

IPsec Between Two IOS Routers with Overlapping Private Networks Configuration Example

Document ID: 107992

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Configure

- Network Diagram

- Configurations

Verify

Troubleshoot

Related Information

Introduction

This document describes how to configure the Cisco IOS router in a site-to-site IPsec VPN with overlapping private network addresses behind VPN gateways.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco IOS 3640 routers that run software version 12.4.

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.

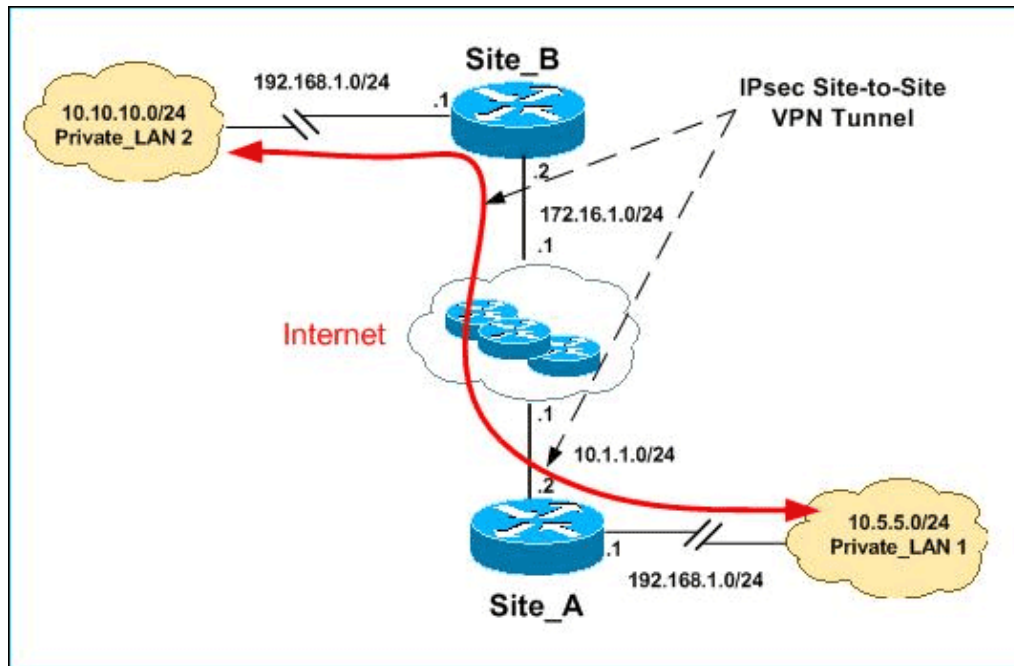
Configure

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:



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.

Both Private_LAN1 and Private_LAN2 have an IP subnet of 192.168.1.0/24. This simulates the overlapping address space behind each side of the IPsec tunnel.

In this example, the Site_A router performs a bi-directional translation so that the two private LANs can communicate over the IPsec tunnel. The translation means that Private_LAN1 "sees" Private_LAN2 as 10.10.10.0/24 through the IPsec tunnel, and Private_LAN2 "sees" Private_LAN1 as 10.5.5.0/24 through the IPsec tunnel.

Configurations

This document uses these configurations:

- Site_A Router SDM Configuration
- Site_A Router CLI Configuration
- Site_B Router Configuration

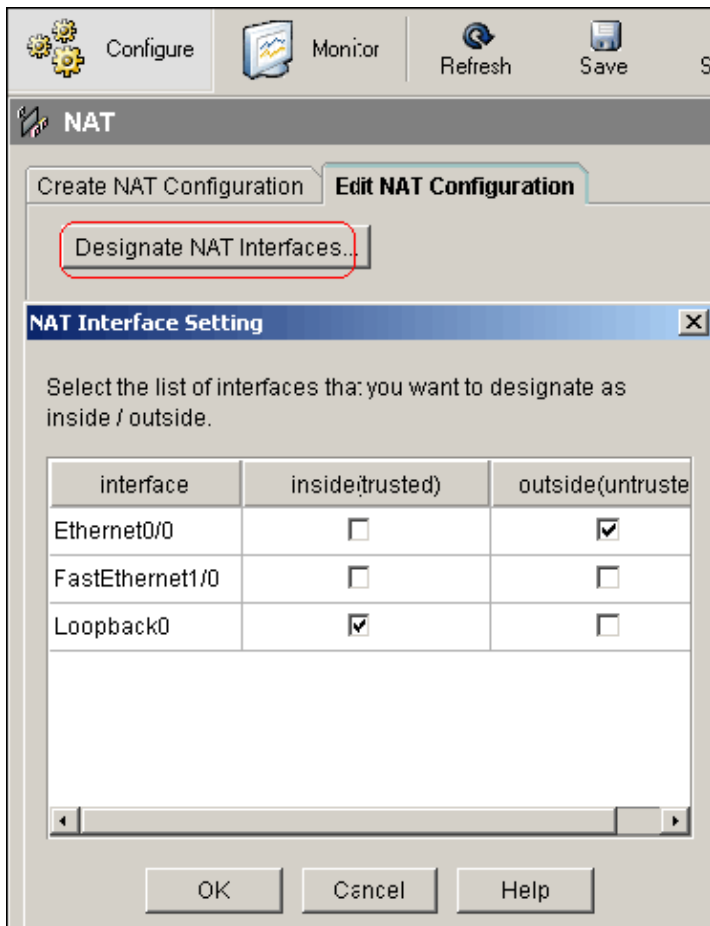
Site_A Router SDM Configuration

Note: This document assumes that the router is configured with basic settings like interface configuration, etc. Refer to Basic Router Configuration using SDM for more information.

