

PIX/ASA 7.x and above: PIX-to-PIX VPN Tunnel Configuration Example

Document ID: 67912

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

Background Information

Configuration

- ASDM Configuration
- PIX CLI Configuration
- Backup Site-to-Site Tunnel

Clear Security Associations (SAs)

Verify

Troubleshoot

- PFS
- Management-Access
- Debug Commands

Related Information

Introduction

This document describes the procedure to configure VPN tunnels between two PIX Firewalls using Cisco Adaptive Security Device Manager (ASDM). ASDM is an application-based configuration tool designed to help you set up, configure, and monitor your PIX Firewall with a GUI. PIX Firewalls are placed at two different sites.

A tunnel is formed using IPsec. IPsec is a combination of open standards that provide data confidentiality, data integrity, and data origin authentication between IPsec peers.

Note: In PIX 7.1 and later, the **sysopt connection permit-ipsec** command is changed to **sysopt connection permit-vpn**. This command allows traffic that enters the security appliance through a VPN tunnel and is then decrypted, to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic. In order to disable this feature, use the **no** form of this command. This command is not visible in the CLI configuration.

Refer to PIX 6.x: Simple PIX-to-PIX VPN Tunnel Configuration Example in order to learn more about the same scenario where the Cisco PIX Security Appliance runs software version 6.x.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document specifies that this peer initiates the first proprietary exchange in order to determine the appropriate peer to which to connect.

- Cisco PIX 500 Series Security Appliance with version 7.x and later
- ASDM version 5.x.and later

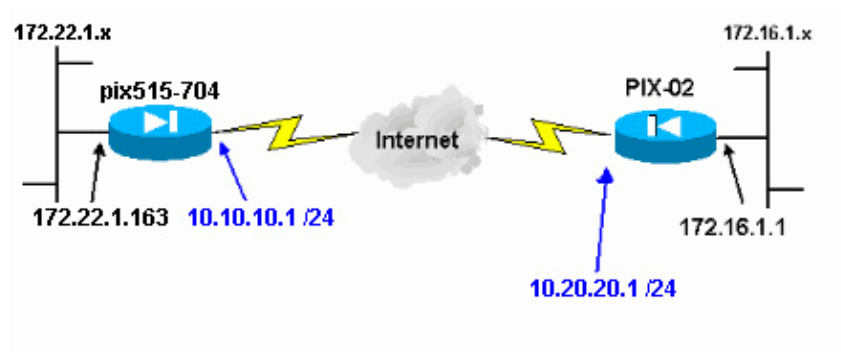
Note: Refer to Allowing HTTPS Access for ASDM in order to allow the ASA to be configured by the ASDM.

Note: The ASA 5500 series version 7.x/8.x runs the same software seen in PIX version 7.x/8.x. The configurations in this document are applicable to both product lines.

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.

Network Diagram

This document uses this network setup:



Conventions

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

Background Information

IPsec negotiation can be broken down into five steps, and includes two Internet Key Exchange (IKE) phases.

1. An IPsec tunnel is initiated by interesting traffic. Traffic is considered interesting when it travels between the IPsec peers.
2. In IKE Phase 1, the IPsec peers negotiate the established IKE Security Association (SA) policy. Once the peers are authenticated, a secure tunnel is created using Internet Security Association and Key Management Protocol (ISAKMP).
3. In IKE Phase 2, the IPsec peers use the authenticated and secure tunnel to negotiate IPsec SA transforms. The negotiation of the shared policy determines how the IPsec tunnel is established.
4. The IPsec tunnel is created and data is transferred between the IPsec peers based on the IPsec parameters configured in the IPsec transform sets.
5. The IPsec tunnel terminates when the IPsec SAs are deleted or when their lifetime expires.

Note: IPsec negotiation between the two PIXes fails if the SAs on both of the IKE phases do not match on the peers.

Configuration

- ASDM Configuration
- PIX CLI Configurations

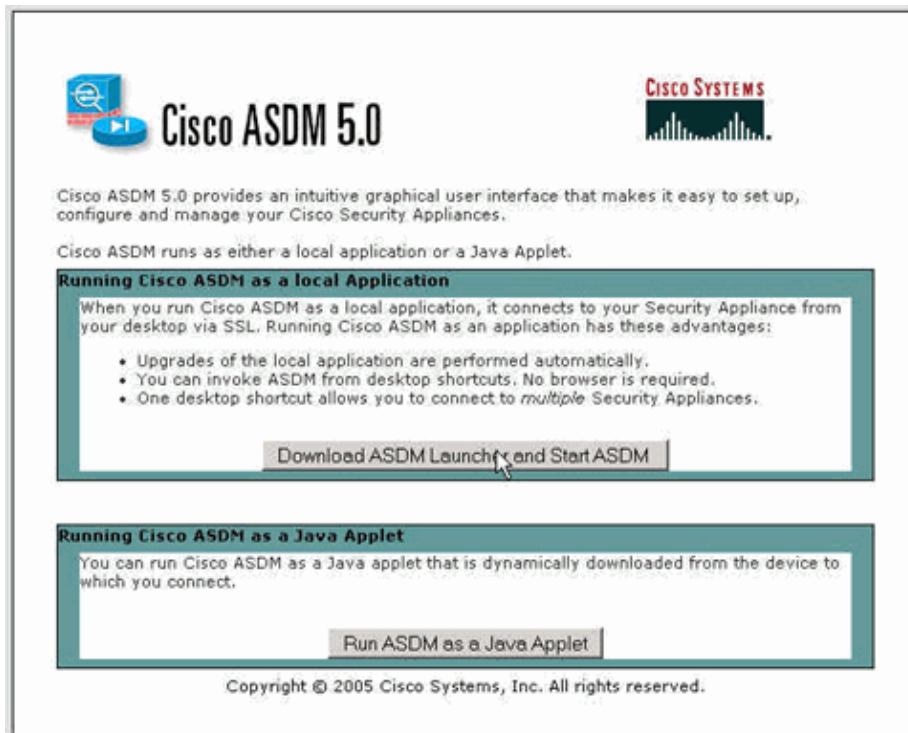
ASDM Configuration

Complete these steps:

1. Open your browser and type **https://<Inside_IP_Address_of_PIX>** to access the ASDM on the PIX.

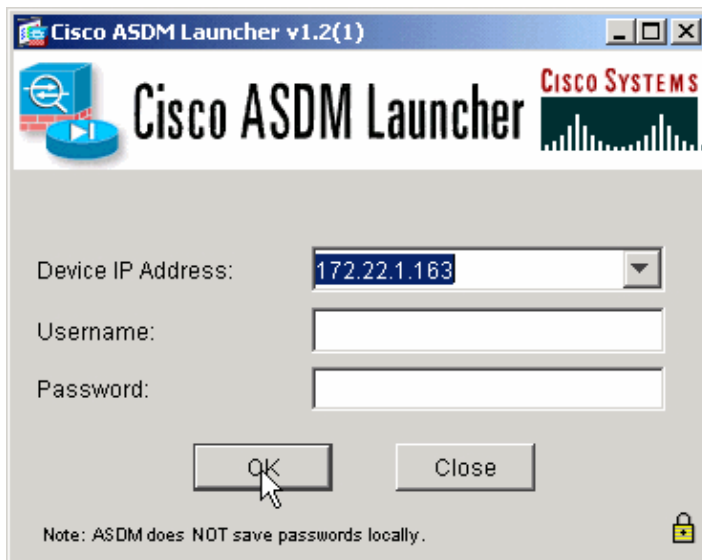
Be sure to authorize any warnings your browser gives you related to SSL certificate authenticity. The default username and password are both blank.

