

# Dynamic IPsec Tunnel Between a Statically Addressed ASA and a Dynamically Addressed Cisco IOS Router that uses CCP Configuration Example

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Verify](#)

[Verify tunnel parameters through CCP](#)

[Verify tunnel status through ASA CLI](#)

[Verify the tunnel parameters through Router CLI](#)

[Troubleshoot](#)

[Related Information](#)

## [Introduction](#)

This document provides a sample configuration for how to enable the PIX/ASA Security Appliance to accept dynamic IPsec connections from the Cisco IOS<sup>®</sup> router. In this scenario, the IPsec tunnel establishes when the tunnel is initiated from the Router end only. ASA could not initiate a VPN tunnel because of the dynamic IPsec configuration.

This configuration enables the PIX Security Appliance to create a dynamic IPsec LAN-to-LAN (L2L) tunnel with a remote VPN router. This router dynamically receive its outside public IP address from its Internet service provider. Dynamic Host Configuration Protocol (DHCP) provides this mechanism in order to allocate IP addresses dynamically from the provider. This allows IP addresses to be reused when hosts no longer need them.

The configuration on the Router is done with the use of the [Cisco Configuration Professional](#) (CCP). CCP is a GUI-based device management tool that allows you to configure Cisco IOS-based routers. Refer to [Basic Router Configuration Using Cisco Configuration Professional](#) for more information on how to configure a router with CCP.

Refer to [Site to Site VPN \(L2L\) with ASA](#) for more information and configuration examples on IPsec

tunnel establishment that use ASA and Cisco IOS Routers.

Refer to [Site to Site VPN \(L2L\) with IOS](#) for more information and a configuration example on dynamic IPsec tunnel establishment with the use of PIX and Cisco IOS Router.

## **Prerequisites**

### **Requirements**

Before you attempt this configuration, ensure that both the ASA and router have Internet connectivity in order to establish the IPSEC tunnel.

### **Components Used**

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

- Cisco IOS Router 1812 that runs Cisco IOS Software Release 12.4
- Cisco ASA 5510 software release 8.0.3

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**

In this scenario, 192.168.100.0 network is behind the ASA and 192.168.200.0 network is behind the Cisco IOS Router. It is assumed that the Router gets its public address through DHCP from its ISP. As this poses a problem in the configuration of a static peer on the ASA end, you need to approach the way of dynamic crypto configuration to establish a site-to-site tunnel between ASA and the Cisco IOS Router.

The Internet users at the ASA end get translated to the IP address of its outside interface. It is assumed that NAT is not configured on the Cisco IOS router end.

Now these are the main steps to be configured on the ASA end in order to establish dynamic tunnel:

1. Phase 1 ISAKMP related configuration
2. Nat exemption configuration
3. Dynamic crypto map configuration

The Cisco IOS router has a static crypto map configured because the ASA is assumed to have a static public IP address. Now this is the list of main steps to be configured on the Cisco IOS Router end to establish dynamic IPSEC tunnel.

1. Phase 1 ISAKMP related configuration

## 2. Static crypto map related configuration

These steps are described in detail in these configurations.