NAT Configuration

Complete these steps in order to use NAT to configure SDM on the Site_A router:

1. Choose **Configure > NAT > Edit NAT Configuration**, and click **Designate NAT Interfaces** in order to define trusted and untrusted interfaces as shown.



2. Click **OK**.
3. Click **Add** in order to configure the NAT translation from inside to outside direction as shown.

Add Address Translation Rule

Static Dynamic

Direction: **From inside to outside**

Translate from interface

Inside Interface(s): Loopback0
 IP address: 192.168.1.0
 Network Mask(optional): 255.255.255.0 or 24

Translate to interface

Outside Interface(s): Ethernet0/0
 Type: IP address
 Interface: Ethernet0/0
 IP address: 10.5.5.0

Redirect Port
 TCP UDP
 Original Port: Translated Port:

OK Cancel Help

4. Click **OK**.

Network Address Translation Rules

Inside Interface(s): Loopback0

Outside Interface(s): Ethernet0/0

Original address	Translated address	Rule Type	Add...
192.168.1.0-192.168.1.255	10.5.5.0-10.5.5.255	Static	

5. Once again, click **Add** in order to configure the NAT translation from outside to inside direction as shown.

Add Address Translation Rule

Static Dynamic

Direction: From outside to inside

Translate from interface

Outside Interface(s): Ethernet0/0

IP address: 10.10.10.0

Network Mask(optional): 255.255.255.0 or 24

Translate to interface

Inside Interface(s): Loopback0

IP address: 192.168.1.0

Redirect Port

TCP UDP

Original Port: Translated Port:

OK Cancel Help

6. Click **OK**.

Network Address Translation Rules

Inside Interface(s): Loopback0

Outside Interface(s): Ethernet0/0

	Original address	Translated address	Rule Type
	192.168.1.0-192.168.1.255	10.5.5.0-10.5.5.255	Static
	192.168.1.0-192.168.1.255	10.10.10.0-10.10.10.255	Static

Note: Here is the equivalent CLI configuration:

Equivalent CLI Configuration
<pre> interface Loopback0 ip nat inside interface Ethernet0/0 ip nat inside ip nat inside source static network 192.168.1.0 10.5.5.0 /24 ip nat outside source static network 192.168.1.0 10.10.10.0 /24 </pre>

VPN Configuration

Complete these steps in order to use VPN to configure SDM on the Site_A router:

1. Choose **Configure > VPN > VPN Components >IKE > IKE Policies > Add** in order to define the IKE policies as shown in this image.

2. Click **OK**.

IKE Policies						
Priority	Encryption	Hash	D-H Group	Authentication	Type	
10	DES	MD5	group1	PRE SHARE	User Defined	

Note: Here is the equivalent CLI configuration:

```

Equivalent CLI Configuration

crypto isakmp policy 10
encr des
hash md5
authentication pre-share
group1
  
```

3. Choose **Configure > VPN > VPN Components >IKE > Pre-shared Keys > Add** in order to set the pre-shared key value with peer IP address.

4. Click **OK**.

Pre-shared Keys		
Peer IP/Name	Subnet Mask	pre-shared key
172.16.1.2	255.255.255.0	*****

Note: Here is the equivalent CLI configuration:

```
crypto isakmp key 6 L2L12345 address 172.16.1.2 255.255.255.0
```

5. Choose **Configure > VPN > VPN Components > IPsec > Transform Sets > Add** in order to create a transform set *myset* as shown in this image.

Add Transform Set

Name:

Data integrity with encryption (ESP)

Integrity Algorithm:

Encryption Algorithm:

