



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957

Fax: 919.217.5769

SETTING UP A CISCO PIX TO CISCO VPN 3000 IPSEC VPN

Products: Cisco Secure PIX Firewall; Cisco VPN 30xx Series Concentrator

Overview

This technical document describes how to create an encrypted VPN tunnel between a Cisco Secure PIX 515 firewall and a Cisco VPN 30xx Series VPN concentrator. This would allow offices to use the Internet as a transport without sacrificing security, as traffic passing across the Internet would be encrypted and verified using industry standard algorithms.

Please note that it should be possible to use the PIX configuration commands contained in this document to also create a PIX-to-PIX VPN tunnel.

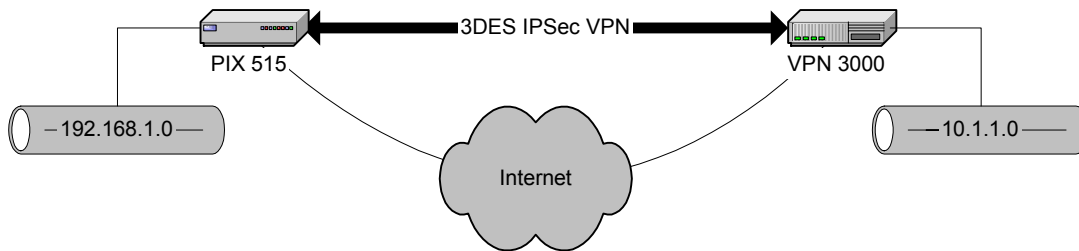


Figure 1. PIX 515 to VPN 3000 IPsec VPN

The PIX configurations outlined in this document, while written for a PIX 515, are applicable to any PIX 5xx firewall (including PIX 506, 520, 525, and 535) with a 3DES IPsec license key and version 5.x of the Cisco Secure PIX firewall software. This document was written using version 5.2(1) of the Cisco Secure PIX firewall software.

More Information

The sections below provide more information on how to configure each end-device in the VPN tunnel (the PIX firewall and the VPN 30xx Series Concentrator). Refer to Figure 1 for more information on the network addresses and devices referenced in the following sections.

Configuring the PIX Firewall

To configure the PIX firewall for a VPN with a VPN 30xx Series Concentrator, a series of commands need to be added to the PIX configuration. These commands are included below, along with a brief description or explanation of the command and its purpose.

```
access-list 101 permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0
nat (inside) 0 access-list 101
```

These two commands define an extended access list and apply that access list to a NAT statement that disables network address translation (NAT). These commands are critical because they define the TCP/IP address spaces that will be connected via the encrypted tunnel. As shown in Figure 1, the VPN connects two networks, 192.168.1.0/24 and 10.1.1.0/24, across the Internet. The access list defines 192.168.1.0/24 as the source network (the network behind the PIX 515 firewall) and 10.1.1.0/24 as the destination network (the network behind the VPN 3000 concentrator at the other end of the tunnel). If additional networks existed behind either the PIX 515 firewall or VPN 3000 concentrator, they would need to be added to this access list.

The `nat` command specifies that any traffic matching access-list 101 will not be translated. This prevents the PIX firewall's NAT engine from attempting to apply address translation rules to traffic passing between networks inside the VPN tunnel.

```
sysopt connection permit-ipsec
```

This command allows IPSec traffic to be passed through the PIX firewall. Otherwise, IPSec traffic would be denied by the firewall and the VPN tunnel would never be established.

```
crypto ipsec transform-set combined-3des-md5 esp-3des esp-md5-hmac
```

This command creates a transform set called "combined-3des-md5". This transform set will use both an ESP (Encapsulating Security Payload) encryption transform (Triple DES, or 168-bit) as well as an ESP authentication transform (MD5-HMAC). Multiple transform sets can be created.

```
isakmp enable outside
isakmp key cisco address 199.72.1.1 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 28800
```