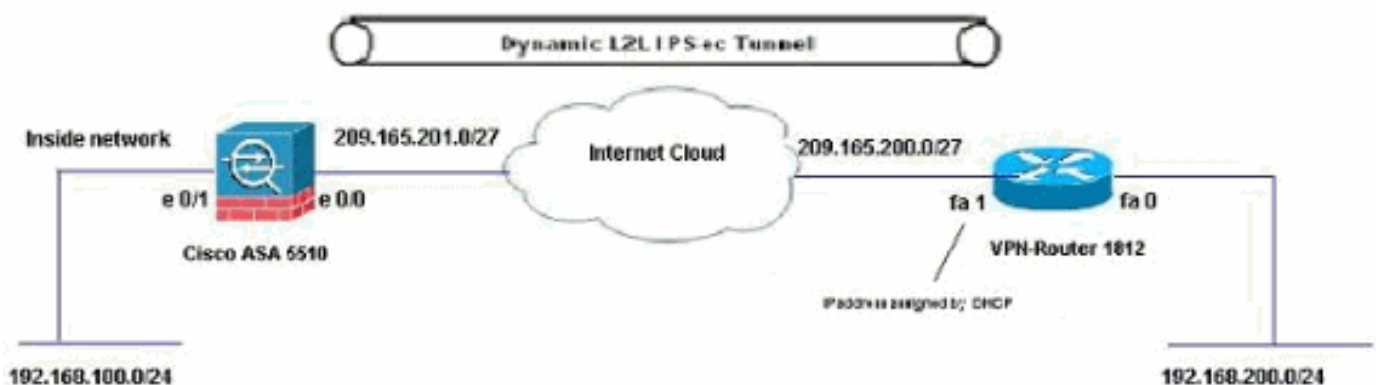
## Configure

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

## Network Diagram

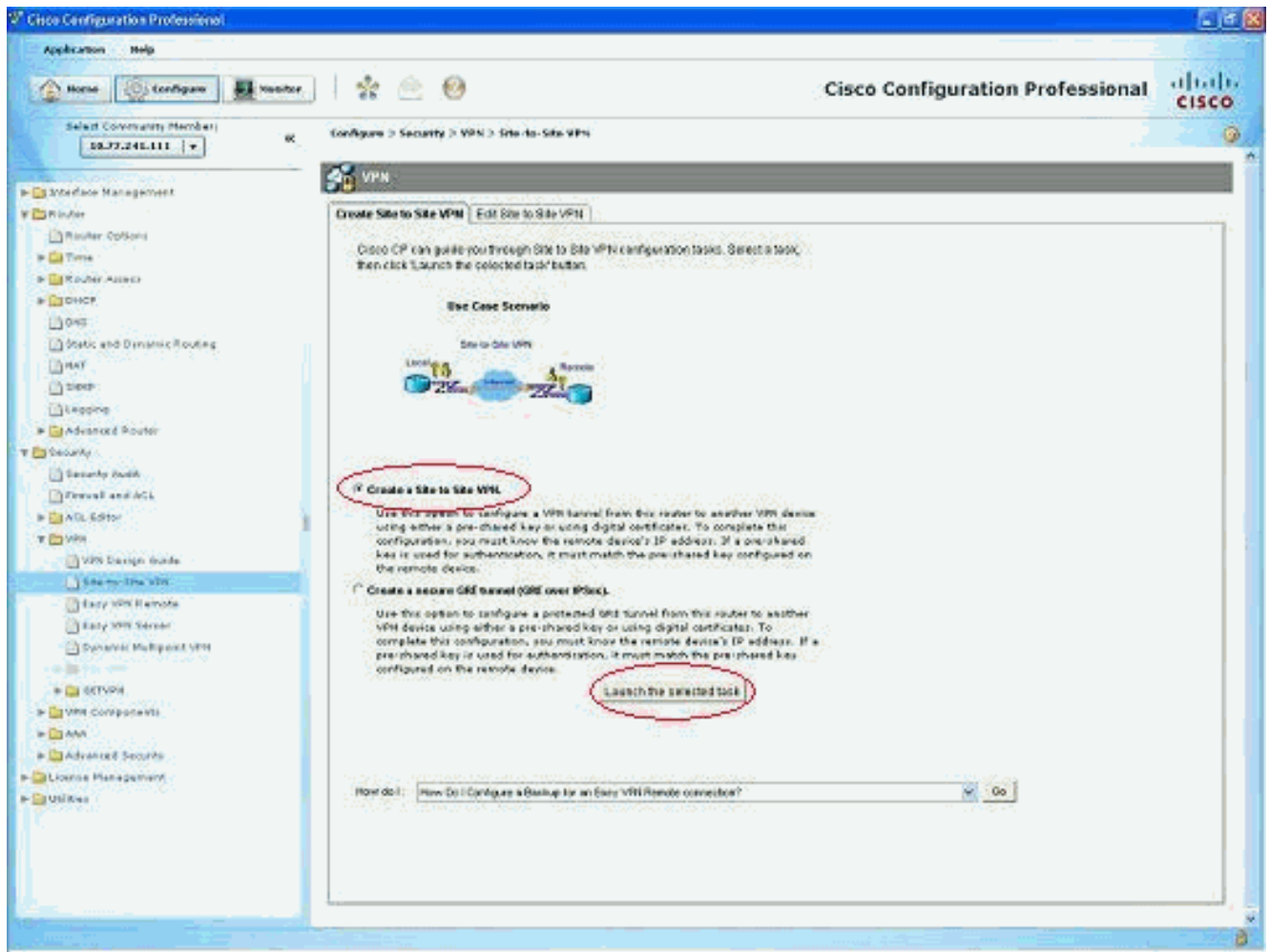
This document uses this network setup:



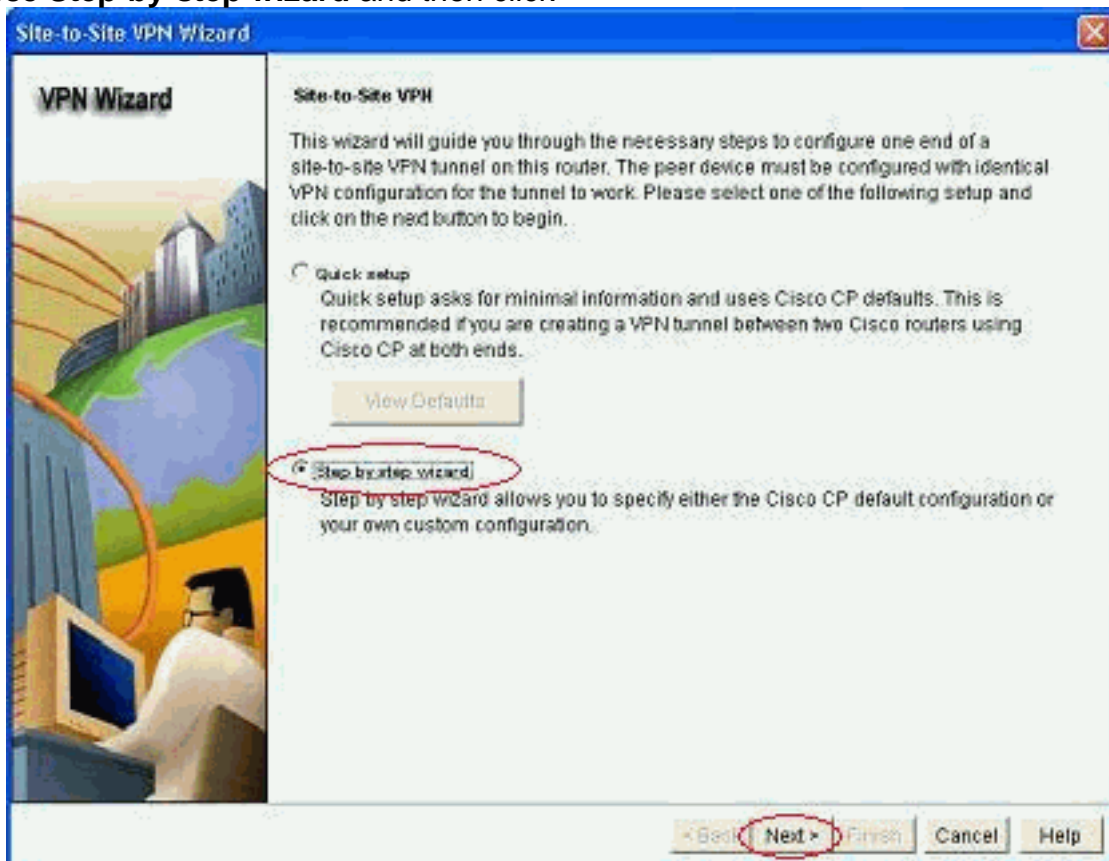
## Configurations

This is the IPsec VPN configuration on the VPN-Router with CCP. Complete these steps:

1. Open the CCP application and choose **Configure > Security > VPN > Site to Site VPN**. Click the **Launch the selected tab**.

