

VPN Hardware Client on a PIX 501/506 Series Security Appliance with VPN 3000 Concentrator Configuration Example

Document ID: 22828

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Sample Output
- Clear VPN Sessions and Remove VPN client Commands

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides a step-by-step configuration example for customers who want to deploy the Cisco VPN Hardware Client feature on a PIX 501/506 Series Security Appliance. This feature was introduced with PIX version 6.2 and is used to create an IPSec tunnel with a VPN 3000 Concentrator, a router that runs Cisco IOS® Software, or a PIX firewall.

The configuration of the PIX 501/506 Hardware Client is the same for the headend VPN device, whether it is a VPN 3000 Concentrator, a router that runs Cisco IOS Software, or a PIX firewall. The devices behind the PIX firewall Hardware Client no longer need to have VPN Clients installed on them in order to securely communicate with devices behind the headend device. This allows for rapid deployment and decreases troubleshooting in order to support VPN remote users.

The VPN Hardware Client operates in either network extension mode (NEM) or client mode. In NEM, the network administrator is able to access the devices behind the PIX firewall VPN Hardware Client for remote control and troubleshooting. In client mode, the network devices behind the PIX 501/506 are not accessible from the headend or other VPN users. This behavior is the same in the VPN 3002 Hardware Client.

Note: The PIX 501 and PIX 506/506E are Easy VPN Remote and Easy VPN Server devices. The PIX 515/515E, PIX 525, and PIX 535 act as Easy VPN Servers only.

Refer to Configure the PIX 501/506 Easy VPN Remote to an IOS Router in Network Extension Mode with Extended Authentication for more information on a similar scenario where the Cisco IOS Router acts as the Easy VPN Server.

Refer to PIX-to-PIX 6.x: Easy VPN (NEM) Configuration Example for more information on a similar scenario where the PIX 506 6.x acts as the Easy VPN Server.

Refer to PIX/ASA 7.x Easy VPN with an ASA 5500 as the Server and PIX 506E as the Client (NEM) Configuration Example for more information on a similar scenario where the PIX/ASA 7.x acts as the Easy VPN Server.

Refer to PIX/ASA 7.x Easy VPN with an ASA 5500 as the Server and Cisco 871 as the Easy VPN Remote Configuration Example for more information on a similar scenario where the Cisco 871 Router acts as the Easy VPN Remote.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on these software and hardware versions:

- PIX Firewall version 6.2 or 6.3

Note: PIX Firewall version 7.x does not support PIX 501/506.

- Cisco 2600 Router that runs Cisco IOS Software version 12.2.7b
- Cisco 3620 Router that runs Cisco IOS Software version 12.2.7b
- Cisco VPN 3000 Concentrator

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for information on document conventions.

Background Information

In this example, the PIX 506 is configured in order to initiate a VPN tunnel with the Cisco VPN 3000 Concentrator in NEM. NEM allows for visibility and communication with those devices behind the PIX 506. The VPN 3000 Concentrator runs Routing Information Protocol (RIP) version 2 in order to learn and advertise routes. Reverse Route Injection (RRI) is enabled on the VPN 3000 Concentrator such that it advertises the remote network that uses RIP, behind the PIX 506 VPN Hardware Client, to a Cisco 2600 router as traffic is initiated from the Cisco 3620 router.

Split tunneling is not enabled on the VPN 3000 Concentrator, so all traffic sourced from the Cisco 3620 router is encrypted and sent to the VPN 3000 Concentrator, which forwards this traffic based on the policy routing information. The policy is defined (and can be modified based on individual company security requirements) on the VPN 3000 Concentrator only and is pushed to the PIX 506 VPN Hardware Client during tunnel negotiation (exactly like a VPN Client on a PC).

The PIX 506 is configured as a Dynamic Host Configuration Protocol (DHCP) server in order to service DHCP clients on the Ethernet (E1) interface. Interface Fa0/1 on the Cisco 3620 router is configured as a DHCP client. The Cisco 2621 router runs RIP version 2. Refer to IPsec with VPN Client to VPN 3000 Concentrator Configuration Example in order to configure the VPN 3000 Concentrator.

