SDM Esempio di VPN IPsec da sito a sito tra ASA/PIX e un router IOS

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Prodotti correlati Convenzioni Configurazione Esempio di rete Configurazione ASDM tunnel VPN **Configurazione SDM router** Configurazione ASA CLI **Configurazione CLI router** Verifica ASA/PIX Security Appliance - Comandi show Router IOS remoto - Comandi show Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene fornita una configurazione di esempio per il tunnel IPsec da LAN a LAN (da sito a sito) tra le appliance di sicurezza Cisco (ASA/PIX) e un router Cisco IOS. Le route statiche vengono utilizzate per maggiore semplicità.

Per ulteriori informazioni sullo stesso scenario in cui la <u>configurazione del tunnel IPsec da LAN a</u> <u>LAN di un router IOS</u> esegue la versione software *7.x*, <u>fare riferimento</u> all'<u>esempio di</u> <u>configurazione</u> del<u>tunnel IPsec da PIX/ASA 7.x</u>.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Prima di avviare questa configurazione, è necessario stabilire la connettività IP end-to-end.
- Ènecessario abilitare la licenza di Security Appliance per la crittografia DES (Data Encryption

Standard) (a un livello di crittografia minimo).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Adaptive Security Appliance (ASA) con versione 8.x e successive
- ASDM versione 6.x e successive
- Cisco 1812 router con software Cisco IOS® versione 12.3
- Cisco Security Device Manager (SDM) versione 2.5

Nota: per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'<u>autorizzazione</u> dell'<u>accesso HTTPS per ASDM</u>.

Nota: per consentire al router di essere configurato dal modello SDM, consultare il documento sulla <u>configurazione base</u> del router<u>utilizzando</u> l'SDM.

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.

Nota: per ulteriori informazioni, fare riferimento al documento <u>Configuration Professional: Esempio</u> <u>di VPN IPsec da sito a sito tra ASA/PIX e un router IOS</u> per una configurazione simile<u>con</u> Cisco Configuration Professional sul router.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco PIX serie 500 Security Appliance, con versione 7.x e successive.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Configurazione

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi <u>RFC 1918</u> utilizzati in un ambiente lab.

- <u>Configurazione ASDM tunnel VPN</u>
- <u>Configurazione SDM router</u>
- <u>Configurazione ASA CLI</u>
- <u>Configurazione CLI router</u>

Configurazione ASDM tunnel VPN

Per creare il tunnel VPN, completare i seguenti passaggi:

 Aprire il browser e immettere https://<IP_Address> dell'interfaccia dell'ASA configurata per l'accesso ASDM> per accedere all'ASDM sull'appliance.Accertarsi di autorizzare gli avvisi che il browser visualizza relativi all'autenticità del certificato SSL. Il nome utente e la password predefiniti sono entrambi vuoti.L'appliance ASA visualizza questa finestra per consentire il download dell'applicazione ASDM. In questo esempio l'applicazione viene caricata nel computer locale e non viene eseguita in un'applet Java.



- 2. Per scaricare il programma di installazione dell'applicazione ASDM, fare clic su **Download ASDM Launcher** e su Start ASDM.
- 3. Una volta scaricato l'utilità di avvio ASDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio Cisco ASDM.
- Immettere l'indirizzo IP dell'interfaccia configurata con il comando http -, nonché un nome utente e una password, se specificati. In questo esempio viene usato cisco123 come nome utente e cisco123 come

	Cisco ASDM Launch		
			cisco
	Device IP Address / Name:	10.77.241.111	*
	Username:	cisco123	
	Password:	* * * * * * *	
	📃 Run in Demo Mode		
password.			1 🗳 🔒

5. Eseguire la **Creazione guidata VPN IPsec** quando l'applicazione ASDM si connette all'appliance

A	SA.

