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) 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 <u>Command Lookup Tool</u> 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.

	olicy (Cryp	co Map) - I	Basic Tunne	l Policy (Crypto	(Map) - 4	Advanced T	rattic Sele	ection		
Int	erface:	outside	•	Policy 1	(ype:	dynamic	•	Priorit	iy: 1	
IPs	sec Propos	als (Transf	form Sets) —							
IKE	v1 IPsec P	proposal:							Select	
IKE	v2 IPsec P	Proposal:							Select	
De	er Settings	- Option	al for Dynam	ic Crypto Map P	otriec					
Pe	er Settings	- Option	al for Dynam	ic Crypto Map E	intries —	1				
Pe Th foi	er Settings e Connecti r LAN-to-L4	 Option Type is N redund 	al for Dynam applicable to ancy, Tunnel	ic Crypto Map E static tunnel p policies of the '	intries olicies or Originate	ily. Uni-direct	tional conr ection type	nection type p e may specify	policies are used up to 10	
Pe Th foi rea	er Settings e Connecti r LAN-to-L4 dundant pe	on Type is N redund ers.	al for Dynam applicable to ancy, Tunnel	ic Crypto Map B) static tunnel p policies of the '	intries olicies or Originate	ily, Uni-direct e Only' conne	tional conr ection type	nection type p e may specify	policies are used up to 10	
Pe Th foi rei	er Settings e Connecti r LAN-to-L4 dundant pe	on Type is N redund eers.	al for Dynam applicable to ancy, Tunnel	ic Crypto Map E) static tunnel p policies of the '	intries olicies or Originate	ily, Uni-direct e Only' conne	tional conr ection type	nection type p e may specify	policies are used up to 10	
Pe Th for rea	er Settings ie Connecti r LAN-to-L4 dundant pe	a - Option on Type is AN redund eers.	al for Dynam applicable to ancy, Tunnel	ic Crypto Map E) static tunnel p policies of the '	intries olicies or Originate	ily, Uni-direct 9 Only' conne	tional conr action type	nection type p e may specify	policies are used up to 10	
Pe Th fou rea	er Settings ie Connecti r LAN-to-LA dundant pe	Option Type is AN redund eers.	al for Dynam applicable to ancy. Tunnel	ic Crypto Map E) static tunnel p policies of the '	intries olicies or Originate	ily, Uni-direct e Only' conne	tional conr ection type	nection type (e may specify	policies are used up to 10	
Pe Th for rea	er Settings e Connecti r LAN-to-LA dundant pe Address ol	on Type is AN redund eers.	al for Dynam applicable to ancy. Tunnel Be Added:	ic Crypto Map E o static tunnel p policies of the	intries – olicies or Originate	ily, Uni-direct e Only' conne	tional conr ection type	nection type p e may specify	policies are used up to 10	
Pe Th foi re	er Settings ie Connecti r LAN-to-LA dundant pe dundant pe	Option Type is AN redund eers.	al for Dynam ; applicable to ancy. Tunnel 3e Added:	ic Crypto Map E o static tunnel p policies of the Add >>	intries olicies or Originate	ily, Uni-direct e Only' conne	tional conr ection type	nection type p e may specify	policies are used up to 10 Move Up	
Pe Th for rea	er Settings e Connecti r LAN-to-L4 dundant pe Address ol	- Option on Type is AN redund eers. f Peer to E	al for Dynam applicable to ancy. Tunnel e Added:	ic Crypto Map E o static tunnel p policies of the Add >>	intries — olicies or Originate	ıly, Uni-direct e Only' conne	tional conr ection type	nection type p e may specify	Move Up	

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.

Interface:	outside 👻	Policy	Type: dynamic •	Priority: 1]
IPsec Propo	sals (Transform Sets)				
IKE v1 IPsec	Proposal: tset			Select	
IKE V2 IPS	Salact IDrac Prop	orals (Transfo	rm Sate)		8
	Select IPSec Prop	osais (Transio	im sets)		
	🖨 add 📝 Edit	Delete			
		Delete			
	Name	Mode	ESP Encryption	ESP Authentication	
Deer Settin	ESP-3DES-SHA	Transport	3DES	SHA	A .
Peer Jetti	ESP-3DES-MDS	Transport	3DES	MD5	
The Conne	ESP-DES-SHA	Tunnel	DES	SHA	
for LAN-to	ESP-DES-MDS	Tunnel	DES	MD5	
redundani	ESP-DES-SHA-T	Transport	DES	SHA	
	ESP-DES-MDS-T	Transport	DES	MDS	=
	tset	Tunnel	AES-256	SHA	•
	Assigned IPsec Pro	nosals			
IP Addres	Assigned in section	posas			
	Assign-> ts	et			
			OK Cancel	Help	

4. 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.

