

Virtual Private Networks

1 Introduction

With SSL and IPsec virtual private networks (VPNs), businesses can securely connect remote offices and remote users using cost-effective, third-party Internet access rather than expensive dedicated WAN links or long-distance remote dial links.

Organizations can reduce WAN bandwidth costs while increasing connectivity speeds by using high-bandwidth Internet connectivity, such as DSL, Ethernet, and cable, and securing it with encrypted IPsec or SSL VPN tunnels.

VPNs provide the highest possible level of security through encryption and authentication technologies that protect data traversing the VPN from unauthorized access. Organizations can take advantage of the easy-to-provision Internet infrastructure to quickly add new sites or users, and can dramatically increase the reach of their networks without significantly expanding infrastructure.

IPSec provides authentication and encryption services to protect unauthorized viewing or modification of data within your network or as it is transferred over an unprotected network, such as the public Internet. IPSec is generally implemented in two types of configurations:

1. Site-to-site—This configuration is used between two IPSec security gateways, such as PIX Firewall units. A site-to-site VPN interconnects networks in different geographic locations.
2. Remote access—This configuration is used to allow secure remote access for VPN clients, such as mobile users. A remote access VPN allows remote users to securely access centralized network resources.

Two different security protocols are included within the IPSec standard:

1. Encapsulating Security Protocol (ESP)—Provides authentication, encryption, and anti-replay services.
2. Authentication Header (AH)—Provides authentication and anti-replay services.

IPSec can be configured to work in two different modes:

1. Tunnel Mode—This is the normal way in which IPSec is implemented between two PIX Firewall units (or other security gateways) that are connected over an untrusted network, such as the public Internet.
2. Transport Mode—This method of implementing IPSec is typically done with L2TP to allow authentication of native Windows 2000 VPN clients.

The main task of IPSec is to allow the exchange of private information over an insecure connection. IPSec uses encryption to protect information from interception or eavesdropping. However, to use

encryption efficiently, both parties should share a secret that is used for both encryption and decryption of the information.

IPSec operates in two phases to allow the confidential exchange of a shared secret:

Phase 1, which handles the negotiation of security parameters required to establish a secure channel between two IPSec peers. Phase 1 is generally implemented through the Internet Key Exchange (IKE) protocol. If the remote IPSec peer cannot perform IKE, you can use manual configuration with pre-shared keys to complete Phase 1.

Phase 2, which uses the secure tunnel established in Phase 1 to exchange the security parameters required to actually transmit user data.

The secure tunnels used in both phases of IPSec are based on security associations (SAs) used at each IPSec end point. SAs describe the security parameters, such as the type of authentication and encryption that both end points agree to use.

2 Site-to-Site VPN

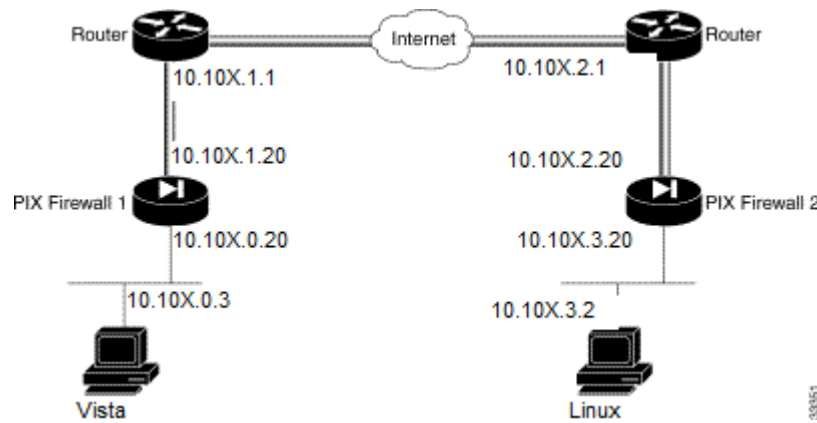


Figure 1: VPN Tunnel Network

In the example illustrated in Figure 1, the intranets use unregistered addresses and are connected over the public Internet by a site-to-site VPN. In this scenario, NAT is required for connections to the public Internet. However, NAT is not required for traffic between the two intranets, which can be transmitted using a VPN tunnel over the public Internet.

2.1 Routers

You will need to configure the routing tables on PIX Firewalls 1 and 2 as well as Routers 1 and 2. Set the default route of the Vista and Linux hosts to the interface of their respective PIX Firewall as they (the hosts) only have single points of egress.

