

PIX/ASA: Easy VPN with an PIX 515E as the Server and ASA 5505 as the Client (NEM) Configuration Example

Document ID: 98528

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Configure

- Network Diagram
- Configurations

Verify

- PIX Easy VPN Server show Commands and Sample Output
- PIX Easy VPN Remote Hardware Client show Commands and Sample Output

Troubleshoot

- Easy VPN Server Commands
- Easy VPN Remote Hardware Client Commands

Related Information

Introduction

This document provides a sample configuration for IPsec between a Cisco PIX 515E and Cisco Adaptive Security Appliance (ASA) 5505 that uses Easy VPN with Network Extension Mode (NEM). A Cisco Easy VPN solution consists of an Easy VPN server at the main site and Easy VPN hardware clients at the remote offices. The Cisco ASA 5505 can function as a Cisco Easy VPN hardware client or as a Cisco Easy VPN server, which is sometimes called a headend device, but not both at the same time. Here, in our topology Cisco PIX 515E acts as the Easy VPN server and the ASA 5505 acts as the Easy VPN remote client (Hardware Client).

The Easy VPN hardware client supports one of two modes of operation: Client Mode or Network Extension Mode (NEM). The mode of operation determines whether the hosts behind the Easy VPN hardware client are accessible from the enterprise network over the tunnel.

Client Mode, also called Port Address Translation (PAT) mode, isolates all devices on the Easy VPN client private network from those on the enterprise network. The Easy VPN client performs PAT for all VPN traffic for its inside hosts. IP address management is neither required for the Easy VPN client inside interface or the inside hosts.

NEM makes the inside interface and all inside hosts routable across the enterprise network over the tunnel. Hosts on the inside network obtain their IP addresses from an accessible subnet (statically or with DHCP) that is preconfigured with static IP addresses. PAT does not apply to VPN traffic in NEM. This mode does not require a VPN configuration for each client. The ASA 5505 configured for NEM mode supports automatic tunnel initiation. The configuration must store the group name, username, and password.

Automatic tunnel initiation is disabled if secure unit authentication is enabled. The network and addresses on the private side of the Easy VPN client are hidden, and cannot be accessed directly.

The Easy VPN hardware client does not have a default mode. But, if you do not specify the mode in Adaptive Security Device Manager (ASDM), ASDM automatically selects client mode. When you configure the Easy VPN hardware client with the use of the CLI, you must specify a mode.

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

Ensure that you meet these requirements before you attempt this configuration:

- A basic understanding of
 - ◆ IPsec
 - ◆ Easy VPN
 - ◆ ASA/PIX Security Appliances

Components Used

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

- The Easy VPN Remote Hardware client is a ASA 5505 that runs version 7.2(1) and later.
- The Easy VPN Server is an PIX 515E that runs version 7.x and later.

Note: The Easy VPN Server configuration in this document are applicable to both PIX/ASA runs with version 7.x and later.

Note: Easy VPN client configuration is only supported on ASA 5505.

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 the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

If you use an Easy VPN solution, this simplifies the deployment and management of a VPN in these ways:

In this configuration example, an IPsec tunnel is configured with these elements:

- Hosts at remote sites no longer have to run VPN client software.
- Security policies reside on a central server and are pushed to the remote hardware clients when a VPN connection is established.

- Few configuration parameters need to be set locally, which minimizes the need for on-site administration.

When used as an Easy VPN hardware client, the ASA 5505 can also be configured to perform basic firewall services, such as to protect devices in a DMZ from unauthorized access. But, if the ASA 5505 is configured to function as an Easy VPN hardware client, it cannot establish other types of tunnels. For example, the ASA 5505 cannot function simultaneously as an Easy VPN hardware client and as one end of a standard peer-to-peer VPN deployment

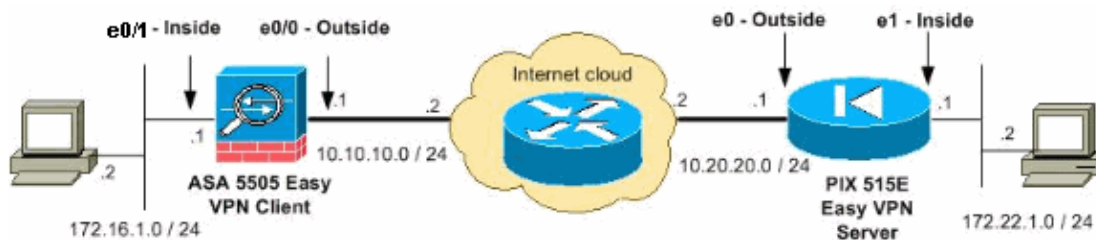
Configure

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) in order to obtain more information on the commands used in this section.

