# Esempio di configurazione di PIX/ASA e VPN Client per VPN Internet pubblica su Memory Stick

### Sommario

Introduzione Prerequisiti Requisiti Componenti usati Prodotti correlati Convenzioni Premesse Hairpinning o inversione a U Configurazioni Esempio di rete Configurazione CLI di PIX/ASA Configurazione di ASA/PIX con ASDM Configurazione client VPN Verifica Verifica client VPN Risoluzione dei problemi Informazioni correlate

# **Introduzione**

In questo documento viene descritto come configurare un'appliance ASA Security 7.2 e versioni successive per eseguire IPSec su una chiave. Questa configurazione è applicabile quando l'ASA non permette lo split tunneling e gli utenti si connettono direttamente all'ASA prima di potersi collegare a Internet.

**Nota:** nella versione 7.2 e successive di PIX/ASA, la parola chiave *intra-interface* permette a tutto il traffico di entrare e uscire dalla stessa interfaccia, e non solo al traffico IPsec.

Per completare una configurazione simile su un router del sito centrale, fare riferimento agli <u>esempi di configurazione di router e client VPN</u> per Internet pubblico su una Memory Stick.

Per ulteriori informazioni sullo scenario in cui il PIX hub reindirizza il traffico dal client VPN al PIX spoke, fare riferimento all'<u>esempio di configurazione dell'autenticazione TACACS+</u> 7.x Enhanced <u>Spoke-to-Client VPN</u>.

Nota: per evitare una sovrapposizione di indirizzi IP nella rete, assegnare un pool di indirizzi IP

completamente diverso al client VPN (ad esempio, 10.x.x.x, 172.16.x.x e 192.168.x.x). Questo schema di indirizzamento IP è utile per risolvere i problemi relativi alla rete.

### **Prerequisiti**

#### **Requisiti**

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

- Hub PIX/ASA Security Appliance deve eseguire la versione 7.2 o successive
- Cisco VPN Client versione 5.x

#### Componenti usati

Le informazioni di questo documento si basano sulle versioni 8.0.2 e 5.0 di Cisco VPN Client per appliance di sicurezza PIX o ASA.

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 7.2 e successive.

#### **Convenzioni**

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

### **Premesse**

#### Hairpinning o inversione a U

Questa funzionalità è utile per il traffico VPN che entra in un'interfaccia ma che viene quindi instradato all'esterno della stessa interfaccia. Ad esempio, se si dispone di una rete VPN hub e spoke, in cui l'appliance di sicurezza è l'hub, e le reti VPN remote sono spoke, affinché uno spoke comunichi con un altro spoke, il traffico deve passare all'appliance di sicurezza e quindi essere di nuovo indirizzato all'altro spoke.

Usare il comando **same-security-traffic** per consentire al traffico di entrare e uscire dalla stessa interfaccia.

**Nota: il** hairpinning o l'inversione a U è applicabile anche per la comunicazione tra client VPN e client VPN.

# **Configurazioni**

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:



Public Internet

### Configurazione CLI di PIX/ASA

• <u>PIX/ASA</u>

Esegui configurazione su PIX/ASA		
PIX Version 8.0(2)		
names		
!		
interface Ethernet0		
nameif outside		

```
security-level 0
ip address 172.18.124.98 255.255.255.0
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
!--- Command that permits IPsec traffic to enter and
exit the same interface. same-security-traffic permit
intra-interface
access-list 100 extended permit icmp any any echo-reply
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
ip local pool vpnpool
  192.168.10.1-192.168.10.254 mask 255.255.255.0
no failover
monitor-interface outside
monitor-interface inside
icmp permit any outside
no asdm history enable
arp timeout 14400
nat-control !--- The address pool for the VPN Clients. !-
-- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP.
global (outside) 1 172.18.124.166
!--- The NAT statement to define what to encrypt (the
```

