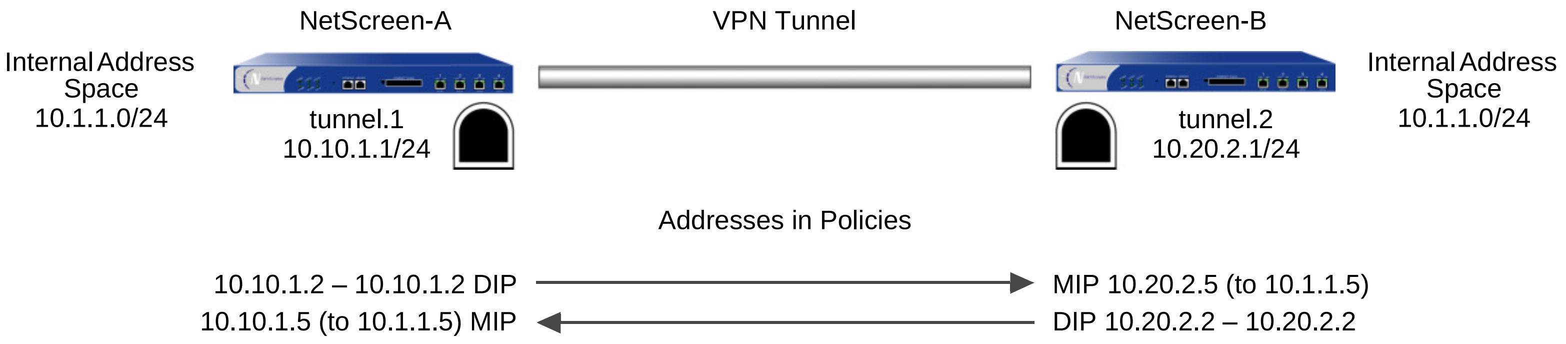
[21] An overlapping address space is when the IP address range in two networks are partially or completely the same.

[22] The range of addresses in a DIP pool must be in the same subnet as the tunnel interface, but the pool must not include the interface IP address or any MIP or VIP addresses that might also be in that subnet. For security zone interfaces, you can also define an extended IP address and an accompanying DIP pool in a different subnet from that of the interface IP address. For more information, see “Extended Interface and DIP” on page **2** -175.

When you want the NetScreen device to perform source and destination address translation on bidirectional VPN traffic through the same tunnel, you have two choices:

- You can define a proxy ID[23] for a policy-based VPN configuration. When you specifically reference a VPN tunnel in a policy, the NetScreen device derives a proxy ID from the components in the policy that references that tunnel. The NetScreen device derives the proxy ID when you first create the policy, and each time the device reboots thereafter. However, if you manually define a proxy ID for a VPN tunnel that is referenced in a policy, the NetScreen device applies the user-defined proxy ID, not the proxy ID derived from the policy.
- You can use a route-based VPN tunnel configuration, which must have a user-defined proxy ID. With a route-based VPN tunnel configuration, you do not specifically reference a VPN tunnel in a policy. Instead, the policy controls access (permit or deny) to a particular destination. The route to that destination points to a tunnel interface that in turn is bound to a VPN tunnel. Because the VPN tunnel is not directly associated with a policy from which it can derive a proxy ID from the source address, destination address, and service, you must manually define a proxy ID for it. (Note that a route-based VPN configuration also allows you to create multiple policies that make use of a single VPN tunnel; that is, a single Phase 2 SA.)

Consider the addresses in following illustration of a VPN tunnel between two sites with overlapping address spaces:


NetScreen-A
VPN Tunnel
NetScreen-B
Internal Address Space 10.1.1.0/24
tunnel.1 10.10.1.1/24
tunnel.2 10.20.2.1/24
Internal Address Space 10.1.1.0/24
Addresses in Policies
10.10.1.2 – 10.10.1.2 DIP
MIP 10.20.2.5 (to 10.1.1.5)
10.10.1.5 (to 10.1.1.5) MIP
DIP 10.20.2.2 – 10.20.2.2

[23] A proxy ID is a kind of agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified tuple of local address, remote address, and service.

If the NetScreen devices in the previous illustration derive proxy IDs from the policies, as they do in policy-based VPN configurations, then the inbound and outbound policies produce the following proxy IDs:

NetScreen-A				**NetScreen-B**			
	Local	Remote	Service		Local	Remote	Service
Outbound	10.10.1.2/32	10.20.2.5/32	Any	Inbound	10.20.2.5/32	10.10.1.2/32	Any
Inbound	10.10.1.5/32	10.20.2.2/32	Any	Outbound	10.20.2.2/32	10.10.1.5/32	Any

As you can see, there are two proxy IDs: one for outbound VPN traffic and another for inbound. When NetScreen-A first sends traffic from 10.10.1.2/32 to 10.20.2.5/32, the two peers perform IKE negotiations and produce Phase 1 and Phase 2 security associations (SAs). The Phase 2 SA results in the above outbound proxy ID for NetScreen-A, and the inbound proxy ID for NetScreen-B.

If NetScreen-B then sends traffic to NetScreen-A, the policy lookup for traffic from 10.20.2.2/32 to 10.10.1.5/32 indicates that there is no active Phase 2 SA for such a proxy ID. Therefore, the two peers use the existing Phase 1 SA (assuming that its lifetime has not yet expired) to negotiate a different Phase 2 SA. The resulting proxy IDs are shown above as the inbound proxy ID for NetScreen-A and the outbound proxy ID for NetScreen-B. There are two Phase 2 SAs—two VPN tunnels—because the addresses are asymmetrical and require different proxy IDs.

To create just one tunnel for bidirectional VPN traffic, you can define the following proxy IDs with addresses whose scope includes both the translated source and destination addresses at each end of the tunnel:

NetScreen-A				**NetScreen-B**		
Local	Remote	Service		Local	Remote	Service
10.10.1.0/24	10.20.2.0/24	Any		10.20.2.0/24	10.10.1.0/24	Any
			or			
0.0.0.0/0	0.0.0.0/0	Any		0.0.0.0/0	0.0.0.0/0	Any

The above proxy IDs encompass addresses appearing in both inbound and outbound VPN traffic between the two sites. The address 10.10.1.0/24 includes both the DIP pool 10.10.1.2 – 10.10.1.2 and the MIP 10.10.1.5. Likewise, the address 10.20.2.0/24 includes both the DIP pool 10.20.2.2 – 10.20.2.2 and the MIP 10.20.2.5[24]. The above

[24] The address 0.0.0.0/0 includes all IP addresses, and thus the addresses of the DIP pool and MIP.

proxy IDs are symmetrical; that is, the local address for NetScreen-A is the remote address for NetScreen-B, and vice versa. If NetScreen-A sends traffic to NetScreen-B, the Phase 2 SA and proxy ID also apply to traffic sent from NetScreen-B to NetScreen-A. Thus, a single Phase 2 SA—that is, a single VPN tunnel—is all that is required for bidirectional traffic between the two sites.

To create one VPN tunnel for bidirectional traffic between sites with overlapping address spaces when the addresses for NAT-src and NAT-dst configured on the same device are in different subnets from each other, the proxy ID for the tunnel must be (local IP) 0.0.0.0/0 – (remote IP) 0.0.0.0/0 – *service type*. If you want to use more restrictive addresses in the proxy ID, then the addresses for NAT-src and NAT-dst must be in the same subnet.

Example: Tunnel Interface with NAT-Src and NAT-Dst

In this example, you configure a VPN tunnel between “NetScreen-A” at a corporate site and “NetScreen-B” at a branch office. The address space for the VPN end entities overlaps; they both use addresses in the 10.1.1.0/24 subnet. To overcome this conflict, you use NAT-src to translate the source address on outbound VPN traffic and NAT-dst to translate the destination address on inbound VPN traffic. The policies permit all addresses in the corporate LAN to reach an FTP server at the branch site, and for all addresses at the branch office site to reach an FTP server at the corporate site.

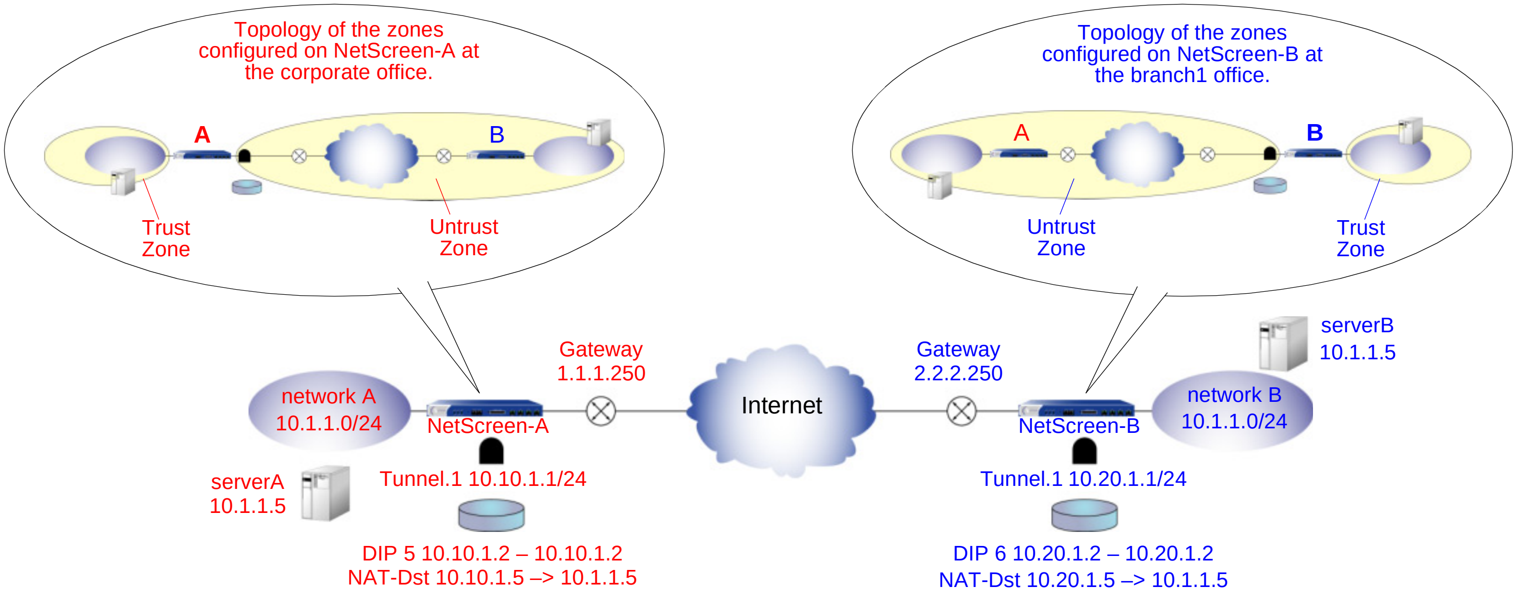
Note: *For more information about source and destination network address translation (NAT-src and NAT-dst), see Chapter 8, “Address Translation”.*

The tunnel configurations at both ends of the tunnel use the following parameters: AutoKey IKE, preshared key (“netscreen1”), and the security level predefined as “Compatible” for both Phase 1 and Phase 2 proposals. (For details about these proposals, see “Tunnel Negotiation” on page 11.)

The outgoing interface on NetScreen-A at the corporate site is ethernet3, which has IP address 1.1.1.1/24 and is bound to the Untrust zone. NetScreen-B at the branch office uses this address as its remote IKE gateway.

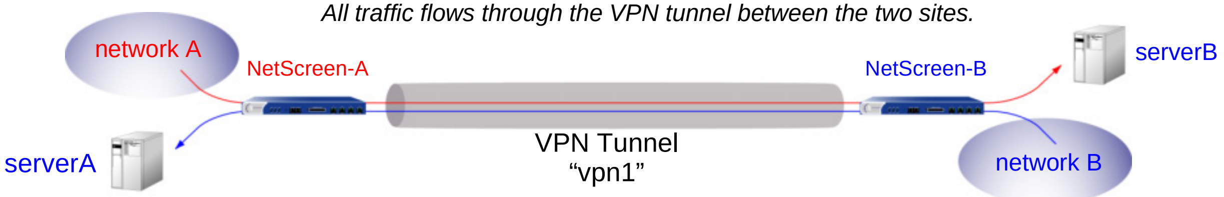
The outgoing interface on NetScreen-B at the branch office is ethernet3 , which has IP address 2.2.2.2/24 and is bound to the Untrust zone. NetScreen-A at the corporate site uses this address as its remote IKE gateway.

The Trust zone interface on both NetScreen devices is ethernet1 and has IP address 10.1.1.1/24. All zones on both NetScreen devices are in the trust-vr routing domain.


Topology of the zones configured on NetScreen-A at the corporate office.
A
B
Trust Zone
Untrust Zone
Topology of the zones configured on NetScreen-B at the branch1 office.
A
B
Untrust Zone
Trust Zone
serverB 10.1.1.5
Gateway 1.1.1.250
Gateway 2.2.2.250
network A 10.1.1.0/24
NetScreen-A
Internet
NetScreen-B
network B 10.1.1.0/24
serverA 10.1.1.5
Tunnel.1 10.10.1.1/24
Tunnel.1 10.20.1.1/24
DIP 5 10.10.1.2 – 10.10.1.2
NAT-Dst 10.10.1.5 –> 10.1.1.5
DIP 6 10.20.1.2 – 10.20.1.2
NAT-Dst 10.20.1.5 –> 10.1.1.5

Users at network A can access server B. Users at network B can access server A.

All traffic flows through the VPN tunnel between the two sites.



WebUI (NetScreen-A)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 10.10.1.1/24

2. DIP

Network > Interfaces > Edit (for tunnel.1) > DIP > New: Enter the following, and then click **OK**:

ID: 5

IP Address Range: (select), 10.10.1.2 ~ 10.10.1.2

Port Translation: (select)

In the same subnet as the interface IP or its secondary IPs: (select)

3. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: virtualA

IP Address/Domain Name:

IP/Netmask: (select), 10.10.1.5/32

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: branch1

IP Address/Domain Name:

IP/Netmask: (select), 10.20.1.2/32

Zone: Untrust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: serverB

IP Address/Domain Name:

IP/Netmask: (select), 10.20.1.5/32

Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: branch1

Type: Static IP: (select), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3[25]

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 10.10.1.0/24

Remote IP / Netmask: 10.20.1.0/24

Service: ANY

[25] The outgoing interface does not have to be in the same zone to which the tunnel interface is bound, although in this case they are in the same zone.

5. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.20.1.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet1/2(untrust-vr)

Gateway IP Address: 1.1.1.250

6. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), corp

Destination Address:

Address Book Entry: (select), serverB

Service: FTP

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Source Translation: (select)

DIP On: 5 (10.10.1.2–10.10.1.2)/X-late

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), branch1

Destination Address:

Address Book Entry: (select), virtualA

Service: FTP

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Destination Translation: (select)

Translate to IP: (select), 10.1.1.5

Map to Port: (clear)

WebUI (NetScreen-B)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 10.20.1.1/24

2. DIP

Network > Interfaces > Edit (for tunnel.1) > DIP > New: Enter the following, and then click **OK**:

ID: 6

IP Address Range: (select), 10.20.1.2 ~ 10.20.1.2

Port Translation: (select)

In the same subnet as the interface IP or its secondary IPs: (select)

3. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: branch1

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: virtualB

IP Address/Domain Name:

IP/Netmask: (select), 10.20.1.5/32

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (select), 10.10.1.2/32

Zone: Untrust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: serverA

IP Address/Domain Name:

IP/Netmask: (select), 10.10.1.5/32

Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: corp

Type: Static IP: (select), Address/Hostname: 1.1.1.1

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3[26]

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 10.20.1.0/24

Remote IP / Netmask: 10.10.1.0/24

Service: ANY

[26] The outgoing interface does not have to be in the same zone to which the tunnel interface is bound, although in this case they are in the same zone.

5. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.10.1.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet1/2(untrust-vr)

Gateway IP Address: 2.2.2.250

6. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), corp

Destination Address:

Address Book Entry: (select), serverA

Service: FTP

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Source Translation: (select)

DIP on: 6 (10.20.1.2–10.20.1.2)/X-late

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), corp

Destination Address:

Address Book Entry: (select), virtualB

Service: FTP

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Destination Translation: (select)

Translate to IP: 10.1.1.5

Map to Port: (clear)

CLI (NetScreen-A)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.10.1.1/24
```

2. DIP

```
set interface tunnel.1 dip 5 10.10.1.2 10.10.1.2
```

3. Addresses

```
set address trust corp 10.1.1.0/24
set address trust virtualA 10.10.1.5/32
set address untrust branch1 10.20.1.2/32
set address untrust serverB 10.20.1.5/32
```

4. VPN

```
set ike gateway branch1 address 2.2.2.2 outgoing-interface ethernet3[27] preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway branch1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.10.1.0/24 remote-ip 10.20.1.0/24 any
```

[27] The outgoing interface does not have to be in the same zone to which the tunnel interface is bound, although in this case they are in the same zone.

5. Routes

```
set vrouter trust-vr route 10.20.1.0/24 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. Policies

```
set policy top from trust to untrust corp serverB ftp nat src dip-id 5 permit
set policy top from untrust to trust branch1 virtualA ftp nat dst ip 10.1.1.5
    permit
save
```

CLI (NetScreen-B)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.20.1.1/24
```

2. DIP

```
set interface tunnel.1 dip 6 10.20.1.2 10.20.1.2
```

3. Addresses

```
set address trust branch1 10.1.1.0/24
set address trust virtualB 10.20.1.5/32
set address untrust corp 10.10.1.2/32
set address untrust serverA 10.10.1.5/32
```

4. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3[28] preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.10.1.0/24 any
```

5. Routes

```
set vrouter trust-vr route 10.10.1.0/24 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

6. Policies

```
set policy top from trust to untrust branch1 serverA ftp nat src dip-id 6
    permit
set policy top from untrust to trust corp virtualB ftp nat dst ip 10.1.1.5
    permit
save
```

[28] The outgoing interface does not have to be in the same zone to which the tunnel interface is bound, although in this case they are in the same zone.

Transparent Mode VPN

When the NetScreen device interfaces are in Transparent mode (that is, they have no IP addresses and are operating at Layer 2 in the OSI model[29]), you can use the VLAN1 IP address as a VPN termination point. In place of an outgoing interface, as used when the interfaces are in Route or NAT mode (that is, they have IP addresses and are operating at Layer 3), a VPN tunnel references an outgoing zone. By default, a tunnel uses the V1-Untrust zone as its outgoing zone. If you have multiple interfaces bound to the same outgoing zone, the VPN tunnel can use any one of them.

Note: *At the time of this release, a NetScreen device whose interfaces are in Transparent mode supports only policy-based VPNs. For more information about Transparent mode, see "Transparent Mode" on page* ***2*** *-92.*

[29] The OSI model is a networking industry standard model of network protocol architecture. The OSI model consists of seven layers, in which layer 2 is the data link layer and layer 3 is the network layer.

Example: Transparent Mode, Policy-Based AutoKey IKE VPN

In this example, you set up a policy-based AutoKey IKE VPN tunnel between two NetScreen devices with interfaces operating in Transparent mode.

Note: *It is not necessary that the interfaces of both NetScreen devices be in Transparent mode. The interfaces of the device at one end of the tunnel can be in Transparent mode and those of the other device can be in Route or NAT mode.*

The key elements of the configuration for the NetScreen devices at both ends of the tunnel are as follows:

Configuration Elements	NetScreen-A	NetScreen-B
V1-Trust Zone	Interface: ethernet1, 0.0.0.0/0 (enable management for the local admin)	Interface: ethernet1, 0.0.0.0/0 (enable management for the local admin)
V1-Untrust Zone	Interface: ethernet3, 0.0.0.0/0	Interface: ethernet3, 0.0.0.0/0
VLAN1 Interface	IP Address: 1.1.1.1/24 Manage IP: 1.1.1.2*	IP Address: 2.2.2.2/24 Manage IP: 2.2.2.3
Addresses	local_lan: 1.1.1.0/24 in V1-Trust peer_lan: 2.2.2.0/24 in V1-Untrust	local_lan: 2.2.2.0/24 in V1-Trust peer_lan: 1.1.1.0/24 in V1-Untrust
IKE gateway	gw1, 2.2.2.2, preshared key h1p8A24nG5, security: compatible	gw1, 1.1.1.1, preshared key h1p8A24nG5, security: compatible
VPN tunnel	security: compatible	security: compatible
Policies	local_lan -> peer_lan, any service, vpn1 peer_lan -> local_lan, any service, vpn1	local_lan -> peer_lan, any service, vpn1 peer_lan -> local_lan, any service, vpn1
External Router	IP Address: 1.1.1.250	IP Address: 2.2.2.250
Route	0.0.0.0/0, use VLAN1 interface to gateway 1.1.1.250	0.0.0.0/0, use VLAN1 interface to gateway 2.2.2.250

* You can separate administrative from VPN traffic by using the manage IP address to receive administrative traffic and the VLAN1 address to terminate VPN traffic.

Configuring a policy-based AutoKey IKE tunnel for a NetScreen device whose interfaces are in Transparent mode involves the following steps:

1. Remove any IP addresses from the physical interfaces, and bind them to the layer-2 security zones.
2. Assign an IP address and manage IP address to the VLAN1 interface.
3. Enter the IP addresses for the local and remote endpoints in the address books for the V1-Trust and V1-Untrust zones.
4. Configure the VPN tunnel and designate its outgoing zone as the V1-Untrust zone.
5. Enter a default route to the external router in the trust-vr.
6. Set up policies for VPN traffic to pass between each site.

WebUI (NetScreen-A)

1. Interfaces

Note: *Moving the VLAN1 IP address to a different subnet causes the NetScreen device to delete any routes involving the previous VLAN1 interface. When configuring a NetScreen device through the WebUI, your workstation must reach the first VLAN1 address and then be in the same subnet as the new address. After changing the VLAN1 address, you must then change the IP address of your workstation so that it is in the same subnet as the new VLAN1 address. You might also have to relocate your workstation to a subnet physically adjacent to the NetScreen device.*

Network > Interfaces > Edit (for the VLAN1 interface): Enter the following, and then click **OK**:

IP Address/Netmask: 1.1.1.1/24

Manage IP: 1.1.1.2

Management Services: WebUI, Telnet, Ping[30]

[30] You enable the management options for WebUI, Telnet, and Ping on both the V1-Trust zone and the VLAN1 interface so that a local admin in the V1-Trust zone can reach the VLAN1 manage IP address. If management via the WebUI is not already enabled on VLAN1 and the V1-Trust zone interfaces, you cannot reach the NetScreen device through the WebUI to make these settings. Instead, you must first set WebUI manageability on these interfaces through a console connection.

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Management Services: WebUI, Telnet

Other Services: Ping

Select the following, and then click **OK**:

Zone Name: V1-Trust

IP Address/Netmask: 0.0.0.0/0

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: V1-Untrust

IP Address/Netmask: 0.0.0.0/0

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: local_lan

IP Address/Domain Name:

IP/Netmask: (select), 1.1.1.0/24

Zone: V1-Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: peer_lan

IP Address/Domain Name:

IP/Netmask: (select), 2.2.2.0/24

Zone: V1-Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: gw1

Security Level: Compatible

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 2.2.2.2

Preshared Key: h1p8A24nG5

Outgoing Zone: V1-Untrust

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway:

Predefined: (select), gw1

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: VLAN1 (VLAN)

Gateway IP Address: 1.1.1.250

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), local_lan

Destination Address:

Address Book Entry: (select), peer_lan

Service: ANY

Action: Tunnel

Tunnel VPN: vpn1

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

WebUI (NetScreen-B)

1. Interfaces

Note: *Moving the VLAN1 IP address to a different subnet causes the NetScreen device to delete any routes involving the previous VLAN1 interface. When configuring a NetScreen device through the WebUI, your workstation must reach the first VLAN1 address and then be in the same subnet as the new address. After changing the VLAN1 address, you must then change the IP address of your workstation so that it is in the same subnet as the new VLAN1 address. You might also have to relocate your workstation to a subnet physically adjacent to the NetScreen device.*

Network > Interfaces > Edit (for the VLAN1 interface): Enter the following, and then click **OK**:

IP Address/Netmask: 2.2.2.2/24

Manage IP: 2.2.2.3

Management Services: WebUI[31], Telnet, Ping

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Management Services: WebUI, Telnet

Other Services: Ping

Select the following, and then click **OK**:

Zone Name: V1-Trust

IP Address/Netmask: 0.0.0.0/0

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: V1-Untrust

IP Address/Netmask: 0.0.0.0/0

[31] If management via the WebUI is not already enabled on VLAN1 and the V1-Trust zone interfaces, you cannot reach the NetScreen device through the WebUI to make these settings. Instead, you must first set WebUI manageability on these interfaces through a console connection.

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: local_lan

IP Address/Domain Name:

IP/Netmask: (select), 2.2.2.0/24

Zone: V1-Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: peer_lan

IP Address/Domain Name:

IP/Netmask: (select), 1.1.1.0/24

Zone: V1-Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: gw1

Security Level: Compatible

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 1.1.1.1

Preshared Key: h1p8A24nG5

Outgoing Zone: V1-Untrust

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway:

Predefined: (select), gw1

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: VLAN1 (VLAN)

Gateway IP Address: 2.2.2.250

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), local_lan

Destination Address:

Address Book Entry: (select), peer_lan

Service: ANY

Action: Tunnel

Tunnel VPN: vpn1

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

CLI (NetScreen-A)

1. Interfaces and Zones

```
unset interface ethernet1 ip
unset interface ethernet1 zone
set interface ethernet1 zone v1-trust
set zone v1-trust manage web
set zone v1-trust manage telnet
set zone v1-trust manage ping[32]

unset interface ethernet3 ip
unset interface ethernet3 zone
set interface ethernet3 zone v1-untrust

set interface vlan1 ip 1.1.1.1/24
set interface vlan1 manage-ip 1.1.1.2
set interface vlan1 manage web
set interface vlan1 manage telnet
set interface vlan1 manage ping
```

2. Addresses

```
set address v1-trust local_lan 1.1.1.0/24
set address v1-untrust peer_lan 2.2.2.0/24
```

3. VPN

```
set ike gateway gw1 address 2.2.2.2 main outgoing-interface v1-untrust preshare
    h1p8A24nG5 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
```

[32] You enable the management options for WebUI, Telnet, and Ping on both the V1-Trust zone and the VLAN1 interface so that a local admin in the V1-Trust zone can reach the VLAN1 manage IP address.

4. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 1.1.1.250
```

5. Policies

```
set policy top from v1-trust to v1-untrust local_lan peer_lan any tunnel vpn
    vpn1
set policy top from v1-untrust to v1-trust peer_lan local_lan any tunnel vpn
    vpn1
save
```

CLI (NetScreen-B)

1. Interfaces and Zones

```
unset interface ethernet1 ip
unset interface ethernet1 zone
set interface ethernet1 zone v1-trust
set zone v1-trust manage

unset interface ethernet3 ip
unset interface ethernet3 zone
set interface ethernet3 zone v1-untrust

set interface vlan1 ip 2.2.2.2/24
set interface vlan1 manage-ip 2.2.2.3
set interface vlan1 manage
```

2. Addresses

```
set address v1-trust local_lan 2.2.2.0/24
set address v1-untrust peer_lan 1.1.1.0/24
```

3. VPN

```
set ike gateway gw1 address 1.1.1.1 main outgoing-interface v1-untrust preshare
    h1p8A24nG5 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
```

4. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 2.2.2.250
```

5. Policies

```
set policy top from v1-trust to v1-untrust local_lan peer_lan any tunnel vpn
    vpn1
set policy top from v1-untrust to v1-trust peer_lan local_lan any tunnel vpn
    vpn1
save
```

5

Dialup VPNs

NetScreen devices can support dialup VPN connections. You can configure a NetScreen device that has a static IP address to secure an IPSec tunnel with a NetScreen-Remote client or with another NetScreen device with a dynamic IP address.

This chapter offers examples of the following dialup VPN concepts:

- “Dialup VPNs” on page 200
  - “Example: Policy-Based Dialup VPN, AutoKey IKE” on page 201
  - “Example: Route-Based Dialup VPN, Dynamic Peer” on page 209
  - “Example: Policy-Based Dialup VPN, Dynamic Peer” on page 220
  - “Example: Bidirectional Dialup VPN Policies” on page 230
- “Group IKE ID” on page 237
  - “Example: Group IKE ID (Certificates)” on page 243
  - “Example: Group IKE ID (Preshared Keys)” on page 252
- “Shared IKE IDs” on page 259
  - “Example: Shared IKE ID (Preshared Keys)” on page 260

Dialup VPNs

You can configure tunnels for VPN dialup users on a per-user basis or form users into a VPN dialup group for which you need only configure one tunnel. You can also create a group IKE ID user, which allows you to define one user whose IKE ID is used as part of the IKE IDs of dialup IKE users. This approach is particularly timesaving when there are large groups of dialup users because you do not have to configure each IKE user individually.

Note: *For more information on creating IKE user groups, see "IKE Users and User Groups" on page* ***2*** *-431. For more information about the Group IKE ID feature, see "Group IKE ID" on page 237.*

If the dialup client can support a virtual internal IP address, which the NetScreen-Remote does, you can also create a dynamic peer dialup VPN, AutoKey IKE tunnel (with a preshared key or certificates). You can configure a NetScreen security gateway with a static IP address to secure an IPSec tunnel with a NetScreen-Remote client or with another NetScreen device with a dynamic IP address.

Note: *For background information about the available VPN options, see Chapter 1, "IPSec". For guidance when choosing among the various options, see Chapter 3, "VPN Guidelines".*

You can configure policy-based VPN tunnels for VPN dialup users. For a dialup dynamic peer client[1], you can configure either a policy-based or route-based VPN. Because a dialup dynamic peer client can support a virtual internal IP address, which the NetScreen-Remote does, you can configure a routing table entry to that virtual internal address via a designated tunnel interface. Doing so allows you to configure a route-based VPN tunnel between the NetScreen device and that peer.

Note: *The dialup dynamic peer is nearly identical to the Site-to-Site dynamic peer except that the internal IP address for the dialup client is a virtual address.*

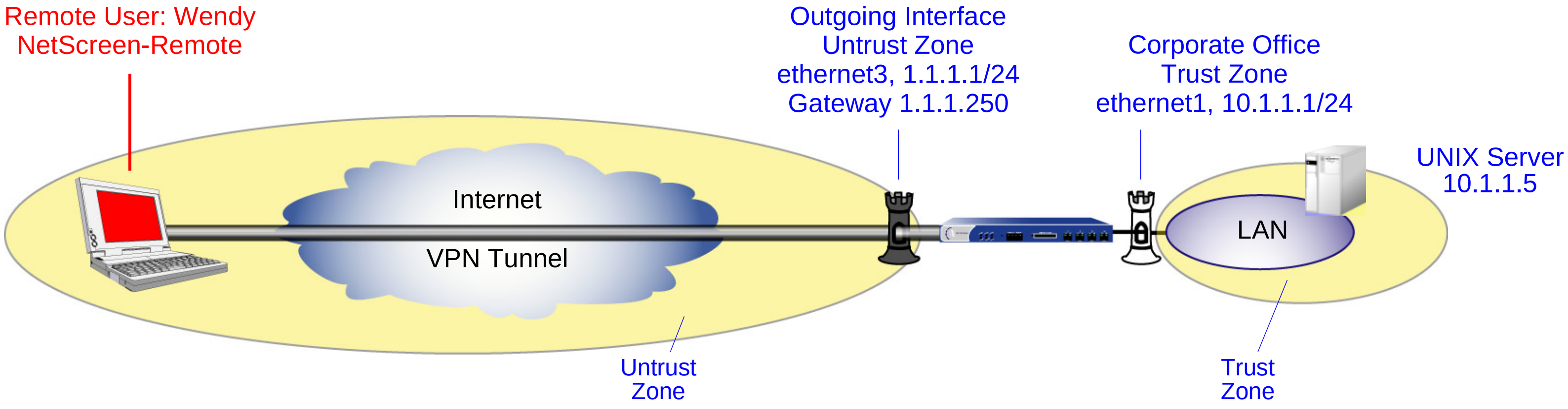
[1] A dialup dynamic peer client is a dialup client that supports a virtual internal IP address.

Example: Policy-Based Dialup VPN, AutoKey IKE

In this example, an AutoKey IKE tunnel using either a preshared key or a pair of certificates (one at each end of the tunnel[2]) provides the secure communication channel between the IKE user Wendy and the UNIX server. The tunnel again uses ESP with 3DES encryption and SHA-1 authentication.

Setting up the AutoKey IKE tunnel using AutoKey IKE with either a preshared key or certificates requires you to do the following at the corporate site:

1. Configure interfaces for the Trust and Untrust zones, both of which are in the trust-vr routing domain.
2. Enter the address of the UNIX server in the Trust zone address book.
3. Define Wendy as an IKE user.
4. Configure the remote gateway and AutoKey IKE VPN.
5. Set up a default route.
6. Create a policy from the Untrust zone to the Trust zone permitting access to the UNIX from the dialup user.



[2] The preshared key is h1p8A24nG5. It is assumed that both participants already have certificates. For more information about certificates, see “Certificates and CRLs” on page 21.

The preshared key is h1p8A24nG5. This example assumes that both participants already have RSA certificates issued by Verisign, and that the local certificate on the NetScreen-Remote contains the U-FQDN wparker@email.com. (For information about obtaining and loading certificates, see “Certificates and CRLs” on page 21.) For the Phase 1 and 2 security levels, you specify one Phase 1 proposal—either pre-g2-3des-sha for the preshared key method or rsa-g2-3des-sha for certificates—and select the predefined “Compatible” set of proposals for Phase 2.

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

2. Address

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: UNIX

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.5/32

Zone: Trust

3. User

Objects > Users > Local > New: Enter the following, and then click **OK**:

User Name: Wendy

Status: Enable (select)

IKE User: (select)

Simple Identity: (select)

IKE Identity: wparker@email.com

4. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: Wendy_NSR

Security Level: Custom

Remote Gateway Type:

Dialup User: (select), User: Wendy

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Wendy_UNIX

Security Level: Compatible

Remote Gateway:

Predefined: (select), Wendy_NSR

5. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

6. Policy

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Dial-Up VPN

Destination Address:

Address Book Entry: (select), UNIX

Service: ANY

Action: Tunnel

Tunnel VPN: Wendy_UNIX

Modify matching bidirectional VPN policy: (clear)

Position at Top: (select)

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Address

```
set address trust unix 10.1.1.5/32
```

3. User

```
set user wendy ike-id u-fqdn wparker@email.com
```

4. VPN

Preshared Key

```
set ike gateway wendy_nsr dialup wendy aggressive outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn wendy_unix gateway wendy_nsr sec-level compatible
```

(or)

Certificates

```
set ike gateway wendy_nsr dialup wendy aggressive outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway wendy_nsr cert peer-ca 1[3]
set ike gateway wendy_nsr cert peer-cert-type x509-sig
set vpn wendy_unix gateway wendy_nsr sec-level compatible
```

5. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. Policy

