Configuration Professional: Site-to-Site IPsec VPN Between ASA/PIX and an IOS Router Configuration Example

Document ID: 112153 **Updated:** Sep 22, 2014

Contents

Introduction

This document provides a sample configuration for the LAN-to-LAN (Site-to-Site) IPsec tunnel between Cisco Security Appliances (ASA/PIX) and a Cisco IOS® Router using Cisco Configuration Professional (Cisco CP). Static routes are used for simplicity.

Refer to PIX/ASA 7.x Security Appliance to an IOS Router LAN-to-LAN IPsec Tunnel Configuration Example in order to learn more about the same scenario where the PIX/ASA Security Appliance runs software version 7.*x*.

Prerequisites

Requirements

Make sure that you meet these requirements before you attempt this configuration:

- End-to-End IP connectivity must be established before starting this configuration.
- The Security Appliance license must be enabled for Data Encryption Standard (DES) encryption (at a minimum encryption level).

Components Used

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

- Cisco Adaptive Security Appliance (ASA) with version 8.x and later
- ASDM version 6.x.and later
- Cisco 1841 Router with Cisco IOS Software Release 12.4(15T)
- Cisco CP Version 2.1

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

Note: Refer to Basic Router Configuration Using Cisco Configuration Professional in order to allow the router to be configured by Cisco CP.

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.

Related Products

This configuration can also be used with the Cisco PIX 500 Series Security Appliance, which runs version 7.x and later.

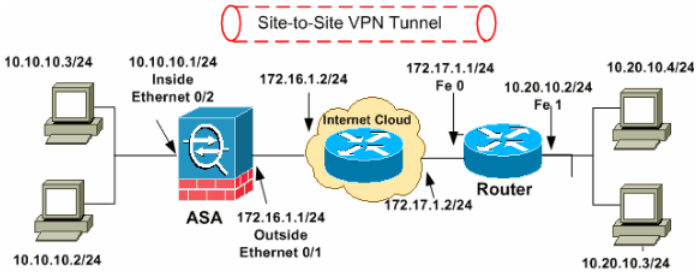
Conventions

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

Configuration

Network Diagram

This document uses this network setup:



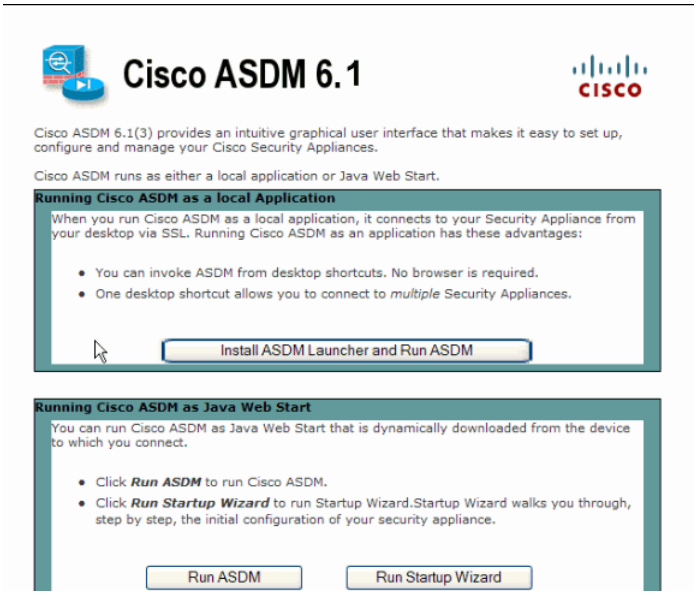
Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses, which have been used in a lab environment.

- VPN Tunnel ASDM Configuration
- Router Cisco CP Configuration
- ASA CLI Configuration
- Router CLI Configuration

VPN Tunnel ASDM Configuration

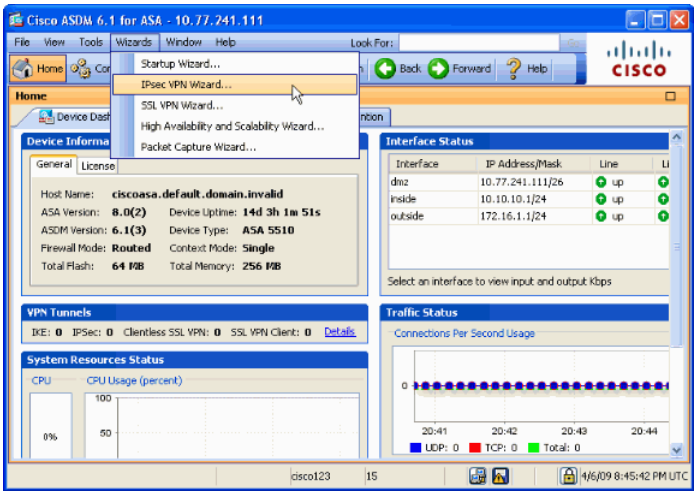
Perform these steps in order to create the VPN tunnel:

1. Open your browser and enter **https://<IP_Address of the interface of ASA that has been configured for ASDM Access>** to access the ASDM on the ASA.
   Make sure to authorize any warnings your browser gives you related to SSL certificate authenticity. The default username and password are both blank.
   The ASA 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.