addresses from the vpn-pool). nat (outside) 1 192.168.10.0 255.255.255.0 nat (inside) 1 0.0.0.0 0.0.0.0 static (inside,outside) 172.16.3.102 172.16.3.102 netmask 255.255.255.255 access-group 100 in interface outside route outside 0.0.0.0 0.0.0.0 172.18.124.98 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 !--- The configuration of group-policy for VPN Clients. group-policy clientgroup internal group-policy clientgroup attributes vpn-idle-timeout 20 !--- Forces VPN Clients over the tunnel for Internet access. split-tunnel-policy tunnelall no snmp-server location no snmp-server contact snmp-server enable traps snmp !--- Configuration of IPsec Phase 2. crypto ipsec transform-set myset esp-3des esp-sha-hmac !--- Crypto map configuration for VPN Clients that connect to this PIX. crypto dynamic-map rtpdynmap 20 set transform-set myset !--- Binds the dynamic map to the crypto map process. crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap !--- Crypto map applied to the outside interface. crypto map mymap interface outside !--- Enable ISAKMP on the outside interface. isakmp identity address isakmp enable outside !--- Configuration of ISAKMP policy. isakmp policy 10 authentication pre-share isakmp policy 10 encryption 3des isakmp policy 10 hash sha isakmp policy 10 group 2 isakmp policy 10 lifetime 86400 isakmp policy 65535 authentication pre-share isakmp policy 65535 encryption 3des isakmp policy 65535 hash sha isakmp policy 65535 group 2 isakmp policy 65535 lifetime 86400 telnet timeout 5 ssh timeout 5 console timeout 0 !--- Configuration of tunnel-group with group information for VPN Clients. tunnel-group rtptacvpn type ipsec-ra

<pre>! Configuration of group parameters for the VPN Clients. tunnel-group rtptacvpn general-attributes address-pool vpnpool</pre>
<pre>! Disable user authentication. authentication-server- group none</pre>
<pre>! Bind group-policy parameters to the tunnel-group for VPN Clients. default-group-policy clientgroup tunnel-group rtptacvpn ipsec-attributes pre-shared-key *</pre>
!
class-map inspection_default match default-inspection-traffic !
<pre>class inspection_default inspect dns maximum-length 512 inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect skinny inspect sqlnet inspect sumpc inspect tftp inspect tftp inspect sip</pre>
inspect xdmcp
1
service-policy global_policy global Cryptochecksum:lalad58226e700404e1053159f0c5fb0 : end

### Configurazione di ASA/PIX con ASDM

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

1. Scegliere **Procedure guidate > Creazione guidata VPN IPSec** dalla finestra Home.

💏 Cisco ASDM 6.0 fo	r PIX - 172.16.3.101	
File View Tools	Wizards Window Help	
Home 🖧 Cor	Startup Wizard	Back 🕥 Forward 🦻
	IPsec VPN Wizard	
Add Delete	High Availability and Scalability W Packet Capture Wizard	izard
172.16.3.101	General Lio	ense
	Host Name	
	PIX Version:	: Device Uptime:
	ASDM Versit	on: Device Type:
	Firewall Mo:	de: Context Mode:
	Total Flash	Total Memory:
	VPN Tunnels	IPcoc:
	INC,	1000

2. Scegliere il tipo di tunnel VPN di **accesso remoto** e verificare che l'interfaccia tunnel VPN sia impostata come desiderato

Lesiderato.		
WPN Wizard		×.
VPN Wizard	VPN Tunnel Type (Step 1 of)	
	Use this wizard to configure new site-to- tunnel between two devices is called a si established by calls from remote users su	site VPN tunnels or new remote access VPN tunnels. A te-to-site tunnel and is bidirectional. A tunnel ich as telecommuters is called remote access tunnel.
ISP UTIL	This wizard creates basic tunnel configur	ations that you can edit later using the ASDM.
Corporate	VPN Tunnel Type:	Site to Site VPN
THE H	C Site-to-Site	Remote
	Remote Access	VPN Remote Access
CA D	VPN Tunnel Interface:	•
	Enable inbound IPsec sessions to by authorization access lists still apply t	pass interface access lists. Group policy and per-user o the traffic.
		≤Back Next> Einish Cancel Help