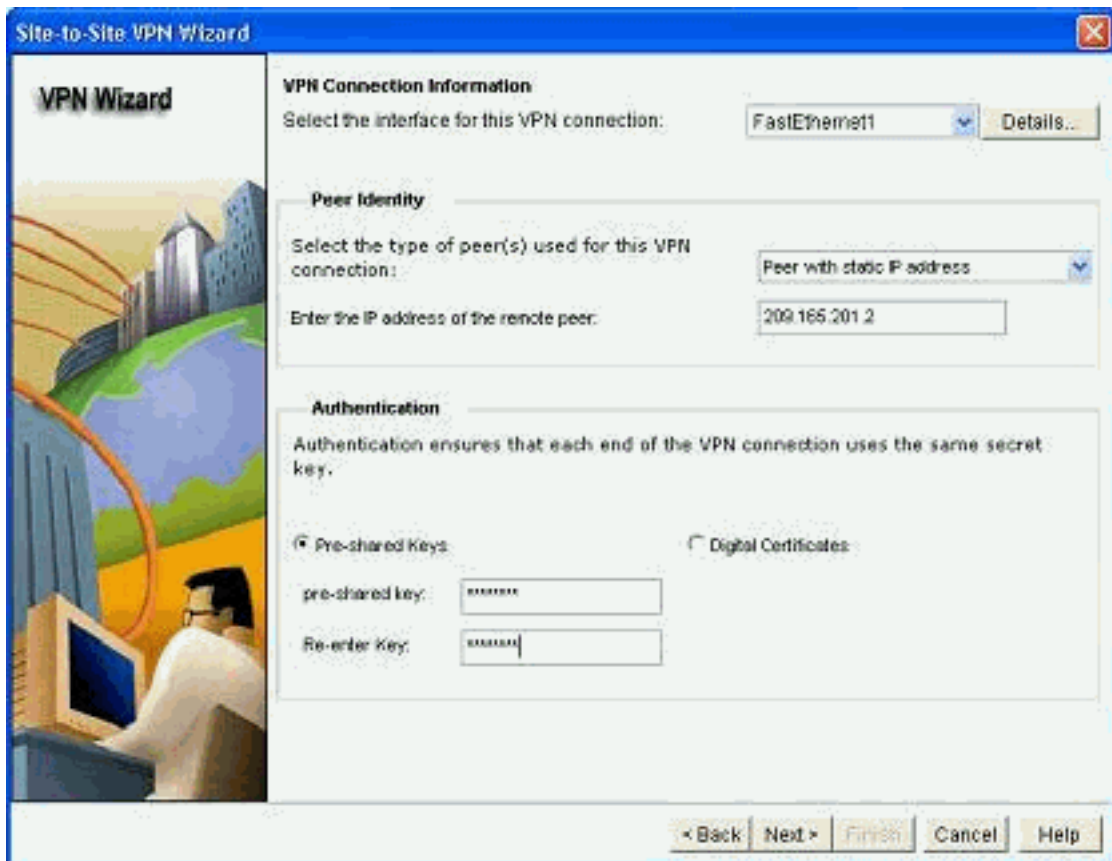


2. Choose **Step-by-step wizard** and then click



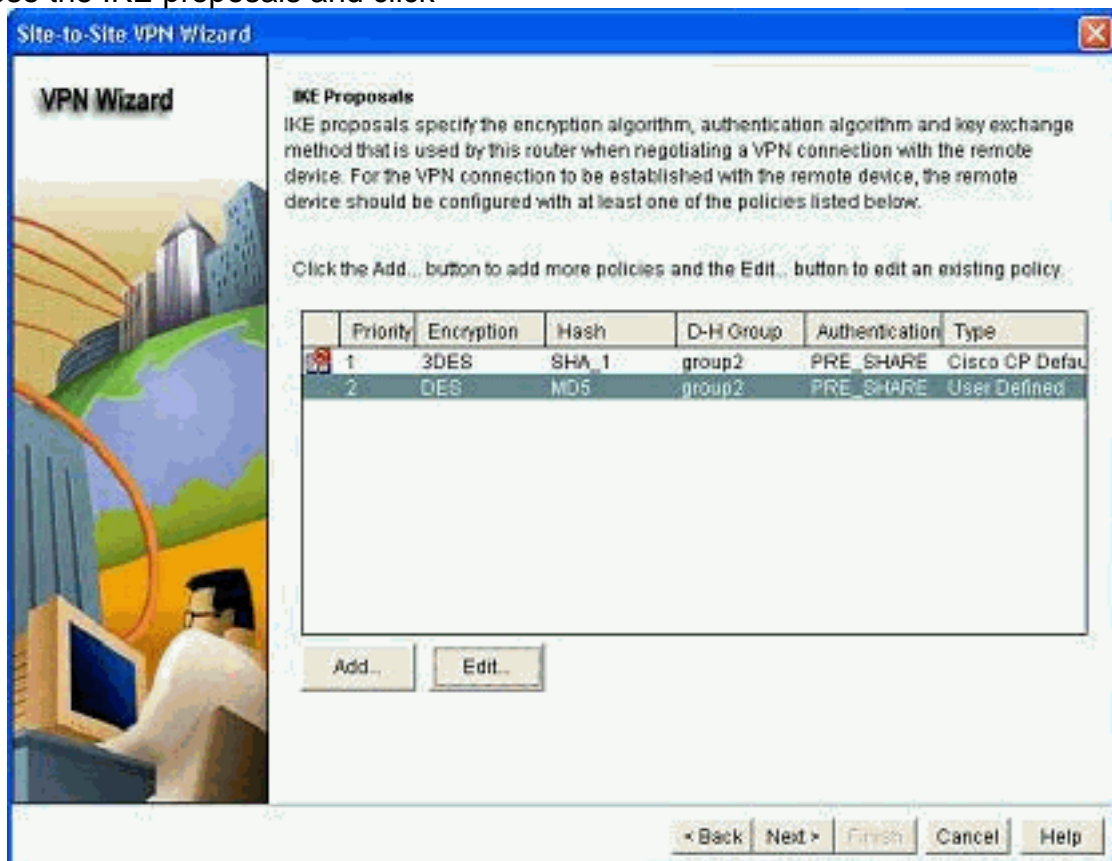
Next.

