# PIX/ASA 7.x ASDM: Limita l'accesso alla rete degli utenti VPN di Accesso remoto

## Sommario

Introduzione Prerequisiti Requisiti Componenti usati Prodotti correlati Esempio di rete Convenzioni Configurazione dell'accesso tramite ASDM Configurazione dell'accesso tramite CLI Verifica Risoluzione dei problemi Informazioni correlate

## Introduzione

In questo documento viene fornita una configurazione di esempio con Cisco Adaptive Security Device Manager (ASDM) per limitare le reti interne a cui gli utenti VPN ad accesso remoto possono accedere dietro PIX Security Appliance o Adaptive Security Appliance (ASA). È possibile limitare gli utenti VPN ad accesso remoto solo alle aree della rete a cui si desidera che accedano quando:

- 1. Creare elenchi degli accessi.
- 2. Associarli ai criteri di gruppo.
- 3. Associare i criteri di gruppo ai gruppi di tunnel.

Per ulteriori informazioni sullo scenario in cui VPN Concentrator blocca l'accesso degli utenti VPN, consultare il documento sulla <u>configurazione di Cisco VPN 3000 Concentrator per il blocco con</u> <u>filtri e</u> l'<u>assegnazione</u> di filtri RADIUS.

## Prerequisiti

## Requisiti

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

- Il PIX può essere configurato usando l'ASDM.**Nota:** per consentire la configurazione del PIX da parte di ASDM, consultare il documento sulla <u>concessione</u> dell'<u>accesso HTTPS</u> per ASDM.
- Èdisponibile almeno una configurazione VPN di accesso remoto valida. Nota: Se non si

dispone di una configurazione di questo tipo, fare riferimento all'<u>ASA come server VPN</u> <u>remoto usando l'esempio di configurazione ASDM</u> per informazioni su come configurare una VPN di accesso remoto valida.

#### Componenti usati

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

- Cisco Secure PIX serie 500 Security Appliance versione 7.1(1)**Nota:** Le appliance di sicurezza PIX 501 e 506E non supportano la versione 7.x.
- Cisco Adaptive Security Device Manager versione 5.1(1)**Nota:** ASDM è disponibile solo in PIX o ASA 7.x.

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 le seguenti versioni hardware e software:

• Cisco ASA serie 5500 Adaptive Security Appliance versione 7.1(1)

#### Esempio di rete

Nel documento viene usata questa impostazione di rete:



In questo esempio di configurazione, è prevista una piccola rete aziendale con tre subnet. Il diagramma mostra la topologia. Le tre subnet sono Intranet, Engineering e Payroll. L'obiettivo di questo esempio di configurazione è consentire al personale del ciclo paghe l'accesso remoto alle subnet Intranet e Ciclo paghe e impedire l'accesso alla subnet Engineering. Inoltre, i tecnici devono essere in grado di accedere in remoto alle subnet Intranet e Engineering, ma non alla subnet Payroll. L'utente del ciclo paghe in questo esempio è "controller1". L'utente che utilizza questo esempio è "engineer1".

### **Convenzioni**

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

## Configurazione dell'accesso tramite ASDM

Completare la procedura seguente per configurare l'appliance di sicurezza PIX utilizzando ASDM:

1. Selezionare Configurazione > VPN > Generale > Criteri di gruppo.

Cisco ASDM 5.1 fo	r PIX - 10.89.129.147	Hala			
Home Conf	iguration Montoring	Back Forward Search	h Refresh Save	) 🧿 Help	Cisco Systems
Interfaces	onfguration > VPN > General +	Group Policy Group Policy Manage VPN group policy Manage VPN group policy pairs that may be stored policy information is refe Name payroll engineering DftGrpPolicy (System D	cies. A VPN group policy internally on the device renced by VPN tunnel g Type Tunnelin Internal - Inherited Internal - Inherited Internal IPSec	y is a collection of use or externally on a RAD roups and user account ng Protocol AAA - N/A - N/A - N/A - N/A	<ul> <li>c-oriented attribute/value</li> <li>DIUS server. The group ints.</li> <li>Berver Group Add ▼</li> <li>Edit</li> <li>Delete</li> </ul>
<u> </u>			cisco NA (2)		🔒 3/13/06 3:07:51 PM UTC

2. In base alla procedura eseguita per configurare i gruppi di tunnel sul PIX, è possibile che esistano già Criteri di gruppo per i gruppi di tunnel di cui si desidera limitare gli utenti. Se esiste già un criterio di gruppo appropriato, selezionarlo e fare clic su Modifica. In caso contrario, fare clic su Aggiungi e scegliere Criteri di gruppo interni....

