* [Home](http://www.cisco.com/c/en/us/index.html)
* [Skip to content](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#fw-content)
* [Skip to footer](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#fw-footer)
* [Worldwide [change]](http://www.cisco.com/web/siteassets/locator/index.html)
* [Log In](http://www.cisco.com/c/login/index.html?referer=/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html)
* [Account](http://www.cisco.com/web/siteassets/account/index.html?referer=http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html)
* [Register](https://tools.cisco.com/RPF/register/register.do?referer=http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html)

[My Cisco](http://www.cisco.com/cisco/psn/web/workspace)

[Cisco.com Worldwide Home](http://www.cisco.com/c/en/us/index.html)

* [**Products & Services**](http://www.cisco.com/c/en/us/products/index.html)
* [**Support**](http://www.cisco.com/c/en/us/support/index.html)
* [**How to Buy**](http://www.cisco.com/c/en/us/buy.html)
* [**Training & Events**](http://www.cisco.com/c/en/us/training-events.html)
* [**Partners**](http://www.cisco.com/c/en/us/partners.html)

Top of Form

Bottom of Form

* [Support](http://www.cisco.com/c/en/us/support/index.html)
* ...
* [Configure](http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-configure.html)
* [Configuration Examples and TechNotes](http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-configuration-examples-list.html)

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

Download

Print

**Updated:**Jul 28, 2010

**Document ID:**[112075](javascript:void(0))

**Contents**

[**Introduction**](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#intro)

[**Prerequisites**](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#prereq)

[Requirements](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#req)

[Components Used](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#hw)

[Conventions](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#conv)

[**Background Information**](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#backinfo)

[**Configure**](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#conf)

[Network Diagram](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#diag)

[Configurations](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#configs)

[**Verify**](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#veri)

[Verify tunnel parameters through CCP](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#verifyccp)

[Verify tunnel status through ASA CLI](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#verifyasa)

[Verify the tunnel parameters through Router CLI](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#verifyrouter)

[**Troubleshoot**](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#tshoot)

[**Related Information**](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#related)

**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**®** 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](http://www.cisco.com/en/US/products/ps9422/index.html) (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](http://www.cisco.com/en/US/products/ps9422/products_configuration_example09186a0080b2f103.shtml) for more information on how to configure a router with CCP.

Refer to [Site to Site VPN (L2L) with ASA](http://www.cisco.com/en/US/products/ps6120/prod_configuration_examples_list.html#anchor11) for more inormation and configuration examples on IPsec tunnel establishment that use ASA and Cisco IOS Routers.

Refer to [Site to Site VPN (L2L) with IOS](http://www.cisco.com/en/US/products/ps6120/prod_configuration_examples_list.html#anchor12) 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 Router1812 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](http://www.cisco.com/warp/customer/459/techtip_conventions.html) 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.

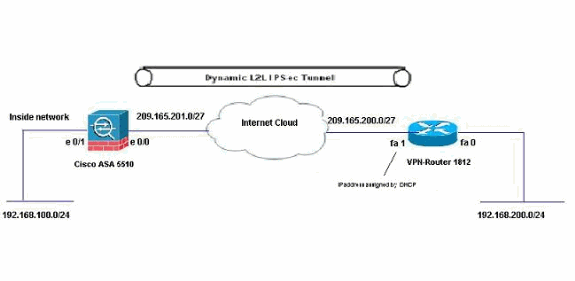
**Configure**

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

**Note:**Use the [Command Lookup Tool](http://tools.cisco.com/Support/CLILookup/cltSearchAction.do) ([registered](http://tools.cisco.com/RPF/register/register.do) customers only) to obtain more information on the commands used in this section.