🔁 Create IPsec F	ule			23
Tunnel Policy (C	rypto Map) - Basic Tur	nnel Policy (Crypto Map) - Adva	nced Traffic Selection	
🔽 Enable NA	'-T			
📝 Enable Rev	erse Route Injection			
Security Associat	on Lifetime Settings —			
Time:		0 hh:mm:ss		
Traffic Volume:	unlimited	4608000 KBytes		
ESP v3				
Validate ind	oming ICMP error messa	ages		
Enable Do	Vot Fragment (DF) polic	εy.		
Enable Tra	fic Flow Confidentiality	(TFC) packets. This is unavailab	ble if IKEv1 is enabled.	
	(OK Cancel	Help	

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

🧧 Creat	e IPsec	Rule	-							23
Tunnel	Policy (Crvoto I	Map) - Basic	Tunnel Poli	icy (Crypto) Map) - Adva	anced	Traffic Select	ion	
Action	n: 💿 P	rotect	🔘 Do not f	Protect	-, (-,,,	···			<u> </u>	
Sourc	e Criteri	ia ——								
Sourc	e:	any4								
Destir	nation C	riteria -								
Destin	nation:	any4								
Servio	:e:	ip								
Descr	iption:									
Mor	e Opti	ons								*
	Enable	Rule								
Sou	rce Serv	/ice:					- (TCP or UDP ser	vice only) 🙃	
Time	e Range		•							
				0	ĸ	Cancel		Help		

Configuration > Site-	-to-Si	te VPN > Advanc	<u>ed</u> > <u>Crypto Map</u>	<u>s</u>		
🖶 Add 🝷 🇹 Edit 👻	Î D	elete 🛧 🗲 🎖	6 🖻 🛍 - Q	Find 🔛 Diag	ram	
Turne : Duinviluu	Traf	fic Selection				Turneferm Cab (IVE1)
Type:Priority	#	Source	Destination	Service	Action	Transform Set (IKEVI)
😑 interface: outside						
dynamic: 65535.1	1	🏟 any4	🌍 any4	IP ip	🖌 Protect	tset
4						
Enable Anti-replay	windo	w 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 V	PN > Advanced > Tunnel Group	<u>95</u>
Configure IPsec site-to-site tunn	el groups.	
Name	Group Policy	IKEv1 Enabled IKEv2 Enabled
DefaultL2LGroup	DfltGrpPolicy	
		Edit IPsec Site-to-site Tunnel Group: DefaultL2LGroup
		Name: DefaultL2LGroup
		IPsec Enabling
		Group Policy Name: DfkGrpPolicy
		(Following two fields are attributes of the group policy selected above.)
		V Enable IKE v1 Enable IKE v2
		IPsec Settings
		IKE v1 Settings
		Authentication
		Pre-shared Key:
		Device Certificate: None V Manage
		IKE Peer ID Validation: Required
		IKE Keepalive
		O Disable keepalives
		Monitor keepalives
		Confidence Interval: 10 seconds
		Retry Interval: 2 seconds
		OK Cancel Help

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.

6. 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.

ane	Туре	Tunneling Protocol	Connection Profiles/Users Assigned To
GrpPolicy (System Defau	t) Internal	kev1;ssl-clentless;l2tp-ipsec	DefaultRAGroup;DefaultWE8VPM
	Name: Tunneling Protocols: Filter: Idle Timeout: Maximum Connect Time:	DfltGrpPolicy Clientless SSL VPN SSL VPN Client IPsec IX None Unlimited 30 minutes Unlimited minutes	Ev1 IPsec IKEv2 VL2TP/IPsec

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.

Con	figuration 2	> Firewall > NAT Rules			
ф	Add 🗸 🗹	🔁 Add NAT Rule	6 5, to 1000		23
	Match 0	Match Criteria: Original Packet			
*	Source Ir	Source Interface:	inside 👻	Destination Interface:	outside 👻
"	Network Ol	Source Address:	10.1.2.0-inside_network	Destination Address:	10.1.1.0-remote_networ
				Service:	any
		Action: Translated Packet			
		Source NAT Type:	Static 👻		
		Source Address:	10.1.2.0-inside_network	Destination Address:	10.1.1.0-remote_networ
		🔲 Use one-to-one address transla	tion		
		PAT Pool Translated Address:		Service:	Original
		Round Robin			
		Extend PAT uniqueness to pe	r destination instead of per int	erface	
		Translate TCP and UDP ports	into flat range 1024-65535	Include range 1-1023	3
		Fall through to interface PAT			
		Use IPv6 for source interface P	AT	Use IPv6 for destin	nation interface PAT
		Options			
		📝 Enable rule			
		Translate DNS replies that mate	h this rule		
		Disable Proxy ARP on egress int	terface		
4		Lookup route table to locate eg	ress interface		
		Direction: Both 👻			
			OK Cancel	Help	