These commands enable and configure ISAKMP (Internet Security and Key Management Protocol). IPSec peers use ISAKMP to negotiate the parameters of an SA (Security Association). The SA defines which encryption and authentication algorithms the peers will use in their communications. These commands define a preshared key ("cisco") and associate that key with a specific peer (the VPN 3000), specify that the preshared key should be used for authentication, apply Triple DES encryption and MD5 hashes to the ISAKMP traffic, specify Diffie-Helman Group 1 keys, and specify the key lifetime. It is possible to define multiple ISAKMP policies; they are weighted according to importance (hence the 10 in the `isakmp policy` commands above; this specifies the weight of this particular ISAKMP policy).

```
crypto map vpn3000 10 ipsec-isakmp
crypto map vpn3000 10 match address 101
crypto map vpn3000 10 set peer 199.72.1.1
crypto map vpn3000 10 set transform-set combined-3des-md5
crypto map vpn3000 interface outside
```

These commands tie everything else together. ISAKMP is specified for SA negotiation, and the cryptography rules are applied to all traffic matching access list 101. As you can see, the access list is very important because it not only prevents unwanted network address translation from occurring but also enforces the IPSec parameters. The access list defines the networks that are

serviced by the VPN, and the `crypto map match address` command causes all traffic between the private networks to actually pass inside the encrypted tunnel. The remaining commands define the IPSec peer, specify the transform to be used, and apply the cryptography rules to the outside interface.

Once these commands have been entered into the PIX and saved, then the VPN 30xx Series concentrator needs to be configured.

Configuring the VPN Concentrator

Configuring the VPN concentrator is fairly straightforward, due to the graphical HTTP interface provided by the VPN 3000 series.

First, the IPSec LAN-to-LAN tunnel is defined. Note that in defining the IPSec LAN-to-LAN tunnel, the authentication method (ESP/MD5/HMAC-128) and encryption method (3DES-168) matched the commands in the PIX 515 firewall that defined the IPSec transform set. The peer was specified as the PIX 515 firewall, and a matching preshared key was added the VPN concentrator (the same preshared key used on the PIX firewall).

The screenshot shows the 'VPN 3000 Concentrator Series Manager' web interface. The breadcrumb trail is 'Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add'. The main content area is titled 'Add a new IPSec LAN-to-LAN connection.' and contains the following configuration fields:

- Name:** PIX515
- Interface:** Ethernet 2 (Public) (208.242.43.104)
- Peer:** 216.231.59.60
- Digital Certificate:** None (Use Preshared Keys)
- Preshared Key:** cisco
- Authentication:** ESP/MD5/HMAC-128
- Encryption:** 3DES-168
- IKE Proposal:** IKE-DES-MD5
- Network Autodiscovery:**

Help text for each field is provided on the right side of the form. The Cisco Systems logo is visible in the bottom left corner of the interface.

Figure 2. Creating a LAN-to-LAN Definition, Part 1

Farther down on the same screen are areas for defining the local network and remote network. This lets the VPN 3000 concentrator know what networks to expect behind itself and behind the PIX 515 at the other end.

This is illustrated in the following screenshot.

