Esempio di configurazione da ASA a ASA da dinamica a statica con IKEv1/IPsec

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Esempio di rete **Configurazione ASDM** Central-ASA (peer statico) Remote-ASA (Dynamic Peer) **Configurazione CLI** Configurazione ASA centrale (peer statico) Remote-ASA (Dynamic Peer) Verifica **ASA** centrale **Remote-ASA** Risoluzione dei problemi Remote-ASA (iniziatore) Central-ASA (risponditore) Informazioni correlate

Introduzione

In questo documento viene descritto come abilitare l'appliance ASA (Adaptive Security Appliance) per accettare connessioni VPN IPsec dinamiche da sito a sito da qualsiasi peer dinamico (in questo caso, ASA). Come mostrato nel diagramma reticolare di questo documento, il tunnel IPsec viene stabilito solo quando il tunnel viene avviato dall'estremità remota dell'appliance ASA. L'appliance ASA centrale non può avviare un tunnel VPN a causa della configurazione IPsec dinamica. L'indirizzo IP di Remote-ASA è sconosciuto.

Configurare l'appliance ASA centrale in modo che accetti dinamicamente le connessioni da un indirizzo IP con caratteri jolly (0.0.0/0) e da una chiave precondivisa con caratteri jolly. Remote-ASA viene quindi configurato per crittografare il traffico dalle subnet locali a Central-ASA come specificato dall'elenco degli accessi crittografati. Entrambe le parti eseguono l'esenzione NAT (Network Address Translation) per ignorare NAT per il traffico IPsec.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stato usato il software firewall Cisco ASA (5510 e 5520) versione 9.x e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento</u> <u>di ricerca dei comandi (solo utenti registrati).</u>



Esempio di rete

Configurazione ASDM

Central-ASA (peer statico)

Su un'ASA con indirizzo IP statico, configurare la VPN in modo che accetti connessioni dinamiche da un peer sconosciuto mentre autentica il peer usando una chiave già condivisa IKEv1:

 Scegliere Configurazione > VPN da sito a sito > Avanzate > Mappe crittografiche. La finestra visualizza l'elenco delle voci della mappa crittografica già presenti (se presenti). Poiché l'ASA non sa quale sia l'indirizzo IP del peer, per accettare la connessione, è necessario configurare la mappa dinamica con il set di trasformazioni corrispondente (proposta IPSec). Fare clic su Add.

File View Tools Wizards Window Help						Pype	topic to search	6
🔥 Home 🔏 Configuration 🔗 Monitoring 🔚 Save 🔇	Refresh 😋 Back (🔵 Forward 💡 Help	1					
Site-to-Site VPN Ø 0	Configuration > 5	Re-to-Site VPN > Adv	anced > Crypto Map	1				
Connection Profiles	♦ Add + 🛒 5:00	- 🏦 Delete 🛧 🗲	正面の一へ	Find 🔠 Diagram				
Certificate Management Advanced Tunnel Groups	Type:Priority	Traffic Selection Source	Destination	Service Action	Transform Set (D/Ev1)	3Psec Proposal (IKEv2)	Peer	PPS P
DE Polices								
Prec Proposals (Transform Sets) Prec Prefragmentation Policies								
Certificate to Connection Profile Maps System Options								
ACL Manager								
Convice Setup								
🕄 Frend								
Remote Access VPN	-							
Steto-Ste VRI	Chable Anti-rep	lay window size: 64	•					
Device Banagement					Apply Reset			

2. Nella finestra Crea regola IPSec, dalla scheda Criterio tunnel (mappa crittografica) - Base, selezionare esterno dall'elenco a discesa Interfaccia e dinamico dall'elenco a discesa Tipo di criterio. Nel campo Priorità, assegnare la priorità per questa voce nel caso in cui vi siano più voci in Mappa dinamica. Quindi, fare clic su Select (Seleziona) accanto al campo IKE v1 IPsec Project (Proposta IPSec IKE v1) per selezionare la proposta IPSec.

