

Configure ASA-to-ASA Dynamic-to-Static IKEv1/IPsec

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[ASDM Configuration](#)

[Central-ASA \(Static Peer\)](#)

[Remote-ASA \(Dynamic Peer\)](#)

[CLI Configuration](#)

[Central ASA \(Static Peer\) Configuration](#)

[Remote-ASA \(Dynamic Peer\)](#)

[Verify](#)

[Central ASA](#)

[Remote-ASA](#)

[Troubleshoot](#)

[Remote-ASA \(Initiator\)](#)

[Central-ASA \(Responder\)](#)

[Related Information](#)

Introduction

This document describes how to enable the ASA to accept dynamic IPsec site-to-site VPN connections from any dynamic peer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of this topic:

- Adaptive Security Appliance (ASA)

Components Used

The information in this document is based on Cisco ASA (5510 and 5520) Firewall Software Release 9.x and later.

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, ensure that you understand the potential impact of any command.

Background Information

This document describes how to enable the Adaptive Security Appliance (ASA) to accept dynamic IPsec site-to-site VPN connections from any dynamic peer (ASA in this case). As the Network Diagram in this document shows, the IPsec tunnel is established when the tunnel is initiated from the Remote-ASA end only. The Central-ASA cannot initiate a VPN tunnel because of the dynamic IPsec configuration. The IP address of Remote-ASA is unknown.

Configure Central-ASA in order to dynamically accept connections from a wild-card IP address (0.0.0.0/0) and a wild-card pre-shared key. Remote-ASA is then configured to encrypt traffic from local to Central-ASA subnets as specified by the crypto access-list. Both sides perform Network Address Translation (NAT) exemption in order to bypass NAT for IPsec traffic.

Configure

 **Note:** Use the [Command Lookup Tool](#) in order to obtain more information on the commands used in this section. Only registered Cisco users have access to internal Cisco tools and information.

Network Diagram

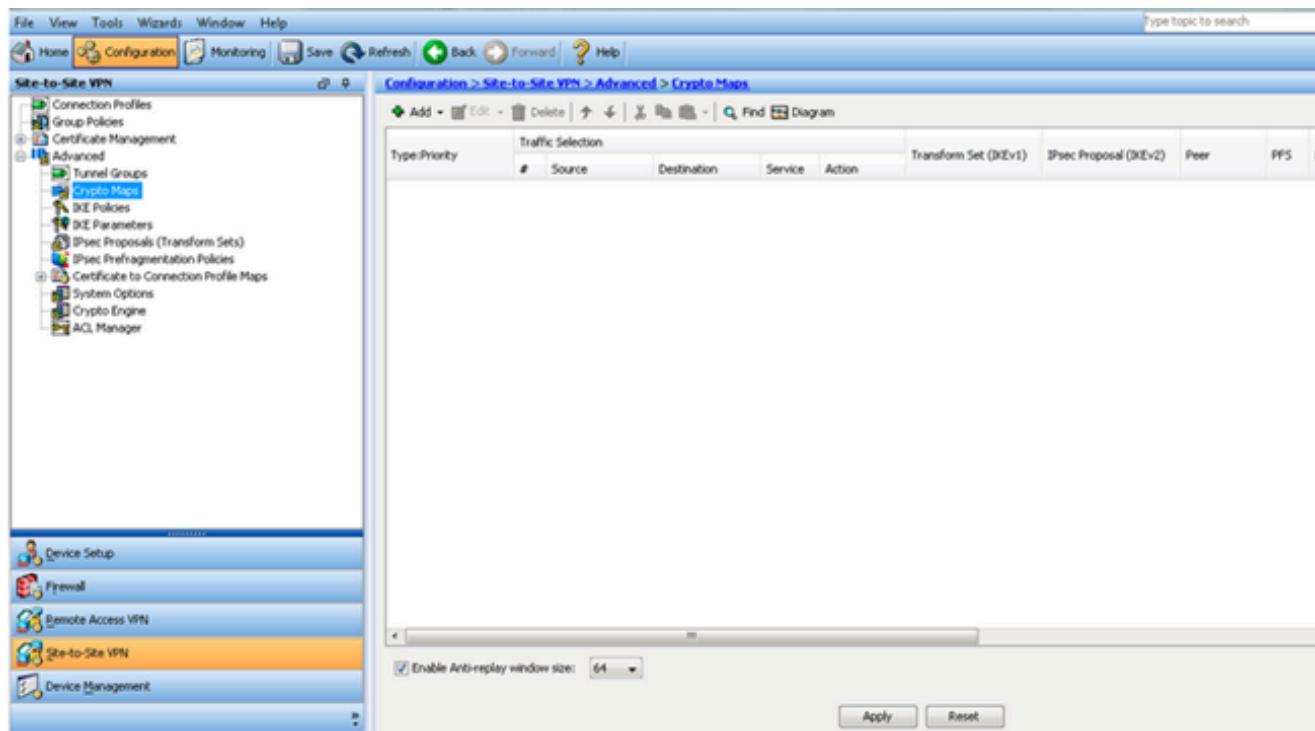


ASDM Configuration

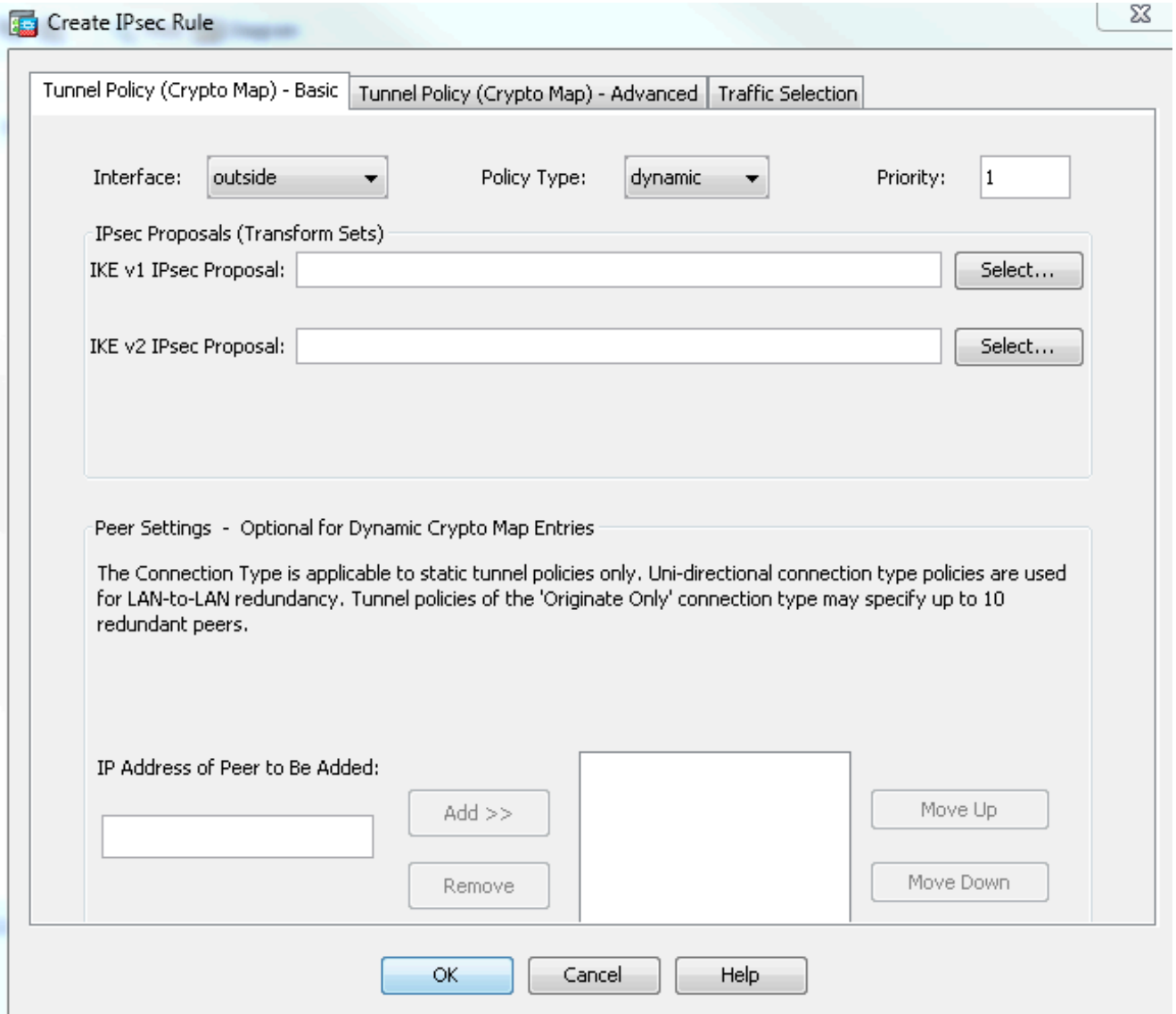
Central-ASA (Static Peer)

On an ASA with a Static IP address, set up the VPN in such a way that it accepts dynamic connections from an unknown peer while it still authenticates the peer using an IKEv1 Pre-shared Key:

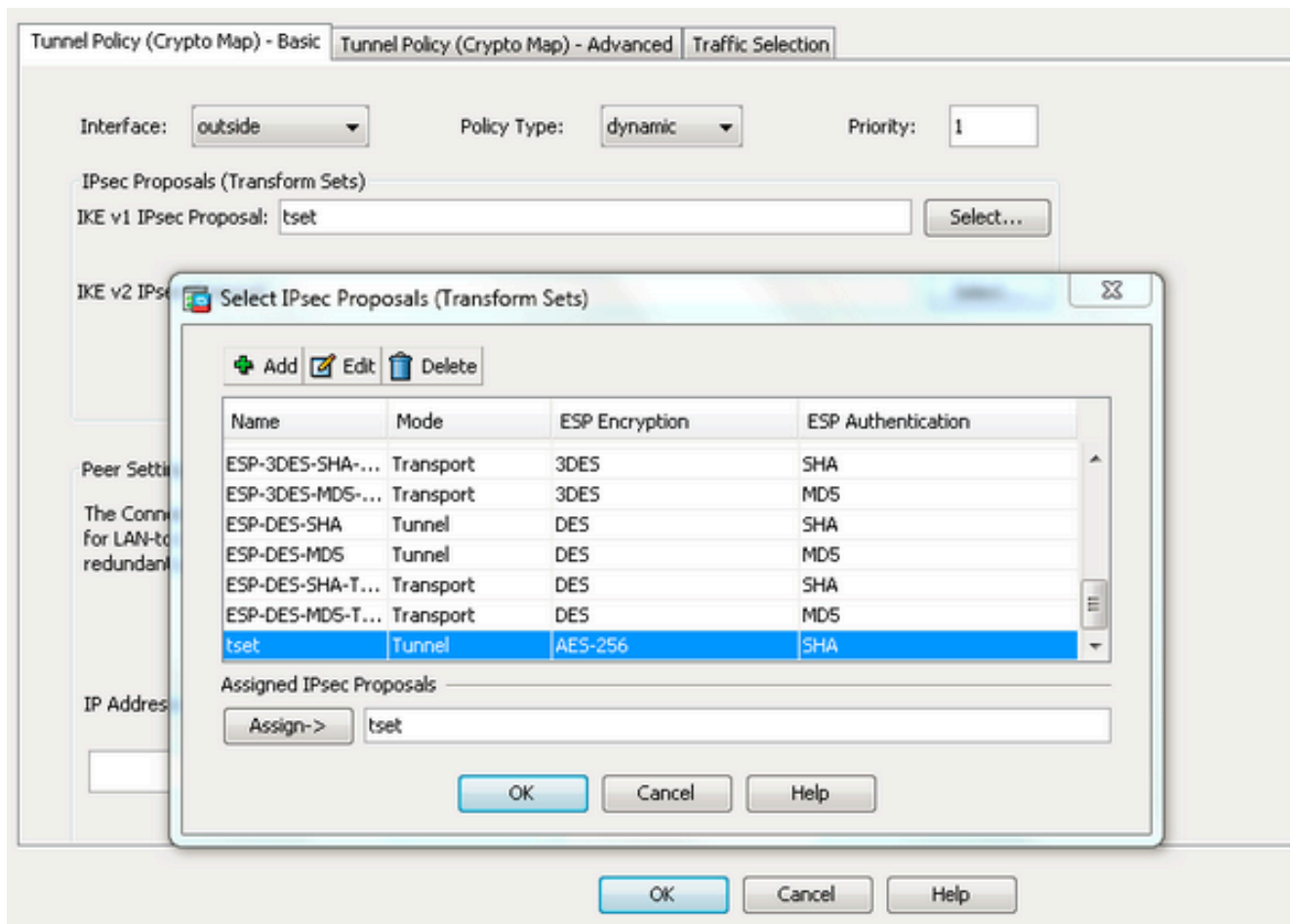
1. Choose **Configuration > Site-to-Site VPN > Advanced > Crypto Maps**. The window displays the list of crypto map entries which are already in place (if there are any). Since ASA does not know what the Peer IP address is, in order for ASA to accept the connection configure **Dynamic-map** with matching transform-set (IPsec Proposal). Click **Add**.



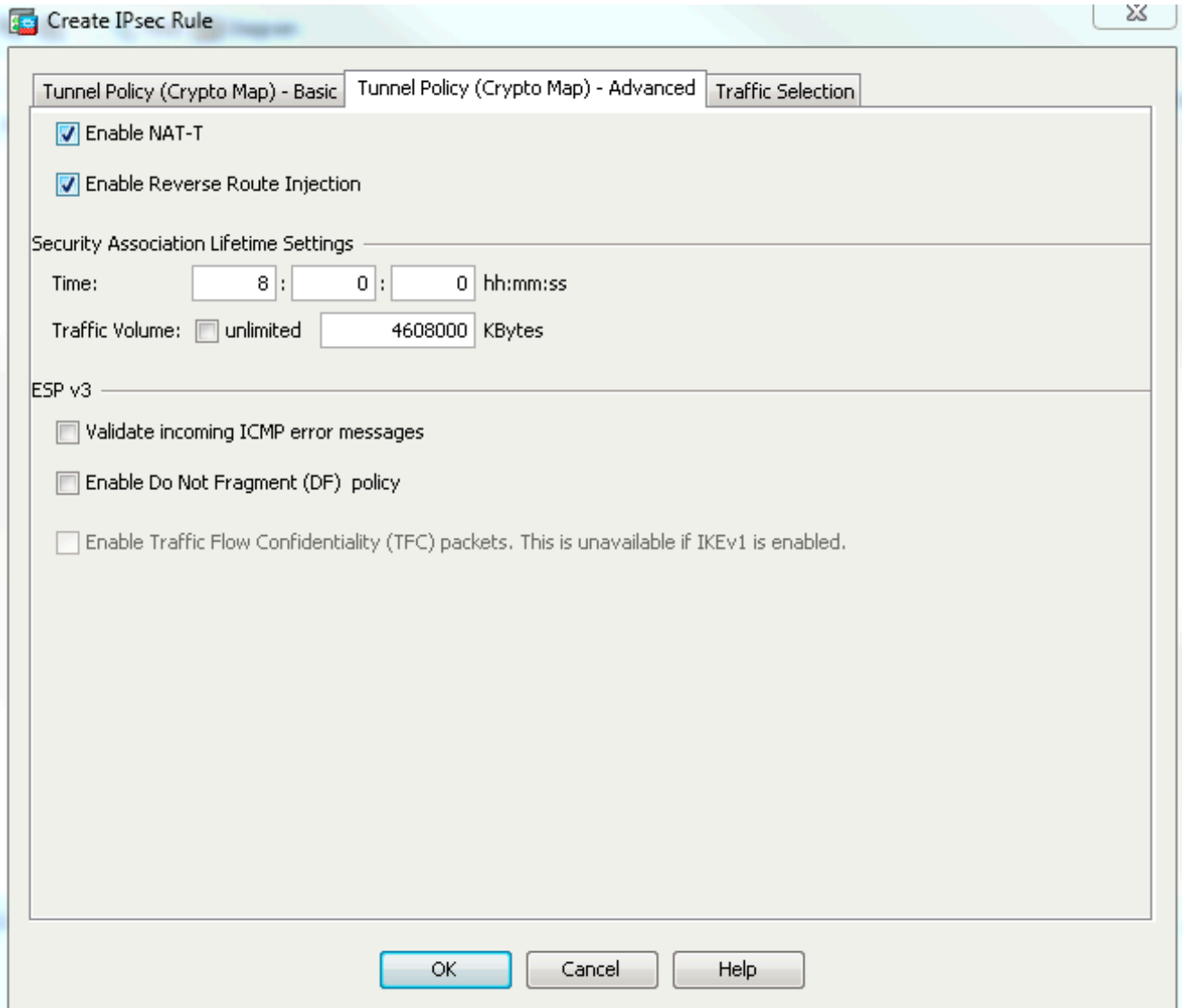
2. In the **Create IPsec Rule** window, from the **Tunnel Policy (Crypto Map) - Basic** tab, choose **outside** from the **Interface** drop-down list and **dynamic** from the **Policy Type** drop-down list. In the **Priority** field, assign the priority for this entry encase there are multiple entries under Dynamic-Map. Next, click **Select** next to the **IKE v1 IPsec Proposal** field in order to select the IPsec proposal.



3. When the **Select IPsec Proposals (Transform Sets)** dialog box opens, choose among the current IPsec proposals or click **Add** in order to create a new one and use the same. Click **OK** when you are done.



- From the **Tunnel Policy (Crypto Map)-Advanced** tab, check the **Enable NAT-T** check box (required if either peer is behind a NAT device) and the **Enable Reverse Route Injection** check box. When the VPN tunnel comes up for the dynamic peer, ASA installs a dynamic route for the negotiated remote VPN network that points to the VPN interface.



Optionally, from the **Traffic Selection** tab you can also define the interesting VPN traffic for the dynamic peer and click **OK**.

Action: Protect Do not Protect

Source Criteria

Source: any4

Destination Criteria

Destination: any4

Service: ip

Description:

More Options

Enable Rule

Source Service: (TCP or UDP service only)

Time Range:

OK

Cancel

Help

Configuration > Site-to-Site VPN > Advanced > Crypto Maps

+ Add ▾ | ✎ Edit ▾ | 🗑 Delete | ⬆ ⬇ | ✂ | 📄 | 🗑 | 🔍 Find | 📊 Diagram

Type:Priority	Traffic Selection					Transform Set (IKEv1)
	#	Source	Destination	Service	Action	
[-] interface: outside						
dynamic: 65535.1	1	any4	any4	IP ip	Protect	tset

Enable Anti-replay window size: 64 ▾

Apply Reset

As mentioned earlier, since ASA does not have any information about the remote dynamic peer IP address, the unknown connection request lands under **DefaultL2LGroup** which exists on ASA by default. In order for authentication to succeed the pre-shared key (cisco123 in this example) configured on the remote peer needs to match with one under **DefaultL2LGroup**.