💼 Cisco ASDM 5.1 for PIX - 10.89.129.147			
File Rules Search Options Tools Wizards Help			
Home Configuration Monitoring Back Forward Search	h Refresh Save	<b>?</b> Help	CISCO SYSTEMS
Image: Security Policy   Image: Securit	cies. A VPN group policy i d internally on the device o erenced by VPN tunnel gro Type Tunneling Internal - Inherited Internal IPSec Apply cisco NA (2)	is a collection of user-oriented att in externally on a RADIUS server. oups and user accounts. g Protocol AAA Server Group N/A	ribute/value The group

- 3. Se necessario, immettere o modificare il nome dei Criteri di gruppo nella parte superiore della finestra visualizzata.
- 4. Nella scheda Generale deselezionare la casella **Eredita** accanto a Filtro e quindi fare clic su **Gestisci**.

Check an Inherit checkbo	x to let the corn	esponding setting take	its value from the default group policy.
Tunneling Protocols:	🔽 Inherit	🗖 IPSec	
Filter:	🗖 Inherit	None	Manage
Connection Settings			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Access Hours:	🔽 Inherit		▼ New
Simultaneous Logins:	🔽 Inherit		
Maximum Connect Tim	e: 🔽 Inherit	Unlimited	minutes
Idle Timeout:	🔽 Inherit	Unlimited	minutes
Servers			
DNS Servers:	🔽 Inherit	Primary:	Secondary:
WINS Servers:	🔽 Inherit	Primary:	Secondary:
DHCP Scope:	🔽 Inherit		

5. Fare clic su **Add ACL** per creare un nuovo elenco degli accessi nella finestra ACL Manager visualizzata.

1	ACL Ma	nager								×
С	onfigure	e ACLs.								
	*	Rule Enabled	Action	Source Host/Network	Destina Host/Ne	tion stwork	Service	Log Level Interval	Time Range	Add ACL
										Add ACE
										EditACE
										Delete
										Move Up
										Move Down
									•	
	🖌 Allo	ow traffic	<b>O</b> (	Deny traffic						
					av 1	Onned	1	Linin [		
						Cancel		нер		

6. Selezionare un numero per il nuovo elenco degli accessi e fare clic su

	付 Add New A	CL		×
	ACL ID:	10	 	]
		ок	Cancel	]
OK.				

7. Con il nuovo ACL selezionato a sinistra, fare clic su Add ACE (Aggiungi voce di controllo di accesso) per aggiungere una nuova voce di controllo di accesso all'elenco.

ĩ¢	CL Ma	nager								×
Co	Infigure	ACLs.								
	#	Rule Enabled	Action	Source Host/Network	De: Ho:	stination st/Network	Service	Log Level Interval	Time Range	Add ACL
	10									Add ACE
										EditACE
										Delete
										Моче Ор
										Move Down
1									•	
	🖌 🎸	w traffic	30	)eny traffic						
					0K	Cance		Help		

 Definire la voce di controllo di accesso (ACE, Access Control Entry) che si desidera aggiungere.Nell'esempio, la prima voce ACE nell'ACL 10 consente l'accesso IP alla subnet del ciclo paghe da qualsiasi origine.Nota: per impostazione predefinita, ASDM seleziona solo il protocollo TCP. È necessario scegliere IP se si desidera consentire o negare agli utenti l'accesso IP completo. Al termine, fare clic su OK.

dd Extended Access List Rule	
Action	Time Range
	Time Range: Not Applied 💌 New
Permit C Deny	Syslog
	Default Syslog More Options
Source Host/Network	Destination Host/Network
IP Address     C Name     C Group	● IP Address         C Name         C Group
IP address: 0.0.0.0	IP address: 10.8.28.0
Mask: 0.0.0.0	Mask: 255.255.255.0
Protocol and Service	
C TCP C UDP C ICMP C P	Manage Service Groups
IP protocol: any	
lease enter the description below (optional):	
ermit IP access from ANY source to the payroll su	ibnet (10.8.28.0 /24)
1	<u>F</u>

9. La voce di controllo di accesso appena aggiunta verrà visualizzata nell'elenco. Scegliere nuovamente **Aggiungi voce ACE** per aggiungere altre righe all'elenco degli accessi.