```
set policy top from untrust to trust “Dial-Up VPN” unix any tunnel vpn
    wendy_unix
save
```

[3] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get pki x509 list ca-cert**.

NetScreen-Remote Security Policy Editor

1. Click **Options > Secure > Specified Connections**.
2. Click **Add a new connection**, and type **UNIX** next to the new connection icon that appears.
3. Configure the connection options:

   Connection Security: Secure

   Remote Party Identity and Addressing:

   ID Type: IP Address, 10.1.1.5

   Protocol: All

   Connect using Secure Gateway Tunnel: (select)

   ID Type: IP Address, 1.1.1.1
4. Click the **PLUS** symbol, located to the left of the UNIX icon, to expand the connection policy.
5. Click **My Identity**: Do either of the following:

   Click **Pre-shared Key** > **Enter Key**: Type **h1p8A24nG5**, and then click **OK**.

   ID Type: (select **E-mail Address**), and type **wparker@email.com**.

   (or)

   Select a certificate from the Select Certificate drop-down list.

   ID Type: (select **E-mail Address**)[4]
6. Click the **Security Policy** icon, and select **Aggressive Mode**.
7. Click the **PLUS** symbol, located to the left of the Security Policy icon, and then the **PLUS** symbol to the left of Authentication (Phase 1) and Key Exchange (Phase 2) to expand the policy further.

[4] The e-mail address from the certificate appears in the identifier field automatically.

8. Click **Authentication (Phase 1)** > **Proposal 1**: Select the following Encryption and Data Integrity Algorithms:

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

9. Click **Key Exchange (Phase 2)** > **Proposal 1**: Select the following IPSec Protocols:

   Encapsulation Protocol (ESP): (select)

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Encapsulation: Tunnel

10. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: Triple DES

    Hash Alg: MD5

    Encapsulation: Tunnel

11. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: SHA-1

    Encapsulation: Tunnel

12. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: MD5

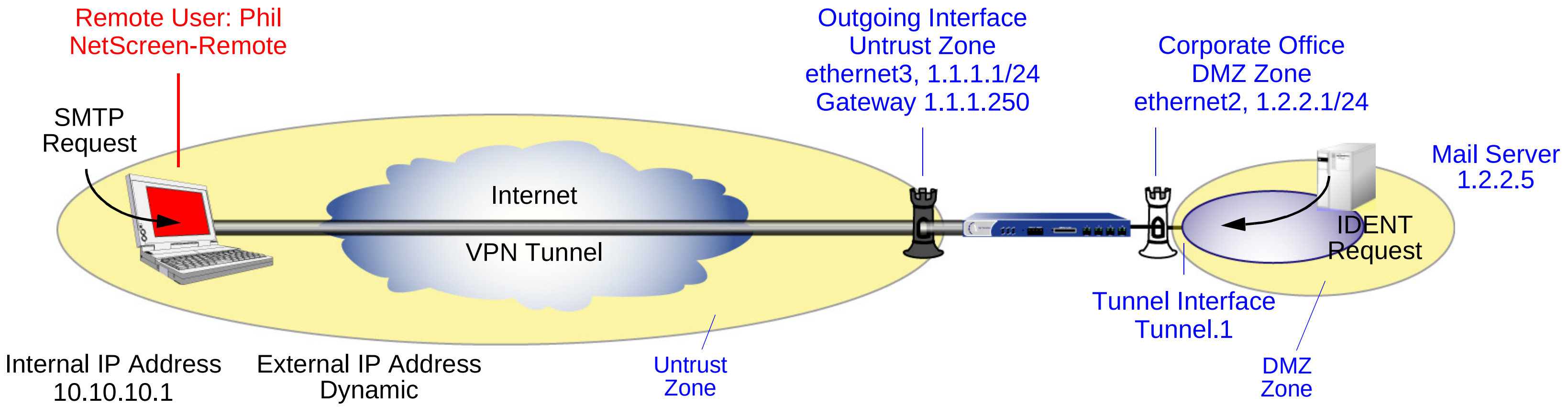
    Encapsulation: Tunnel

13. Click **Save**.

Example: Route-Based Dialup VPN, Dynamic Peer

In this example, a VPN tunnel securely connects the user behind the NetScreen-Remote to the Untrust zone interface of the NetScreen device protecting the mail server in the DMZ zone. The Untrust zone interface has a static IP address. The NetScreen-Remote client has a dynamically assigned external IP address and a static (virtual) internal IP address. The administrator of the NetScreen device must know the peer's internal IP address so that he can add it to the Untrust address book for use in policies to tunnel traffic from that source. After the NetScreen-Remote client establishes the tunnel, traffic through the tunnel can originate from either end.

All zones on the NetScreen device are in the trust-vr routing domain.



In this example, Phil wants to get his e-mail from the mail server at the company site. When he attempts to do so, he is authenticated by the mail server program, which sends him an IDENT request through the tunnel.

Note: *The mail server can send the IDENT request through the tunnel only if the NetScreen administrator adds a custom service for it (TCP, port 113) and sets up an outgoing policy allowing that traffic through the tunnel to 10.10.10.1.*

The preshared key is h1p8A24nG5. It is assumed that both participants already have RSA certificates issued by Verisign, and that the local certificate on the NetScreen-Remote contains the U-FQDN *pm@netscreen.com.* (For information about obtaining and loading certificates, see "Certificates and CRLs" on page 21.) For the Phase 1 and 2 security levels, you specify one Phase 1 proposal—either pre-g2-3des-sha for the preshared key method or rsa-g2-3des-sha for certificates—and select the predefined "Compatible" set of proposals for Phase 2.

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet2): Enter the following, and then click **OK**:

Zone Name: DMZ

Static IP: (select this option when present)

IP Address/Netmask: 1.2.2.1/24

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (select)

Interface: ethernet3 (trust-vr)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Mail Server
IP Address/Domain Name:
IP/Netmask: (select), 1.2.2.5/32
Zone: DMZ

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Phil
IP Address/Domain Name:
IP/Netmask: (select), 10.10.10.1/32
Zone: Untrust

3. Services

Objects > Services > Custom > New: Enter the following, and then click **OK**:

Service Name: Ident
Service Timeout:
Use protocol default: (select)
Transport Protocol: TCP (select)
Source Port: Low 1, High 65535
Destination Port: Low 113, High 113

Objects > Services > Group > New: Enter the following, move the following services, and then click **OK**:

Group Name: Remote_Mail

Group Members << Available Members:

Ident
MAIL
POP3

4. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Phil

Security Level: Custom

Remote Gateway Type:

Dynamic IP Address: (select), Peer ID: pm@netscreen.com

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: corp_Phil

Security Level: Compatible

Remote Gateway:

Predefined: (select), To_Phil

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface: (select), tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 1.2.2.5/32

Remote IP / Netmask: 10.10.10.1/32

Service: Any

5. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 10.10.10.1/32

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

6. Policies

Policies > (From: Untrust, To: DMZ) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Phil

Destination Address:

Address Book Entry: (select), Mail Server

Service: Remote_Mail

Action: Permit

Position at Top: (select)

Policies > (From: DMZ, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Mail Server

Destination Address:

Address Book Entry: (select), Phil

Service: Remote_Mail

Action: Permit

Position at Top: (select)

CLI

1. Interfaces

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. Addresses

```
set address dmz “Mail Server” 1.2.2.5/32
set address untrust phil 10.10.10.1/32
```

3. Services

```
set service ident protocol tcp src-port 1-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

4. VPN

Preshared Key

```
set ike gateway to_phil dynamic pm@netscreen.com aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn corp_phil gateway to_phil sec-level compatible
set vpn corp_phil bind interface tunnel.1
set vpn corp_phil proxy-id local-ip 1.2.2.5/32 remote-ip 10.10.10.1/32 any
```

(or)

Certificates

```
set ike gateway to_phil dynamic pm@netscreen.com aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_phil cert peer-ca 1[5]
set ike gateway to_phil cert peer-cert-type x509-sig
set vpn corp_phil gateway to_phil sec-level compatible
set vpn corp_phil bind interface tunnel.1
set vpn corp_phil proxy-id local-ip 1.2.2.5/32 remote-ip 10.10.10.1/32 any
```

5. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.10.10.1/32 interface tunnel.1
```

6. Policies

```
set policy top from dmz to untrust “Mail Server” phil remote_mail permit
set policy top from untrust to dmz phil “Mail Server” remote_mail permit
save
```

[5] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get pki x509 list ca-cert**.

NetScreen-Remote

1. Click **Options** > **Global Policy Settings**, and select the **Allow to Specify Internal Network Address** check box.
2. **Options > Secure > Specified Connections**.
3. Click the **Add a new connection** button, and type **Mail** next to the new connection icon that appears.
4. Configure the connection options:

   Connection Security: Secure

   Remote Party Identity and Addressing:

   ID Type: IP Address, 1.2.2.5

   Protocol: All

   Connect using Secure Gateway Tunnel: (select)

   ID Type: IP Address, 1.1.1.1
5. Click the **PLUS** symbol, located to the left of the unix icon, to expand the connection policy.
6. Click the **Security Policy** icon, and select **Aggressive Mode**.
7. Click **My Identity** and do either of the following:

   Click **Pre-shared Key** > **Enter Key**: Type **h1p8A24nG5**, and then click **OK**.

   ID Type: E-mail Address; pm@netscreen.com

   Internal Network IP Address: 10.10.10.1

   or

   Select the certificate that contains the e-mail address “pm@netscreen.com” from the Select Certificate drop-down list.

   ID Type: E-mail Address; pm@netscreen.com

   Internal Network IP Address: 10.10.10.1

8. Click the **PLUS** symbol, located to the left of the Security Policy icon, and then the **PLUS** symbol to the left of Authentication (Phase 1) and Key Exchange (Phase 2) to expand the policy further.

9. Click **Authentication (Phase 1)** > **Proposal 1**: Select the following Encryption and Data Integrity Algorithms:

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

10. Click **Key Exchange (Phase 2)** > **Proposal 1**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: Triple DES

    Hash Alg: SHA-1

    Encapsulation: Tunnel

11. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: Triple DES

    Hash Alg: MD5

    Encapsulation: Tunnel

12. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: SHA-1

    Encapsulation: Tunnel

13. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

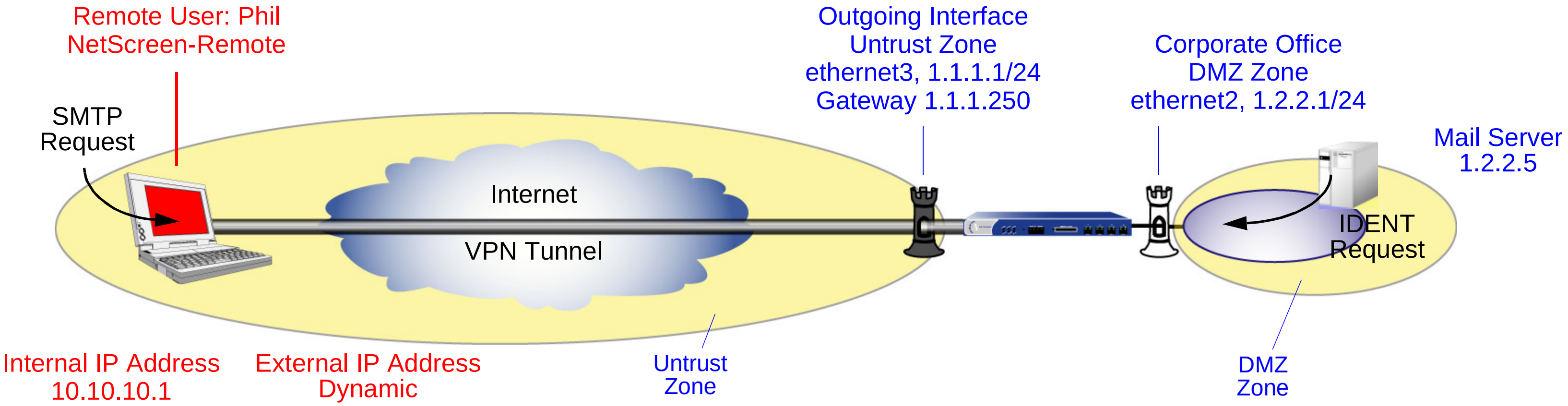
    Hash Alg: MD5

    Encapsulation: Tunnel

14. Click the **Save** button.

Example: Policy-Based Dialup VPN, Dynamic Peer

In this example, a VPN tunnel securely connects the user behind the NetScreen-Remote to the Untrust zone interface of the NetScreen device protecting the mail server in the DMZ zone. The Untrust zone interface has a static IP address. The NetScreen-Remote client has a dynamically assigned external IP address and a static (virtual) internal IP address. The administrator of the NetScreen device must know the client's internal IP address so that he can add it to the Untrust address book for use in policies to tunnel traffic from that source. After the NetScreen-Remote client establishes the tunnel, traffic through the tunnel can originate from either end.



In this example, Phil wants to get his e-mail from the mail server at the company site. When he attempts to do so, he is authenticated by the mail server program, which sends him an IDENT request through the tunnel.

Note: *The mail server can send the IDENT request through the tunnel only if the NetScreen administrator adds a custom service for it (TCP, port 113) and sets up an outgoing policy allowing that traffic through the tunnel to 10.10.10.1.*

The preshared key is h1p8A24nG5. This example assumes that both participants have RSA certificates issued by Verisign, and that the local certificate on the NetScreen-Remote contains the U-FQDN *pm@netscreen.com.* (For more information about obtaining and loading certificates, see “Certificates and CRLs” on page 21.) For the Phase 1 and 2 security levels, you specify one Phase 1 proposal—either pre-g2-3des-sha for the preshared key method or rsa-g2-3des-sha for certificates—and select the predefined “Compatible” set of proposals for Phase 2.

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet2): Enter the following, and then click **OK**:

Zone Name: DMZ

Static IP: (select this option when present)

IP Address/Netmask: 1.2.2.1/24

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Mail Server

IP Address/Domain Name:

IP/Netmask: (select), 1.2.2.5/32

Zone: DMZ

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Phil

IP Address/Domain Name:

IP/Netmask: (select), 10.10.10.1/32

Zone: Untrust

3. Services

Objects > Services > Custom > New: Enter the following, and then click **OK**:

Service Name: Ident

Service Timeout:

Use protocol default: (select)

Transport Protocol: TCP (select)

Source Port: Low 1, High 65535

Destination Port: Low 113, High 113

Objects > Services > Group > New: Enter the following, move the following services, and then click **OK**:

Group Name: Remote_Mail

Group Members << Available Members:

Ident
MAIL
POP3

4. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: To_Phil

Security Level: Custom

Remote Gateway Type:

Dynamic IP Address: (select), Peer ID: pm@netscreen.com

Preshared Key

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(Or)

Certificates

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: corp_Phil

Security Level: Compatible

Remote Gateway:

Predefined: (select), To_Phil

5. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

6. Policies

Policies > (From: Untrust, To: DMZ) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Phil

Destination Address:

Address Book Entry: (select), Mail Server

Service: Remote_Mail

Action: Tunnel

VPN Tunnel: corp_Phil

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

CLI

1. Interfaces

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Addresses

```
set address dmz “mail server” 1.2.2.5/32
set address untrust phil 10.10.10.1/32
```

3. Services

```
set service ident protocol tcp src-port 1-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

4. VPN

Preshared Key

```
set ike gateway to_phil dynamic pm@netscreen.com aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn corp_phil gateway to_phil sec-level compatible
```

(or)

Certificates

```
set ike gateway to_phil dynamic pm@netscreen.com aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_phil cert peer-ca 1[6]
set ike gateway to_phil cert peer-cert-type x509-sig
set vpn corp_phil gateway to_phil sec-level compatible
```

5. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. Policies

```
set policy top from untrust to dmz phil “mail server” remote_mail tunnel vpn
    corp_phil
set policy top from dmz to untrust “mail server” phil remote_mail tunnel vpn
    corp_phil
save
```

[6] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get pki x509 list ca-cert**.

NetScreen-Remote

1. Click **Options** > **Global Policy Settings**, and select **Allow to Specify Internal Network Address**.
2. **Options > Secure > Specified Connections**.
3. Click **Add a new connection**, and type **Mail** next to the new connection icon that appears.
4. Configure the connection options:

   Connection Security: Secure

   Remote Party Identity and Addressing:

   ID Type: IP Address, 1.2.2.5

   Protocol: All

   Connect using Secure Gateway Tunnel: (select)

   ID Type: IP Address, 1.1.1.1

5. Click the **PLUS** symbol, located to the left of the unix icon, to expand the connection policy.
6. Click the **Security Policy** icon, and select **Aggressive Mode**.
7. Click **My Identity** and do either of the following:

   Click **Pre-shared Key** > **Enter Key**: Type **h1p8A24nG5**, and then click **OK**.

   Internal Network IP Address: 10.10.10.1

   ID Type: E-mail Address; pm@netscreen.com

   or

   Select the certificate that contains the e-mail address “pmason@email.com” from the Select Certificate drop-down list.

   Internal Network IP Address: 10.10.10.1

   ID Type: E-mail Address; pm@netscreen.com

8. Click the **PLUS** symbol, located to the left of the Security Policy icon, and then the **PLUS** symbol to the left of Authentication (Phase 1) and Key Exchange (Phase 2) to expand the policy further.

9. Click **Authentication (Phase 1)** > **Proposal 1**: Select the following Encryption and Data Integrity Algorithms:

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

10. Click **Key Exchange (Phase 2)** > **Proposal 1**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: Triple DES

    Hash Alg: SHA-1

    Encapsulation: Tunnel

11. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: Triple DES

    Hash Alg: MD5

    Encapsulation: Tunnel

12. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: SHA-1

    Encapsulation: Tunnel

13. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: MD5

    Encapsulation: Tunnel

14. Click **Save**.

Bidirectional Policies for Dialup VPN Users

You can create bidirectional policies for dialup VPNs. This configuration provides similar functionality as a dynamic peer VPN configuration. However, with a dynamic peer VPN configuration, the NetScreen device admin must know the internal IP address space of the dialup user, so that the admin can use it as the destination address when configuring an outgoing policy (see “Example: Policy-Based Dialup VPN, Dynamic Peer” on page 220). With a dialup VPN user configuration, the admin at the LAN site does not need to know the internal address space of the dialup user. The NetScreen device protecting the LAN uses the predefined address “Dial-Up VPN” as the source address in the incoming policy and the destination in the outgoing policy.

The ability to create bidirectional policies for a dialup VPN tunnel allows traffic to originate from the LAN end of the VPN connection after the connection has been established. Note that unlike a dialup dynamic peer VPN tunnel, this feature requires that the services on the incoming and outgoing policies be identical.

***Note:** NetScreen does not support service groups and address groups in bidirectional policies referencing a dialup VPN configuration.*

Be mindful that the internal address space of two or more concurrently connected dialup VPN users might overlap. For example, dialup users A and B might both have an internal IP address space of 10.2.2.0/24. If that happens, the NetScreen device sends all outbound VPN traffic to both user A and user B through the VPN referenced in the first policy it finds in the policy list. For example, if the outbound policy referencing the VPN to user A appears first in the policy list, then the NetScreen device sends all outbound VPN traffic intended for users A and B to user A.

Similarly, the internal address of a dialup user might happen to overlap an address in any other policy—whether or not that other policy references a VPN tunnel. If that occurs, the NetScreen device applies the first policy that matches the basic traffic attributes of source address, destination address, source port number, destination port number, service. To avoid a bidirectional dialup VPN policy with a dynamically derived address superseding another policy with a static address, NetScreen recommends positioning the bidirectional dialup VPN policy lower in the policy list.

Example: Bidirectional Dialup VPN Policies

In this example, you configure bidirectional policies for a dialup AutoKey IKE VPN tunnel named *VPN_dial* for IKE user *dialup-j* with IKE ID *jf@ns.com*. For Phase 1 negotiations, you use the proposal *pre-g2-3des-sha*, with the preshared key *Jf11d7uU*. You select the predefined “Compatible” set of proposals for Phase 2 negotiations.

The IKE user initiates a VPN connection to the NetScreen device from the Untrust zone to reach corporate servers in the Trust zone. After the IKE user establishes the VPN connection, traffic can initiate from either end of the tunnel.

The Trust zone interface is ethernet1, has IP address 10.1.1.1/24, and is in NAT mode. The Untrust zone interface is ethernet3 and has IP address 1.1.1.1/24. The default route points to the external router at 1.1.1.250.

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

2. Objects

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: trust_net

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Users > Local > New: Enter the following, and then click **OK**:

User Name: dialup-j

Status: Enable

IKE User: (select)

Simple Identity: (select); jf@ns.com

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: dialup1

Security Level: Custom

Remote Gateway Type:

Dialup User: (select); dialup-j

Preshared Key: Jf11d7uU

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: VPN_dial

Security Level: Compatible

Remote Gateway:

Create a Simple Gateway: (select)

Gateway Name: dialup1

Type:

Dialup User: (select); dialup-j

Preshared Key: Jf11d7uU

Security Level: Compatible

Outgoing Interface: ethernet3

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet1

Gateway IP Address: 1.1.1.250

5. Policies

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Dial-Up VPN

Destination Address:

Address Book Entry: (select), trust_net

Service: ANY

Action: Tunnel

VPN Tunnel: VPN_dial

Modify matching bidirectional VPN policy: (select)

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Objects

```
set address trust trust_net 10.1.1.0/24
set user dialup-j ike-id u-fqdn jf@ns.com
```

3. VPN

```
set ike gateway dialup1 dialup dialup-j aggressive outgoing-interface ethernet3
    preshare Jf11d7uU proposal pre-g2-3des-sha
set vpn VPN_dial gateway dialup1 sec-level compatible
```

4. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. Policies

```
set policy from untrust to trust “Dial-Up VPN” trust_net any tunnel vpn
    VPN_dial
set policy from trust to untrust trust_net “Dial-Up VPN” any tunnel vpn
    VPN_dial
save
```

NetScreen-Remote Security Policy Editor

1. Click **Options > Secure > Specified Connections**.
2. Click **Add a new connection**, and type **Corp** next to the new connection icon that appears.
3. Configure the connection options:

   Connection Security: Secure

   Remote Party Identity and Addressing

   ID Type: IP Subnet

   Subnet: 10.1.1.0

   Mask: 255.255.255.0

   Protocol: All

   Connect using Secure Gateway Tunnel: (select)

   ID Type: IP Address, 1.1.1.1
4. Click the **PLUS** symbol, located to the left of the UNIX icon, to expand the connection policy.
5. Click **My Identity**: Do either of the following:

   Click **Pre-shared Key** > **Enter Key**: Type **Jf11d7uU**, and then click **OK**.

   ID Type: (select **E-mail Address**), and type **jf@ns.com**.
6. Click the **Security Policy** icon, and select **Aggressive Mode**.
7. Click the **PLUS** symbol, located to the left of the Security Policy icon, and then the **PLUS** symbol to the left of Authentication (Phase 1) and Key Exchange (Phase 2) to expand the policy further.

8. Click **Authentication (Phase 1)** > **Proposal 1**: Select the following Encryption and Data Integrity Algorithms:

   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2

9. Click **Key Exchange (Phase 2)** > **Proposal 1**: Select the following IPSec Protocols:

   Encapsulation Protocol (ESP): (select)
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Encapsulation: Tunnel

10. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel

11. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

12. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel

13. Click **Save**.

Group IKE ID

Some organizations have many dialup VPN users. For example, a sales department might have hundreds of users, many of whom require secure dialup communication when off site. With so many users, it is impractical to create a separate user definition, dialup VPN configuration, and policy for each one.

To avoid this difficulty, the Group IKE ID method makes one user definition available for multiple users. The group IKE ID user definition applies to all users having certificates with specified values in the distinguished name (dn) or to all users whose full IKE ID and preshared key on their VPN client match a partial IKE ID and preshared key on the NetScreen device.

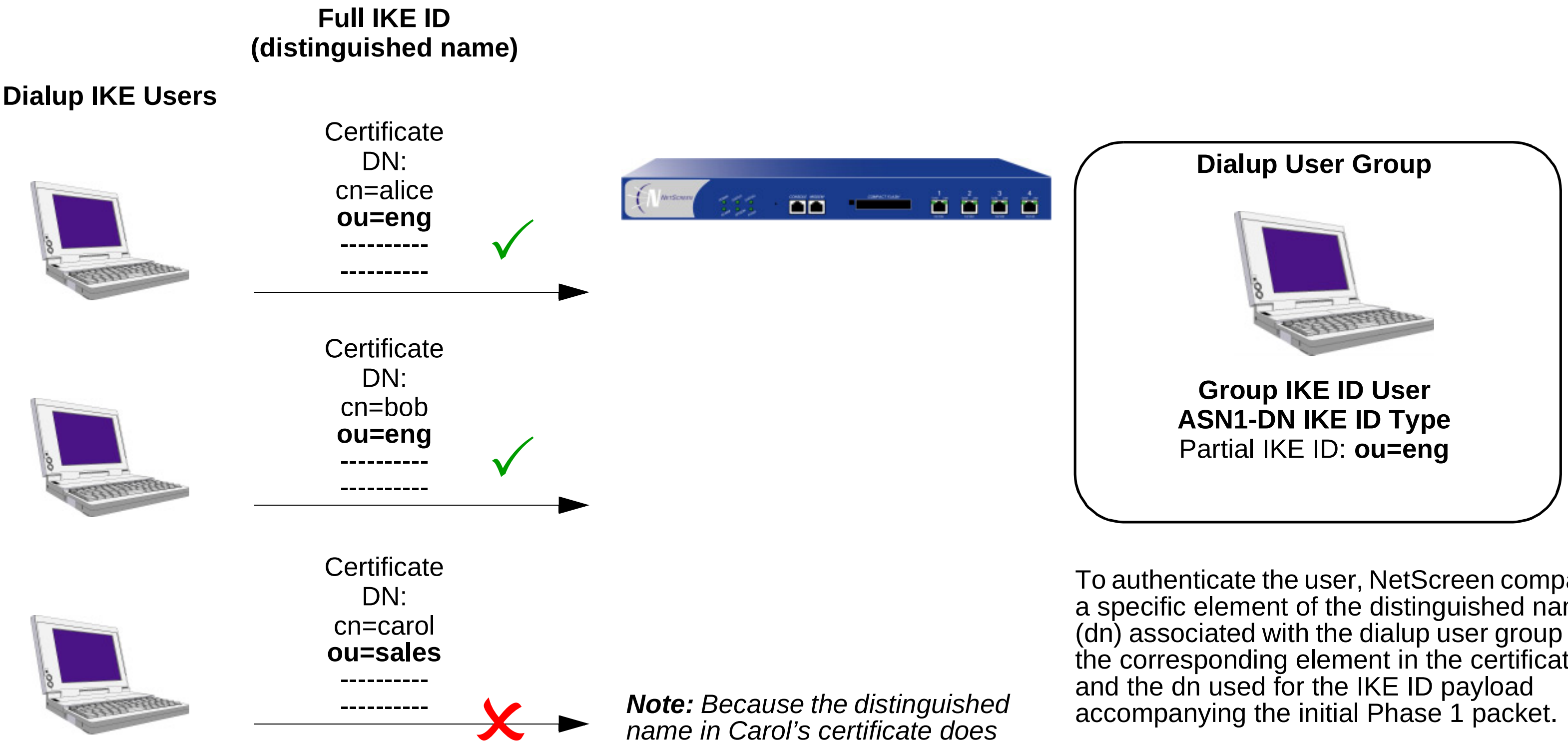
Note: *When a dialup IKE user connects to the NetScreen device, the NetScreen device first extracts and uses the full IKE ID to search its peer gateway records in case the user does not belong to a group IKE ID user group. If the full IKE ID search produces no matching entry, the NetScreen device then checks for a partial IKE ID match between the incoming embedded IKE ID and a configured group IKE ID user.*

You add a single group IKE ID user to an IKE dialup VPN user group and specify the maximum number of concurrent connections that that group supports. The maximum number of concurrent sessions cannot exceed the maximum number of allowed Phase 1 SAs or the maximum number of VPN tunnels allowed on the NetScreen platform.

Group IKE ID with Certificates

Group IKE ID with certificates is a technique for performing IKE authentication for a group of dialup IKE users without configuring a separate user profile for each one. Instead, the NetScreen device uses a single group IKE ID user profile that contains a partial IKE ID. A dialup IKE user can successfully build a VPN tunnel to a NetScreen device if the VPN configuration on his VPN client specifies a certificate that contains distinguished name elements that match those configured as the partial IKE ID definition in the group IKE ID user profile on the NetScreen device.

Group IKE ID with Certificates



To authenticate the user, NetScreen compares a specific element of the distinguished name (dn) associated with the dialup user group with the corresponding element in the certificate and the dn used for the IKE ID payload accompanying the initial Phase 1 packet.

Note: *Because the distinguished name in Carol's certificate does not include* ***ou=eng****, NetScreen rejects the connection request.*

You can set up group IKE ID with certificates as follows:

On the NetScreen Device:

1. Create a new group IKE ID user with a partial IKE identity (such as *ou=sales,o=netscreen*), and specify how many dialup users can use the group IKE ID profile to log on.
2. Assign the new group IKE ID user to a dialup user group[7], and name the group.
3. In the dialup AutoKey IKE VPN configuration, specify the name of the dialup user group, that the Phase 1 negotiations be in Aggressive mode, and that certificates (RSA or DSA, depending on the type of certificate loaded on the dialup VPN clients) be used for authentication.
4. Create a policy permitting inbound traffic via the specified dialup VPN.

On the VPN Client:

1. Obtain and load a certificate whose distinguished name contains the same information as defined in the partial IKE ID on the NetScreen device.
2. Configure a VPN tunnel to the NetScreen device using Aggressive mode for Phase 1 negotiations, specify the certificate that you have previously loaded, and select *Distinguished Name* for the local IKE ID type.

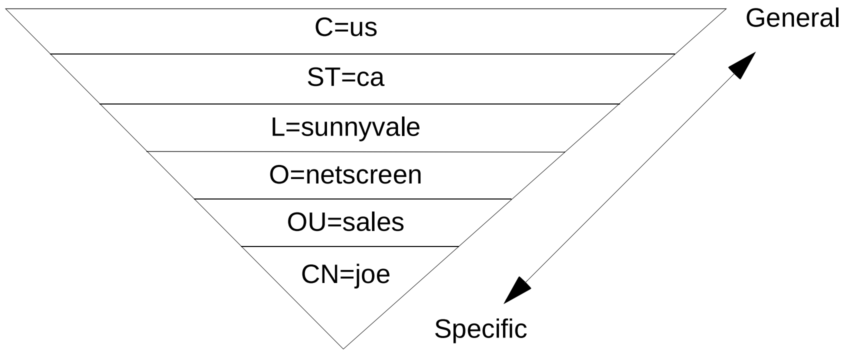
Thereafter, each individual dialup IKE user with a certificate with distinguished name elements that match the partial IKE ID defined in the group IKE ID user profile can successfully build a VPN tunnel to the NetScreen device. For example, if the group IKE ID user has IKE ID *OU=sales,O=netscreen,* the NetScreen device accepts Phase 1 negotiations from any user with a certificate containing those elements in its distinguished name. The maximum number of such dialup IKE users that can connect to the NetScreen device depends upon the maximum number of concurrent sessions that you specify in the group IKE ID user profile.

[7] You can put only one group IKE ID user in an IKE user group.

Wildcard and Container ASN1-DN IKE ID Types

When you define the IKE ID for a group IKE user, you must use the Abstract Syntax Notation, version 1, distinguished name (ASN1-DN) as the IKE ID type of identity configuration. This notation is a string of values, which is frequently, though not always, ordered from general to specific. For example:

ASN1-DN: C=us,ST=ca,L=sunnyvale,O=netscreen,OU=sales,CN=joe



Legend:

C = Country

ST = State

L = Locality

O = Organization

OU = Organizational Unit

CN = Common Name

When configuring the group IKE ID user, you must specify the peer's ASN1-DN ID as one of two types:

- **Wildcard:** NetScreen authenticates a dialup IKE user's ID if the values in the dialup IKE user's ASN1-DN identity fields match those in the group IKE user's ASN1-DN identity fields. The wildcard ID type supports only one value per identity field (for example, "ou=eng" or "ou=sw", but not "ou=eng,ou=sw"). The ordering of the identity fields in the two ASN1-DN strings is inconsequential.
- **Container:** NetScreen authenticates a dialup IKE user's ID if the values in the dialup IKE user's ASN1-DN identity fields exactly match the values in the group IKE user's ASN1-DN identity fields. The container ID type supports multiple entries for each identity field (for example, "ou=eng,ou=sw,ou=screenos"). The ordering of the values in the identity fields of the two ASN1-DN strings must be identical.

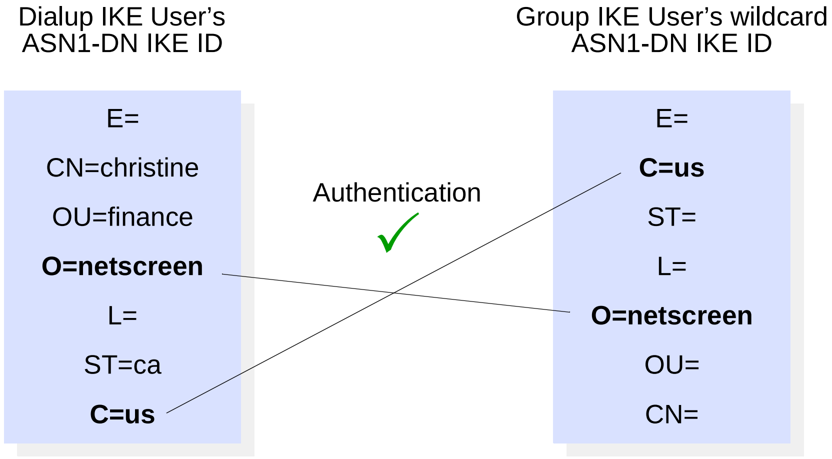
When configuring an ASN1-DN ID for a remote IKE user, specify the type as either "wildcard" or "container" and define the ASN1-DN ID that you expect to receive in the peer's certificate (for example, "c=us,st=ca,cn=jrogers"). When configuring an ASN1-DN ID for a local IKE ID, use the following keyword: [DistinguishedName]. Include the brackets and spell it exactly as shown.

Wildcard ASN1-DN IKE ID

A wildcard ASN1-DN requires values in the remote peer's distinguished name IKE ID to match values in the group IKE user's partial ASN1-DN IKE ID. The sequencing of these values in the ASN1-DN string is inconsequential. For example, if the dialup IKE user's ID and the group IKE user's ID are as follows

- Dialup IKE user's full ASN1-DN IKE ID: CN=christine,OU=finance,**O=netscreen**,ST=ca,**C=us**
- Group IKE user's partial ASN1-DN IKE ID: **C=us**,**O=netscreen**

then a wildcard ASN1-DN IKE ID successfully matches the two IKE IDs, even though the order of values in the two IDs is different.

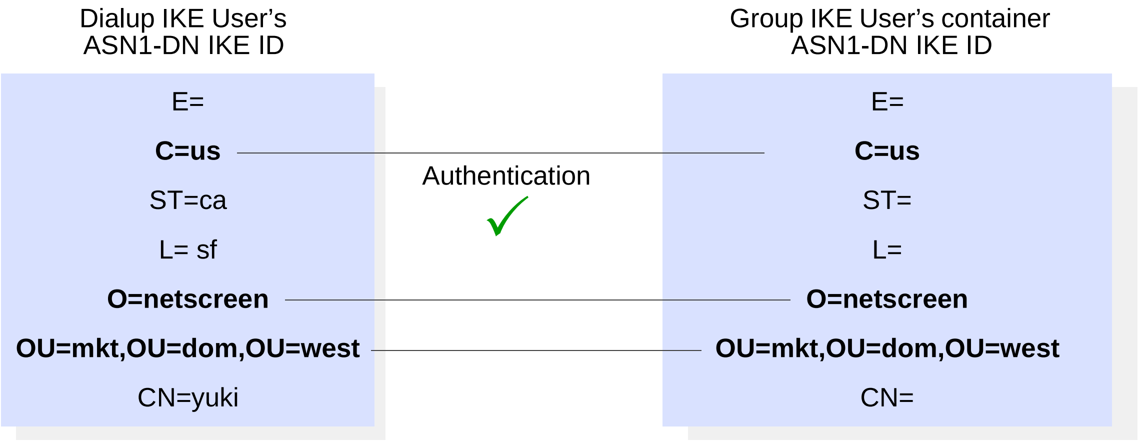


The dialup IKE user's ASN1-DN contains the values specified in the group IKE user's ASN1-DN. The order of the values does not matter.

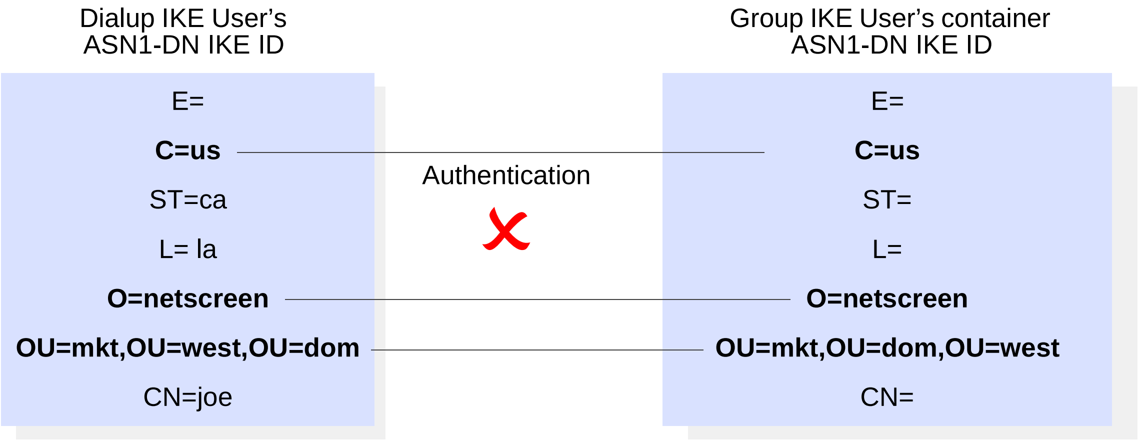
Container ASN1-DN IKE ID

A container ASN1-DN ID allows the group IKE user’s ID to have multiple entries in each identity field. NetScreen authenticates a dialup IKE user if the dialup user’s ID contains values that exactly match the values in the group IKE user’s ID. Unlike the wildcard type, the order of the ASN1-DN fields must be identical in both the dialup IKE user’s and group IKE user’s IDs and the order of multiple values in those fields must be identical.