3. L'unico tipo di client VPN disponibile è già selezionato. Fare clic su Next

(Avanti).	
💼 VPN Wizard	×
VPN Wizard	Remote Access Client (Step 2 of)
	Remote access users of various types can open VPN tunnels to this PIX. Select the type of VPN client for this tunnel.
	B VPN Client Type:
(Corporate)	Cisco VPN Client, Release 3.x or higher,
Network	or other Easy VPN Remote product
	<ul> <li>C Microsoft Windows client using L2TP over IPsec</li> <li>Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.</li> <li>□ PAP □ CHAP □ MS-CHAP-V1 □ MS-CHAP-V2 □ EAP-PROXY</li> <li>Specify if the client will send tunnel group name as - username@tunnelgroup.</li> <li>□ Client will send tunnel group name as username@tunnelgroup.</li> <li>If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared liey and ppp authentication are also modified.</li> </ul>
	≤Back Next > Einish ⊆ancel Help

4. Immettere un nome per il nome del gruppo di tunnel. Specificare le informazioni di autenticazione da utilizzare.In questo esempio viene scelta la **chiave già condivisa**.

💼 VPN Wizard	X
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Brands Brands Fish Fish Fish Fish Fish Fish Fish Fis	The PIX allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client. Authentication Method Pre-shared key Pre-Shared Key: cisco123 Certificate Certificate Signing Algorithm: rsa-sig
JUM	Certificate Name:
58-	Tunnel Group Tunnel Group Name: rtptacypn
	<u>≤Back</u> Next> Einish: ⊆ancel Help

**Nota:** non è possibile nascondere/crittografare la chiave già condivisa sull'ASDM. Infatti, l'ASDM deve essere utilizzata solo da utenti che hanno configurato l'ASA o da utenti che hanno assistito il cliente nella configurazione.

5. 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 6.Nota: per informazioni su come configurare un gruppo di server AAA esterno tramite 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)
and a second	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.
Network	Authenticate using the local user database
	C Authenticate using an AAA server group AAA Server Group Name:
	<u>≤Back N</u> ext> Einish <u>C</u> ancel <u>H</u> elp

6. Se necessario, aggiungere utenti al database locale.Nota: non rimuovere gli utenti correnti da questa finestra. Scegliere Configurazione > Amministrazione dispositivi > Amministrazione > 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)	
erando erando	Add new users into the user authent or to remove them from the databas Users/AAA > User Accounts in the m	ication database. To edit existing entries in the database e, go to Configuration > Device Management > ain ASDM window.
ното	User to Be Added	
Corporate Network	Usernamé:	stick
	Password (optional):	Delete
	Confirm Password (optional):	
		- Park   Mosta   Circle   Carried   High
		Z Dack Next > Disse Cancel Help

7. Definire un pool di indirizzi locali da assegnare dinamicamente ai client VPN remoti quando si

connettono.

📸 VPN Wizard		×
VPN Wizard	Address Pool (Step 6 of 11)	
	Enter a pool of local addresses to be us clients.	ed for assigning dynamic IP addresses to remote VPN
Corporato Network	Tunnel Group Name :	rtptacvpn
The state	Pool Name:	vpnpool
	-Pool Settings	
	Range Start Address:	192.168.10.1
	Range End Address:	192,168,10,254
	Subnet Mask:	255.255.255.0
S.P-		
		<u>≤Back N</u> ext > Einish, <u>Cancel</u> <u>H</u> elp

8. *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)
	Attributes you configure below are pushed to the VPN client when the client connects to the PIX. If you do not want an attribute pushed to the client, leave the corresponding field blank.
Corporate")	Tunnel Group: rtptacvpn
Norwork	Primary DNS Server:
	Secondary DNS Server:
	Primary WINS Server:
	Secondary WINS Server:
SA-	Default Domain Name:
	<u>≤ Back</u> <u>N</u> ext > Einish <u>ancel</u> <u>H</u> elp

 Specificare i parametri per IKE, noto anche come IKE fase 1.Le configurazioni su entrambi i lati del tunnel devono corrispondere esattamente, ma il client VPN Cisco sceglie automaticamente la configurazione appropriata per se stesso. Sul PC client non è necessaria alcuna configurazione IKE.