The PIX presents this window to allow the download of the ASDM application. This example loads the application onto the local computer and does not run in a Java applet.

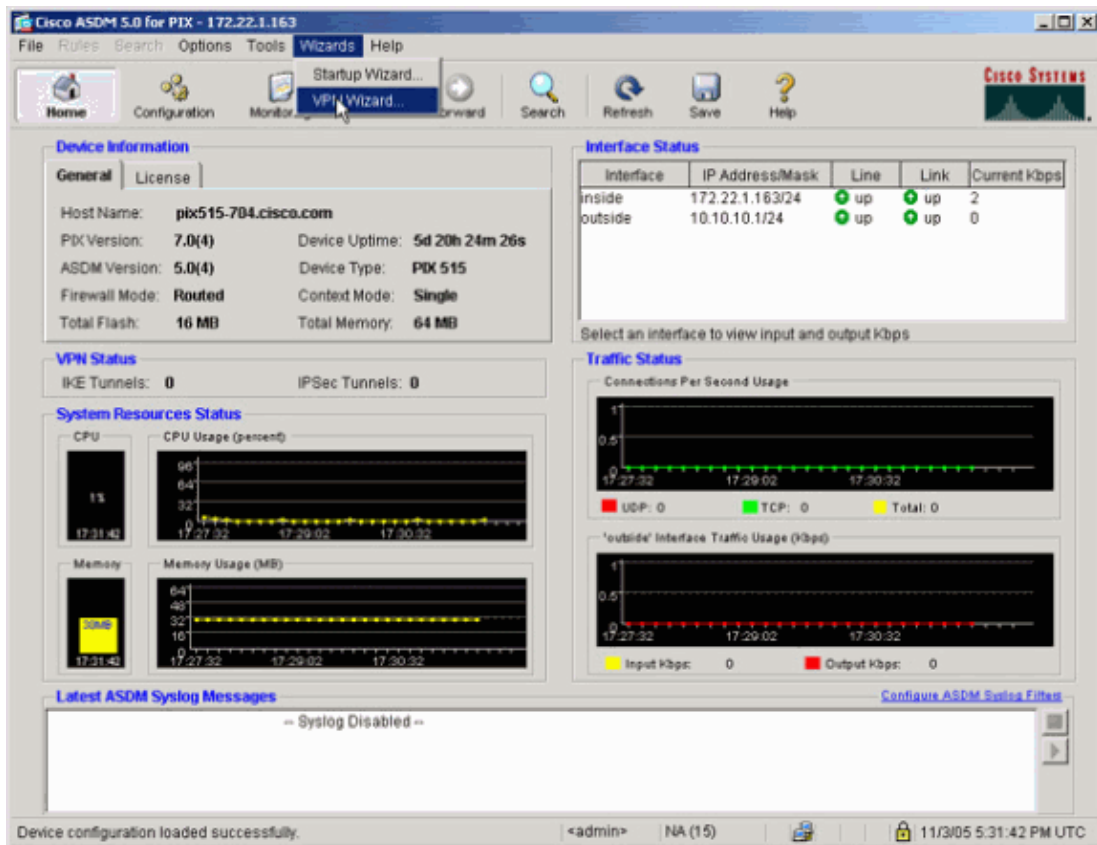


2. Click **Download ASDM Launcher and Start ASDM** to download the installer for the ASDM application.
3. Once the ASDM Launcher downloads, follow the prompts in order to install the software and run the Cisco ASDM Launcher.
4. Enter the IP address for the interface you configured with the **http** – command and a username and password if you specified one.

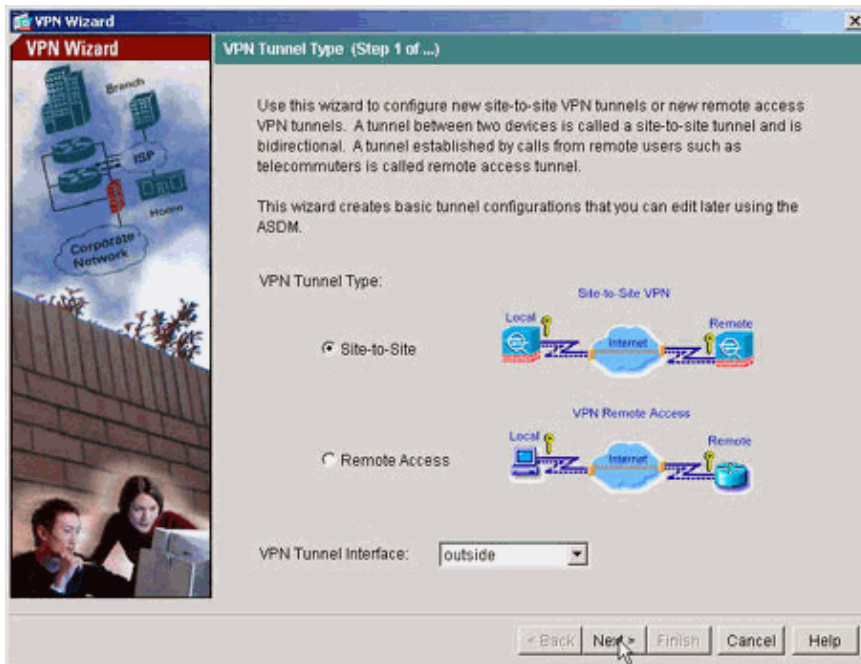
This example uses the default blank username and password.