<u>í</u>	ICL Ma	nager							×
C	onfigur	e ACLs.							
Γ	*	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	10								Add ACE
Ŀ	1		1	🧇 any	<b>10.8.28.0/24</b>	💌 ip		Not Applied	Edit ACE
									Delete
									Move Up
									Move Down
1	- Allo	w traffic	<b>0</b> 1	Denutraffic				•	
	<ul> <li>Mail</li> </ul>	W LIGHTC	<b>0</b> (	Jony Dame					
				0	K Cance	1	Help		

Nell'esempio, una seconda voce ACE viene aggiunta all'ACL 10 per consentire l'accesso alla subnet

Intranet.

Action		Time Range
		Time Range:   Not Applied 💌 New
Permit	C Deny	Syslog
		Default Syslog More Options
Source Host/Netwo	rk	Destination Host/Network
IP Address	C Name C Group	
IP address: 0.0	1.0.0	IP address: 10.8.27.0
Mask: 0.0	.0.0	Mask: 255.255.255.0 💌
IP protocol:	CICMP © IP	Manage Service Groups
ease enter the des	cription below (optional):	tueed by all employees (10.9.27.0.(24)
armit IP access from	IT ANY SOURCE TO THE SUBHE	it used by all employees (10.8.27.0724)

10. Dopo aver aggiunto le voci ACE, fare clic su **OK**.

1	AC	L Ma	nager							x
C	:on	figure	e ACLs.							
		#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	Ξ	10						1		Add ACE
		1	N	<b>~</b>	🧼 any	AD:5.28.0/24	😕 ip		Not Applied	EditACE
		2		1	🧇 any	<b>10.8.27.0/24</b>	🕑 ip		Not Applied	<u></u>
										Delete
										Move Up
										Move Down
Ŀ	•								•	
	*	2 Allo	ow traffic	<b>1</b>	Deny traffic					
					0	Cance	el	Help		

 Selezionare l'ACL definito e compilato negli ultimi passaggi da utilizzare come filtro per Criteri di gruppo. Al termine, fare clic su OK.

Check an innert checkbo	to let the com	esponding setting take i	ts value from the default group policy
Tunneling Protocols:	🔽 Inherit	F IPSec	
Filter:	🗆 Inherit	10	Manage
Connection Settings Access Hours:	🔽 Inherit	None 10	New
Simultaneous Logins:	🔽 Inherit		
Maximum Connect Tim	e: 🔽 Inherit	Unlimited	minutes
Idle Timeout	🔽 Inherit	Unlimited	minutes
Servers			
DNS Servers:	🔽 Inherit	Primary:	Secondary:
WINS Servers:	🔽 Inherit	Primary:	Secondary;
DHCP Scope:	🔽 Inherit		

12. Fare clic su **Applica** per inviare le modifiche al PIX.

File Rules Search Options Tools Wizards Help	
Image: Second	Cisco Systems
Image: Security Policy         Image: Policy         Im	er-oriented attribute/value DIUS server. The group runts. A Server Group Add A A A Delete Delete

Se è stata configurata per eseguire questa operazione in Opzioni > Preferenze, ASDM visualizza in anteprima i comandi che sta per inviare al PIX. Fare clic su Invia.

Preview CLI Commands				
The following CLI commands are send the commands to the PIX, cli shanges in ASDM click Cancel	generated based on ck Send. To not sen	the changes you n d the commands a	nade in ASDM. To nd continue making	
access-list 10 line 1 remark po access-list 10 line 2 extended access-list 10 line 3 remark po	ermit IP access from permit ip any 10.8.2 ermit IP access from	ANY source to the 8.0 255.255.255.0 ANY source to the	payroll subnet (10.8. subnet used by all e	28.0 /24 <u>*</u>
access-list 10 line 4 extended group-policy payroll attributes vpn-filter value 10	permit ip any 10.8.2	7.0 265.255.265.0		
•				Þ
	Send	Cancel		

14. Applicare i Criteri di gruppo appena creati o modificati al gruppo di tunnel corretto. Fare clic su **Tunnel Group** nel frame di sinistra.