		~
VPN Wizard	IKE Policy (Step 8 of 11)	12.02 0.0000
	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.	
Contraction of the second seco	Encryption: 3DES	
	DH Group:	
	< Back   Nevt >   Eloich   Caricel   He	

10. Specificare i parametri per IPSec, noto anche come IKE fase 2.Le configurazioni su entrambi i lati del tunnel devono corrispondere esattamente, ma il client VPN Cisco sceglie automaticamente la configurazione appropriata per se stesso. Sul PC client non è necessaria alcuna configurazione IKE.

💏 VPN Wizard	×
VPN Wizard	IPsec Encryption and Authentication (Step 9 of 11)
Brandh Brandh FSP Homme	Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.
Consortante Internationalité	Encryption: SES
	≤Back Next > Einish ⊆ancel Help

11. Specificare gli eventuali host interni o reti che possono essere esposti agli utenti VPN remoti.Se si lascia vuoto questo elenco, gli utenti VPN remoti possono accedere all'intera rete interna dell'appliance ASA.In questa finestra è anche possibile abilitare il tunneling suddiviso. Il tunneling ripartito cripta il traffico diretto alle risorse definite in precedenza in questa procedura e fornisce l'accesso non crittografato a Internet in senso lato evitando il tunneling del traffico. Se il tunneling suddiviso *non* è abilitato, tutto il traffico proveniente dagli utenti VPN remoti viene tunneling verso l'appliance ASA. In base alla configurazione, questa operazione può richiedere un uso intensivo della larghezza di banda e del processore.

VPN Wizard	Address Translation Exemption and Split Tunneling (Op	ptional) (Step 10 of 11)
	Network Address Translation (NAT) is used to hide the interna make exceptions to NAT to expose the entire or part of the in users protected by VPN. To expose the entire network behind the most secure interfa- leave the selection list blank.	al network from outside users. You can nternal network to authenticated remot ace to remote VPN users without NAT,
(Corporate)		Selected Hosts/Networks:
THE A	Host/Network	Add
	Address: any	Delete
S.P	Enable split tunneling to let remote users have simultane defined above, and unencrypted access to the internet.	ous encrypted access to the resources
	< Back Ne	ext >   Finish   Cancel   Help

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



13. Configurare il comando **same-security-traffic** per abilitare il traffico tra due o più host connessi alla stessa interfaccia quando si seleziona la casella di controllo come mostrato:

Home Ra Configuration M	v Help onitoring 🔲 Save 🙉 Refi	Look For	Forwe	rd 🦻 H	elp Find	· T	ili.ili.
Device Setup	Configuration > Device S	Setup > Interfa	ces	1 0	- 1		C
Startup Wizard	Interface	Name	Enabled	Security Level	IP Address	SI	Add 🔫
E-49+ Routing	Ethernet0	outside	Yes	0	172,18.124.98	255.2	
Device Name/Password	Ethernet1	inside	Yes	100	172.16.3.101	255.2	Edit
System Time	Ethernet2		No	1.2.		1.1	Dalasia
	Ethernet3		No				Teola
	Ethernet4		No				
	Ethernet5		No			1.1	
A Device Setup							
A Device Setup							
Device Setup Firewall							
Device Setup Firewall Remote Access VPN	✓[	wo or more inter	faces which a	are configure	ed with same secur	ky levels	
Device Setup         Firewall         Remote Access VPN         Ste-to-Ske VPN         Device Management	✓ Enable traffic between to the first of the traffic between to	two or more interl	faces which a	are configure	ed with same secur interface	ity levels :	

14. Scegliere **Configurazione > Firewall > Regole NAT**, quindi fare clic su **Aggiungi regola NAT dinamica** per creare questa traduzione dinamica con l'uso di ASDM.