The first dialup IKE user’s ASN1-DN contains exact matches of the group IKE user’s ASN1-DN. The order of the multiple entries in the OU ID field is also identical.

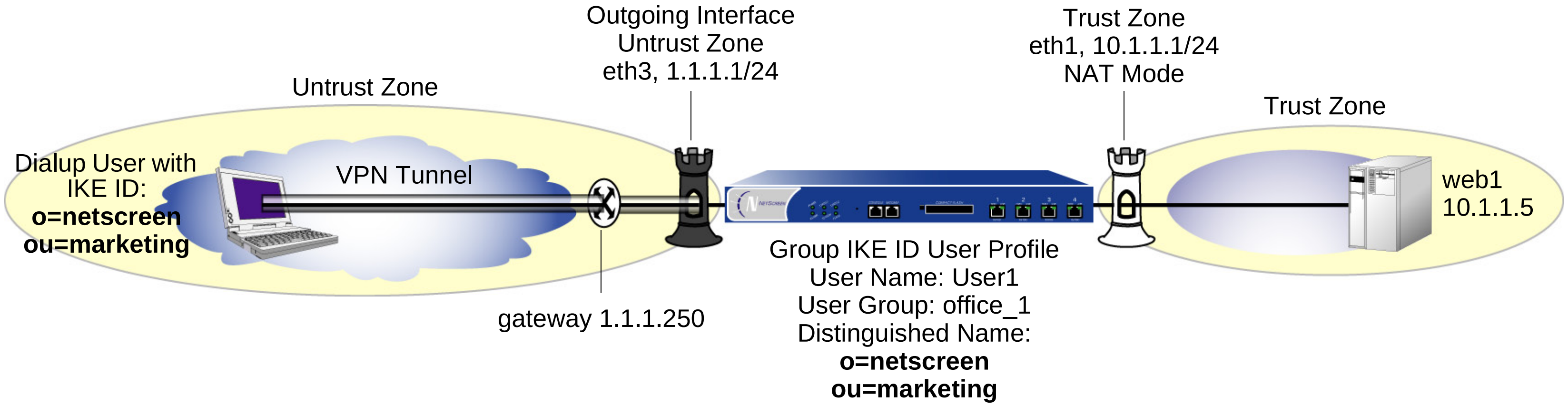


The second dialup IKE user’s ASN1-DN contains exact matches of the group IKE user’s ASN1-DN. However, the order of the multiple entries in the OU ID field is not identical.



Example: Group IKE ID (Certificates)

In this example, you create a new group IKE ID user definition named *User1*. You configure it to accept up to 10 Phase 1 negotiations concurrently from VPN clients with RSA certificates containing *O=netscreen* and *OU=marketing*. The certificate authority (CA) is Verisign. You name the dialup IKE user group *office_1*.



The dialup IKE users send a distinguished name as their IKE ID. The distinguished name (dn) in a certificate for a dialup IKE user in this group might appear as the following concatenated string:

> C=us,ST=ca,L=sunnyvale,**O=netscreen**,**OU=marketing**,CN=michael zhang,CN=a2010002,CN=ns500, CN=4085557800,CN=rsa-key,CN=10.10.5.44

Because the values *O=netscreen* and *OU=marketing* appear in the peer’s certificate and the user uses the distinguished name as its IKE ID type, the NetScreen device authenticates the user.

For the Phase 1 and 2 security levels, you specify one Phase 1 proposal—rsa-g2-3des-sha for certificates—and select the predefined “Compatible” set of proposals for Phase 2.

You configure a dialup VPN and a policy permitting HTTP traffic via the VPN tunnel to reach the Web server *Web1*. The configuration of the remote VPN client (using NetScreen-Remote) is also included.

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **OK**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

2. Address

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: web1

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.5/32

Zone: Trust

3. Users

Objects > Users > Local > New: Enter the following, then click **OK**:

User Name: User1

Status Enable: (select)

IKE User: (select)

Number of Multiple Logins with same ID: 10

Use Distinguished Name For ID: (select)

OU: marketing

Organization: netscreen

Objects > User Groups > Local > New: Type **office_1** in the Group Name field, do the following, and then click **OK**:

Select **User1** and use the **<<** button to move her from the Available Members column to the Group Members column.

4. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: Corp_GW

Security Level: Custom

Remote Gateway Type: Dialup User Group: (select), Group: office_1

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Custom

Phase 1 Proposal (For Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Corp_VPN

Security Level: Compatible

Remote Gateway: Predefined: (select), Corp_GW

5. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

6. Policy

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Dial-Up VPN

Destination Address:

Address Book Entry: (select), web1

Service: HTTP

Action: Tunnel

Tunnel VPN: Corp_VPN

Modify matching bidirectional VPN policy: (clear)

Position at Top: (select)

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Address

```
set address trust web1 10.1.1.5/32
```

3. Users

```
set user User1 ike-id asn1-dn wildcard o=netscreen,ou=marketing share-limit 10
set user-group office_1 user User1
```

4. VPN

```
set ike gateway Corp_GW dialup office_1 aggressive outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway Corp_GW cert peer-ca 1[8]
set ike gateway Corp_GW cert peer-cert-type x509-sig
set vpn Corp_VPN gateway Corp_GW sec-level compatible
```

5. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. Policy

```
set policy top from untrust to trust “Dial-Up VPN” web1 http tunnel vpn Corp_VPN
save
```

[8] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get pki x509 list ca-cert**.

NetScreen-Remote Security Policy Editor

1. Click **Options > Secure > Specified Connections**.
2. Click **Add a new connection**, and type **web1** next to the new connection icon that appears.
3. Configure the connection options:

   Connection Security: Secure

   Remote Party Identity and Addressing

   ID Type: IP Address, 10.1.1.5

   Protocol: Highlight **All**, type **HTTP**, press the **Tab** key, and type **80**.

   Connect using Secure Gateway Tunnel: (select)

   ID Type: IP Address, 1.1.1.1
4. Click the **PLUS** symbol, located to the left of the web1 icon, to expand the connection policy.
5. Click **My Identity**: Select the certificate that has *o=netscreen,ou=marketing* as elements in its distinguished name from the Select Certificate drop-down list[9].

   ID Type: Select **Distinguished Name** from the drop-down list.
6. Click the **Security Policy** icon, and select **Aggressive Mode**.
7. Click the **PLUS** symbol, located to the left of the Security Policy icon, and then the **PLUS** symbol to the left of Authentication (Phase 1) and Key Exchange (Phase 2) to expand the policy further.
8. Click **Authentication (Phase 1)** > **Proposal 1**: Select the following Encryption and Data Integrity Algorithms:

   Authentication Method: RSA Signatures

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

[9] This example assumes that you have already loaded a suitable certificate on the NetScreen-Remote client. For information on loading certificates on the NetScreen-Remote, refer to NetScreen-Remote documentation.

9. Click **Key Exchange (Phase 2)** > **Proposal 1**: Select the following IPSec Protocols:

   Encapsulation Protocol (ESP): (select)
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Encapsulation: Tunnel

10. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

   Encapsulation Protocol (ESP): (select)
   Encrypt Alg: Triple DES
   Hash Alg: MD5
   Encapsulation: Tunnel

11. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

   Encapsulation Protocol (ESP): (select)
   Encrypt Alg: DES
   Hash Alg: SHA-1
   Encapsulation: Tunnel

12. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

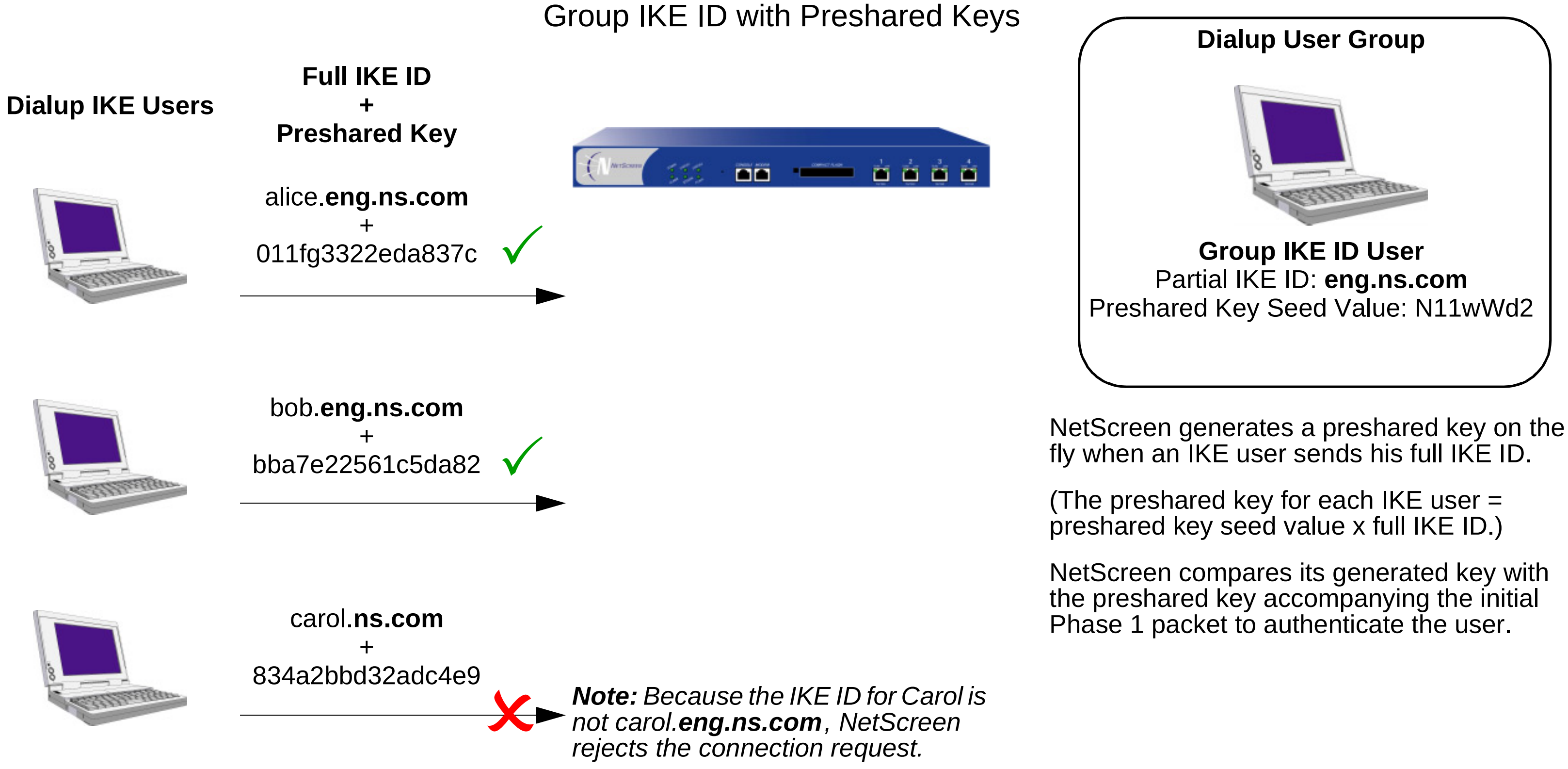
   Encapsulation Protocol (ESP): (select)
   Encrypt Alg: DES
   Hash Alg: MD5
   Encapsulation: Tunnel

13. Click **Save**.

Group IKE ID with Preshared Keys

Group IKE ID with preshared keys is a technique for performing IKE authentication for a group of dialup IKE users without configuring a separate user profile for each one. Instead, the NetScreen device uses a single group IKE ID user profile, which contains a partial IKE ID. A dialup IKE user can successfully build a VPN tunnel to a NetScreen device if the VPN configuration on his VPN client has the correct preshared key and if the rightmost part of the user’s full IKE ID matches the group IKE ID user profile’s partial IKE ID.

Group IKE ID with Preshared Keys



Note: *Because the IKE ID for Carol is not carol.**eng.ns.com**, NetScreen rejects the connection request.*

NetScreen generates a preshared key on the fly when an IKE user sends his full IKE ID.

(The preshared key for each IKE user = preshared key seed value x full IKE ID.)

NetScreen compares its generated key with the preshared key accompanying the initial Phase 1 packet to authenticate the user.

The IKE ID type that you can use for the Group IKE ID with Preshared Key feature can be either an e-mail address or a fully qualified domain name (FQDN).

You can set up group IKE ID with preshared keys as follows:

On the NetScreen Device:

1. Create a new group IKE ID user with a partial IKE identity (such as **netscreen.com**), and specify how many dialup users can use the group IKE ID profile to log on.
2. Assign the new group IKE ID user to a dialup user group.
3. In the dialup AutoKey IKE VPN configuration, assign a name for the remote gateway (such as **road1**), specify the dialup user group, and enter a preshared key seed value.
4. Use the following CLI command to generate an individual dialup user’s preshared key using the preshared key seed value and the full user IKE ID (such as **joe@netscreen.com**)

   exec ike preshare-gen *name_str usr_name_str*

   (for example) **exec ike preshare-gen road1 joe@netscreen.com**
5. Record the preshared key for use when configuring the remote VPN client.

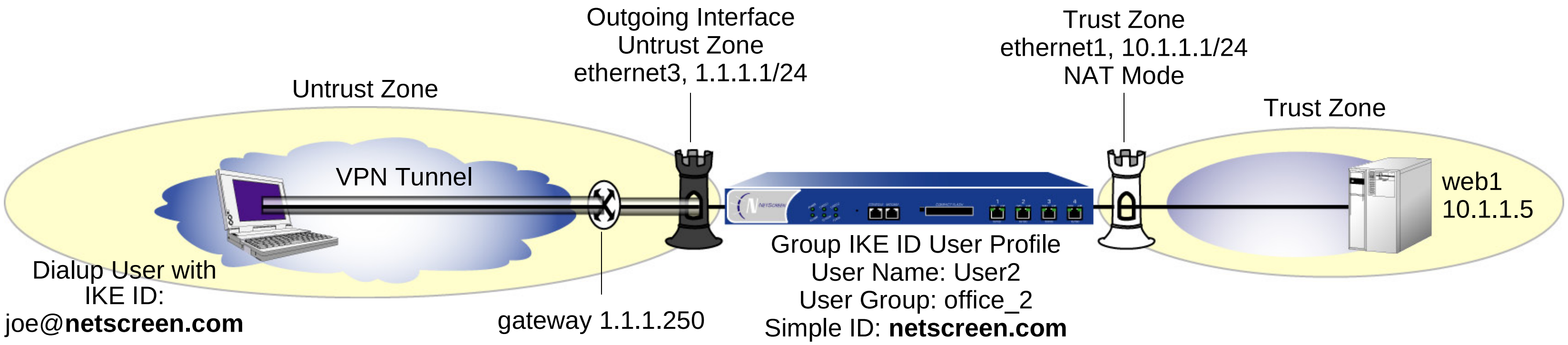
On the VPN Client:

Configure a VPN tunnel to the NetScreen device using Aggressive mode for Phase 1 negotiations and enter the preshared key that you previously generated on the NetScreen device.

Thereafter, the NetScreen device can successfully authenticate each individual user whose full IKE ID contains a section that matches the partial group IKE ID user profile. For example, if the group IKE ID user has IKE identity **netscreen.com**, any user with that domain name in his IKE ID can initiate Phase 1 IKE negotiations in Aggressive mode with the NetScreen device. For example: **alice@netscreen.com**, **bob@netscreen.com** and **carol@netscreen.com**. How many such users can log on depends upon a maximum number of concurrent sessions specified in the group IKE ID user profile.

Example: Group IKE ID (Preshared Keys)

In this example, you create a new group IKE ID user named *User2*. You configure it to accept up to 10 Phase 1 negotiations concurrently from VPN clients with preshared keys containing an IKE ID ending with the string *netscreen.com*. The seed value for the preshared key is *jk930k*. You name the dialup IKE user group *office_2*.



For both the Phase 1 and 2 negotiations, you select the security level predefined as “Compatible”. All the security zones are in the trust-vr routing domain.

WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **OK**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

2. Address

Objects > Addresses > List > New : Enter the following, and then click **OK**:

Address Name: web1

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.5/32

Zone: Trust

3. Users

Objects > Users > Local > New: Enter the following, then click **OK**:

User Name: User2

Status: Enable

IKE User: (select)

Number of Multiple Logins with same ID: 10

Simple Identity: (select)

IKE Identity: netscreen.com

Objects > User Groups > Local > New: Type **office_2** in the Group Name field, do the following, and then click **OK**:

Select **User2** and use the **<<** button to move him from the Available Members column to the Group Members column.

4. VPN

> ***Note:*** *The WebUI allows you to enter only a value for a preshared key, not a seed value from which the NetScreen device derives a preshared key. To enter a preshared key seed value when configuring an IKE gateway, you must use the CLI.*

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Corp_VPN

Security Level: Compatible

Remote Gateway: Predefined: (select), Corp_GW

5. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

6. Policy

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Dial-Up VPN

Destination Address:

Address Book Entry: (select), web1

Service: HTTP

Action: Tunnel

Tunnel VPN: Corp_VPN

Modify matching bidirectional VPN policy: (clear)

Position at Top: (select)

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Address

```
set address trust web1 10.1.1.5/32
```

3. Users

```
set user User2 ike-id u-fqdn netscreen.com share-limit 10
set user-group office_2 user User2
```

4. VPN

```
set ike gateway Corp_GW dialup office_2 aggressive seed-preshare jk930k
    sec-level compatible
set vpn Corp_VPN gateway Corp_GW sec-level compatible
```

5. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. Policy

```
set policy top from untrust to trust “Dial-Up VPN” web1 http tunnel vpn
    Corp_VPN
save
```

Obtaining the Preshared Key

You can only obtain the preshared key by using the following CLI command:

exec ike preshare-gen *name_str usr_name_str*

The preshared key, based on the preshared key seed value *jk930k* (as specified in the configuration for the remote gateway named *Corp_GW*) and the full identity of individual user *joe@netscreen.com* is *11ccce1d396f8f29ffa93d11257f691af96916f2*.

NetScreen-Remote Security Policy Editor

1. Click **Options > Secure > Specified Connections**.
2. Click **Add a new connection**, and type **web1** next to the new connection icon that appears.
3. Configure the connection options:

   Connection Security: Secure

   Remote Party Identity and Addressing

   ID Type: IP Address, 10.1.1.5

   Protocol: Highlight **All**, type **HTTP**, press the **Tab** key, and type **80**.

   Connect using Secure Gateway Tunnel: (select)

   ID Type: IP Address, 1.1.1.1
4. Click the **PLUS** symbol, located to the left of the web1 icon, to expand the connection policy.
5. Click the **Security Policy** icon, and select **Aggressive Mode**.
6. Click **My Identity**: Click **Pre-shared Key** > **Enter Key**: Type **11ccce1d396f8f29ffa93d11257f691af96916f2**, and then click **OK**.

   ID Type: (select **E-mail Address**), and type **joe@netscreen.com**.
7. Click the **PLUS** symbol, located to the left of the Security Policy icon, and then click the **PLUS** symbol to the left of Authentication (Phase 1) and Key Exchange (Phase 2) to expand the policy further.

8. Click **Authentication (Phase 1)** > **Proposal 1**: Select the following Encryption and Data Integrity Algorithms:

   Authentication Method: Pre-Shared Key

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

9. Click **Authentication (Phase 1)** > **Create New Proposal**: Select the following IPSec Protocols:

   Encapsulation Protocol (ESP): (select)

   Encrypt Alg: Triple DES

   Hash Alg: MD5

   Key Group: Diffie-Hellman Group 2

10. Click **Authentication (Phase 1)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: SHA-1

    Key Group: Diffie-Hellman Group 2

11. Click **Authentication (Phase 1)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: MD5

    Key Group: Diffie-Hellman Group 2

12. Click **Key Exchange (Phase 2)** > **Proposal 1**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: Triple DES

Hash Alg: SHA-1

Encapsulation: Tunnel

13. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: Triple DES

    Hash Alg: MD5

    Encapsulation: Tunnel

14. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: SHA-1

    Encapsulation: Tunnel

15. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: MD5

    Encapsulation: Tunnel

16. Click **Save**.

Shared IKE IDs

The shared IKE ID feature facilitates the deployment of a large number of dialup users. With this feature, the NetScreen device authenticates multiple dialup VPN users using a single group IKE ID and preshared key. Thus, it provides IPSec protection for large remote user groups through a common VPN configuration.

This feature is similar to the Group IKE ID with pre-shared keys feature, with the following differences:

- With the group IKE ID feature, the IKE ID can be an e-mail address or an FQDN (fully-qualified domain name). For this feature, the IKE ID must be an e-mail address.
- Instead of using the preshared key seed value and the full user IKE ID to generate a preshared key for each user, you specify a single preshared key for all users in the group.
- You must use XAuth to authenticate the individual users.

To set up a shared IKE ID and preshared key on the NetScreen device:

1. Create a new group IKE ID user, and specify how many dialup users can use the group IKE ID to log on. For this feature, use an e-mail address as the IKE ID.
2. Assign the new group IKE ID to a dialup user group.
3. In the dialup-to-LAN autokey IKE VPN configuration, create a shared IKE ID gateway.
4. Define the XAuth users and enable XAuth on the remote IKE gateway.

On the VPN Client:

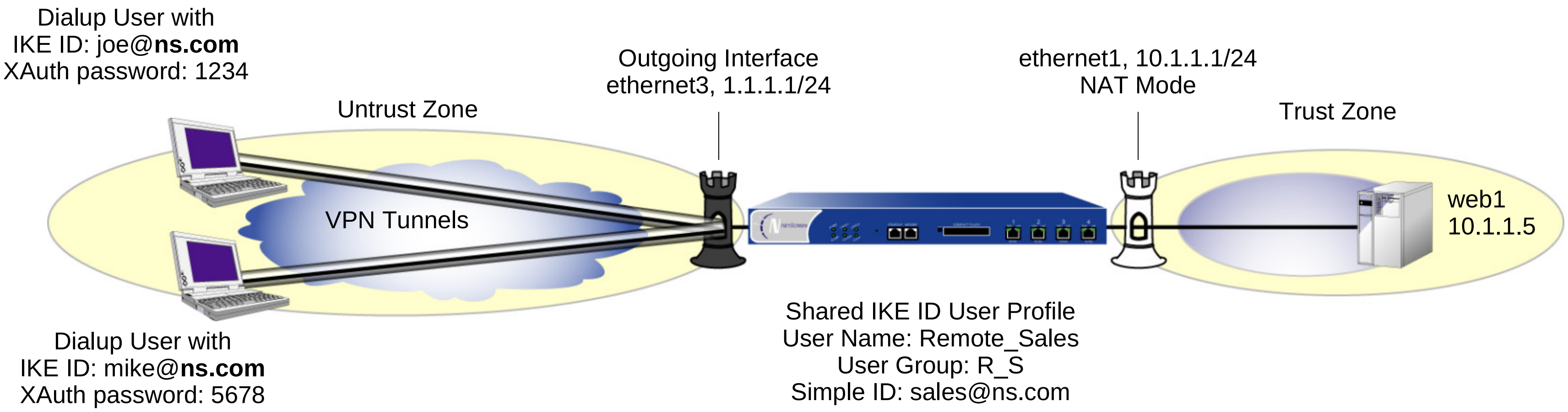
Configure a VPN tunnel to the NetScreen device using Aggressive mode for Phase 1 negotiations and enter the preshared key that you previously defined on the NetScreen device.Thereafter, the NetScreen device authenticates each remote user as follows:

During Phase 1 negotiations, the NetScreen device first authenticates the VPN client by matching the IKE ID and preshared key that the client sends with the IKE ID and preshared key on the NetScreen device. If there is a match, then the NetScreen device uses XAuth to authenticate the individual user. It sends a login prompt to the user at the remote site between Phase 1 and Phase 2 IKE negotiations. If the remote user successfully logs on with the correct user name and password, Phase 2 negotiations begin.

Example: Shared IKE ID (Preshared Keys)

In this example, you create a new group IKE ID user named Remote_Sales. It accepts up to 250 Phase 1 negotiations concurrently from VPN clients with the same preshared key (abcd1234). You name the dialup IKE user group *R_S*. In addition, you configure two XAuth users, Joe and MIke.

For both the Phase 1 and 2 negotiations, you select the security level predefined as “Compatible”. All the security zones are in the trust-vr routing domain.



WebUI

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

2. Address

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: web1

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.5/32

Zone: Trust

3. Users

Objects > Users > Local > New: Enter the following, then click **OK**:

User Name: Remote_Sales

Status: Enable

IKE User: (select)

Number of Multiple Logins with same ID: 250

Simple Identity: (select)

IKE Identity: sales@ns.com

Objects > User Groups > Local > New: Type **R_S** in the Group Name field, do the following, and then click **OK**:

Select **Remote_sales** and use the **<<** button to move him from the Available Members column to the Group Members column.

Objects > Users > Local > New: Enter the following, then click **OK**:

User Name: Joe

Status: Enable

XAuth User: (select)

Password: 1234

Confirm Password: 1234

Objects > Users > Local > New: Enter the following, then click **OK**:

User Name: Mike

Status: Enable

XAuth User: (select)

Password: 5678

Confirm Password: 5678

4. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: sales_gateway

Security Level: Compatible (select)

Remote Gateway Type: Dialup Group (select), R_S

Preshared Key: abcd1234

Outgoing Interface: ethernet3

> Advanced: Enter the following, and then click **Return** to return to the base Gateway configuration page:

Enable XAuth: (select)

Local Authentication: (select)

Allow Any: (select)

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: Sales_VPN

Security Level: Compatible

Remote Gateway: Predefined: (select) sales_gateway

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Zone, Untrust-Tun

5. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

6. Policy

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Dial-Up VPN

Destination Address:

Address Book Entry: (select), web1

Service: HTTP

Action: Tunnel

Tunnel VPN: Sales_VPN

Modify matching bidirectional VPN policy: (clear)

Position at Top: (select)

CLI

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Address

```
set address trust web1 10.1.1.5/32
```

3. Users

```
set user Remote_Sales ike-id sales@ns.com share-limit 250
set user-group R_S user Remote_Sales
set user Joe password 1234
set user Joe type xauth
set user Mike password 5678
set user Mike type xauth
```

4. VPN

```
set ike gateway sales_gateway dialup R_S aggressive outgoing-interface
    ethernet3 preshare abcd1234 sec-level compatible
set ike gateway sales_gateway xauth
set vpn sales_vpn gateway sales_gateway sec-level compatible
set vpn sales_vpn bind zone untrust-tun
```