**Network Diagram**

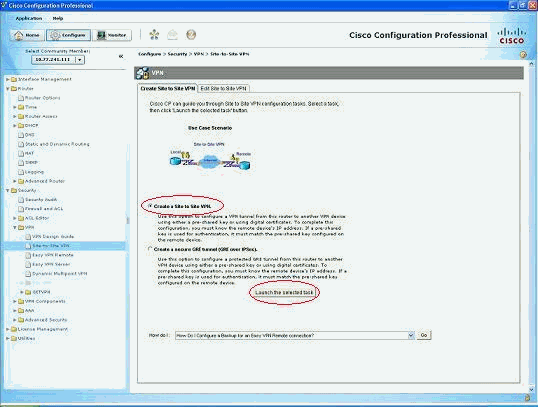
This document uses this network setup:

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-01.gif)

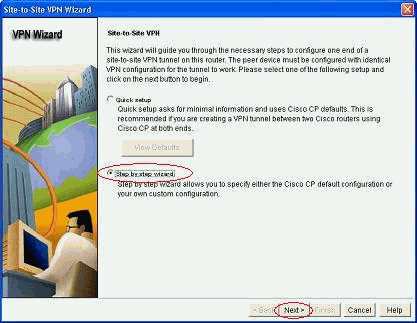
**Configurations**

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

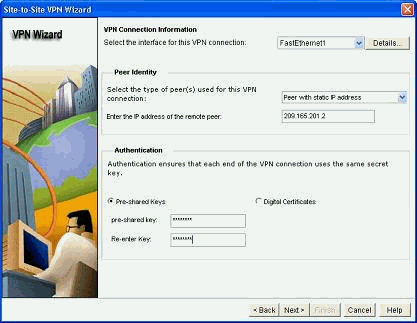
1. Open the CCP application and choose **Configure > Security > VPN > Site to Site VPN**. Click the **Launch the selected tab**.

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-02.gif)

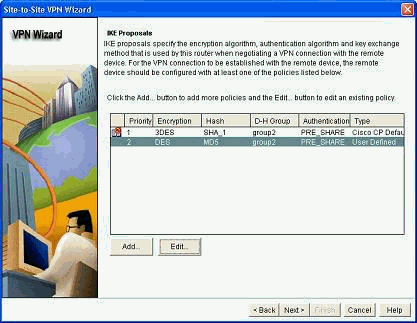
1. Choose **Step-by-step wizard** and then click **Next**.

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-03.gif)

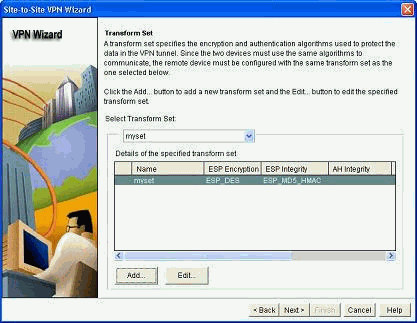
1. Fill in the remote peer IP address along with the authentication details.

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-04.gif)

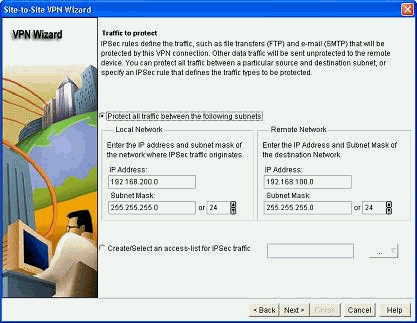
1. Choose the IKE proposals and click **Next**.

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-05.gif)

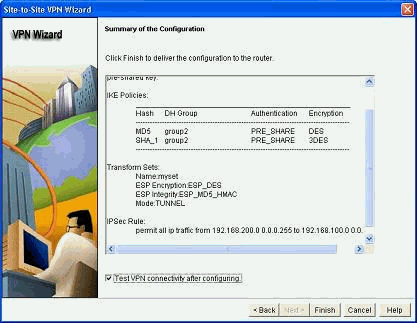
1. Define the transform-set details and click **Next**.