5. Choose **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups**, select **DefaultL2LGroup**, click **Edit** and configure the desired pre-shared key. Click **OK** when you are done.

Configuration > Site-to-Site VPN > Advanced > Tunnel Groups

Configure IPsec site-to-site tunnel groups.

Name	Group Policy	IKEv1 Enabled	IKEv2 Enabled
DefaultL2LGroup	DfltGrpPolicy	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Edit IPsec Site-to-site Tunnel Group: DefaultL2LGroup

Name:

IPsec Enabling

Group Policy Name:

(Following two fields are attributes of the group policy selected above.)

Enable IKE v1 Enable IKE v2

IPsec Settings

IKE v1 Settings

Authentication

Pre-shared Key:

Device Certificate:

IKE Peer ID Validation:


IKE Keepalive

Disable keepalives

Monitor keepalives

Confidence Interval: seconds

Retry Interval: seconds

 **Note:** This creates a wildcard pre-shared key on the static peer (Central-ASA). Any device/peer who knows this pre-shared key and its matching proposals can successfully establish a VPN tunnel and access resources over VPN. Ensure this pre-shared key is not shared with unknown entities and is not easy to guess.

- Choose **Configuration > Site-to-Site VPN > Group Policies** and select the group-policy of your choice (default group-policy in this case). Click **Edit** and edit the group policy in the Edit Internal Group Policy dialog box. Click **OK** when you are done.

Configuration > Site-to-Site VPN > Group Policies

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. Policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an [LDAP attribute map](#).

Add Edit Delete Assign

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
DfltGrpPolicy (System Default)	Internal	ikev1;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultWEBVPNGroup;

Edit Internal Group Policy: DfltGrpPolicy

Name:

Tunneling Protocols: Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec

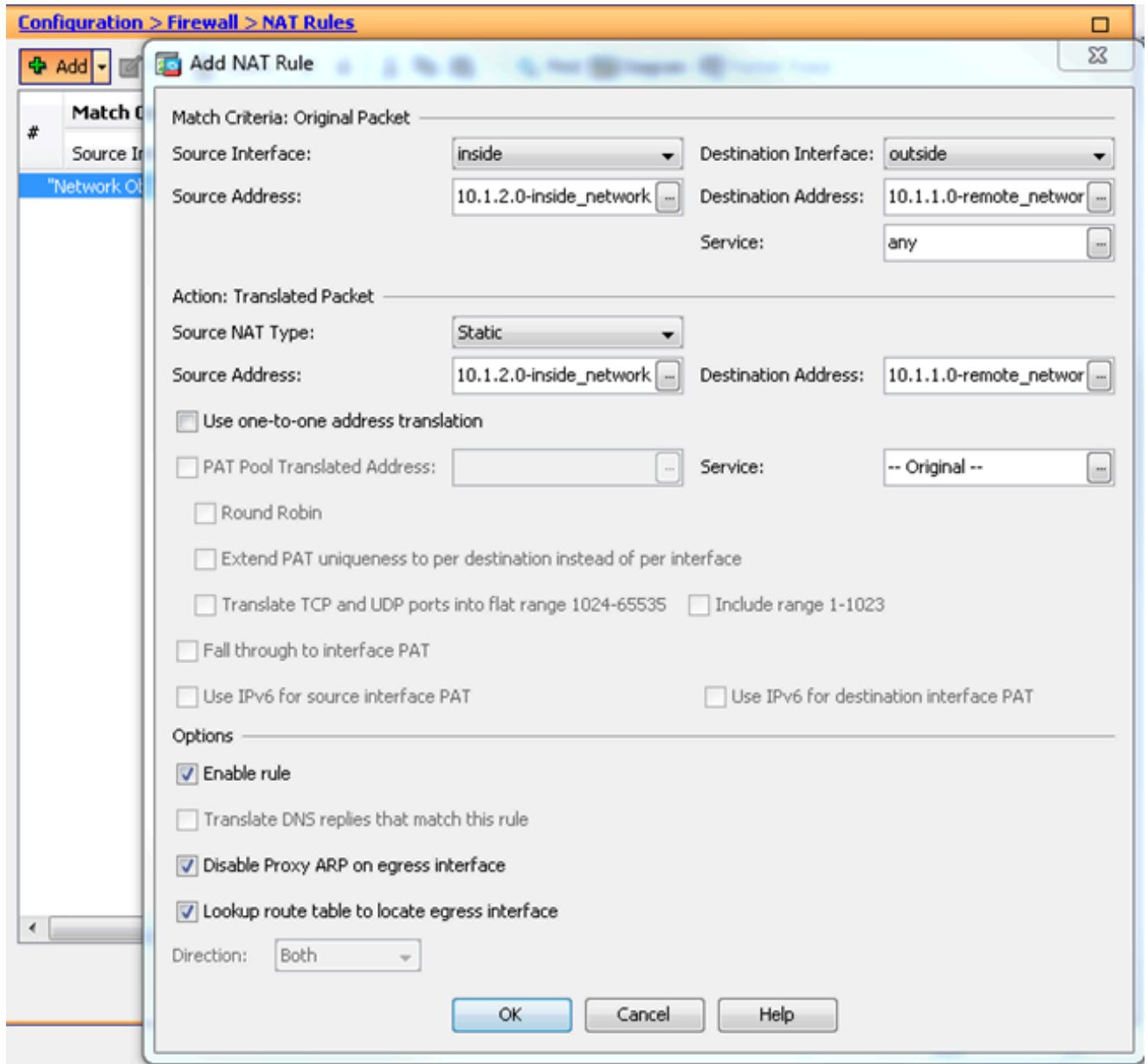
Filter:

Idle Timeout: Unlimited minutes

Maximum Connect Time: Unlimited minutes

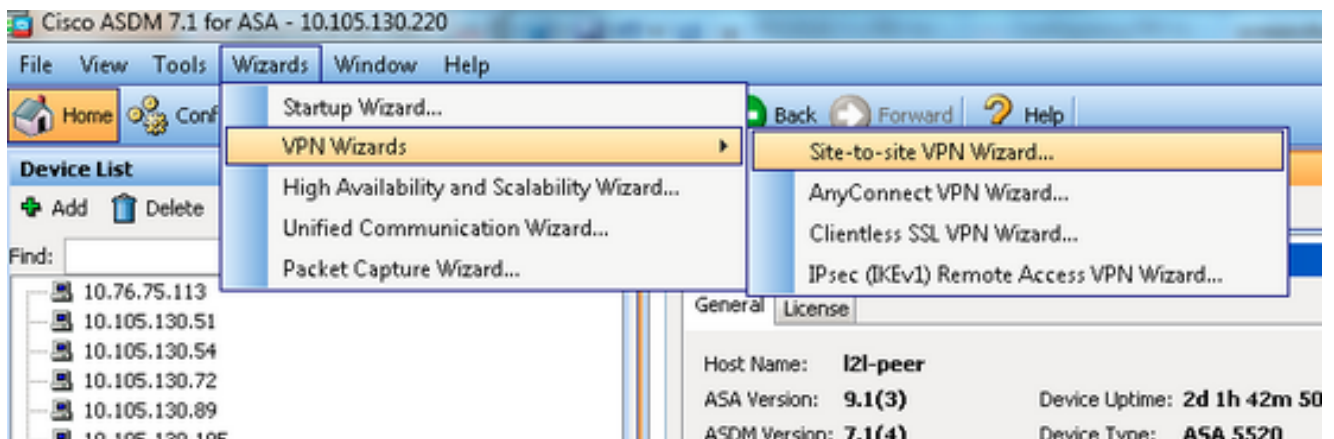
Find: Match Case

7. Choose **Configuration > Firewall > NAT Rules** and from the Add Nat Rule window, configure a no nat (NAT-EXEMPT) rule for VPN traffic. Click **OK** when you are done.