	Policy (Crypl	to Map) - Basic	Tunnel Po	licy (Crypto Map)	- Advanced Traffic S	election	
Ir	nterface:	outside	•	Policy Type:	dynamic 👻	Priority:	1
I] ا	Psec Proposa	als (Transform	Sets)				
Ik	E v1 IPsec F	roposal:					Select
IK	E v2 IPsec F	roposal:					Select
P	eer Settings	- Optional for	[,] Dynamic Cr	ypto Map Entries			
T	'he Connecti	on Type is app	, licable to sta	tic tunnel policies	only. Uni-directional o	onnection type poli	cies are used
f	or LAN-to-LA	N redundancy	. Tunnel poli	cies of the 'Origin	ate Only' connection ty	ype may specify up	to 10
r	edundant pe	ers.					
	P Address of	Peer to Be Ad	ded:				
I			_ [Add >>		Mov	/e Up
I							
I [
I [Remove		Move	Down

3. Quando viene visualizzata la finestra di dialogo Seleziona proposte IPSec (set di trasformazioni), scegliere una delle proposte IPSec correnti o fare clic su **Aggiungi** per crearne una nuova e utilizzarla allo stesso modo. Al termine, fare clic su **OK**.

	outside 👻	Policy	Type: dynamic 🔻	Priority: 1]
Psec Proposa	als (Transform Sets)				
E v1 IPsec P	roposal: tset			Select	
	-				_
E V2 IPS	Select IPsec Prop	osals (Transfo	rm Sets)		23
	Jelect Ir see riop		in sets,		
	🖨 Add 📝 Edit	Delete			
	- Mod Car	Delete			
	Name	Mode	ESP Encryption	ESP Authentication	
eer Settie	ESP-3DES-SHA	Transport	3DES	SHA	A .
eer Jetti	ESP-3DES-MDS	Transport	3DES	MD5	
he Conne	ESP-DES-SHA	Tunnel	DES	SHA	
or LAN-to	ESP-DES-MDS	Tunnel	DES	MD5	
coundant	ESP-DES-SHA-T	Transport	DES	SHA	
	ESP-DES-MDS-T	Transport	DES	MD5	=
	tset	Tunnel	AES-256	SHA	-
	Assigned IPsec Pro	posals			
P Addres	Assign-> (S	ec			
P Addres					
P Addres					

4. Dalla scheda Tunnel Policy (Crypto Map)-Advanced (Avanzate), selezionare la casella di controllo **Enable NAT-T** (obbligatorio se uno dei peer si trova dietro un dispositivo NAT) e la casella di controllo **Enable Reverse Route Injection**. Quando il tunnel VPN arriva per il peer dinamico, ASA installa un percorso dinamico per la rete VPN remota negoziata che punta all'interfaccia

VPN.

Create IPsec Rule	23
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
C Enable NAT-T	
Enable Reverse Route Injection	
Security Association Lifetime Settings	
Time: 8:0:0 hh:mm:ss	
Traffic Volume: 🔲 unlimited 4608000 KBytes	
Validate incoming ICMP error messages	
Enable Do Not Fragment (DF) policy	
Enable Traffic Flow Confidentiality (TFC) packets, This is unavailable if IKEv1 is enabled,	
OK Cancel Help	

Facoltativamente, nella scheda Selezione traffico è possibile anche definire il traffico VPN interessante per il peer dinamico e fare clic su OK.