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-06.gif)

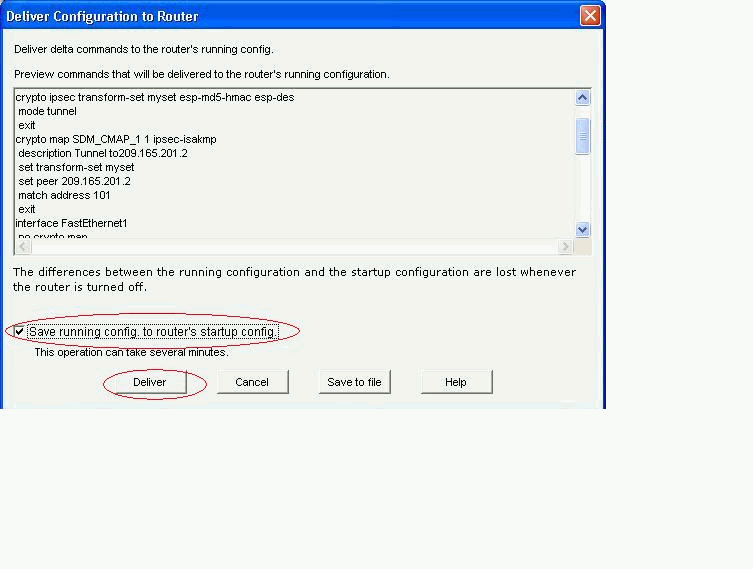
1. Define the traffic that needs to be encrypted and click **Next**.

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-07.gif)

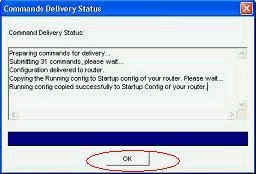
1. Verify the summary of the crypto IPsec configuration and click **Finish**.

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-08.gif)

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

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-09.gif)

1. Click **OK**.

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-10.gif)

CLI Configuration

* [Ciscoasa](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#t1-ciscoasa)
* [VPN-Router](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#t2-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.HJSRDfQO1  !  !  *!--- 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 |

**Verify**

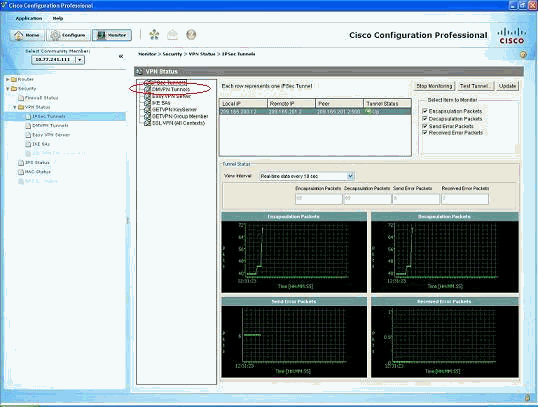
Use this section to confirm that your configuration works properly.

The [Output Interpreter Tool](https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl) ([registered](http://tools.cisco.com/RPF/register/register.do) customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

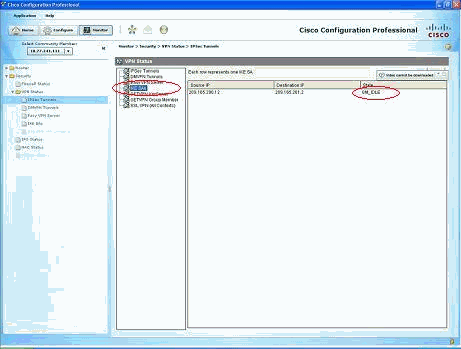
* [Verifying the tunnel parameters through CCP](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#verifyccp)
* [Verifying the tunnel status through ASA CLI](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#verifyasa)
* [Verifying the tunnel parameters through Router CLI](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html#verifyrouter)

**Verify tunnel parameters through CCP**

* Monitor the traffic passes through the IPsec tunnel.

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-11.gif)

* Monitor the status of the phase I ISAKMP SA.

[](http://www.cisco.com/c/dam/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp-12.gif)

**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**](http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a00800949c5.shtml#dbg_ci)in [Understanding and Using debug Commands](http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a00800949c5.shtml) for more information on debug commangs.