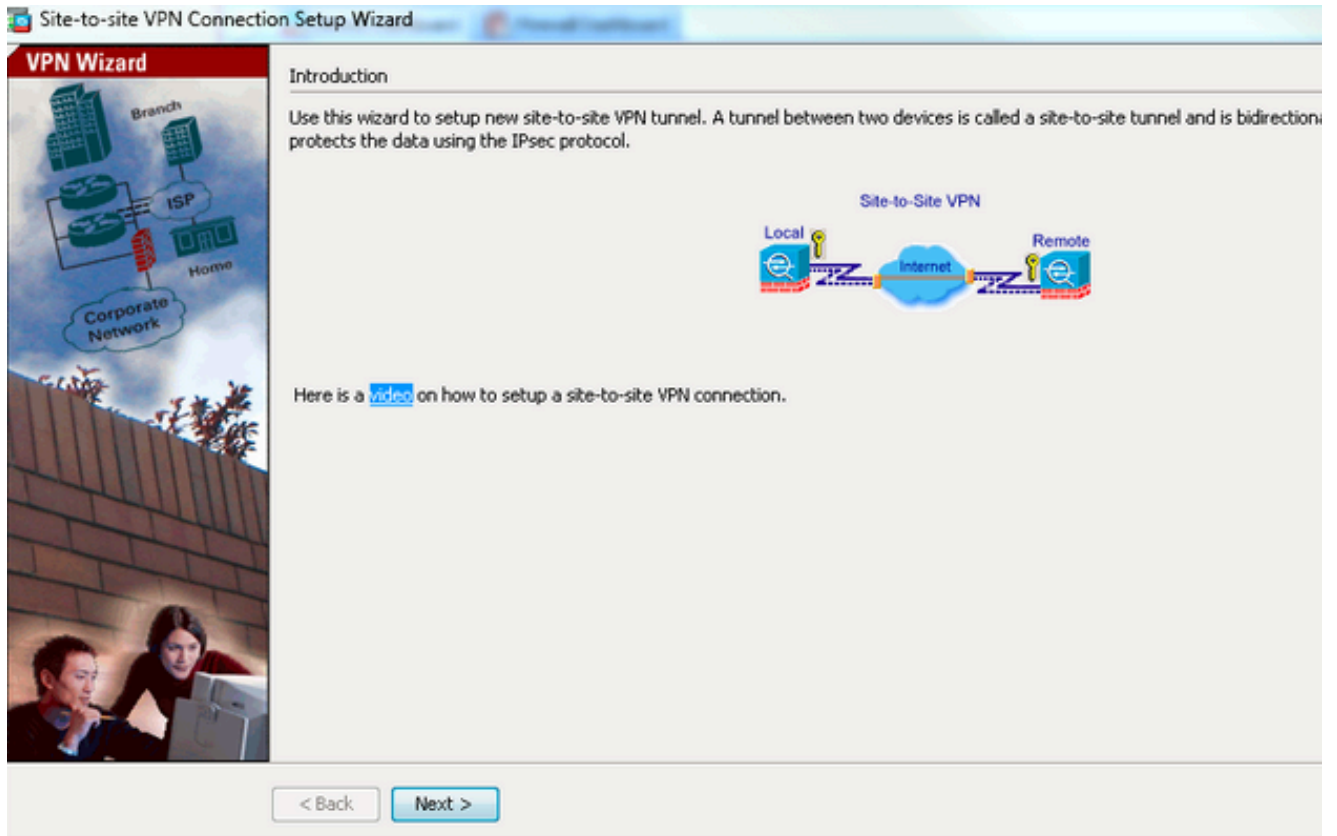


Remote-ASA (Dynamic Peer)

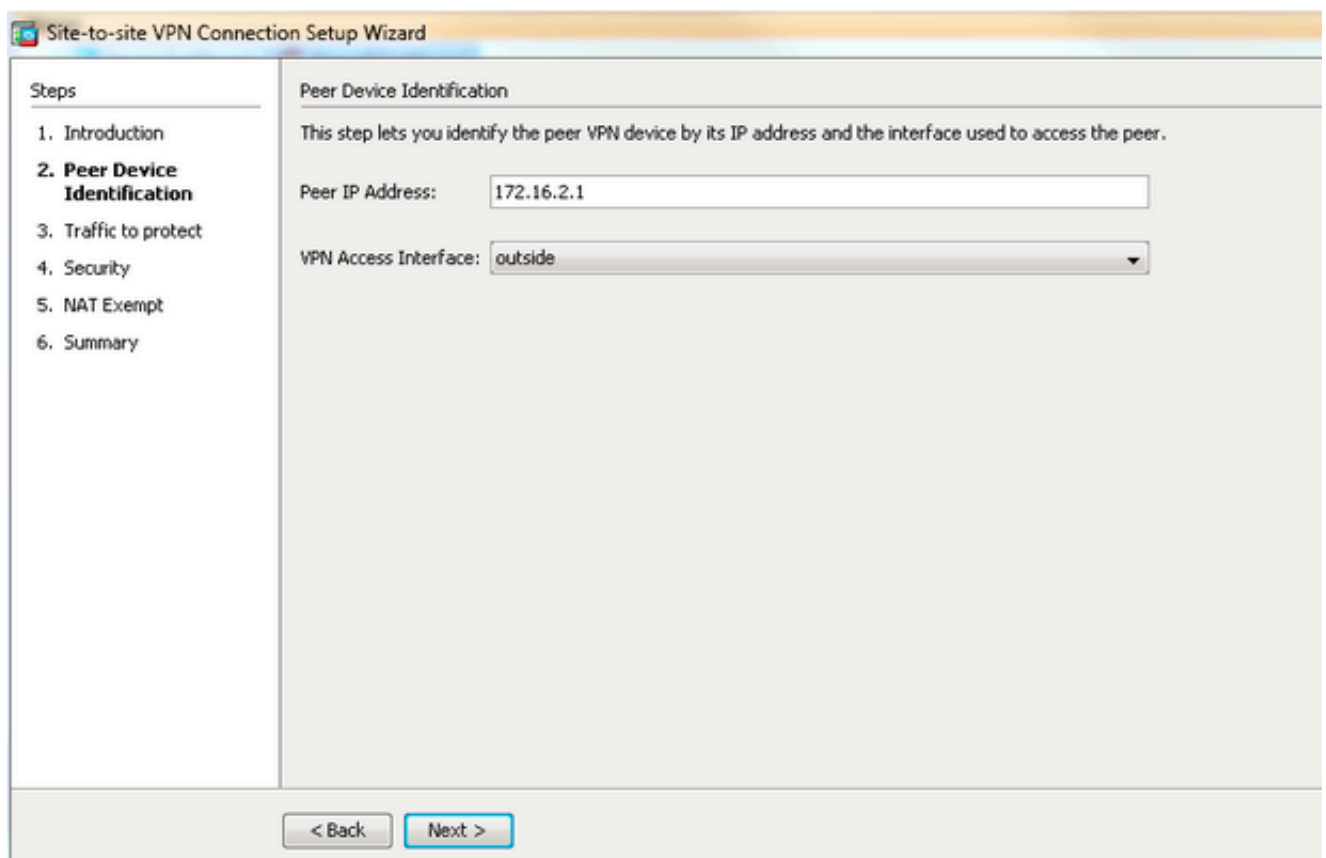
1. Choose **Wizards > VPN Wizards > Site-to-site VPN Wizard** once the ASDM application connects to the ASA.



2. Click **Next**.

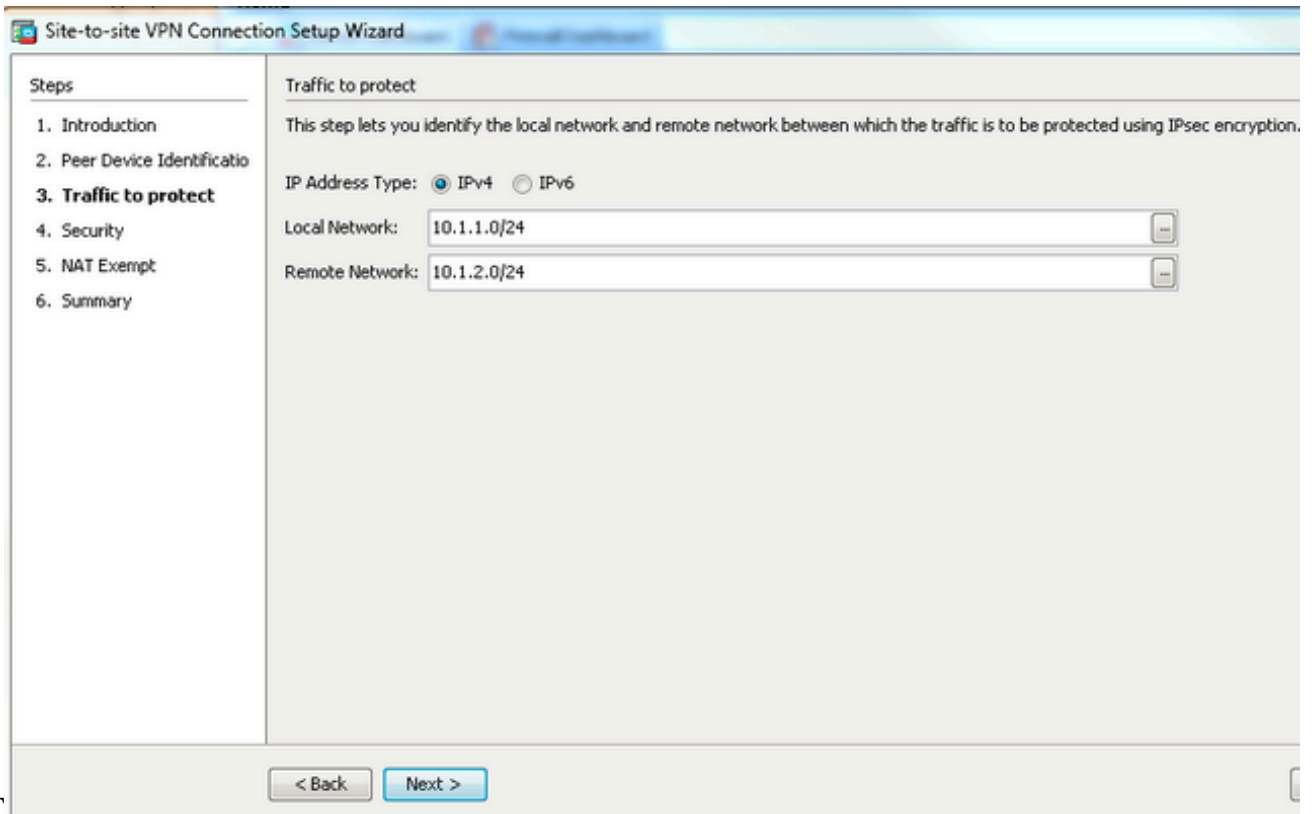


3. Choose **outside** from the **VPN Access Interface** drop-down list in order to specify the outside IP address of the remote peer. Select the interface (**WAN**) where the crypto map is applied. Click **Next**.