5. Route

```
set route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. Policy

```
set policy top from untrust to trust “Dial-Up VPN” web1 http tunnel vpn sales_vpn
save
```

NetScreen-Remote Security Policy Editor

This example shows the configuration for the user named Joe.

1. Click **Options > Secure > Specified Connections**.
2. Click **Add a new connection**, and type **web1** next to the new connection icon that appears.
3. Configure the connection options:

   Connection Security: Secure

   Remote Party ID Type: IP Address

   IP Address: 10.1.1.5

   Connect using Secure Gateway Tunnel: (select)

   ID Type: IP Address; 1.1.1.1
4. Click the **PLUS** symbol, located to the left of the web1 icon, to expand the connection policy.
5. Click the **Security Policy** icon, and select **Aggressive Mode**.
6. Click **My Identity**: Click **Pre-shared Key** > **Enter Key**: Type **abcd1234**, and then click **OK**.

   ID Type: (select **E-mail Address**), and type **sales@ns.com**.
7. Click the **PLUS** symbol, located to the left of the Security Policy icon, and then click the **PLUS** symbol to the left of Authentication (Phase 1) and Key Exchange (Phase 2) to expand the policy further.
8. Click **Authentication (Phase 1)** > **Proposal 1**: Select the following Encryption and Data Integrity Algorithms:

   Authentication Method: Pre-Shared Key; Extended Authentication

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

9. Click **Authentication (Phase 1)** > **Create New Proposal**: Select the following IPSec Protocols:

   Encapsulation Protocol (ESP): (select)
   Encrypt Alg: Triple DES
   Hash Alg: MD5
   Key Group: Diffie-Hellman Group 2

10. Click **Authentication (Phase 1)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Key Group: Diffie-Hellman Group 2

11. Click **Authentication (Phase 1)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)
    Encrypt Alg: DES
    Hash Alg: MD5
    Key Group: Diffie-Hellman Group 2

12. Click **Key Exchange (Phase 2)** > **Proposal 1**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)
    Encrypt Alg: Triple DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

13. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel

14. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

15. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel

16. Click **Save**.

6

L2TP

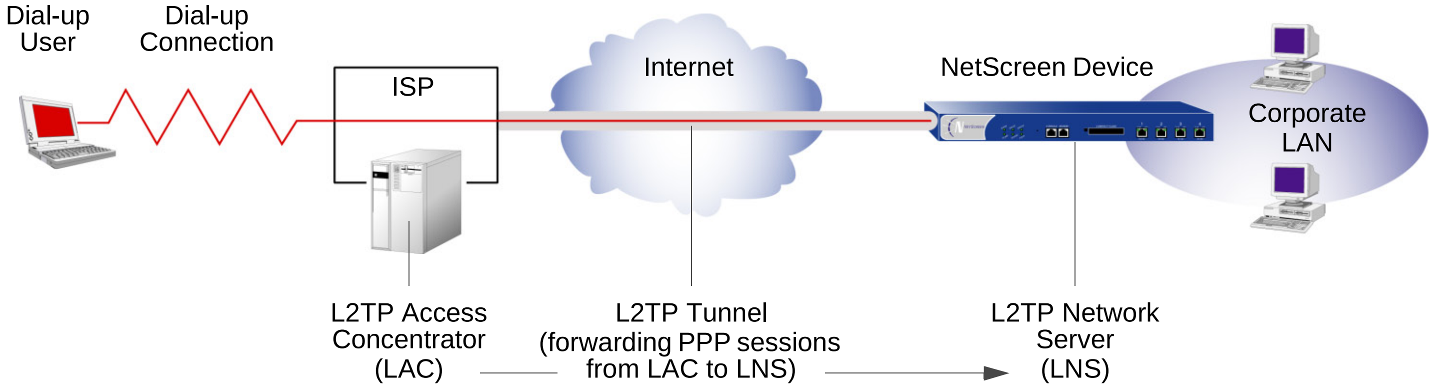
This chapter provides an introduction to Layer 2 Tunneling Protocol (L2TP), its use alone and with IPSec support, and then some configuration examples for L2TP and L2TP-over-IPSec:

- “Introduction to L2TP” on page 270
- “Packet Encapsulation and Decapsulation” on page 274
- “L2TP Parameters” on page 276
  - “Example: Configuring an IP Pool and L2TP Default Settings” on page 277
- “L2TP and L2TP-over-IPSec” on page 279
  - “Example: Configuring L2TP” on page 280
  - “Example: Configuring L2TP-over-IPSec” on page 286

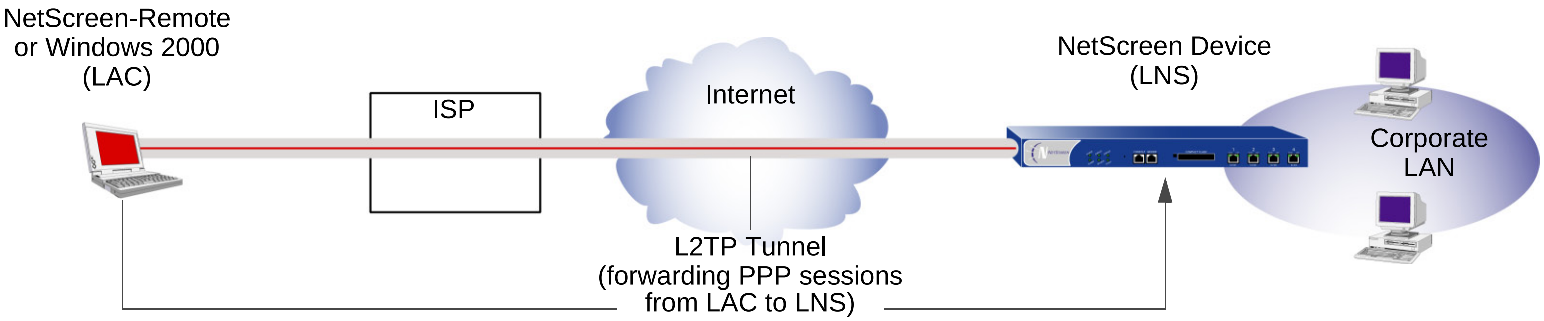
INTRODUCTION TO L2TP

Layer 2 Tunneling Protocol (L2TP) provides a way for a dial-up user to make a virtual Point-to-Point Protocol (PPP) connection to an L2TP network server (LNS), which can be a NetScreen device. L2TP sends PPP frames through a tunnel between an L2TP access concentrator (LAC) and the LNS.

Originally, L2TP was designed so that a LAC residing at an ISP site tunneled to an LNS at either another ISP or corporate site. The L2TP tunnel did not extend completely to the dial-up user's computer, but only to the LAC at the dial-up user's local ISP. (This is sometimes referred to as a compulsory L2TP configuration.)

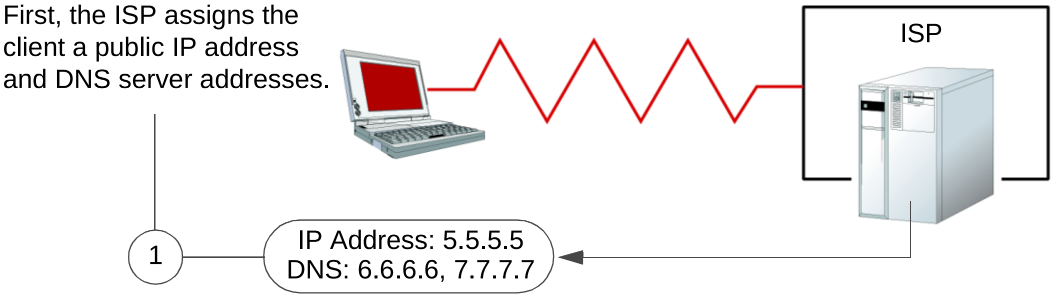

Dial-up User
Dial-up Connection
ISP
Internet
NetScreen Device
Corporate LAN
L2TP Access Concentrator (LAC)
L2TP Tunnel (forwarding PPP sessions from LAC to LNS)
L2TP Network Server (LNS)

With the capability of a NetScreen-Remote client on Windows 2000 or Windows NT, or a Windows 2000 client by itself, to act as a LAC, the L2TP tunnel can extend directly to the dial-up user's computer, thus providing end-to-end tunneling. (This approach is sometimes referred to as a voluntary L2TP configuration.)

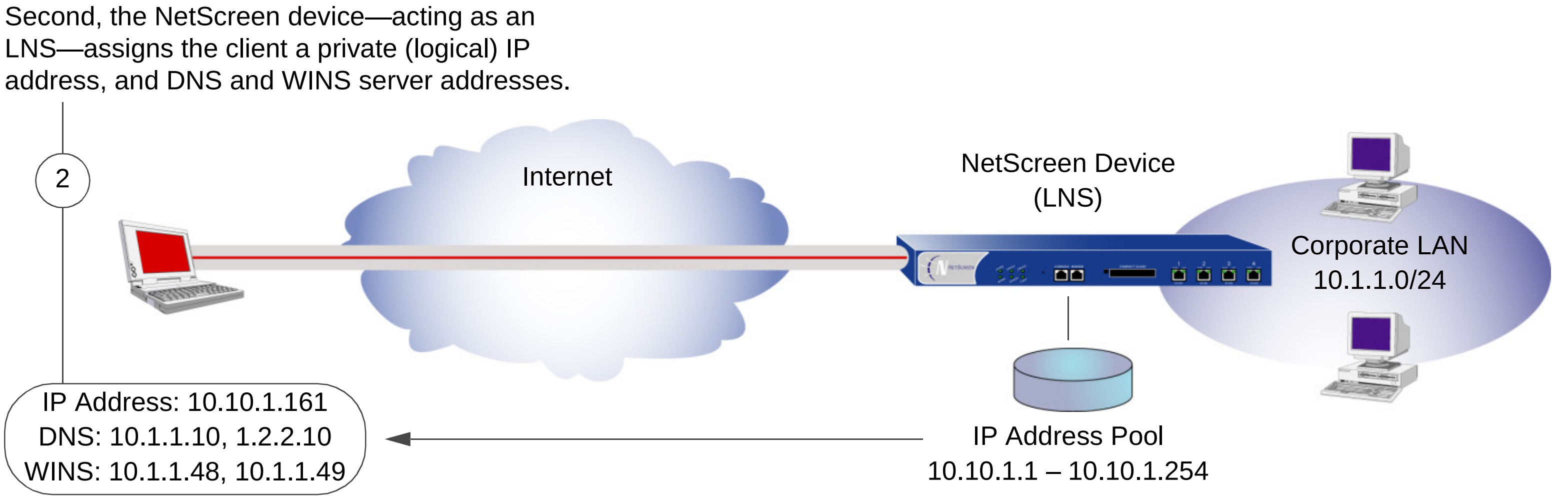


Because the PPP link extends from the dial-up user across the Internet to the NetScreen device (LNS), it is the NetScreen device, not the ISP, that assigns the client its IP address, DNS and WINS servers addresses, and authenticates the user, either from the local database or from an external auth server (RADIUS, SecurID, or LDAP).

In fact, the client receives two IP addresses—one for its physical connection to the ISP, and a logical one from the LNS. When the client contacts its ISP, perhaps using PPP, the ISP makes IP and DNS assignments, and authenticates the client. This allows users to connect to the Internet with a public IP address, which becomes the outer IP address of the L2TP tunnel.


First, the ISP assigns the
client a public IP address
and DNS server addresses.
ISP
1
IP Address: 5.5.5.5
DNS: 6.6.6.6, 7.7.7.7

Then, when the L2TP tunnel forwards the encapsulated PPP frames to the NetScreen device, the NetScreen device assigns the client an IP address, and DNS and WINS settings. The IP address can be from the set of private addresses not used on the Internet. This address becomes the inner IP address of the L2TP tunnel.


Second, the NetScreen device—acting as an LNS—assigns the client a private (logical) IP address, and DNS and WINS server addresses.
2
Internet
NetScreen Device (LNS)
Corporate LAN 10.1.1.0/24
IP Address: 10.10.1.161
DNS: 10.1.1.10, 1.2.2.10
WINS: 10.1.1.48, 10.1.1.49
IP Address Pool 10.10.1.1 – 10.10.1.254

Note: *The IP addresses assigned to the L2TP client must be in a different subnet from the IP addresses in the corporate LAN.*

The current version of ScreenOS provides the following L2TP support:

- L2TP tunnels originating from a host running Windows 2000[1]
- A combination of L2TP and IPSec in transport mode (L2TP-over-IPSec)
  - For NetScreen-Remote: L2TP-over-IPSec with Main mode negotiations using certificates, and Aggressive mode using either a preshared key or certificates
  - For Windows 2000: L2TP-over-IPSec with Main mode negotiations using certificates
- User authentication using either the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) from the local database or an external auth server (RADIUS, SecurID, or LDAP)

> ***Note:*** *The local database and RADIUS servers support both PAP and CHAP. SecurID and LDAP servers support PAP only.*

- The assignment of dialup users' IP address, Domain Name System (DNS) servers, and Windows Internet Naming Service (WINS) servers from either the local database or a RADIUS server
- L2TP tunnels and L2TP-over-IPSec tunnels for the root system and virtual systems

> ***Note:*** *To use L2TP, the NetScreen device must be operating at Layer 3, with security zone interfaces in NAT or Route mode. When the NetScreen device is operating at Layer 2, with security zone interfaces in Transparent mode, no L2TP-related material appears in the WebUI, and L2TP-related CLI commands elicit error messages.*

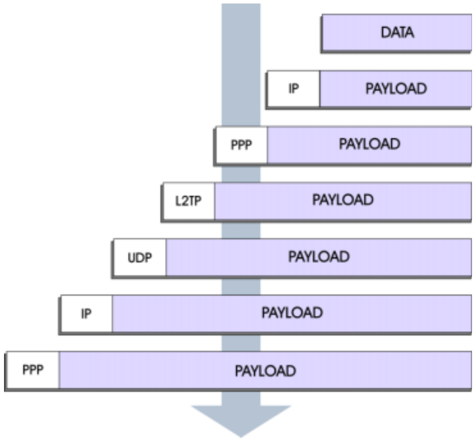
[1] By default, Windows 2000 performs L2TP-over-IPSec. To force it to use L2TP only, you must navigate to the ProhibitIPSec key in the registry and change **0** (L2TP-over-IPSec) to **1** (L2TP only). (Before performing this, NetScreen recommends that you backup your registry.) Click **Start** > **Run**: Type **regedit**. Double-click **HKEY_LOCAL_MACHINE** > **System** > **CurrentControlSet** > **Services** > **RasMan** > **Parameters**. Double-click **ProhibitIPSec**: Type **1** in the Value data field, select **Hexadecimal** as the base value, and then click **OK**. Reboot. (If you do not find such an entry in the registry, see Microsoft WIndows documentation for information on how to create one.)

Packet Encapsulation and Decapsulation

L2TP employs encapsulation of packets as the means for transporting PPP frames from the LAC to the LNS. Before looking at specific examples for setting up L2TP and L2TP-over-IPSec, an overview of the encapsulation and decapsulation involved in the L2TP process is presented.

Encapsulation

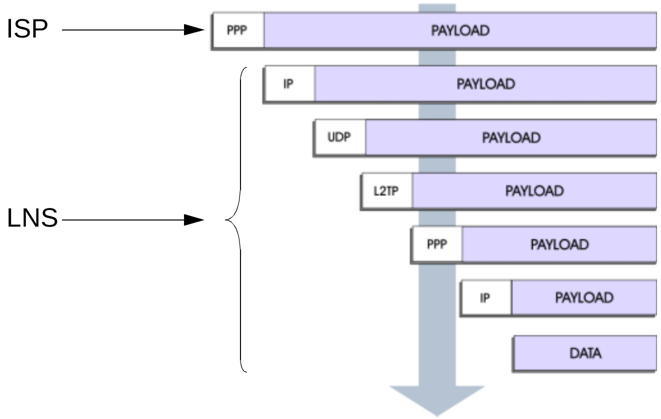
When a dialup user on an IP network sends data over an L2TP tunnel, the LAC encapsulates the IP packet within a series of layer 2 frames, layer 3 packets, and layer 4 segments. Assuming that the dialup user connects to the local ISP over a PPP link, the encapsulation proceeds as follows:



1. The data is placed in an IP payload.
2. The IP packet is encapsulated in a PPP frame.
3. The PPP frame is encapsulated in an L2TP frame.
4. The L2TP frame is encapsulated in a UDP segment.
5. The UDP segment is encapsulated in an IP packet.
6. The IP packet is encapsulated in a PPP frame to make the physical connection between the dialup user and the ISP.

Decapsulation

When the LAC initiates the PPP link to the ISP, the decapsulation and forwarding of the nested contents proceed as follows:



1. The ISP completes the PPP link and assigns the user’s computer an IP address.

   Inside the PPP payload is an IP packet.
2. The ISP removes the PPP header and forwards the IP packet to the LNS.
3. The LNS removes the IP header.

   Inside the IP payload is a UDP segment specifying port 1701, the port number reserved for L2TP.
4. The LNS removes the UDP header.

   Inside the UDP payload is an L2TP frame.
5. The LNS processes the L2TP frame, using the tunnel ID and call ID in the L2TP header to identify the specific L2TP tunnel. The LNS then removes the L2TP header.

   Inside the L2TP payload is a PPP frame.
6. The LNS processes the PPP frame, assigning the user’s computer a logical IP address.

   Inside the PPP payload is an IP packet.
7. The LNS routes the IP packet to its ultimate destination, where the IP header is removed and the data in the IP packet is extracted.

L2TP Parameters

The LNS uses L2TP to provide the PPP settings for a dial-up user that typically come from an ISP. These settings are as follows:

- IP address – The NetScreen device selects an address from a pool of IP addresses and assigns it to the dial-up user’s computer. The selection process operates cyclically through the IP address pool; that is, in a pool from 10.10.1.1 to 10.10.1.3, the addresses are selected in the following cycle: 10.10.1.1 – 10.10.1.2 – 10.10.1.3 – 10.10.1.1 – 10.10.1.2 …
- DNS primary and secondary server IP addresses – The NetScreen device provides these addresses for the dial-up user’s computer to use.
- WINS primary and secondary server IP addresses – The NetScreen device also provides these addresses for the dial-up user’s computer to use.

The LNS also authenticates the user through a user name and password. You can enter the user in the local database or in an external auth server (RADIUS, SecurID, or LDAP).

Note: *The RADIUS or SecurID server that you use for authenticating L2TP users can be the same server you use for network users, or it can be a different server.*

In addition, you can specify one of the following schemes for the PPP authentication:

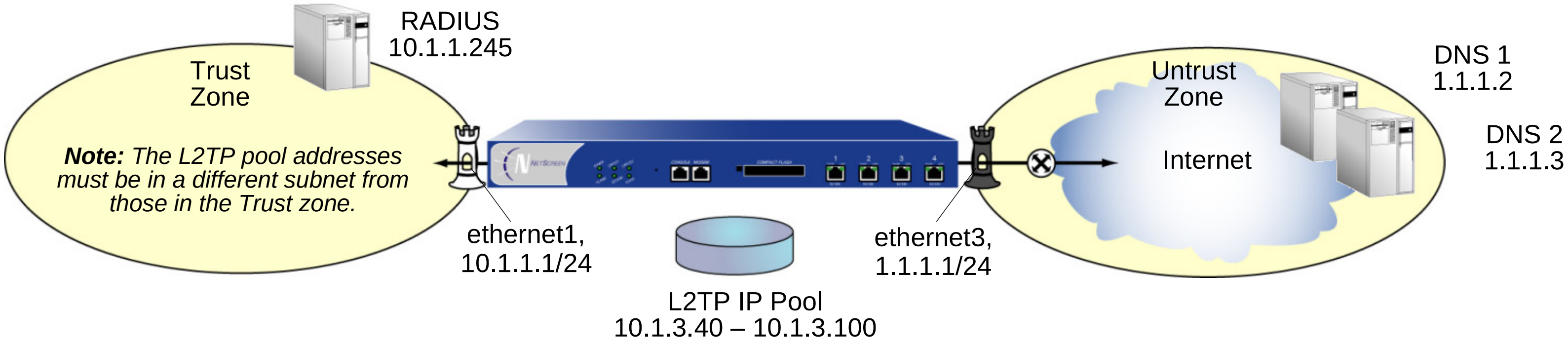
- Challenge Handshake Authentication Protocol (CHAP), in which the NetScreen device sends a challenge (encryption key) to the dial-up user after he or she makes a PPP link request, and the user encrypts his or her login name and password with the key. The local database and RADIUS servers support CHAP.
- Password Authentication Protocol (PAP), which sends the dial-up user’s password in the clear along with the PPP link request. The local database and RADIUS, SecurID, and LDAP servers support PAP.
- “ANY”, meaning that the NetScreen device negotiates CHAP, and then if that fails, PAP.

You can apply to dial-up users and dialup user groups the default L2TP parameters that you configure on the L2TP Default Configuration page (VPNs > L2TP > Default Settings) or with the **set l2tp default** command. You can also apply L2TP parameters that you configure specifically for L2TP users on the User Configuration page (Users > Users > Local > New) or with the **set user** *name_str* **remote-settings** command. The user-specific L2TP settings supersede the default L2TP settings.

Example: Configuring an IP Pool and L2TP Default Settings

In this example, you define an IP address pool with addresses ranging from 10.1.3.40 to 10.1.3.100. You specify DNS server IP addresses 1.1.1.2 (primary) and 1.1.1.3 (secondary). The NetScreen device performs PPP authentication using CHAP.

> ***Note:*** *You specify the auth server on a per-L2TP tunnel basis.*



WebUI

1. IP Pool

Objects > IP Pools > New: Enter the following, and then click **OK**:

IP Pool Name: Sutro

Start IP: 10.1.3.40

End IP: 10.1.3.100

2. Default L2TP Settings

VPNs > L2TP > Default Settings: Enter the following, and then click **Apply**:

IP Pool Name: Sutro

PPP Authentication: CHAP

DNS Primary Server IP: 1.1.1.2

DNS Secondary Server IP: 1.1.1.3

WINS Primary Server IP: 0.0.0.0

WINS Secondary Server IP: 0.0.0.0

CLI

1. IP Pool

```
set ippool sutro 10.1.3.40 10.1.3.100
```

2. Default L2TP Settings

```
set l2tp default ippool sutro
set l2tp default ppp-auth chap
set l2tp default dns1 1.1.1.2
set l2tp default dns2 1.1.1.3
save
```

L2TP AND L2TP-OVER-IPSEC

Although the dial-up user can be authenticated using CHAP or PAP, an L2TP tunnel is not encrypted, and therefore is not a true VPN tunnel. The purpose of L2TP is simply to permit the administrator of the local NetScreen device to assign IP addresses to remote dial-up users. These addresses can then be referenced in policies.

To encrypt an L2TP tunnel, you need to apply an encryption scheme to the L2TP tunnel. Because L2TP assumes that the network between the LAC and the LNS is IP, you can employ IPSec to provide encryption. This combination is called L2TP-over-IPSec. L2TP-over-IPSec requires setting up both an L2TP tunnel and an IPSec tunnel with the same endpoints, and then linking them together in a policy. L2TP-over-IPSec requires that the IPSec tunnel be in transport mode so that the tunnel endpoint addresses remain in the clear. (For information about transport mode and tunnel mode, see “Modes” on page 4.)

You can create an L2TP tunnel between a NetScreen device and a host running Windows 2000 if you change the Windows 2000 registry settings. (For instructions on how to change the registry, see the footnote on page 273.)

You can create an L2TP-over-IPSec tunnel between a NetScreen device and either of the following VPN clients:

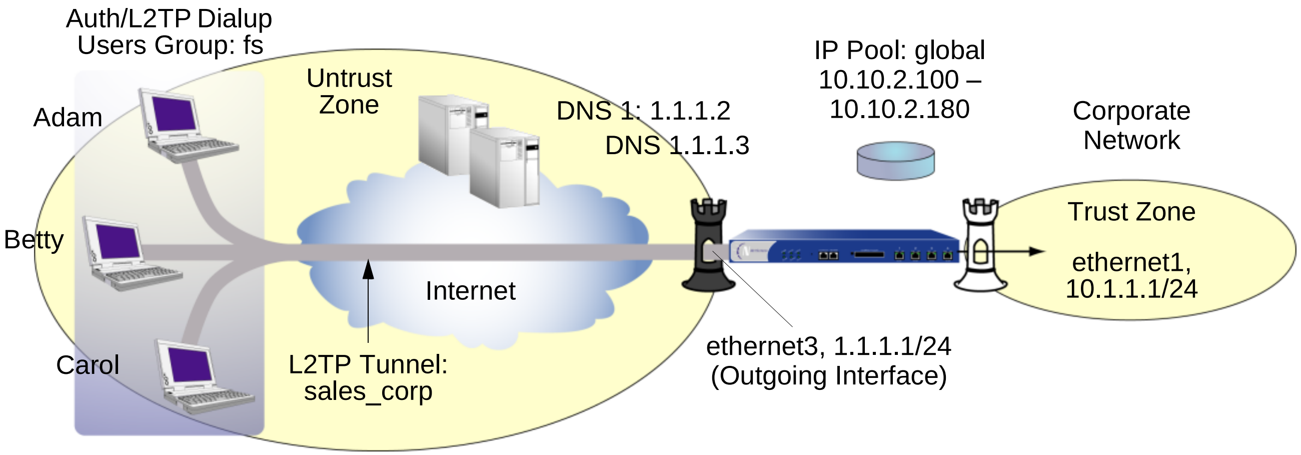
- A host running NetScreen-Remote on a Windows 2000 or Windows NT operating system
- A host running Windows 2000 (without NetScreen-Remote)

Example: Configuring L2TP

In this example, you create a dialup user group called “fs” (for “field-sales”) and configure an L2TP tunnel called “sales_corp,” using ethernet3 (Untrust zone) as the outgoing interface for the L2TP tunnel. The NetScreen device applies the following default L2TP tunnel settings to the dialup user group:

- The L2TP users are authenticated via the local database.
- PPP authentication uses CHAP.
- The range of addresses in the IP pool (named “global”) is from 10.10.2.100 to 10.10.2.180[2].
- The DNS servers are 1.1.1.2 (primary) and 1.1.1.3 (secondary)

Note: *An L2TP-only configuration is not secure. It is recommended only for debugging purposes.*



The remote L2TP clients are on Windows 2000 operating systems. For information on how to configure L2TP on the remote clients, refer to Windows 2000 documentation. Only the configuration for the NetScreen device end of the L2TP tunnel is provided below.

[2] The addresses in the L2TP IP pool must be in a different subnet than the addresses in the corporate network.

WebUI

1. L2TP Users

Objects > Users > Local > New: Enter the following, and then click **OK**:

User Name: Adam

Status: Enable

L2TP User: (select)

User Password: AJbioJ15

Confirm Password: AJbioJ15

Objects > Users > Local > New: Enter the following, and then click **OK**:

User Name: Betty

Status: Enable

L2TP User: (select)

User Password: BviPsoJ1

Confirm Password: BviPsoJ1

Objects > Users > Local > New: Enter the following, and then click **OK**:

User Name: Carol

Status: Enable

L2TP User: (select)

User Password: Cs10kdD3

Confirm Password: Cs10kdD3

2. L2TP User Group

Objects > User Groups > Local > New: Type **fs** in the Group Name field, do the following, and then click **OK**:

Select **Adam** and use the **<<** button to move him from the Available Members column to the Group Members column.

Select **Betty** and use the **<<** button to move her from the Available Members column to the Group Members column.

Select **Carol** and use the **<<** button to move her from the Available Members column to the Group Members column.

3. Default L2TP Settings

Objects > IP Pools > New: Enter the following, and then click **OK**:

IP Pool Name: global

Start IP: 10.10.2.100

End IP: 10.10.2.180

VPNs > L2TP > Default Settings: Enter the following, and then click **OK**:

IP Pool Name: global

PPP Authentication: CHAP

DNS Primary Server IP: 1.1.1.2

DNS Secondary Server IP: 1.1.1.3

WINS Primary Server IP: 0.0.0.0

WINS Secondary Server IP: 0.0.0.0

4. L2TP Tunnel

VPNs > L2TP > Tunnel > New: Enter the following, and then click **OK**:

Name: sales_corp

Use Custom Settings: (select)

Authentication Server: Local

Dialup Group: Local Dialup Group - fs

Outgoing Interface: ethernet3

Peer IP: 0.0.0.0[3]

Host Name (optional): Enter the name of the computer acting as the LAC[4].

Secret (optional): Enter a secret shared between the LAC and the LNS.

> ***Note:*** *To add a secret to the LAC for authenticating the L2TP tunnel, you must modify the Windows 2000 registry as follows:*
>
> *(1) Click **Start > Run**, and then type **regedit**. The Registry Editor opens.*
>
> *(2) Click **HKEY_LOCAL_MACHINE**.*
>
> *(3) Right-click **SYSTEM**, and then select **Find** from the pop-up menu that appears.*
>
> *(4) Type **ms_l2tpminiport**, and then click **Find Next**.*
>
> *(5) In the Edit menu, highlight **New**, and then select **String Value**.*
>
> *(6) Type **Password**.*
>
> *(7) Double-click **Password**. The Edit String dialog box appears.*
>
> *(8) Type the password in the Value data field. This must be the same as the word in the L2TP Tunnel Configuration Secret field on the NetScreen device.*
>
> *(9) Reboot the computer running Windows 2000.*
>
> *When using L2TP-over-IPSec, which is the Windows 2000 default, tunnel authentication is unnecessary; all L2TP messages are encrypted and authenticated inside IPSec.*

Keep Alive: 60[5]

[3] Because the peer’s ISP dynamically assigns it an IP address, enter **0.0.0.0** here.

[4] To find the name of a computer running Windows 2000, do the following: Click **Start > Settings > Control Panel > System**. The System Properties dialog box appears. Click the **Network Identification** tab, and see entry following **Full computer name**.

5. Policy

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Dial-Up VPN

Destination Address:

Address Book Entry: (select), Any

NAT: Off

Service: ANY

Action: Tunnel

Tunnel L2TP: sales_corp

Position at Top: (select)

CLI

1. Dialup Users

```
set user adam type l2tp
set user adam password AJbioJ15
unset user adam type auth[6]
set user betty type l2tp
set user betty password BviPsoJ1
unset user betty type auth
set user carol type l2tp
set user carol password Cs10kdD3
unset user carol type auth
```

[5] The Keep Alive value is the number of seconds of inactivity before the NetScreen device sends an L2TP hello signal to the LAC.

[6] Defining a password for a user automatically classifies the user as an auth user. Therefore, to define the user type strictly as L2TP, you must unset the auth user type.

2. L2TP User Group

```
set user-group fs location local
set user-group fs user adam
set user-group fs user betty
set user-group fs user carol
```

3. Default L2TP Settings

```
set ippool global 10.10.2.100 10.10.2.180
set l2tp default ippool global
set l2tp default auth server Local
set l2tp default ppp-auth chap
set l2tp default dns1 1.1.1.2
set l2tp default dns2 1.1.1.3
```

4. L2TP Tunnel

```
set l2tp sales_corp outgoing-interface ethernet3
set l2tp sales_corp auth server Local user-group fs
```

5. Policy

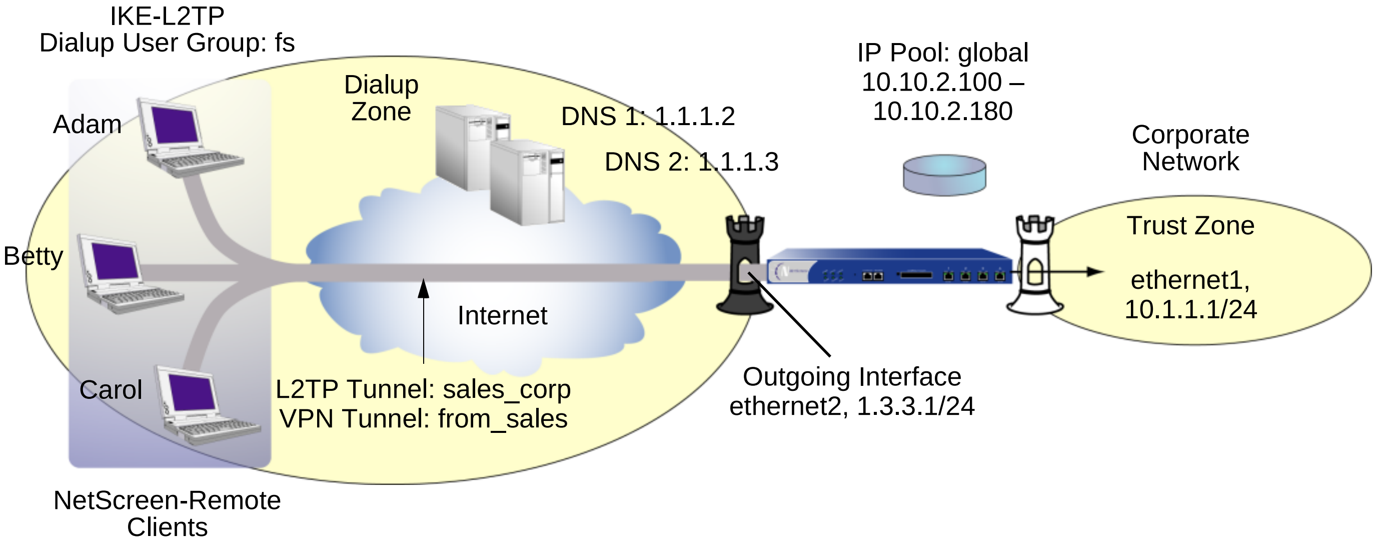
```
set policy top from untrust to trust “Dial-Up VPN” any any tunnel l2tp
    sales_corp
save
```

Example: Configuring L2TP-over-IPSec

This example uses the same L2TP tunnel created in the previous example (“Example: Configuring L2TP” on page 280). Additionally, you overlay an IPSec tunnel onto the L2TP tunnel to provide encryption. The IPSec tunnel negotiates Phase 1 in Aggressive Mode using a previously loaded RSA certificate, 3DES encryption and SHA-1 authentication. The certificate authority (CA) is Verisign. (For information on obtaining and loading certificates, see Chapter 2, “Public Key Cryptography” on page 15.)The Phase 2 negotiation uses the security level predefined as “Compatible” for Phase 2 proposals. The IPSec tunnel is in transport mode.

The predefined Trust zone and the user-defined Dialup zone are in the trust-vr routing domain. The interfaces for the Dialup and Trust zones are ethernet2 (1.3.3.1/24) and ethernet1 (10.1.1.1/24) respectively. The Trust zone is in NAT mode.

The dialup users Adam, Betty, and Carol use NetScreen-Remote clients on a Windows 2000 operating system[7]. The NetScreen-Remote configuration for dialup user Adam is also included below. (The NetScreen-Remote configuration for the other two dialup users is the same as that for Adam.)



[7] To configure an L2TP-over-IPSec tunnel for Windows 2000 (without the NetScreen-Remote), the Phase 1 negotiations must be in Main mode and the IKE ID type must be ASN1-DN.

WebUI

1. User-Defined Zone

Network > Zones > New: Enter the following, and then click **OK**:

Zone Name: Dialup

Virtual Router Name: trust-vr

Zone Type: Layer 3 (select)

Block Intra-Zone Traffic: (select)

TCP/IP Reassembly for ALG: (clear)

Note: *The Trust zone is preconfigured. You do not need to create it.*

2. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet2): Enter the following, and then click **OK**:

Zone Name: Dialup

Static IP: (select this option when present)

IP Address/Netmask: 1.3.3.1/24

3. IKE/L2TP Users

Objects > Users > Local > New: Enter the following, and then click **OK**:

User Name: Adam

Status: Enable

IKE User: (select)

Simple Identity: (select)[8]

IKE Identity: ajackson@abc.com

L2TP User: (select)

User Password: AJbioJ15

Confirm Password: AJbioJ15

Objects > Users > Local > New: Enter the following, and then click **OK**:

User Name: Betty

Status: Enable

IKE User: (select)

Simple Identity: (select)

IKE Identity: bdavis@abc.com

L2TP User: (select)

User Password: BviPsoJ1

Confirm Password: BviPsoJ1

[8] The IKE ID that you enter must be the same as the one that the NetScreen-Remote client sends, which is the e-mail address that appears in the certificate that the client uses for authentication.

Objects > Users > Local > New: Enter the following, and then click **OK**:

User Name: Carol

Status: Enable

IKE User: (select)

Simple Identity: (select)

IKE Identity: cburnet@abc.com

L2TP User: (select)

User Password: Cs10kdD3

Confirm Password: Cs10kdD3

4. IKE/L2TP User Group

Objects > User Groups > Local > New: Type **fs** in the Group Name field, do the following, and then click **OK**:

Select **Adam** and use the **<<** button to move him from the Available Members column to the Group Members column.

Select **Betty** and use the **<<** button to move her from the Available Members column to the Group Members column.

Select **Carol** and use the **<<** button to move her from the Available Members column to the Group Members column.

5. IP Pool

Objects > IP Pools > New: Enter the following, and then click **OK**:

IP Pool Name: global

Start IP: 10.10.2.100

End IP: 10.10.2.180

6. Default L2TP Settings

VPNs > L2TP > Default Settings: Enter the following, and then click **Apply**:

IP Pool Name: global

PPP Authentication: CHAP

DNS Primary Server IP: 1.1.1.2

DNS Secondary Server IP: 1.1.1.3

WINS Primary Server IP: 0.0.0.0

WINS Secondary Server IP: 0.0.0.0

7. L2TP Tunnel

VPNs > L2TP > Tunnel > New: Enter the following, and then click **OK**:

Name: sales_corp

Dialup Group: (select), Local Dialup Group - fs

Authentication Server: Local

Outgoing Interface: ethernet2

Peer IP: 0.0.0.0[9]

Host Name (optional): If you want to restrict the L2TP tunnel to a specific host, enter the name of the computer acting as the LAC[10].

Secret (optional): Enter a secret shared between the LAC and the LNS[11]

Note: *The host name and secret settings can usually be ignored. Only advanced users are recommended to use these settings.*

Keep Alive: 60[12]

[9] Because the IP address of the peer is dynamic, enter **0.0.0.0** here.

[10] To find the name of a computer running Windows 2000, do the following: Click **Start > Settings > Control Panel > System**. The System Properties dialog box appears. Click the **Network Identification** tab, and see entry following **Full computer name**.

[11] To add a secret to the LAC for authenticating the L2TP tunnel, you must modify the Windows 2000 registry. See the note in the previous example.

[12] The Keep Alive value is the number of seconds of inactivity before the NetScreen device sends an L2TP hello signal to the LAC.

8. VPN Tunnel

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: field

Security Level: Custom

Remote Gateway Type:

Dialup User Group: (select), Group: fs

Outgoing Interface: ethernet2

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: User Defined: Custom

Phase 1 Proposal: rsa-g2-3des-sha

Mode (Initiator): Aggressive[13]

Preferred Certificate (Optional):

Peer CA: Verisign

Peer Type: X509-SIG

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

Name: from_sales

Security Level: Compatible

Remote Gateway: Predefined: field

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Security Level: Compatible

Transport Mode: (select)

[13] Windows 2000 (without NetScreen-Remote) supports Main mode negotiations only.

9. Policy

Policies > (From: Dialup, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Dial-Up VPN

Destination Address:

Address Book Entry: (select), Any

Service: ANY

Action: Tunnel

Tunnel VPN: from_sales

Modify matching bidirectional VPN policy: (clear)

L2TP: sales_corp

Position at Top: (select)

CLI

1. User-Defined Zone

```
set zone name dialup
set zone dialup vrouter trust-vr
set zone dialup block
```

2. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet2 zone dialup
set interface ethernet2 ip 1.3.3.1/24
```

3. L2TP/IKE Users

```
set user adam type ike l2tp
set user adam password AJbioJ15
unset user adam type auth
set user adam ike-id u-fqdn ajackson@abc.com
set user betty type ike l2tp
set user betty password BviPsoJ1
unset user betty type auth
set user betty ike-id u-fqdn bdavis@abc.com
set user carol type ike l2tp
set user carol password Cs10kdD3
unset user carol type auth
set user carol ike-id u-fqdn cburnet@abc.com
```

4. IKE/L2TP User Group

```
set user-group fs location Local
set user-group fs user adam
set user-group fs user betty
set user-group fs user carol
```

5. IP Pool

```
set ippool global 10.10.2.100 10.10.2.180
```

6. Default L2TP Settings

```
set l2tp default ippool global
set l2tp default ppp-auth chap
set l2tp default dns1 1.1.1.2
set l2tp default dns2 1.1.1.3
```

7. L2TP Tunnel

```
set l2tp sales_corp outgoing-interface ethernet2
set l2tp sales_corp auth server Local user-group fs
```

8. VPN Tunnel

```
set ike gateway field dialup fs aggressive[14] outgoing-interface ethernet2
    proposal rsa-g2-3des-sha
set ike gateway field cert peer-ca1[15]
set ike gateway field cert peer-cert-type x509-sig
set vpn from_sales gateway field transport sec-level compatible
```

9. Policy

```
set policy top from dialup to trust “Dial-Up VPN” any any tunnel vpn from_sales
    l2tp sales_corp
save
```

[14] Windows 2000 (without NetScreen-Remote) supports Main mode negotiations only.

[15] The number 1 is the CA ID number. To discover the CA’s ID number, use the following command: **get pki x509 list ca-cert**.

NetScreen-Remote Security Policy Editor (Adam[16])

1. Click **Options > Secure > Specified Connections**.
2. Click **Add a new connection**, and type **AJ** next to the new connection icon that appears.
3. Configure the connection options:

   Connection Security: Secure

   Remote Party ID Type: IP Address

   IP Address: 1.3.3.1

   Protocol: UDP

   Port: L2TP

   Connect using Secure Gateway Tunnel: (clear)

4. Click the **PLUS** symbol, located to the left of the AJ icon, to expand the connection policy.
5. Click **My Identity**, and configure the following:

   Select the certificate with the e-mail address specified as the user’s IKE ID on the NetScreen device from the Select Certificate drop-down list

   ID Type: E-mail Address[17]

   Port: L2TP

6. Click the **Security Policy** icon, and select **Aggressive Mode**.
7. Click the **PLUS** symbol, located to the left of the Security Policy icon, and then the **PLUS** symbol to the left of Authentication (Phase 1) and Key Exchange (Phase 2) to expand the policy further.

[16] To configure L2TP-over-IPSec tunnels for Betty and Carol’s NetScreen-Remote clients, follow the same procedure as that provided here for Adam.

[17] The e-mail address from the certificate appears in the identifier field automatically.

8. Click **Authentication (Phase 1)** > **Proposal 1**: Select the following Encryption and Data Integrity Algorithms:

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

9. Click **Key Exchange (Phase 2)** > **Proposal 1**: Select the following IPSec Protocols:

   Encapsulation Protocol (ESP): (select)

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Encapsulation: Transport

10. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: Triple DES

    Hash Alg: MD5

    Encapsulation: Transport

11. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: SHA-1

    Encapsulation: Transport

12. Click **Key Exchange (Phase 2)** > **Create New Proposal**: Select the following IPSec Protocols:

    Encapsulation Protocol (ESP): (select)

    Encrypt Alg: DES

    Hash Alg: MD5

    Encapsulation: Transport

13. Click **Save**.
14. You also need to set up the network connection for your Windows 2000 operating system using the Network Connection Wizard.

    Note: *When configuring the Network Connection Wizard, you must enter a destination host name or IP address. Enter 1.3.3.1. Later, when initiating a connection and are prompted for a user name and password, enter adam, AJbioJ15. For more information, consult Microsoft Windows 2000 documentation.*

7

Advanced VPN Features

The material in this chapter covers the following more advanced uses of VPN technology:

- "IPSec NAT Traversal" on page 301
  - "Traversing a NAT Device" on page 302
  - "UDP Checksum" on page 303
  - "The Keepalive Frequency Value" on page 303
  - "IPSec NAT-Traversal and Initiator/Responder Symmetry" on page 304
- "VPN Monitoring" on page 307
  - "Rekey and Optimization Options" on page 307
  - "Source Interface and Destination Address" on page 308
  - "Policy Considerations" on page 310
  - "Configuring the VPN Monitoring Feature" on page 310
  - "Security Consideration for a Route-Based VPN Design" on page 323
  - "SNMP VPN Monitoring Objects and Traps" on page 325
- "Multiple Tunnels per Tunnel Interface" on page 326
  - "Route-to-Tunnel Mapping" on page 327
  - "Remote Peers' Addresses" on page 328
  - "Manual and Automatic Table Entries" on page 330
- "Redundant VPN Gateways" on page 382
  - "VPN Groups" on page 383
  - "Monitoring Mechanisms" on page 384
  - "TCP SYN-Flag Checking" on page 388

- “Back-to-Back VPNs” on page 401
  - “Example: Back-to-Back VPNs” on page 402
- “Hub-and-Spoke VPNs” on page 412
  - “Example: Hub-and-Spoke VPNs” on page 413

IPSec NAT Traversal

Network Address Translation (NAT) and Network Address Port Translation (NAPT) are Internet standards that allow a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. NAT devices generate these external addresses from predetermined pools of IP addresses.

When setting up an IPSec tunnel, the presence of a NAT device along the data path has no effect on Phase 1 and Phase 2 IKE negotiations, which always encapsulate IKE packets within User Datagram Protocol (UDP) packets. However, after the Phase 2 negotiations are completed, performing NAT on the IPSec packets causes the tunnel to fail. Of the many reasons why NAT causes disruption to IPSec[1], one reason is that, for the Encapsulating Security Protocol (ESP), NAT devices cannot discern the location of the Layer 4 header (because it is encrypted) for port translation. For the Authentication Header (AH) protocol, NAT devices can modify the port number, but the authentication check, which includes the entire IPSec packet, fails.