Show Advanced

OK Cancel Help

6. Click **OK**.

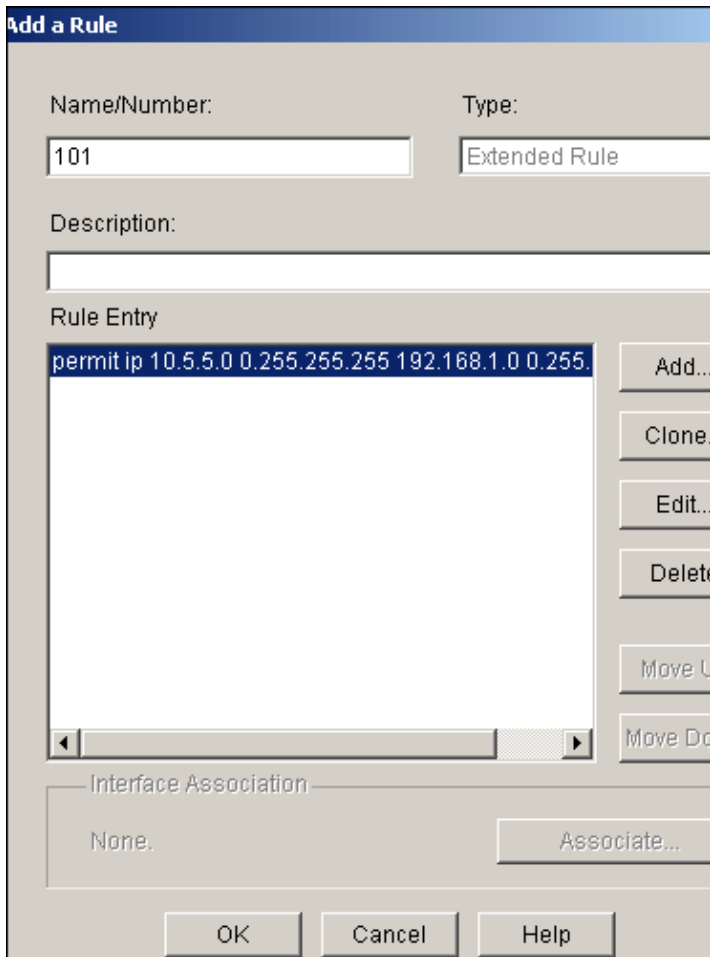
Name	ESP Encryption	ESP Integrity	AH Integrity
myset	ESP_DES	ESP_MD5_HMAC	

Add...

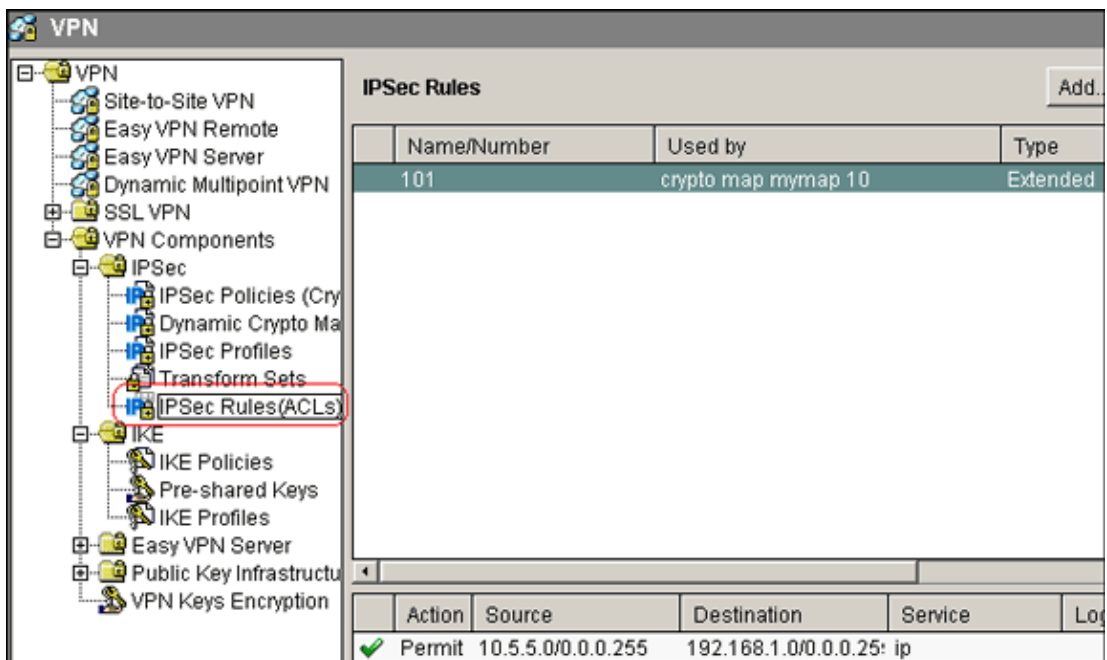
Note: Here is the equivalent CLI configuration:

```
crypto ipsec transform-set myset esp-des esp-md5-hmac
```

7. Choose **Configure > VPN > VPN Components > IPsec > IPsec Rules(ACLs) > Add** in order to create a crypto Access Control List(ACL) *101*.