🖆 Cisco ASDM 6.	1 for ASA - 10.77.241.111			
File View Tools	Wizards Window Help Lo	ook For:	Go.	ahaha
Home 03 Cor	TPser VPN Wizard	Back D Forward	d 7 Help	CISCO
Home	SSL VPN Wizard High Availability and Scalability Wizard Packet Capture Wizard	ntion Interface Status		
General Licens	e	Interface	IP Address/Mask	Line Li
Host Name: ASA Version: ASDM Version: Firewall Mode: Total Flash:	ciscoasa.default.domain.invalid 8.0(2) Device Uptime: 14d 3h 1m 51s 6.1(3) Device Type: ASA 5510 Routed Context Mode: Single 64 MB Total Memory: 256 MB	dm2 1 inside 1 outside 1 Select an interface to	0.77.241.111/26 0.10.10.1/24 72.16.1.1/24 view input and output	Cup C Cup C Cup C Kbps
VPN Tunnels IKE: 0 IPSec: 0	0 Clientless SSL VPN: 0 SSL VPN Client: 0 Details	Connections Per Sec	cond Usage	
System Resource CPU CPU 100 0% 50	ces Status Usage (percent)	0 20:41 UDP: 0	20:42 20:43 TCP: 0 Total: 0	20:44
	cisco123	15	4	'6/09 8:45:42 PM UTC

6. Scegliere il tipo di tunnel VPN IPsec **da sito a sito** e fare clic su **Avanti** come mostrato di seguito.

🖆 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch Pranch Provide	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
Corporate	VPN Tunnel Type: Site-to-Site VPN
THE PART	Site-to-Site
	Remote Access Remote Access Remote Access
	VPN Tunnel Interface:
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	< Back Next > Finish Cancel Help

7. Specificare l'indirizzo IP esterno del peer remoto. 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 sarà l'indirizzo IP esterno per impostazione predefinita se si configura la VPN L2L. Fare clic su Next (Avanti).

🖆 VPN Wizard	2	ĸ
VPN Wizard	Remote Site Peer (Step 2 of 6)	
Branch	Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel. Peer IP Address: 172.17.1.1 CAuthentication Method	
Home	Pre-shared key	
Corporate	Pre-Shared Key: cisco123	
Num	 Certificate 	
1.4	Certificate Signing Algorithm: rsa-sig	
	Certificate Name:	
T-T-T-TIM	Challenge/response authentication (CRACK)	
	Tunnel Group	
-6	For site-to-site connections with pre-shared key authentication, the tunnel group name must be the same as either the peer IP address or the peer hostname, whichever is used as the peer's identity.	
	Tunnel Group Name: 172.17.1.1	
	< Back Next > Finish Cancel Help	

8. Specificare gli attributi da utilizzare per IKE, noti anche come fase 1. Questi attributi devono essere gli stessi sia sull'ASA che sul router IOS. Fare clic su **Next** (Avanti).

🖆 VPN Wizard		×	
VPN Wizard	IKE Policy (Step 3 of 6)		
Branch Branch ISP Hoeve Corporate	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.		
Network	Encryption: DES		
A A A A A A A A A A A A A A A A A A A	Authentication: SHA		
- THU	DH Group:		
	< Back Next Finish Cancel He	P	

9. Specificare gli attributi da utilizzare per IPsec, noti anche come fase 2. Questi attributi devono corrispondere sia sull'appliance ASA sia sul router IOS. Fare clic su **Next** (Avanti).

🖆 VPN Wizard		×	
VPN Wizard	IPsec Encryption and Authentication (Step 4 of 6)		
Branch Branch File Softwork Network	Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.		
FILE THINK			
	Authentication: SHA		
	< Back Next > Finish Cancel Help		

10. Specificare gli host il cui traffico deve poter passare attraverso il tunnel VPN. In questo passaggio, è necessario fornire le **reti locale** e **remota** per il tunnel VPN. Fare clic sul pulsante accanto a **Reti locali** come mostrato di seguito per scegliere l'indirizzo di rete locale dall'elenco a discesa.

🖆 VPN Wizard		×
VPN Wizard	Hosts and Networks (Step 5 of 6)	
Branch Franch Franch Franch	An IPsec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPsec tunnel.	
	Action: Protect Do not Protect	
Home	Local Networks: any	
Network	Remote Networks: any	
	Exempt ASA side host/network from address translation:	▼
	< Back Next > Finish Cancel Help	

11. Scegliere l'indirizzo **di rete locale**, quindi fare clic su **OK** come mostrato di seguito.

🖆 Browse Local Networks 🛛 🛛 🔀				
🗣 Add 🔹 📝 Edit 🕅				
Filter:				Filter Clear
Name	1 IP Address	Netmask	Description	
⊡ Network Objects	1			
	0.0.0.0	0.0.0.0		
- 📑 dmz-network	10.77.241.64	255.255.255.192		
🔄 🛃 inside-network	10.10.10.0	255.255.255.0		
	rk 172.16.1.0	255.255.255.0		
Selected Local Networks				
Local Networks ->	any			
			0	Cancel

12. Fare clic sul pulsante accanto a **Reti remote** come mostrato di seguito per scegliere l'indirizzo di rete remoto dall'elenco a discesa.

