## ASA/PIX: Esempio di server VPN remoto con NAT in entrata per il traffico dei client VPN con CLI e ASDM

## Sommario

Introduzione Prerequisiti Requisiti Componenti usati Prodotti correlati Convenzioni Premesse Configurazione di ASA/PIX come server VPN remoto con ASDM Configurazione di ASA/PIX per il traffico del client VPN in entrata NAT con ASDM Configurare l'ASA/PIX come server VPN remoto e per il protocollo NAT in entrata con la CLI Verifica ASA/PIX Security Appliance - Comandi show Risoluzione dei problemi Informazioni correlate

## **Introduzione**

Questo documento descrive come configurare Cisco serie 5500 Adaptive Security Appliance (ASA) in modo che agisca come server VPN remoto usando Adaptive Security Device Manager (ASDM) o CLI e NAT per il traffico del client VPN in entrata. 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 tramite il client VPN Cisco.

## **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. Si presume che l'ASA sia configurata anche per il protocollo NAT in uscita. Per ulteriori informazioni su come configurare il protocollo NAT in uscita, fare riferimento a <u>Consenti accesso degli host interni alle reti esterne</u> <u>con l'utilizzo del protocollo PAT</u>.

**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.

### **Premesse**

Le configurazioni di accesso remoto forniscono accesso remoto sicuro per i client VPN Cisco, ad esempio gli utenti mobili. Una VPN ad accesso remoto consente agli utenti remoti di accedere in modo sicuro alle risorse di rete centralizzate. Il client VPN Cisco è conforme al protocollo IPSec ed è progettato in modo specifico per l'utilizzo con l'appliance di sicurezza. L'appliance di sicurezza può tuttavia stabilire connessioni IPSec con molti client conformi al protocollo. Per ulteriori informazioni su IPSec, consultare le <u>guide alla configurazione delle appliance ASA</u>.

I gruppi e gli utenti sono concetti fondamentali nella gestione della sicurezza delle VPN e nella configurazione dell'appliance di sicurezza. Specificano gli attributi che determinano l'accesso e l'utilizzo della VPN da parte degli utenti. Un gruppo è una raccolta di utenti trattati come un'unica entità. Gli utenti ottengono gli attributi dai criteri di gruppo. I gruppi di tunnel identificano i Criteri di gruppo per connessioni specifiche. Se non si assegna un determinato criterio di gruppo agli utenti, verrà applicato il criterio di gruppo predefinito per la connessione.

Un gruppo di tunnel è costituito da un set di record che determina i criteri di connessione al tunnel. Questi record identificano i server a cui gli utenti del tunnel sono autenticati, nonché gli eventuali server di accounting a cui vengono inviate le informazioni di connessione. Identificano inoltre un criterio di gruppo predefinito per le connessioni e contengono parametri di connessione specifici del protocollo. I gruppi di tunnel includono un piccolo numero di attributi relativi alla creazione del tunnel stesso. I gruppi di tunnel includono un puntatore a un criterio di gruppo che definisce gli attributi orientati all'utente.

## **Configurazioni**

#### Configurazione di ASA/PIX come server VPN remoto con ASDM

Per configurare Cisco ASA come server VPN remoto con ASDM, completare la procedura seguente:

 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.

Eisco ASDM 6.1	cisco			
Cisco ASDM 6.1(3) provides an intuitive graphical user interface that makes it easy to configure and manage your Cisco Security Appliances.	o set up,			
Cisco ASDM runs as either a local application or Java Web Start.				
Running Cisco ASDM as a local Application When you run Cisco ASDM as a local application, it connects to your Security Applyour desktop via SSL. Running Cisco ASDM as an application has these advantage <ul> <li>You can invoke ASDM from desktop shortcuts. No browser is required.</li> <li>One desktop shortcut allows you to connect to <i>multiple</i> Security Appliances</li> </ul>	iance from s:			
Running Cisco ASDM as Java Web Start         You can run Cisco ASDM as Java Web Start that is dynamically downloaded from the device to which you connect.         • Click Run ASDM to run Cisco ASDM.         • Click Run Startup Wizard to run Startup Wizard.Startup Wizard walks you through, step by step, the initial configuration of your security appliance.         Run ASDM         Run ASDM         Run Startup Wizard				