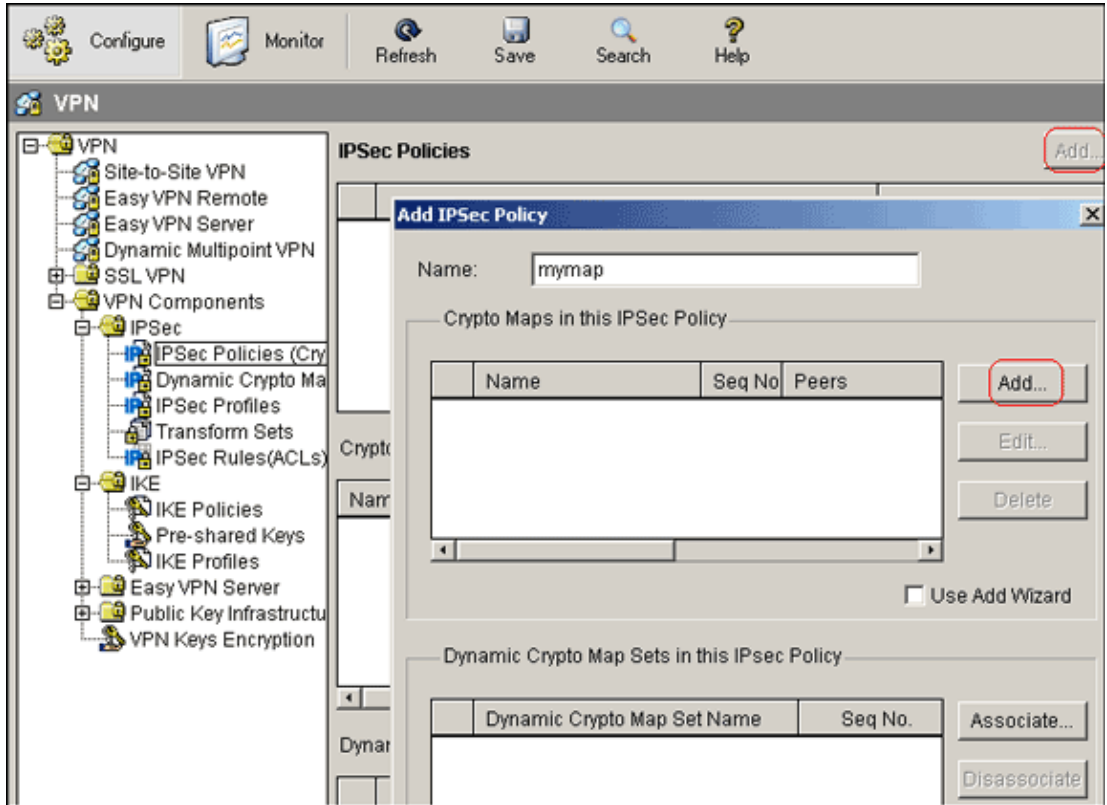
8. Click **OK**.



Note: Here is the equivalent CLI configuration:

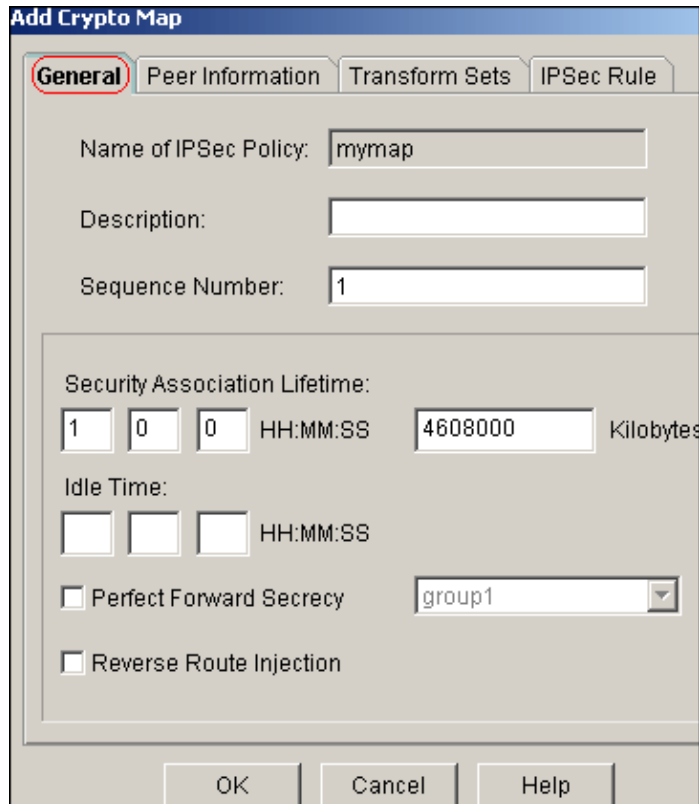
Equivalent CLI Configuration
access-list 101 permit ip 10.5.5.0 0.0.0.255 192.168.1.0 0.0.0.255

9. Choose **Configure > VPN > VPN Components > IPSec > IPSec Policies > Add** in order to create crypto map *mymap* as shown in this image.