3. Fill in the remote peer IP address along with the authentication



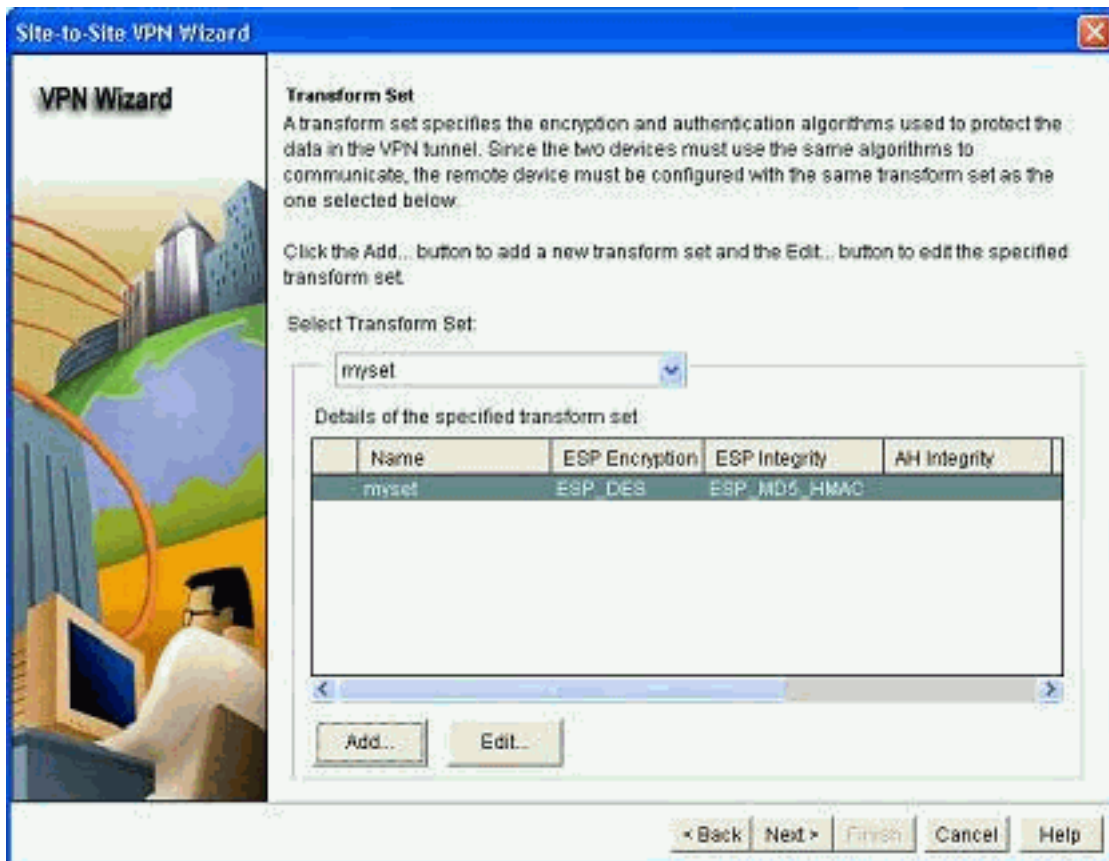
details.

4. Choose the IKE proposals and click



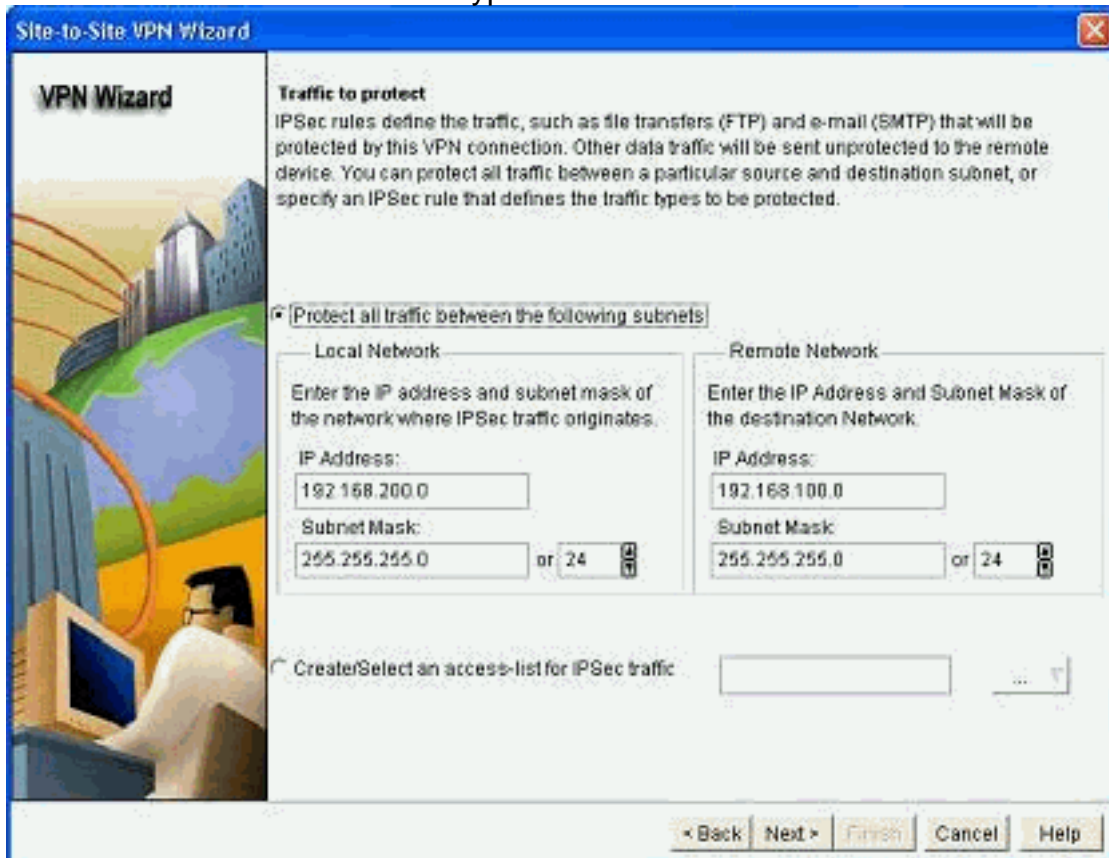
Next.

