ASA/PIX: Esempio di indirizzamento IP statico per client VPN IPSec con CLI e ASDM

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Prodotti correlati Convenzioni Configurazione Esempio di rete Configurare la VPN di accesso remoto (IPSec) Configurazione di ASA/PIX con CLI Configurazione client VPN Cisco Verifica Comandi show Risoluzione dei problemi Cancella associazioni di protezione Comandi per la risoluzione dei problemi Informazioni correlate

Introduzione

Questo documento descrive come configurare Cisco serie 5500 Adaptive Security Appliance (ASA) per fornire l'indirizzo IP statico al client VPN con Adaptive Security Device Manager (ASDM) o CLI. ASDM offre funzionalità di monitoraggio e gestione della sicurezza di altissimo livello attraverso un'interfaccia di gestione intuitiva e basata su Web. Una volta completata la configurazione di Cisco ASA, è possibile verificarla con il client VPN Cisco.

Per configurare la connessione VPN di accesso remoto tra un client VPN Cisco (4.x per Windows) e l'appliance di sicurezza PIX serie 500 7.x, fare riferimento agli <u>esempi di configurazione</u> dell'autenticazione PIX/ASA 7.x e Cisco VPN Client 4.x con Windows 2003 RADIUS (con Active <u>Directory</u>). L'utente client VPN remoto esegue l'autenticazione in Active Directory con un server RADIUS Microsoft Windows 2003 Internet Authentication Service (IAS).

Per configurare una connessione VPN di accesso remoto tra un client VPN Cisco (4.x per Windows) e l'appliance di sicurezza PIX serie 500 7.x con un Cisco Secure Access Control Server (ACS versione 3.2) per l'autenticazione estesa (Xauth), fare riferimento agli <u>esempi di configurazione</u> di <u>PIX/ASA 7.x e Cisco VPN Client 4.x per l'autenticazione ACS sicura (Cisco).</u>

Prerequisiti

Requisiti

In questo documento si presume che l'ASA sia completamente operativa e configurata per consentire a Cisco ASDM o CLI di apportare modifiche alla configurazione.

Nota: per ulteriori informazioni, fare riferimento al documento sull'<u>autorizzazione dell'accesso</u> <u>HTTPS per ASDM</u> o <u>PIX/ASA 7.x: Esempio di configurazione dell'interfaccia interna ed esterna</u> per consentire la configurazione remota del dispositivo da parte di ASDM o Secure Shell (SSH).

Componenti usati

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

- Software Cisco Adaptive Security Appliance versione 7.x e successive
- Adaptive Security Device Manager versione 5.x e successive
- Cisco VPN Client versione 4.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.

Prodotti correlati

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

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

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

Esempio di rete

Nel documento viene usata questa impostazione di rete:



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

Configurare la VPN di accesso remoto (IPSec)

Procedura ASDM

Per configurare la VPN di accesso remoto, completare i seguenti passaggi:

1. Per creare un criterio ISAKMP, scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Criteri IKE > Aggiungi

Aggiungi.			
🚰 Cisco ASDM 6.1 for ASA	- 10.77.241.11		
File View Tools Wizards W	/indow Help		
Home 🚱 Configuration 📝	Monitoring 🔚 Sa	ve 🔇 Refresh 🔇 Back 🚫 Forwa	rd 🦻 Help
Remote Access	Configuration >	Remote Access VPN > Network (C	lient) Access > Advance
Network (Client) Access AnyConnect Connection IPsec Connection Profile	Configure species	fic Internet Key Exchange (IKE) algorithr t 📋 Delete	ns and parameters, within t
Group Policies	Priority #	Encryption	Hash
Address Assignment			
용~ 🙀 Endpoint Security 용~ 🏨 SSL VPN			
IPsec Copto Maps KE Policies KE Parameters IPsec Transform = IPsec Prefragms			
. Fornire i dettagli del criterio)		

ISAKMP.

🗲 Add IKE Polic	ey.			
Priority:	2	Authentication:	pre-share 🗸	
Encryption:	des 💌	D-H Group:	2 🗸	
Hash:	sha 👻	Lifetime:	Unlimited86400	seconds 💌
Cancel Help				

Fare clic su OK e su Applica.

3. Scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Parametri IKE per abilitare IKE sull'interfaccia

esterna.	
🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111	
File View Tools Wizards Window Help	
🚯 Home 🖓 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help	
Remote Access d P × Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Paramete	r)
Introduction Enable IKE NAT Transparency	
AnyConnect Connection	
Pisec Connection Profile Pisec enabled Enable Enable UKT Keenables 20 and	
-De Dynamic Access Policie Inside No. Disable Disable	
Address Assignment Outside Yes Enable IPsec over TCP	
E-B Advanced Enter up to 10 comma-separated TCP port	
Gat Endpoint Security values (1* 65535):	
B IB IBear	
Hit Crysto Maps	
- KE Policies	
Identity to Be Sent to Peer	
Prec Prefragme	
Certificate to Co	
Jerona Software	
Section Options	
ACL Manager	
Clambers SSL VPN Access Alert peers before disconnecting	
AAAALocal Users	
Contificate Manager	

 Scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Set trasformazioni IPSec > Aggiungi per creare il set di trasformazioni ESP-DES-SHA, come mostrato.

G Add Transform Set				
Set Name:	ESP-DES-SHA			
Properties]	
Mode:	💿 Tunnel	🔿 Tr	ansport	
ESP Encryption	ו:	DES	~	
ESP Authentic	ation:	SHA	~	
Qt	Ca		Help	
	2			Fare cli

su OK e su Applica.

5. Scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Avanzate > IPSec > Mappe crittografiche > Aggiungi per creare una mappa crittografica con criterio dinamico di priorità 1, come mostrato.

🖆 Create IPsec Rule	×
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
Interface: outside 💙 Policy Type: dynamic 💙	Priority: 1
Transform Sets Transform Set to Be Added: ESP-DES-MD5 Remove	Move Up Move Down
Peer Settings - Optional for Dynamic Crypto Map Entries The Connection Type is applicable to static tunnel policies only. Uni-directional connecti for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may redundant peers.	on type policies are used y specify up to 10
OK Cancel Help	

Fare clic su **OK** e su **Applica**.

 Scegliere Configurazione > VPN ad accesso remoto > Configurazione AAA > Utenti locali > Aggiungi per creare l'account utente (ad esempio, nome utente - cisco123 e password cisco123) per l'accesso ai client VPN.

🖆 Add User Account						
Identity						
	Username:	cisco123				
	Password:	******				
	Confirm Password:	*****				
	User authentica	ated using MSCHAP				
	Access Restriction					
	Select one of the	options below to restrict ASDM, SSH, Telnet and Console acco	ess.			
	Note: All users have network access, regardless of these settings.					
	 Full access(ASDM, SSH, Telnet and Console) 					
	Privilege lev	vel is used with command authorization.				
	Privilege Le	evel: 2				
	🚫 CLI login pron	mpt for SSH, Telnet and console (no ASDM access)				
	This setting	g is effective only if AAA authenticate console command is con	ifigured.			
	🔘 No ASDM, SSI	iH, Telnet or Console access				
	This setting	g is effective only if AAA authenticate console command is con	ifigured.			
Find:		Next Previous				
	(OK Cancel Help				

7. Andare a **VPN Policy** (Policy VPN) e aggiungere l'**indirizzo IP statico/dedicato** per l'utente "cisco123", come indicato di

seguito.						
🖆 Cisco ASDA 6.1 for ASA	- 10.77	.241.111				
File View Tools Wizards W	vindow H	+ep				
🔄 Home 🚱 Configuration 🔯) Monitorin	ig 🔚 Save 💽 Refrest	Back 🔘 Forward 🦻 Help			
Remote Access a # ×	Config	uration > Remote Acce	ss VPN > AAA/Local Users > Local	Users.		
⊢ y Introduction ⊨ Network (Client) Access	Cre	🚰 Add User Accou	int			
AnyConnect Connection P Psec Connection Profiles	Con	dentity	Check an Inherit checkbox to let th	ne correspond	ing setting take its value	from the
Dynamic Access Policies	AAA	C MAKINGUN	Group Policy:	🔽 Inherit		
Assignment Policy	Us	6	Tunneling Protocols:	🗹 Inherit	Clientless SSL VPN	SSL
GI- Advanced Clientless SSL VPN Access			Filter:	🗹 Inherit		
AAA/Local Users			Tunnel Group Lock:	🗹 Inherit		
LDAP Attribute Map			Store Password on Client System:	🖌 Inherit	O Yes O No	
- A Secure Desktop Manager			Connection Settings			
E- Certificate Management			Access Hours:	🗹 înherit		
			Simultaneous Logins:	🗹 Inherit		
- Advanced			Maximum Connect Time:	🖌 Inherit	Unlimited	Minute
			Idle Timeout:	🗹 înherit	Unlimited	Minute
			Dedicated IP Address (Optional)			
			IP Address: 192.168.5.1	Subnet Mask	:: 255.255.255.0	
			· · · · · · · · · · · · · · · · · · ·			/

8. Scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) >

Assegnazione indirizzi > Pool di indirizzi e fare clic su Aggiungi per aggiungere il client VPN per gli utenti client

VPN.

🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111					
File View Tools Wizards W	Indow Help				
🔥 Home 🕞 Configuration 📴	Monitoring 🔚 Save 🔇 Refresh 🔇 Back 💭 Forward 🦻 Help				
Remote Access B P ×	Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools				
Network (Client) Access	Configure named IP Address pools.				
AnyConnect Connection Pr	This parameter is enforced in either a VPN IPsec Connection Profiles, AnyConnect Connection Profiles or Group Policie				
IPsec Connection Profiles	🖉 Add IP Pool				
- Dynamic Access Policies	Add Edit Delete				
🖙 🏭 Address Assignment	Pool Name Star				
- M Accignment Policy					
B-B Advanced	Name: vpnclient1				
Clientless SSL VPN Access					
- AAA/Local Users	Starting IP Addre 192.168.5.10				
Certificate Management	Ending ID Addresses 192 168 5 100				
- 🐯 Language Localization	Biding in Address. 192-100-0-100				
- M Load Balancing	Subnet Mask: 255/255/255/0				
- 💀 Advanced					
	OK Cancel Help				

 Scegliere Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione IPSec > Aggiungi per aggiungere un gruppo di tunnel (ad esempio, TunnelGroup1 e la chiave già condivisa cisco123), come

mostrato.

110311410.						
File View Tools Wizards Window He	þ		Look For:			
🚳 Home 🦓 Configuration 😰 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🕥 Forward 🦻 Help						
Remote Access VPN P P Introduction Network (Client) Access Network (Client) Access AnyConnect Connection Profiles Network (Client) Access Network (Client) Access	Configuration > Remote Acce Access Interfaces Enable interfaces for IPsec ac	ase VPN > Network (Client) Ar	ccess > IPsec Connection Profi	109.		
IPsec Connection Profiles	Interface	Alow A	ccess			
Group Policies	outside	<u>v</u>				
- Dynamic Access Policies	dmz					
Address Assignment	inside					
P-15 Clientless SSL VPN Access						
🕀 🚽 AAA/Local Users						
🕀 👸 Secure Desktop Manager						
😥 🚰 Certificate Management	Connection Profiles					
	Connection profile (tunnel gro	up) specifies how user is authent	icated and other parameters.			
DHCP Server	🗢 Add 🔀 Edit 🏢 De	lete				
H-R Advanced	Name	IPsec Enabled	L2TP/IPsec Enabled	Autentication		
	DefaultWEBVPNGroup			LOCAL		
	DefaultRAGroup	A	Y	LOCAL		
Remote Access VPN						
Ste-to-Site VPN						
195						
Device Management						
»			Apply Reset			

Nella scheda **Base**, scegliere il gruppo di server come **LOCALE** per il campo Autenticazione utente.Selezionare **vpnclient1** come pool di indirizzi client per gli utenti VPN Client.

🐔 Home 🥵 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🕥 Forward 🧳 Help				
Remote Access 🗗 🔍 🗵	Configuration > Rem	ote Access VPN > Net	work (Client) Access > IPsec Connection Pro	ofiles
	· · · · · · · · · · · · · · · · · · ·			
Network (Client) Access	🌃 Add IPsec Remote	Access Connection	n Profile	
Psec Connection Profile	r-Basic	Name:	TunnelGroup1	
Group Policies	Advanced			
Dynamic Access Policies		IKE Peer Authentication		
B-Sp Address Assignment				
Address Pools		Pre-shared Key:	*****	
Address Pools		Identity Contification	Aleen	Managar
Clientiess SSI VPN Access		toendry Certificate:	None	manage
AAA/Local Users		11		
- AAA Server Groups		User Authentication		
		Server Group:	LOCAL	Manage
- 🕼 Local Users				9/8/88226/0
🗜 🚮 Secure Desktop Manager		Fallback:	Use LOCAL if Server Group fails	
- Certificate Management				
Englage Localization		Client Address Assignme	ent	
- St Load Balancing		DHCP Servers:		
B DHCP Server				000000000000000000000000000000000000000
Advanced		Client Address Pools	vpnclient1	Select.
o Bo Movanced				
		Default Group Policy —		
		Group Policy:	DfltGrpPolicy Y	Manage
			(Following fields are attributed of the group policy	selected a
			Lenable (Psec protocol	
			Enable L2TP over IPsec protocol	

Fare clic su OK.