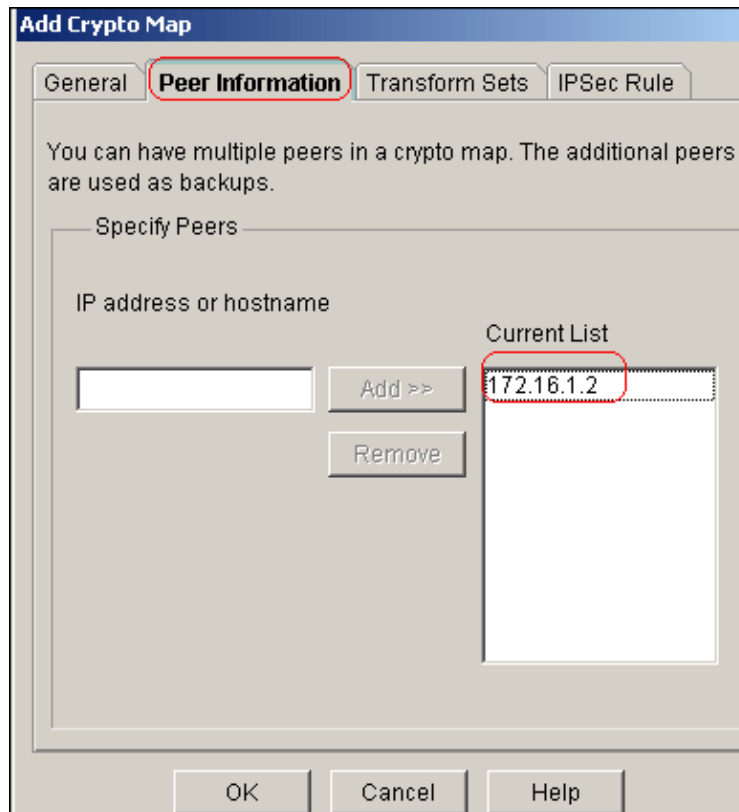


10. Click **Add**.

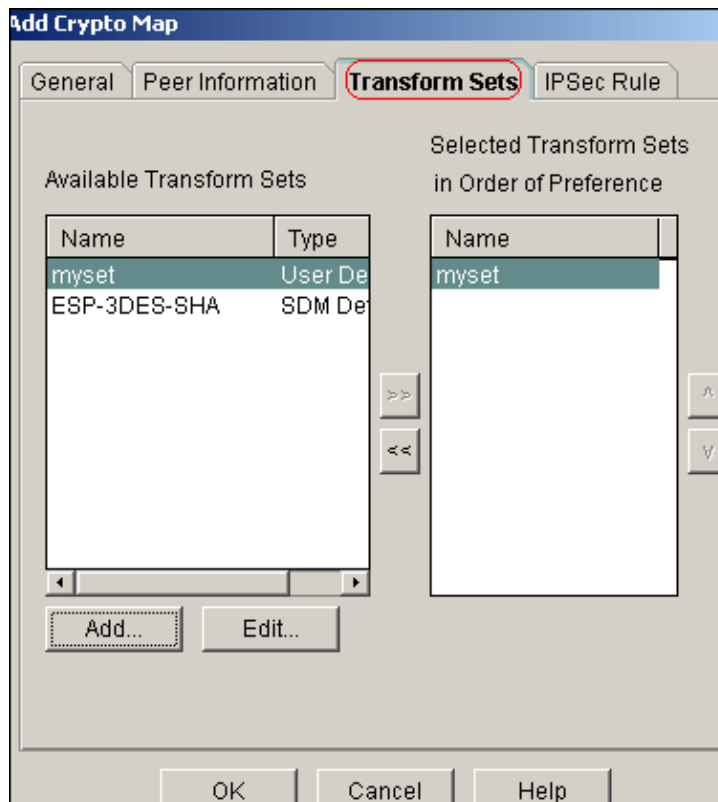
- a. Click the **General** tab and retain the default settings.



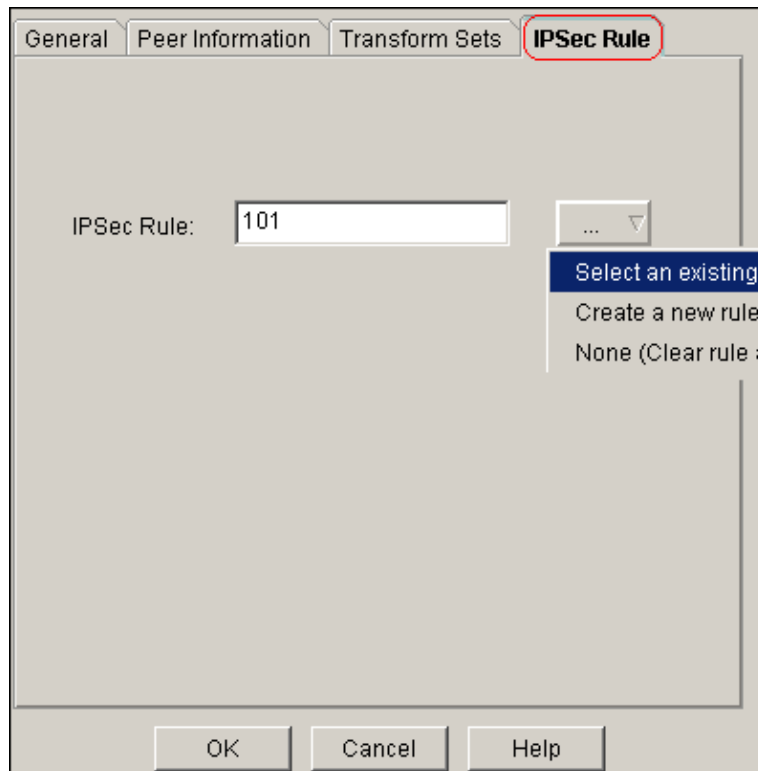
- b. Click the **Peer Information** tab in order to add the peer IP address 172.16.1.2.



c. Click the **Transform Sets** tab in order to select the desired transform set *myset*.



d. Click the **IPSec Rule** tab in order to select the existing crypto ACL 101.