- 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.
- 4. Immettere l'indirizzo IP dell'interfaccia configurata con il comando http -, nonché un nome utente e una password, se specificati.In questo esempio viene utilizzato cisco123 come nome utente e cisco123 come

	Cisco ASDM Launch	er v1.5(30)	
		cisco	
	Device IP Address / Name:	10.77.241.111	<b>*</b>
	Username:	cisco123	
	Password:	* * * * * * *	
	🔄 Run in Demo Mode		
password.			1 🗐 🍰

5. Selezionare Procedure guidate > Creazione guidata VPN IPSec dalla finestra

	G Cisco ASDM 6.1 for ASA - 10.77.241.111								
	File	View	Tools	Wiza	ards	Window	Help		
	Home 🖧 Cor			Star	tup Wizaro	i		-	
			IPsec VPN Wizard						
			-	551	VDN Wizer	<u>а</u>	16		
	💠 A	dd 🏛	Delete		SSE VEN WIZHU				
	10.77.241.10			High Availa		Availability and Scalability Wizard			
Home.	ome 10.77.241.1				Packet Capture Wizard				

6. Selezionare il tipo di tunnel VPN di **accesso remoto** e verificare che l'interfaccia tunnel VPN sia impostata come desiderato, quindi fare clic su **Avanti** come mostrato di seguito.

🖆 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Brandh Frankh Fr	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
	Site-to-Site
	Remote Access
	VPN Tunnel Interface: Outside
	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. Viene scelto il tipo di client VPN, come mostrato. Cisco VPN Client è scelto qui. Fare clic su Next

(Avanti).

🖆 VPN Wizard	Σ	<
VPN Wizard	Remote Access Client (Step 2 of)	
Branch	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.	
	VPN Client Type:	
Home	Circo WMI Clerk, Deleger 2 v or history	
Corporate Notwork	or other Easy VON Remote product	
cuto .	or other basy why relince product	
The Take	Microsoft Windows client using L2TP over IPsec	
	Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.	
- Tanull	PAP CHAP MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY	
THE THE	Specify if the client will send tunnel group name as - username@tunnelgroup.	
A-	Client will send tunnel group name as username@tunnelgroup.	
	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.	
	< Back Next > Finish Cancel Help	

 Immettere un nome per il nome del gruppo di tunnel. 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 usato in questo esempio è cisco. Fare clic su Next (Avanti).

🖆 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Branch Home Coreporate Network	The ASA allows you to group remote access tunnel users based on common connection parameters attributes configured in the subsequent screens. Configure authentication method and tunel group for this remote connection. Use the same tunnel group name for the device and the remote clent.   Authentication Method   Pre-shared key   Pre-Shared Key:   clertificate   Certificate   Certificate Signing Algorithm:   rsa-sig   Certificate Name:   Challenge/response authentication (CRACK)
	< Back Next > Finish Cancel Help

9. Specificare se si desidera che gli utenti remoti vengano autenticati nel database degli utenti locale o in un gruppo di server AAA esterno.Nota: aggiungere gli utenti al database locale nel passo 10.Nota: per informazioni su come configurare un gruppo di server AAA esterno con ASDM, fare riferimento all'esempio di configurazione dell'autenticazione e dell'autorizzazione PIX/ASA 7.x per utenti VPN tramite ASDM.

🖆 VPN Wizard		×
VPN Wizard	Client Authentication (Step 4 of)	
Bandh Bandh Bandh Bandh Home Corporate Network	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.	
	Cancel Hel	5
		۳.

10. Fornire un nome utente e una password facoltativa e fare clic su Aggiungi per aggiungere nuovi utenti al database di autenticazione degli utenti. Fare clic su Next (Avanti).Nota: non rimuovere gli utenti esistenti da questa finestra. Selezionare Configurazione > Gestione dispositivi > Utenti/AAA > Account utente nella finestra principale di ASDM per modificare le voci esistenti nel database o rimuoverle dal database.