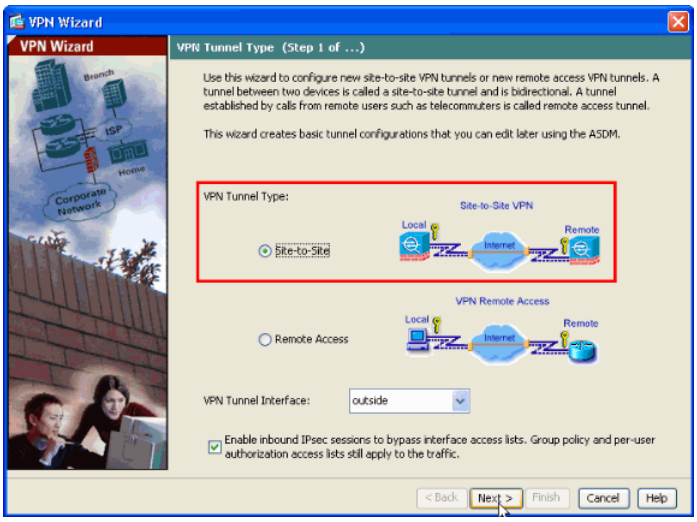


2. Click **Download ASDM Launcher and Start ASDM** in order to download the installer for the ASDM application.
3. Once the ASDM Launcher downloads, perform the steps directed by the prompts in order to install the software and run the Cisco ASDM Launcher.
4. Enter the IP address for the interface you configured with the **http -** command. Also, enter a username and password if you specified one.
   This example uses *cisco123* for both the username and the password.

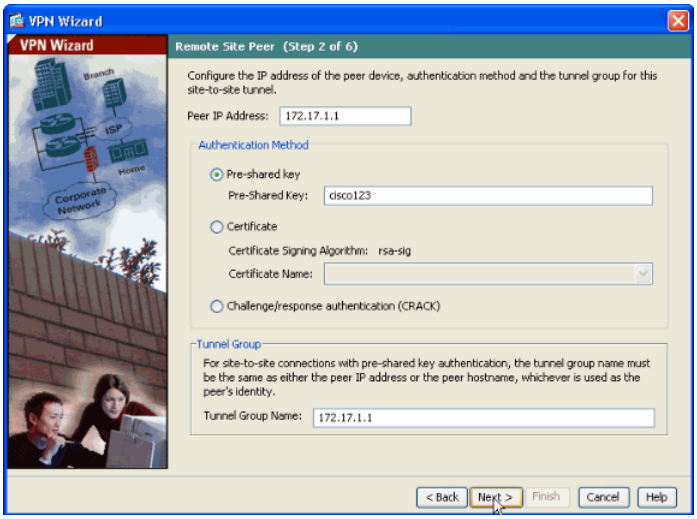
5. Run the **IPsec VPN Wizard** once the ASDM application connects to the ASA.



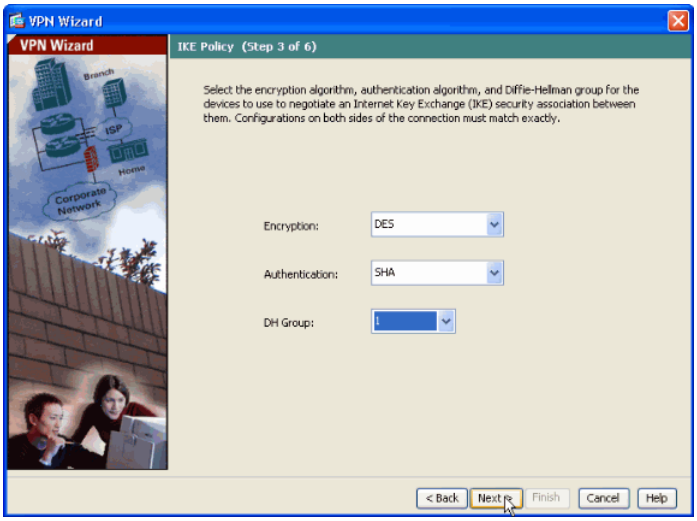
3. Choose **Site-to-Site** for the IPsec VPN Tunnel Type, and click **Next**.



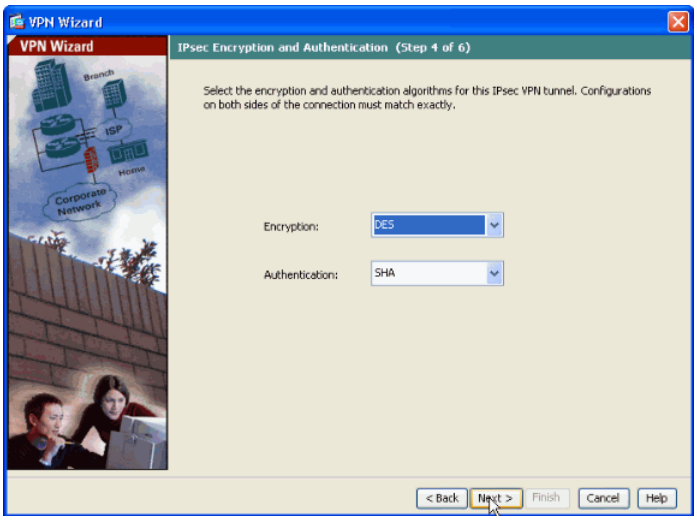
7. Specify the outside IP address of the remote peer. Enter the authentication information to use, which is the pre-shared key in this example. The pre-shared key used in this example is *cisco123*. The Tunnel Group Name will be your outside IP address by default if you configure L2L VPN. Click **Next**.