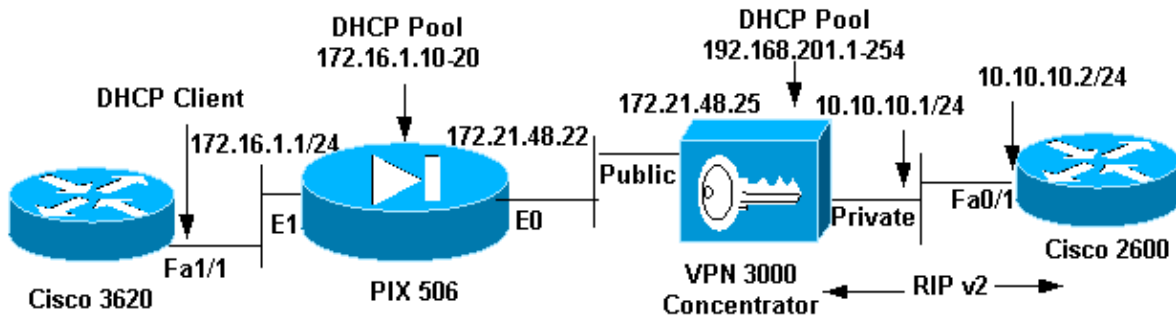
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) or more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses that have been used in a lab environment.

Configurations

This document uses these configurations:

Cisco 3620 Router

```
interface FastEthernet0/1
  ip address dhcp

!--- The DHCP client requests an IP address from the PIX,
!--- which is configured as a DHCP server.
```

Cisco 2621 Router

```
Configuration of 2621 router
2621#write terminal
!
hostname 2621
!
interface FastEthernet0/1
ip address 10.10.10.2 255.255.255.0
ip rip send version 2

!--- Send only RIP version 2.

ip rip receive version 2

!--- Receive only RIP version 2.
```

```
!  
router rip  
version 2  
  
!--- RIP version 2 enabled.  
  
network 10.0.0.0  
no auto-summary  
!
```

PIX Configuration

It is not necessary to define an Access Control List (ACL) or a conduit in order to permit traffic because the connection is initiated from the PIX 506, rather than the VPN 3000 Concentrator or the VPN Client behind the PIX 506. By default, traffic is permitted from inside to outside.

PIX 506

```
506#write terminal  
Building configuration...  
: Saved  
:  
PIX Version 6.2(0)243  
nameif ethernet0 outside security0  
  
!--- On PIX 501/506, this is the default configuration.  
  
nameif ethernet1 inside security100  
enable password 2KFQnbNIdI.2KYOU encrypted  
passwd 2KFQnbNIdI.2KYOU encrypted  
hostname 506  
fixup protocol ftp 21  
fixup protocol http 80  
fixup protocol h323 h225 1720  
fixup protocol h323 ras 1718-1719  
fixup protocol ils 389  
fixup protocol rsh 514  
fixup protocol rtsp 554  
fixup protocol smtp 25  
fixup protocol sqlnet 1521  
fixup protocol sip 5060  
fixup protocol skinny 2000  
names  
pager lines 24  
logging console debugging  
logging monitor debugging  
logging buffered debugging  
interface ethernet0 auto  
interface ethernet1 auto  
  
!--- You should manually specify speed/duplex if your attached  
!--- devices do not support auto negotiation.  
  
mtu outside 1500  
mtu inside 1500  
ip address outside 172.21.48.22 255.255.255.224  
ip address inside 172.16.1.1 255.255.255.0  
ip audit info action alarm  
ip audit attack action alarm  
pdm history enable  
arp timeout 14400  
route outside 0.0.0.0 0.0.0.0 172.21.48.25 1  
timeout xlate 3:00:00  
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip
```

```
0:30:00 sip_med
ia 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
telnet timeout 5
ssh timeout 5

dhcpd address 172.16.1.10-172.16.1.20 inside

!--- This is the pool for the DHCP server to service local requests.

dhcpd lease 3600

!--- This is optional.

dhcpd ping_timeout 750

!--- This is optional.

dhcpd domain cisco.com
dhcpd enable inside

!--- You should enable this on the inside interface.

vpnclient vpngroup beta password *****

!--- Group name and password must match, as defined on
!--- the VPN 3000 Concentrator (or on ACS, if you use
!--- ACS with a VPN 3000 Concentrator).

vpnclient username cisco password *****

!--- User Name/Password must match as defined on
!--- the VPN 3000 Concentrator (or on ACS, if you use
!--- ACS with a VPN 3000 Concentrator).

vpnclient server 172.21.48.25

!--- This is the IP address of the headend
!--- VPN 3000 Concentrator. There can be from 1 to 10 secondary
!--- Cisco Easy VPN Servers (backup VPN headends) configured.
!--- However, check your platform-specific documentation for
!--- applicable peer limits on your PIX Firewall platform.

vpnclient mode network-extension-mode

!--- Using NEM.
```

```
vpnclient enable

terminal width 80
Cryptochecksum:f719695f4d56b84be0c944975caf9f12
: end
[OK]
```