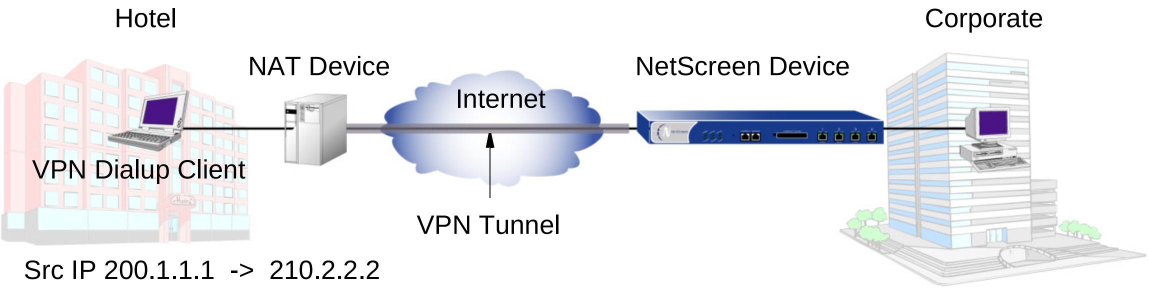
To solve this problem, NetScreen devices (with ScreenOS 3.0.0 or later) and the NetScreen-Remote client (version 6.0 or later) can apply the NAT-traversal (NAT-T) feature. NAT-T adds a layer of UDP encapsulation after detecting one or more NAT devices along the data path during Phase 1 exchanges.

Note: *NetScreen does not support NAT-T for Manual Key tunnels. NetScreen only supports NAT-T for AutoKey IKE tunnels using the Encapsulating Security Protocol (ESP).*

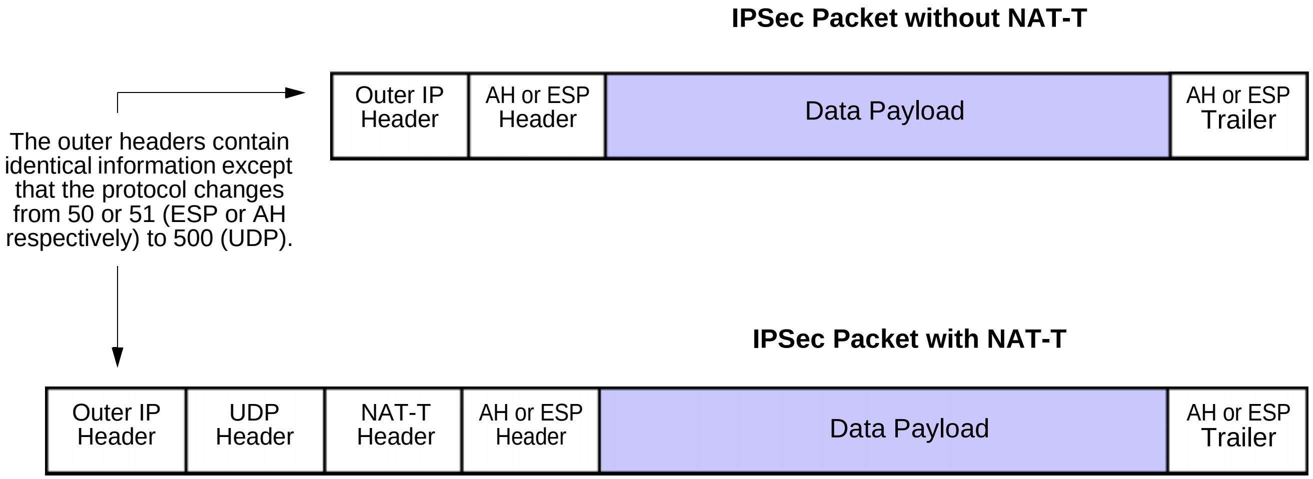
[1] For a list of IPSec/NAT incompatibilities, see *draft-ietf-ipsec-nat-regts-00.txt* by Bernard Aboba.

Traversing a NAT Device

In the following illustration, a NAT device at the perimeter of a hotel LAN receives a packet from a VPN dialup client with IP address 200.1.1.1, assigned by its ISP. For all outbound traffic, the NAT device replaces the original source IP address in the outer header with a new address 210.2.2.2. During Phase 1 negotiations, the VPN client and the NetScreen device detect that both VPN participants support NAT-T, that a NAT device is present along the data path, and that it is located in front of the VPN client.



Encapsulating the IPSec packets within UDP packets—which both the VPN client and the NetScreen device do—solves the problem of the authentication check failure. The NAT device processes them as UDP packets, changing the source port in the UDP header and leaving the SPI in the AH or ESP header unmodified. The VPN participants strip off the UDP layer and process the IPSec packets, which pass the authentication check because none of the authenticated content has been changed.



Note: *When NAT-T is enabled, the NetScreen device applies it only when necessary; that is, when it detects a NAT device between the remote host and the NetScreen device.*

UDP Checksum

All UDP packets contain a UDP checksum, a calculated value that ensures UDP packets are free of transmission errors. A NetScreen device does not require use of the UDP checksum for NAT-T, so the WebUI and CLI present the checksum as an optional setting. Even so, some NAT devices require a checksum, so you might have to enable this setting.

The Keepalive Frequency Value

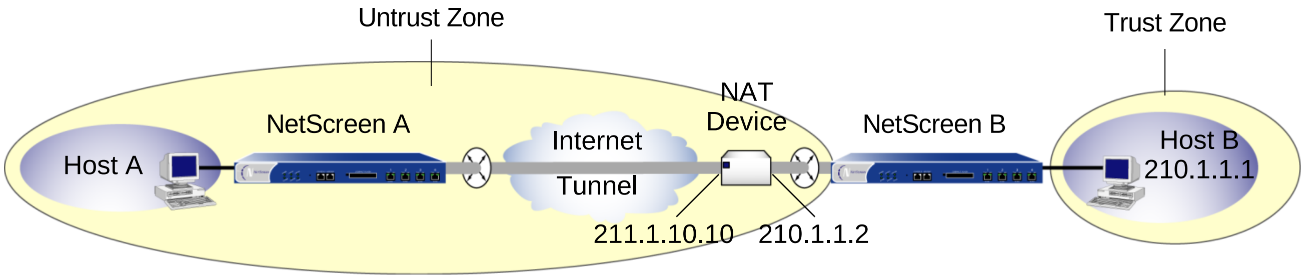
When a NAT device assigns an IP address to a host, the NAT device determines how long the new address remains valid when no traffic occurs. For example, a NAT device might invalidate any generated IP address that remains unused for 20 seconds. Therefore, it is usually necessary for the IPSec participants to send periodic keepalive packets—empty UDP packets—through the NAT device, so that the NAT mapping does not change until the Phase 1 and Phase 2 SAs expire.

Note: *NAT devices have different session timeout intervals, depending on the manufacturer and model. It is important to determine what the interval is for the NAT device, and to set the keepalive frequency value below that.*

IPSec NAT-Traversal and Initiator/Responder Symmetry

When two NetScreen devices establish a tunnel in the absence of a NAT device, either device can serve as initiator or responder. However, if either host resides behind a NAT device, such initiator/responder symmetry might be impossible. This happens whenever the NAT device generates IP addresses dynamically.

Note: *Security zones depicted below are from the perspective of NetScreen B.*



In the above illustration, NetScreen B resides in a subnet located behind a NAT device. If the NAT device generates the new IP address (210.1.1.1) dynamically from a pool of IP addresses, NetScreen A cannot unambiguously identify NetScreen B. Therefore, NetScreen A cannot successfully initiate a tunnel with NetScreen B. NetScreen A must be the responder, NetScreen B must be the initiator, and they must perform Phase 1 negotiations in Aggressive mode.

However, if the NAT device generates the new IP address using a mapped IP (MIP) address, or some other one-to-one addressing method, NetScreen A can unambiguously identify NetScreen B. Consequently, either NetScreen A or NetScreen B can be the initiator, and both can use Main mode or Aggressive mode for Phase 1.

Note: *If you enable NAT-T on a NetScreen device acting as the responder and configure it to perform IKE negotiations in Main mode, then that device and all its peers of the following types that are configured on the same outgoing interface must use the same Phase 1 proposals presented in the same order as each other:*

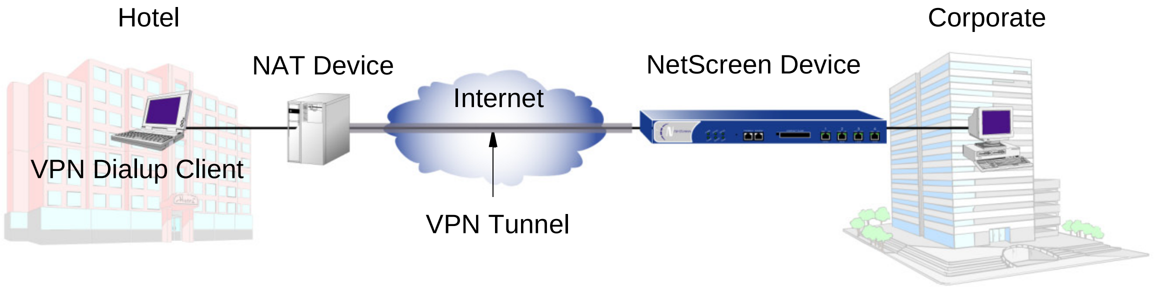
- *Dynamic peer (peers with dynamically assigned IP addresses)*
- *Dialup VPN users*
- *Peers with static IP addresses behind a NAT device*

Because it is not possible to know the identity of a peer when negotiating Phase 1 in Main mode until the last two messages, the Phase 1 proposals must all be the same so that IKE negotiations can proceed.

The NetScreen device automatically checks that all Phase 1 proposals are the same and in the same order when you configure IKE in Main mode to one of the above peer types on the same outgoing interface. If the proposals are different, the NetScreen device generates an error message.

Example: Enabling NAT-Traversal

In the following example, a NAT device at the perimeter of a hotel LAN assigns an address to the VPN dialup client used by Michael Smith, a salesman attending a convention. For Michael Smith to reach the corporate LAN via a dialup VPN tunnel, you must enable NAT-T for the remote gateway “msmith,” configured on the NetScreen device, and for the remote gateway configured on the VPN dialup client. You also enable the NetScreen device to include a UDP checksum in its transmissions, and you set the keepalive frequency to 8 seconds.



WebUI

VPNs > AutoKey Advanced > Gateway > New: Enter the necessary parameters for the new tunnel gateway as described in Chapter 4, "Site-to-Site VPNs" on page 69 or Chapter 5, "Dialup VPNs" on page 199, enter the following, and then click **OK**:

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Enable Nat-Traversal: (select)

UDP Checksum: Enable

Keepalive Frequency: 8

Note: *The NetScreen device automatically enables NAT traversal for dial-up VPNs.*

CLI

```
set ike gateway msmith nat-traversal
set ike gateway msmith nat-traversal enable-udp-checksum
set ike gateway msmith nat-traversal keepalive-frequency 8
save
```

VPN Monitoring

When you enable VPN monitoring for a specific tunnel, the NetScreen device sends ICMP echo requests (or "pings") through the tunnel at specified intervals (configurable in seconds) to monitor network connectivity through the tunnel.[2] If the ping activity indicates that the VPN monitoring status has changed, the NetScreen device triggers one of the following Simple Network Management Protocol (SNMP) traps:

- **Up to Down:** This trap occurs when the state of VPN monitoring for the tunnel is up, but a specified consecutive number of ICMP echo requests does not elicit a reply and there is no other incoming VPN traffic.[3] Then the state changes to down.
- **Down to Up:** When the state of VPN monitoring for the tunnel is down, but the ICMP echo request elicits a single response, then the state changes to up. The down-to-up trap occurs only if you have disabled the rekey option and the Phase 2 SA is still active when an ICMP echo request elicits a reply through the tunnel.

Note: *For more information about the SNMP data that VPN monitoring provides, see "SNMP VPN Monitoring Objects and Traps" on page 325.*

Rekey and Optimization Options

If you enable the rekey option, the NetScreen device starts sending ICMP echo requests immediately upon completion of the tunnel configuration and continues to send them indefinitely. The echo requests trigger an attempt to initiate IKE negotiations to establish a VPN tunnel until the state of VPN monitoring for the tunnel is up. The NetScreen device then uses the pings for VPN monitoring purposes. If the state of VPN monitoring for the tunnel changes from up to down, the NetScreen device deactivates its Phase 2 security association (SA) for that peer. The NetScreen device continues to send echo requests to its peer at defined intervals, triggering attempts to reinitiate IKE Phase 2 negotiations—and Phase 1 negotiations, if necessary—until it succeeds. At that point, the NetScreen device reactivates the Phase 2 SA, generates a new key, and reestablishes the tunnel. A message appears in the event log stating that a successful rekey operation has occurred[4].

[2] To change the ping interval, you can use the following CLI command: **set vpnmonitor interval** *number*. The default is 10 seconds.

[3] To change the threshold for the number of consecutive unsuccessful ICMP echo requests, you can use the following CLI command: **set vpnmonitor threshold** *number*. The default is 10 consecutive requests.

[4] If a NetScreen device is a DHCP client, a DHCP update to a different address causes IKE to rekey. However, a DHCP update to the same address does not provoke the IKE rekey operation.

You can use the rekey option to ensure that an AutoKey IKE tunnel is always up, perhaps to monitor devices at the remote site or to allow dynamic routing protocols to learn routes at a remote site and transmit messages through the tunnel. Another use to which you can apply VPN monitoring with the rekey option is for automatic population of the next-hop tunnel binding table (NHTB table) and the route table when multiple VPN tunnels are bound to a single tunnel interface. For an example of this last use, see "Multiple Tunnels per Tunnel Interface" on page 326.

If you disable the rekey option, the NetScreen device performs VPN monitoring only when the tunnel is active with user-generated traffic.

By default, VPN monitoring optimization is disabled. If you enable it (**set vpn** *name* **monitor optimized**), the VPN monitoring behavior changes as follows:

- The NetScreen device considers incoming traffic through the VPN tunnel to be the equivalent of ICMP echo replies. Accepting incoming traffic as a substitute for ICMP echo replies can reduce false alarms that might occur when traffic through the tunnel is heavy and the echo replies do not get through.
- If there is both incoming and outgoing traffic through the VPN tunnel, the NetScreen device suppresses VPN monitoring pings altogether. Doing so can help reduce network traffic.

Although VPN monitoring optimization offers some benefits, be aware that VPN monitoring can no longer provide accurate SNMP statistics, such as VPN network delay time, when the optimization option is active. Also, if you are using VPN monitoring to track the availability of a particular destination IP address at the remote end of a tunnel, the optimization feature can produce misleading results.

Source Interface and Destination Address

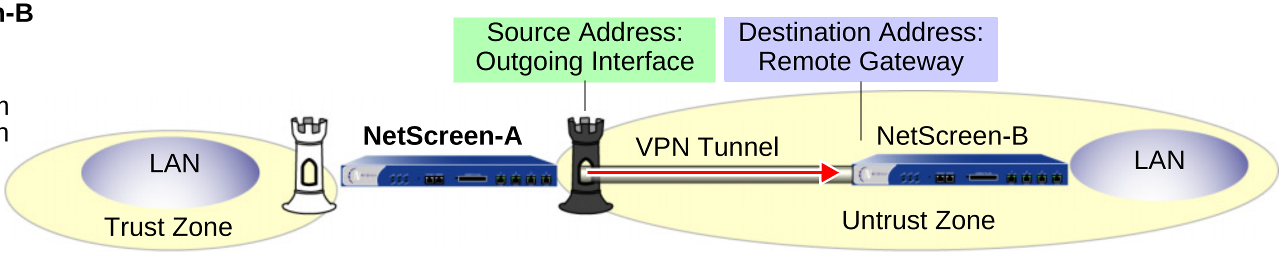
By default, the VPN monitoring feature uses the IP address of the local outgoing interface as the source address and the IP address of the remote gateway as the destination address. If the remote peer is a VPN dialup client—such as the NetScreen-Remote—that has an internal IP address, the NetScreen device automatically detects its internal address and uses that as the destination. The VPN client can be an XAuth user with an assigned internal IP address, or a dialup VPN user or a member of a dialup VPN group with an internal IP address. You can also specify the use of other source and destination IP addresses for VPN monitoring—mainly to provide support for VPN monitoring when the other end of a VPN tunnel is not a NetScreen device.

Because VPN monitoring operates independently at the local and remote sites, the source address configured on the device at one end of a tunnel does not have to be the destination address configured on the device at the other end. In fact, you can enable VPN monitoring at both ends of a tunnel or only at one end.

NetScreen-A –> NetScreen-B

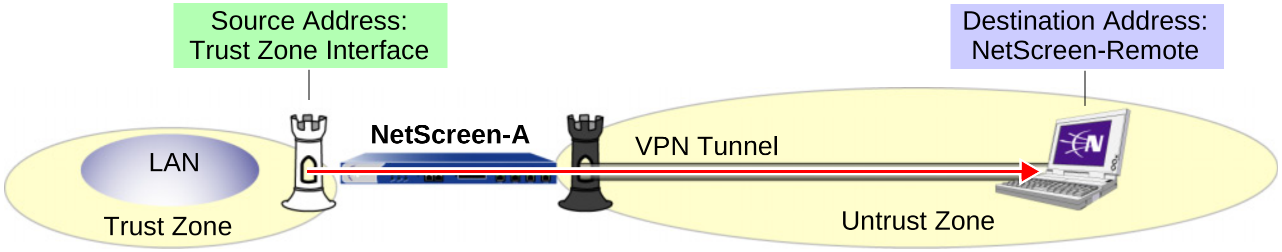
NetScreen-A pings from its outgoing interface to the remote gateway; that is, from the Untrust zone interface on NetScreen-A to the Untrust zone interface on NetScreen-B.

(Default Behavior)



NetScreen-A –> NetScreen-Remote

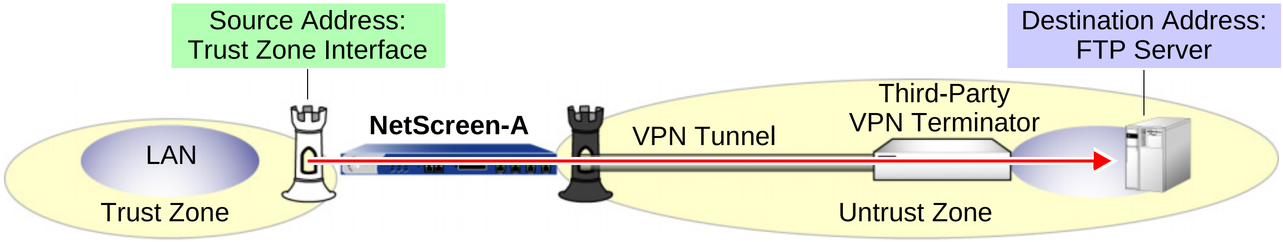
NetScreen-A pings from its Trust zone interface to the NetScreen-Remote. The NetScreen-Remote requires a policy permitting inbound ICMP traffic from an address beyond the remote gateway; that is, from beyond the Untrust zone interface of NetScreen-A.



Note: *NetScreen-A requires a policy permitting ping traffic from the Trust to Untrust zones.*

NetScreen-A –> Third-Party VPN Terminator

NetScreen-A pings from its Trust zone interface to a device beyond the remote gateway. This might be necessary if the remote peer does not respond to pings but can support policies permitting inbound ping traffic.



Note: *NetScreen-A requires a policy permitting ping traffic from the Trust to Untrust zones.*

Note: *If the other end of a tunnel is the NetScreen-Remote VPN client that receives its address through XAuth, then the NetScreen device, by default, uses the XAuth-assigned IP address as the destination for VPN monitoring. For information about XAuth, see "XAuth Users and User Groups" on page* ***2*** *-436.*

Policy Considerations

You must create a policy on the sending device to permit pings from the zone containing the source interface to pass through the VPN tunnel to the zone containing the destination address if:

- The source interface is in a different zone from the destination address.
- The source interface is in the same zone as the destination address, and intrazone blocking is enabled.

Likewise, you must create a policy on the receiving device to permit pings from the zone containing the source address to pass through the VPN tunnel to the zone containing the destination address if:

- The destination address is in a different zone from the source address.
- The destination address is in the same zone as the source address, and intrazone blocking is enabled.

Note: *If the receiving device is a third-party product that does not respond to the ICMP echo requests, change the destination to an internal host in the remote peer's LAN that does respond. The remote peer's firewall must have a policy permitting the ICMP echo requests to pass through it.*

Configuring the VPN Monitoring Feature

To enable VPN monitoring, do the following:

WebUI

VPNs > AutoKey IKE > New: Configure the VPN, click **Advanced**, enter the following, click **Return** to go back to the basic VPN configuration page, and then click **OK**:

VPN Monitor: Select to enable VPN monitoring of this VPN tunnel.

Source Interface: Choose an interface from the drop-down list. If you choose "default", the NetScreen device uses the outgoing interface.

Destination IP: Enter a destination IP address. If you do not enter anything, the NetScreen device uses the remote gateway IP address.

Rekey: Select this option if you want the NetScreen device to attempt IKE Phase 2 negotiations—and IKE Phase 1 negotiations if necessary—if the tunnel status changes from up to down. When you select this option, the

NetScreen device attempts IKE negotiations to set up the tunnel and begin VPN monitoring immediately after you finish configuring the tunnel.

Clear this option if you do not want the NetScreen device to attempt IKE negotiations if the tunnel status changes from up to down. When the rekey option is disabled, VPN monitoring begins after user-generated traffic has triggered IKE negotiations and stops when the tunnel status changes from up to down.

(Or)

VPNs > Manual Key > New: Configure the VPN, click **Advanced**, enter the following, click **Return** to go back to the basic VPN configuration page, and then click **OK**:

VPN Monitor: Select to enable VPN monitoring of this VPN tunnel.

Source Interface: Choose an interface from the drop-down list. If you choose "default", the NetScreen device uses the outgoing interface.

Destination IP: Enter a destination IP address. If you do not enter anything, the NetScreen device uses the remote gateway IP address.

CLI

```
set vpnmonitor frequency number[5]
set vpnmonitor threshold number[6]
set vpn name_str monitor [ source-interface interface[7] [ destination-ip
    ip_addr[8] ] ] [optimized] [ rekey[9] ]
save
```

[5] The VPN monitoring frequency is in seconds. The default setting is 10-second intervals.

[6] The VPN monitoring threshold number is the consecutive number of successful or unsuccessful ICMP echo requests that determines whether the remote gateway is reachable through the VPN tunnel or not. The default threshold is 10 consecutive successful or 10 consecutive unsuccessful ICMP echo requests.

[7] If you do not choose a source interface, the NetScreen device uses the outgoing interface as the default.

[8] If you do not choose a destination IP address, the NetScreen device uses the IP address for the remote gateway.

[9] The rekey option is not available for Manual Key VPN tunnels.

Example: Specifying Source and Destination Addresses for VPN Monitoring

In this example, you configure an AutoKey IKE VPN tunnel between two NetScreen devices (NetScreen-A and NetScreen-B). On device A, you set up VPN monitoring from its Trust zone interface (ethernet1) to the Trust zone interface (10.2.1.1/24) on NetScreen-B. On the NetScreen-B, you set up VPN monitoring from its Trust zone interface (ethernet1) to a corporate intranet server (10.1.1.5) behind NetScreen-A.

NetScreen-A	NetScreen-B
Zones and Interfaces	
• ethernet1 - Zone: Trust - IP address: 10.1.1.1/24 - Interface mode: NAT	• ethernet1 - Zone: Trust - IP address: 10.2.1.1/24 - Interface mode: NAT
• ethernet3 - Zone: Untrust - IP address: 1.1.1.1/24	• ethernet3 - Zone: Untrust - IP address: 2.2.2.2/24
Route-Based AutoKey IKE Tunnel Parameters	
• Phase 1 - Gateway name: gw1 - Gateway static IP address: 2.2.2.2 - Security level: Compatible[*] - Preshared Key: Ti82g4aX - Outgoing interface: ethernet3 - Mode: Main	• Phase 1 - Gateway name: gw1 - Gateway static IP address: 1.1.1.1 - Proposals: Compatible - Preshared Key: Ti82g4aX - Outgoing interface: ethernet3 - Mode: Main
• Phase 2 - VPN tunnel name: vpn1 - Security level: Compatible[†] - VPN Monitoring: src = ethernet1; dst = 10.2.1.1 - Bound to interface: tunnel.1	• Phase 2 - VPN tunnel name: vpn1 - Security level: Compatible - VPN Monitoring: src = ethernet1; dst = 10.1.1.5 - Bound to interface: tunnel.1

[*] A Phase 1 security level of Compatible includes the following proposals: pre-g2-3des-sha, pre-g2-3des-md5, pre-g2-des-sha, and pre-g2-des-md5.

[†] A Phase 1 security level of Compatible includes the following proposals: nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, and nopfs-esp-des-md5.

NetScreen-A	NetScreen-B
Routes	
To 0.0.0.0/0, use ethernet3, gateway 1.1.1.250	To 0.0.0.0/0, use ethernet3, gateway 2.2.2.250
To 10.2.1.0/0, use tunnel.1, no gateway	To 10.1.1.0/0, use tunnel.1, no gateway

Because both devices ping from an interface in their Trust zone to an address in their Untrust zone, the admins at both ends of the VPN tunnel must define policies permitting pings to pass from zone to zone.

Note: *Because both VPN terminators are NetScreen devices in this example, you can use the default source and destination addresses for VPN monitoring. The use of other options is included purely to illustrate how you can configure a NetScreen device to use them.*

WebUI (NetScreen-A)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Enter the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Tunnel IF New: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Trust (trust-vr)

Unnumbered: (select)

Interface: ethernet1(trust-vr)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Remote_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.2.1.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway:

Create a Simple Gateway: (select)

Gateway Name: gw1

Type:

Static IP: (select), Address/Hostname: 2.2.2.2

Preshared Key: Ti82g4aX

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 10.1.1.0/24

Remote IP / Netmask: 10.2.1.0/24

Service: ANY

VPN Monitor: (select)

Source Interface: ethernet1

Destination IP: 10.2.1.1

Rekey: (clear)

4. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.2.1.0/24

Gateway: (select)

Interface: Tunnel.1

Gateway IP Address: 0.0.0.0

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Remote_LAN

Service: ANY

Action: Permit

Position at Top: (select)

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Remote_LAN

Destination Address:

Address Book Entry: (select), Trust_LAN

Service: Any

Action: Permit

Position at Top: (select)

WebUI (NetScreen-B)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.2.1.1/24

Enter the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > Tunnel IF New: Enter the following, and then click **OK** :

Tunnel Interface Name: tunnel.1

Zone (VR): Trust (trust-vr)

Unnumbered: (select)

Interface: ethernet1(trust-vr)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.2.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Remote_LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway:

Create a Simple Gateway: (select)

Gateway Name: gw1

Type:

Static IP: (select), Address/Hostname: 1.1.1.1

Preshared Key: Ti82g4aX

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 10.2.1.0/24

Remote IP / Netmask: 10.1.1.0/24

Service: ANY

VPN Monitor: (select)

Source Interface: ethernet1

Destination IP: 10.1.1.5

Rekey: (clear)

4. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.1.1.0/24

Gateway: (select)

Interface: Tunnel.1

Gateway IP Address: 0.0.0.0

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Trust_LAN

Destination Address:

Address Book Entry: (select), Remote_LAN

Service: ANY

Action: Permit

Position at Top: (select)

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Remote_LAN

Destination Address:

Address Book Entry: (select), Trust_LAN

Service: Any

Action: Permit

Position at Top: (select)

CLI (NetScreen-A)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
```

2. Addresses

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Remote_LAN 10.2.1.0/24
```

3. VPN

```
set ike gateway gw1 address 2.2.2.2 main outgoing-interface ethernet3 preshare
    Ti82g4aX sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.1.0/24 any
set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.2.1.1
```

4. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.1.0/24 interface tunnel.1
```

5. Policies

```
set policy top from trust to untrust Trust_LAN Remote_LAN any permit
set policy top from untrust to trust Remote_LAN Trust_LAN any permit
save
```

CLI (NetScreen-B)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
```

2. Addresses

```
set address trust Trust_LAN 10.2.1.0/24
set address untrust Remote_LAN 10.1.1.0/24
```

3. VPN

```
set ike gateway gw1 address 1.1.1.1 main outgoing-interface ethernet3 preshare
    Ti82g4aX sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.2.1.0/24 remote-ip 10.1.1.0/24 any
set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.1.1.5
```

4. Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
```

5. Policies

```
set policy top from trust to untrust Trust_LAN Remote_LAN any permit
set policy top from untrust to trust Remote_LAN Trust_LAN any permit
save
```

Security Consideration for a Route-Based VPN Design

When using VPN monitoring with a route-based VPN tunnel configuration, the state of a tunnel might change from up to down. When this occurs, all route table entries referencing that interface change to inactive. Then, when the NetScreen device does a route lookup for traffic originally intended to be encrypted and sent through a VPN tunnel bound to that tunnel interface, it bypasses the route referencing the tunnel interface and searches for a route with the next longest match. The route that it finds might be the default route. Using this route, the NetScreen device would then send the traffic unencrypted out through a non-tunnel interface to the public WAN.

To avoid rerouting traffic originally intended for a tunnel interface to a non-tunnel interface, you can configure the NetScreen device to drop such traffic instead of sending it out unencrypted. To accomplish this, use either of the following work-arounds:

- Decoy Tunnel Interface

  1. Create a second tunnel interface, but do not bind it to a VPN tunnel. Instead, bind it to a tunnel zone that is in the same virtual routing domain as the first tunnel interface[10].
  2. Define a second route to the same destination using this second tunnel interface, and assign it a high metric.

     Then, when the state of the functioning tunnel interface changes from up to down and the route table entry referencing that interface becomes inactive, all subsequent route lookups find this second route to the nonfunctioning tunnel interface. The NetScreen device forwards traffic to the second tunnel interface and because it is not bound to a VPN tunnel, the device drops the traffic.

[10] If a tunnel interface is bound to a tunnel zone, its status is always up.

- Virtual Router for Tunnel Interfaces

1. Create a separate virtual router to use for all routes pointing to tunnel interfaces and name it, for example, “VR-VPN”.
2. Create a security zone—named, for example, “VPN zone”—and bind it to VR-VPN.
3. Bind all tunnel interfaces to the VPN zone, and also put all addresses for remote sites that you want to reach through VPN tunnels in this zone.
4. Configure static routes in all other virtual routers to VR-VPN for traffic that you want encrypted and sent through the tunnels. If necessary, define static routes for decrypted traffic from VR-VPN to the other virtual routers. Such routes are necessary to allow inbound VPN traffic through the tunnel if it is initiated from the remote site.

   If the state of a tunnel interface changes from up to down, the NetScreen device still forwards traffic to VR-VPN, where—because the state of the route to that interface is now inactive and there are no other matching routes—the NetScreen device drops the traffic.

SNMP VPN Monitoring Objects and Traps

ScreenOS provides the ability to determine the status and condition of active VPNs through the use of Simple Network Management Protocol (SNMP) VPN monitoring objects and traps. The VPN monitoring MIB notes whether each ICMP echo request elicits a reply, a running average of successful replies, the latency of the reply, and the average latency over the last 30 attempts.

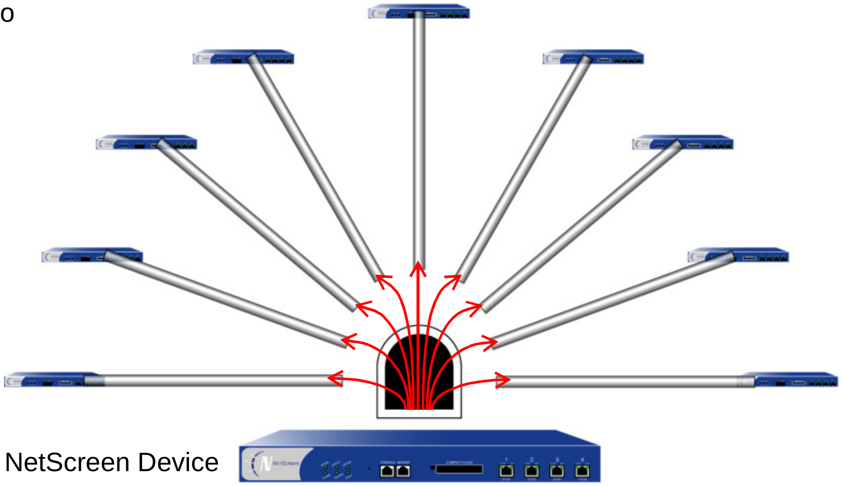
Note: *To enable your SNMP manager application to recognize the VPN monitoring MIBs, you must import the NetScreen-specific MIB extension files into the application. You can find the MIB extension files on the NetScreen documentation CD that shipped with your NetScreen device.*

By enabling the VPN monitoring feature on an AutoKey IKE or Manual Key VPN tunnel, the NetScreen device activates its SNMP VPN monitoring objects, which include data on the following:

- The total number of active VPN sessions
- The time each session started
- The Security Association (SA) elements for each session:
  - ESP encryption (DES or 3DES) and authentication algorithm (MD5 or SHA-1) types
  - AH algorithm type (MD5 or SHA-1)
  - Key exchange protocol (AutoKey IKE or Manual Key)
  - Phase 1 authentication method (Preshared Key or certificates)
  - VPN type (dialup or peer-to-peer)
  - Peer and local gateway IP addresses
  - Peer and local gateway IDs
  - Security Parameter Index (SPI) numbers
- Session status parameters
  - VPN monitoring status (up or down)
  - Tunnel status (up or down)
  - Phase 1 and 2 status (inactive or active)
  - Phase 1 and 2 lifetime (time in seconds before rekeying; Phase 2 lifetime is also reported in remaining bytes before rekeying)

Multiple Tunnels per Tunnel Interface

You can bind multiple IPSec VPN tunnels to a single tunnel interface. To link a specific destination to one of a number of VPN tunnels bound to the same tunnel interface, the NetScreen device uses two tables: the route table and the next-hop tunnel binding (NHTB). The NetScreen device maps the next-hop gateway IP address specified in the route table entry to a particular VPN tunnel specified in the NHTB table. With this technique, a single tunnel interface can support many VPN tunnels. (See "Route-to-Tunnel Mapping" on page 327.)



Route-based VPN tunnels to multiple remote peers.

All tunnels share the same tunnel interface.

Local NetScreen Device

The NetScreen device can sort VPN traffic sent through a single tunnel interface to as many VPN tunnels as the route table or VPN tunnel capacity—whichever is lower—can support.

The maximum number of VPN tunnels is not limited by the number of tunnel interfaces that you can create, but by either route table capacity or the maximum number of dedicated VPN tunnels allowed—whichever is lower. For instance, if your NetScreen device supports 4000 routes and 1000 dedicated VPN tunnels, you can create 1000 VPN tunnels and bind them to a single tunnel interface. If your NetScreen device supports 8192 routes and 10,000 dedicated VPN tunnels, then you can create over 8000 VPN tunnels and bind them to a single tunnel interface[11]. To see the maximum route and tunnel capacities for your NetScreen device, refer to the relevant product data sheet.

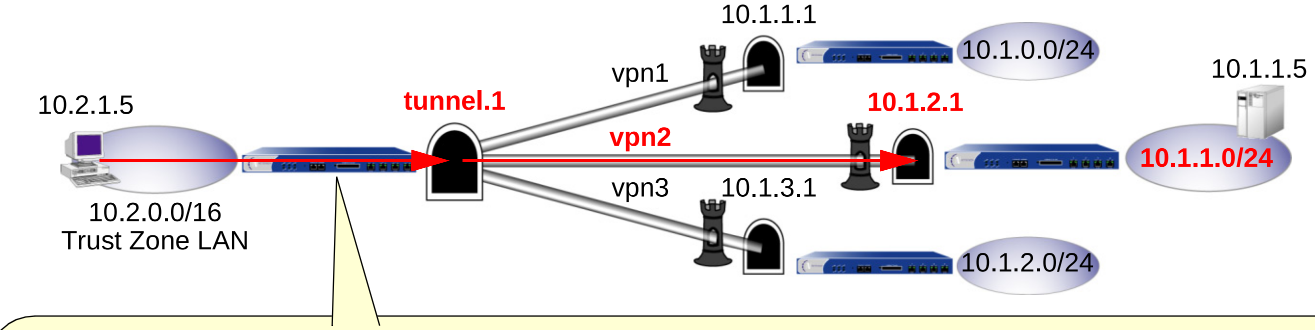
[11] If route table capacity is the limiting factor, you must subtract the routes automatically generated by security zone interfaces and any other static routes—such as the route to the default gateway—that you might need to define from the total available for route-based VPN tunnels.

Route-to-Tunnel Mapping

To sort traffic among multiple VPN tunnels bound to the same tunnel interface, the NetScreen device maps the next-hop gateway IP address specified in the route to a particular VPN tunnel name. The mapping of entries in the route table to entries in the NHTB table is shown below. In the following illustration, the local NetScreen device routes traffic sent from 10.2.1.5 to 10.1.1.5 through the tunnel.1 interface and then through vpn2.

Local NetScreen device with multiple tunnels bound to the tunnel.1 interface

Remote VPN peers—with dynamically assigned external IP addresses and fixed tunnel interface IP addresses—and their protected LANs



Route Table

ID	IP-Prefix (Dst)	Interface	Gateway
1	10.1.0.0/24	tunnel.1	**10.1.1.1**
2	**10.1.1.0/24**	**tunnel.1**	**10.1.2.1**
3	10.1.2.0/24	tunnel.1	**10.1.3.1**

Next-Hop Tunnel Binding Table

Next-Hop	VPN	Flag
10.1.1.1	vpn1	static
10.1.2.1	**vpn2**	static
10.1.3.1	vpn3	static

You can employ Border Gateway Protocol (BGP) to populate the route table automatically, or you can manually enter these routes. The IP address for the gateway is the address of the tunnel interface at the remote peer's site.

During Phase 2 negotiations, the two IKE peers exchange tunnel interface addresses and automatically enter these next-hop-to-tunnel bindings. Optionally, you can manually enter these. The next-hop IP address is the remote peer's tunnel interface IP address.

In the above entries, the IP address for the gateway in the route table, which is also the next-hop IP address in the NHTB table, is the tunnel interface at the remote peer's site. This IP address links the route—and consequently the tunnel interface specified in the route—to a particular VPN tunnel for traffic destined to the specified IP-prefix.

The NetScreen device uses the IP address of the remote peer's tunnel interface as the gateway and next-hop IP address. You can enter the route manually, or you can allow Border Gateway Protocol (BGP) to enter a route referencing the peer's tunnel interface IP address as the gateway in the route table automatically[12]. The same IP address must also be entered as the next hop, along with the appropriate VPN tunnel name, in the NHTB table. Again, there are two options: you can either enter it manually, or you can allow the NetScreen device to obtain it from the remote peer during Phase 2 negotiations and enter it automatically.

The NetScreen device uses the gateway IP address in the route table entry and the next-hop IP address in the NHTB table entry as the common element to link the tunnel interface with the corresponding VPN tunnel. The NetScreen device can then direct traffic destined for the IP-prefix specified in the route with the correct VPN tunnel specified in the NHTB table.

Remote Peers' Addresses

The internal addressing scheme for all remote peers reached through route-based VPNs must be unique among each other. One way to accomplish this is for each remote peer to perform network address translation (NAT) for the source and destination addresses. In addition, the tunnel interface IP addresses must also be unique among all remote peers. If you intend to connect to large numbers of remote sites, an address plan becomes imperative. The following is a possible addressing plan for up to 1000 VPN tunnels:

Dst in Local Route Table	Local Tunnel Interface	Gateway/Next-Hop (Peer's Tunnel Interface)	VPN Tunnel
10.0.3.0/24	tunnel.1	10.0.2.1/24	vpn1
10.0.5.0/24	tunnel.1	10.0.4.1/24	vpn2
10.0.7.0/24	tunnel.1	10.0.6.1/24	vpn3
…	…	…	…
10.0.251.0/24	tunnel.1	10.0.250.1/24	vpn125

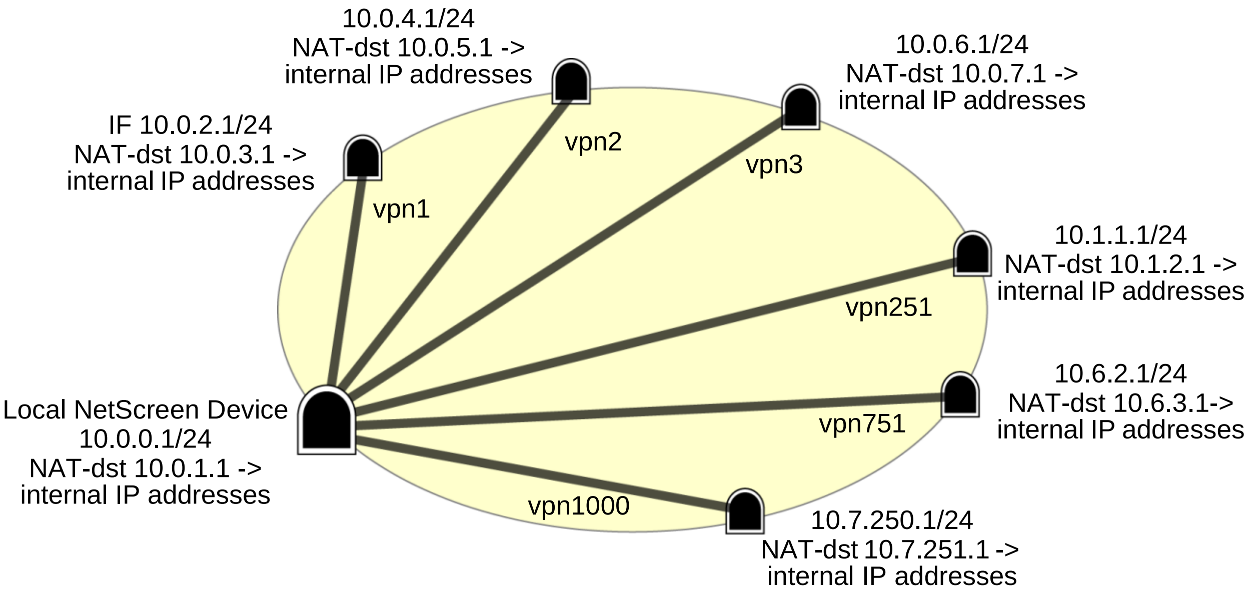
[12] Because a tunnel interface bound to multiple tunnels cannot send dynamic routing protocol broadcasts and multicasts, it cannot support the Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). See "Automatic Table Entries" on page 331.

Dst in Local Route Table	Local Tunnel Interface	Gateway/Next-Hop (Peer's Tunnel Interface)	VPN Tunnel
10.1.3.0/24	tunnel.1	10.1.2.1/24	vpn126
10.1.5.0/24	tunnel.1	10.1.4.1/24	vpn127
10.1.7.0/24	tunnel.1	10.1.6.1/24	vpn128
…	…	…	…
10.1.251.0/24	tunnel.1	10.1.250.1/24	vpn250
10.2.3.0/24	tunnel.1	10.2.2.1/24	vpn251
…	…	…	…
10.2.251.0/24	tunnel.1	10.2.250.1/24	vpn375
…	…	…	…
10.7.3.0/24	tunnel.1	10.7.2.1/24	vpn876
…	…	…	…
10.7.251.0/24	tunnel.1	10.7.250.1/24	vpn1000

The tunnel interface on the local NetScreen device: is 10.0.0.1/24. On all remote hosts, there is a tunnel interface with an IP address, which appears as the gateway/next-hop IP address in the local route table and NHTB table.

For an example illustrating multiple tunnels bound to a single tunnel interface with address translation, see "Example: Multiple VPNs on One Tunnel Interface to Overlapping Subnets" on page 333.

The local NetScreen device and all its peers perform NAT-dst with IP shifting on inbound VPN traffic and NAT-src from the egress tunnel interface IP address with port translation on outbound VPN traffic. For more information about NAT-src and NAT-dst, see "Address Translation" on page **2** -245.



Manual and Automatic Table Entries

You can make entries in the NHTB and route tables manually. You can also automate the populating of the NHTB and route tables. For a small number of tunnels bound to a single tunnel interface, the manual method works well. For a large number of tunnels, the automatic method reduces administrative setup and maintenance as the routes dynamically self-adjust if tunnels or interfaces become unavailable on the tunnel interface at the hub site.

Manual Table Entries

You can manually map a VPN tunnel to the IP address of a remote peer's tunnel interface in the next-hop tunnel binding (NHTB) table. First, you must contact the remote admin and learn the IP address used for the tunnel interface at that end of a tunnel. Then, you can associate that address with the VPN tunnel name in the NHTB table with the following command:

set interface tunnel.1 nhtb *peer's_tunnel_interface_addr* **vpn** *name_str*

After that, you can enter a static route in the route table that uses that tunnel interface IP address as the gateway. You can enter the route either through the WebUI or through the following CLI command:

set vrouter *name-str* **route** *dst_addr* **interface tunnel.1 gateway** *peer's_tunnel_interface_addr*

Automatic Table Entries

To make the population of both the NHTB and route tables automatic, the following conditions must be met:

- The remote peers for all VPN tunnels bound to a single local tunnel interface must be NetScreen devices running ScreenOS 5.0.0.
- Each remote peer must bind its tunnel to a tunnel interface, and that interface must have an IP address unique among all peer tunnel interface addresses.
- At both ends of each VPN tunnel, enable VPN monitoring with the rekey option, or enable the IKE heartbeat reconnect option for each remote gateway[13].
- The local and remote peers must have an instance of Border Gateway Protocol (BGP) enabled on their connecting tunnel interfaces.

The use of VPN monitoring with the rekey option allows the NetScreen devices at both ends of a tunnel to set up the tunnel without having to wait for user-originated VPN traffic[14]. After you enable VPN monitoring with the rekey option at both ends of a VPN tunnel, the two NetScreen devices perform Phase 1 and Phase 2 IKE negotiations to establish the tunnel. (For more information, see "VPN Monitoring" on page 307.)

During Phase 2 negotiations, the NetScreen devices exchange tunnel interface IP addresses with each other. Each IKE module can then automatically enter the tunnel interface IP address and its corresponding VPN tunnel name in the NHTB table.

[13] If you are running BGP on the tunnel interfaces, traffic generated by the protocol can trigger IKE negotiations even without enabling VPN monitoring with the rekey option or enabling the IKE heartbeat reconnect option. Still, NetScreen recommends that you not rely on dynamic routing traffic to trigger IKE negotiations. Instead use VPN monitoring with the rekey option or the IKE heartbeat reconnect option.

[14] For remote peers with a dynamically assigned external IP address or with a fully-qualified domain name (FQDN) mapped to a dynamic IP address, the remote peer must first initiate IKE negotiations. However, because the Phase 2 SA on the local NetScreen device caches the remote peer's dynamically assigned IP address, either peer can reinitiate IKE negotiations to reestablish a tunnel whose VPN monitoring state has changed from up to down.

To enable the local NetScreen device to enter routes to remote destinations automatically in its route table, you must enable an instance of BGP on the local and remote tunnel interfaces. The basic steps are as follows:

1. Create a BGP routing instance on the virtual router that contains the tunnel interface to which you have bound multiple VPN tunnels.
2. Enable the routing instance on the virtual router.
3. Enable the routing instance on the tunnel interface leading to the BPG peers.

The remote peers also perform these steps.

On the local (or hub) device, you must also define a default route and a static route to each peer’s tunnel interface IP address. Static routes to the peers’ tunnel interfaces are necessary for the hub device to reach its BGP neighbors initially through the correct VPN tunnel.

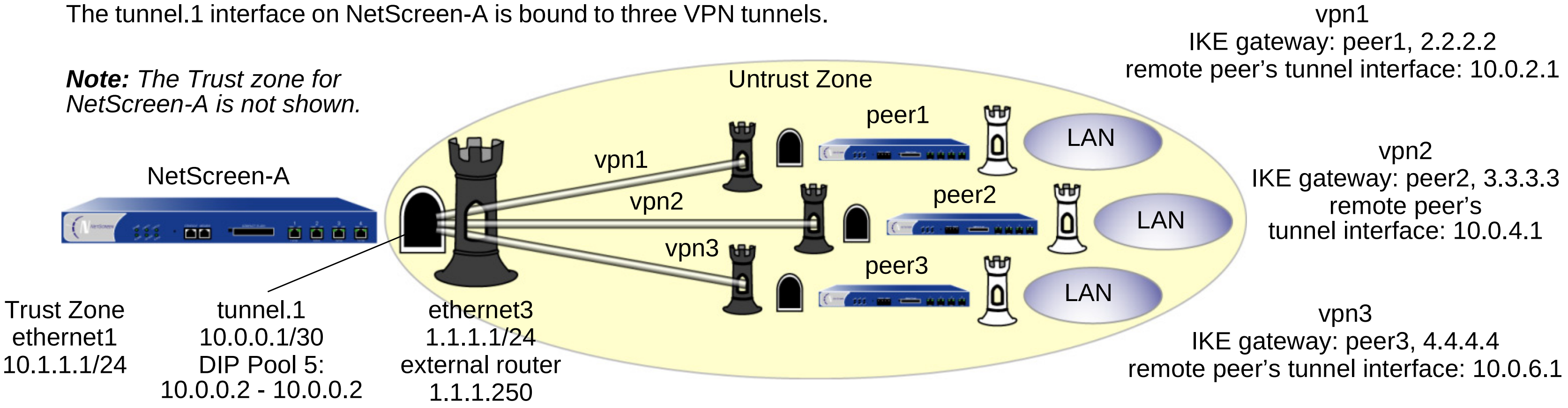
After establishing communications, the BGP neighbors exchange routing information so that they can each automatically populate their route tables. After the two peers establish a VPN tunnel between themselves, the remote peers can send and receive routing information to and from the local device. When the dynamic routing instance on the local NetScreen device learns a route to a peer through a local tunnel interface, it includes the IP address of the remote peer’s tunnel interface as the gateway in the route.

For an example illustrating the configuration of multiple tunnels bound to a single tunnel interface where the “hub” device populates its NHTB and route tables automatically, see “Example: Automatic Route and NHTB Table Entries” on page 364.

Example: Multiple VPNs on One Tunnel Interface to Overlapping Subnets

In this example, you bind three route-based AutoKey IKE VPN tunnels—vpn1, vpn2, and vpn3—to a single tunnel interface—tunnel.1. The tunnels lead from NetScreen-A to three remote peers—peer1, peer2, and peer3. You manually add both the route table and NHTB table entries on NetScreen-A for all three peers.

The tunnel.1 interface on NetScreen-A is bound to three VPN tunnels.



Note: *The Trust zone for NetScreen-A is not shown.*

The VPN tunnel configurations at both ends of each tunnel use the following parameters: AutoKey IKE, preshared key (peer1: “netscreen1”, peer2: “netscreen2”, peer3: “netscreen3”), and the security level predefined as “Compatible” for both Phase 1 and Phase 2 proposals. (For details about these proposals, see “Tunnel Negotiation” on page 11.)

All security zones and interfaces on each device are in the trust-vr virtual routing domain for that device.

This example uses the same address space—10.1.1.0/24—for every LAN to show how you can use source and destination network address translation (NAT-src and NAT-dst) to overcome addressing conflicts among IPSec peers. For more information about NAT-src and NAT-dst, see “Address Translation” on page **2** -245.

WebUI (NetScreen-A)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Enter the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 10.0.0.1/30

Network > Interfaces > Edit (for tunnel.1) > DIP > New: Enter the following, and then click **OK**:

ID: 5

IP Address Range: (select), 10.0.0.2 ~ 10.0.0.2

Port Translation: (select)

In the same subnet as the interface IP or its secondary IPs: (select)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: oda1

IP Address/Domain Name:

IP/Netmask: (select), 10.0.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: peers

IP Address/Domain Name:

IP/Netmask: (select), 10.0.0.0/16

Zone: Untrust

3. VPNs

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: peer1

Type: Static IP: (select), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: peer2

Type: Static IP: (select), Address/Hostname: 3.3.3.3

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn3

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: peer3

Type: Static IP: (select), Address/Hostname: 4.4.4.4

Preshared Key: netscreen3

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. Routes

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.1.0/24

Gateway: (select)

Interface: ethernet1

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.3.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 10.0.2.1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.2.2/32

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 10.0.2.1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.5.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 10.0.4.1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.4.2/32

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 10.0.4.1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.7.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 10.0.6.1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.6.2/32

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 10.0.6.1

Network > Interfaces > Edit (for tunnel.1) > NHTB > New: Enter the following, and then click **Add**:

New Next Hop Entry:

IP Address: 10.0.2.1

VPN: vpn1

Network > Interfaces > Edit (for tunnel.1) > NHTB: Enter the following, and then click **Add**:

New Next Hop Entry:

IP Address: 10.0.4.1

VPN: vpn2

Network > Interfaces > Edit (for tunnel.1) > NHTB: Enter the following, and then click **Add**:

New Next Hop Entry:

IP Address: 10.0.6.1

VPN: vpn3

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book: (select), corp

Destination Address:

Address Book: (select), peers

Service: Any

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Source Translation: (select)

DIP On: 5 (10.0.0.2–10.0.0.2)/X-late

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), peers

Destination Address:

Address Book Entry: (select), oda1

Service: Any

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Destination Translation: (select)

Translate to IP Range: (select), 10.1.1.0 - 10.1.1.254

CLI (NetScreen-A)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.0.0.1/30
set interface tunnel.1 dip 5 10.0.0.2 10.0.0.2
```

2. Addresses

```
set address trust corp 10.1.1.0/24
set address trust oda1 10.0.1.0/24
set address untrust peers 10.0.0.0/16
```

3. VPNs

```
set ike gateway peer1 address 2.2.2.2 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway peer1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set ike gateway peer2 address 3.3.3.3 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
```

```
set vpn vpn2 gateway peer2 sec-level compatible
set vpn vpn2 bind interface tunnel.1
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set ike gateway peer3 address 4.4.4.4 outgoing-interface ethernet3 preshare
    netscreen3 sec-level compatible
set vpn vpn3 gateway peer3 sec-level compatible
set vpn vpn3 bind interface tunnel.1
set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. Routes

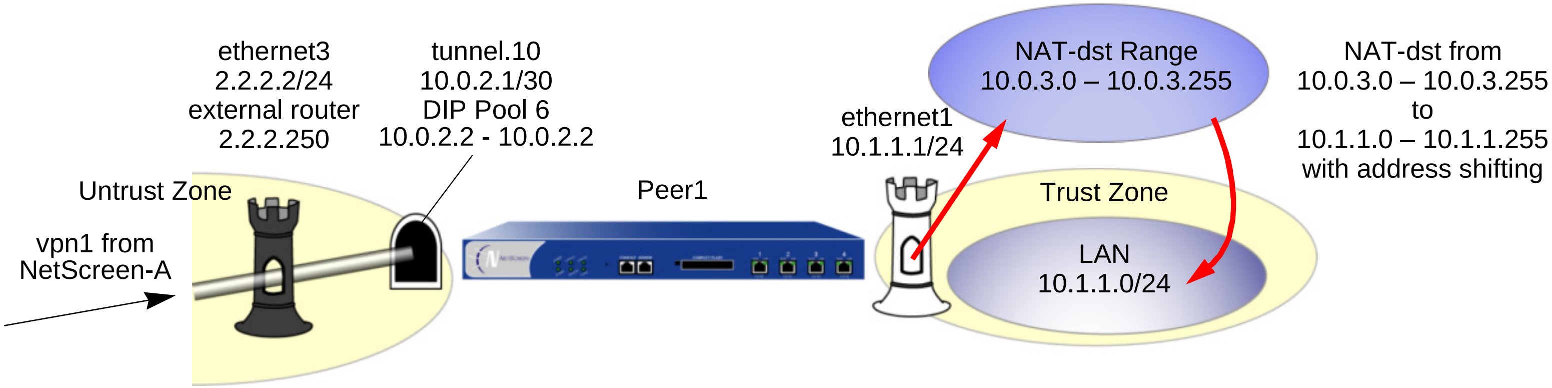
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.0.1.0/24 interface ethernet1
set vrouter trust-vr route 10.0.3.0/24 interface tunnel.1 gateway 10.0.2.1
set vrouter trust-vr route 10.0.2.2/32 interface tunnel.1 gateway 10.0.2.1
set vrouter trust-vr route 10.0.5.0/24 interface tunnel.1 gateway 10.0.4.1
set vrouter trust-vr route 10.0.4.2/32 interface tunnel.1 gateway 10.0.4.1
set vrouter trust-vr route 10.0.7.0/24 interface tunnel.1 gateway 10.0.6.1
set vrouter trust-vr route 10.0.6.2/32 interface tunnel.1 gateway 10.0.6.1
set interface tunnel.1 nhtb 10.0.2.1 vpn vpn1
set interface tunnel.1 nhtb 10.0.4.1 vpn vpn2
set interface tunnel.1 nhtb 10.0.6.1 vpn vpn3
```

5. Policies

```
set policy from trust to untrust corp peers any nat src dip-id 5 permit
set policy from untrust to trust peers oda1 any nat dst ip 10.1.1.0 10.1.1.254
    permit
save
```

Peer1

The following configuration is what the remote admin for the NetScreen device at the peer1 site must enter to create a VPN tunnel to NetScreen-A at the corporate site. The remote admin configures the NetScreen device to perform source and destination NAT (NAT-src and NAT-dst) because the internal addresses are in the same address space as those in the corporate LAN: 10.1.1.0/24. Peer1 performs NAT-src using DIP pool 6 to translate all internal source addresses to 10.0.2.2 when sending traffic through VPN1 to NetScreen-A. Peer1 performs NAT-dst on VPN traffic sent from NetScreen-A, translating addresses from 10.0.3.0/24 to 10.1.1.0/24 with address shifting in effect.



***Note:** For more information about NAT-src and NAT-dst, see “Address Translation” on page **2** -245.*

WebUI (Peer1)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Enter the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.10

Zone (VR): Untrust (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 10.0.2.1/30

Network > Interfaces > Edit (for tunnel.10) > DIP > New: Enter the following, and then click **OK**:

ID: 6

IP Address Range: (select), 10.0.2.2 ~ 10.0.2.2

Port Translation: (select)

In the same subnet as the interface IP or its secondary IPs: (select)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: lan

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: oda2

IP Address/Domain Name:

IP/Netmask: (select), 10.0.3.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: to_corp

IP Address/Domain Name:

IP/Netmask: (select), 10.0.1.0/24

Zone: Untrust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: fr_corp

IP Address/Domain Name:

IP/Netmask: (select), 10.0.0.2/32

Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: corp

Type: Static IP: (select), Address/Hostname: 1.1.1.1

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.10

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. Routes

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.3.0/24

Gateway: (select)

Interface: ethernet1

Gateway IP Address: 0.0.0.0

Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.0.0/8

Gateway: (select)

Interface: tunnel.10

Gateway IP Address: 0.0.0.0

Metric: 10

5. Policies

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), fr_corp

Destination Address:

Address Book Entry: (select), oda2

Service: Any

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Destination Translation: (select)

Translate to IP Range: (select), 10.1.1.0 - 10.1.1.254

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), lan

Destination Address:

Address Book Entry: (select), to_corp

Service: Any

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Source Translation: (select)

DIP On: 6 (10.0.2.2–10.0.2.2)/X-late

CLI (Peer1)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.10 zone untrust
set interface tunnel.10 ip 10.0.2.1/30
set interface tunnel.10 dip 6 10.0.2.2 10.0.2.2
```

2. Addresses

```
set address trust lan 10.1.1.0/24
set address trust oda2 10.0.3.0/24
set address untrust to_corp 10.0.1.0/24
set address untrust fr_corp 10.0.0.2/32
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.10
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. Routes

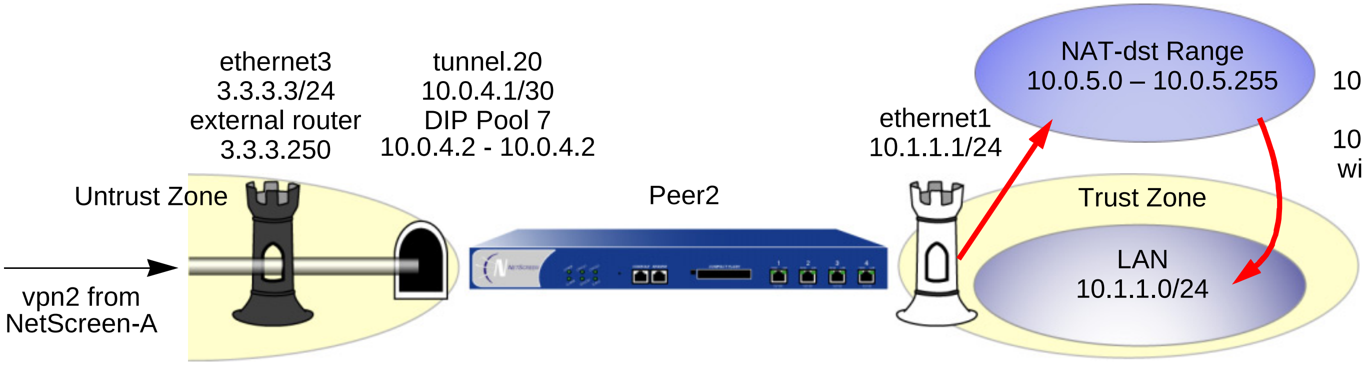
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250 metric 1
set vrouter trust-vr route 10.0.3.0/24 interface ethernet1 metric 1
set vrouter trust-vr route 10.0.0.0/8 interface tunnel.10 metric 10
```

5. Policies

```
set policy from trust to untrust lan to_corp any nat src dip-id 6 permit
set policy from untrust to trust fr_corp oda2 any nat dst ip 10.1.1.0
    10.1.1.254 permit
save
```

Peer2

The following configuration is what the remote admin for the NetScreen device at the peer2 site must enter to create a VPN tunnel to NetScreen-A at the corporate site. The remote admin configures the NetScreen device to perform source and destination NAT (NAT-src and NAT-dst) because the internal addresses are in the same address space as those in the corporate LAN: 10.1.1.0/24. Peer2 performs NAT-src using DIP pool 7 to translate all internal source addresses to 10.0.4.2 when sending traffic through VPN2 to NetScreen-A. Peer2 performs NAT-dst on VPN traffic sent from NetScreen-A, translating addresses from 10.0.5.0/24 to 10.1.1.0/24 with address shifting in effect.



Note: *For more information about NAT-src and NAT-dst, see “Address Translation” on page* ***2*** *-245.*

WebUI (Peer2)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Enter the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.20

Zone (VR): Untrust (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 10.0.4.1/30

Network > Interfaces > Edit (for tunnel.20) > DIP > New: Enter the following, and then click **OK**:

ID: 7

IP Address Range: (select), 10.0.4.2 ~ 10.0.4.2

Port Translation: (select)

In the same subnet as the interface IP or its secondary IPs: (select)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: lan

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: oda3

IP Address/Domain Name:

IP/Netmask: (select), 10.0.5.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: to_corp

IP Address/Domain Name:

IP/Netmask: (select), 10.0.1.0/24

Zone: Untrust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: fr_corp

IP Address/Domain Name:

IP/Netmask: (select), 10.0.0.2/32

Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: corp

Type: Static IP: (select), Address/Hostname: 1.1.1.1

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.20

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. Routes

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 3.3.3.250

Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.5.0/24

Gateway: (select)

Interface: ethernet1

Gateway IP Address: 0.0.0.0

Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.1.0/24

Gateway: (select)

Interface: tunnel.20

Gateway IP Address: 0.0.0.0

Metric: 10

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), lan

Destination Address:

Address Book Entry: (select), to_corp

Service: Any

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Source Translation: (select)

DIP On: 7 (10.0.4.2–10.0.4.2)/X-late

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), fr_corp

Destination Address:

Address Book Entry: (select), oda3

Service: Any

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Destination Translation: (select)

Translate to IP Range: (select), 10.1.1.0 - 10.1.1.254

CLI (Peer2)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface tunnel.20 zone untrust
set interface tunnel.20 ip 10.0.4.1/30
set interface tunnel.20 dip 7 10.0.4.2 10.0.4.2
```

2. Addresses

```
set address trust lan 10.1.1.0/24
set address trust oda3 10.0.5.0/24
set address untrust to_corp 10.0.1.0/24
set address untrust fr_corp 10.0.0.2/32
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn2 gateway corp sec-level compatible
set vpn vpn2 bind interface tunnel.20
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. Routes

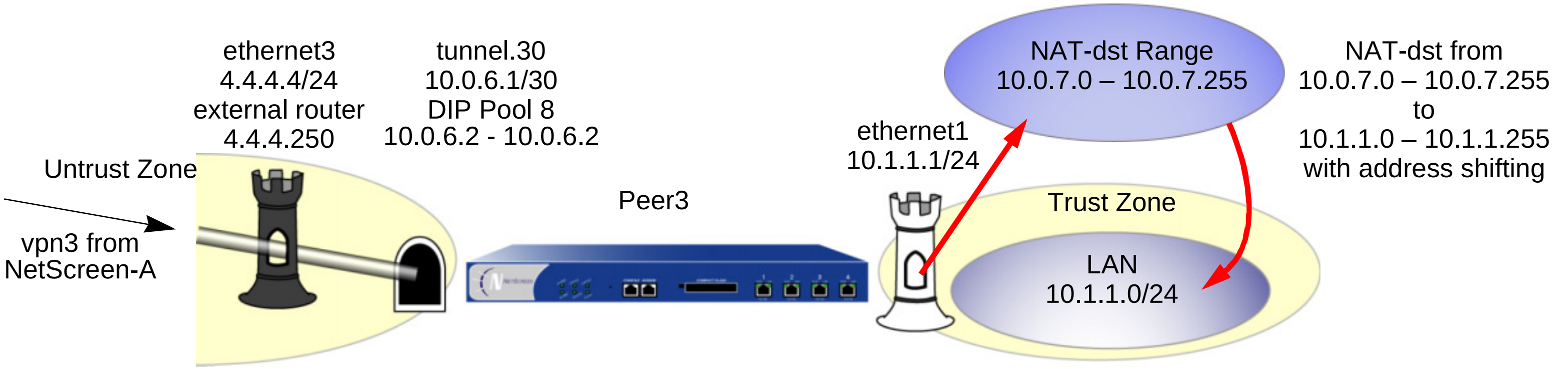
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250 metric 1
set vrouter trust-vr route 10.0.5.0/24 interface ethernet1 metric 1
set vrouter trust-vr route 10.0.0.0/8 interface tunnel.20 metric 10
```

5. Policies

```
set policy from trust to untrust lan to_corp any nat src dip-id 7 permit
set policy from untrust to trust fr_corp oda3 any nat dst ip 10.1.1.0
    10.1.1.254 permit
save
```

Peer3

The following configuration is what the remote admin for the NetScreen device at the peer3 site must enter to create a VPN tunnel to NetScreen-A at the corporate site. The remote admin configures the NetScreen device to perform source and destination NAT (NAT-src and NAT-dst) because the internal addresses are in the same address space as those in the corporate LAN: 10.1.1.0/24. Peer3 performs NAT-src using DIP pool 8 to translate all internal source addresses to 10.0.6.2 when sending traffic through VPN3 to NetScreen-A. Peer3 performs NAT-dst on VPN traffic sent from NetScreen-A, translating addresses from 10.0.7.0/24 to 10.1.1.0/24 with address shifting in effect.