Create IPsec	Rule	Σ
Tunnel Policy ((Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
Action: 💿 F	Protect 💿 Do not Protect	
Source Criter	ia	
Source:	any4	
Destination C	Iriteria	
Destination:	any4	
Service:	ip	
Description:		
More Opti	ons	۲
📝 Enable	Rule	
Source Ser	vice: (TCP or UDP service only) 😗	
Time Range	e:	
	OK Cancel Help	

Configuration > Site-	to-Si	te VPN > Advance	<u>d > Crypto Maps</u>			
🖶 Add 🝷 🗹 Edit 🝷	<u>Î</u> De	elete 🛧 🗲 👗	🗈 💼 - Q, Fin	d 融 Diag	ram	
To a set Defending	Traf	ic Selection	Transform Set (IVEu1)			
Type:Priority	#	Source	Destination	Service	Action	Transform Set (IKEVI)
🖃 interface: outside						
dynamic: 65535.1	1	🏟 any4	🌍 any4	IP ip	🖌 Protect	tset
•						
📝 Enable Anti-replay	windov	w size: 64 👻				
					Apply	Reset

Come accennato in precedenza, poiché l'appliance ASA non dispone di informazioni sull'indirizzo IP dinamico remoto del peer, la richiesta di connessione sconosciuta termina in DefaultL2LGroup, che esiste sull'appliance ASA per impostazione predefinita. Affinché l'autenticazione riesca, la chiave già condivisa (cisco123 in questo esempio) configurata sul peer remoto deve corrispondere a quella in DefaultL2LGroup.

 Scegliere Configurazione > VPN da sito a sito > Avanzate > Gruppi di tunnel, selezionare DefaultL2LGroup, fare clic su Modifica e configurare la chiave precondivisa desiderata. Al termine, fare clic su OK.

	Group Policy	IKEv1 Enabled	IKEv2 Enabled
faultL2LGroup	DfltGrpPolicy	₹	
		Edit IPsec Site-to-site Tunnel Group: Default	L2LGroup
		Name: DefaultL2LGroup	
		IPsec Enabling	
		Group Policy Name: DfltGrpPolicy	
		(Following two fields are	attributes of the group policy selected ab
		📝 Enable IKE v1 📃 E	nable IKE v2
		IDsec Settings	
		IKE v1 Settings	
		Authentication	
		Pre-shared Key: ••••••	
		Device Certificate: None	 Manage
		IKE Peer ID Validation: Required	-
		IKE Keepalive	
		 Disable keepalives 	
		Monitor keepalives	
		Confidence Interval: 10 seco	onds

Nota: In questo modo viene creata una chiave già condivisa con caratteri jolly sul peer statico (Central-ASA). Tutti i dispositivi/peer che conoscono questa chiave precondivisa e le relative proposte corrispondenti possono stabilire un tunnel VPN e accedere alle risorse tramite VPN. Assicurarsi che questa chiave non sia condivisa con entità sconosciute e che non sia facile da indovinare.

6. Scegliere Configurazione > VPN da sito a sito > Criteri di gruppo e selezionare i criteri di gruppo desiderati (in questo caso i criteri di gruppo predefiniti). Fare clic su Modifica e modificare i criteri di gruppo nella finestra di dialogo Modifica criteri di gruppo interni. Al termine, fare clic su OK.

	Туре	Tunneling Protocol	Connection Profiles/Users Assigned To
irpPolicy (System Default)	Internal	kev1;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultWEBVPI
	Edit Internal Group Pol	icy: DfltGrpPolicy	2
	Name:	DfltGrpPolicy	
	Tunneling Protocols:	Clientless SSL VPN 📄 SSL VPN Client 🕑 IPser	c IKEv1 🔄 IPsec IKEv2 📝 L2TP/IPsec
	Filter:	None	▼ Manage
	Idle Timeout:	Unlimited 30 minutes	
	Maximum Connect Time:	V Linimited minutes	
	PidAmuni Comico, milo,	• or minored	
	Prevention Competer Inter		
	PROVINGIN CONNECC. HINES		
	PROVINGIN CONNECC. HINES	OK Cancel Help	

 Scegliere Configurazione > Firewall > Regole NAT e nella finestra Aggiungi regola NAT configurare una regola no nat (NAT-FREE) per il traffico VPN. Al termine, fare clic su OK.