🖆 VPN Wizard		×
VPN Wizard	User Accounts (Step 5 of 11)	
	Add new users into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Device Management > Users/AAA > User Accounts in the main ASDM window.	
Home	User to Be Added	
Corporate Network	Username: dscol23	
	ciscol   Password (optional):   •••••••   Confirm Password (optional):   •••••••	
	< Back Next > Finish Cancel Help	2

 Per definire un pool di indirizzi locali da assegnare dinamicamente ai client VPN remoti, fare clic su Nuovo per creare un nuovo pool IP.

🖆 VPN Wizard		×
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Branch ISP Home Corporate Home	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients. Tunnel Group Name : cisco	
	Pool Name:       New         Pool Settings       Range Start Address:         Range End Address:       Subnet Mask:	
	< Back Next > Finish Cancel Help	2

12. Nella nuova finestra Add IP Pool fornire queste informazioni e fare clic su OK.Nome del pool IPIndirizzo IP inizialeIndirizzo IP finaleSubnet

<b>1</b>	Add IP Pool		×
	Name:	vpnpool	
	Starting IP Address:	192.168.1.1	
	Ending IP Address:	192.168.1.254	
	Subnet Mask:	255.255.255.0	~
sk	ОКЪС	Cancel Help	

13. Dopo aver definito il pool di indirizzi locali da assegnare dinamicamente ai client VPN remoti quando si connettono, fare clic su Avanti.

🖆 VPN Wizard					×
VPN Wizard	Address Pool	(Step 6 of 11)			
Branch Branch Branch Branch Home	Enter a poo clients.	ol of local addresses to be use	ed for assigning dynamic IP a	addresses to remote VPN	
Corporate Network		Tunnel Group Name :	cisco		
THE IN		Pool Name:	vpnpool 👻	New	
		Pool Settings			
Territiu		Range Start Address:	192.168.1.1		
- Icastilly		Range End Address:	192.168.1.254		
The state		Subnet Mask:	255.255.255.0		
	L				
			< Back Next >	Finish Cancel Hel	P

14. *Facoltativo:* Specificare le informazioni sui server DNS e WINS e un nome di dominio predefinito da inserire nei client VPN remoti.

🖆 VPN Wizard		
VPN Wizard	Attributes Pushed to Client (Optional)	(Step 7 of 11)
Bronch Bronch	Attributes you configure below are push ASA. If you do not want an attribute pu	ed to the VPN client when the client connects to the shed to the client, leave the corresponding field blank.
Corporate	Tunnel Group:	disco
Sector 10	Primary DNS Server:	
	Secondary DNS Server:	
TIM	Primary WINS Server:	
	Secondary WINS Server:	
	Default Domain Name:	
		< Back Next > Finish Cancel Help

15. Specificare i parametri per IKE, noto anche come IKE fase 1.Le configurazioni su entrambi i lati del tunnel devono corrispondere esattamente. Tuttavia, il client VPN Cisco seleziona automaticamente la configurazione corretta. Non è pertanto necessaria alcuna configurazione IKE sul PC client.

🖆 VPN Wizard		×				
VPN Wizard	IKE Policy (Step 8 of 11)					
Branch Branch Destate Home Home	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.					
Notwork	Encryption: DES					
	Authentication:					
	Diffie-Helman Group: 2					
	< Back Next Finish Cancel Help	2				

 Questa finestra mostra un riepilogo delle azioni intraprese. Se la configurazione è soddisfacente, fare clic su Fine.



#### Configurazione di ASA/PIX per il traffico del client VPN in entrata NAT con ASDM

Completare questa procedura per configurare Cisco ASA per il traffico del client VPN in entrata NAT con ASDM:

1. Scegliere **Configurazione > Firewall > Regole Nat**, quindi fare clic su **Aggiungi**. Nell'elenco a discesa selezionare **Aggiungi regola NAT** 



#### dinamica.

2. Nella finestra **Aggiungi regola NAT dinamica**, scegliere **Esterno** come interfaccia, quindi fare clic sul pulsante Sfoglia accanto alla casella **Origine**.