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Branch	An IPsec tunnel protects remote sites. Please ider	data exchanged by selected hosts and networks at the local and htify hosts and networks to be used in the IPsec tunnel.
	Action: (Protect O Do not Protect
Home	Local Networks: i	nside-network/24
Network	Remote Networks: a	iny R
	☑ Exempt ASA side ho	ost/network from address translation:
		< Back Next > Finish Cancel Help

13. Scegliere l'indirizzo di **rete remota**, quindi fare clic su **OK** come mostrato di seguito.**Nota:** se la rete remota non è presente nell'elenco, è necessario aggiungerla all'elenco facendo clic su

Aggiungi.

🖆 Browse Remote Networks 🛛 🛛 🔀				
🗣 Add 🝷 📝 Edit 🍿 Delete 🔍				
Filter:				Filter Clear
Name ^	1 IP Address	Netmask	Description	
Network Objects				
	0.0.0.0	0.0.0		
🔤 dmz-network	10.77.241.64	255.255.255.192		
🚮 inside-network	10.10.10.0	255.255.255.0		
- 🛃 outside-networ	k 172.16.1.0	255.255.255.0		
i 🔂 10.20.10.0	10.20.10.0	255.255.255.0		
Selected Remote Network	s			
Remote Networks ->	any			
				K Cancel

14. Per evitare che il traffico del tunnel venga **convertito** dall'indirizzo di **rete**, selezionare la casella di controllo **Esenzione host/rete lato ASA dalla conversione degli indirizzi**. Fare quindi clic su **Avanti**.

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Brondh	An IPsec tunnel protec remote sites. Please id	ts data exchanged by selected hosts and networks at the local and entify hosts and networks to be used in the IPsec tunnel.
	Action:	Protect O Do not Protect
Home	Local Networks:	inside-network/24
Network	Remote Networks:	10.20.10.0/24
	✓ Exempt ASA side	host/network from address translation:
		< Back Next > Finish Cancel Help

15. In questo riepilogo vengono visualizzati gli attributi definiti dalla Creazione guidata VPN. Verificare la configurazione e fare clic su **Finish** (Fine) quando le impostazioni sono corrette.



Configurazione SDM router

Completare questa procedura per configurare il tunnel VPN da sito a sito sul router Cisco IOS:

 Aprire il browser e immettere https://<Indirizzo_IP dell'interfaccia del router configurata per l'accesso SDM> per accedere al modulo SDM sul router.Accertarsi di autorizzare gli avvisi che il browser visualizza relativi all'autenticità del certificato SSL. Il nome utente e la password predefiniti sono entrambi vuoti.Il router visualizza questa finestra per consentire il download dell'applicazione SDM. In questo esempio l'applicazione viene caricata nel computer locale e non viene eseguita in un'applet



- 2. Il download dell'SDM ha inizio ora. Una volta scaricato l'utilità di avvio SDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio SDM di Cisco.
- 3. Immettere il **Nome utente** e la **Password**, se specificati, e fare clic su **OK**.In questo esempio viene utilizzato **cisco123** come nome utente e **cisco123** come

Authentication Required 🛛 🛛 🔀					
Java ⁻					
Enter login details to access level_15 or view_access on /10.77.241.109:					
User name:	cisco123				
Password:	•••••				
Save this password in your password list					
Cancel					
Authentication	scheme: Basic				

password.

4. Scegliere Configurazione->VPN->da sito a sito VPN e fare clic sul pulsante di opzione

accanto a **Crea VPN da sito a sito** nella home page SDM. Fare quindi clic su **Avvia l'attività selezionata** come illustrato di

seguito:



5. Scegliere **Procedura guidata dettagliata** per procedere con la configurazione:



6. Nella finestra successiva fornire le informazioni sulla connessione VPN negli spazi corrispondenti. Selezionare l'interfaccia del tunnel VPN dall'elenco a discesa. In questo caso, viene scelto FastEthernet0. Nella sezione Identità peer, scegliere Peer con indirizzo IP statico e fornire l'indirizzo IP del peer remoto. Quindi, fornire la chiave già condivisa (cisco123 nell'esempio) nella sezione Authentication (Autenticazione) come mostrato. Fare quindi clic su Avanti.