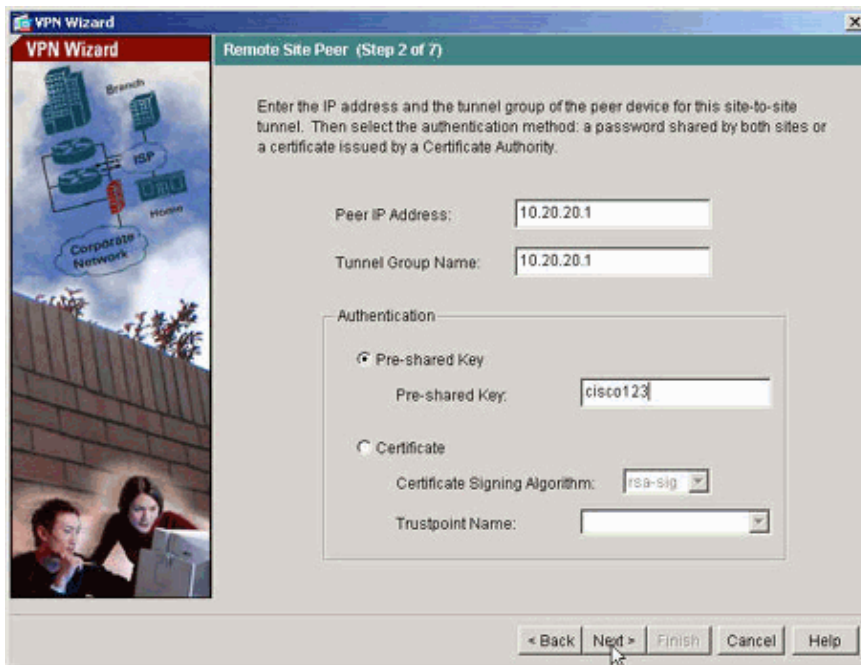
5. Run the VPN Wizard once the ASDM application connects to the PIX.



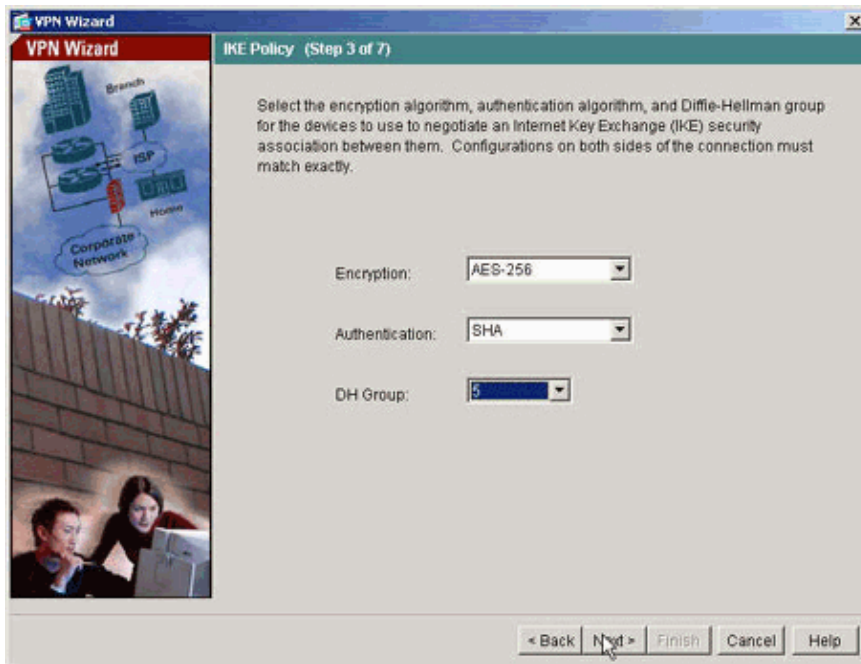
6. Choose the **Site-to-Site** VPN tunnel type.



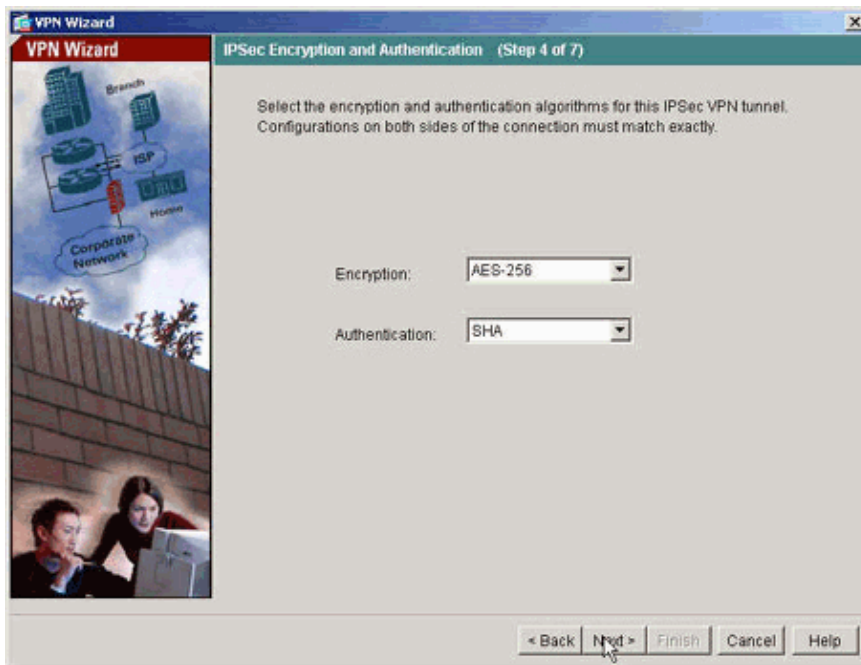
7. Specify the outside IP address of the remote peer. Enter the authentication information to use (pre-shared key in this example).



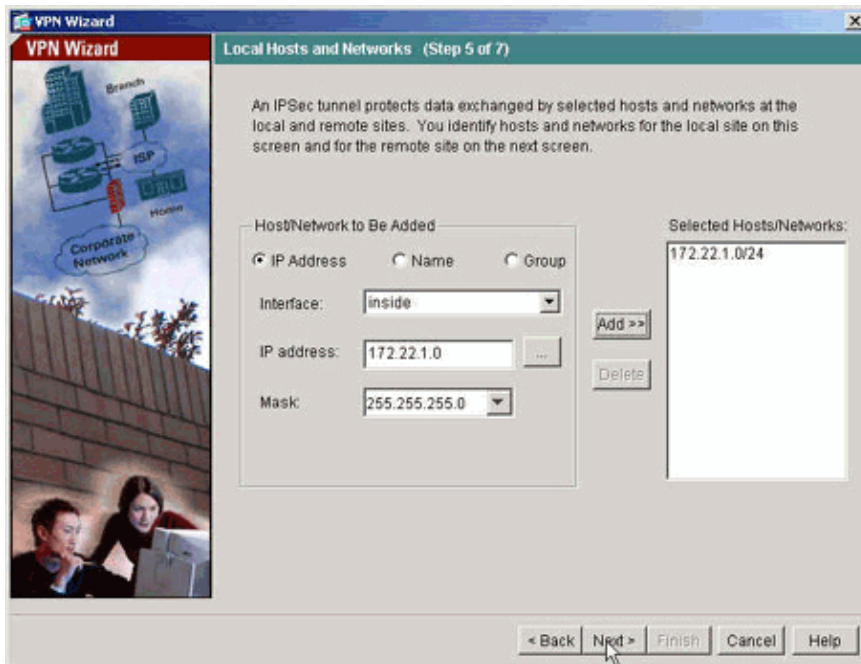
8. Specify the attributes to use for IKE, also known as "Phase 1". These attributes must be the same on both sides of the tunnel.