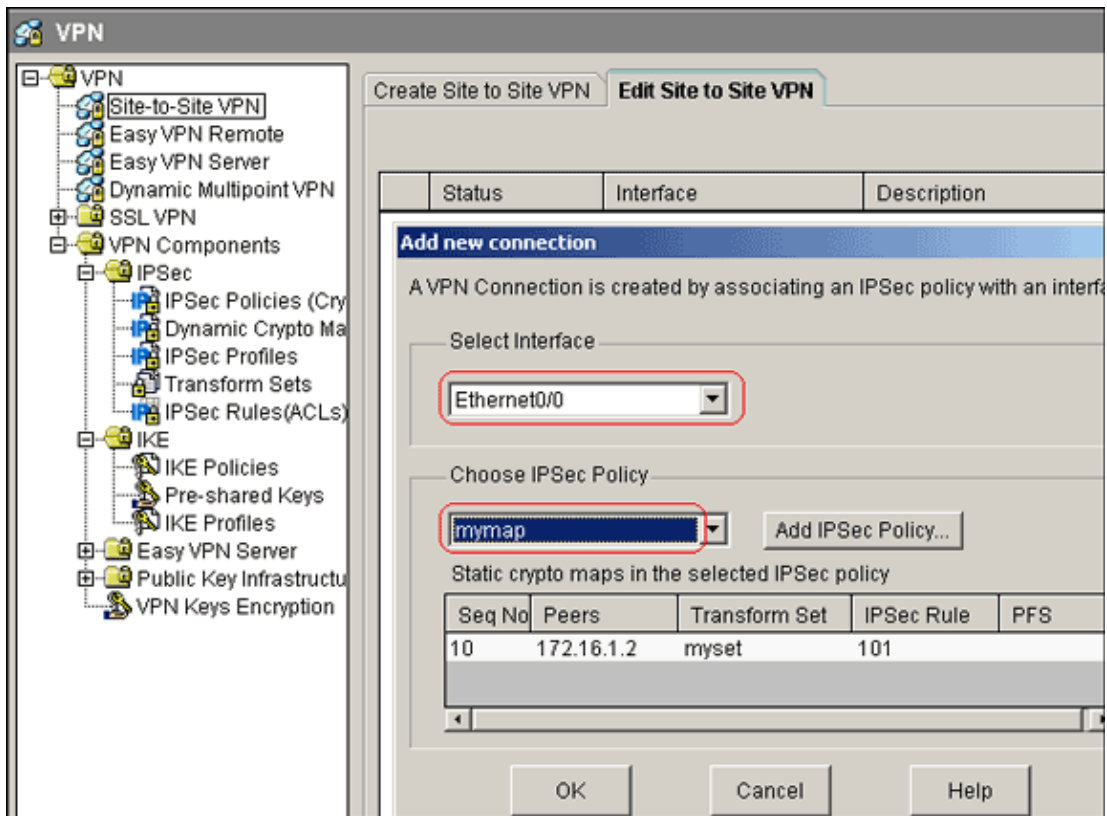


e. Click **OK**.

Note: Here is the equivalent CLI configuration:

Equivalent CLI Configuration
<pre>crypto map mymap 10 ipsec-isakmp set peer 172.16.1.2 set transform-set myset match address 101</pre>

11. Choose **Configure > VPN > Site-to-Site VPN > Edit Site-to-Site VPN > Add** in order to apply crypto map *mymap* to the interface Ethernet0/0.



12. Click **OK**.

Note: Here is the equivalent CLI configuration:

Equivalent CLI Configuration
<pre>interface Ethernet0/0 crypto map mymap</pre>

Site_A Router CLI Configuration

Site_A Router
<pre>Site_A#show running-config *Sep 25 21:15:58.954: %SYS-5-CONFIG_I: Configured from console by console Building configuration... Current configuration : 1545 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname Site_A ! boot-start-marker boot-end-marker ! ! no aaa new-model ! resource policy ! ! !</pre>

```
ip cef
!
!
crypto isakmp policy 10
  hash md5
  authentication pre-share

!--- Defines ISAKMP policy.

crypto isakmp key 6 L2L12345 address 172.16.1.2 255.255.255.0

!--- Defines pre-shared secret used for IKE authentication
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac

!--- Defines IPSec encryption and authentication algorithms.
!
crypto map mymap 10 ipsec-isakmp
  set peer 172.16.1.2
  set transform-set myset
  match address 101

!--- Defines crypto map.
!
!
!
!
interface Loopback0
  ip address 192.168.1.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly
!
interface Ethernet0/0
  ip address 10.1.1.2 255.255.255.0
  ip nat outside
  ip virtual-reassembly
  half-duplex
  crypto map mymap

!--- Apply crypto map on the outside interface.
!
!

!--- Output Suppressed

!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
ip nat inside source static network 192.168.1.0 10.5.5.0 /24

!--- Static translation defined to translate Private_LAN1
!--- from 192.168.1.0/24 to 10.5.5.0/24.
!--- Note that this translation is used for both
!--- VPN and Internet traffic from Private_LAN1.
!--- A routable global IP address range, or an extra NAT
```

```

!--- at the ISP router (in front of Site_A router), is
!--- required if Private_LAN1 also needs internal access.

ip nat outside source static network 192.168.1.0 10.10.10.0 /24

!--- Static translation defined to translate Private_LAN2
!--- from 192.168.1.0/24 to 10.10.10.0/24.

!
access-list 101 permit ip 10.5.5.0 0.0.0.255 192.168.1.0 0.0.0.255

!--- Defines IPSec interesting traffic.
!--- Note that the host behind Site_A router communicates
!--- to Private_LAN2 using 10.10.10.0/24.
!--- When the packets arrive at the Site_A router, they are first
!--- translated to 192.168.1.0/24 and then encrypted by IPSec.

!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
Site_A#