Note: *For more information about NAT-dst, see “Destination Network Address Translation” on page* ***2*** *-276.*

WebUI (Peer3)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Enter the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 4.4.4.4/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.30

Zone (VR): Untrust (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 10.0.6.1/30

Network > Interfaces > Edit (for tunnel.320) > DIP > New: Enter the following, and then click **OK**:

ID: 7

IP Address Range: (select), 10.0.6.2 ~ 10.0.6.2

Port Translation: (select)

In the same subnet as the interface IP or its secondary IPs: (select)

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: lan

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: oda4

IP Address/Domain Name:

IP/Netmask: (select), 10.0.7.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: to_corp

IP Address/Domain Name:

IP/Netmask: (select), 10.0.1.0/24

Zone: Untrust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: fr_corp

IP Address/Domain Name:

IP/Netmask: (select), 10.0.0.2/32

Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn3

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: corp

Type: Static IP: (select), Address/Hostname: 1.1.1.1

Preshared Key: netscreen3

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.30

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. Routes

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 4.4.4.250

Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.7.0/24

Gateway: (select)

Interface: ethernet1

Gateway IP Address: 0.0.0.0

Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.0.0.0/8

Gateway: (select)

Interface: tunnel.20

Gateway IP Address: 10.0.0.1

Metric: 10

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), lan

Destination Address:

Address Book Entry: (select), to_corp

Service: Any

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Source Translation: (select)

DIP On: 8 (10.0.6.2–10.0.6.2)/X-late

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), fr_corp

Destination Address:

Address Book Entry: (select), oda4

Service: Any

Action: Permit

Position at Top: (select)

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Policy configuration page:

NAT:

Destination Translation: (select)

Translate to IP Range: (select), 10.1.1.0 - 10.1.1.254

CLI (Peer3)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 4.4.4.4/24
set interface tunnel.30 zone untrust
set interface tunnel.30 ip 10.0.6.1/30
set interface tunnel.30 dip 8 10.0.6.2 10.0.6.2
```

2. Addresses

```
set address trust lan 10.1.1.0/24
set address trust oda4 10.0.7.0/24
set address untrust to_corp 10.0.1.0/24
set address untrust fr_corp 10.0.0.2/32
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen3 sec-level compatible
set vpn vpn3 gateway corp sec-level compatible
set vpn vpn3 bind interface tunnel.30
set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. Routes

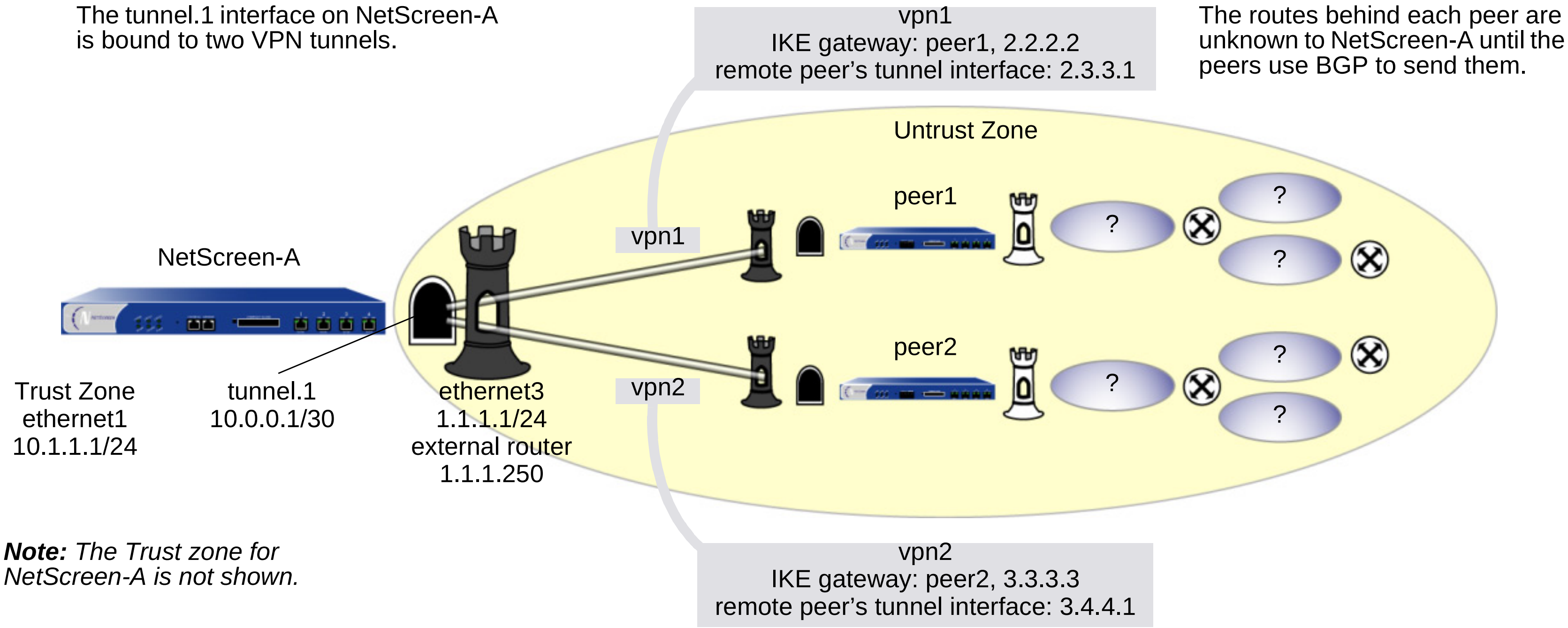
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250 metric 1
set vrouter trust-vr route 10.0.7.0/24 interface ethernet1 metric 1
set vrouter trust-vr route 10.0.0.0/8 interface tunnel.30 metric 10
```

5. Policies

```
set policy from trust to untrust lan to_corp any nat src dip-id 8 permit
set policy from untrust to trust fr_corp oda4 any nat dst ip 10.1.1.0
    10.1.1.254 permit
save
```

Example: Automatic Route and NHTB Table Entries

In this example, you bind two route-based AutoKey IKE VPN tunnels—vpn1, vpn2—to a single tunnel interface—tunnel.1 on NetScreen-A at the corporate site. The network that each remote peer protects has multiple routes behind the connected route. Using Border Gateway Protocol (BGP), the peers communicate their routes to NetScreen-A. This example permits VPN traffic from the corporate site behind NetScreen-A to the peer sites.



The tunnel.1 interface on NetScreen-A is bound to two VPN tunnels.

vpn1
IKE gateway: peer1, 2.2.2.2
remote peer’s tunnel interface: 2.3.3.1

The routes behind each peer are unknown to NetScreen-A until the peers use BGP to send them.

vpn2
IKE gateway: peer2, 3.3.3.3
remote peer’s tunnel interface: 3.4.4.1

Note: *The Trust zone for NetScreen-A is not shown.*

The VPN tunnel configurations at both ends of each tunnel use the following parameters: AutoKey IKE, preshared key (peer1: “netscreen1”, peer2: “netscreen2”), and the security level predefined as “Compatible” for both Phase 1 and Phase 2 proposals. (For details about these proposals, see “Tunnel Negotiation” on page 11.)

By configuring the following two features, you can enable NetScreen-A to populate its NHTB and route tables automatically[15]:

- VPN monitoring with the rekey option (or the IKE heartbeats reconnect option)[16]
- BGP dynamic routing on tunnel.1

When you enable VPN monitoring with the rekey option for an AutoKey IKE VPN tunnel, NetScreen-A establishes a VPN connection with its remote peer as soon as you and the admin at the remote site finish configuring the tunnel. The devices do not wait for user-generated VPN traffic to perform IKE negotiations. During Phase 2 negotiations, the NetScreen devices exchange their tunnel interface IP address, so that NetScreen-A can automatically make a VPN-to-next-hop mapping in its NHTB table.

The rekey option ensures that when the Phase 1 and Phase 2 key lifetimes expire, the devices automatically negotiate the generation of new keys without the need for human intervention. VPN monitoring with the rekey option enabled essentially provides a means for keeping a VPN tunnel up continually, even when there is no user-generated traffic. This is necessary so that the BGP dynamic routing instances that you and the remote admins create and enable on the tunnel interfaces at both ends of the tunnels can send routing information to NetScreen-A and automatically populate its route table with the routes it needs to direct traffic through the VPN tunnel before those routes are required for user-generated traffic. (The admins at the peer sites still need to enter a single static route to the rest of the virtual private network through the tunnel interface at each respective site.)

You enter a default route and static routes on NetScreen-A to reach its BGP neighbors through the correct VPN tunnels. All security zones and interfaces on each device are in the trust-vr virtual routing domain for that device.

[15] If you are running a dynamic routing protocol on the tunnel interfaces, traffic generated by the protocol can trigger IKE negotiations even without enabling VPN monitoring with the rekey option or enabling the IKE heartbeat reconnect option. Still, NetScreen recommends that you not rely on dynamic routing traffic to trigger IKE negotiations. Instead use VPN monitoring with the rekey option or the IKE heartbeat reconnect option.

[16] If you are running BGP on the tunnel interfaces, the BGP-generated traffic can trigger IKE negotiations even without enabling VPN monitoring with the rekey option or enabling the IKE heartbeat reconnect option. Still, NetScreen recommends that you not rely on BGP traffic to trigger IKE negotiations. Instead, use VPN monitoring with the rekey option or the IKE heartbeat reconnect option.

WebUI (NetScreen-A)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/24

Enter the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 10.0.0.1/30

2. VPNs

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: peer1

Type: Static IP: (select), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

VPN Monitor[17]: (select)

Rekey: (select)

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: peer2

Type: Static IP: (select), Address/Hostname: 3.3.3.3

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

[17] Leave the Source Interface and Destination IP options at their default settings. For information about these options, see "VPN Monitoring" on page 307.

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

VPN Monitor[18]: (select)

Rekey: (select)

3. Static Route

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 2.3.3.1/32

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 2.3.3.1

[18] Leave the Source Interface and Destination IP options at their default settings. For information about these options, see "VPN Monitoring" on page 307.

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 3.4.4.1/32

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 3.4.4.1

4. Dynamic Routing

Network > Routing > Virtual Routers > Edit (for trust-vr) > Create BGP Instance: Enter the following, and then click **OK**:

AS Number (required): 99

BGP Enabled: (select)

Network > Interfaces > Edit (for tunnel.1) > BGP: Select the **Protocol BGP** check box, and then click **OK**.

Network > Routing > Virtual Routers > Edit (for trust-vr) > Edit BGP Instance > Neighbors: Enter the following, and then click **Add**:

AS Number: 99

Remote IP: 2.3.3.1

Outgoing Interface: tunnel.1

Network > Routing > Virtual Routers > Edit (for trust-vr) > Edit BGP Instance > Neighbors: Enter the following, and then click **Add**:

AS Number: 99

Remote IP: 3.4.4.1

Outgoing Interface: tunnel.1

5. Policy

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book: (select), Any

Destination Address:

Address Book: (select), Any

Service: ANY

Action: Permit

CLI (NetScreen-A)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.0.0.1/30
```

2. VPNs

```
set ike gateway peer1 address 2.2.2.2 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway peer1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn1 monitor rekey
set ike gateway peer2 address 3.3.3.3 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn2 gateway peer2 sec-level compatible
set vpn vpn2 bind interface tunnel.1
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn2 monitor rekey
```

3. Static Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 2.3.3.1/32 interface tunnel.1 gateway 2.3.3.1
set vrouter trust-vr route 2.4.4.1/32 interface tunnel.1 gateway 2.4.4.1
```

4. Dynamic Routing

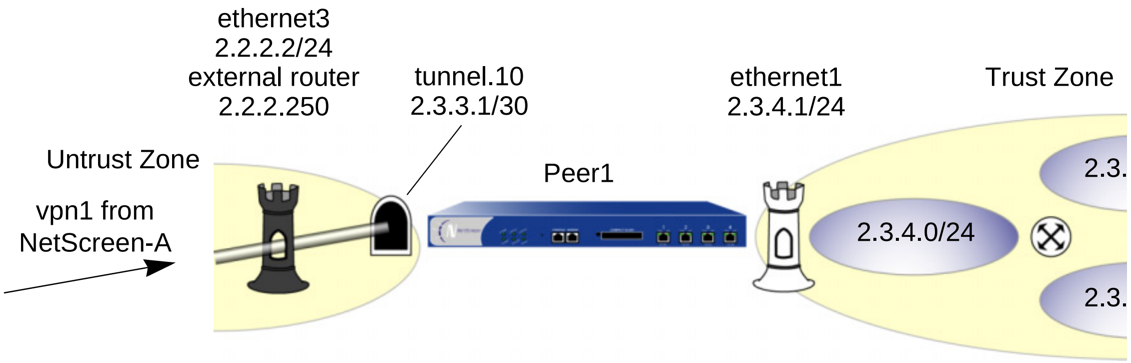
```
ns-> set vrouter trust-vr protocol bgp 99
ns-> set vrouter trust-vr protocol bgp enable
ns-> set interface tunnel.1 protocol bgp
ns-> set vrouter trust-vr
ns(trust-vr)-> set protocol bgp
ns(trust-vr/bgp)-> set neighbor 2.3.3.1 remote-as 99 outgoing interface
    tunnel.1
ns(trust-vr/bgp)-> set neighbor 2.3.3.1 enable
ns(trust-vr/bgp)-> set neighbor 3.4.4.1 remote-as 99 outgoing interface
    tunnel.1
ns(trust-vr/bgp)-> set neighbor 3.4.4.1 enable
ns(trust-vr/bgp)-> exit
ns(trust-vr)-> exit
```

5. Policy

```
set policy from trust to untrust any any any permit
save
```

Peer1

The following configuration is what the remote admin for the NetScreen device at the peer1 site must enter to create a VPN tunnel to NetScreen-A at the corporate site. The remote admin configures the NetScreen device to permit inbound traffic from the corporate site. He also configures the NetScreen device to communicate internal routes to its BGP neighbor through vpn1.



WebUI (Peer 1)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **OK**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 2.3.4.1/24

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.10

Zone (VR): Untrust (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 2.3.3.1/30

2. Address

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: corp

Type: Static IP: (select), Address/Hostname: 1.1.1.1

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.10

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. Static Routes

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.1.1.0/24

Gateway: (select)

Interface: tunnel.10

Gateway IP Address: 0.0.0.0

Metric: 1

5. Dynamic Routing

Network > Routing > Virtual Routers > Edit (for trust-vr) > Create BGP Instance: Enter the following, and then click **OK**:

AS Number (required): 99

BGP Enabled: (select)

Network > Interfaces > Edit (for tunnel.10) > BGP: Select the **Protocol BGP** check box, and then click **OK**.

Network > Routing > Virtual Routers > Edit (for trust-vr) > Edit BGP Instance > Neighbors: Enter the following, and then click **Add**:

AS Number: 99

Remote IP: 10.0.0.1

Outgoing Interface: tunnel.10

6. Policy

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), corp

Destination Address:

Address Book Entry: (select), Any

Service: ANY

Action: Permit

CLI (Peer1)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 2.3.4.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface tunnel.10 zone untrust
set interface tunnel.10 ip 2.3.3.1/30
```

2. Address

```
set address untrust corp 10.1.1.0/24
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.10
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. Static Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250 metric 1
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.10 metric 1
```

5. Dynamic Routing

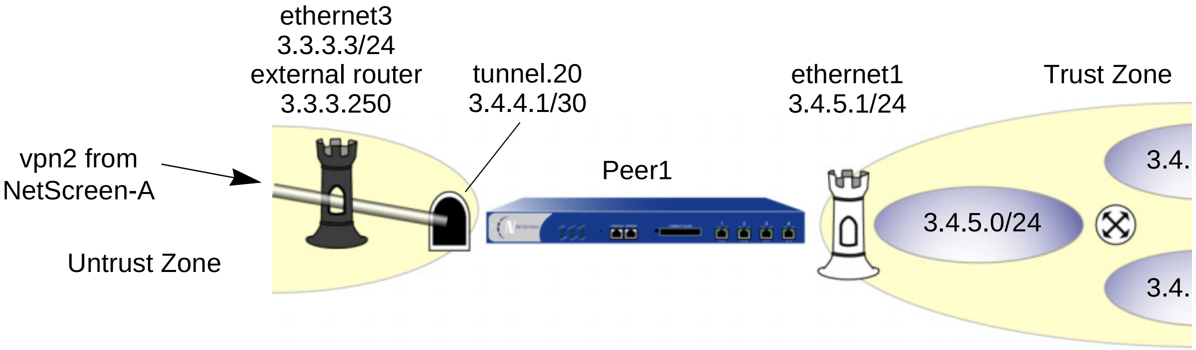
```
ns-> set vrouter trust-vr protocol bgp 99
ns-> set vrouter trust-vr protocol bgp enable
ns-> set interface tunnel.10 protocol bgp
ns-> set vrouter trust-vr
ns(trust-vr)-> set protocol bgp
ns(trust-vr/bgp)-> set neighbor 10.0.0.1 remote-as 99 outgoing interface
    tunnel.10
ns(trust-vr/bgp)-> set neighbor 10.0.0.1 enable
ns(trust-vr/bgp)-> exit
ns(trust-vr)-> exit
```

6. Policy

```
set policy from untrust to trust corp any any permit
save
```

Peer2

The following configuration is what the remote admin for the NetScreen device at the peer2 site must enter to create a VPN tunnel to NetScreen-A at the corporate site. The remote admin configures the NetScreen device to permit inbound traffic from the corporate site. He also configures the NetScreen device to communicate internal routes to its BGP neighbor through vpn2.



WebUI (Peer 2)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **OK**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 2.3.4.1/24

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.20

Zone (VR): Untrust (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 3.4.4.1/30

2. Address

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (select), 10.1.1.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: vpn2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: corp

Type: Static IP: (select), Address/Hostname: 1.1.1.1

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Bind to: Tunnel Interface, tunnel.20

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. Static Routes

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 3.3.3.250

Metric: 1

Network > Routing > Routing Entries > (trust-vr) New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.1.1.0/24

Gateway: (select)

Interface: tunnel.20

Gateway IP Address: 0.0.0.0

Metric: 1

5. Dynamic Routing

Network > Routing > Virtual Routers > Edit (for trust-vr) > Create BGP Instance: Enter the following, and then click **OK**:

AS Number (required): 99

BGP Enabled: (select)

Network > Interfaces > Edit (for tunnel.20) > BGP: Select the **Protocol BGP** check box, and then click **OK**.

Network > Routing > Virtual Routers > Edit (for trust-vr) > Edit BGP Instance > Neighbors: Enter the following, and then click **Add**:

AS Number: 99

Remote IP: 10.0.0.1

Outgoing Interface: tunnel.20

6. Policy

Policies > (From: Untrust, To: Trust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), corp

Destination Address:

Address Book Entry: (select), Any

Service: ANY

Action: Permit

CLI (Peer2)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 3.4.5.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24

set interface tunnel.20 zone untrust
set interface tunnel.20 ip 3.4.4.1/30
```

2. Address

```
set address untrust corp 10.1.1.0/24
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.20
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. Static Routes

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250 metric 1
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.20 metric 1
```

5. Dynamic Routing

```
ns-> set vrouter trust-vr protocol bgp 99
ns-> set vrouter trust-vr protocol bgp enable
ns-> set interface tunnel.20 protocol bgp
ns-> set vrouter trust-vr
ns(trust-vr)-> set protocol bgp
ns(trust-vr/bgp)-> set neighbor 10.0.0.1 remote-as 99 outgoing interface
    tunnel.20
ns(trust-vr/bgp)-> set neighbor 10.0.0.1 enable
ns(trust-vr/bgp)-> exit
ns(trust-vr)-> exit
```

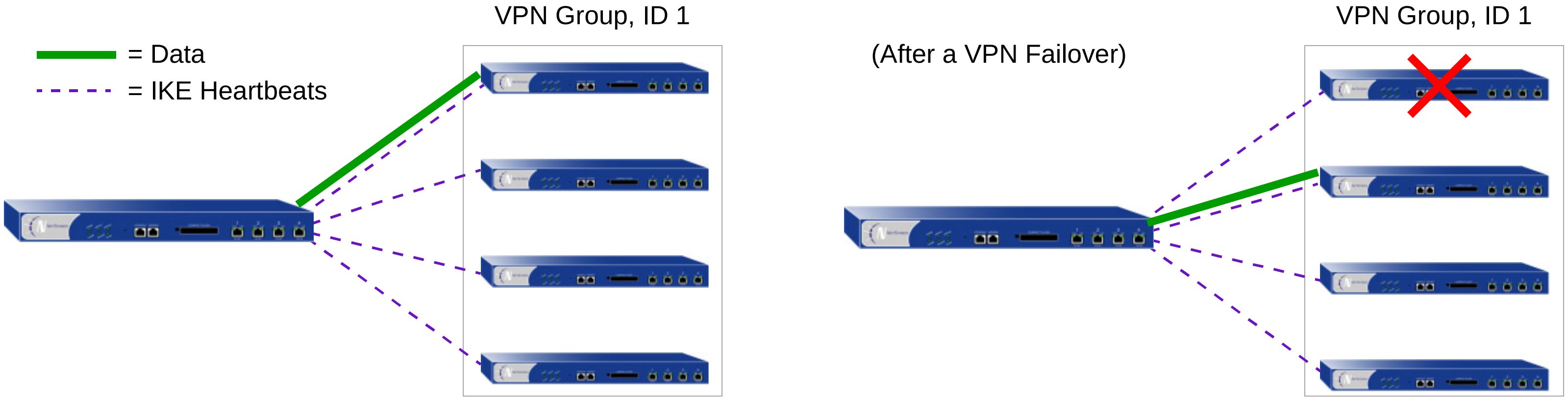
6. Policy

```
set policy from untrust to trust corp any any permit
save
```

Redundant VPN Gateways

The NetScreen redundant gateway feature provides a solution for continuous VPN connectivity during and after a site-to-site failover. You can create a VPN group to provide a set of up to four redundant gateways to which policy-based site-to-site or site-to-site dynamic peer AutoKey IKE IPSec[19] VPN tunnels can connect. When the NetScreen device first receives traffic matching a policy referencing a VPN group, it performs Phase 1 and Phase 2 IKE negotiations with all members in that group. The NetScreen device sends data through the VPN tunnel to the gateway with the highest priority, or "weight", in the group. For all other gateways in the group, the NetScreen device maintains the Phase 1 and 2 SAs and keeps the tunnels active by sending IKE keepalive packets through them. If the active VPN tunnel fails, the tunnel can fail over to the tunnel and gateway with the second highest priority in the group.

Note: *This scheme assumes that the sites behind the redundant gateways are connected so that data is mirrored among hosts at all sites. Furthermore, each site—being dedicated to high availability (HA)—has a redundant cluster of NetScreen devices operating in HA mode. Therefore, the VPN failover threshold must be set higher than the device failover threshold or VPN failovers might occur unnecessarily.*

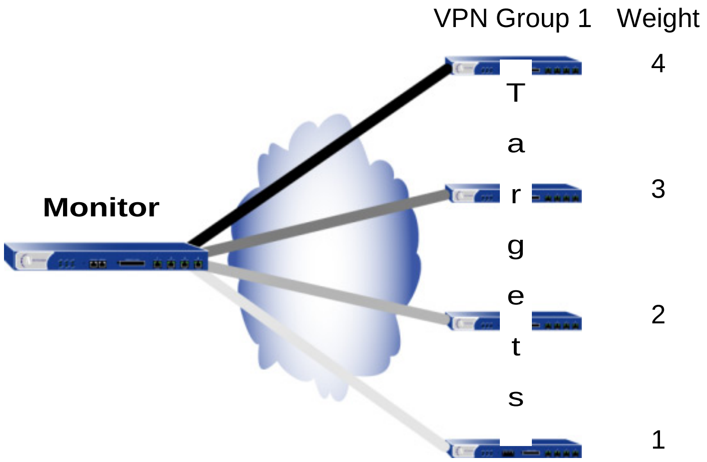


[19] VPN groups do not support L2TP, L2TP-over-IPSec, dialup, Manual Key, or route-based VPN tunnel types. In a Site-to-Site Dynamic Peer arrangement, the NetScreen device monitoring the VPN group must be the one whose untrust IP address is dynamically assigned, while the untrust IP addresses of the VPN group members must be static.

VPN Groups

A VPN group is a set of VPN tunnel configurations for up to four targeted remote gateways. The Phase 1 and Phase 2 security association (SA) parameters for each tunnel in a group can be different or identical (except for the IP address of the remote gateway, which obviously must be different). The VPN group has a unique ID number, and each member in the group is assigned a unique weight to indicate its place in rank of preference to be the active tunnel. A value of 1 indicates the lowest, or least preferred, ranking.

__Note:__ In this illustration, the shading symbolizes the weight of each tunnel. The darker the tunnel is shaded, the higher its priority.



The NetScreen device communicating with VPN group members and the members themselves have a monitor-to-target relationship. The monitoring device continually monitors the connectivity and wellbeing of each targeted device. The tools that the monitor uses to do this are as follows:

- IKE heartbeats
- IKE recovery attempts

Both tools are presented in the next section, “Monitoring Mechanisms” on page 384.

Note: *The monitor-to-target relationship need not be one way. The monitoring device might also be a member of a VPN group and thus be the target of another monitoring device.*

Monitoring Mechanisms

NetScreen uses two mechanisms to monitor members of a VPN group to determine their ability to terminate VPN traffic:

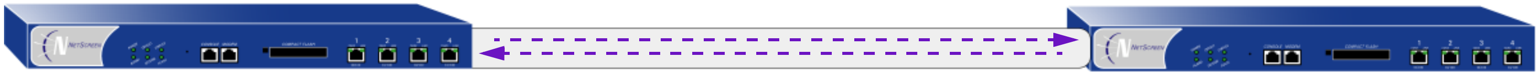
- IKE heartbeats
- IKE recovery attempts

Using these two tools, plus the TCP application failover option (see “TCP SYN-Flag Checking” on page 388), NetScreen devices can detect when a VPN failover is required and shift traffic to the new tunnel without disrupting VPN service.

IKE Heartbeats

IKE heartbeats are hello messages that IKE peers send to each other under the protection of an established Phase 1 security association (SA) to confirm the connectivity and wellbeing of the other. If, for example, device_m (the “monitor”) does not receive a specified number of heartbeats (the default is 5) from device_t (the “target”), device_m concludes that device_t is down. Device_m clears the corresponding Phase 1 and Phase 2 security associations (SAs) from its SA cache and begins the IKE recovery procedure. (See “IKE Recovery Procedure” on page 385.) Device_t also clears its SAs.

Note: *The IKE heartbeats feature must be enabled on the devices at both ends of a VPN tunnel in a VPN group. If it is enabled on device_m but not on device_t, device_m suppresses IKE heartbeat transmission and generates the following message in the event log: “Heartbeats have been disabled because the peer is not sending them.*”



IKE Heartbeats must flow both
ways through the VPN tunnel.

To define the IKE heartbeat interval and threshold for a specified VPN tunnel (the default is 5), do the following:

WebUI

VPNs > AutoKey Advanced > Gateway > Edit (for the gateway whose IKE heartbeat threshold you want to modify) > Advanced: Enter the new values in the Heartbeat Hello and Heartbeat Threshold fields, and then click **OK**.

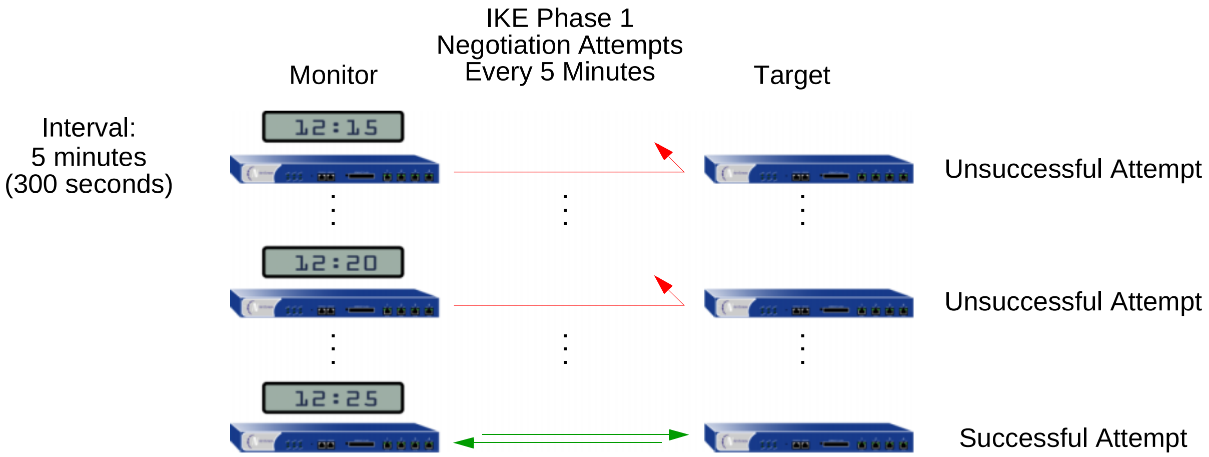
CLI

set ike gateway *name_str* heartbeat hello *number*

set ike gateway *name_str* heartbeat threshold *number*

IKE Recovery Procedure

After the monitoring NetScreen device determines that a targeted device is down, the monitor stops sending IKE heartbeats and clears the SAs for that peer from its SA cache. After a defined interval, the monitor attempts to initiate Phase 1 negotiations with the failed peer. If the first attempt is unsuccessful, the monitor continues to attempt Phase 1 negotiations at regular intervals until negotiations are successful.



To define the IKE recovery interval for a specified VPN tunnel (the minimum setting is 60 seconds), do either of the following:

WebUI

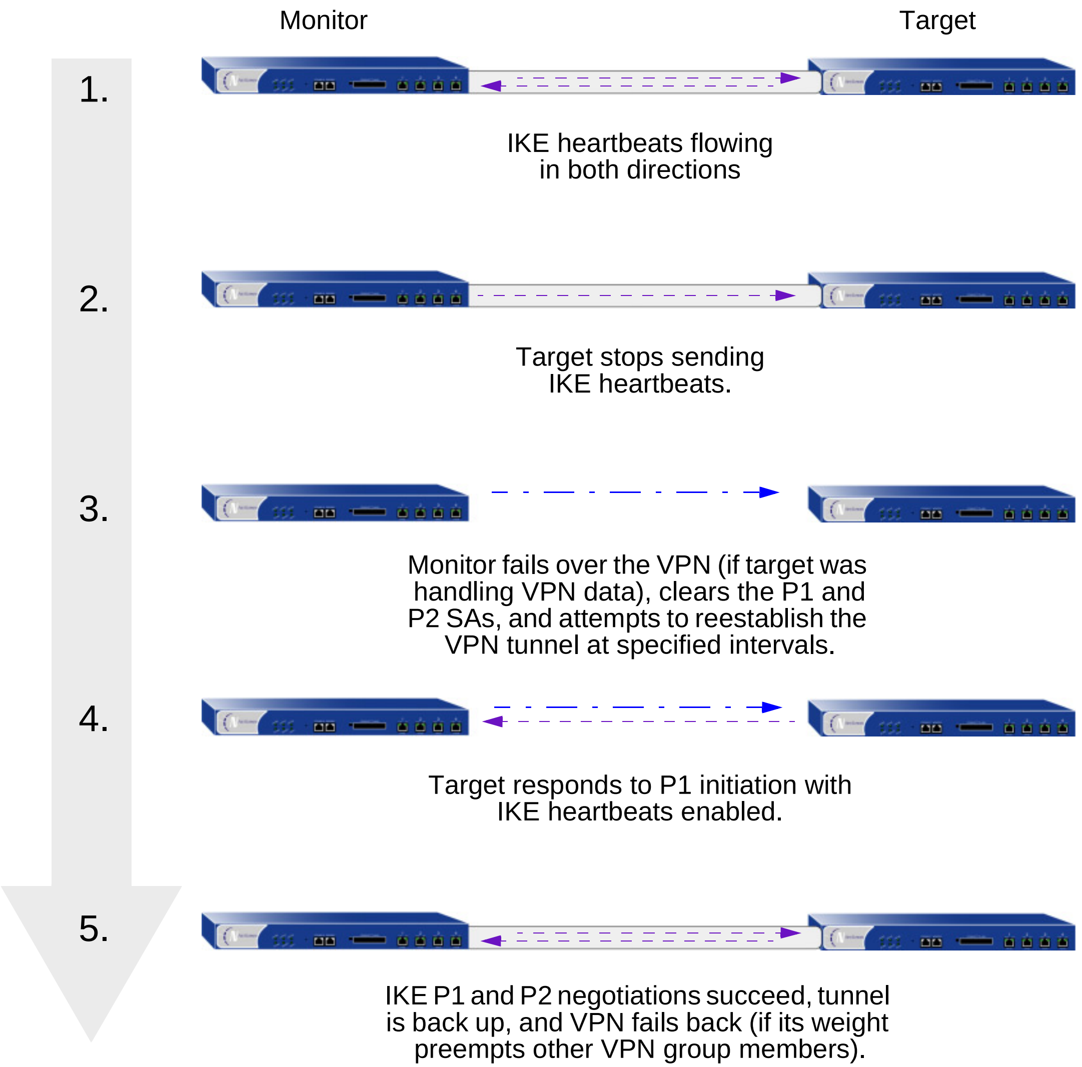
VPNs > AutoKey Advanced > Gateway > Edit (for the gateway whose IKE reconnect interval you want to modify) > Advanced: Enter the value in seconds in the Heartbeat Reconnect field, and then click **OK**.

CLI

set ike gateway *name_str* heartbeat reconnect *number*

When a VPN group member with the highest weight fails over the tunnel to another group member and then reconnects with the monitoring device, the tunnel automatically fails back to the first member. The weighting system always causes the best ranking gateway in the group to handle the VPN data whenever it can do so.

The following illustration presents the process that a member of a VPN group undergoes when the missing heartbeats from a targeted gateway surpass the failure threshold.


Monitor
Target
1.
IKE heartbeats flowing in both directions
2.
Target stops sending IKE heartbeats.
3.
Monitor fails over the VPN (if target was handling VPN data), clears the P1 and P2 SAs, and attempts to reestablish the VPN tunnel at specified intervals.
4.
Target responds to P1 initiation with IKE heartbeats enabled.
5.
IKE P1 and P2 negotiations succeed, tunnel is back up, and VPN fails back (if its weight preempts other VPN group members).

TCP SYN-Flag Checking

For a seamless VPN failover to occur, the handling of TCP sessions must be addressed. If, after a failover, the new active gateway receives a packet in an existing TCP session, the new gateway treats it as the first packet in a new TCP session and checks if the SYN flag is set in the packet header. Because this packet is really part of an existing session, it does not have the SYN flag set. Consequently, the new gateway rejects the packet. With TCP SYN flag checking enabled, all TCP applications have to reconnect after the failover occurs.

To resolve this, you can disable SYN-flag checking for TCP sessions in VPN tunnels, as follows:

WebUI

You cannot disable SYN-flag checking via the WebUI.

CLI

```
unset flow tcp-syn-check-in-tunnel
```

Note: *By default, SYN-flag checking is enabled.*

Example: Redundant VPN Gateways

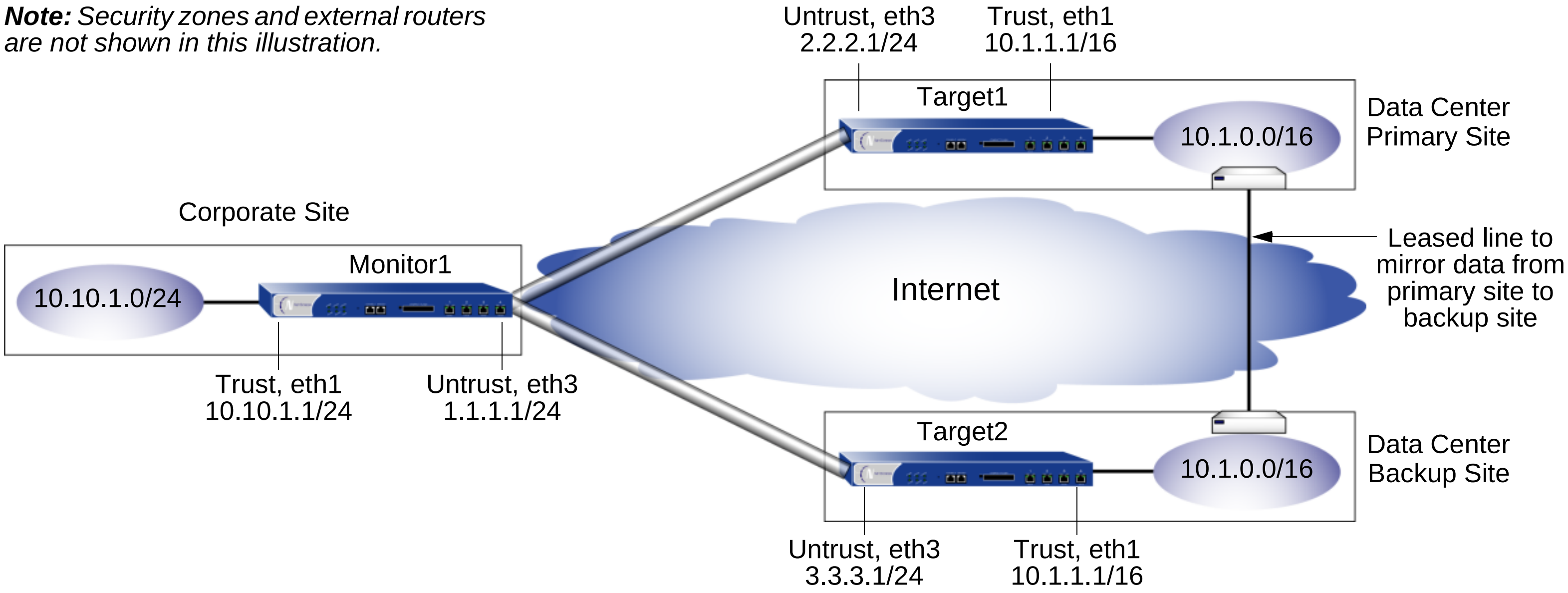
In this example, a corporate site has one VPN tunnel to a data center and a second tunnel to a backup data center. All the data is mirrored via a leased line connection between the two data center sites. The data centers are physically separate to provide continuous service even in the event of a catastrophic failure such as an all-day power outage or a natural disaster.

The device location and name, the physical interfaces and their IP addresses for the Trust and Untrust zones, and the VPN group ID and weight for each NetScreen device are as follows:

Device Location	Device Name	Physical Interface and IP Address (Trust Zone)	Physical Interface, IP Address, Default Gateway (Untrust Zone)	VPN Group ID and Weight
Corporate	Monitor1	ethernet1, 10.10.1.1/24	ethernet3, 1.1.1.1/24, (GW) 1.1.1.2	– –
Data Center (Primary)	Target1	ethernet1, 10.1.1.1/16	ethernet3, 2.2.2.1/24, (GW) 2.2.2.2	ID = 1, Weight = 2
Data Center (Backup)	Target2	ethernet1, 10.1.1.1/16	ethernet3, 3.3.3.1/24, (GW) 3.3.3.2	ID = 1, Weight =1

Note: *The internal address space at both data center sites must be identical.*

All security zones are in the trust-vr routing domain. All the Site-to-Site AutoKey IKE tunnels use the security level predefined as “Compatible” for both Phase 1 and Phase 2 proposals. Preshared keys authenticate the participants.



WebUI (Monitor1)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.10.1.1/24

Enter the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: in_trust

IP Address/Domain Name:

IP/Netmask: (select), 10.10.1.0/24

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: data_ctr

IP Address/Domain Name:

IP/Netmask: (select), 10.1.0.0/16

Zone: Untrust

3. VPNs

VPNs > AutoKey Advanced > VPN Group: Enter 1 in the VPN Group ID field, and then click **Add**.

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: target1

Security Level: Compatible

Remote Gateway Type: Static IP Address: (select), IP Address: 2.2.2.1

Preshared Key: SLi1yoo129

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Compatible

Mode (Initiator): Main (ID Protection)

Heartbeat:

Hello: 3 Seconds

Reconnect: 60 seconds

Threshold: 5

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: to_target1

Security Level: Compatible

Remote Gateway: Predefined: (select), target1

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

VPN Group: VPN Group-1

Weight: 2

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: target2

Security Level: Compatible

Remote Gateway Type: Static IP Address: (select), IP Address: 3.3.3.1

Preshared Key: CMFwb7oN23

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Compatible

Mode (Initiator): Main (ID Protection)

Heartbeat:

Hello: 3 Seconds

Reconnect: 60 seconds

Threshold: 5

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: to_target2

Security Level: Compatible

Remote Gateway: Predefined: (select), target2

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

VPN Group: VPN Group -1

Weight: 1

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.2(untrust)

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), in_trust

Destination Address:

Address Book Entry: (select), data_ctr

Service: ANY

Action: Tunnel

VPN: VPN Group -1

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

WebUI (Target1)

1. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.1.1.1/16

Enter the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.1/24

2. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: in_trust

IP Address/Domain Name:

IP/Netmask: (select), 10.1.0.0/16

Zone: Trust

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (select), 10.10.1.0/24

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: Enter the following, and then click **OK**:

Gateway Name: monitor1

Security Level: Compatible

Remote Gateway Type:

Static IP Address: (select), IP Address/Hostname: 1.1.1.1

Preshared Key: SLi1yoo129

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic Gateway configuration page:

Security Level: Compatible

Mode (Initiator): Main (ID Protection)

Heartbeat:

Hello: 3 Seconds

Reconnect: 0 seconds

VPN > AutoKey IKE > New: Enter the following, and then click **OK**:

Name: to_monitor1

Security Level: Compatible

Remote Gateway: Predefined: (select), monitor1

4. Route

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.2

5. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), in_trust

Destination Address:

Address Book Entry: (select), corp

Service: ANY

Action: Tunnel

Tunnel VPN: monitor1

Modify matching bidirectional VPN policy: (select)

Position at Top: (select)

WebUI (Target2)

> ***Note:*** *Follow the Target1 configuration steps to configure Target2, but define the Untrust zone interface IP address as 3.3.3.1/24, the default gateway IP address as 3.3.3.2, and use CMFwb7oN23 to generate the preshared key.*

CLI (Monitor1)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.10.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. Addresses

```
set address trust in_trust 10.10.1.0/24
set address untrust data_ctr 10.1.0.0/16
```

3. VPNs

```
set ike gateway target1 address 2.2.2.1 main outgoing-interface ethernet3
    preshare SLi1yoo129 sec-level compatible
set ike gateway target1 heartbeat hello 3
set ike gateway target1 heartbeat reconnect 60
set ike gateway target1 heartbeat threshold 5
set vpn to_target1 gateway target1 sec-level compatible
set ike gateway target2 address 3.3.3.1 main outgoing-interface ethernet3
    preshare CMFwb7oN23 sec-level compatible
set ike gateway target2 heartbeat hello 3
set ike gateway target2 heartbeat reconnect 60
set ike gateway target2 heartbeat threshold 5
set vpn to_target2 gateway target2 sec-level compatible
set vpn-group id 1 vpn to_target1 weight 2
set vpn-group id 1 vpn to_target2 weight 1
unset flow tcp-syn-check-in-tunnel
```

4. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.2
```

5. Policies

```
set policy top from trust to untrust in_trust data_ctr any tunnel “vpn-group 1”
set policy top from untrust to trust data_ctr in_trust any tunnel “vpn-group 1”
save
```

CLI (Target1)

1. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/16
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.1/24
```

2. Addresses

```
set address trust in_trust 10.1.0.0/16
set address untrust corp 10.10.1.0/24
```

3. VPN

```
set ike gateway monitor1 address 1.1.1.1 main outgoing-interface ethernet3
    preshare SLi1yoo129 sec-level compatible
set ike gateway monitor1 heartbeat hello 3
set ike gateway monitor1 heartbeat threshold 5
set vpn to_monitor1 gateway monitor1 sec-level compatible
```

4. Route

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.2
```

5. Policies

```
set policy top from trust to untrust in_trust corp any tunnel vpn to_monitor
set policy top from untrust to trust corp in_trust any tunnel vpn to_monitor
save
```

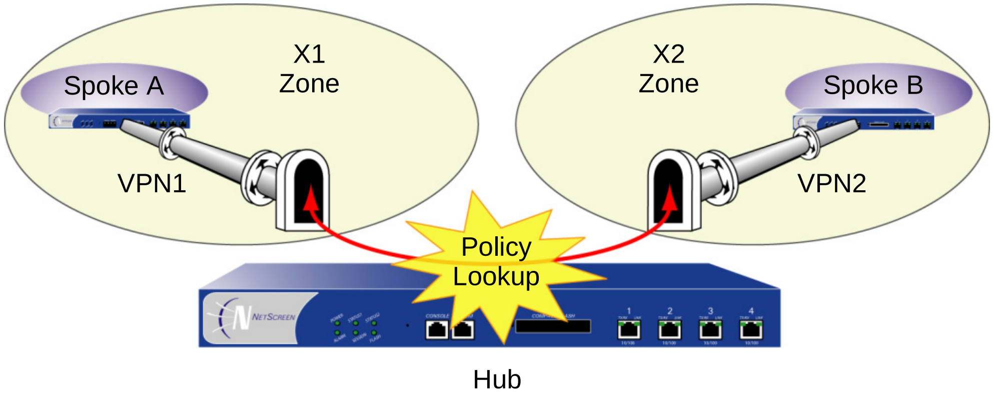
CLI (Target2)

Note: *Follow the Target1 configuration steps to configure Target2, but define the Untrust zone interface IP address as 3.3.3.1/24, the default gateway IP address as 3.3.3.2, and use CMFwb7oN23 to generate the preshared key.*

Back-to-Back VPNs

You can enforce interzone policies at the hub site for traffic passing from one VPN tunnel to another by putting the spoke sites in different zones[20]. Because they are in different zones, the NetScreen device at the hub must do a policy lookup before routing the traffic from one tunnel to another. Thus you can control the traffic flowing via the VPN tunnels between the spoke sites. Such an arrangement is called back-to-back VPNs.