Configuration 2	> Firewall > NAT Rules							
🗣 Add 🗸 🗹	🔁 Add NAT Rule	6 4 m 8 m	· · · · · ·	X				
# Match 0	Match Criteria: Original Packet							
" Source Ir	Source Interface:	inside 🔹 👻	Destination Interface:	outside 🔹 👻				
"Network Ot	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	er destination instead of per int	erface					
	Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023							
	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 in	terface						
	Lookup route table to locate eg	ress interface						
	Direction: Both 👻							
		OK Cancel	Help					

Remote-ASA (Dynamic Peer)

1. Scegliere Procedure guidate > Creazioni guidate VPN > Creazione guidata VPN da sito a sito dopo la connessione dell'applicazione ASDM all'ASA

Cisco ASDM 7.1 fo	r ASA - 10	0.105.130.220					
File View Tools	Wizards	Window Help	_	_			
Home 🖧 Conf	Sta	rtup Wizard		Bac	k 👩 Forward 🕴	2 Help	
Device List	VPI	V Wizards	•		Site-to-site VPN W	îzard	
Add Delete	High Availability and Scalability Wizard Unified Communication Wizard				AnyConnect VPN Wizard		
				Clientless		SL VPN Wizard	
Find:	Pac	ket Capture Wizard			IPsec (IKEv1) Remo	te Access VPN Wiz	ard
- 10.105.130.51			Gene	al Lio	ense		
- 🗷 10.105.130.54			Host	Name:	121-peer		
- B 10.105.130.72			ASA	Version	n: 9.1(3)	Device Uptime:	2d 1h 42m 50
B 10.105.100.09			ASD	M Versi	on: 7.1(4)	Device Type:	ASA 5520
2. Fare clic su Nez	xt						

(Avanti).



 Per specificare l'indirizzo IP esterno del peer remoto, selezionare external (esterno) dall'elenco a discesa VPN Access Interface (Interfaccia di accesso VPN). Selezionare l'interfaccia (WAN) a cui applicare la mappa crittografica. Fare clic su Next (Avanti).

Site-to-site VPN Connec	ction Setup Wizard
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
3. Traffic to protect	
4. Security	VPN Access Interface: outside
5. NAT Exempt	
6. Summary	
	<back next=""></back>

4. Specificare gli host/le reti a cui deve essere consentito il passaggio attraverso il tunnel VPN. In questo passaggio, è necessario fornire le reti locali e remote per il tunnel VPN. Fare clic sui pulsanti accanto ai campi Rete locale e Rete remota e scegliere l'indirizzo in base alle esigenze. Al termine, fare clic su

Avanti.

Site-to-site VPN Connection	Setup Wizard	
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 IP Address Type: IPv6 Local Network: 10.1.1.0/24 Remote Network: 10.1.2.0/24	traffic is to be protected using IPsec encryption.
	< Back Next >	[

5. Immettere le informazioni di autenticazione da utilizzare, ovvero la chiave già condivisa in questo esempio. La chiave già condivisa utilizzata in questo esempio è cisco123. Il nome del gruppo di tunnel è l'indirizzo IP peer remoto per impostazione predefinita se si configura una VPN da LAN a LAN

(L2L).	on Setup Wizard
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 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.
	<back next=""> Cancel Help</back>

OÈpossibile personalizzare la configurazione per includere i criteri IKE e IPsec desiderati. Tra i peer deve essere presente almeno un criterio di corrispondenza:Nella scheda Metodi di autenticazione immettere la chiave già condivisa IKE versione 1 nel campo Chiave già condivisa. Nell'esempio, questo valore è **cisco123**.