🖆 Add Dyn	amic NAT Rule		
Original — Interface: Source: Translated – Select a di	Outside		
Pool ID 0 0	Interface (outbound) (inbound)	Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
Connectio	on Settings	OK Cancel Help	*

3. Nella finestra Sfoglia origine, selezionare gli oggetti di rete appropriati e scegliere l'**origine** nella sezione Origine selezionata, quindi fare clic su **OK**. In questo caso, viene scelto l'oggetto di rete

192.168.1.0.

🖆 Browse Source					×
🗣 Add 🗹 Edit 📋 De	lete 🔍				
Filter:					Filter Clear
Name	<sup>1</sup> IP Addres	s	Netmask	Description	
Network Objects					
- 🎲 any	0.0.0.0		0.0.0.0		
📲 inside-network	172.16.1.0		255.255.255.0		
🙀 Outside-netwo	rk 10.10.10.0	1 1	255.255.255.0		
192.168.1.0	192.168.1.	0	255.255.255.0		
				—	
Selected Source					
Source -> 192.1	.68.1.0/24				
				L or	Cancel

4. Fare clic su **Gestisci**.

C	Add Dyna	amic NAT Rule		
O Ti	riginal Interface: Source: ranslated —	Outside 192.168.0.0		
	Select a glo	bal pool for dynami	: translation.	,
	Pool ID	Interface	Addresses Pool	
	0	(outbound)	Same as original address (identity)	
	0	(inbound)	Same as original address (identity)	Manage
	Connection	n Settings		*
			OK Cancel Help	

5. Nella finestra Gestisci pool globale fare clic su

🕵 Manage	Global Pool		
BbA 🔁	f Edit 🍵 Delete		
Pool ID	Interface	Addresses Pool	
	Ĭ.		
	ΟΚ	Cancel	

Aggiungi.
6. Nella finestra Aggiungi pool di indirizzi globale, scegliere Interno come interfaccia e 2 come ID pool. Verificare inoltre che il pulsante di opzione accanto a PAT using IP Address of the interface (PAT che utilizza l'indirizzo IP dell'interfaccia) sia selezionato. Fare clic su Add>>, quindi su OK.

🞼 Add Global Address Pool		
Interface: inside  Pool ID: 2		
IP Addresses to Add  Range Starting IP Address: Ending IP Address: Netmask (optional): IP Address Translation (PAT) IP Address: Netmask (optional):	Add >> << Delete	Addresses Pool
Port Address Translation (PAT) using IP     Address of the interface     OK     OK	Cancel	Help

7. Fare clic su **OK** dopo aver selezionato il pool globale con l'**ID pool 2** configurato nel passaggio

precedente.	-		
🕵 Add Dyna	amic NAT Rule		
Original			
Interface:	Outside	~	
Source:	192.168.1.0/24		
Translated —			
Select a glo	bal pool for dynamic	translation.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
2	inside	🔤 inside	Manage
Connection	n Settings		۲
		Cancel Help	

8. A questo punto, fare clic su **Apply** (Applica) per applicare la configurazione all'appliance ASA. La configurazione è stata completata.

Configura	ation > Firewall >	NAT Rules				
💠 Add	🝷 📝 Edit 🎁 Dele	te 🛉 🗲 🖌 🐰	🐚 🏨 - 🛛 🔍 Find 🗄	🔁 Diagram 🗐	Packet Trace	
	Turne	Original			Translated	
#	Туре	Source	Destination	Service	Interface	Addre:
🖬 Outsid	de (1 Dynamic rules)					
1	Dynamic	192.168.1.0/2	4		inside	🔤 insia
inside ⊡	(1 Exempt rules, 1 D	namic rules)				
1	🔁 Exempt	🌍 апу	192.168.1.0/24		(outbound)	
2	<b>Dynamic</b>	🌍 any			Outside	🎫 Out
						2
C See h	la braffic bhuarada bh a	لتحمينها ستكمينا	voss tuppelation			
Enab	e trarric through the	nrewall without add	ress translation			
			Appiy Reset	J		