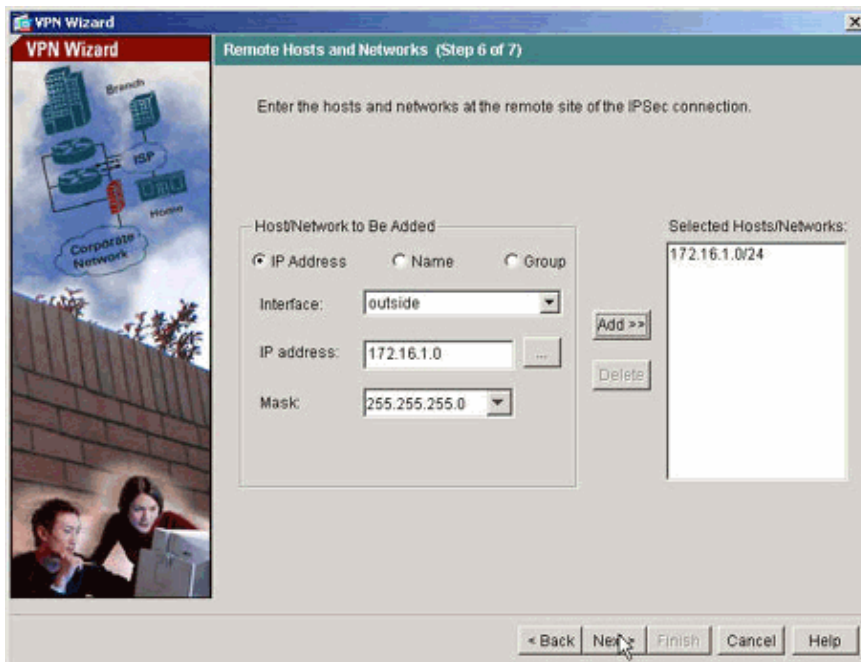
9. Specify the attributes to use for IPsec, also known as "Phase 2". These attributes must match on both sides.



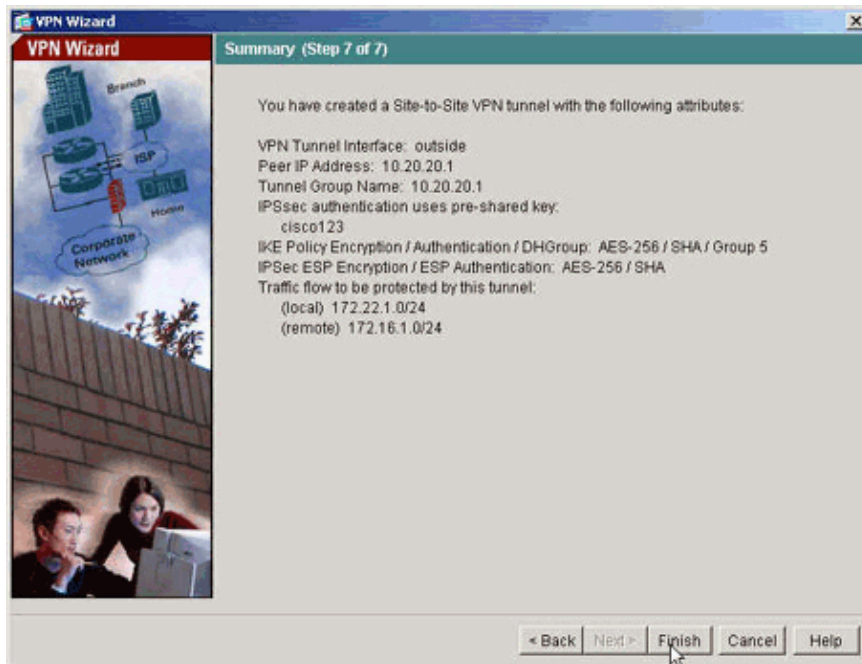
10. Specify the hosts whose traffic should be allowed to pass through the VPN tunnel. In this step, the hosts local to pix515-704 are specified.



11. The hosts and networks on the remote side of the tunnel are specified.



12. The attributes defined by the VPN Wizard are displayed in this summary. Double check the configuration and click **Finish** when you are satisfied the settings are correct.



PIX CLI Configuration

pix515-704

```

pixfirewall#show run
: Saved
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.10.10.1 255.255.255.0

!--- Configure the outside interface.
!

interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.22.1.163 255.255.255.0

!--- Configure the inside interface.
!

!-- Output suppressed
!

passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

```

```
access-list inside_nat0_outbound extended permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

```
!--- This access list (inside_nat0_outbound) is used with the nat zero command.  
!--- This prevents traffic which matches the access list from undergoing  
!--- network address translation (NAT). The traffic specified by this ACL is  
!--- traffic that is to be encrypted and  
!--- sent across the VPN tunnel. This ACL is intentionally  
!--- the same as (outside_cryptomap_20).  
!--- Two separate access lists should always be used in this configuration.
```

```
access-list outside_cryptomap_20 extended permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

```
!--- This access list (outside_cryptomap_20) is used with the crypto map  
!--- outside_map to determine which traffic should be encrypted and sent  
!--- across the tunnel.  
!--- This ACL is intentionally the same as (inside_nat0_outbound).  
!--- Two separate access lists should always be used in this configuration.
```

```
pager lines 24  
mtu inside 1500  
mtu outside 1500  
no failover
```

```
asdm image flash:/asdm-511.bin
```

```
!--- Enter this command to specify the location of the ASDM image.
```

```
asdm history enable  
arp timeout 14400
```

```
nat (inside) 0 access-list inside_nat0_outbound
```

```
!--- NAT 0 prevents NAT for networks specified in the ACL inside_nat0_outbound.
```

```
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  
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00  
timeout uauth 0:05:00 absolute
```

```
http server enable
```

```
!--- Enter this command in order to enable the HTTPS server for ASDM.
```

```
http 172.22.1.1 255.255.255.255 inside
```

```
!--- Identify the IP addresses from which the security appliance  
!--- accepts HTTPS connections.
```

```
no snmp-server location  
no snmp-server contact
```

```
!--- PHASE 2 CONFIGURATION ---!  
!--- The encryption types for Phase 2 are defined here.
```

```
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
!--- Define the transform set for Phase 2.

crypto map outside_map 20 match address outside_cryptomap_20
!--- Define which traffic should be sent to the IPsec peer.

crypto map outside_map 20 set peer 10.20.20.1
!--- Sets the IPsec peer

crypto map outside_map 20 set transform-set ESP-AES-256-SHA
!--- Sets the IPsec transform set "ESP-AES-256-SHA"
!--- to be used with the crypto map entry "outside_map".

crypto map outside_map interface outside
!--- Specifies the interface to be used with
!--- the settings defined in this configuration.

!--- PHASE 1 CONFIGURATION ---!

!--- This configuration uses isakmp policy 10.
!--- Policy 65535 is included in the config by default.
!--- The configuration commands here define the Phase
!--- 1 policy parameters that are used.

isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400

isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400

tunnel-group 10.20.20.1 type ipsec-l2l
!--- In order to create and manage the database of connection-specific records
!--- for ipsec-l2l IPsec (LAN-to-LAN) tunnels, use the tunnel-group
!--- command in global configuration mode.
!--- For L2L connections the name of the tunnel group MUST be the IP
!--- address of the IPsec peer.

tunnel-group 10.20.20.1 ipsec-attributes
pre-shared-key *
```