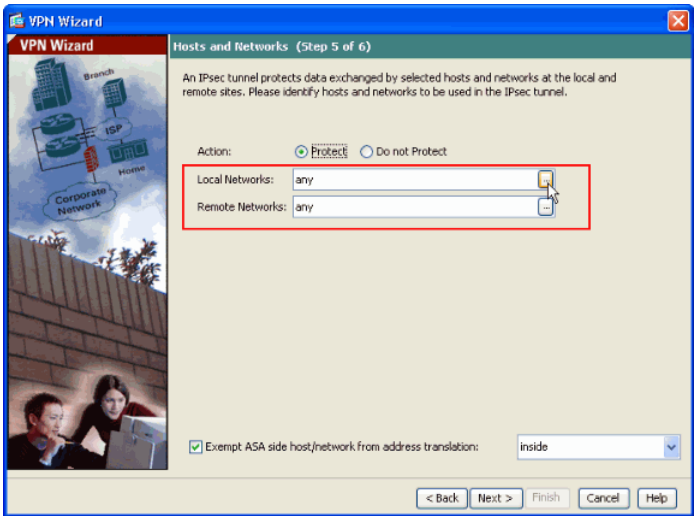
8. Specify the attributes to use for IKE, also known as Phase 1. These attributes must be the same on both the ASA and the IOS Router. Click **Next**.



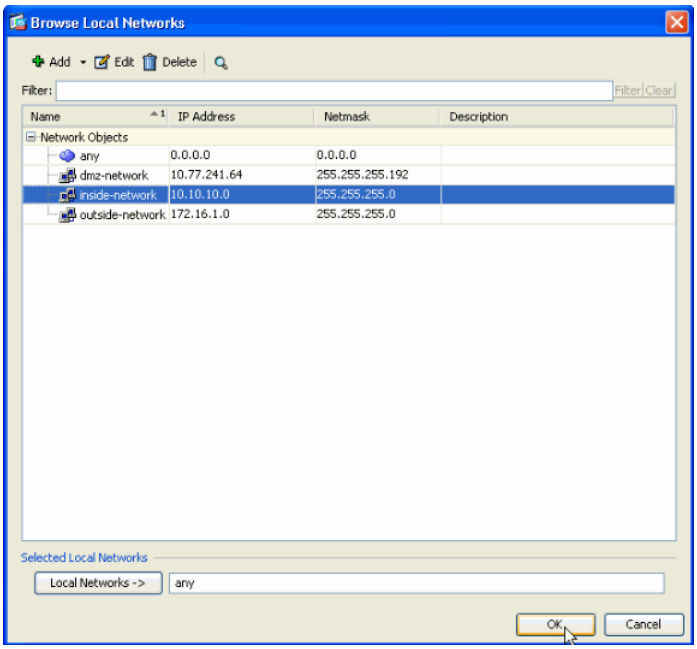
). Specify the attributes to use for IPsec, also known as Phase 2. These attributes must match on both the ASA and the IOS Router. Click **Next**.



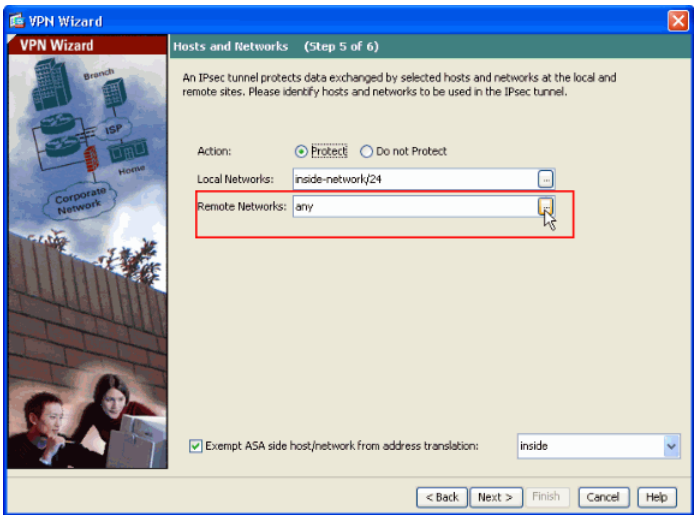
). Specify the hosts whose traffic should be allowed to pass through the VPN tunnel. In this step, you have to provide the Local Networks and Remote Networks for the VPN Tunnel. Click the button next to **Local Networks** as shown here to choose the local network address from the drop-down menu.



). Choose the **Local Network** address, and click **OK**.