```

Site_B Router CLI Configuration

Site_B Router
<pre> Site_B#show running-config Building configuration... Current configuration : 939 bytes ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname Site_B ! ! ip subnet-zero ! ! crypto isakmp policy 10 hash md5 authentication pre-share crypto isakmp key L2L12345 address 10.1.1.2 255.255.255.0 ! ! crypto ipsec transform-set myset esp-des esp-md5-hmac ! crypto map mymap 10 ipsec-isakmp set peer 10.1.1.2 set transform-set myset match address 101 </pre>

```

!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1
 ip address 172.16.1.2 255.255.255.0
 crypto map mymap
!

!--- Output Suppressed

!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
ip http server
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 10.5.5.0 0.0.0.255
!
line con 0
line aux 0
line vty 0 4
!
end

Site_B#

```

Verify

This section provides information you can use to confirm your configuration is working properly.

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

- **show crypto isakmp sa** Displays all current Internet Key Exchange (IKE) security associations (SAs) at a peer.

```

Site_A#show crypto isakmp sa
dst          src          state          conn-id slot status
172.16.1.2   10.1.1.2     QM_IDLE        1          0 ACTIVE

```

- **show crypto isakmp sa detail** Displays the details of all current IKE SAs at a peer.

```

Site_A#show cryto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local          Remote          I-VRF          Status Encr Hash Auth DH Lifetime
Cap.
1     10.1.1.2        172.16.1.2     ACTIVE des  md5  psk  1  23:59:42

Connection-id:Engine-id = 1:1(software)

```

- **show crypto ipsec sa** Displays the settings used by current SAs.

```

Site_A#show crypto ipsec sa

interface: Ethernet0/0
Crypto map tag: mymap, local addr 10.1.1.2

```

```

protected vrf: (none)
local ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 172.16.1.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
  #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 3, #recv errors 0

local crypto endpt.: 10.1.1.2, remote crypto endpt.: 172.16.1.2
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x1A9CDC0A(446487562)

inbound esp sas:
  spi: 0x99C7BA58(2580003416)
  transform: esp-des esp-md5-hmac ,
  in use settings = {Tunnel, }
  conn id: 2002, flow_id: SW:2, crypto map: mymap
  sa timing: remaining key lifetime (k/sec): (4478520/3336)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x1A9CDC0A(446487562)
  transform: esp-des esp-md5-hmac ,
  in use settings = {Tunnel, }
  conn id: 2001, flow_id: SW:1, crypto map: mymap
  sa timing: remaining key lifetime (k/sec): (4478520/3335)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

Site_A#

- **show ip nat translations** Displays translation slot information.

```

Site_A#show ip nat translations
Pro Inside global      Inside local          Outside local        Outside global
--- ---                ---                  10.10.10.1          192.168.1.1
--- ---                ---                  10.10.10.0          192.168.1.0
--- 10.5.5.1           192.168.1.1          ---                  ---
--- 10.5.5.0           192.168.1.0          ---                  ---

```

- **show ip nat statistics** Displays static information about the translation.