!--- Enter the pre-shared-key in order to configure the authentication method.

```
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    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
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf
: end
```

PIX-02

```
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
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 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
  domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip 172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0

!--- Note that this ACL is a mirror of the inside_nat0_outbound
!--- ACL on pix515-704.

access-list outside_cryptomap_20 extended permit ip 172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
```

```
!--- Note that this ACL is a mirror of the outside_cryptomap_20
!--- ACL on pix515-704.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image flash:/asdm-511.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 10.10.10.1
crypto map outside_map 20 set transform-set ESP-AES-256-SHA
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
  pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    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
Cryptochecksum:6774691244870705f858ad4e9b810874
: end
pixfirewall#
```

Backup Site-to-Site Tunnel

In order to specify the connection type for the Backup Site-to-Site feature for this crypto map entry, use the **crypto map set connection-type** command in global configuration mode. Use the no form of this command in order to return to the default setting.

Syntax:

```
crypto map map-name seq-num set connection-type {answer-only | originate-only | bidirectional}
```

- **answer-only** This specifies that this peer only responds to inbound IKE connections first during the initial proprietary exchange in order to determine the appropriate peer to which to connect.
- **bidirectional** This specifies that this peer can accept and originate connections based on this crypto map entry. This is the default connection type for all Site-to-Site connections.
- **originate-only** This specifies that this peer initiates the first proprietary exchange in order to determine the appropriate peer to which to connect.

The **crypto map set connection-type** command specifies the connection types for the Backup LAN-to-LAN feature. It allows multiple backup peers to be specified at one end of the connection. This feature works only between these platforms:

- Two Cisco ASA 5500 series security appliances
- Cisco ASA 5500 series security appliance and a Cisco VPN 3000 Concentrator
- Cisco ASA 5500 series security appliance and a security appliance that runs Cisco PIX Security Appliance Software version 7.0 or later

In order to configure a backup LAN-to-LAN connection, Cisco recommends that you configure one end of the connection as originate-only with the `originate-only` keyword, and the end with multiple backup peers as answer-only with the `answer-only` keyword. On the originate-only end, use the **crypto map set peer** command in order to order the priority of the peers. The originate-only security appliance attempts to negotiate with the first peer in the list. If that peer does not respond, the security appliance works its way down the list until either a peer responds or there are no more peers in the list.

When configured in this way, the originate-only peer initially attempts to establish a proprietary tunnel and negotiate with a peer. Thereafter, either peer can establish a normal LAN-to-LAN connection and data from either end can initiate the tunnel connection.

Note: If you configured VPN with multiple peer IP addresses for a crypto entry, the VPN gets established with the backup peer IP once the primary peer goes down. However, once the primary peer comes back, the VPN does not preempt to the primary IP address. You must manually delete the existing SA in order to reinitiate the VPN negotiation to switch it over to the primary IP address. As the conclusion says, the VPN preempt is not supported in the site-to-site tunnel.

Supported Backup LAN-to-LAN Connection Types

Remote Side	Central Side
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

Example

This example, entered in global configuration mode, configures the **crypto map mymap** and sets the connection-type to *originate-only*.

```
hostname(config)#crypto map outside_map 20 connection-type originate-only
```

Clear Security Associations (SAs)

In the privilege mode of the PIX, use the following the commands:

- **clear [crypto] ipsec sa** Deletes the active IPsec SAs. The keyword *crypto* is optional.
- **clear [crypto] isakmp sa** Deletes the active IKE SAs. The keyword *crypto* is optional.

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.

If there is interesting traffic to the peer, the tunnel is established between pix515-704 and PIX-02.

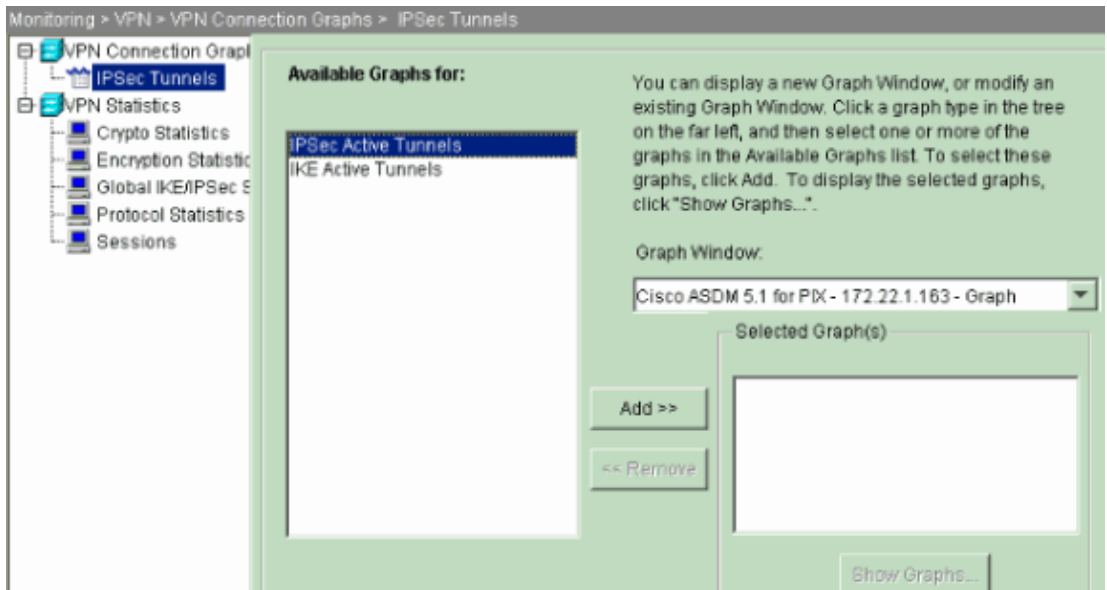
1. View the VPN Status under **Home** in the ASDM in order to verify the formation of the tunnel.