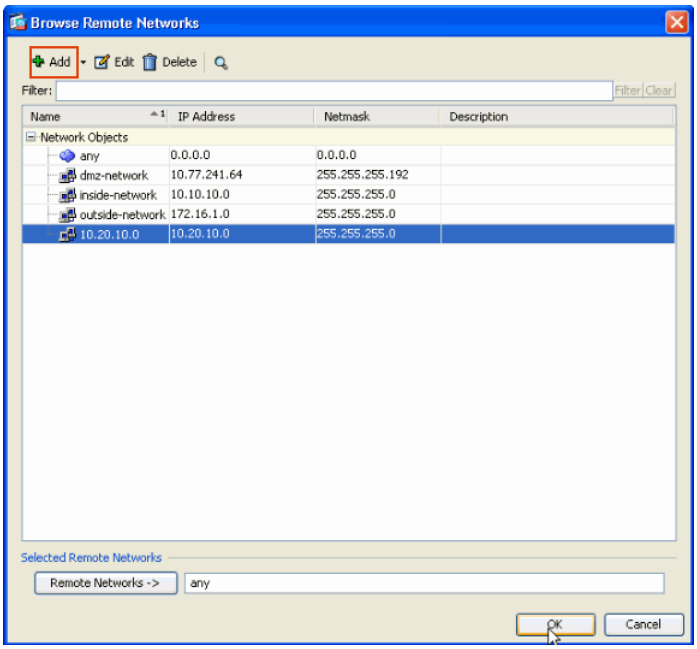


2. Click the button next to **Remote Networks** in order to choose the remote network address from the drop-down menu.

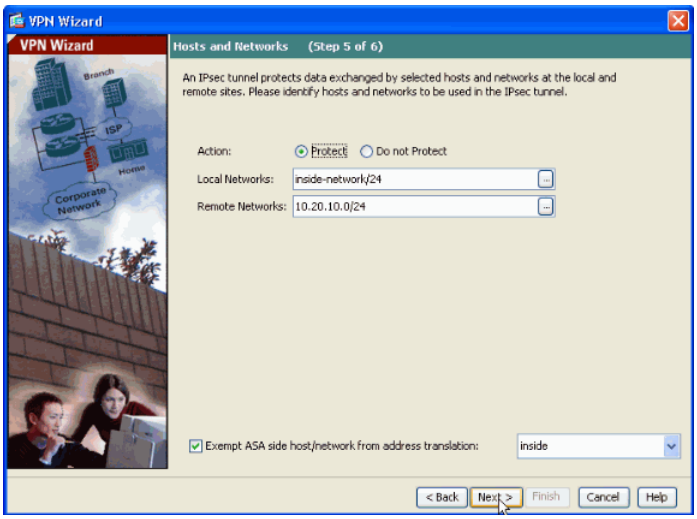


3. Choose the **Remote Network** address, and click **OK**.

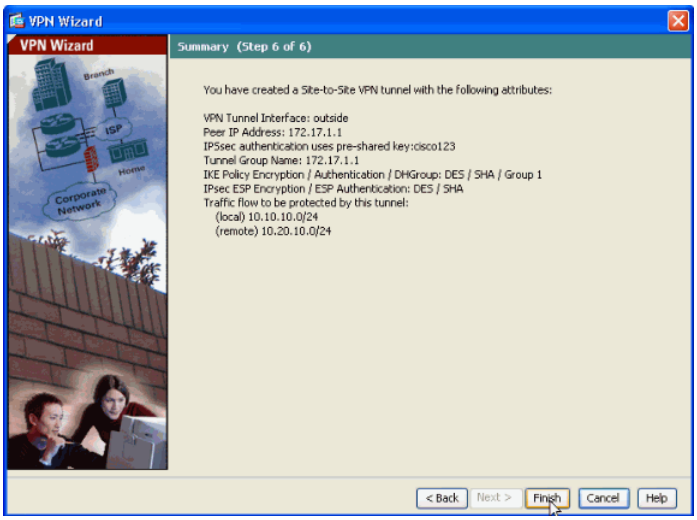
Note: If you do not have the Remote Network in the list, then the network has to be added to the list. Click **Add** in order to do so.



4. Check the **Exempt ASA side host/network from address translation** checkbox in order to prevent the tunnel traffic from undergoing Network Address Translation. Click **Next**.



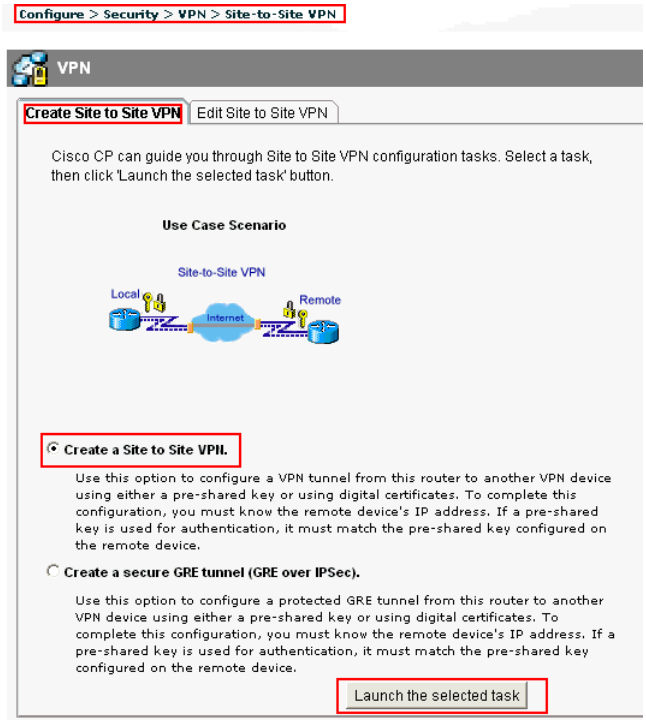
5. The attributes defined by the VPN Wizard are displayed in this summary. Double check the configuration and click **Finish** when you are satisfied that the settings are correct.



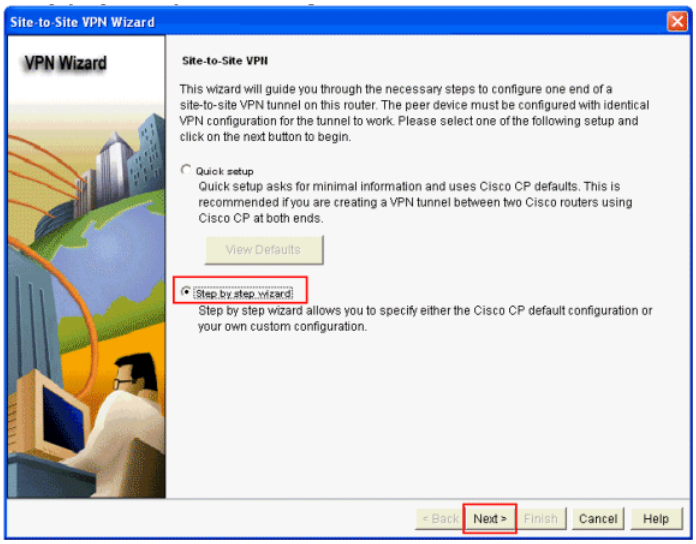
Router Cisco CP Configuration

Perform these steps in order to configure Site-to-Site VPN Tunnel on the Cisco IOS Router:

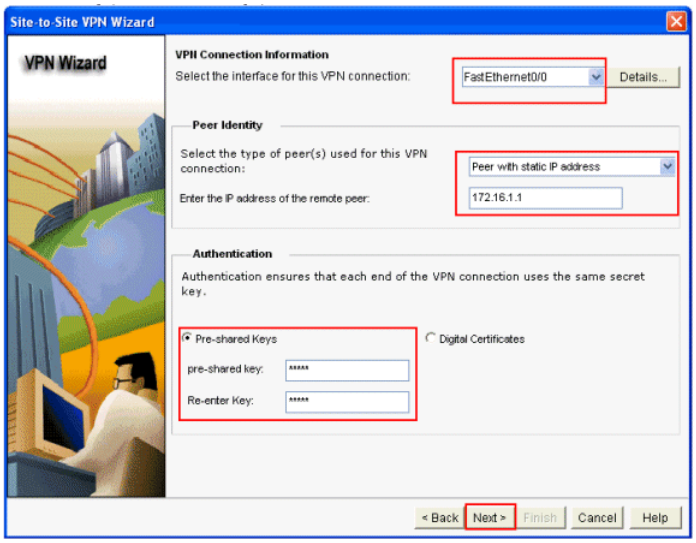
1. Choose **Configure** > **Security** > **VPN** > **Site-to-Site VPN**, and click the radio button next to **Create a Site-to-Site VPN**. Click **Launch the selected task**.



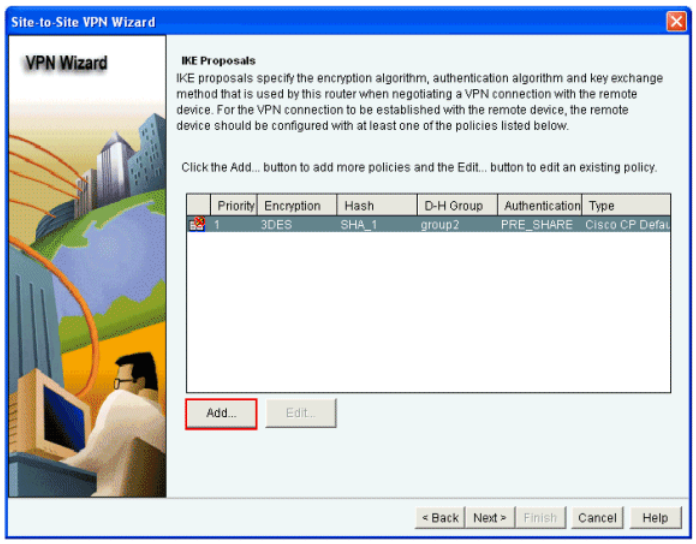
2. Choose **Step by step wizard** in order to proceed with the configuration, and click **Next**.



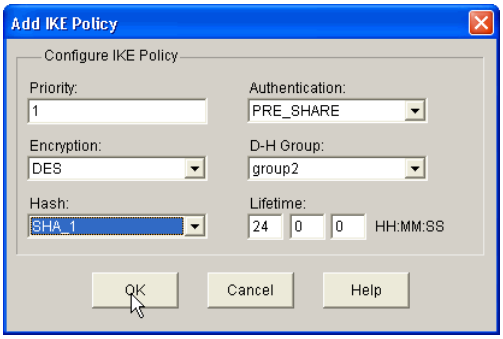
3. In the next window, provide the VPN Connection Information in the respective spaces. Choose the interface of the VPN Tunnel from the drop-down menu. Here, **FastEthernet0** is chosen. In the Peer Identity section, choose **Peer with static IP address** and provide the remote peer IP address. Then, provide the Pre-shared Keys (*cisco123* in this example) in the Authentication section. Lastly, click **Next**.



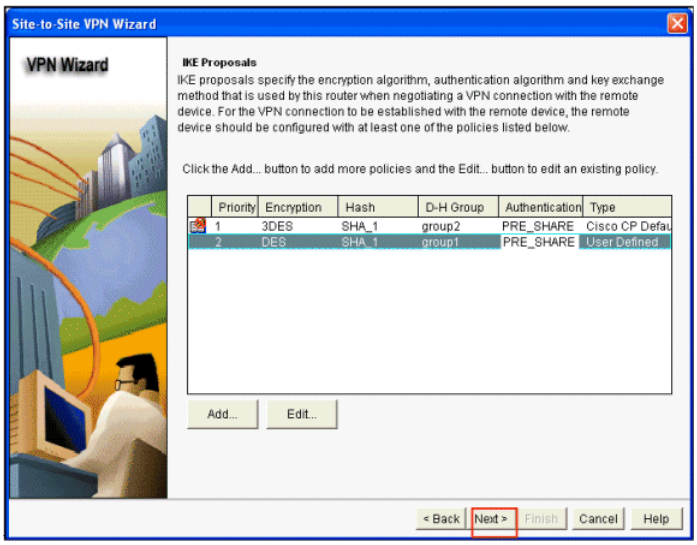
4. Click **Add** in order to add IKE proposals which specify the Encryption Algorithm, Authentication Algorithm, and the Key Exchange Method.