Back-to-Back VPNs



[20] Optionally, you can enable intrazone blocking and define an intrazone policy to control traffic between the two tunnel interfaces within the same zone.

A few benefits of back-to-back VPNs:

- You can conserve the number of VPNs you need to create. For example, perimeter site A can link to the hub, and to perimeter sites B, C, D…, but A only has to set up one VPN tunnel. Especially for NetScreen-5XP users, who can use a maximum of ten VPN tunnels concurrently, applying the hub-and-spoke method dramatically increases their VPN options and capabilities.
- The administrator at the hub device can completely control VPN traffic between perimeter sites. For example,
  - He or she might permit only HTTP traffic to flow from sites A to B, but allow any kind of traffic to flow from B to A.
  - He or she can allow traffic originating from A to reach C, but deny traffic originating from C to reach A.
  - He or she can allow a specific host at A to reach the entire D network, while allowing only a specific host at D to reach a different host at A.
- The administrator at the hub device can completely control outbound traffic from all perimeter networks. At each perimeter site, there must first be a policy that tunnels all outbound traffic through the spoke VPNs to the hub; for example: **set policy top from trust to untrust any any any tunnel vpn** *name_str* (where *name_str* defines the specific VPN tunnel from each perimeter site to the hub). At the hub, the administrator can control Internet access, allowing certain kinds of traffic (such as HTTP only), performing URL blocking on undesirable Web sites, and so on.
- Regional hubs can be used and interconnected via spoke tunnels, allowing spoke sites in one region to reach spoke sites in another.

Example: Back-to-Back VPNs

The following example is similar to “Example: Hub-and-Spoke VPNs” on page 413 except that the NetScreen device at the hub site in New York performs policy checking on the traffic it routes between the two tunnels to the branch offices in Tokyo and Paris. By putting each remote site in a different zone, you control the VPN traffic at the hub.

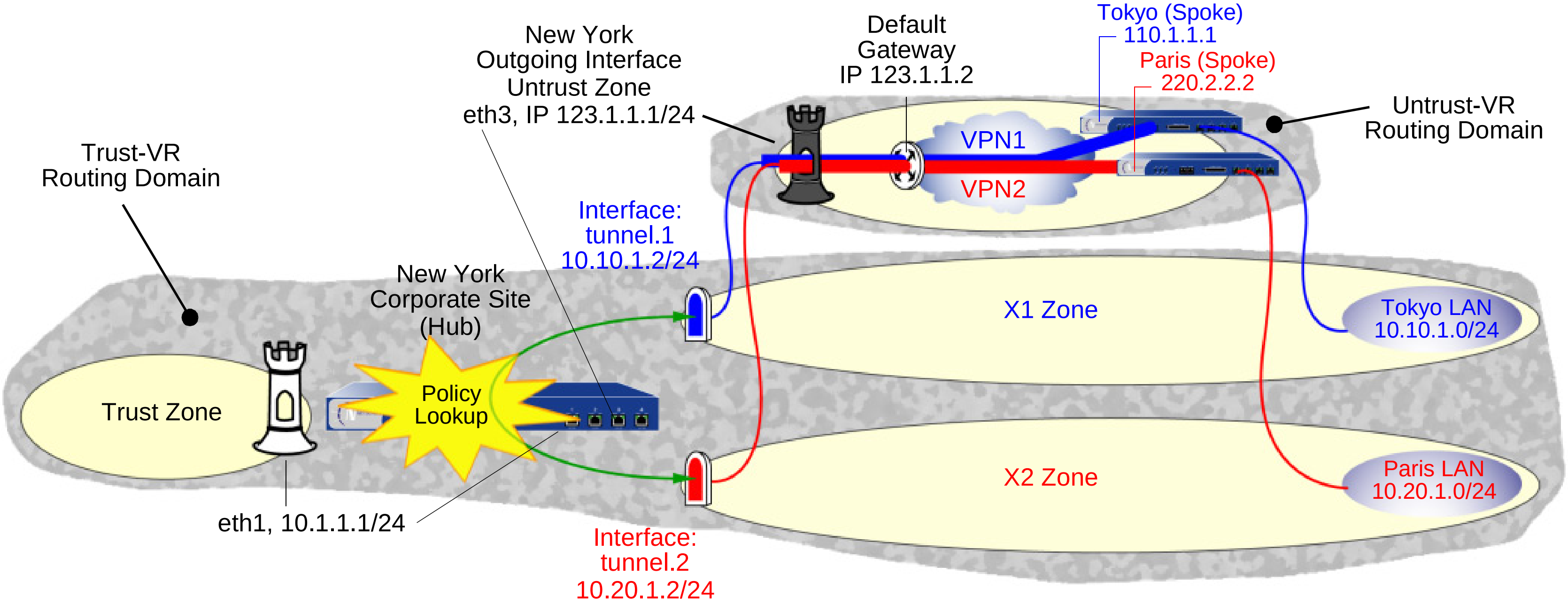
The Tokyo LAN address is in the user-defined X1 zone, and the Paris LAN address is in the user-defined X2 zone. Both zones are in the Trust-VR routing domain.

Note: *To create user-defined zones, you must first obtain and load a zone software key on the NetScreen device.*

You bind the VPN1 tunnel to the tunnel.1 interface and the VPN2 tunnel to the tunnel.2 interface. Although you do not assign IP addresses to the X1 and X2 zone interfaces, you do give addresses to both tunnel interfaces. Routes for these interfaces automatically appear in the Trust-VR routing table. By putting the IP address for a tunnel interface in the same subnet as that of the destination, traffic destined for that subnet is routed to the tunnel interface.

The outgoing interface is ethernet3, which is bound to the Untrust zone. As you can see in the illustration below, both tunnels terminate in the Untrust zone; however, the endpoints for the traffic that makes use of the tunnels are in the X1 and X2 zones. The tunnels use AutoKey IKE, with preshared keys. You select the security level predefined as “Compatible” for both Phase 1 and Phase 2 proposals. You bind the Untrust zone to the untrust-vr. Because the tunnels are route-based (that is, the correct tunnel is determined by routing, not by a tunnel name specified in a policy), proxy IDs are included in the configuration of each tunnel.

Note: *Only the configuration for the NetScreen device at the hub site is provided below.*



WebUI

1. Security Zones and Virtual Routers

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

IP Address/Netmask: 0.0.0.0/0

Manage IP: 0.0.0.0

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Null

Network > Zones > Edit (for Untrust): Enter the following, and then click **OK**:

Virtual Router Name: untrust-vr

Block Intra-Zone Traffic: (select)

Network > Zones > New: Enter the following, and then click **OK**:

Zone Name: X1

Virtual Router Name: trust-vr

Block Intra-Zone Traffic: (select)

Network > Zones > New: Enter the following, and then click **OK**:

Name: X2

Virtual Router Name: trust-vr

Block Intra-Zone Traffic: (select)

2. Interfaces

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 123.1.1.1/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): X1 (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 10.10.1.2/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.2

Zone (VR): X2 (trust-vr)

Fixed IP: (select)

IP Address / Netmask: 10.20.1.2/24

3. VPN for Tokyo Office

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: VPN1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: Tokyo

Type: Static IP: (select), Address/Hostname: 110.1.1.1

Preshared Key: netscreen1

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Proxy-ID: (select)[21]

Local IP / Netmask: 10.20.1.0/24

Remote IP / Netmask: 10.10.1.0/24

Service: ANY

[21] When configuring the VPN tunnel on the NetScreen device protecting the Tokyo and Paris offices, do either of the following:
(Route-based VPN) Select the **Enable Proxy-ID** check box and enter **10.10.1.0/24** (Tokyo) and **10.20.1.0/24** (Paris) for the Local IP and Netmask, and **10.20.1.0/24** (Tokyo) and **10.10.1.0/24** (Paris) for the Remote IP and Netmask.
(Policy-based VPN) Make an entry in the Trust zone address book for 10.10.1.0/24 (Tokyo) and 10.20.1.0/24 (Paris) and another in the Untrust zone address book for 10.20.1.0/24 (Tokyo) and 10.10.1.0/24 (Paris). Use those as the source and destination addresses in the policy referencing the VPN tunnel to the hub site.

4. VPN for Paris Office

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: VPN2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: Paris

Type: Static IP: (select), Address/Hostname: 220.2.2.2

Preshared Key: netscreen2

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Proxy-ID: (select)

Local IP / Netmask: 10.10.1.0/24

Remote IP / Netmask: 10.20.1.0/24

Service: ANY

5. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Next Hop Virtual Router Name: (select), untrust-vr

Network > Routing > Routing Entries > untrust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 123.1.1.2

6. Addresses

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Tokyo LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.10.1.0/24

Zone: X1

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Paris LAN

IP Address/Domain Name:

IP/Netmask: (select), 10.20.1.0/24

Zone: X2

7. Policies

Policy > (From: X1, To: X2) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Tokyo LAN

Destination Address:

Address Book Entry: (select), Paris LAN

Service: ANY

Action: Permit

Position at Top: (select)

Policy > (From: X2, To: X1) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Paris LAN

Destination Address:

Address Book Entry: (select), Tokyo LAN

Service: ANY

Action: Permit

Position at Top: (select)

CLI

1. Security Zones and Virtual Routers

```
unset interface ethernet3 ip
unset interface ethernet3 zone
set zone untrust vrouter untrust-vr
set zone untrust block
set zone name X1
set zone x1 vrouter trust-vr
set zone x1 block
set zone name x2
set zone x2 vrouter trust-vr
set zone x2 block
```

2. Interfaces

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 123.1.1.1/24
set interface tunnel.1 zone x1
set interface tunnel.1 ip 10.10.1.2/24
set interface tunnel.2 zone x2
set interface tunnel.2 ip 10.20.1.2/24
```

3. VPN for Tokyo Office

```
set ike gateway Tokyo address 110.1.1.1 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn VPN1 gateway Tokyo sec-level compatible
set vpn VPN1 bind interface tunnel.1
set vpn VPN1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.10.1.0/24 any[22]
```

4. VPN for Paris Office

```
set ike gateway Paris address 220.2.2.2 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
```

```
set vpn VPN2 gateway Paris sec-level compatible
set vpn VPN2 bind interface tunnel.2
set vpn VPN2 proxy-id local-ip 10.10.1.0/24 remote-ip 10.20.1.0/24 any
```

5. Routes

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 123.1.1.2
```

6. Addresses

```
set address x1 “Tokyo LAN” 10.10.1.0/24
set address x2 “Paris LAN” 10.20.1.0/24
```

7. Policies

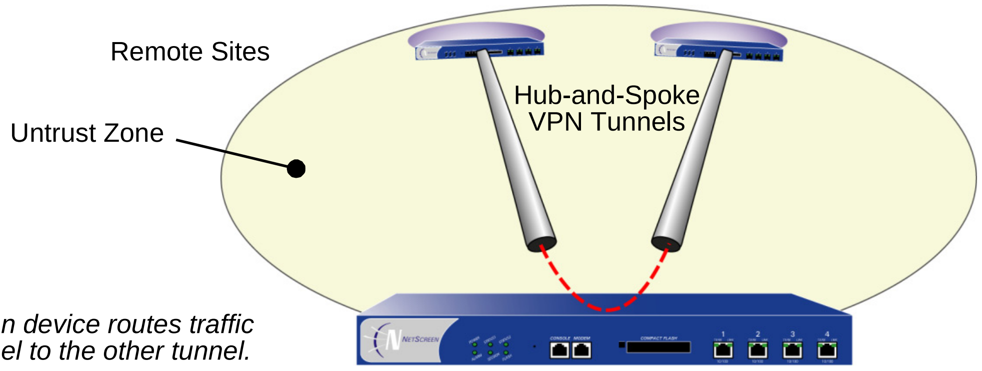
```
set policy top from x1 to x2 “Tokyo LAN” “Paris LAN” any permit[23]
set policy top from x2 to x1 “Paris LAN” “Tokyo LAN” any permit
save
```

[22] When configuring the VPN tunnel on the NetScreen device protecting the Tokyo and Paris offices, do either of the following:
(Route-based VPN) Enter the following commands: **set vpn VPN1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.10.1.0/24** (Tokyo) and **set vpn VPN1 proxy-id local-ip 10.10.1.0/24 remote-ip 10.20.1.0/24** (Paris).
(Policy-based VPN) Make an entry in the Trust zone address book for 10.10.1.0/24 (Tokyo) and 10.20.1.0/24 (Paris) and another in the Untrust zone address book for 10.20.1.0/24 (Tokyo) and 10.10.1.0/24 (Paris). Use those as the source and destination addresses in the policies referencing the VPN tunnel to the hub site.

[23] You can ignore the following message, which appears because tunnel interfaces are in NAT mode: *Warning: Some interfaces in the <zone_name> zone are in NAT mode. Traffic might not pass through them!*

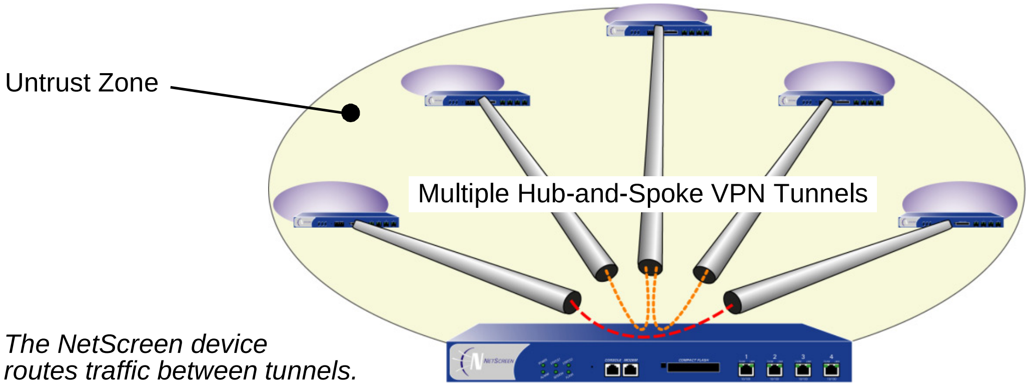
Hub-and-Spoke VPNs

If you create two VPN tunnels that terminate at a NetScreen device, you can set up a pair of routes so that the NetScreen device directs traffic exiting one tunnel to the other tunnel. If both tunnels are contained within a single zone, you do not need to create a policy to permit the traffic to pass from one tunnel to the other. You only need to define the routes. Such an arrangement is known as hub-and-spoke VPNs.



The NetScreen device routes traffic from one tunnel to the other tunnel.

You can also configure multiple VPNs in one zone and route traffic between any two tunnels.



The NetScreen device routes traffic between tunnels.

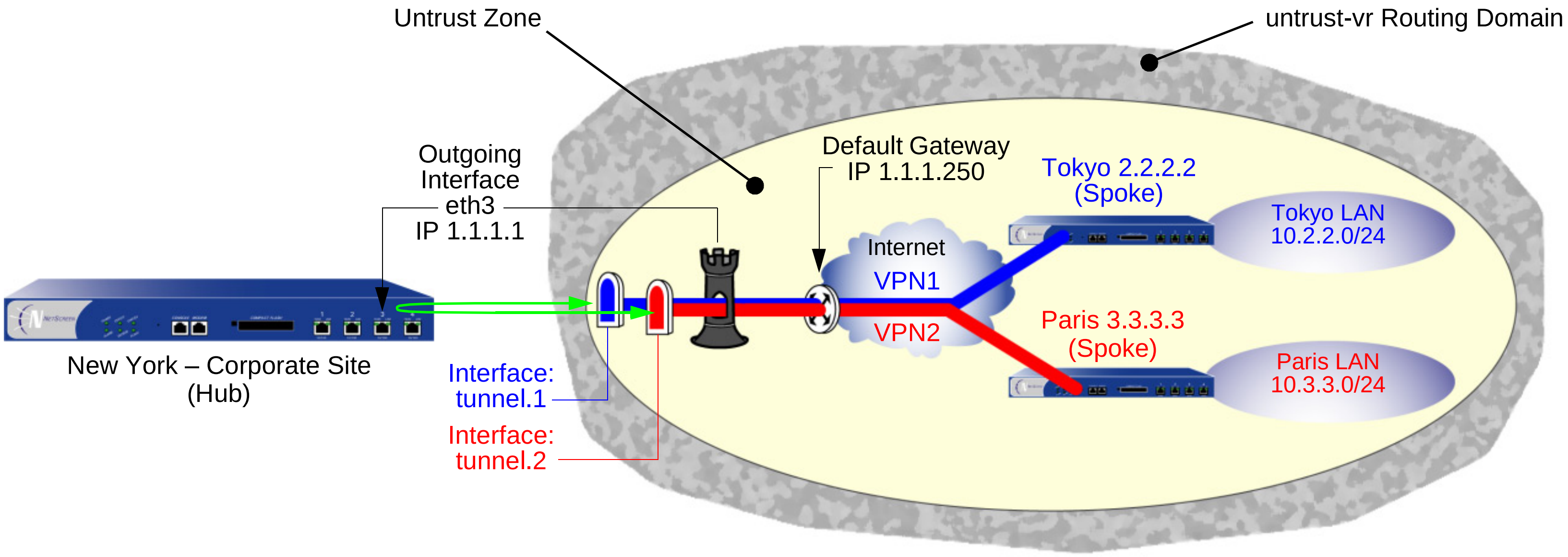
Example: Hub-and-Spoke VPNs

In this example, two branch offices in Tokyo and Paris communicate with each other via a pair of VPN tunnels—VPN1 and VPN2. Each tunnel originates at the remote site and terminates at the corporate site in New York. The NetScreen device at the corporate site routes traffic exiting one tunnel into the other tunnel.

By disabling intrazone blocking, the NetScreen device at the corporate site only needs to do a route lookup—not a policy lookup—when conducting traffic from tunnel to tunnel because both remote endpoints are in the same zone (the Untrust Zone)[24].

You bind the tunnels to the tunnel interfaces—tunnel.1 and tunnel.2—which are both unnumbered. The tunnels use AutoKey IKE, with the preshared keys. You select the security level predefined as “Compatible” for both Phase 1 and Phase 2 proposals. You bind the Untrust zone to the untrust-vr. The Untrust zone interface is ethernet3.

Note: *The following configuration is for route-based VPNs. If you configure policy-based hub-and-spoke VPNs, you must use the Trust and Untrust zones in the policies; you cannot use user-defined security zones.*



[24] Optionally, you can leave intrazone blocking enabled and define an intrazone policy permitting traffic between the two tunnel interfaces.

WebUI (New York)

1. Security Zones and Virtual Routers

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

IP Address/Netmask: 0.0.0.0/0

Manage IP: 0.0.0.0

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Null

Network > Zones > Edit (for Untrust): Enter the following, and then click **OK**:

Virtual Router Name: untrust-vr

Block Intra-Zone Traffic: (clear)

2. Interfaces

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (untrust-vr)

Unnumbered: (select)

Interface: ethernet3 (untrust-vr)

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.2

Zone (VR): Untrust (untrust-vr)

Unnumbered: (select)

Interface: ethernet3 (untrust-vr)

3. VPN for Tokyo Office

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: VPN1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: Tokyo

Type: Static IP: (select), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. VPN for Paris Office

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: VPN2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: Paris

Type: Static IP: (select), Address/Hostname: 3.3.3.3

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

5. Routes

Network > Routing > Routing Entries > untrust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.2.2.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > untrust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.3.3.0/24

Gateway: (select)

Interface: tunnel.2

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > untrust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

WebUI (Tokyo)

1. Security Zones and Virtual Routers

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

IP Address/Netmask: 0.0.0.0/0

Manage IP: 0.0.0.0

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Null

Network > Zones > Edit (for Untrust): Enter the following, and then click **OK**:

Virtual Router Name: untrust-vr

Block Intra-Zone Traffic: (select)

2. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.2.2.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (untrust-vr)

Unnumbered: (select)

Interface: ethernet3 (untrust-vr)

3. Address

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Paris

IP Address/Domain Name:

IP/Netmask: (select), 10.3.3.0/24

Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: VPN1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: New York

Type: Static IP: (select), Address/Hostname: 1.1.1.1

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

5. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Next Hop Virtual Router Name: (select); untrust-vr

Network > Routing > Routing Entries > untrust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > untrust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.3.3.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

6. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Any

Destination Address:

Address Book Entry: (select), Paris

Service: ANY

Action: Permit

WebUI (Paris)

1. Security Zones and Virtual Routers

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

IP Address/Netmask: 0.0.0.0/0

Manage IP: 0.0.0.0

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Null

Network > Zones > Edit (for Untrust): Enter the following, and then click **OK**:

Virtual Router Name: untrust-vr

Block Intra-Zone Traffic: (select)

2. Interfaces

Network > Interfaces > Edit (for ethernet1): Enter the following, and then click **Apply**:

Zone Name: Trust

Static IP: (select this option when present)

IP Address/Netmask: 10.3.3.1/24

Select the following, and then click **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (for ethernet3): Enter the following, and then click **OK**:

Zone Name: Untrust

Static IP: (select this option when present)

IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > New Tunnel IF: Enter the following, and then click **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (untrust-vr)

Unnumbered: (select)

Interface: ethernet3 (untrust-vr)

3. Address

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: Tokyo

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.0/24

Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: Enter the following, and then click **OK**:

VPN Name: VPN2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (select)

Gateway Name: New York

Type: Static IP: (select), Address/Hostname: 1.1.1.1

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: Enter the following advanced settings, and then click **Return** to return to the basic AutoKey IKE configuration page:

Proxy-ID: (select)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

5. Routes

Network > Routing > Routing Entries > trust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Next Hop Virtual Router Name: (select); untrust-vr

Network > Routing > Routing Entries > untrust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 0.0.0.0/0

Gateway: (select)

Interface: ethernet3

Gateway IP Address: 3.3.3.250

Network > Routing > Routing Entries > untrust-vr New: Enter the following, and then click **OK**:

Network Address / Netmask: 10.2.2.0/24

Gateway: (select)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

6. Policies

Policies > (From: Trust, To: Untrust) New: Enter the following, and then click **OK**:

Source Address:

Address Book Entry: (select), Any

Destination Address:

Address Book Entry: (select), Tokyo

Service: ANY

Action: Permit

CLI (New York)

1. Security Zones and Virtual Routers

```
unset interface ethernet3 ip
unset interface ethernet3 zone
set zone untrust vrouter untrust-vr
unset zone untrust block
```

2. Interfaces

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.2 zone untrust
set interface tunnel.2 ip unnumbered interface ethernet3
```

3. VPN for Tokyo Office

```
set ike gateway Tokyo address 2.2.2.2 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn VPN1 gateway Tokyo sec-level compatible
set vpn VPN1 bind interface tunnel.1
set vpn VPN1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. VPN for Paris Office

```
set ike gateway Paris address 3.3.3.3 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn VPN2 gateway Paris sec-level compatible
set vpn VPN2 bind interface tunnel.2
set vpn VPN2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. Routes

```
set vrouter untrust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter untrust-vr route 10.3.3.0/24 interface tunnel.2
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
save
```

CLI (Tokyo)

1. Security Zones and Virtual Routers

```
unset interface ethernet3 ip
unset interface ethernet3 zone
set zone untrust vrouter untrust-vr
```

2. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

3. Address

```
set address untrust Paris 10.3.3.0/24
```

4. VPN

```
set ike gateway “New York” address 1.1.1.1 outgoing-interface ethernet3
    preshare netscreen1 sec-level compatible
set vpn VPN1 gateway “New York” sec-level compatible
set vpn VPN1 bind interface tunnel.1
set vpn VPN1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. Routes

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter untrust-vr route 10.3.3.0/24 interface tunnel.1
```

6. Policies

```
set policy from trust to untrust any Paris any permit
set policy from untrust to trust Paris any any permit
save
```

CLI (Paris)

1. Security Zones and Virtual Routers

```
unset interface ethernet3 ip
unset interface ethernet3 zone
set zone untrust vrouter untrust-vr
```

2. Interfaces

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.3.3.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

3. Address

```
set address untrust Tokyo 10.2.2.0/24
```

4. VPN

```
set ike gateway “New York” address 1.1.1.1 outgoing-interface ethernet3
    preshare netscreen2 sec-level compatible
set vpn VPN2 gateway “New York” sec-level compatible
set vpn VPN2 bind interface tunnel.1
set vpn VPN2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 an
```

5. Routes

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250
set vrouter untrust-vr route 10.2.2.0/24 interface tunnel.1
```

6. Policies

```
set policy from trust to untrust any Tokyo any permit
set policy from untrust to trust Tokyo any any permit
save
```

Index

Symbols

3DES 8

A

AES (Advanced Encryption Standard) 8
Aggressive Mode 12
AH 3, 7
anti-replay checking 46, 54
attacks
  Replay 14
authentication
  algorithms 7, 44, 49, 53, 57
Authentication Header
  See AH
AutoKey IKE VPN 9
  management 9

C

CA certificates 18, 22
certificates 10
  CA 18, 22
  loading 26
  local 22
  requesting 23
  revocation 21, 36
  via e-mail 22
Challenge Handshake Authentication Protocol
  See CHAP
CHAP 273, 276
character types, ScreenOS supported x
CLI
  conventions vi
container 242
conventions
  CLI vi
  illustration ix
  names x
  WebUI vii
CRL (Certificate Revocation List) 20, 36
  loading 20
cryptographic options 40–57
  anti-replay checking 46, 54
  authentication algorithms 44, 49, 53, 57
  authentication types 42, 51
  certificate bit lengths 43, 51
  dialup 50–57
  dialup VPN recommendations 57
  Diffie-Hellman groups 43, 46, 52, 55
  encryption algorithms 44, 48, 52, 57
  ESP 48, 56
  IKE ID 44–46, 53–54
  IPSec protocols 47, 56
  key methods 42
  PFS 46, 55
  Phase 1 modes 42, 51
  site-to-site 41–49
  site-to-site VPN recommendations 49
  Transport mode 56
  Tunnel mode 56

D

Data Encryption Standard
  See DES
DES 8
Diffie-Hellman exchange 13
Diffie-Hellman groups 13, 43, 46, 52, 55
digital signature 16
DIP pools
  extended interfaces 168
  NAT for VPNs 168
DN (distinguished name) 237
DNS
  L2TP settings 276

E

Encapsulating Security Payload
  See ESP
encryption
  algorithms 8, 44, 48, 52, 57
ESP 3, 7, 8
  authenticate only 48
  encrypt and authenticate 48, 56
  encrypt only 48

G

group IKE ID
  certificates 238–249
  preshared key 250–258
group IKE ID user 237–258
  certificates 238
  preshared key 250

H

hash-based message authentication code
  See HMAC
HMAC 7

I

IKE 9, 77, 91, 201
  group IKE ID user 237–258
  group IKE ID, container 242
  group IKE ID, wildcard 241
  heartbeats 384
  hello messages 384
  IKE ID 44–46, 53–54
  IKE ID recommendations 68
  IKE ID, Windows 200 288
  local ID, ASN1-DN 240
  Phase 1 proposals, predefined 11
  Phase 2 proposals, predefined 14
  proxy IDs 14
  redundant gateways 382–400
  remote ID, ASN1-DN 240
  shared IKE ID user 259–267
illustration
  conventions ix

interfaces
- extended 168

Internet Key Exchange
- *See* IKE

IP addresses
- extended 168

IP Security
- *See* IPSec

IPSec 3
- AH 2, 47, 56
- digital signature 16
- ESP 2, 47, 56
- SAs 2, 10, 11, 13
- SPI 2
- transport mode 4, 273, 279, 286
- tunnel 2
- tunnel mode 5
- tunnel negotiation 11

K

keepalive
- frequency, NAT-T 303
- L2TP 283

L

L2TP 269–298
- access concentrator, *See* LAC
- compulsory configuration 270
- decapsulation 275
- default parameters 276
- encapsulation 274
- hello signal 284
- Keep Alive 283, 284
- L2TP-only on Windows 2000 273
- network server, *See* LNS
- operational mode 273
- RADIUS server 276
- ScreenOS support 273
- SecurID server 276
- tunnel 279
- voluntary configuration 270
- Windows 2000 291
- Windows 2000 tunnel authentication 283

L2TP-over-IPSec 4, 279, 286
- tunnel 279

LAC 270
- NetScreen-Remote 5.0 270
- Windows 2000 270

Layer 2 Tunneling Protocol
- *See* L2TP

LNS 270

local certificate 22

M

Main Mode 12

Manual Key 131, 142
- management 9

MD5 7

Message Digest version 5
- *See* MD5

MIB files, importing 325

MIP
- VPNs 168

modulus 13

N

names
- conventions x

NAT
- IPSec and NAT 301
- NAT servers 301

NAT-dst
- VPNs 168

NAT-src
- VPNs 171

NAT-T 301
- enabling 305
- keepalive frequency 303

NAT-Traversal
- *See* NAT-T

NetScreen-Remote
- AutoKey IKE VPN 201
- dynamic peer 209, 220
- NAT-T option 301

NHTB table 326–331
- addressing scheme 328
- automatic entries 331
- manual entries 330
- mapping routes to tunnels 327

O

OCSP (Online Certificate Status Protocol) 36
- client 36
- responder 36

P

packet flow
- inbound VPN 63–64
- outbound VPN 61–62
- policy-based VPN 65–66
- route-based VPN 60–64

PAP 273, 276

Password Authentication Protocol
- *See* PAP

Perfect Forward Secrecy
- See PFS

PFS 14, 46, 55

Phase 1 11
- proposals 11
- proposals, predefined 11

Phase 2 13
- proposals 13
- proposals, predefined 14

PKI 18

Point-to-Point Protocol
- *See* PPP

policies
- bidirectional VPNs 143

policy-based VPNs 58

PPP 271

preshared key 9, 201

proposals
- Phase 1 11, 67
- Phase 2 13, 67

protocols
- CHAP 273
- PAP 273
- PPP 271

proxy IDs 14
- matching 67
- VPNs and NAT 168–169

- Public key infrastructure
  - *See* PKI
- Public/private key pair 19

R

- RADIUS
  - L2TP 276
- redundant gateways 382–400
  - recovery procedure 385
  - TCP SYN flag checking 388
- rekey option, VPN monitoring 308
- replay protection 14
- route-based VPNs 58

S

- SAs 10, 11, 13
  - check in packet flow 62
- SCEP (Simple Certificate Enrollment Protocol) 30
- Secure Hash Algorithm-1
  - *See* SHA-1
- SecurID
  - L2TP 276
- security association
  - *See* SAs
- SHA-1 7
- SNMP
  - MIB files, importing 325
  - VPN monitoring 325

T

- TCP
  - SYN flag checking 388
- transport mode 4, 273, 279, 286
- Triple DES
  - *See* 3DES
- tunnel mode 5

U

- UDP
  - checksum 303
  - NAT-T encapsulation 301
- users
  - group IKE ID 237–258
  - shared IKE ID 259–267

V

- Valicert 36
- Verisign 36
- VPN monitoring 307–322
  - destination address 308–311
  - destination address, XAuth 309
  - ICMP echo requests 325
  - outgoing interface 308–311
  - policies 310
  - rekey option 308, 331
  - routing design 323
  - SNMP 325
  - status changes 307, 310
- VPNs
  - Aggressive mode 12
  - AutoKey IKE 9
  - configuration tips 67–68
  - cryptographic options 40–57
  - Diffie-Hellman exchange 13
  - Diffie-Hellman groups 13
  - FQDN aliases 152
  - FQDN for gateway 151–167
  - Main mode 12
  - MIP 168
  - multiple tunnels per tunnel interface 326–381
  - NAT for overlapping addresses 168–185
  - NAT-dst 168
  - NAT-src 171
  - packet flow 60–66
  - Phase 1 11
  - Phase 2 13
  - proxy IDs, matching 67
  - redundant gateways 382–400
  - redundant groups, recovery procedure 385
  - replay protection 14
  - route- vs policy-based 58
  - SAs 10
  - tunnel always up 308
  - VPN groups 382
  - VPN monitoring and rekey 308

W

- WebUI
  - conventions vii
- wildcard 241
- WINS
  - L2TP settings 276

X

- XAuth
  - VPN monitoring 309