2.2 Firewalls

Before you begin to configure the VPN, set the outside and inside interfaces of each Firewall and ensure that it is not shutdown.

Follow these steps to configure PIX Firewall 1:

Step 1 Define a host name:

```
hostname Vista
```

Step 2 Configure an ISAKMP policy:

```
isakmp enable outside
isakmp policy 9 authentication pre-share
isakmp policy 9 encrypt des
```

Step 3 Configure a pre-shared key and associate with the peer:

```
crypto isakmp key cisco1234 address 10.10X.2.20
```

Step 4 Configure the supported IPsec transforms:

```
crypto ipsec transform-set strong esp-des esp-sha-hmac
```

Step 5 Create an access list:

```
access-list 90 extended permit ip 10.10X.0.0 255.255.255.0 10.10X.3.0
255.255.255.0
```

This access list defines traffic from network 10.10X.0.0 to 10.10X.3.0. Both of these networks use unregistered addresses.

Note Steps 5 and 6 are not required if you want to enable NAT for all traffic.

Step 6 Exclude traffic between the intranets from NAT:

```
nat (inside) 0 access-list 90
```

This excludes traffic matching access list 90 from NAT. The **nat 0** command is always processed before any other **nat** commands.

Step 7 Enable NAT for all other traffic:

```
nat (inside) 1 0 0
```

Step 8 Assign a pool of global addresses for NAT and PAT:

```
global (outside) 1 10.10X.4.51-10.10X.4.59
global (outside) 1 10.10X.4.60
```

The pool of registered addresses are only used for connections to the public Internet.

Step 9 Define a crypto map:

```
crypto map toLinux 20 ipsec-isakmp
crypto map toLinux 20 match address 90
crypto map toLinux 20 set transform-set strong
crypto map toLinux 20 set peer 10.10X.3.20
```

Step 10 Apply the crypto map to the outside interface:

```
crypto map toLinux interface outside
```

Step 11 Specify that VPN traffic be implicitly trusted (permitted):

```
sysopt connection permit-vpn
```

Follow these steps to configure PIX Firewall 2:

Step 1 Define a host name:

```
hostname Linux
```

Step 2 Create a net static:

```
static (inside,outside) 10.10X.3.0 10.10X.3.0 netmask 255.255.255.0
```

Step 3 Configure the ISAKMP policy:

```
isakmp enable outside  
isakmp policy 8 authentication pre-share  
isakmp policy 8 encryption des
```

Step 4 Configure a pre-shared key and associate it with the peer:

```
crypto isakmp key cisco1234 address 10.10X.1.20
```

Step 5 Configure IPsec supported transforms:

```
crypto ipsec transform-set strong esp-des esp-sha-hmac
```

Step 6 Create an access list:

```
access-list 80 permit ip 10.10X.3.0 255.255.255 10.10X.0.0 255.255.255.0
```

This access list defines traffic from network 10.0.0.0 to 192.168.12.0. Both of these networks use unregistered addresses.

Note Step 7 and Step 8 are not required if you want to enable NAT for all traffic.

Step 7 Exclude traffic between the intranets from NAT:

```
nat (inside) 0 access-list 80
```

This excludes traffic matching access list 80 from NAT. The **nat 0** command is always processed before any other **nat** commands.

Step 8 Enable NAT for all other traffic:

```
nat (inside) 1 0 0
```

Step 9 Assign a pool of global addresses for NAT and PAT:

```
global (outside) 1 10.10X.4.61-10.10X.4.69  
global (outside) 1 10.10X.4.70
```

The pool of registered addresses are only used for connections to the public Internet.

Step 10 Define a crypto map:

```
crypto map toVista 10 ipsec-isakmp  
crypto map toVista 10 match address 80  
crypto map toVista 10 set transform-set strong  
crypto map toVista 10 set peer 10.10X.1.20
```

Step 11 Apply the crypto map to an interface:

```
crypto map toVista interface outside
```

Step 12 Specify that VPN traffic be implicitly trusted (permitted):
`sysopt connection permit-vpn`

2.3 Experiment

Verify network connectivity end-to-end. The Vista host should be able to PING/SSH into the Linux Host. If you run into trouble, ensure that your routing tables are correct and make use of the **logging console informational** command on the Firewalls. Compare the running configurations on the Firewalls, they should “mirror” each other. Also be sure to disable the Wireless NIC on the Vista Host and delete any extra default gateways on the Linux Host.