5. Define the transform-set details and click



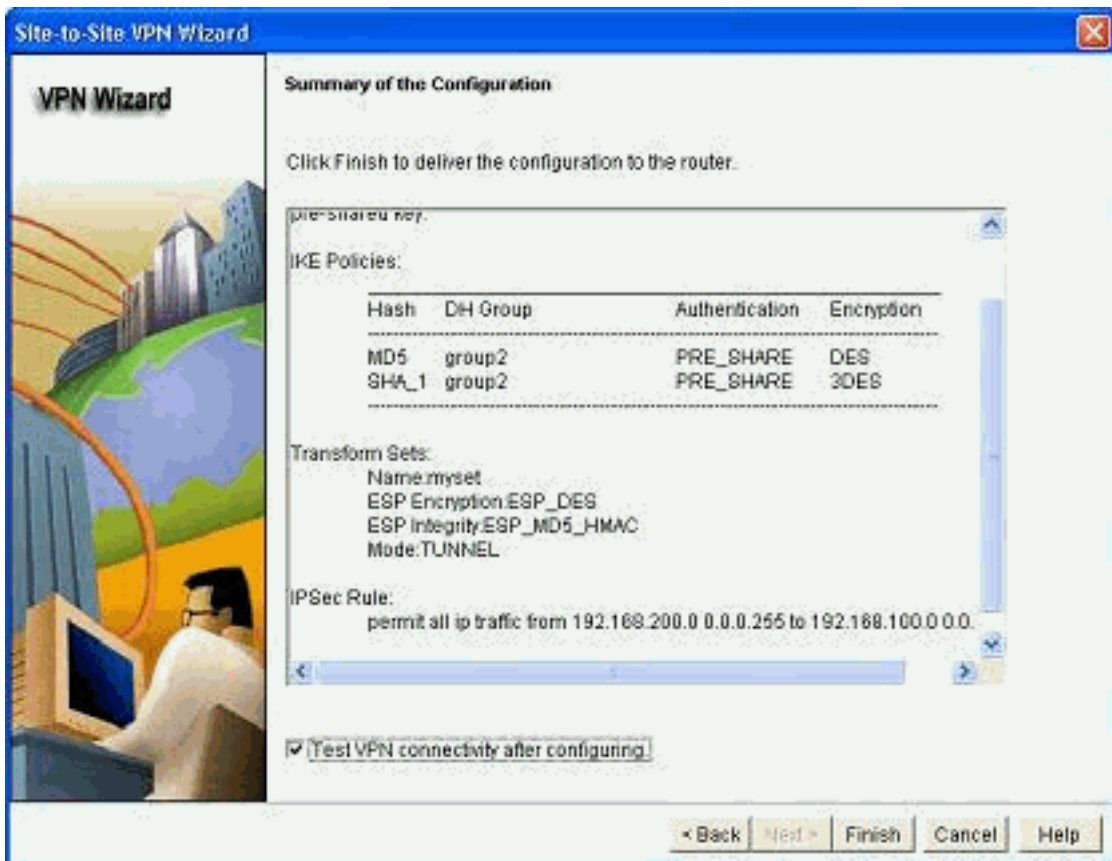
Next.

6. Define the traffic that needs to be encrypted and click



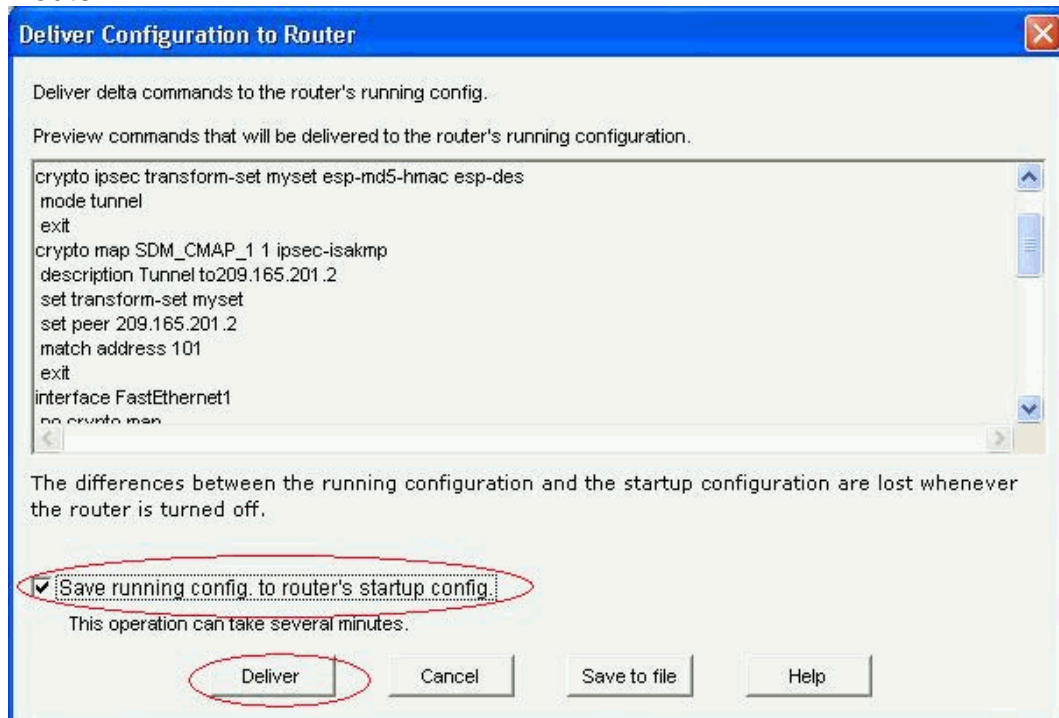
Next.