Cisco VPN 3000 Concentrator Configuration

Refer to IPsec with VPN Client to VPN 3000 Concentrator Configuration Example and Configuring the Cisco EzVPN Client on Cisco IOS with the VPN 3000 Concentrator for sample configurations.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

• Routes After the Cisco 3620 is Configured

```
3620#show ip route
Gateway of last resort is 172.16.1.1 to network 0.0.0.0

172.16.0.0/24 is subnetted, 1 subnets
C 172.16.1.0 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [254/0] via 172.16.1.1

!--- Point default to PIX as received with DHCP.
```

• DHCP Lease Information on the Cisco 3620

```
3620#show dhcp lease
Temp IP addr: 172.16.1.10 for peer on Interface: FastEthernet0/1
Temp sub net mask: 255.255.255.0
DHCP Lease server: 172.16.1.1, state: 3 Bound
DHCP transaction id: 11CD
Lease: 3600 secs, Renewal: 1800 secs, Rebind: 3150 secs
Temp default-gateway addr: 172.16.1.1
Next timer fires after: 00:14:39
Retry count: 0 Client-ID: cisco-0008.215d.7be2-Fa0/1
```

• Routes After the Cisco 2621 is Configured

```
2621#show ip route
172.16.0.0/24 is subnetted, 1 subnets
R 172.16.1.0 [120/1] via 10.10.10.1, 00:00:06, FastEthernet0/1

!--- This is the remote network connected to the
!--- private interface of the PIX 506 VPN Hardware Client.
!--- As RRI is configured on the VPN 3000 Concentrator, it uses
!--- RIP in order to advertise this remote network after it sees
!--- traffic from the remote end.

172.21.0.0/27 is subnetted, 1 subnets
R 172.21.48.0 [120/1] via 10.10.10.1, 00:00:06, FastEthernet0/1
R 192.168.201.0/24 [120/1] via 10.10.10.1, 00:00:06, FastEthernet0/1
10.0.0.0/24 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, FastEthernet0/1
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Sample Output

This sample output shows the current state before traffic is initiated between the Cisco 3620 and Cisco 2621 routers.

```
506#show crypto isakmp sa
Total : 1
Embryonic : 0
  dst          src          state    pending  created
  172.21.48.25 172.21.48.22 QM_IDLE    0         0

506#show crypto ipsec sa
interface: outside
Crypto map tag: _vpnc_cm, local addr. 172.21.48.22

local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

!--- Proxy information exchange is complete as defined on the headend,
!--- although no interesting traffic has been initiated. In Cisco IOS
!--- this exchange occurs only when there is interesting traffic.

current_peer: 172.21.48.25
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.21.48.22, remote crypto endpt.: 172.21.48.25
path mtu 1500, ipsec overhead 0, media mtu 1500
current outbound spi: 0

!--- Security Parameter Index (SPI) is created thus far.

inbound esp sas:

!--- No inbound Security Association (SA) is created thus far.

inbound ah sas:

inbound pcp sas:

outbound esp sas:

!--- No outbound SA is created thus far.

outbound ah sas:
```

outbound pcp sas:

This sample output shows the state after a ping is initiated between the Cisco 3620 and Cisco 2621 routers.