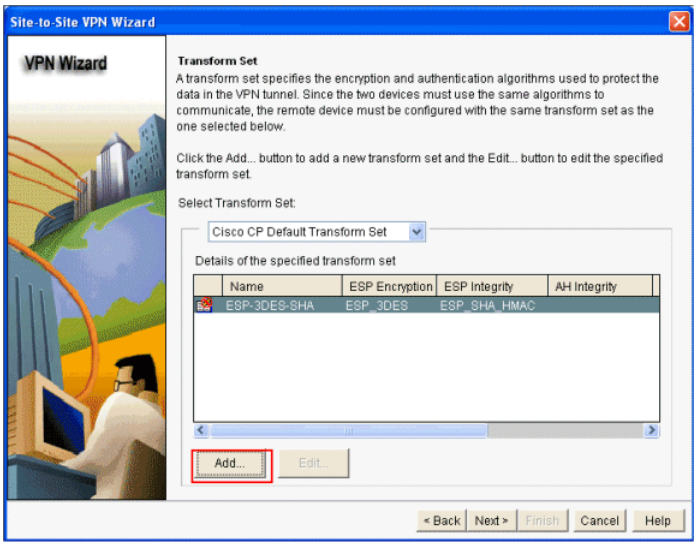
5. Provide the Encryption Algorithm, Authentication Algorithm, and Key Exchange method, and then click **OK**. The Encryption Algorithm, Authentication Algorithm, and the Key Exchange method values should match with the data provided in the ASA.



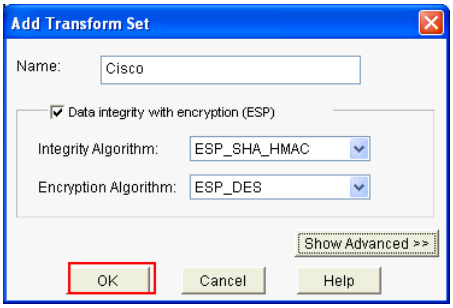
6. Click **Next**.



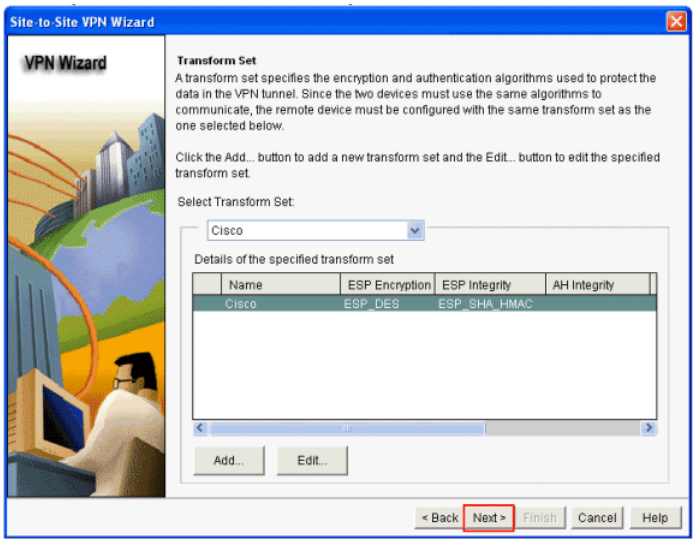
7. In this new window, the Transform Set details are provided. The Transform Set specifies the Encryption and Authentication algorithms used to protect Data in VPN Tunnel. Click **Add** in order to provide these details. You can add any number of Transform Sets as needed by using this method.



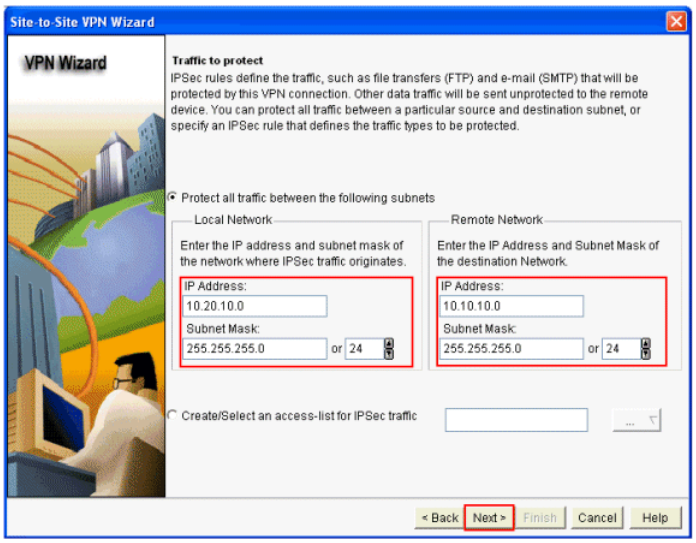
8. Provide the Transform Set details (Integrity and Encryption Algorithms), and click **OK**.



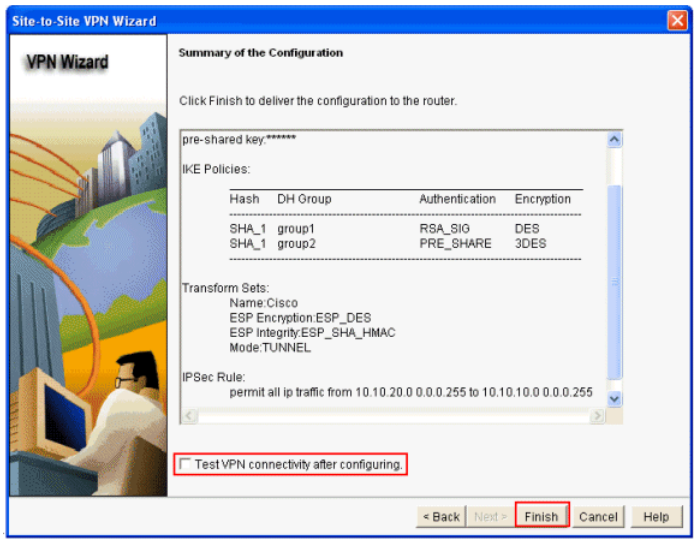
9. Choose the required **Transform Set** to be used from the drop-down menu, and click **Next**.