Cisco ASDM 6.0 for PIX - 172.16.3.	101		
File View Tools Wizards Window	Help	Loc	kFor:
Home 🔥 Configuration 🔗 Mor	nitoring 🔚 Save 🛞 Refresh 🔇 Back (	Derward ? Help	
Device List 🖃 🕫 🗙	Configuration > Firewall > NAT Rules		
Add Delete S Connect	🗣 Add 🔸 📑 Edit. 🏥 Delete 🔶 🗳	🕺 🖻 🏨 - 🔍 Find 🖽 Di	igram 💐 Packet Trace
172.16.3.101	Add Static NAT Rule	[	- Filter Clear 🔀
	Add Dynamic NAT Rule	Original	Transla
	Add NAT Exempt Rule	Destination Service	Interface Ad
	Add Static Policy NAT Rule		
	Add Dynamic Policy NAT Rule		
	👲 Insert		
Firewall of 0 ×	Tinsert After		
- 9 Access Rules			
- Q Service Policy Rules			
AAA Rules			
URL Filtering Servers			
- Detection			
E-Im Objects			
a a horaited			
Device Setup			
Receival	4		henenenenenenenen <b>s</b>
Remote Access VPN	#		- 🔹 🔲
Ste-to-Site VPN	Source Address Real Addres	s NAT Type	Destination Address
Device Management	Enable traffic through the firewall without an	dress translation	

15. Scegliere inside come interfaccia di origine e immettere gli indirizzi che si desidera utilizzare per NAT. Per Traduci indirizzo su interfaccia, scegliete esterno e fate clic su OK

urce:	0.0.0.0	-	
slated			
lect a glo	bal pool for dynamic translation.		
Pool IE	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
1	outside	172.18.124.166	Manage
opectio	n Settinos		

16. Scegliere **esterno** come interfaccia di origine e immettere gli indirizzi che si desidera utilizzare per NAT. Per Traduci indirizzo su interfaccia, scegliete **esterno** e fate clic su

terrace: joi	1tside 12 168 10 0	<u> </u>	
slated			
ect a globa	I pool for dynamic translation.		
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
1	outside	172.18.124.166	Manage

17. La traduzione viene visualizzata in Regole di conversione in **Configurazione > Firewall > Regole** NAT.

Cisco ASDM 6.0 for PIX - 172.	16.3.101						
le <u>V</u> iew <u>T</u> ools Wi <u>z</u> ards <u>W</u> ir	ndow <u>H</u> elp				Look	For:	
home 🖧 Configuration	Monitoring	🔚 Save 🔇	Refresh 🔇 Back 🔇	) Forward 🧖 Help			
)evice List _⊟ ≏ ×	Configura	tion > Firewall >	NAT Rules				
Add 📋 Delete 🚿 Connect	🗣 Add	• 🗹 Edit 📋 (	Delete 🛉 🗲 👗	B - QF	ind 🔛 Diagram	2 Packet Tra	ace
- A 10.77.241.143 - A 172.16.3.101	Filter: Or	iginal Source		II.		Filter	Clear 🛛
				Original			Translated
	#	Type	Source	Destination	Service 1	Interface	Addres
	🖂 inside						CONTRACTOR
1	1	Dynamic	🛃 0.0.0.0		outsid	8	172.18.124
	2	Dynamic	192.168.10.0		outside	8	172.18.124
Advanced							
Device Setup							
Firewall	•						<u>•</u>
Remote Access VPN		<b></b> 0.0.0.	0 0000	172 18	124.166	<u>1</u>	E
Ste-to-Site VPN				Dynamic	Des Des	tination Addre	55
Device Management	Enable	e traffic through the	e firewali without address t	ranslation			
				and the second se	and the second second second		

**Nota 1:** È necessario configurare il comando <u>syspot connection allow-vpn</u>. Il comando <u>show</u> <u>running-config syspot</u> verifica se è configurato.

Nota 2: Aggiungere questo output per il trasporto UDP opzionale:

<u>group-policy clientgroup attributes</u> <u>vpn-idle-timeout 20</u> <u>ipsec-udp enable</u> <u>ipsec-udp-port 10000</u>

split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel

**Nota 3:** Configurare questo comando nella configurazione globale dell'accessorio PIX per consentire ai client VPN di connettersi tramite IPsec su TCP:

isakmp ipsec-over-tcp port 10000

**Nota:** fare riferimento al video <u>Hair-Pinning su Cisco ASA</u> per ulteriori informazioni su diversi scenari in cui è possibile utilizzare lo hair-pinning.