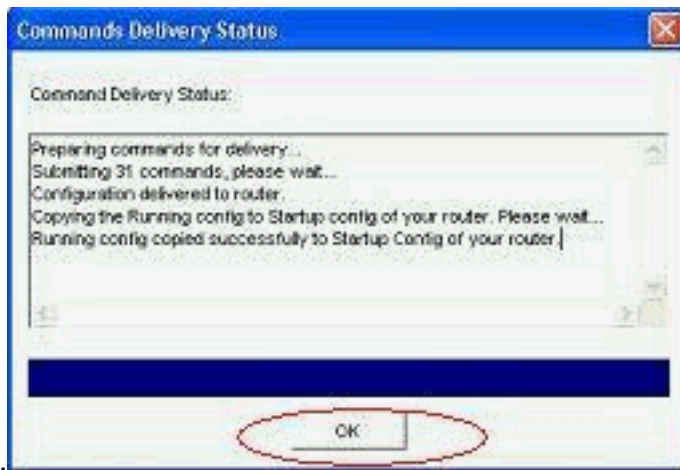
7. Verify the summary of the crypto IPsec configuration and click



**Finish.**

8. Click **Deliver** in order to send the configuration to the VPN-Router.





9. Click **OK**.

## CLI Configuration

- [Ciscoasa](#)
- [VPN-Router](#)

### Ciscoasa

```
ciscoasa(config)#show run : Saved : ASA Version 8.0(3) !
hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif outside
security-level 0 ip address 209.165.201.2
255.255.255.224 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 192.168.100.1
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive !--- Output suppressed access-list
nonat extended permit ip 192.168.100.0 255.255.255.0
192.168.200.0 255.255.255.0 no pager mtu outside 1500
mtu inside 1500 icmp unreachable rate-limit 1 burst-size
1 asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 ! !--- Define the nat-translation for
Internet users global (outside) 1 interface nat (inside)
1 192.168.100.0 255.255.255.0 ! ! !--- Define the nat-
exemption policy for VPN traffic nat (inside) 0 access-
list nonat ! route outside 0.0.0.0 0.0.0.0 209.165.201.1
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 ! !--- Configure the IPsec transform-set
crypto ipsec transform-set myset esp-des esp-md5-hmac !
! !--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset crypto dynamic-map
mymap 1 set reverse-route crypto map dyn-map 10 IPSec-
isakmp dynamic mymap crypto map dyn-map interface
outside ! !--- Configure the phase I ISAKMP policy
crypto isakmp policy 10 authentication pre-share
encryption des hash md5 group 2 lifetime 86400 ! ! !---
Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes pre-
shared-key * ! 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 prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa(config)#

```

CCP creates this configuration on the VPN-Router.

## VPN-Router

```

VPN-Router#show run Building configuration... ! version
12.4 service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname VPN-Router ! ! username cisco
privilege 15 secret 5 $1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRdfQ01 ! ! !--- Output
suppressed no aaa new-model ip subnet-zero ! ip cef !
crypto isakmp enable outside ! crypto isakmp policy 1
encrypt 3des authentication pre-share group 2 ! crypto
isakmp policy 2 hash md5 authentication pre-share group
2 ! ! crypto isakmp key cisco123 address 209.165.201.2 !
! crypto ipsec transform-set myset esp-des esp-md5-hmac
! ! crypto map SDM_CMAP_1 1 IPsec-isakmp description
Tunnel to209.165.201.2 set peer 209.165.201.2 set
transform-set myset match address 101 ! ! ! interface
BRI0 no ip address shutdown ! interface Dot11Radio0 no
ip address shutdown speed basic-1.0 basic-2.0 basic-5.5
6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root ! interface Dot11Radio1 no ip address
shutdown speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0
36.0 48.0 54.0 station-role root ! interface
FastEthernet0 ip address 192.168.200.1 255.255.255.0
duplex auto speed auto ! interface FastEthernet1 ip
address dhcp duplex auto speed auto crypto map
SDM_CMAP_1 ! interface FastEthernet2 no ip address
shutdown ! interface FastEthernet3 no ip address
shutdown ! interface FastEthernet4 no ip address
shutdown ! interface FastEthernet5 no ip address
shutdown ! interface FastEthernet6 no ip address
shutdown ! interface FastEthernet7 no ip address
shutdown ! interface FastEthernet8 no ip address
shutdown ! interface FastEthernet9 no ip address
shutdown ! interface Vlan1 no ip address ! ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1 ! ! !--- Output
suppressed ! ip http server ip http authentication local
ip http secure-server ! access-list 100 permit ip
0.0.0.0 255.255.255.0 0.0.0.0 255.255.255.0 access-list
101 remark CCP_ACL Category=4 access-list 101 remark
IPSEC Rule access-list 101 permit ip 192.168.200.0
0.0.0.255 192.168.100.0 0.0.0.255 ! ! ! ! control-plane
! ! line con 0 line aux 0 line vty 0 4 privilege level
15 login local transport input telnet ssh line vty 5 15
privilege level 15 login local transport input telnet
ssh ! no scheduler allocate end