Site-to-Site VPN Wizard		
VPN Wizard	VPN Connection Information Select the interface for this VPN connection:	FastEthernet0 💌 Details
	Peer Identity Select the type of peer(s) used for this VPN connection: Enter the IP address of the remote peer: Authentication Authentication ensures that each end of the Pre-shared Keys pre-shared key: Re-enter Key: *******	Peer with static IP address 172.16.1.1 VPN connection uses the same secret key. C Digital Certificates
		< Back Next > Finish Cancel Help

7. Fare clic su Add per aggiungere le proposte IKE che specificano l'algoritmo di crittografia, l'algoritmo di autenticazione e il metodo di scambio chiave.

Site-to-Site VPN Wizard					
VPN Wizard IKE Proposals IKE proposals specify the encryption algorithm, authentication is method that is used by this router when negotiating a VPN con- device. For the VPN connection to be established with the remo- device should be configured with at least one of the policies list Click the Add button to add more policies and the Edit buttor				on algorithm and connection with t emote device, the s listed below. putton to edit an e	d key exchange he remote e remote existing policy.
	Priority Encryption	Hash	D-H Group	Authentication	Туре
D	Add Edit				
			< Back Nex	t> Finish C	ancel Help

8. Specificare Algoritmo di crittografia, Algoritmo di autenticazione e il metodo di scambio chiavi, come mostrato di seguito, quindi fare clic su OK. I valori Encryption Algorithm, Authentication Algorithm e il metodo Key Exchange devono corrispondere ai dati forniti nell'appliance

Add IKE Policy	
Configure IKE Policy	
Priority:	Authentication:
1	PRE_SHARE
Encryption:	D-H Group:
DES	▼ group2 ▼
Hash:	Lifetime:
SHA_1	✓ 24 0 0 HH:MM:SS
· · · ·	
9K I	Cancel Help
ASA.	

9. Fare clic su **Next** (Avanti) come mostrato di seguito.

Site-to-Site VPN Wizard						
VPN Wizard IKE Proposals IKE proposals specify the encryption algorithm, authentication algorithm and key method that is used by this router when negotiating a VPN connection with the redevice. For the VPN connection to be established with the remote device, the rendevice should be configured with at least one of the policies listed below. Click the Add button to add more policies and the Edit button to edit an exist					d key exchange he remote e remote existing policy.	
	Priori	y Encryption	Hash	D-H Group	Authentication	Туре
	1	3DES	SHA_1	group2	PRE_SHARE	User Defined
	2	DES	SHA_1	group1	PRE_SHARE	User Defined
	Add	Edit				
				« Back Next	t> Finish (Cancel Help

10. In questa nuova finestra devono essere forniti i dettagli Set di trasformazioni. Il set di trasformazioni specifica gli algoritmi di crittografia e autenticazione utilizzati per proteggere i dati nel tunnel VPN. Quindi, fare clic su Add (Aggiungi) per specificare i dettagli. È possibile aggiungere qualsiasi numero di set di trasformazioni in base alle esigenze facendo clic su Aggiungi e fornendo i dettagli.

Site-to-Site VPN Wizard		\mathbf{X}
VPN Wizard	Transform Set A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below. Click the Add button to add a new transform set and the Edit button to edit the specified transform set. Select Transform Set Default Transform Set Details of the specified transform set	
	Details of the specified transform set Name ESP Encryption ESP Integrity AH Integrity ESP-3DES-SHA ESP_3DES ESP_SHA_HMAC	
	Ada Edit Back Next > Finish Cancel Hels	p

11. Specificare i dettagli del **set di trasformazioni** (**algoritmo di crittografia e autenticazione**) e fare clic su **OK** come

	Add Transform Set	×
	Name: ASA-IPSEC	
	✓ Data integrity with encryption (ESP)	-
	Integrity Algorithm: ESP_SHA_HMAC 💌	
	Encryption Algorithm: ESP_DES	
	Show Advanced >	>
mostrato	OK Cancel Help	