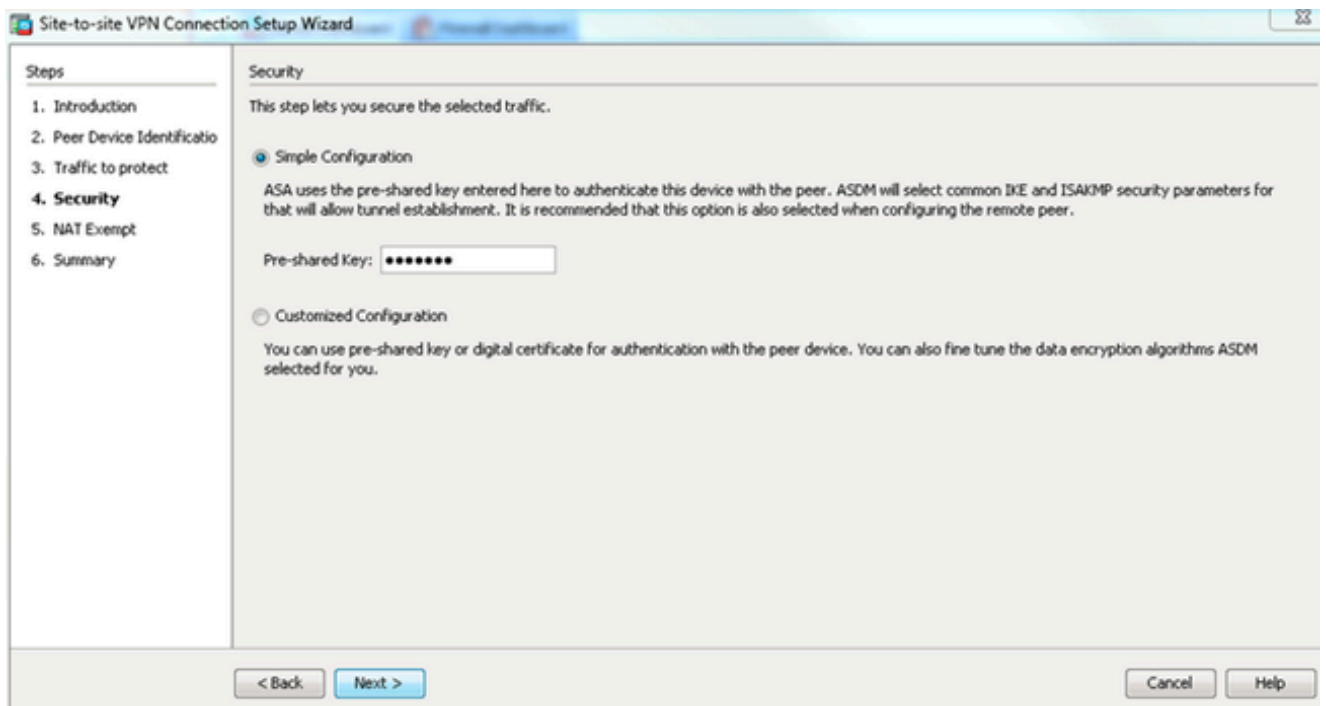
4. Specify the hosts/networks that must be allowed to pass through the VPN tunnel. In this step, you need to provide the Local Networks and Remote Networks for the VPN Tunnel. Click the buttons next to the Local Network and Remote Network fields and choose the address as per requirement. Click

Next when you are done.



T

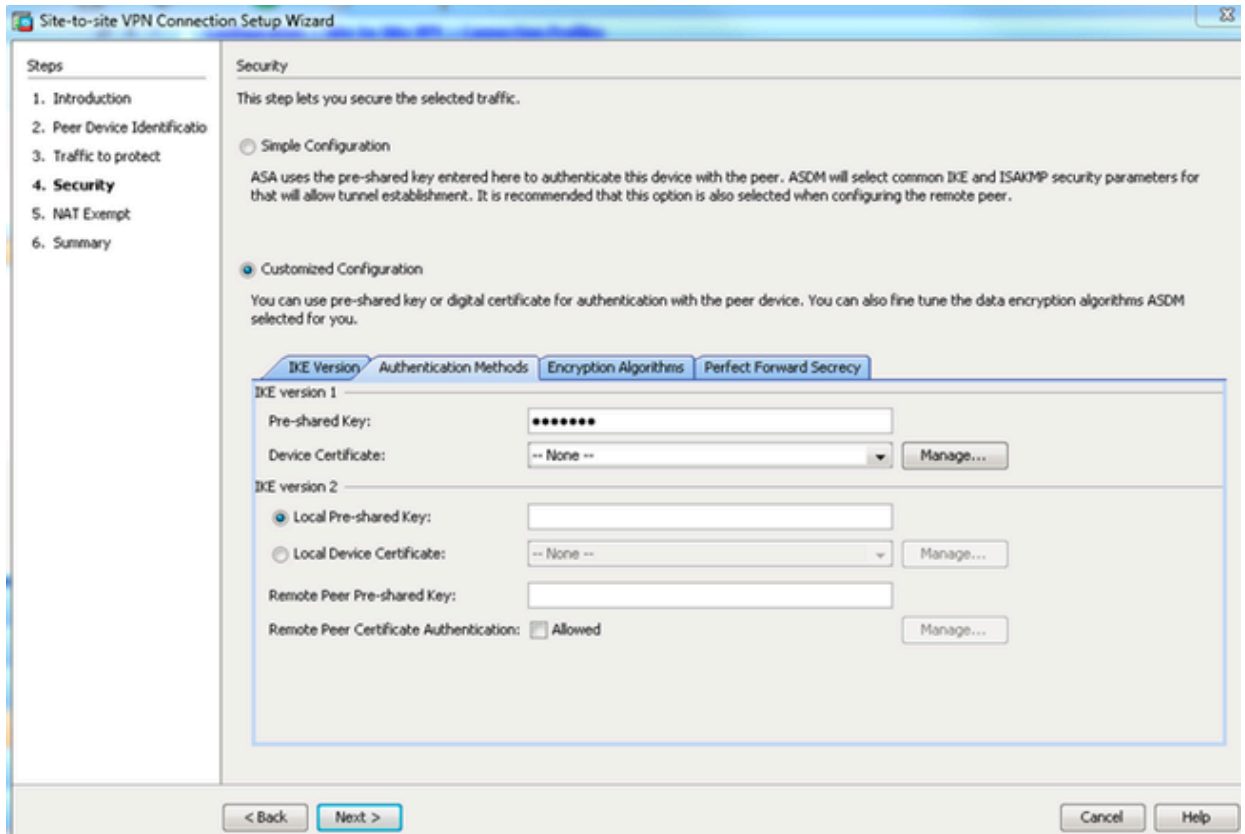
5. Enter the authentication information to use, which is pre-shared key in this example. The pre-shared key used in this example is **cisco123**. The **Tunnel Group Name** is the remote peer IP address by default if you configure LAN-to-LAN (L2L) VPN.



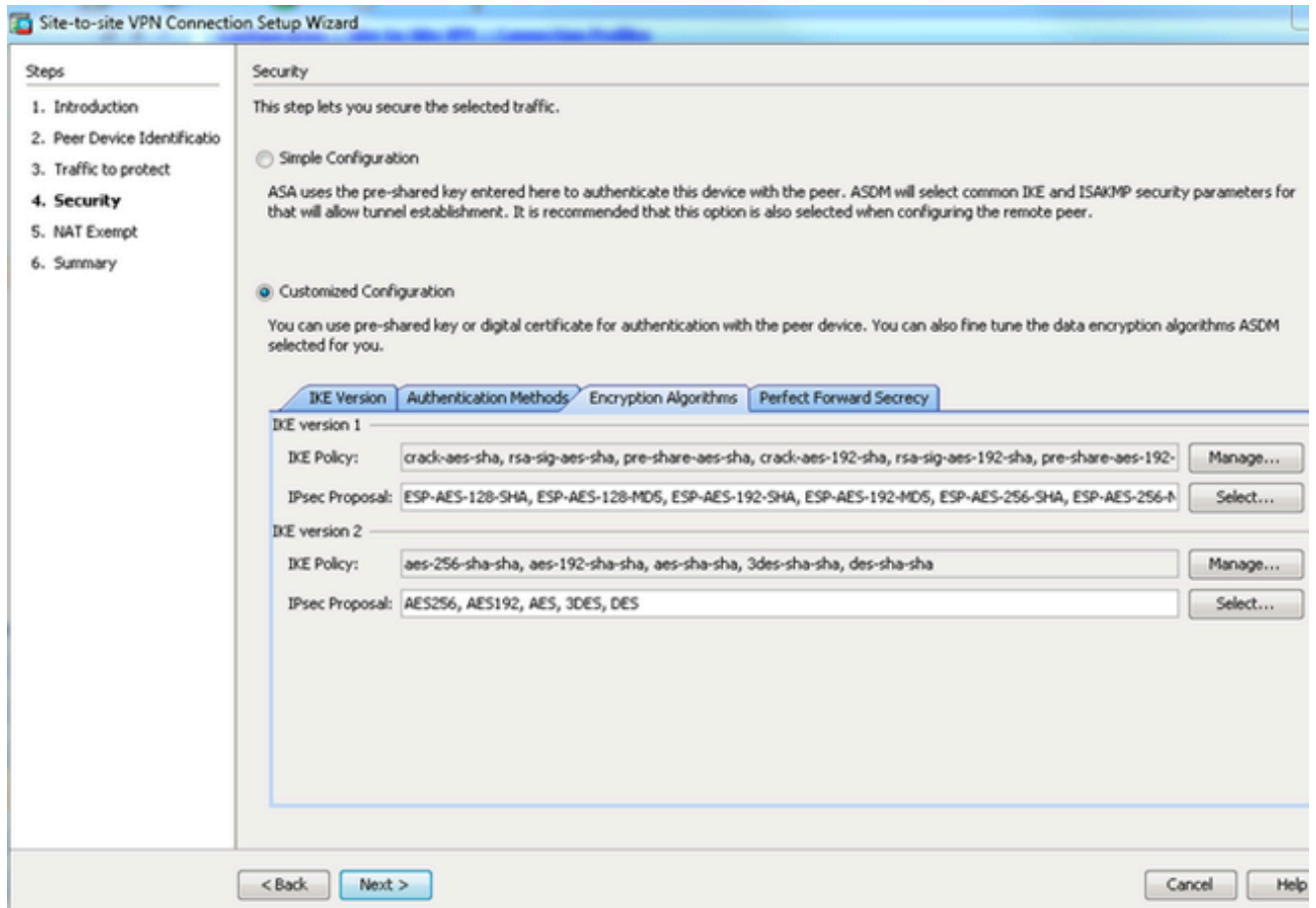
OR

You can customize the configuration to include the IKE and IPsec policy of your choice. There needs to be at least one matching policy between the peers:

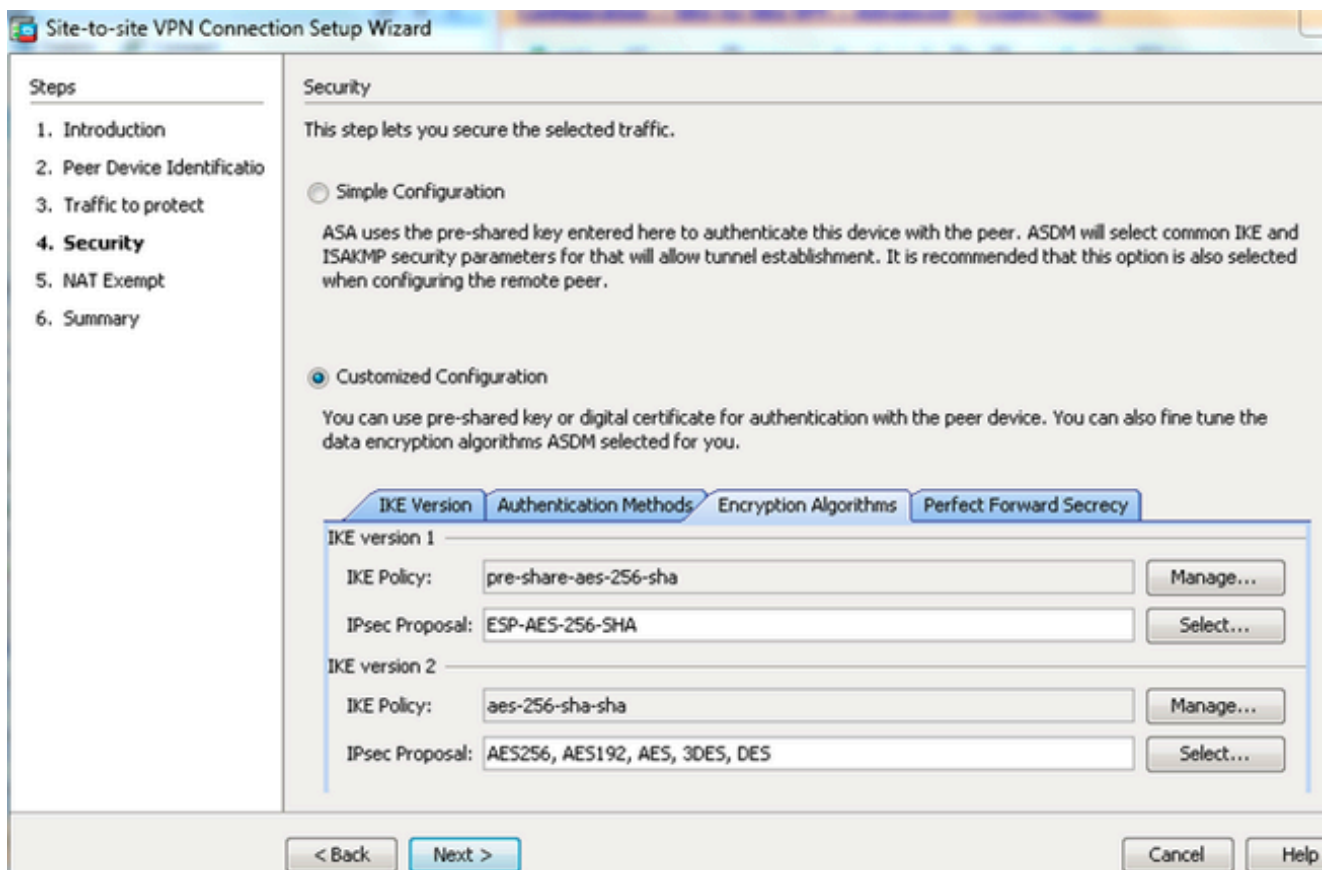
- a. From the **Authentication Methods** tab, enter the **IKE version 1** pre-shared Key in the **Pre-shared Key** field. In this example, it is **cisco123**.



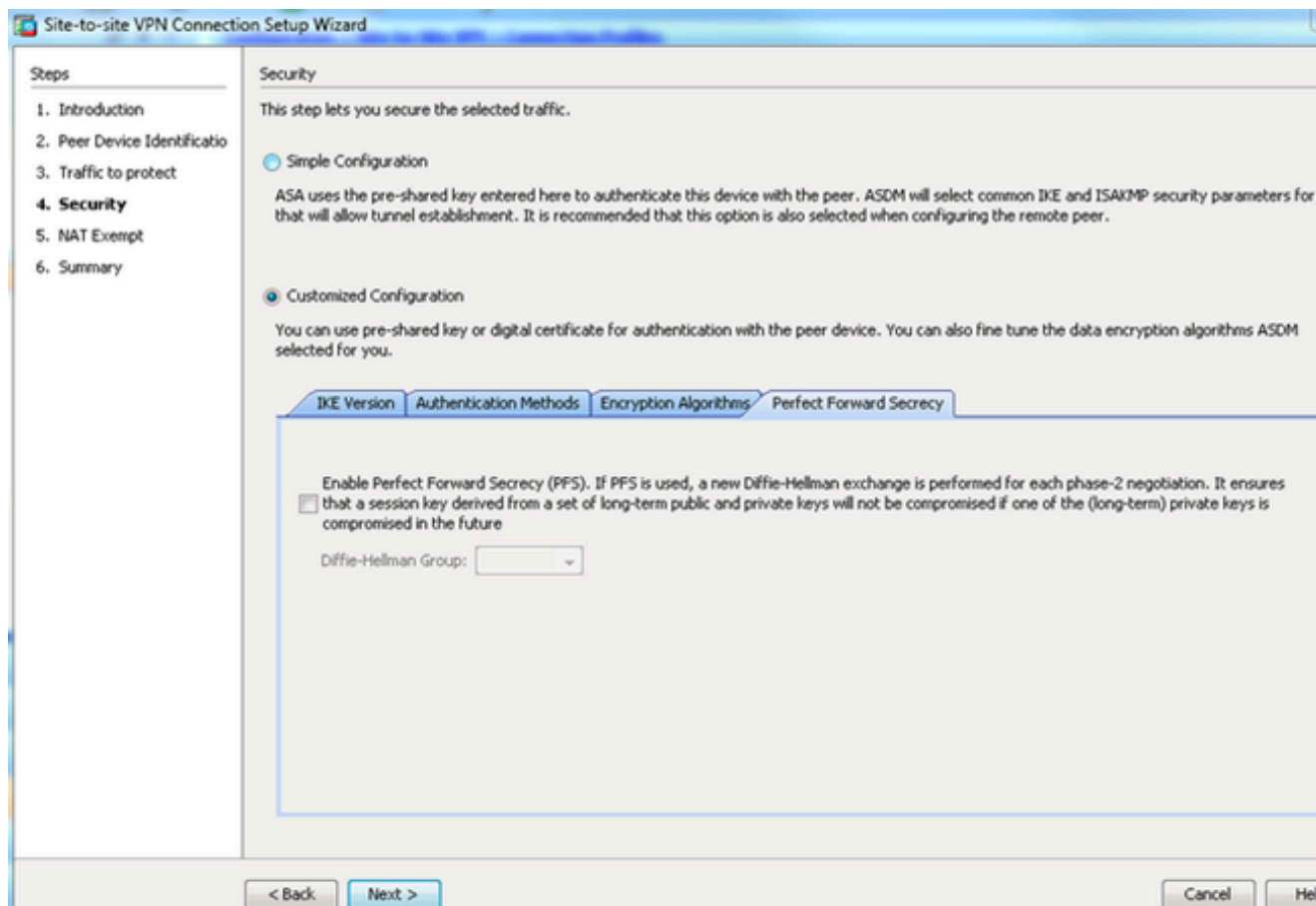
- b. Click the **Encryption Algorithms** tab.
6. Click **Manage** next to the **IKE Policy** field, click **Add** and configure a custom IKE Policy (phase-1). Click **OK** when you are done.