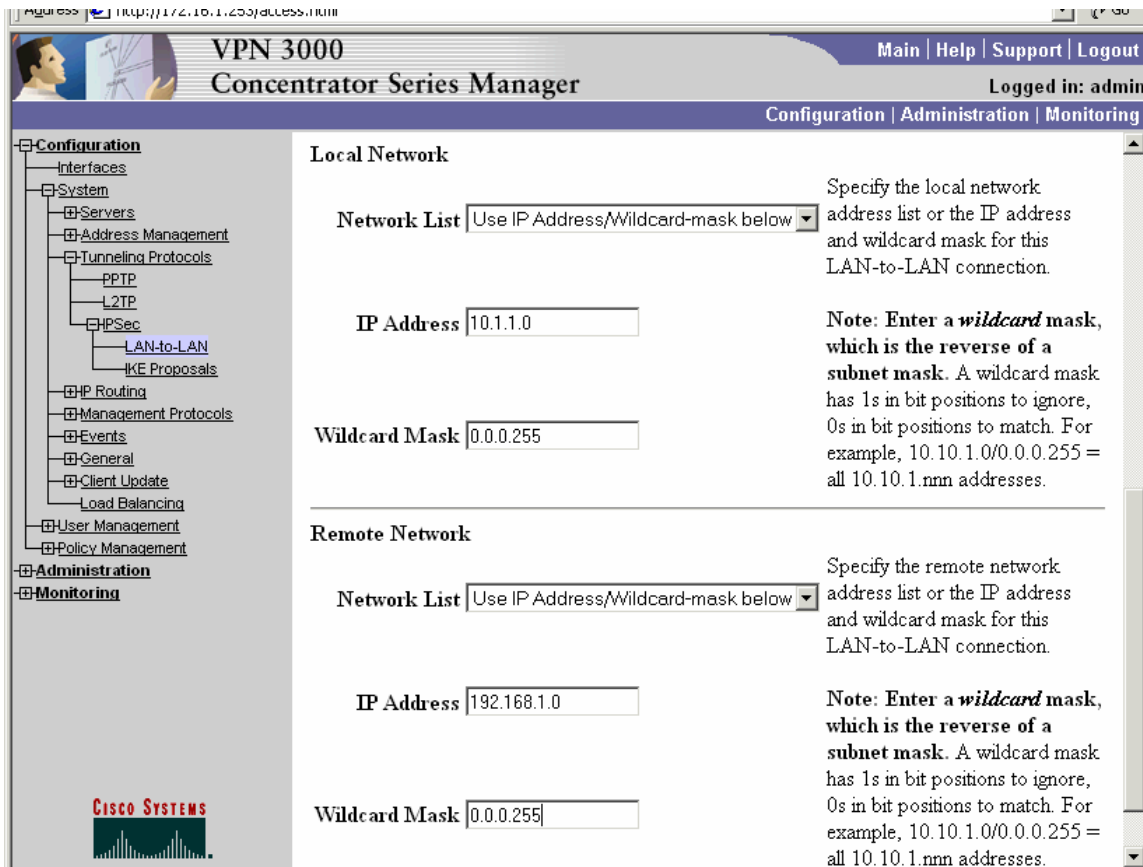


Figure 3. Creating a LAN-to-LAN Definition, Part 2

When this LAN-to-LAN configuration is added using the Add button at the bottom of the screen (not shown above), the VPN 3000 automatically adds several related items.

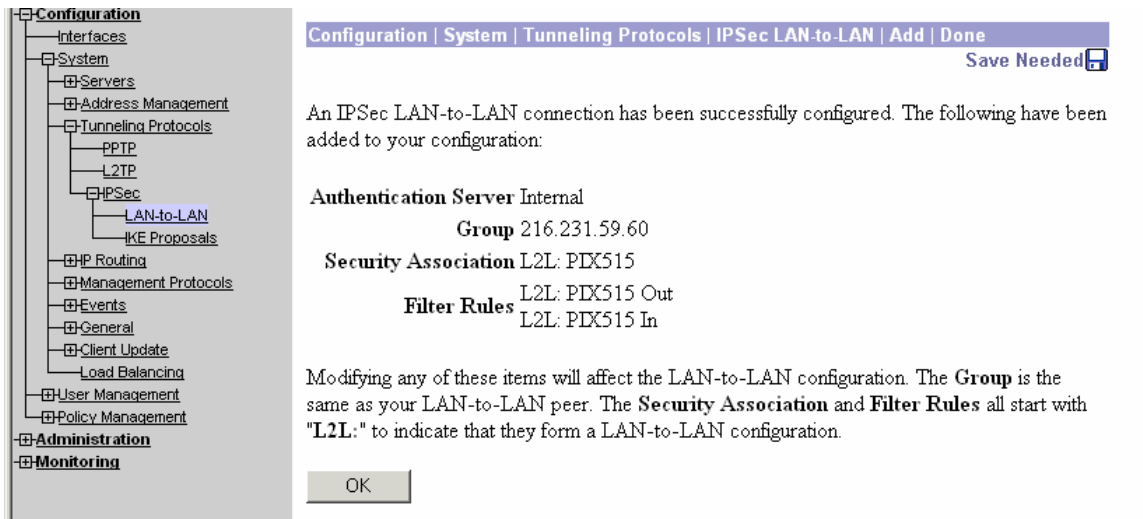


Figure 4. Successful Creation of the LAN-to-LAN Definition

Finally, to complete the VPN configuration, we next must configure the IKE proposal. This is shown below in Figure 5.