```

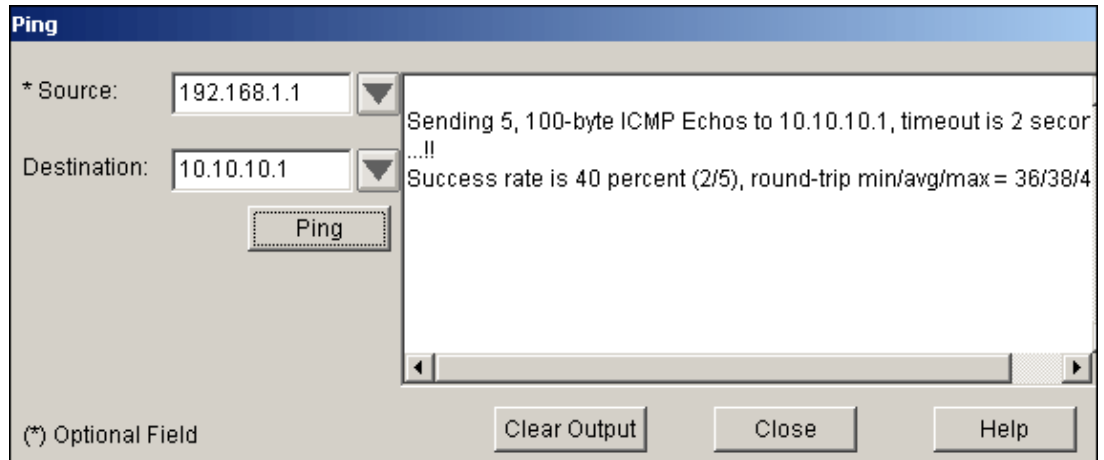
Site_A#show ip nat statistics
Total active translations: 4 (2 static, 2 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Loopback0
Hits: 42 Misses: 2
CEF Translated packets: 13, CEF Punted packets: 0
Expired translations: 7
Dynamic mappings:

```

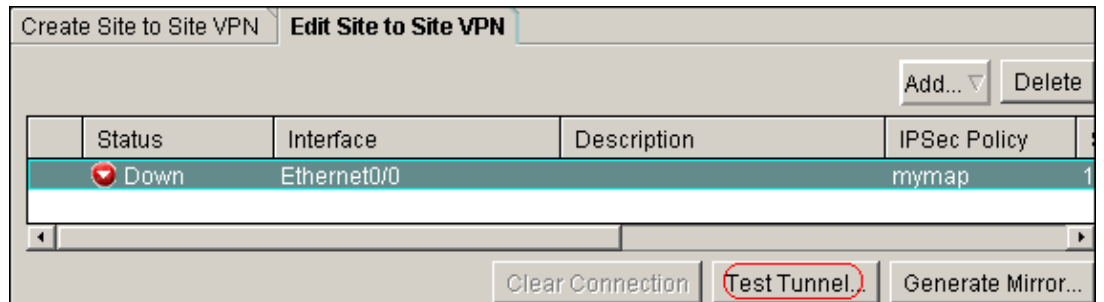
Queued Packets: 0
Site_A#

- Complete these steps in order to verify the connection:

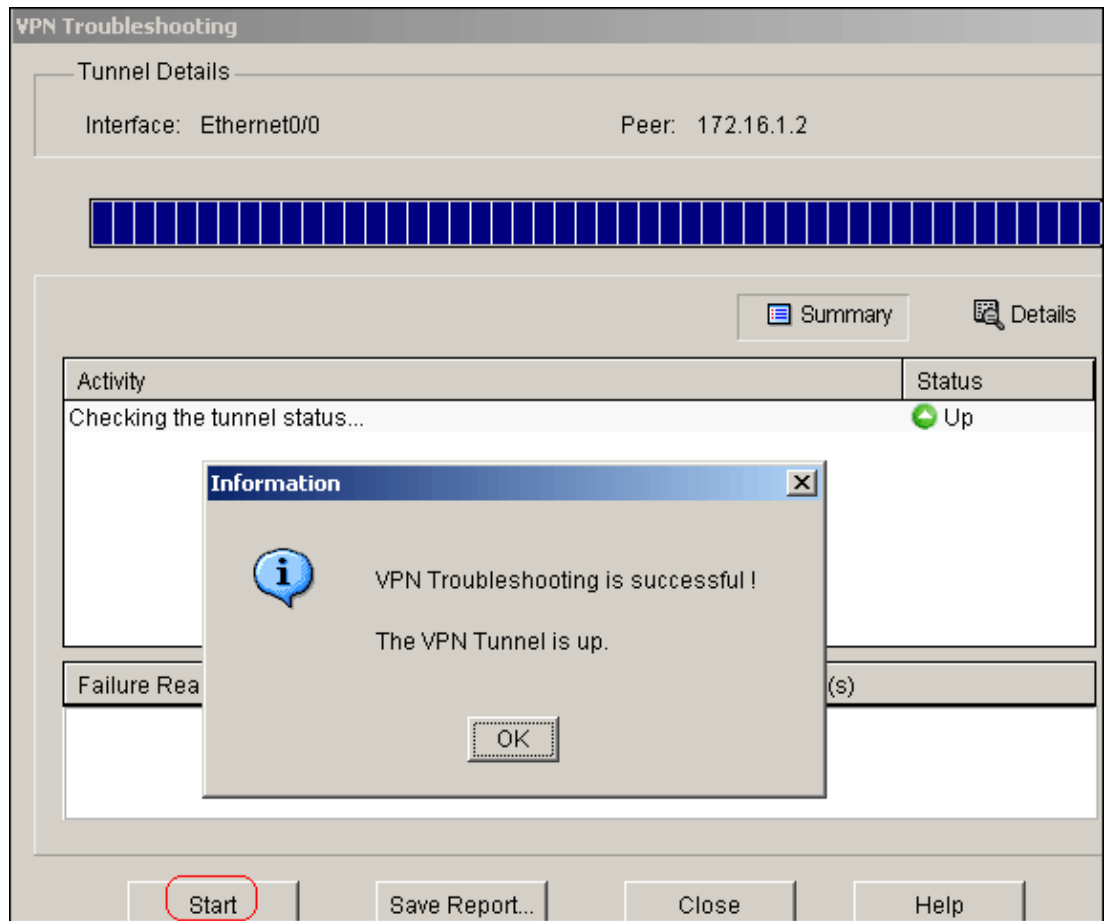
1. In SDM, choose **Tools > Ping** in order to establish the IPsec VPN tunnel with source IP as 192.168.1.1 and destination IP as 10.10.10.1.



2. Click **Test Tunnel** in order to check the IPsec VPN tunnel is established as shown in this image.



3. Click **Start**.



Troubleshoot

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

```

Site_A#debug ip packet
IP packet debugging is on
Site_A#ping
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/52 ms
Site_A#
*Sep 30 18:08:10.601: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.601: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.641: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB

```

*Sep 30 18:08:10.641: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.645: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.645: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.685: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.685: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.685: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.689: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.729: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.729: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.729: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.729: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.769: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.769: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.773: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.773: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.813: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.813: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4

Related Information

- [Most Common L2L and Remote Access IPSec VPN Troubleshooting Solutions](#)
- [IPSec between ASA/PIX and Cisco VPN 3000 Concentrator with Overlapping Private Networks Configuration Example](#)
- [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: Sep 24, 2008

Document ID: 107992