**Related Information**

* [**IPSEC Negotiation/IKE Protocols Support Page**](http://www.cisco.com/en/US/tech/tk583/tk372/tsd_technology_support_protocol_home.html?referring_site=bodynav)
* [**Documentation for Cisco ASA Security Appliance OS Software**](http://www.cisco.com/en/US/products/ps6120/prod_configuration_examples_list.html?referring_site=bodynav)
* [**Most Common IPSEC VPN Troubleshooting Solutions**](http://www.cisco.com/en/US/products/ps6120/products_tech_note09186a00807e0aca.shtml?referring_site=bodynav)
* [**Requests for Comments (RFCs)**](http://www.ietf.org/rfc.html?referring_site=bodynav)**[leavingcisco.com](http://www.cisco.com/swa/i/icon_popup_short.gif)**
* [**Technical Support & Documentation - Cisco Systems**](http://www.cisco.com/en/US/support/index.html?referring_site=bodynav)

Contributed by Cisco Engineers

Was this Document Helpful?

Yes No[[http://www.cisco.com/web/fw/i/sm_0000EE_oo1.gif](javascript:%20void(0))Feedback](javascript:%20void(0))

Viewers of This Document Also Viewed

* [ASA-to-ASA Dynamic-to-Static IKEv1/IPsec Configuration Example](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/119007-config-asa9x-ike-ipsec-00.html?referring_site=RE&pos=1&page=http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html)
* [Dynamic Site to Site IKEv2 VPN Tunnel Between Two ASAs Configuration Example](http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118652-configure-asa-00.html?referring_site=RE&pos=2&page=http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html)
* [Dynamic Site to Site IKEv2 VPN Tunnel Between an ASA and an IOS Router Configuration Example](http://www.cisco.com/c/en/us/support/docs/ip/internet-key-exchange-ike/118743-configure-asa-00.html?referring_site=RE&pos=3&page=http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112075-dynamic-ipsec-asa-router-ccp.html)
* + Show 3 More

Let Us Help

* [Open a Support Case](https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case)login required
* (Requires a [Cisco Service Contract](http://www.cisco.com/c/en/us/services/order-services.html))

**Campus Wired LAN Design Guide**

Optimize your network with a validated design.

[**Get Design Guide**](https://grs.cisco.com/grsx/cust/grsCustomerSurvey.html?SurveyCode=8537&ad_id=US-BN-SWT-M-CAMPUSWIREDLANDG-GEN&KeyCode=000385822)

Related Support Community Discussions

* [Cisco Prime Infrastructure FAQ](https://supportforums.cisco.com/document/12172606/cisco-prime-infrastructure-faq)

Last Reply 7 months ago

in [Network Management](https://supportforums.cisco.com/community/5931/network-management)

* [Cisco ASA 5500-X Series Next-Generation Firewalls](https://supportforums.cisco.com/discussion/12053241/cisco-asa-5500-x-series-next-generation-firewalls)

Last Reply 2 years ago

in [Firewalling](https://supportforums.cisco.com/community/5966/firewalling)

* [Cisco ASA 5500-Xシリーズ Firewall 設定ガイド](https://supportforums.cisco.com/ja/document/12712756)

Last Reply 6 months ago

in [システムズエンジニアリング](https://supportforums.cisco.com/ja/community/12255886/systemsengineering)

[Cisco Support Community](https://supportforums.cisco.com/index.jspa)

This Document Applies to These Products

* [1800 Series Integrated Services Routers](http://www.cisco.com/c/en/us/support/routers/1800-series-integrated-services-routers/tsd-products-support-series-home.html)
* [1800 Series Integrated Services Routers](http://www.cisco.com/c/en/us/support/routers/1800-series-integrated-services-routers-isr/tsd-products-support-series-home.html)
* [2800 Series Integrated Services Routers](http://www.cisco.com/c/en/us/support/routers/2800-series-integrated-services-routers-isr/tsd-products-support-series-home.html)
* [3800 Series Integrated Services Routers](http://www.cisco.com/c/en/us/support/routers/3800-series-integrated-services-routers-isr/tsd-products-support-series-home.html)
* [ASA 5500-X Series Firewalls](http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html)

+ Show All 6 Products

Share

[Information For](http://www.cisco.com/c/en/us/solutions/index.html)