#### **Configurazione client VPN**

Completare questa procedura per configurare il client VPN:

#### 1. Scegliere

👌 status: D	isconr	nected	VPN CI	ient - Versi	on 5.0.03.(	0530	
Connection Er	ntries S	tatus Cer	tificates	Log Options	; Help		
Connect	ter Ner		nport	Modify	Delete		alialia cisco
Connection E	ntries	Certificate	es Log				
	Conne	ection Entry	1		Ho	ist	Transport
•							
Not connected	ł.						

2. Immettere l'indirizzo IP dell'interfaccia esterna PIX e il nome del gruppo di tunnel insieme alla password di

autenticazione.

VPN Client	Create New VPN Con	nectio	n Entry	
Connection Entry: pix	1			
Description: pix		ululu cisco		
Host: 17.	18.124.98			
Authentication T	ransport   Backup Serve	rs   Di	al-Up	
Group Authentic	ation	01	Mutual Group.	Authentication
Name:	rtptacvpn			
Password:	*****			
Confirm Password	t:  ******			
C Certificate Authe Name: Send CA Cert	ntication ificate Chain	Ŧ		
Erase User Password	E		Save	Cancel

3. (*Facoltativo*) Fare clic su **Abilita tunneling trasparente** nella scheda Trasporto. (Questa operazione è opzionale e richiede la configurazione PIX/ASA aggiuntiva indicata nella <u>nota</u>

VPN Client	Create Ne	w VPN Conne	ction Entry	
Connection Entry:	pix1			
Description:	pix on a stick for	internet connecti	on	CISCO
Host	172.18.124.98			
Authentication	Transport	Backup Servers	Dial-Up	
Enable Tran	sparent Tunnelin	g		
· IPSec ove	UDP (NAT / P	AT)		
C IPSec ov	er TCP TO	P Port: 10000		
Allow Local	LAN Access			
Peer response t	meout (seconds):	90		
			-	1

4. Salvare il profilo.

# **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**.

- show crypto isakmp sa: visualizza tutte le associazioni di sicurezza IKE correnti in un peer.
- <u>show crypto ipsec sa</u>: visualizza tutte le SA correnti. Cercare i pacchetti crittografati e decrittografati sull'appliance ASA che definiscono il traffico del client VPN.

Tentare di eseguire il ping o di individuare un indirizzo IP pubblico dal client (ad esempio, www.cisco.com).

**Nota:** non è possibile eseguire il ping dell'interfaccia interna del PIX per la formazione di un tunnel a meno che il comando <u>management-access</u> non sia configurato in modalità di conferma globale.

PIX1(config)#management-access inside
PIX1(config)#show management-access

### Verifica client VPN

Completare questa procedura per verificare il client VPN.

- 1. Fare clic con il pulsante destro del mouse sull'icona di blocco del client VPN presente sulla barra delle applicazioni dopo una connessione riuscita e scegliere l'opzione per **le statistiche** per visualizzare le crittografie e le decrittografazioni.
- 2. Fare clic sulla scheda Dettagli percorso per verificare l'elenco dei tunnel non suddivisi trasmesso dall'accessorio.

# Risoluzione dei problemi

**Nota:** per ulteriori informazioni su come risolvere i problemi relativi alla VPN, consultare il documento sulla <u>risoluzione dei problemi relativi alla VPN</u>.

# Informazioni correlate

- Esempio di configurazione VPN Enhanced Spoke-to-Client per PIX Security Appliance
   versione 7.0
- <u>Cisco VPN Client</u>
- Negoziazione IPSec/protocolli IKE
- Software Cisco PIX Firewall
- <u>Riferimenti per i comandi di Cisco Secure PIX Firewall</u>
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- Fissaggio per capelli su Cisco ASA
- <u>RFC (Requests for Comments)</u>
- Documentazione e supporto tecnico Cisco Systems