Network Diagram

When configured in Easy VPN Network Extension Mode, the ASA 5505 does not hide the IP addresses of local hosts by the substitution of a public IP address. Therefore, hosts on the other side of the VPN connection can communicate directly with hosts on the local network. When you configure NEM, the network behind the Easy VPN client should not overlap your the network behind the Easy VPN server. The Figure shows a sample network topology with the ASA 5505 that runs in Network Extension Mode.



Configurations

This document uses these configurations:

- Easy VPN Server
- Easy VPN Remote Hardware Client

Easy VPN Server (PIX 515E)

```

pixfirewall#write terminal
PIX Version 8.0(2)
!
hostname pixfirewall
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configure the outside and inside interfaces.

interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.20.20.1 255.255.255.0
!
```

```
interface Ethernet1
  nameif inside
  security-level 100
  ip address 172.22.1.1 255.255.255.0
!
!
!--- Output Suppressed
!
interface Ethernet5
  shutdown
  no nameif
  no security-level
  no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

!
!--- This access list is used for a nat zero command that prevents
!--- traffic, which matches the access list, so it does
!--- not undergo network address translation (NAT).

access-list no-nat extended permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0

!
!--- This access list is used to define the traffic
!--- that should pass through the tunnel.
!--- It is bound to the group policy, which defines
!--- a dynamic crypto map.

access-list ezvpn1 extended permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0

pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-602.bin
no asdm history enable
arp timeout 14400

!
!--- Specify the NAT configuration.
!--- NAT 0 prevents NAT for the ACL defined in this configuration.
!--- The nat 1 command specifies NAT for all other traffic.

global (outside) 1 interface
nat (inside) 0 access-list no-nat
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

!
!--- PHASE 2 CONFIGURATION ---!
```

```
!--- The encryption types for Phase 2 are defined here.
!--- A single DES encryption with
!--- the md5 hash algorithm is used.

crypto ipsec transform-set mySET esp-des esp-md5-hmac

!--- This command defines a dynamic crypto map
!--- with the specified encryption settings.

crypto dynamic-map myDYN-MAP 5 set transform-set mySET

!--- This command binds the dynamic map to
!--- the IPsec/ISAKMP process.

crypto map myMAP 60 ipsec-isakmp dynamic myDYN-MAP

!--- This command specifies the interface to be used
!--- with the settings defined in this configuration.

crypto map myMAP interface outside

!--- PHASE 1 CONFIGURATION ---!

!--- This configuration uses isakmp policy 1.
!--- Policy 65535 is included in the default
!--- configuration. These configuration commands
!--- define the Phase 1 policies that are used.

crypto isakmp enable outside
crypto isakmp policy 1
  authentication pre-share
  encryption des
  hash md5
  group 2
  lifetime 86400
crypto isakmp policy 65535
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
```

```

inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global

!--- This defines the group policy you use with Easy VPN.
!--- Specify the networks that should pass through
!--- the tunnel and that you want to
!--- use network extension mode.

group-policy myGROUP internal
group-policy myGROUP attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value ezvpn1
nem enable

!--- The username and password associated with
!--- this VPN connection are defined here. You
!--- can also use AAA for this function.

username cisco password 3USUCOPFUIMCO4Jk encrypted

!--- The tunnel-group commands bind the configurations
!--- defined in this configuration to the tunnel that is
!--- used for Easy VPN. This tunnel name is the one
!--- specified on the remote side.

tunnel-group mytunnel type ipsec-ra
tunnel-group mytunnel general-attributes
default-group-policy myGROUP
tunnel-group mytunnel ipsec-attributes

!--- The pre-shared-key used is "cisco".

pre-shared-key *
prompt hostname context
Cryptochecksum:a16e3c19d5b2ab400151e0c13d26b074
: end

```

ASA 5505 – Easy VPN Remote Hardware Client

```

ciscoasa#write terminal
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0