ps .	Security				
Introduction	This step lets you secure the selected traffic.				
Peer Device Identificatio					
Traffic to protect	Simple Configuration				
Security	ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IXE and ISAKMP security parameters for				
NAT Exempt	chac will allow cunnel escapionment. It is rec	onmended that this option is also selecte	a when coninganini	one remote peer.	
Summary					
	Customized Configuration				
	You can use pre-shared key or digital certifi	cate for authentication with the peer dev	ice. You can also f	ine tune the data encr	yption algorithms ASDM
	selected for you.				
		You want You want			
	IKE Version Authentication Method	Encryption Algorithms Perfect Forw	vard Secrecy		
	IKE version 1	[
	Pre-shared Key:				
	Device Certificate:	None	•	Manage	
	IXE version 2				
	IKE version 2				
	IKE version 2 Local Pre-shared Key: Local Device Certificate:			Manage	
	IKE version 2 Clocal Pre-shared Key: Clocal Device Certificate:	- None	y	Manage	
	IKE version 2 Cocal Pre-shared Key: Local Device Certificate: Remote Peer Pre-shared Key:	None	y	Manage	
	IKE version 2 Cocal Pre-shared Key: Local Device Certificate: Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	None		Manage	
	IKE version 2 Cocal Pre-shared Key: Local Device Certificate: Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	None		Manage	
	IKE version 2 Cocal Pre-shared Key: Local Device Certificate: Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	None		Manage	
	IKE version 2 Cocal Pre-shared Key: Local Device Certificate: Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	None		Manage	
	IKE version 2 Cocal Pre-shared Key: Local Device Certificate: Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	None		Manage	
	IKE version 2 Cocal Pre-shared Key: Local Device Certificate: Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	None		Manage	

Fare clic sulla scheda Algoritmi di crittografia.

6. Fare clic su **Gestisci** accanto al campo Criterio IKE, quindi su **Aggiungi** e configurare un criterio IKE personalizzato (fase 1). Al termine, fare clic su **OK**.

Site-to-site VPN Connection	on Setup Wizard	de Distancia Inde	L			
Steps	Security					
 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	This step lets you see Simple Configurat ASA uses the pre-st that will allow turned Customized Confi You can use pre-sh selected for you. IKE Version 1 DKE version 1 DKE Policy: IPsec Proposal:	ure the selected traffic. ion hared key entered here to authenticate this device with the peer. ASDM will select common IXE and ISAKMP security i establishment. It is recommended that this option is also selected when configuring the remote peer. guration ared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption alg Authentication Methods Encryption Algorithms Perfect Forward Secrecy crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-share-aes-192- ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-MA, ESP-AES-256-M	ASDM will select common IXE and ISAKMP security parameters for 5 when configuring the remote peer. ce. You can also fine tune the data encryption algorithms ASDM ard Secrecy 12-sha, rsa-sig-aes-192-sha, pre-share-aes-192- Manage			
	DE 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			
	< Back Next		ncel Hel;			

7. Fare clic su Select (Seleziona) accanto al campo IPsec Project (Proposta IPSec) e

selezionare la proposta IPSec desiderata. Al termine, fare clic su **Avanti**.



Se lo si desidera, è possibile passare alla scheda Segretezza inoltro perfetta e selezionare la casella di controllo **Attiva segretezza inoltro perfetta (PFS)**. Al termine, fare clic su

Avanti.

Reps	Security
Reps 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 that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer. Image: 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 ASD selected for you. Image: Reversion Authentication Methods Encryption Algorithms Perfect Forward Secrecy Enable Perfect Forward Secrecy (PFS). If PFS is used, a new Diffie-Heliman exchange is performed for each phase-2 negotiation. It ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is compromised if one of the (long-term) private keys is com

8. Per evitare che il traffico del tunnel venga generato dall'avvio di Network Address

Translation, selezionare la casella di controllo **Esenzione host/rete lato ASA dalla conversione degli indirizzi**. Per impostare l'interfaccia in cui è possibile raggiungere la rete locale, selezionare **local o inside** (locale) dall'elenco a discesa. Fare clic su **Next (Avanti).**

teps	NAT Exempt
1. Introduction	This step allows you to exempt the local network addresses from network translation.
 Peer Device Identificatio Traffic to protect 	Exempt ASA side host/network from address translation inside 👻
A. Security	
5. Summary	

9. ASDM visualizza un riepilogo della VPN appena configurata. Verificare e fare clic su **Fine**.

Summary	
Here is the summary of the configuration.	
Name	Value
Summary	
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-256-5HA
□ IKE v2	
IKE Policy	aes-256-sha-sha
IPsec Proposal	AES256, AES192, AES, 3DES, DES
Network Address Translation	The protected traffic is not subjected to network address translation
< Back Finish	Cancel Help