12. Selezionate il **set di trasformazioni** richiesto da utilizzare dall'elenco a discesa come mostrato.

Site-to-Site VPN Wizard		×
VPN Wizard	Transform Set A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below. Click the Add button to add a new transform set and the Edit button to edit the specified transform set. Select Transform Set SDM Default Transform Set BDM Default Transform Set	
	Add	
	< Back Next > Finish Cancel Hel	р

13. Fare clic su **Next** (Avanti).

Site-to-Site VPN Wizard					×
VPN Wizard	Transform Set A transform set specifies the data in the VPN tunnel. Since communicate, the remote der one selected below. Click the Add button to add a transform set. Select Transform Set ASA IPSEC Details of the specified tra	encryption and aut the two devices mo vice must be config a new transform se mesform set	hentication algorithm ust use the same alg ured with the same t and the Edit butto	ns used to protect the gorithms to transform set as the on to edit the specified	1
	Details of the specified tra Name ASA-IPSEC Image: Astronomy of the specified transmission of the specified transmiss	Insform set	ESP Integrity ESP_SHA_HMAC	AH Integrity	
		< [Back Next > Fini	sh Cancel He	lp

14. Nella finestra seguente vengono forniti i dettagli sul **traffico da proteggere** tramite il tunnel VPN. Specificare le **reti di origine e di destinazione** del traffico da proteggere in modo che il traffico tra le reti di origine e di destinazione specificate sia protetto. Nell'esempio, la rete di origine è 10.20.10.0 e la rete di destinazione è 10.10.10.0. Quindi, fare clic su **Avanti**.

Site-to-Site VPN Wizard		
VPN Wizard	Traffic to protect IPSec rules define the traffic, such as file transfi protected by this VPN connection. Other data tra device. You can protect all traffic between a part specify an IPSec rule that defines the traffic type Protect all traffic between the following subne Local Network Enter the IP address and subnet mask of the network where IPSec traffic principales	ers (FTP) and e-mail (SMTP) that will be affic will be sent unprotected to the remote ticular source and destination subnet, or is to be protected. ts Remote Network Enter the IP Address and Subnet Mask of the destination Network
	The network where IPSec traffic originates. IP Address: 10.20.10.0 Subnet Mask: 255.255.255.0 or 24	the destination Network. IP Address: 10.10.10.0 Subnet Mask: 255.255.255.0 or 24
		Back Next > Finish Cancel Help

15. In questa finestra viene visualizzato il riepilogo della configurazione della VPN da sito a sito eseguita. Selezionare la casella di controllo **Test connettività VPN dopo la configurazione** se si desidera verificare la connettività VPN. In questo caso, la casella è selezionata in quanto è necessario selezionare la connettività. Fare quindi clic su **Fine**.

Site-to-Site VPN Wizard				
VPN Wizard	Summary of the Configurat	tion		
	Click Finish to deliver the co Interface:FastEthernet0 Peer Device:172.16.1.1 Authentication Type : Pre-s pre-shared key:****** IKE Policies: Hash DH Group SHA_1 group1 SHA_1 group1 SHA_1 group2 Transform Sets: Name:ASA-IPSEC	onfiguration to the router. hared key Authentication PRE_SHARE PRE_SHARE	Encryption DES 3DES	
	ESP Encryption:ES ESP Integrity:ESP Mode:TUNNEL	BP_DES _SHA_HMAC er configuring.]		>
		< Back Next	Finish C	ancel Help

16. Fare clic su **Start** come mostrato per controllare la connettività VPN.

VPN Troubleshooting	N 100 100 100 100 100 100 100 100 100 10
Tunnel Details	
Interface: FastEthernet0 Peer:	172.16.1.1
	_
	🔲 Summary 🛛 🕅 Details
Activity	Status
Failure Reason(s) Recomme	ended Action(s)
Start Save Report C	lose Help

17. Nella finestra successiva viene fornito il risultato del test di connettività VPN. Qui potete vedere se il tunnel è Su o Giù. In questa configurazione di esempio, il tunnel è attivo, come mostrato in

verde.

VPN Troubleshooting		
Tunnel Details		
Interface: FastEthernet0	Peer: 172.16.1.1	
1		
	🔲 Summary	🕰 Details
Activity		Status
Checking the tunnel status		⊖Up
Failure Reason(s)	Recommended Action(s)	
Start Corp Banait	Close	Holp
Start Save Report		Help

La configurazione sul router Cisco IOS è stata completata.