# Configurare l'ASA/PIX come server VPN remoto e per il protocollo NAT in entrata con la CLI

Esecuzione della configurazione sul dispositivo ASA			
ciscoasa# <b>snow running-config</b>			
: Saved			
ASA Version 8.0(3)			
!			
hostname ciscoasa			
enable password 8Ry2YjIyt7RRXU24 encrypted			
names			
!			
interface Ethernet0/0			
nameif Outside			
security-level 0			
ip address 10.10.10.2 255.255.255.0			

interface Ethernet0/1 nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside\_nat0\_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2 192.168.1.0 255.255.255.0 outside nat (inside) 0 access-list inside\_nat0\_outbound nat (inside) 1 0.0.0.0 0.0.0.0 route Outside 0.0.0.0 0.0.0.0 10.10.10.3 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-policy-record DfltAccessPolicy http server enable no snmp-server location no snmp-server contact !--- 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 ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5hmac crypto dynamic-map SYSTEM\_DEFAULT\_CRYPTO\_MAP 65535 set pfs group1 crypto dynamic-map SYSTEM\_DEFAULT\_CRYPTO\_MAP 65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto map Outside\_map 65535 ipsec-isakmp dynamic SYSTEM\_DEFAULT\_CRYPTO\_MAP crypto map Outside\_map interface Outside crypto isakmp enable Outside !--- 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 10 authentication pre-share encryption des hash sha group 2 lifetime 86400 crypto isakmp policy 30 authentication pre-share encryption des hash md5 group 2 lifetime 86400 telnet timeout 5 ssh timeout 60 console timeout 0 management-access inside threat-detection basic-threat threat-detection statistics access-list group-policy cisco internal group-policy cisco attributes vpn-tunnel-protocol IPSec !--- Specifies the username and password with their !--respective privilege levels username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0 username cisco attributes vpn-group-policy cisco tunnel-group cisco type remote-access tunnel-group cisco general-attributes address-pool vpnpool default-group-policy cisco !--- Specifies the pre-shared key "cisco123" which must !--- be identical at both peers. This is a global !--configuration mode command. tunnel-group cisco ipsecattributes pre-shared-key \* class-map inspection\_default match default-inspection-traffic Ţ policy-map type inspect dns migrated\_dns\_map\_1 parameters message-length maximum 512 policy-map global\_policy class inspection\_default inspect dns migrated\_dns\_map\_1 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
prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3
: end
ciscoasa#
```

## **Verifica**

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

1. Fare clic su

New.			
VPN Client - Version 5.0.03.0530			
Connection Entries Status Certificates Log Options	; Help		
Connect News Import Modify	) Delete		ahaha cisco
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
Not connected.			

 Specificare i dettagli della nuova connessione.Il campo Host deve contenere l'indirizzo IP o il nome host dell'appliance Cisco ASA configurata in precedenza. Le informazioni di autenticazione del gruppo devono corrispondere a quelle utilizzate nel passaggio 4. Al termine, fare clic su

Connection Entry: MyVPNClient Description: Host: 10.10.10.2 Authentication Transport Backup Servers Dial-Up  Group Authentication Name: Cisco Password: Servers Confirm Password: Servers Confirm Password: Servers Confirm Catter Chain	VPN Client   Create New VPN Connection Entry	×
Description:   Host:   10.10.10.2     Authentication   Transport   Backup Servers   Dial-Up     Image: Cisco   Password: Confirm Password:   Image: Confirm Password:     Image: Confirm Password: <td>Connection Entry: MyVPNClient</td> <td></td>	Connection Entry: MyVPNClient	
Host: 10.10.10.2     Authentication Transport   Backup Servers Dial-Up     Image: Cisco   Password: Image: Cisco   Password: Image: Confirm Password:	Description:	
Authentication Transport Backup Servers Dial-Up   Group Authentication Mutual Group Authentication   Name: cisco   Password: ********   Confirm Password: ********	Host: 10.10.10.2	cisco
Group Authentication     Mame:     cisco     Password:     ******* Confirm Password:     *******      Confirm Password:     *******      Confirm Password:     *******      Confirm Password:     ********	Authentication Transport Backup Servers Dial-Up	
Name: cisco   Password: ********   Confirm Password: *******   Confirm Password: ********	Group Authentication	Authentication