 Scegliere Avanzate > Indirizzamento client e selezionare la casella di controllo Usa pool di indirizzi per assegnare l'indirizzo IP ai client VPN.Nota: deselezionare le caselle di controllo Usa server di autenticazione e Usa DHCP.

🚰 Add IPsec Remote /	Access Connection Profile
Advanced General Authentication Authorization Accounting IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Global Client Address Assignment Policy This policy affects all Network (Client) Access connections. The following are tried in order until an address is found. Use authentication server Use DHCP ✓ Use address pool Interface-Specific Address Pools ▲ Add Edit Delete Interface Address Pools
Find:	💿 Next 💿 Previous
	OK Cancel Help

Fare clic su OK.

11. Attivare l'interfaccia **esterna** per l'accesso IPSec. Fare clic su **Apply** (Applica) per continuare.

🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111						
File View Tools Wizards Wi	File View Tools Wizards Window Help					
Home 😪 Configuration 📝	Monitoring 🔚 Save 🔇 Refresh 🔇 Ba	ck 🚫 Forward 🛛 🦓 Help				
Remote Access B A × Introduction Network (Client) Access AnyConnect Connection Profiles Group Policies Address Assignment Address Policy Address Pools Address Pools Address SSL VPN Access Address SSL VPN Access AAA/Local Users AAA/Local Users AAA/Local Users AAA/Local Users Certificate Management Certificate Management Local Balancing DHCP Server NS Advanced	Configuration > Remote Access VPN > Access Interfaces Enable interfaces for IPsec access. Interface Allow outside anz dmz inside Connection Profiles connection profile (tunnel group) specifies	Network (Client) Access > IPsec Conne Access Access P P P P P P P P P P P P P P P P P P				

Configurazione di ASA/PIX con CLI

Completare questa procedura per configurare il server DHCP in modo che fornisca indirizzi IP ai client VPN dalla riga di comando. Per ulteriori informazioni su ciascun comando usato, consultare il documento sulla <u>configurazione delle VPN di accesso remoto</u> o sulla <u>guida di riferimento dei</u> <u>comandi di Cisco ASA serie 5500 Adaptive Security Appliance</u>.