Configurazione CLI

Configurazione ASA centrale (peer statico)

1. Configurare una regola NO-NAT/NAT-EXCEPTION per il traffico VPN come mostrato nell'esempio:

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. Configurare la chiave già condivisa in DefaultL2LGroup per autenticare qualsiasi peer remoto Dynamic-L2L:

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

3. Definire la policy per la fase 2/ISAKMP:

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

- 4. Definire il set di trasformazioni/criterio IPSec per la fase 2:
- crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac 5. Configurare la manna dinamica con i coquenti parametri: Inciente di tra
- 5. Configurare la mappa dinamica con i seguenti parametri: Insieme di trasformazioni richiestoAbilita Reverse Route Injection (RRI), che consente a Security Appliance di ottenere informazioni di routing per i client connessi (facoltativo)

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

 Associare la mappa dinamica alla mappa crittografica, applicare la mappa crittografica e abilitare ISAKMP/IKEv1 sull'interfaccia esterna:

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. Configurare una regola di esenzione NAT per il traffico VPN: 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. Configurare un gruppo di tunnel per un peer VPN statico e una chiave già condivisa.

tunnel-group 172.16.2.1 type ipsec-12l tunnel-group 172.16.2.1 ipsec-attributes ikev1 pre-shared-key cisco123

3. Definizione delle regole PHASE-1/ISAKMP:

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

- 4. Definire un set di trasformazioni/criterio IPSec per la fase 2: crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
- 5. Configurare un elenco degli accessi che definisca il traffico/la rete VPN interessata: access-list outside_cryptomap extended permit ip object 10.1.1.0-inside_network object 10.1.2.0-remote_network
- 6. Configurare la mappa crittografica statica con questi parametri: Access-list VPN/crittograficaIndirizzo IP peer IPsec remotoInsieme di trasformazioni richiesto 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. Applicare la mappa crittografica e abilitare ISAKMP/IKEv1 sull'interfaccia esterna: crypto map outside_map interface outside crypto ikev1 enable outside

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo <u>strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi</u> **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

- show crypto isakmp sa: visualizza tutte le associazioni di sicurezza IKE correnti in un peer.
- show crypto ipsec sa: visualizza tutte le SA IPsec correnti.

In questa sezione viene mostrato un esempio di verifica dei due appliance ASA.

ASA centrale

```
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
   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:
         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:
```

Remote-ASA

```
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
                             State : MM_ACTIVE
          : no
   Rekey
 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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Lo <u>strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi</u> **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Nota: consultare le <u>informazioni importanti sui comandi di debug prima di usare i comandi di</u> debug.

Utilizzare i seguenti comandi come illustrato:

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

Attenzione: Il comando **clear crypto isakmp sa** è intrusivo in quanto cancella tutti i tunnel VPN attivi.

Nel software PIX/ASA versione 8.0(3) e successive, una singola associazione di protezione IKE può essere cancellata usando il comando **clear crypto isakmp sa** *<indirizzo ip peer>*. Nelle versioni software precedenti alla 8.0(3), usare il comando <u>vpn-sessiondb logoff tunnel-group</u> *<tunnel-group-name>* per cancellare le associazioni di sicurezza IKE e IPsec per un singolo tunnel.

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
Debug utilizzati:

debug cry condition peer <remote peer public IP> debug cry ikev1 127 debug cry ipsec 127

Remote-ASA (iniziatore)

Immettere questo comando packet-tracer per avviare il tunnel:

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed
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 (risponditore)

```
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 received172.16.1.1
:
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 0Jan 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 (msqid=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

Informazioni correlate

- <u>Riferimenti per i comandi Cisco ASA serie 1000</u>
- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- <u>RFC (Requests for Comments)</u>
- Documentazione e supporto tecnico Cisco System