```

```
ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!

!--- Output Suppressed

!
interface Ethernet0/7
  shutdown
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400

!--- Set the standard NAT configuration.
!--- Easy VPN provides the NAT exceptions needed.

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 10.10.10.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0

!--- Easy VPN Client Configuration ---!
!--- Specify the IP address of the VPN server.

vpnclient server 10.20.20.1

!--- This example uses network extension mode.

vpnclient mode network-extension-mode

!--- Specify the group name and the pre-shared key.

vpnclient vpngroup mytunnel password *****

!--- Specify the authentication username and password.

vpnclient username cisco password *****

!--- In order to enable the device as hardware vpnclient, use this command.
```

```

vpnclient enable

threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
  match default-inspection-traffic
!

!--- Output suppressed

!
service-policy global_policy global
prompt hostname context
Cryptochecksum:dfcc004fbc2988e4370226f8d592b205
: end

```

Verify

Use this section in order to confirm that your configuration works properly.

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

- PIX Easy VPN Server show Commands and Sample Output
- PIX Easy VPN Remote Hardware Client show Commands and Sample Output

PIX Easy VPN Server show Commands and Sample Output

- **show crypto isakmp sa** This command displays all current Internet Key Exchange (IKE) security associations (SA) at a peer.

```

pixfirewall#show crypto isakmp sa

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.10.10.1
  Type    : user           Role    : responder
  Rekey   : no           State   : AM_ACTIVE

```

- **show crypto ipsec sa** This command displays IPsec SAs built between peers.

```

pixfirewall#show crypto ipsec sa
interface: outside
Crypto map tag: myDYN-MAP, seq num: 5, local addr: 10.20.20.1

local ident (addr/mask/prot/port): (172.22.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer: 10.10.10.1, username: cisco
dynamic allocated peer ip: 0.0.0.0

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #rcv errors: 0

local crypto endpt.: 10.20.20.1, remote crypto endpt.: 10.10.10.1

```

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 4DC131C7

inbound esp sas:

spi: 0x6F48BB47 (1867037511)
transform: esp-des esp-md5-hmac none
in use settings = {RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: myDYN-MAP
sa timing: remaining key lifetime (sec): 28656
IV size: 8 bytes
replay detection support: Y

outbound esp sas:

spi: 0x4DC131C7 (1304506823)
transform: esp-des esp-md5-hmac none
in use settings = {RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: myDYN-MAP
sa timing: remaining key lifetime (sec): 28656
IV size: 8 bytes
replay detection support: Y

Crypto map tag: myDYN-MAP, seq num: 5, local addr: 10.20.20.1

local ident (addr/mask/prot/port): (172.22.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
current_peer: 10.10.10.1, username: cisco
dynamic allocated peer ip: 0.0.0.0

#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 comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.20.20.1, remote crypto endpt.: 10.10.10.1

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: DC1F63B2

inbound esp sas:

spi: 0x5288CD4D (1384697165)
transform: esp-des esp-md5-hmac none
in use settings = {RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: myDYN-MAP
sa timing: remaining key lifetime (sec): 28634
IV size: 8 bytes
replay detection support: Y

outbound esp sas:

spi: 0xDC1F63B2 (3693044658)
transform: esp-des esp-md5-hmac none
in use settings = {RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: myDYN-MAP
sa timing: remaining key lifetime (sec): 28634
IV size: 8 bytes
replay detection support: Y

Crypto map tag: myDYN-MAP, seq num: 5, local addr: 10.20.20.1

local ident (addr/mask/prot/port): (10.20.20.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
current_peer: 10.10.10.1, username: cisco
dynamic allocated peer ip: 0.0.0.0

#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 comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.20.20.1, remote crypto endpt.: 10.10.10.1

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: CADED9A2

inbound esp sas:
 spi: 0xD04E7073 (3494801523)
  transform: esp-des esp-md5-hmac none
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: myDYN-MAP
  sa timing: remaining key lifetime (sec): 28628
  IV size: 8 bytes
  replay detection support: Y
outbound esp sas:
 spi: 0xCADED9A2 (3403602338)
  transform: esp-des esp-md5-hmac none
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: myDYN-MAP
  sa timing: remaining key lifetime (sec): 28628
  IV size: 8 bytes
  replay detection support: Y

```

PIX Easy VPN Remote Hardware Client show Commands and Sample Output

- **vpnclient enable** This command enables an Easy VPN remote connection. In Network Extension Mode (NEM), the tunnel is up even when there is no interesting traffic to be exchanged with the headend Easy VPN server.