The screenshot displays the Cisco ASDM 5.0 interface for a PIX device. The main window is titled "Cisco ASDM 5.0 for PIX - 172.22.1.163". The interface is divided into several sections:

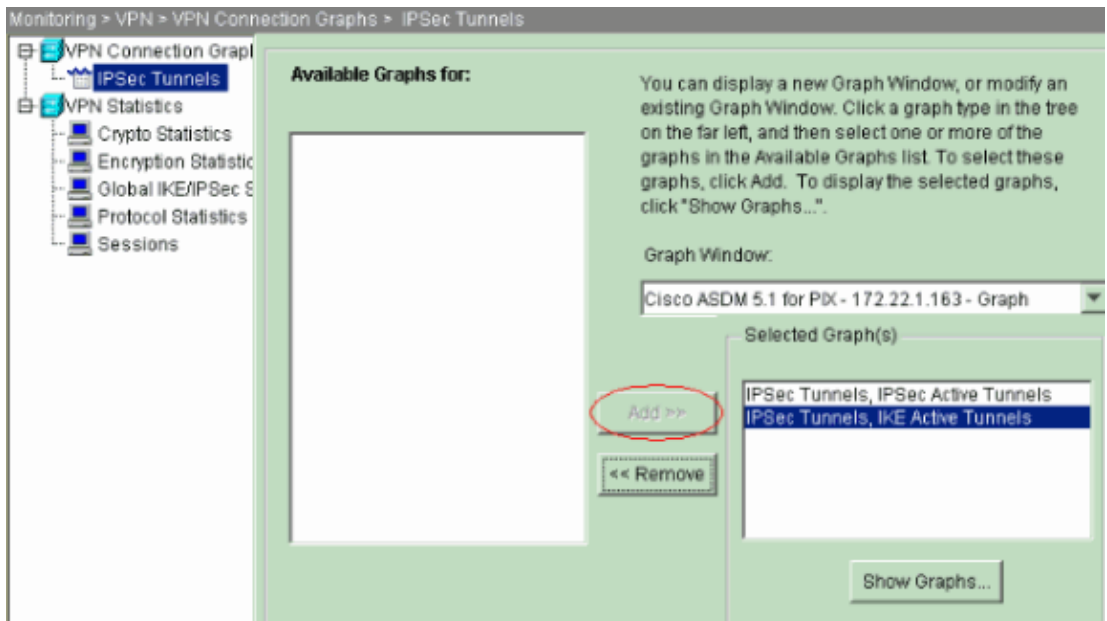
- Device Information:** Shows Host Name: pix515-704.cisco.com, PIX Version: 7.0(4), Device Uptime: 5d 20h 55m 16s, ASDM Version: 5.0(4), Device Type: PIX 515, Firewall Mode: Routed, Context Mode: Single, Total Flash: 16 MB, and Total Memory: 64 MB.
- Interface Status:** A table showing the status of the inside and outside interfaces.
- VPN Status:** Shows 1 IKE Tunnel and 1 IPSec Tunnel.
- System Resources Status:** Includes CPU Usage (2%) and Memory Usage (20MB).
- Traffic Status:** Shows Connections Per Second Usage and 'outside' Interface Traffic Usage (Kbps).
- Latest ASDM Syslog Messages:** Shows "-- Syslog Disabled --".

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	172.22.1.163/24	up	up	2
outside	10.10.10.1/24	up	up	1

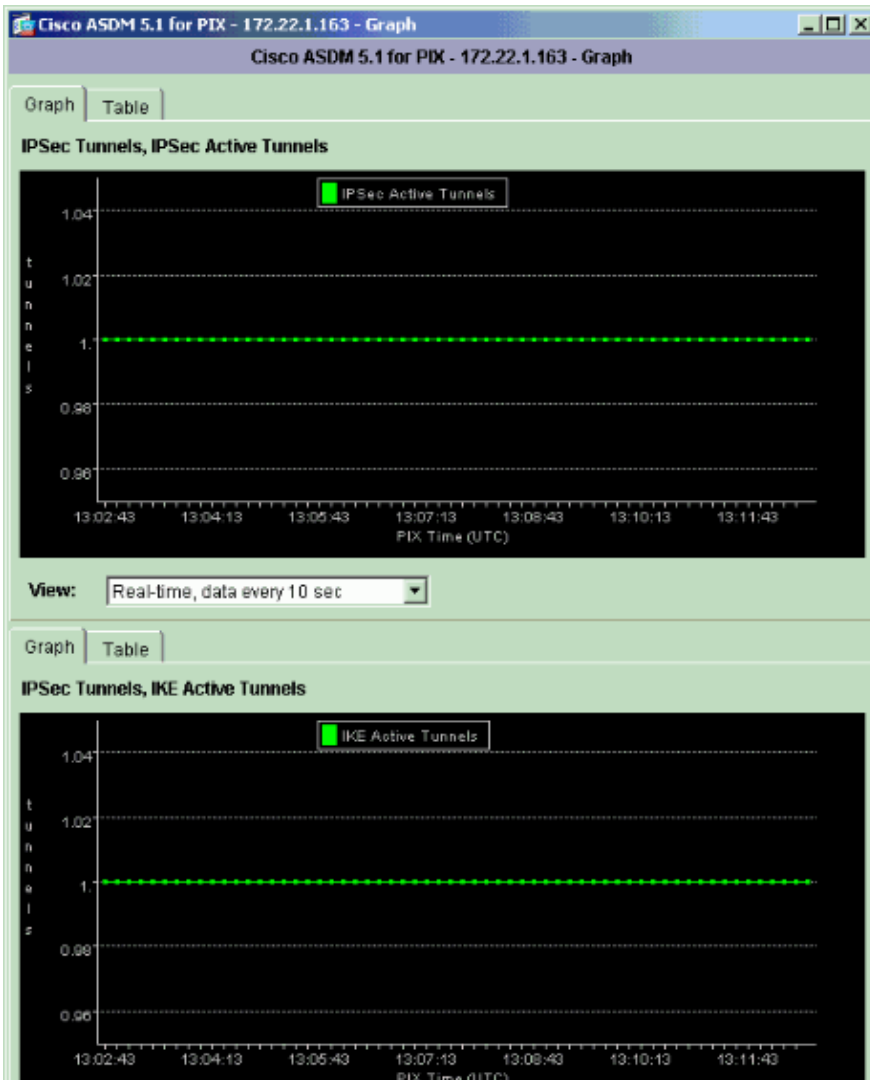
2. Choose **Monitoring > VPN > VPN Connection Graphs > IPSec Tunnels** in order to verify the details about the tunnel establishment.