```

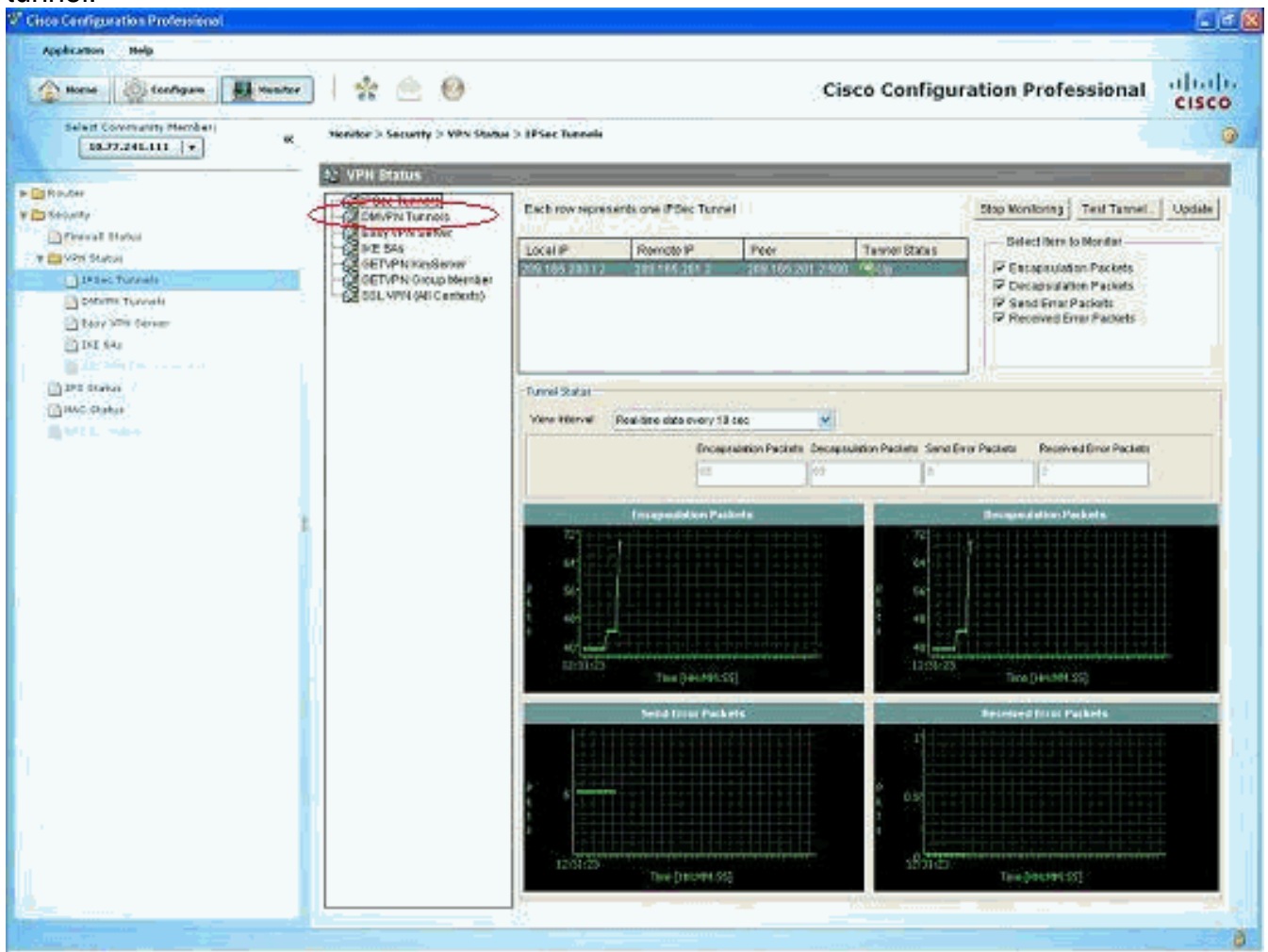
Use this section to confirm that your configuration works properly.

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

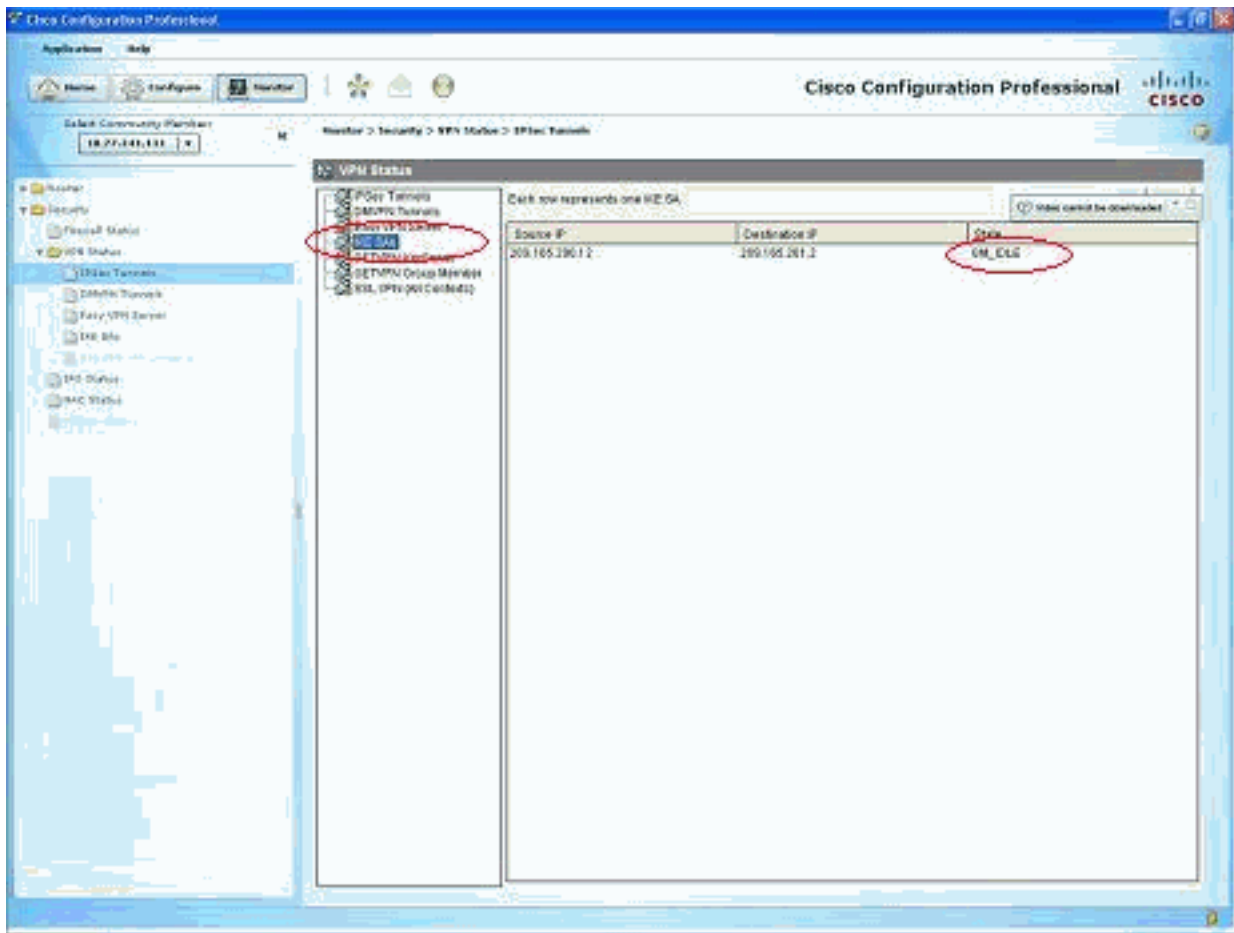
- [Verifying the tunnel parameters through CCP](#)
- [Verifying the tunnel status through ASA CLI](#)
- [Verifying the tunnel parameters through Router CLI](#)