--- Specify the location of the ASDM image for ASA to fetch the image for ASDM access. asdm image disk0:/asdm-613.bin no asdm history enable arp timeout 14400 global (outside) 1 192.168.1.5 nat (inside) 0 access-list 101 nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policyrecord DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto dynamic-map outside_dyn_map 1 set transform-set ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp dynamic outside_dyn_map !--- Specifies the interface to be used with !--- the settings defined in this configuration. crypto map outside_map interface outside !--- PHASE 1 CONFIGURATION ---! !--- This configuration uses ISAKMP policy 2. !---The configuration commands here define the Phase !--- 1 policy parameters that are used. crypto isakmp enable outside crypto isakmp policy 2 authentication pre-share encryption des hash sha group 2 lifetime 86400 no crypto isakmp nat-traversal !--- Specifies that the IP address to the vpn clients are assigned by the local and not by AAA or dhcp. The CLI vpn-addr-assign local for VPN address assignment through ASA is hidden in the CLI provided by show run command. no vpn-addr-assign aaa no vpn-addr-assign dhcp telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list 1 class-map inspection_default match default-inspection-traffic 1 policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip

```
inspect xdmcp
service-policy global_policy global
1
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal
!--- In order to identify remote access users to the
Security Appliance, !--- you can also configure
usernames and passwords on the device. !--- specify the
IP address to assign to a particular user, use the vpn-
framed-ip-address command !--- in username mode
username cisco123 password ffIRPGpDSOJh9YLq encrypted
username cisco123 attributes
 vpn-framed-ip-address 192.168.5.1 255.255.255.0
!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

Configurazione client VPN Cisco

Provare a connettersi all'appliance Cisco ASA con il client VPN Cisco per verificare che l'appliance ASA sia configurata correttamente.

- 1. Scegliere Start > Programmi > Cisco Systems VPN Client > VPN Client.
- 2. Fare clic su Nuovo per avviare la finestra Crea nuova voce di connessione

🥔 status: Dis	сопп	ected VP	N Clie	nt - Ver	sion 5.0.03.0530	
Connection Entri	ies Sl	tatus Certific	ates l	og Optio	ns Help	
Connect	ter Nev	v Impo	a) nt	Modify) Delete	
Connection Entr	ies	Certificates	Log			
Con	nectio	n Entry 🛛 🖄			Host	

VPN.

 Specificare i dettagli della nuova connessione.Immettere il nome della voce di connessione insieme a una descrizione. Immettere l'indirizzo IP esterno dell'appliance ASA nella casella Host. Quindi, immettere il nome del gruppo di tunnel VPN (TunnelGroup1) e la password (Chiave già condivisa - cisco123) come configurato nell'ASA. Fare clic su

VPN Client	Create New VPN Connect	ion Entry	X			
Connection Entry:	ASA					
Description:		alialia				
Host:		cisco				
Authentication	Transport Backup Servers	Dial-Up				
Group Auther	ntication	Mutual Group /	Authentication			
Name:	TunnelGroup1					
Password:	*****					
Confirm Password: ******						
C Certificate Au Name:	thentication Pertificate Chain					
Erase User Passw	vord	Save	Cancel			

Salva.

4. Fare clic sulla connessione che si desidera utilizzare e fare clic su **Connetti** nella finestra principale del client

status: Connected VPN Client - \	Version 5.0.03.0530	
Connection Entries Status Certificates Log	Options Help	
Connect New Import M	fodfy Delete	dia cisc
Connection Entries Certificates Log		
Connection Entry	Host	Transport
ASA ASA	192.168.1.1	IPSec/UDP

5. Quando richiesto, immettere il **nome utente: cisco123** e **password: cisco123** è stato configurato nell'ASA per Xauth e fare clic su **OK** per connettersi alla rete

		enneder to complete	une user
authentication.			
Username:	cisco123		
cisco Password:	******		

6. Il client VPN è connesso all'ASA sulla postazione centrale.

🥝 status: Connected VPN Client - V	ersion 5.0.03.0530		_ 🗆 🛛
Connection Entries Status Certificates Log	Options Help		
Disconnect New Import	odiy Delete		lulu Isco
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
ASA	192.168.1.1	IPSec/UDP	
			the second se

7. Una volta stabilita la connessione, scegliere **Statistiche** dal menu Stato per verificare i dettagli del

tunnel.						
🥔 status: (Connected	VPN Client	- Version 5.0.03	.0530		
Connection E	intries Status	Certificates	Log Options Help			
Disconnect Connection B	Entries	atistics otifications eset Stats	Ctrl+S Ctrl+N Delete			dhaha cisco
	Connection	Entry /		Host	Transport	
۵	ASA			192.168.1.1	IPSec/UDP	

Verifica

Comandi show

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**.

- show crypto isakmp sa: visualizza tutte le associazioni di sicurezza IKE correnti in un peer.
- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione correnti.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione. Viene visualizzato anche l'output di esempio del comando debug.

Nota: per ulteriori informazioni sulla risoluzione dei problemi relativi alle VPN IPSec di accesso remoto, vedere <u>la sezione relativa alle soluzioni per la risoluzione dei problemi delle VPN IPSec di accesso remoto e L2L più comuni</u>.

Cancella associazioni di protezione

Quando si esegue la risoluzione dei problemi, assicurarsi di cancellare le associazioni di protezione esistenti dopo aver apportato una modifica. In modalità privilegiata di PIX, utilizzare i seguenti comandi:

- clear [crypto] ipsec sa: elimina le associazioni di protezione IPSec attive. La parola chiave crypto è facoltativa.
- clear [crypto] isakmp sa: elimina le SA IKE attive. La parola chiave crypto è facoltativa.

Comandi per la risoluzione dei problemi

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> 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.

Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance Pagina di supporto</u>
- Riferimenti per i comandi di Cisco ASA serie 5500 Adaptive Security Appliance
- <u>Cisco PIX serie 500 Security Appliance Pagina di supporto</u>

- Cisco PIX serie 500 Security Appliance Guida di riferimento ai comandi
- <u>Cisco Adaptive Security Device Manager</u>
- Pagina di supporto per la negoziazione IPSec/i protocolli IKE
- Pagina di supporto per Cisco VPN Client
- <u>Software Cisco PIX Firewall</u>
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- <u>Avvisi sui prodotti per la sicurezza (inclusi PIX)</u>
- <u>RFC (Requests for Comments)</u>
- Documentazione e supporto tecnico Cisco Systems