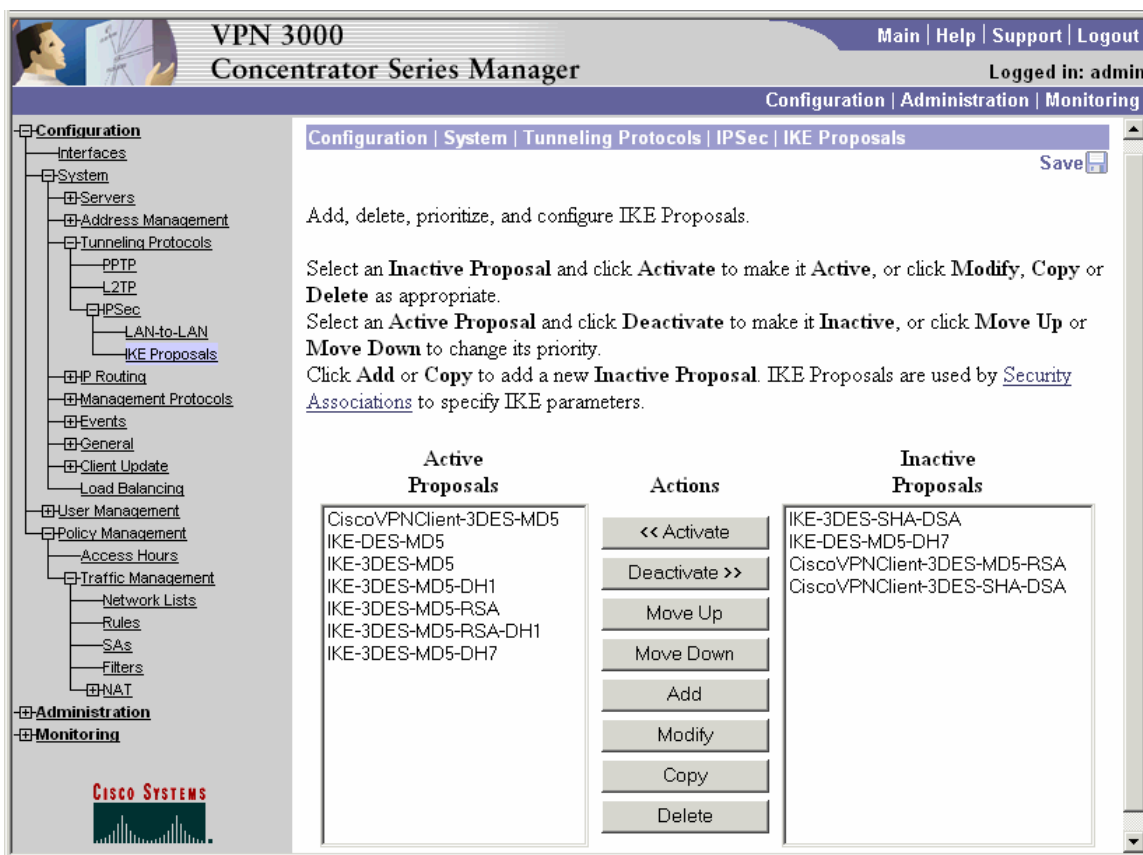


Figure 5. Configuring the IKE Proposal

At least one active IKE proposal must match the ISAKMP parameters defined on the PIX 515 firewall. In this example, IKE-3DES-MD5 matches the ISAKMP parameters defined on the PIX 515, so that IKE proposal must be active in order to establish the VPN.

Once these changes have been made and saved, the VPN tunnel should automatically be created. The Monitoring section of the VPN concentrator can display currently active tunnels, and the active tunnel to the PIX firewall should appear in the LAN-to-LAN section. If the tunnel is not automatically established, generate some traffic to the remote network (such as using Ping to try to connect to a remote host).

Other Notes

The information in this technical document was derived from sample configurations available on Cisco's web site. See <http://www.cisco.com/> for more information and additional sample configurations for both Cisco Secure PIX firewalls and Cisco VPN 30xx Series VPN concentrators. Cisco's web site also offers additional information on troubleshooting VPN tunnels.

Note that implementations of this type in the field have experienced delays in re-establishing the IPSec tunnel automatically if the VPN 30xx Series concentrator shuts down or loses network connectivity. This is due to a live IPSec SA on the PIX, which prevents the PIX from re-establishing the VPN tunnel to the VPN concentrator. The resolution is to use the `clear ipsec sa` and `clear isakmp sa` commands on the PIX firewall to remove the IPSec SA. The PIX firewall and VPN concentrator will then renegotiate security parameters and establish a new tunnel.

Related Articles/Resources

None

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.