Remote-ASA (Dynamic Peer)

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

Cisco ASDM 7.1 fo	r ASA - 10.105.130.220
File View Tools	Wizards Window Help
Home 🖧 Conf	Startup Wizard Back 🕥 Forward 🤣 Help
Dauisa List	VPN Wizards Site-to-site VPN Wizard
Add 1 Delete	High Availability and Scalability Wizard AnyConnect VPN Wizard
Find:	Packet Capture Wizard IPsec (IKEv1) Remote Access VPN Wizard
- 3 10.76.73.113 - 3 10.105.130.51 - 3 10.105.130.54 - 3 10.105.130.72 - 3 10.105.130.89 - 3 10.105.130.89 - 3 10.105.130.89	General License Host Name: 121-peer ASA Version: 9.1(3) Device Uptime: 2d 1h 42m 50 ASDM Version: 7.1(4) Device Type: ASA 5520

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.

Steps	Peer Device Identification
1. Introduction	This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.
2. Peer Device Identification	Peer IP Address: 172.16.2.1
 Iramic to protect Security 	VPN Access Interface: outside
5. NAT Exempt	
6. Summary	

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.

Steps	Traffic to protect
 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption IP Address Type: IPv4 IPv6 Local Network: 10.1.1.0/24 Remote Network: 10.1.2.0/24
	< Back Next >

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.

1. Introduction This step lets you secure the selected traffic. 2. Peer Device Identification Simple Configuration 3. Traffic to protect ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IRE and ISARMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer. 5. NAT Exempt Pre-shared Key: 6. Summary Customized Configuration 7. You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.	Steps	Security
	 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	This step lets you secure the selected traffic. Simple Configuration ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer. Pre-shared Key: Customized Configuration You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

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 Preshared Key field. In this example, it is cisco123.

s ps	Security				
1. Introduction 2. Peer Device Identificatio 3. Traffic to protect 4. Security 5. NAT Exempt 6. Summary	Security This step lets you secure the selected traffic. Simple Configuration ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer. Customized Configuration You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM				
	IKE Version Authentication Methods	Encryption Algorithms	Perfect Forward Secrecy		
	Pre-shared Key:	•••••			
	Device Certificate: IXE version 2	None	•	Manage	
	Local Pre-shared Key: Local Device Certificate:	None		Manage	
	Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	Allowed		Manage	

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.

sceps	Security		
1. Introduction	This step lets you see	ure the selected traffic.	
2. Peer Device Identificatio			
3. Traffic to protect	Simple Configurat	ion	
4. Security	ASA uses the pre-s	hared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security al establishment. It is recommended that this option is also selected when configuring the remote peer.	parameters for
5. NAT Exempt	UID. WE DOW COLO	o estado ment. A o recommended cha cho aporno apo selected milen consigning che remote peer.	
6. Summary			
	Customized Confi	guration	
	selected for you.		
	IKE Version	Authentication Methods Encryption Algorithms Perfect Forward Secrecy	
	IKE Policy:	crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-share-aes-192-	Manage
	IPsec Proposal:	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-N	Select
	IKE version 2		
	IKE Policy:	aes-256-sha-sha, aes-192-sha-sha, aes-sha-sha, 3des-sha-sha, des-sha-sha	Manage
	IPsec Proposal:	AES256, AES192, AES, 3DES, DES	Select