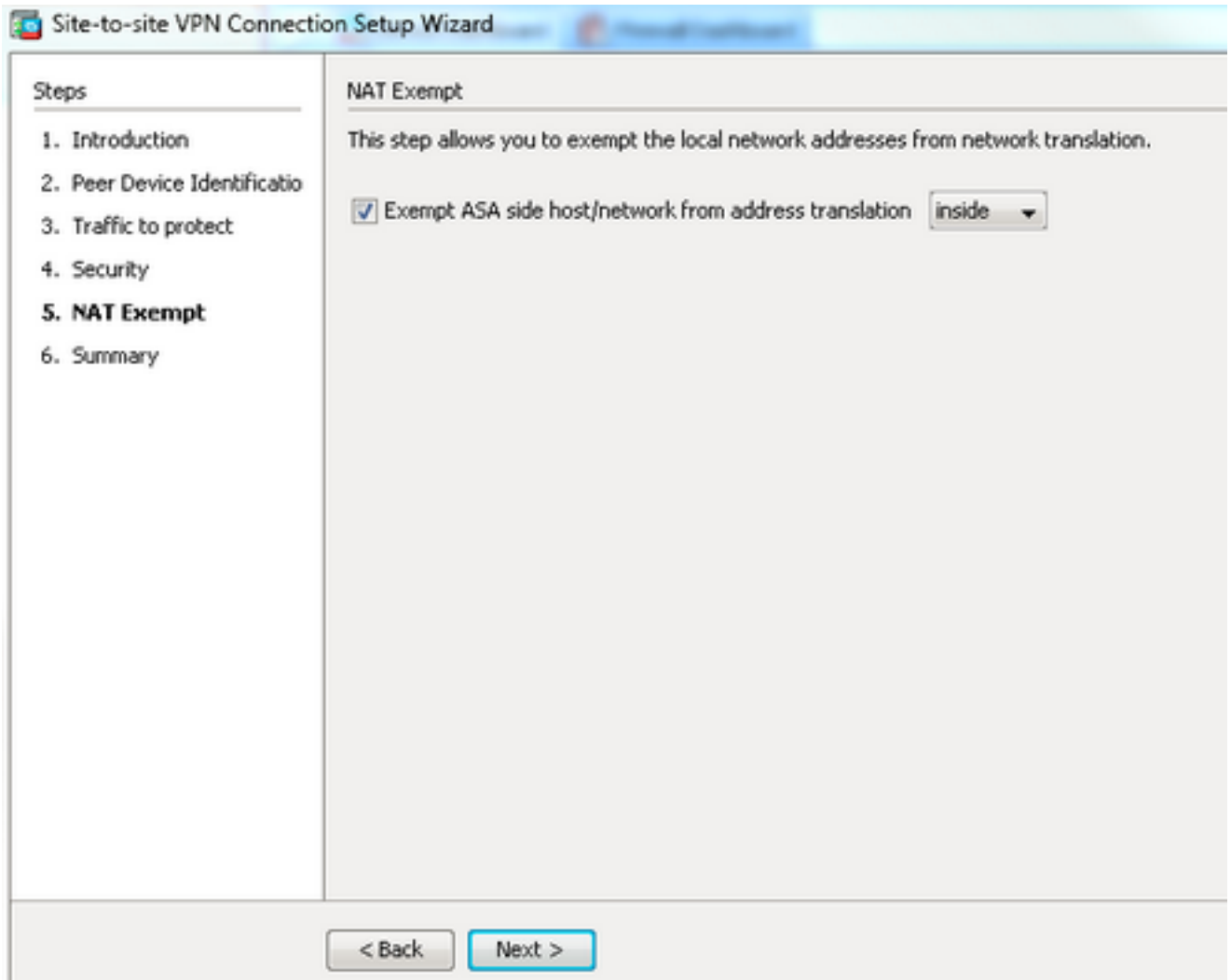
7. Click **Select** next to the the **IPsec Proposal** field and select the desired IPsec Proposal. Click **Next** when you are done.



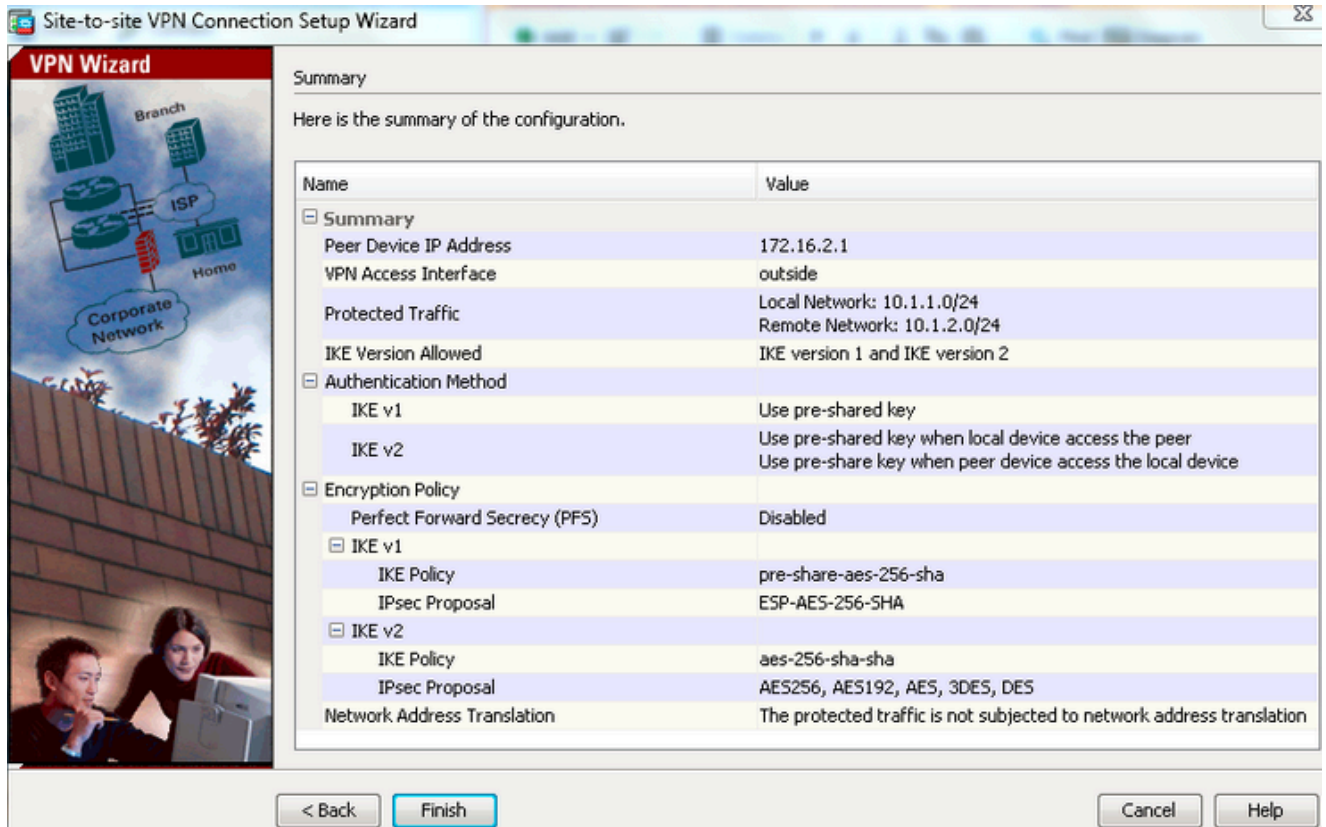
Optionally, you can go to the **Perfect Forward Secrecy** tab and check the **Enable Perfect Forward Secrecy (PFS)** check box. Click **Next** when you are done.



8. Check the box next to **Exempt ASA side host/network from address translation** in order to prevent the tunnel traffic from the start of Network Address Translation. Choose either **local** or **inside** from the drop-down list in order to set the interface where local network is reachable. Click **Next**.



9. ASDM displays a summary of the VPN just configured. Verify and click **Finish**.



CLI Configuration

Central ASA (Static Peer) Configuration

1. Configure a NO-NAT/ NAT-EXEMPT rule for VPN traffic as this example shows:

```
object network 10.1.1.0-remote_network
  subnet 10.1.1.0 255.255.255.0
```

```
object network 10.1.2.0-inside_network
  subnet 10.1.2.0 255.255.255.0
```

```
nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup
```

2. Configure the pre-shared key under **DefaultL2LGroup** in order to authenticate any remote Dynamic-L2L-peer:

```
tunnel-group DefaultL2LGroup ipsec-attributes
  ikev1 pre-shared-key cisco123
```

3. Define the phase-2/ISAKMP policy:

```
crypto ikev1 policy 10
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
```

4. Define the phase-2 transform set/IPsec policy:

```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```

5. Configure the dynamic map with these parameters:

- Required transform-set
- Enable Reverse Route Injection (RRI), which allows the Security Appliance to learn routing information for connected clients (Optional)

```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
crypto dynamic-map outside_dyn_map 1 set reverse-route
```

6. Bind the dynamic map to the crypto map, apply the crypto map and enable ISAKMP/IKEv1 on the outside interface:

```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

crypto map outside_map interface outside
crypto ikev1 enable outside
```

Remote-ASA (Dynamic Peer)

1. Configure a NAT exemption rule for VPN traffic:

```
object network 10.1.1.0-inside_network
  subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-remote_network
  subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
no-proxy-arp route-lookup
```

2. Configure a tunnel-group for a static VPN peer and pre-shared key.