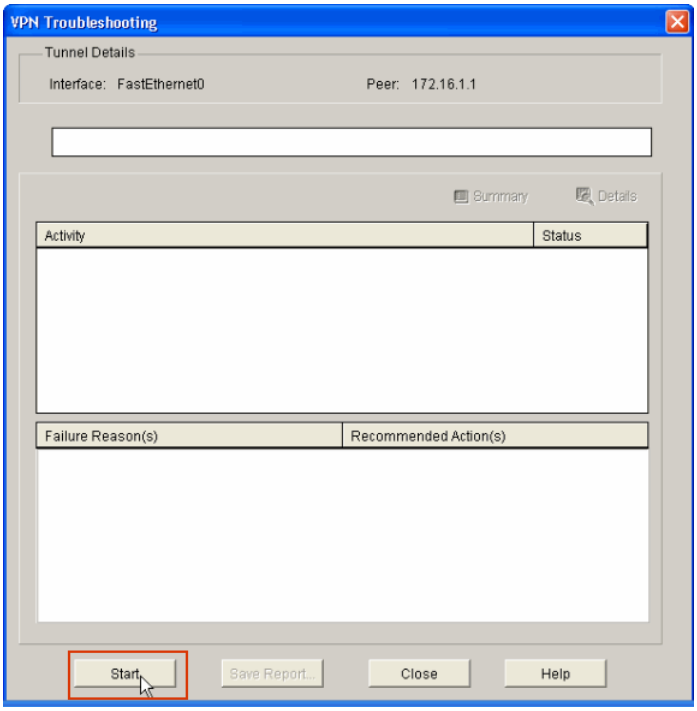
). In the following window, provide the details about the Traffic to be protected through the VPN Tunnel. Provide the Source and Destination Networks of the traffic to be protected so that the traffic between the specified source and destination networks are protected. In this example, the Source network is *10.20.10.0* and the Destination network is *10.10.10.0*. Click **Next**.



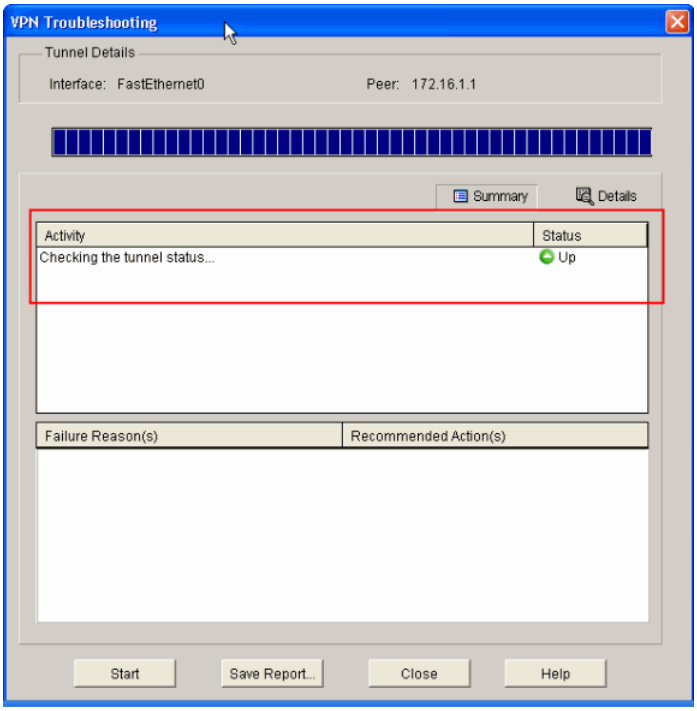
I. This window shows the summary of the Site-to-Site VPN configuration. Check the **Test VPN Connectivity after configuring** checkbox if you want to test the VPN connectivity. Here, the box is checked as the connectivity needs to be checked. Click **Finish**.



2. Click **Start** in order to check the VPN connectivity.



3. In the next window, the result of the VPN connectivity Test is provided. Here, you can see if the tunnel is Up or Down. In this example configuration, the Tunnel is "Up", as shown in green.



This completes the configuration on the Cisco IOS Router.

ASA CLI Configuration

```
ASA# show run
: Saved
ASA Version 8.2
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!

!--- Configure the outside interface. !

interface Ethernet0/1
 nameif outside
```

```
 security-level 0
 ip address 172.16.1.1 255.255.255.0

!--- Configure the inside interface. !

interface Ethernet0/2
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0



 !-- Output suppressed !

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

access-list 100 extended permit ip any any
access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0

 !--- This access list (inside_nat0_outbound) is used !--- with the nat zero command. This prevents traffic which !--- matches the access list from undergoing network ac
configuration.

access-list outside_1_cryptomap extended permit ip 10.10.10.0 255.255.255.0
10.20.10.0 255.255.255.0

!--- This access list (outside_cryptomap) is used !--- with the crypto map outside_map !--- to determine which traffic should be encrypted and sent !--- across the tunne

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm-613.bin
asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 10.10.10.0 255.255.255.0

nat (inside) 0 access-list inside_nat0_outbound

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


access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 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
http 0.0.0.0 0.0.0.0 dmz
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-DES-SHA esp-des esp-sha-hmac

!--- Define the transform set for Phase 2.



crypto map outside_map 1 match address outside_1_cryptomap

!--- Define which traffic should be sent to the IPsec peer.


crypto map outside_map 1 set peer 172.17.1.1

!--- Sets the IPsec peer


crypto map outside_map 1 set transform-set ESP-DES-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. !--- The configuration commands here define the Phase !--- 1 policy parameters that are us


crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 1
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!



tunnel-group 172.17.1.1 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 command !--- tunnel-group in globa


tunnel-group 172.17.1.1 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
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!


 !-- Output suppressed!

username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d
: end
```