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

teps	Security			
1. Introduction	This step lets you sec	ure the selected traffic.		
 Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	Simple Configuration ASA uses the pre-sl ISAKMP security pa when configuring the security pa	ion hared key entered here to authenticate this device rameters for that will allow tunnel establishment. I he remote peer.	with the peer. ASDM will sele t is recommended that this op	ect common IKE ar tion is also selecte
	You can use pre-sh data encryption alg IKE Version	ared key or digital certificate for authentication wit orithms ASDM selected for you. Authentication Methods Encryption Algorithms	h the peer device. You can al	so fine tune the
	You can use pre-sh data encryption alg IKE Version IKE version 1	ared key or digital certificate for authentication wit orithms ASDM selected for you. Authentication Methods Encryption Algorithms	h the peer device. You can al	so fine tune the
	You can use pre-sh data encryption alg IKE Version IKE version 1 IKE Policy:	ared key or digital certificate for authentication wit orithms ASDM selected for you. Authentication Methods Encryption Algorithms pre-share-aes-256-sha	h the peer device. You can al	so fine tune the
	You can use pre-sh data encryption alg IKE Version IKE version 1 IKE Policy: IPsec Proposal:	ared key or digital certificate for authentication wit orithms ASDM selected for you. Authentication Methods Encryption Algorithms pre-share-aes-256-sha ESP-AES-256-SHA	h the peer device. You can al	Manage
	You can use pre-sh data encryption alg IKE Version IKE version 1 IKE Policy: IPsec Proposal: IKE version 2	ared key or digital certificate for authentication wit orithms ASDM selected for you. Authentication Methods Encryption Algorithms pre-share-aes-256-sha ESP-AES-256-SHA	h the peer device. You can al	Manage
	You can use pre-sh data encryption alg IKE Version 1 IKE version 1 IKE Policy: IPsec Proposal: IKE version 2 IKE Policy:	ared key or digital certificate for authentication wit orithms ASDM selected for you. Authentication Methods Encryption Algorithms pre-share-aes-256-sha ESP-AES-256-SHA aes-256-sha-sha	h the peer device. You can al	Manage Manage

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.

C Site-to-site VPN Connectio	on Setup Wizard
Steps	Security
Steps 1. Introduction 2. Peer Device Identificatio 3. Traffic to protect 4. Security 5. NAT Exempt 6. Summary	Security This step lets you secure the selected traffic. Simple Configuration ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKIMP security parameters for that will allow turnel establishment. It is recommended that this option is also selected when configuring the remote peer. Customized Configuration You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you. INE Version Authentication Methods Encryption Algorithms Perfect Forward Secrecy Enable Perfect Forward Secrecy (PFS). If PFS is used, a new Diffie-Hellman exchange is performed for each phase-2 negotiation. It ensures that will allow the future Diffie-Hellman Group:
	<back next=""> Cancel Hel</back>

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**.

Site-to-site VPN Connection	on Setup Wizard
Steps	NAT Exempt
 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	NAT Exempt This step allows you to exempt the local network addresses from network translation. Exempt ASA side host/network from address translation inside
	< Back Next >

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

Branch	Here is the summary of the configuration.			
	Name	Value		
ISP ISP	🗆 Summary			
TORU	Peer Device IP Address	172.16.2.1		
	VPN Access Interface	outside		
	Protected Traffic	Local Network: 10.1.1.0/24 Remote Network: 10.1.2.0/24		
	IKE Version Allowed	IKE version 1 and IKE version 2		
	Authentication Method			
	IKE v1	Use pre-shared key		
	IKE v2	Use pre-shared key when local device access the peer Use pre-share key when peer device access the local device		
	Encryption Policy			
	Perfect Forward Secrecy (PFS)	Disabled		
	IKE v1			
	IKE Policy	pre-share-aes-256-sha		
	IPsec Proposal	ESP-AES-256-SHA		
	□ IKE v2			
	IKE Policy	aes-256-sha-sha		
	IPsec Proposal	AES256, AES192, AES, 3DES, DES		
а.	Network Address Translation	The protected traffic is not subjected to network address translation		

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-12l
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 <u>Output Interpreter Tool</u> 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 outout 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 IKE Peer: 172.16.1.1 1 Role : responder Type : L2L Rekey State : MM_ACTIVE : no 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: 0x0000000 0x000001F 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: 0x0000000 0x0000001

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 : L2L Role Туре : 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:
              0x0000000 0x000001F
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:
              0x0000000 0x0000001
```

Troubleshoot

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

The <u>Output Interpreter Tool</u> 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 <u>vpn-sessiondb logoff tunnel-group <*tunnel-group-name*> command in order to clear IKE and IPsec SAs for a single tunnel.</u>

<#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
2
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
2
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
2
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
1
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
2
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
1
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
2
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
2
Jan 19 22:00:06 [IKEv1]
Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED
```

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
1
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
2
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
5
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
2
```

```
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
    5
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,
                           Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Transmitting Proxy Id:
Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0
    2
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
                         Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
(0) total length : 172
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
 (msqid=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

- <u>Requests for Comments (RFCs)</u>
 <u>Cisco Technical Support & Downloads</u>