* [Small Business](http://www.cisco.com/c/en/us/solutions/small-business.html)
* [Midsize Business](http://www.cisco.com/c/en/us/solutions/midsize/overview.html)
* [Service Provider](http://www.cisco.com/c/en/us/solutions/service-provider/index.html)

[Industries](http://www.cisco.com/c/en/us/solutions/industries.html)

[Marketplace](https://marketplace.cisco.com/)

[Contacts](http://www.cisco.com/web/siteassets/contacts/index.html)

* [Contact Cisco](http://www.cisco.com/web/siteassets/contacts/index.html)
* [Meet our Partners](http://www.cisco.com/c/en/us/solutions/partner-ecosystem.html)
* [Find a Reseller](https://tools.cisco.com/WWChannels/LOCATR/openBasicSearch.do)

[News & Alerts](https://newsroom.cisco.com/)

* [Newsroom](https://newsroom.cisco.com/)
* [Blogs](http://blogs.cisco.com/)
* [Field Notices](http://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html)
* [Security Advisories](https://tools.cisco.com/security/center/publicationListing.x)

[Technology Trends](http://www.cisco.com/c/en/us/solutions/technology-trends.html)

* [Cloud](http://www.cisco.com/c/en/us/solutions/cloud/overview.html)
* [Internet of Things (IoT)](http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html)
* [Software Defined Networking (SDN)](http://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html)

[Support](http://www.cisco.com/c/en/us/support/index.html)

* [Downloads](https://software.cisco.com/download/navigator.html?i=!ch)
* [Documentation](http://www.cisco.com/cisco/web/psa/default.html)

[Communities](https://communities.cisco.com/welcome)

* [DevNet](https://developer.cisco.com/)
* [Learning Network](https://learningnetwork.cisco.com/)
* [Support Community](https://supportforums.cisco.com/index.jspa)

[Video Portal](http://video.cisco.com/)

[About Cisco](http://www.cisco.com/c/en/us/about.html)

* [Investor Relations](http://investor.cisco.com/)
* [Corporate Social Responsibility](http://csr.cisco.com/)
* [Environmental Sustainability](http://csr.cisco.com/pages/environment)
* [Trust and Transparency Center](http://www.cisco.com/c/en/us/about/trust-transparency-center/overview.html)
* [There's Never Been A Better Time](http://www.cisco.com/c/m/en_us/never-better/index.html?CAMPAIGN=NBT-00+NBABT&COUNTRY_SITE=us&POSITION=link&REFERRING_SITE=cisco.com&CREATIVE=fat+footer+nbabt+text)
* [Our People](http://weare.cisco.com/)

[Careers](http://www.cisco.com/c/en/us/about/careers.html)

* [Search Jobs](https://jobs.cisco.com/?utm_source=careersite&utm_campaign=CDC_MainFooter)
* [Life at Cisco](http://www.cisco.com/c/en/us/about/careers/life-at-cisco.html)

Programs

* [Cisco Designated VIP Program](http://www.cisco.com/web/communities/vip/index.html)
* [Cisco Powered](http://www.cisco.com/c/en/us/solutions/cisco-powered/overview.html)
* [Financing Options](http://www.cisco.com/web/ciscocapital/americas/us/index.html)
* [Contacts](http://www.cisco.com/cisco/web/siteassets/contacts/index.html)
* Leave Feedback[Feedback](https://secure.opinionlab.com/ccc01/o.asp?id=jBjOhqOJ)
* [Help](http://www.cisco.com/web/help/index.html)
* [Site Map](http://www.cisco.com/web/siteassets/sitemap/index.html)
* [Terms & Conditions](http://www.cisco.com/web/siteassets/legal/terms_condition.html)
* [Privacy Statement](http://www.cisco.com/web/siteassets/legal/privacy_full.html)
* [Cookie Policy](http://www.cisco.com/web/siteassets/legal/privacy_full.html#cookies)
* [Trademarks](http://www.cisco.com/web/siteassets/legal/trademark.html)