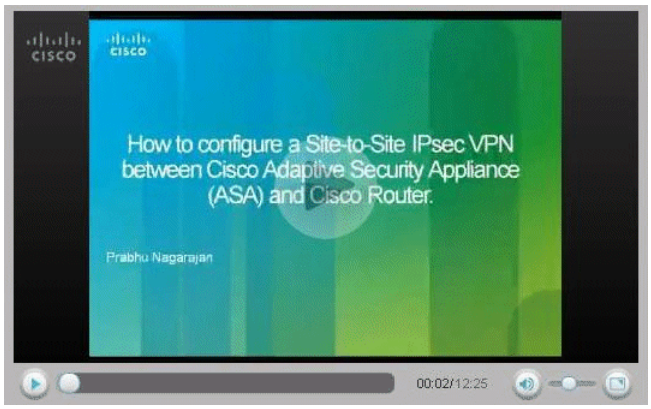
Router CLI Configuration

Router

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7 1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!


!--- Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are used
e chosen.


crypto isakmp policy 2
 authentication pre-share


!--- Specifies the pre-shared key "cisco123" which should !--- be identical at both peers. This is a global !--- configuration mode command.

crypto isakmp key cisco123 address 172.16.1.1
!
!

!--- Configuration for IPsec policies. !--- Enables the crypto transform configuration mode, !--- where you can specify the transform sets that are used !--- during an I

crypto ipsec transform-set ASA-IPSEC esp-des esp-sha-hmac
!


!--- Indicates that IKE is used to establish !--- the IPsec Security Association for protecting the !--- traffic specified by this crypto map entry.

crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1


!--- Sets the IP address of the remote end.

 set peer 172.16.1.1


!--- Configures IPsec to use the transform-set !--- "ASA-IPSEC" defined earlier in this configuration.

 set transform-set ASA-IPSEC


!--- !--- Specifies the interesting traffic to be encrypted.

 match address 100
!
!
!

!--- Configures the interface to use the !--- crypto map "SDM_CMAP_1" for IPsec.
```

```
interface FastEthernet0
 ip address 172.17.1.1 255.255.255.0
 duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface FastEthernet1
 ip address 10.20.10.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
!
interface Vlan1
 ip address 10.77.241.109 255.255.255.192
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!

!--- Configure the access-lists and map them to the Crypto map configured.

access-list 100 remark SDM_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
!
!
!

!--- This ACL 110 identifies the traffic flows using route map

access-list 110 deny ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
end
```

This video posted to the Cisco Support Community demonstrates how to configure Site-to-Site IPsec VPN between Cisco ASA and a Cisco Router:



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.

- ASA/PIX Security Appliance - **show** Commands
- Remote IOS Router - **show** Commands

ASA/PIX Security Appliance - show Commands

- **show crypto isakmp sa** - Shows all current IKE SAs at a peer.

```
ASA# 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: 172.17.1.1
```

```
      Type    : L2L             Role    : initiator
      Rekey   : no              State   : MM_ACTIVE
```

- **show crypto ipsec sa** - Shows all current IPsec SAs at a peer.

```
ASA# show crypto ipsec sa
                    interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
      current_peer: 172.17.1.1

     #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 9, #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.: 172.16.1.1, remote crypto endpt.: 172.17.1.1

      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 434C4A7F

    inbound esp sas:
      spi: 0xB7C1948E (3082917006)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x434C4A7F (1129073279)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
```

Remote IOS Router - show Commands

- **show crypto isakmp sa** - Shows all current IKE SAs at a peer.

```
Router# show crypto isakmp sa

dst             src             state          conn-id slot status
172.17.1.1      172.16.1.1      QM_IDLE              3    0 ACTIVE
```

- **show crypto ipsec sa** - Shows all current IPsec SAs at a peer.

```
Router# show crypto ipsec sa
                interface: FastEthernet0
    Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)

     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

- **show crypto engine connections active**—Shows current connections and information about encrypted and decrypted packets (router only).

```
Router#show crypto engine connections active

  ID Interface        IP-Address    State  Algorithm           Encrypt  Decrypt
   3 FastEthernet0    172.17.1.1    set    HMAC_SHA+DES_56_CB        0        0
```

```
2001 FastEthernet0    172.17.1.1    set    DES+SHA                0        59
2002 FastEthernet0    172.17.1.1    set    DES+SHA               59         0
```

Troubleshoot

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

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

Note: Refer to Important Information on Debug Commands and IP Security Troubleshooting - Understanding and Using debug Commands before you use **debug** commands.

- **debug crypto ipsec 7** - Displays the IPsec negotiations of phase 2.

  debug crypto isakmp 7 - Displays the ISAKMP negotiations of phase 1.
- **debug crypto ipsec** - Displays the IPsec negotiations of phase 2.

  debug crypto isakmp - Displays the ISAKMP negotiations of phase 1.

Refer to Most Common L2L and Remote Access IPSec VPN Troubleshooting Solutions for more information on troubleshooting Site-to-Site VPN.

Related Information

- **Cisco Configuration Professional Quick Start Guide**
- **Cisco Adaptive Security Device Manager**
- **Cisco PIX Firewall Software**
- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Cisco PIX Firewall Software**
- **Cisco Secure PIX Firewall Command References**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation - Cisco Systems**

© 2015 Cisco and/or its affiliates. All rights reserved.