Configurazione ASA CLI

ASA
ASA#show run
: Saved
ASA Version 8.0(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
<i>! Configure the outside interface. !</i> interface
Ethernet0/1 nameif outside security-level 0 ip address
172.16.1.1 255.255.255.0 ! Configure the inside
<i>interface. !</i> interface Ethernet0/2 nameif inside
security-level 100 ip address 10.10.10.1 255.255.255.0
<pre>! Output suppressed ! passwd 2KFQnbNIdI.2KYOU</pre>

encrypted ftp mode passive dns server-group DefaultDNS domain-name default.domain.invalid access-list 100 extended permit ip any any access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0 10.20.10.0 255.255.255.0 !--- This access list (inside_nat0_outbound) is used !--- with the **nat zero** command. This prevents traffic which !--- matches the access list from undergoing network address translation (NAT). !--- The traffic specified by this ACL is traffic that is to be encrypted and !--sent across the VPN tunnel. This ACL is intentionally !--- the same as (outside_1_cryptomap). !--- Two separate access lists should always be used in this configuration. access-list outside_1_cryptomap extended permit ip 10.10.10.0 255.255.255.0 10.20.10.0 255.255.255.0 !--- This access list (outside_cryptomap) is used !--with the crypto map **outside_map** !--- to determine which traffic should be encrypted and sent !--- across the tunnel. !--- This ACL is intentionally the same as (inside_nat0_outbound). !--- Two separate access lists should always be used in this configuration. pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm-613.bin asdm history enable arp timeout 14400 global (outside) 1 interface nat (inside) 1 10.10.10.0 255.255.255.0 nat (inside) 0 access-list inside_nat0_outbound !--- NAT 0 prevents NAT for networks specified in !--the ACL inside_nat0_outbound. access-group 100 in interface outside route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute http server enable http 0.0.0.0 0.0.0.0 dmz no snmp-server location no snmp-server contact !--- PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac !--- Define the transform set for Phase 2. crypto map outside_map 1 match address outside_1_cryptomap !--- Define which traffic should be sent to the IPsec peer. crypto map outside_map 1 set peer 172.17.1.1 !--- Sets the IPsec peer crypto map outside_map 1 set



Configurazione CLI router

Router
Building configuration
Current configuration : 2403 bytes
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname R3
!

boot-start-marker boot-end-marker no logging buffered 1 username ciscol23 privilege 15 password 7 1511021F07257A767B no aaa new-model ip subnet-zero 1 ! ip cef ip ips po max-events 100 no ftp-server write-enable !--- Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are used during an IKE negotiation. Encryption and Policy details are hidden as the default values are chosen. crypto isakmp policy 2 authentication pre-share !--- Specifies the pre-shared key "cisco123" which should !--- be identical at both peers. This is a global !--- configuration mode command. crypto isakmp key cisco123 address 172.16.1.1 !--- Configuration for IPsec policies. !--- Enables the crypto transform configuration mode, !--- where you can specify the transform sets that are used !--- during an IPsec negotiation. crypto ipsec transform-set ASA-IPSEC esp-des esp-sha-hmac 1 !--- !--- Indicates that IKE is used to establish !--the IPsec Security Association for protecting the !--traffic specified by this crypto map entry. crypto map SDM_CMAP_1 1 ipsec-isakmp description Tunnel to172.16.1.1 !--- !--- Sets the IP address of the remote end. set peer 172.16.1.1 !--- !--- Configures IPsec to use the transform-set !---"ASA-IPSEC" defined earlier in this configuration. set transform-set ASA-IPSEC !--- !--- Specifies the interesting traffic to be encrypted. match address 100 1 1 !--- Configures the interface to use the !--- crypto map "SDM_CMAP_1" for IPsec. interface FastEthernet0 ip address 172.17.1.1 255.255.255.0 duplex auto speed auto crypto map SDM_CMAP_1 1 interface FastEthernet1 ip address 10.20.10.2 255.255.255.0

```
duplex auto
 speed auto
interface FastEthernet2
no ip address
!
interface Vlan1
ip address 10.77.241.109 255.255.255.192
1
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
1
ip nat inside source route-map nonat interface
FastEthernet0 overload
ip http server
ip http authentication local
ip http secure-server
!
!--- Configure the access-lists and map them to the
Crypto map configured. access-list 100 remark SDM_ACL
Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!--- This ACL 110 identifies the traffic flows using
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
match ip address 110
1
control-plane
!
1
line con 0
login local
line aux 0
line vty 0 4
privilege level 15
login local
transport input telnet ssh
1
end
```