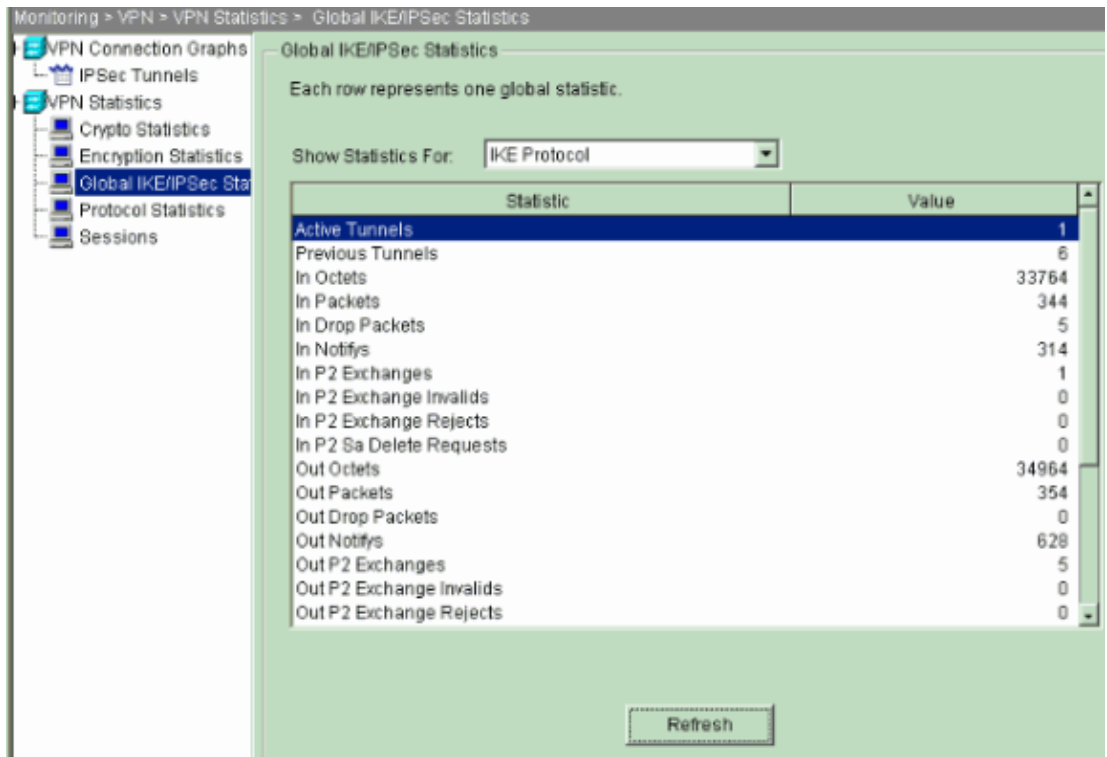
3. Click **Add** to select the graphs available in order to view in the graph window.



4. Click **Show Graphs** in order to view the graphs of both IKE and IPsec active tunnels.



5. Choose **Monitoring > VPN > VPN Statistics > Global IKE/IPsec Statistics** in order to know about the statistical information of the VPN tunnel.



You can also verify the formation of tunnels using CLI. Issue the **show crypto isakmp sa** command to check the formation of tunnels and issue the **show crypto ipsec sa** command to observe the number of packets encapsulated, encrypted, and so forth.

pix515-704

```

pixfirewall(config)#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    : L2L           Role    : initiator
   Rekey   : no           State   : MM_ACTIVE

```

pix515-704

```

pixfirewall(config)#show crypto ipsec sa
interface: outside
  Crypto map tag: outside_map, seq num: 20, local addr: 10.10.10.1

  access-list outside_cryptomap_20 permit ip 172.22.1.0
    255.255.255.0 172.16.1.0 255.255.255.0
  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: 10.20.20.1

  #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
  #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 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 76, media mtu 1500

```

```
current outbound spi: 44532974

inbound esp sas:
  spi: 0xA87AD6FA (2826622714)
  transform: esp-aes-256 esp-sha-hmac
  in use settings = {L2L, Tunnel, }
  slot: 0, conn_id: 1, crypto-map: outside_map
  sa timing: remaining key lifetime (kB/sec): (3824998/28246)
  IV size: 16 bytes
  replay detection support: Y
outbound esp sas:
  spi: 0x44532974 (1146300788)
  transform: esp-aes-256 esp-sha-hmac
  in use settings = {L2L, Tunnel, }
  slot: 0, conn_id: 1, crypto-map: outside_map
  sa timing: remaining key lifetime (kB/sec): (3824998/28245)
  IV size: 16 bytes
  replay detection support: Y
```

Troubleshoot

PFS

In IPsec negotiations, Perfect Forward Secrecy (PFS) ensures that each new cryptographic key is unrelated to any previous key. Either enable or disable PFS on both the tunnel peers, otherwise the L2L IPsec tunnel is not established in PIX/ASA.

PFS is disabled by default. In order to enable PFS use the **pfs** command with the *enable* keyword in group-policy configuration mode. In order to disable PFS, enter the *disable* keyword.

```
hostname(config-group-policy)#pfs {enable | disable}
```

In order to remove the PFS attribute from the running configuration, enter the **no** form of this command. A group policy can inherit a value for PFS from another group policy. Enter the **no** form of this command in order to prevent inheriting a value.

```
hostname(config-group-policy)#no pfs
```

Management-Access

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

The inside interface of the PIX cannot be pinged from the other end of the tunnel unless the **management-access** command is configured in the global configuration mode.

```
PIX-02(config)#management-access inside
PIX-02(config)#show management-access
management-access inside
```

Debug Commands

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

debug crypto isakmp Displays debug information about IPsec connections, and shows the first set of attributes that are denied due to incompatibilities on both ends.