```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```

3. Define PHASE-1/ISAKMP policy:

```
crypto ikev1 policy 10
  authentication pre-share
  encryption aes-256
  hash sha
```

```
group 2
lifetime 86400
```

4. Define a phase-2 transform set/IPsec policy:

```
<#root>
```

```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```

5. Configure an access-list that defines interesting VPN traffic/network:

```
access-list outside_cryptomap extended permit ip object
10.1.1.0-inside_network object 10.1.2.0-remote_network
```

6. Configure static crypto map with these parameters:

- Crypto/VPN access-list
- Remote IPsec peer IP address
- Required transform-set

```
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set peer 172.16.2.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
```

7. Apply the crypto map and enable ISAKMP/IKEv1 on the outside interface:

```
crypto map outside_map interface outside
crypto ikev1 enable outside
```

Verify

Use this section to confirm that configuration works properly.

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

Note: Only registered Cisco users can access internal Cisco tools and information.

- **show crypto isakmp sa**—Displays all current IKE Security Associations (SAs) at a peer.
- **show crypto ipsec sa**—Displays all current IPsec SAs.

This section shows example verification output for the two ASAs.

Central ASA

```
<#root>
```

```
Central-ASA#
```

```
show crypto isakmp sa
```

```
IKEv1 SAs:
```

```
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: 172.16.1.1
Type      : L2L           Role      : responder
Rekey     : no           State     : MM_ACTIVE
```

```
Central-ASA# show crypto ipsec sa
interface: outside
```

```
Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1
```

```
local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
current_peer: 172.16.1.1
```

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #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
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 30D071C0
current inbound spi : 38DA6E51
```

```
inbound esp sas:
```

```
spi: 0x38DA6E51 (953839185)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings = {L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
sa timing: remaining key lifetime (kB/sec): (3914999/28588)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F
```

```
outbound esp sas:
```

```
spi: 0x30D071C0 (818966976)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings = {L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
sa timing: remaining key lifetime (kB/sec): (3914999/28588)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

Remote-ASA

```
<#root>
```

```
Remote-ASA#
```

```
show crypto isakmp sa
```

IKEv1 SAs:

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:

172.16.2.1

Type : L2L Role :
initiator

Rekey : no State :
MM_ACTIVE

Remote-ASA#

show crypto ipsec sa

interface: outside
Crypto map tag:

outside_map

, seq num: 1, local addr: 172.16.1.1

access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0

local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)

current_peer: 172.16.2.1

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #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
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 38DA6E51
current inbound spi : 30D071C0

inbound esp sas:

spi: 0x30D071C0 (818966976)

transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373999/28676)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F

outbound esp sas:

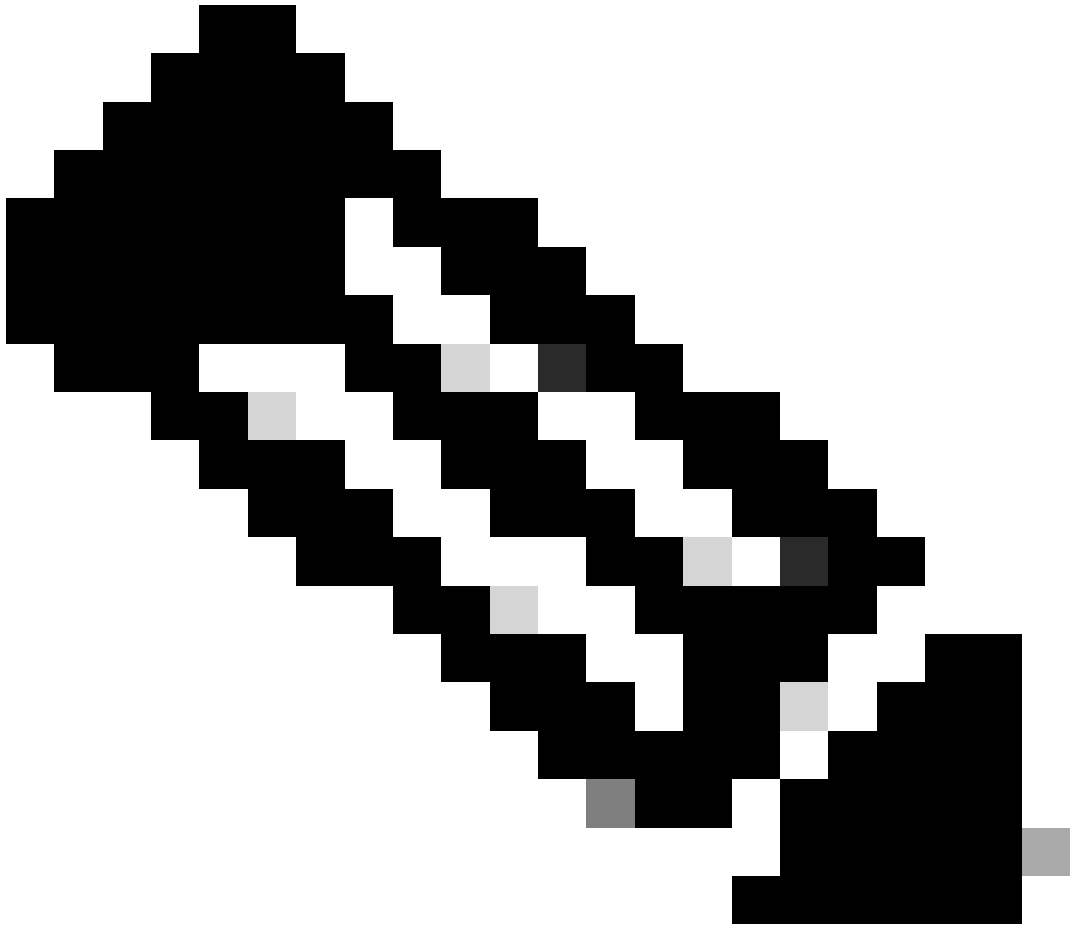
spi: 0x38DA6E51 (953839185)

transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373999/28676)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

Troubleshoot

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

The [Output Interpreter Tool](#) supports certain `show` commands. Use the Output Interpreter Tool in order to view an analysis of `show` command output.




Note: Only registered Cisco users can access internal Cisco tools and information.



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

Make use of these commands as shown:

```
clear crypto ikev1 sa <peer IP address>  
Clears the Phase 1 SA for a specific peer.
```

 **Caution:** The `clear crypto isakmp sa` command is intrusive as it clears all active VPN tunnels.

In PIX/ASA software release 8.0(3) and later, an individual IKE SA can be cleared using the `clear crypto isakmp sa<peer ip address>` command. In software releases earlier than 8.0(3), use the [vpn-sessiondb logoff tunnel-group <tunnel-group-name>](#) command in order to clear IKE and IPsec SAs for a single tunnel.

<#root>

Remote-ASA#

```
vpn-sessiondb logoff tunnel-group 172.16.2.1
```

Do you want to logoff the VPN session(s)? [confirm]

INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1

```
clear crypto ipsec sa peer <peer IP address>
```

!!! Clears the required Phase 2 SA for specific peer.

```
debug crypto condition peer < Peer address>
```

!!! Set IPsec/ISAKMP debug filters.

```
debug crypto isakmp sa <debug level>
```

!!! Provides debug details of ISAKMP SA negotiation.

```
debug crypto ipsec sa <debug level>
```

!!! Provides debug details of IPsec SA negotiations

```
undebug all
```

!!! To stop the debugs

Debugs used:

```
debug cry condition peer <remote peer public IP>
```

```
debug cry ikev1 127
```

```
debug cry ipsec 127
```

Remote-ASA (Initiator)

Enter this **packet-tracer** command in order to initiate the tunnel:

```
<#root>
```

```
Remote-ASA#
```

```
packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed
```

```
<#root>
```

```
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
```

```
Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
```

```
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple:
```

```
Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
```

```
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
```

```
Jan 19 22:00:06
```

```
[IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
```

```
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
```

```
10.1.2.0, Crypto map (outside_map)
```

```
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06

[IKEv1]IP = 172.16.2.1
,
Connection landed on tunnel_group 172.16.2.1

<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,

Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device

Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,

processing ID payload

Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,

ID_IPV4_ADDR ID received

172.16.2.1

:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin quick mode
Jan 19 22:00:06

[IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED

Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
```

IKE Initiator

starting QM

: msg id = c45c7b30

:

.

Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1,

IP = 172.16.2.1, Transmitting Proxy Id:

Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0

Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0

:

.

Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message

(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE

(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200

Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message

(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +

ID (5) + ID (5) + NONE (0) total length : 172

:

.

Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,

processing ID payload

Jan 19 22:00:06

[IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,

ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0

Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload

Jan 19 22:00:06

[IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,

ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0

:

.

Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,

Security negotiation complete for LAN-to-LAN Group (172.16.2.1)

Initiator,

Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51

:

.

Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message

(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76

:

.

Jan 19 22:00:06 [IKEv1]

Group = 172.16.2.1, IP = 172.16.2.1,

PHASE 2 COMPLETED

(msgid=c45c7b30)

Central-ASA (Responder)

<#root>

```
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length
:
132
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 20 12:42:35
[IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group
DefaultL2LGroup

Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,

ID_IPV4_ADDR ID received    172.16.1.1

:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +
VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1]

Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED

:
.
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1,

IKE Responder starting QM

:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
```

```
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
Received remote
IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1,
Received local
IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0,
Protocol 0, Port 0
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35
[IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map
check, map outside_dyn_map, seq = 1 is a successful match
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
.
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup)
Responder,
Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED
(msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
Adding static
route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0
```

Related Information

- [IPsec Negotiation/IKE Protocols Support Page](#)
- [ASA Command Reference](#)
- [Requests for Comments \(RFCs\)](#)
- [Cisco Technical Support & Downloads](#)