Verifica

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

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

- PIX Security Appliance Comandi show
- Router IOS remoto Comandi show

ASA/PIX Security Appliance - Comandi show

• show crypto isakmp sa: visualizza tutte le associazioni di protezione IKE correnti in un peer.

```
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: 172.17.1.1
     Type : L2L
                               Role
                                      : initiator
     Rekey
             : no
                               State : MM_ACTIVE

    show crypto ipsec sa: visualizza tutte le SA IPsec correnti in un peer.

 ASA#show crypto ipsec sa
 interface: outside
     Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1
       local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
       remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
       current_peer: 172.17.1.1
      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
       #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0
       #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
       #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.1.1
       path mtu 1500, ipsec overhead 58, media mtu 1500
       current outbound spi: 434C4A7F
     inbound esp sas:
       spi: 0xB7C1948E (3082917006)
          transform: esp-des esp-sha-hmac none
          in use settings ={L2L, Tunnel, PFS Group 2, }
          slot: 0, conn_id: 12288, crypto-map: outside_map
          sa timing: remaining key lifetime (kB/sec): (4274999/3588)
          IV size: 8 bytes
          replay detection support: Y
     outbound esp sas:
       spi: 0x434C4A7F (1129073279)
          transform: esp-des esp-sha-hmac none
          in use settings ={L2L, Tunnel, PFS Group 2, }
          slot: 0, conn_id: 12288, crypto-map: outside_map
          sa timing: remaining key lifetime (kB/sec): (4274999/3588)
          IV size: 8 bytes
          replay detection support: Y
```

Router IOS remoto - Comandi show

• **show crypto isakmp sa**: visualizza tutte le associazioni di protezione IKE correnti in un peer. Router#show crypto isakmp sa

dst	src	state	conn-id slot	status
172.17.1.1	172.16.1.1	QM_IDLE	3 0	ACTIVE

show crypto ipsec sa: visualizza tutte le SA IPsec correnti in un peer.

```
Router#show crypto ipsec sa
interface: FastEthernet0
   Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1
  protected vrf: (none)
  local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  current peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)
     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
     outbound ah sas:
```

outbound pcp sas:

 show crypto engine connections active: visualizza le connessioni correnti e le informazioni sui pacchetti crittografati e decrittografati (solo router).
 Router#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
3	FastEthernet0	172.17.1.1	set	HMAC_SHA+DES_56_CB	0	0
2001	FastEthernet0	172.17.1.1	set	DES+SHA	0	59
2002	FastEthernet0	172.17.1.1	set	DES+SHA	59	0

Risoluzione dei problemi

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

configurazione.

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

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> e sulla <u>risoluzione dei problemi di</u> <u>sicurezza IP - Comprensione e uso dei comandi di debug</u> prima di usare i comandi di **debug**.

- debug crypto ipsec 7: visualizza le negoziazioni IPsec della fase 2.debug crypto isakmp 7: visualizza le negoziazioni ISAKMP della fase 1.
- debug crypto ipsec: visualizza le negoziazioni IPsec della fase 2.debug crypto isakmp: visualizza le negoziazioni ISAKMP della fase 1.

Per ulteriori informazioni sulla risoluzione dei problemi relativi alla VPN da sito a sito, fare riferimento alle <u>soluzioni di risoluzione dei problemi più comuni per VPN IPSec da sito a sito e da</u> <u>accesso remoto</u>.

Informazioni correlate

- <u>Software Cisco PIX Firewall</u>
- <u>Cisco Adaptive Security Device Manager</u>
- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- Configuration Professional: Esempio di VPN IPsec da sito a sito tra ASA/PIX e una configurazione di router IOS
- <u>Riferimenti per i comandi di Cisco Secure PIX Firewall</u>
- <u>Cisco Router e Security Device Manager</u>
- <u>RFC (Requests for Comments)</u>
- Documentazione e supporto tecnico Cisco Systems