debug crypto isakmp

```
pixfirewall(config)#debug crypto isakmp 7
Nov 27 12:01:59 [IKEv1 DEBUG]: Pitcher: received a key acquire message,
spi 0x0
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE Initiator: New Phase 1,
Intf 2, IKE Peer 10.20.20.1 local Proxy Address 172.22.1.0, remote
Proxy Address 172.16.1.0, Crypto map (outside_map)
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing ISAKMP SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing Fragmentation
VID + extended capabilities payload
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message
(msgid=0) with payloads : HDR +
  SA (1) + VENDOR (13) + NONE (0) total length : 148
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 112
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Oakley proposal is acceptable
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Fragmentation VID
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, IKE Peer included
IKE fragmentation capability flags
: Main Mode:          True Aggressive Mode: True
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing Cisco Unity VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing xauth V6 VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send IOS VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send Altiga/
Cisco VPN3000/Cisco ASA GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NONE (0) total length
: 320
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
NONE (0) total length : 320
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ISA_KE payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Cisco Unity client VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received xauth V6 VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing VPN3000/ASA
spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Altiga/Cisco VPN3000/Cisco ASA
GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating keys
for Initiator...
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Computing hash for ISAKMP
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Constructing IOS keep alive payload: proposal=32767/32767 sec.
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
```

```
constructing dpd vid payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) +
NONE (0) total length : 119
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) +
NONE (0) total length : 96
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Computing hash for ISAKMP
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Processing IOS keep alive payload: proposal=32767/32767 sec.
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Received DPD VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel_group 10.20.20.1
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Oakley begin quick mode
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, PHASE 1 COMPLETED
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Keep-alive type for this connection: DPD
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Starting phase 1 rekey timer: 73440000 (ms)
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, IKE got
SPI from key engine: SPI = 0x44ae0956
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
oakley constructing quick mode
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing blank hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing IPsec SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing IPsec nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing proxy ID
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Transmitting Proxy Id:
  Local subnet: 172.22.1.0 mask 255.255.255.0 Protocol 0 Port 0
  Remote subnet: 172.16.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
constructing qm hash payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message
(msgid=d723766b) with payloads
: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) +
NONE (0) total length : 200
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE RECEIVED Message
(msgid=d723766b) with payloads
: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
total length : 172
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
loading all IPSEC SAs
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Generating Quick Mode Key!
```

```

Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Generating Quick Mode Key!
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,
Security negotiation complete for LAN-to-LAN Group (10.20.20.1)
Initiator, Inbound SPI = 0x44ae0956, Outbound SPI = 0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
oakley constructing final quick mode
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE SENDING Message
(msgid=d723766b) with payloads
: HDR + HASH (8) + NONE (0) total length : 76
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
IKE got a KEY_ADD msg for SA: SPI = 0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1,
Pitcher: received KEY_UPDATE, spi 0x44ae0956
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,
Starting P2 Rekey timer to expire in 24480 seconds
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1,
PHASE 2 COMPLETED (msgid=d723766b)

```

debug crypto ipsec Displays debug information about IPsec connections.

```

debug crypto ipsec
pixl(config)#debug crypto ipsec 7

exec mode commands/options:
<1-255> Specify an optional debug level (default is 1)
<cr>
pixl(config)# debug crypto ipsec 7
pixl(config)# IPSEC: New embryonic SA created @ 0x024211B0,
SCB: 0x0240AEB0,
Direction: inbound
SPI      : 0x2A3E12BE
Session ID: 0x00000001
VPIF num : 0x00000001
Tunnel type: l2l
Protocol  : esp
Lifetime  : 240 seconds
IPSEC: New embryonic SA created @ 0x0240B7A0,
SCB: 0x0240B710,
Direction: outbound
SPI      : 0xB283D32F
Session ID: 0x00000001
VPIF num : 0x00000001
Tunnel type: l2l
Protocol  : esp
Lifetime  : 240 seconds
IPSEC: Completed host OBSA update, SPI 0xB283D32F
IPSEC: Updating outbound VPN context 0x02422618, SPI 0xB283D32F
Flags: 0x00000005
SA      : 0x0240B7A0
SPI     : 0xB283D32F
MTU     : 1500 bytes
VCID    : 0x00000000
Peer    : 0x00000000
SCB     : 0x0240B710
Channel: 0x014A45B0
IPSEC: Completed outbound VPN context, SPI 0xB283D32F
VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
Rule ID: 0x01FA0290
IPSEC: New outbound permit rule, SPI 0xB283D32F
Src addr: 10.10.10.1
Src mask: 255.255.255.255
Dst addr: 10.20.20.1

```

```
Dst mask: 255.255.255.255
Src ports
  Upper: 0
  Lower: 0
  Op   : ignore
Dst ports
  Upper: 0
  Lower: 0
  Op   : ignore
Protocol: 50
Use protocol: true
SPI: 0xB283D32F
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xB283D32F
  Rule ID: 0x0240AF40
IPSEC: Completed host IBSA update, SPI 0x2A3E12BE
IPSEC: Creating inbound VPN context, SPI 0x2A3E12BE
  Flags: 0x00000006
  SA   : 0x024211B0
  SPI  : 0x2A3E12BE
  MTU  : 0 bytes
  VCID : 0x00000000
  Peer : 0x02422618
  SCB  : 0x0240AEB0
  Channel: 0x014A45B0
IPSEC: Completed inbound VPN context, SPI 0x2A3E12BE
  VPN handle: 0x0240BF80
IPSEC: Updating outbound VPN context 0x02422618, SPI 0xB283D32F
  Flags: 0x00000005
  SA   : 0x0240B7A0
  SPI  : 0xB283D32F
  MTU  : 1500 bytes
  VCID : 0x00000000
  Peer : 0x0240BF80
  SCB  : 0x0240B710
  Channel: 0x014A45B0
IPSEC: Completed outbound VPN context, SPI 0xB283D32F
  VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
  Rule ID: 0x01FA0290
IPSEC: Completed outbound outer SPD rule, SPI 0xB283D32F
  Rule ID: 0x0240AF40
IPSEC: New inbound tunnel flow rule, SPI 0x2A3E12BE
  Src addr: 172.16.1.0
  Src mask: 255.255.255.0
  Dst addr: 172.22.1.0
  Dst mask: 255.255.255.0
  Src ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Protocol: 0
  Use protocol: false
  SPI: 0x00000000
  Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x2A3E12BE
  Rule ID: 0x0240B108
IPSEC: New inbound decrypt rule, SPI 0x2A3E12BE
  Src addr: 10.20.20.1
  Src mask: 255.255.255.255
  Dst addr: 10.10.10.1
  Dst mask: 255.255.255.255
```

```
Src ports
  Upper: 0
  Lower: 0
  Op   : ignore
Dst ports
  Upper: 0
  Lower: 0
  Op   : ignore
Protocol: 50
Use protocol: true
SPI: 0x2A3E12BE
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x2A3E12BE
Rule ID: 0x02406E98
IPSEC: New inbound permit rule, SPI 0x2A3E12BE
Src addr: 10.20.20.1
Src mask: 255.255.255.255
Dst addr: 10.10.10.1
Dst mask: 255.255.255.255
Src ports
  Upper: 0
  Lower: 0
  Op   : ignore
Dst ports
  Upper: 0
  Lower: 0
  Op   : ignore
Protocol: 50
Use protocol: true
SPI: 0x2A3E12BE
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x2A3E12BE
Rule ID: 0x02422C78
```

Related Information

- [Redundant Tunnel Creation between Firewalls using PDM](#)
- [Cisco PIX Firewall Software](#)
- [Cisco Adaptive Security Device Manager](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Security Product Field Notices \(including PIX\)](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

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

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 21, 2009

Document ID: 67912