Password:       *******         Confirm Password:       *******         C Certificate Authentication       ********         Name:       *******         Send CA Certificate Chain       *******	Name: cisco	
Confirm Password: ****** C Certificate Authentication Name: Send CA Certificate Chain	Password:	
<ul> <li>Certificate Authentication</li> <li>Name:</li> <li>Send CA Certificate Chain</li> </ul>	Confirm Password: ******	
Erase User Password Save Cancel	<ul> <li>Certificate Authentication</li> <li>Name:</li> <li>Send CA Certificate Chain</li> <li>Erase User Password</li> <li>Save </li> </ul>	Cancel

3. Selezionare la connessione appena creata e fare clic su **Connetti**.

Status: Disconnected   VPN Client - Versio	n 5.0.03.0530		
Connection Entries Status Certificates Log Options	Help		
Connection Entries Certificates Log	X Delete		cisco
Connection Entry	Host	Transport	
MyVPNClient	10.10.10.2	IPSec/UDP	
Not connected.			

4. Immettere un nome utente e una password per l'autenticazione estesa. Queste informazioni devono corrispondere a quelle specificate nei **passaggi 5 e** 

	VPN Client   User Authentication for "MyVPNClient"						
	The server has requested the following information to complete the user authentication.						
	Username: cisco123 CISCO Password: ******						
6.	OK Cancel						

5. Una volta stabilita la connessione, scegliere **Statistics** dal menu Status per verificare i dettagli del

tunnel.

🥔 status: Connected   Vi	PN Client - Version	5.0.03.0530			X
Connection Entries Status Ce	ertificates Log Options	Help			
Disconnect N	tics Ctrl+S tations Ctrl+N	X Delete		ciso	ı. :0
Connection Entries Reset	Stats				
Connection Entry	Δ	Host	Transport		
MyVPNClient		10.10.10.2	IPSec/UDP		
Connected to "MyVPNClient".			Connected Time: 0 day(s),	00:00.36	•

In questa finestra vengono visualizzate le informazioni sul traffico e sulla



Questa finestra mostra le informazioni sul tunneling

Т	unnel Details	Route Details Fi	irewall	
Ŀ	ocal LAN Rout	es	Secured F	loutes
	Network	Subnet Mask	Network	Subnet Mask
			0.0.0.0	0.0.0

#### 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
     IKE Peer: 10.10.10.1
 1
                               Role
     Type : user
                                      : responder
                               State
     Rekey
                                       : AM_ACTIVE
             : no
• show crypto ipsec sa: visualizza tutte le SA IPsec correnti in un peer.
 ASA#show crypto ipsec sa
 interface: Outside
     Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10
 .10.2
       local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
       current_peer: 10.10.10.1, username: cisco123
       dynamic allocated peer ip: 192.168.1.1
       #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
       #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 20, #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.: 10.10.10.2, remote crypto endpt.: 10.10.10.1
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: F49F954C
    inbound esp sas:
      spi: 0x3C10F9DD (1007745501)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn id: 24576, crypto-map: SYSTEM DEFAULT CRYPTO MAP
         sa timing: remaining key lifetime (sec): 27255
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xF49F954C (4104099148)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 27255
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#debug icmp trace
!--- Inbound Nat Translation is shown below for Outside to Inside ICMP echo request
translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3
2
!--- Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply
untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
ICMP echo request from Outside: 192.168.1.1 to inside: 172.16.1.3 ID=768 seg=8192
len=32
ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3
ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32
```

## 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**.

Per ulteriori informazioni su come risolvere i problemi relativi alla VPN da sito a sito, fare riferimento a <u>L2L e alle soluzioni di risoluzione dei problemi per le VPN IPSec di accesso remoto più comuni</u>.

## Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- <u>Cisco Adaptive Security Device Manager</u>
- Cisco ASA serie 5500 Adaptive Security Appliance Risoluzione dei problemi e avvisi

Documentazione e supporto tecnico – Cisco Systems