## [Verify tunnel parameters through CCP](#)

- Monitor the traffic passes through the IPsec tunnel.



- Monitor the status of the phase I ISAKMP



SA.

## Verify tunnel status through ASA CLI

- Verify the status of phase I ISAKMP SA. `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: 209.165.200.12 Type : L2L Role : **responder** Rekey : no State : **MM\_ACTIVE**  
`ciscoasa#` **Note:** Observe the Role to be responder, which states that the initiator of this tunnel is at the other end, for example, the VPN-Router.
- Verify the parameters of phase II IPSEC SA. `ciscoasa#show crypto ipsec sa interface: outside`  
 Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2 local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0) current\_peer: 209.165.200.12 #pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29 #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 29, #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.: 209.165.201.2, remote crypto endpt.: 209.165.200.12 path mtu 1500, IPsec overhead 58, media mtu 1500 current outbound spi: E7B37960 inbound esp sas: spi: 0xABB49C64 (2880740452) transform: esp-des esp-md5-hmac none in use settings = {L2L, Tunnel, } slot: 0, conn\_id: 4096, crypto-map: mymap sa timing: remaining key lifetime (kB/sec): (4274997/3498) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xE7B37960 (3887298912) transform: esp-des esp-md5-hmac none in use settings = {L2L, Tunnel, } slot: 0, conn\_id: 4096, crypto-map: mymap sa timing: remaining key lifetime (kB/sec): (4274997/3498) IV size: 8 bytes replay detection support: Y

## Verify the tunnel parameters through Router CLI

- Verify the status of phase I ISAKMP SA. `VPN-Router#show crypto isakmp sa dst src state conn-id slot status` 209.165.201.2 209.165.200.12 **QM\_IDLE** 1 0 **ACTIVE**
- Verify the parameters of phase II IPSEC SA. `VPN-Router#show crypto ipsec sa interface:`

```
FastEthernet1 Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12 protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0) current_peer 209.165.201.2 port 500
PERMIT, flags={origin_is_acl,} #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39 #pkts
decaps: 39, #pkts decrypt: 39, #pkts verify: 39 #pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress
failed: 0 #send errors 6, #recv errors 0 local crypto endpt.: 209.165.200.12, remote crypto
endpt.: 209.165.201.2 path mtu 1500, ip mtu 1500 current outbound spi:
0xABB49C64(2880740452) inbound esp sas: spi: 0xE7B37960(3887298912) transform: esp-des esp-
md5-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): (4481818/3375) IV size: 8 bytes replay
detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0xABB49C64(2880740452) transform: esp-des esp-md5-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): (4481818/3371) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound
ah sas: outbound pcp sas:
```

## Troubleshoot

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

- Tearing down the existing crypto connections.`ciscoasa#clear crypto ipsec sa ciscoasa#clear crypto isakmp sa VPN-Router#clear crypto isakmp`
- Use **debug** commands in order to troubleshoot the problems with VPN tunnel.**Note:** If you enable debugging, this can disrupt the operation of the router when internetworks experience high load conditions.**Use debug commands with caution.** In general, it is recommended that these commands only be used under the direction of your router technical support representative when troubleshooting specific problems.`ciscoasa#debug crypto engine ciscoasa#debug crypto isakmp ciscoasa#debug crypto IPsec ciscoasa# VPN-Router#debug crypto engine` Crypto Engine debugging is on VPN-Router#`debug crypto isakmp` Crypto ISAKMP debugging is on VPN-Router#`debug crypto ipsec` Crypto IPSEC debugging is on VPN-Router#

Refer to [debug crypto isakmp](#) in [Understanding and Using debug Commands](#) for more information on debug commangs.

## Related Information

- [IPSEC Negotiation/IKE Protocols Support Page](#)
- [Documentation for Cisco ASA Security Appliance OS Software](#)
- [Most Common IPSEC VPN Troubleshooting Solutions](#)
- [Requests for Comments \(RFCs\)](#) 
- [Technical Support & Documentation - Cisco Systems](#)