```
3620#ping 10.10.10.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
```

```
..!!!
```

```
!--- The initial ping failed because the SAs were created after the PIX
```

```
!--- detected interesting traffic.
```

```
Success rate is 60 percent (3/5), round-trip min/avg/max = 4/4/4 ms
```

```
3620#
```

```
506#show crypto isakmp sa
```

```
Total: 1
```

```
Embryonic: 0
```

dst	src	state	pending	created
172.21.48.25	172.21.48.22	QM_IDLE	0	1

```
506#show crypto ipsec sa
```

```
interface: outside
```

```
Crypto map tag: _vpnc_cm, local addr. 172.21.48.22
```

```
local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer: 172.21.48.25
```

```
PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
```

```
!--- This shows the number of packets encrypted.
```

```
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
```

```
#send errors 1, #recv errors 0
```

```
local crypto endpt.: 172.21.48.22, remote crypto endpt.: 172.21.48.25
```

```
path mtu 1500, ipsec overhead 56, media mtu 1500
```

```
current outbound spi: 5c5b2a9
```

```
!--- SPI is created now.
```

```
inbound esp sas:
```

```
!--- One inbound SA is created after interesting traffic is detected.
```

```
spi: 0x3db858ad(1035491501)
```

```
transform: esp-3des esp-md5-hmac ,
```

```
in use settings ={Tunnel, }
```

```
slot: 0, conn id: 2, crypto map: _vpnc_cm
```

```
sa timing: remaining key lifetime (k/sec): (4607999/28499)
```

```
IV size: 8 bytes
```

```
replay detection support: Y
```

```
inbound ah sas:
```

```
!--- Authentication Header (AH) was not an option on the headend.
```

```
inbound pcp sas:
```

!--- Payload Compression Protocol (PCP) was not an option on the headend.

outbound esp sas:

!--- One outbound SA is created after interesting traffic is detected.

spi: 0x5c5b2a9(96842409)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: _vpnc_cm
sa timing: remaining key lifetime (k/sec): (4607999/28499)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

!--- AH was not an option on the headend.

outbound pcp sas:

!--- PCP was not an option on the headend.

Logging Information on the Cisco VPN 3000 Concentrator

54 04/02/2002 15:14:45.560 SEV=4 IKE/52 RPT=19 172.21.48.22
Group [beta] User [cisco]
User (cisco) authenticated.
!--- Group/User authentication is successful.

55 04/02/2002 15:14:46.630 SEV=4 AUTH/22 RPT=2
User cisco connected

56 04/02/2002 15:14:46.630 SEV=4 IKE/119 RPT=2 172.21.48.22
Group [beta] User [cisco]
PHASE 1 COMPLETED

!--- Phase I is successful.

57 04/02/2002 15:14:46.630 SEV=5 IKE/35 RPT=2 172.21.48.22
Group [beta] User [cisco]
Received remote IP Proxy Subnet data in ID Payload:

!--- Proxy info exchange.

Address 172.16.1.0, Mask 255.255.255.0, Protocol 0, Port 0

60 04/02/2002 15:14:46.630 SEV=5 IKE/34 RPT=2 172.21.48.22
Group [beta] User [cisco]
Received local IP Proxy Subnet data in ID Payload:

!--- Proxy info exchange.

Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

63 04/02/2002 15:14:46.630 SEV=5 IKE/66 RPT=2 172.21.48.22
Group [beta] User [cisco]
IKE Remote Peer configured for SA: ESP-3DES-MD5:

!--- Transform set being used.

```
64 04/02/2002 15:14:46.640 SEV=4 IKE/49 RPT=2 172.21.48.22
Group [beta] User [cisco]
Security negotiation complete for User (cisco)
Responder, Inbound SPI = 0x05c5b2a9, Outbound SPI = 0x3db858ad
```

*!--- Both inbound and outbound SPIs are created. These numbers will be the
!--- same, but swapped, on the other end.*

```
67 04/02/2002 15:14:46.640 SEV=4 IKE/120 RPT=2 172.21.48.22
Group [beta] User [cisco]
PHASE 2 COMPLETED (msgid=017e9e02)
```

!--- Phase II is successful.

Clear VPN Sessions and Remove VPN client Commands

Clear VPN Session

The **no vpnclient connect** and **vpnclient disconnect** commands disconnect current VPN sessions, but do not prevent initiation of new VPN tunnels.

Note: The **no vpnclient enable** command closes all established VPN tunnels and prevents initiation of new VPN tunnels until you enter a **vpnclient enable** command.

Remove VPN Client commands

The **clear vpnclient** command clears the Easy VPN Remote configuration and security policy stored in Flash memory.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [Cisco PIX Firewall Documentation](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Cisco PIX 500 Series Security Appliances Field Notices](#)
- [IPSec Negotiation/IKE Protocols Support Page](#)
- [Requests for Comments \(RFCs\)](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Mar 13, 2007

Document ID: 22828