```
ciscoasa(config)#vpnclient enable
```

- **show crypto isakmp sa** This command displays all current IKE SAs at a peer.

```

ciscoasa#show crypto isakmp sa
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.20.20.1
  Type      : user           Role       : initiator
  Rekey     : no           State      : AM_ACTIVE

```

- **show crypto ipsec sa** This command displays IPsec SAs built between peers.

```

ciscoasa#show crypto ipsec sa
interface: outside
Crypto map tag: _vpnc_cm, seq num: 10, local addr: 10.10.10.1

access-list _vpnc_acl permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.25
5.255.0
local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.22.1.0/255.255.255.0/0/0)
current_peer: 10.20.20.1, username: 10.20.20.1
dynamic allocated peer ip: 0.0.0.0

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0

```

#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.20.20.1

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 6F48BB47

inbound esp sas:

spi: 0x4DC131C7 (1304506823)
transform: esp-des esp-md5-hmac none
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: _vpnc_cm
sa timing: remaining key lifetime (sec): 28786
IV size: 8 bytes
replay detection support: Y

outbound esp sas:

spi: 0x6F48BB47 (1867037511)
transform: esp-des esp-md5-hmac none
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: _vpnc_cm
sa timing: remaining key lifetime (sec): 28786
IV size: 8 bytes
replay detection support: Y

Crypto map tag: _vpnc_cm, seq num: 10, local addr: 10.10.10.1

access-list _vpnc_acl permit ip host 10.10.10.1 172.22.1.0 255.255.255.0
local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.22.1.0/255.255.255.0/0/0)
current_peer: 10.20.20.1, username: 10.20.20.1
dynamic allocated peer ip: 0.0.0.0

#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 comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.20.20.1

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: 5288CD4D

inbound esp sas:

spi: 0xDC1F63B2 (3693044658)
transform: esp-des esp-md5-hmac none
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: _vpnc_cm
sa timing: remaining key lifetime (sec): 28759
IV size: 8 bytes
replay detection support: Y

outbound esp sas:

spi: 0x5288CD4D (1384697165)
transform: esp-des esp-md5-hmac none
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: _vpnc_cm
sa timing: remaining key lifetime (sec): 28759
IV size: 8 bytes
replay detection support: Y

Crypto map tag: _vpnc_cm, seq num: 10, local addr: 10.10.10.1

```

access-list _vpnc_acl permit ip host 10.10.10.1 host 10.20.20.1
local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.20.20.1/255.255.255.255/0/0)
current_peer: 10.20.20.1, username: 10.20.20.1
dynamic allocated peer ip: 0.0.0.0

#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 comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.20.20.1

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: D04E7073

inbound esp sas:
spi: 0xCADED9A2 (3403602338)
  transform: esp-des esp-md5-hmac none
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: _vpnc_cm
  sa timing: remaining key lifetime (sec): 28752
  IV size: 8 bytes
  replay detection support: Y
outbound esp sas:
spi: 0xD04E7073 (3494801523)
  transform: esp-des esp-md5-hmac none
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: _vpnc_cm
  sa timing: remaining key lifetime (sec): 28752
  IV size: 8 bytes
  replay detection support: Y

```

- **show vpnclient** This command displays VPN Client or Easy VPN remote device configuration information.

```
ciscoasa#show vpnclient
```

LOCAL CONFIGURATION

```

vpnclient server 10.20.20.1
vpnclient mode network-extension-mode
vpnclient vpngroup mytunnel password *****
vpnclient username cisco password *****
vpnclient enable

```

DOWNLOADED DYNAMIC POLICY

```

Current Server                : 10.20.20.1
PFS Enabled                   : No
Secure Unit Authentication Enabled : No
User Authentication Enabled   : No
Split Tunnel Networks        : 172.22.1.0/255.255.255.0
Backup Servers                : None

```

Troubleshoot

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

If you have set up the Easy VPN remote hardware client and Easy VPN server as this document describes and you still experience problems, gather the **debug** output from each PIX and the output from the **show** commands for analysis by Cisco Technical Support. Refer to Troubleshooting the PIX to Pass Data Traffic on

an Established IPsec Tunnel and IP Security Troubleshooting – Understanding and Using debug Commands for more information. Enable IPsec debugging on the PIX.

These sections display PIX **debug** commands and sample output.

- Easy VPN Server Commands
- Easy VPN Remote Hardware Client Commands

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

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Easy VPN Server Commands

- **debug crypto ipsec** This command displays the IPsec negotiations of Phase 2.
- **debug crypto isakmp** This command displays the ISAKMP negotiations of Phase 1.

This is a sample of the output:

```
pixfirewall#debug crypto isakmp 2
Aug 08 03:26:09 [IKEv1]: IP = 10.10.10.1, Connection landed on tunnel_group mytunnel
Aug 08 03:26:09 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, User (cisco) authenticated.
Aug 08 03:26:09 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, PHASE 1 COMPLETED
Aug 08 03:26:09 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, IKE: requesting SPI!
Aug 08 03:26:09 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, Security negotiation complete for User (cisco) Responder, Inbound SPI = 0xe6b089b7, Outbound SPI = 0xcb705206
```

Easy VPN Remote Hardware Client Commands

- **debug crypto ipsec** This command displays the IPsec negotiations of Phase 2.
- **debug crypto isakmp** This command displays the ISAKMP negotiations of Phase 1.

```
ciscoasa#debug crypto isakmp 2

Aug 08 14:16:09 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1
Aug 08 14:16:09 [IKEv1]: IP = 10.20.20.1, Received encrypted packet with no matching SA, dropping
Aug 08 14:16:09 [IKEv1]: IP = 10.20.20.1, Received encrypted packet with no matching SA, dropping
Aug 08 14:16:09 [IKEv1]: IP = 10.20.20.1, Received encrypted packet with no matching SA, dropping
Aug 08 14:16:10 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, PHASE 1 COMPLETED
Aug 08 14:16:10 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, Security negotiation complete for peer (10.20.20.1) Initiator, Inbound SPI = 0xcb705206, Outbound SPI = 0xe6b089b7
Aug 08 14:16:10 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, PHASE 2 COMPLETED (msgid=670ff816)
Aug 08 14:16:10 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, IKE Initiator: New Phase 2, Intf inside, IKE Peer 10.20.20.1 local Proxy Address 172.16.1.0, remote Proxy Address 172.22.1.0, Crypto map (_vpnc_cm)
Aug 08 14:16:10 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, Security negotiation complete for peer (10.20.20.1) Initiator, Inbound SPI = 0x3bfa93fb, Outbound SPI = 0x3b11bf8b
```

```
Aug 08 14:16:10 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, PHASE 2 COMPLETED
(msgid=29791739)
Aug 08 14:16:13 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, IKE Initiator: New
Phase 2, Intf NP Identity Ifc, IKE Peer 10.20.20.1 local Proxy Address 10.10.1
0.1, remote Proxy Address 172.22.1.0, Crypto map (_vpnc_cm)
Aug 08 14:16:13 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, Security negotiati
on complete for peer (10.20.20.1) Initiator, Inbound SPI = 0xd329cacc, Outbound
SPI = 0xdec3clb6
Aug 08 14:16:13 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, PHASE 2 COMPLETED
(msgid=b303dbac)

Aug 08 03:26:09 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, PH
ASE 2 COMPLETED (msgid=670ff816)
Aug 08 03:26:10 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, IK
E: requesting SPI!
Aug 08 03:26:10 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, Se
curity negotiation complete for User (cisco) Responder, Inbound SPI = 0x3b11bf8
b, Outbound SPI = 0x3bfa93fb
Aug 08 03:26:10 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, PH
ASE 2 COMPLETED (msgid=29791739)
Aug 08 03:26:12 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, IK
E: requesting SPI!
Aug 08 03:26:12 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, Se
curity negotiation complete for User (cisco) Responder, Inbound SPI = 0xdec3clb
6, Outbound SPI = 0xd329cacc
Aug 08 03:26:12 [IKEv1]: Group = mytunnel, Username = cisco, IP = 10.10.10.1, PH
ASE 2 COMPLETED (msgid=b303dbac)
```

Related Information

- [Cisco PIX 500 Series Security Appliances](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Cisco PIX Firewall Software](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Security Product Field Notices \(including PIX\)](#)
- [Requests for Comments \(RFCs\)](#)
- [IPsec Negotiation/IKE Protocols](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 02, 2008

Document ID: 98528