📬 Cisco ASDM 5.	.1 for PIX - 10.89.129.147				
File Rules Se	arch Options Tools Wizards	Help			
Since Contract of the second s	Configuration Monitoring	Back Forward Sear	ch Refresh	Save Help	CISCO SYSTEMS
Interfaces Security Policy NAT Security Policy NAT Security NAT Security Routing Global Objects Properties	Configuration > VPN > General >	Tunnel Group  Manage VPN tunnel gr IPSec or WebVPN com  Rame  Payroll  engineering DefaultL2LGroup  Specify the delimeter to are received when tunn Group Delimiter:	oups. A VPN tunnel ( nection. Upsec-ra ipsec-ra ipsec-ra ipsec-l2l	group represents a connection Group Policy payroll engineering DfIIGrpPolicy DfIIGrpPolicy ing tunnel group names from t lated. Reset	specific record for a
Configuration cha	anges saved successfully.		cisco N	A (2)	8/1 3/1 3/06 3:22:11 PM UTC

15. Selezionare il gruppo di tunnel a cui si desidera applicare i Criteri di gruppo e fare clic su **Modifica**.

🔯 Cisco ASDM 5.1	1 for PIX - 10.89.129.147				
File Rules Sea	arch Options Tools Wizards He	db			
Home C	Configuration Montoring Bas	sk Forward Searc	h Refresh Sa	ve Help	CISCO SYSTEMS
NAT Security Policy NAT WPN Colored Co	Configuration × VPN > General > Tu ⊕ ♠ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ ♥ General - ♥ Client Update - ♥ Default Tunnel Gat - ♥ Group Policy - ♥ WPN System Option ♥ NKE ⊕ ♥ P Address Manageme ⊕ ♥ P Sec	Annel Group	ups. A VPN tunnel gro ection. Type ipsec-ra ipsec-ra ipsec-ra ipsec-l2l be used when parsing els are being negotiate None V	up represents a connection of Group Policy payroll engineering DritOrpPolicy DritOrpPolicy DritOrpPolicy	specific record for a
Configuration cha	anges saved successfully.		cisco NA (2	Z) 🚽 🚮	🔒 3/13/06 3:22:31 PM UTC

16. Se i Criteri di gruppo sono stati creati automaticamente (vedere il passaggio 2), verificare che i Criteri di gruppo appena configurati siano selezionati nella casella a discesa. Se i Criteri di gruppo non sono stati configurati automaticamente, selezionarli dall'elenco a discesa. Al termine, fare clic su OK.

🔂 Edit Tunnel Group	×
Name: payroll Type: ipsec-ra	
General IPSec	
Configure general access attributes from the following sub-tabs.	
Basic AAA Client Address Assignment Advanced	
Oraus Baliar naurall	
Group Policy. payroll	
Strip the realm from username before passing it on to the A	AA server
Strip the group from username before passing it on to the A	AA server
OK N Cancel	Help
k]	

- 17. Fare clic su **Apply** (Applica), quindi, se richiesto, su **Send** per aggiungere la modifica alla configurazione PIX.Se i Criteri di gruppo sono già stati selezionati, è possibile che venga visualizzato il messaggio "Non sono state apportate modifiche". Fare clic su **OK**.
- 18. Ripetere i passaggi da 2 a 17 per ogni gruppo di tunnel aggiuntivo a cui si desidera aggiungere restrizioni. In questo esempio di configurazione, è anche necessario limitare l'accesso dei tecnici. Mentre la procedura è la stessa, queste sono alcune finestre in cui le differenze sono notevoli:Nuovo elenco accessi 20

🔂 A	CL Ma	nager							X
Co	nfigure	e ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	10								Add ACE
	1	V	<b>~</b>	🧼 any	A 10.8.28.0/24	💌 ip		Not Applied	EditACE
	2	V	<b>~</b>	🧼 any	A 10.8.27.0/24	💌 ip		Not Applied	Editrice
8	20								Delete
	1	V	<b>~</b>	🧇 any	A 192.168.1.0/24	😕 ip		Not Applied	Maustin
	2		<ul> <li>Ø</li> </ul>	🤹 any	<b>5</b> 10.8.27.0/24	🕑 ip		Not Applied	Move Op
									Move Down
1			-					•	
	P Allo	w traffic	3	Deny traffic					
				0	Cance		Help		

Scegliere **Elenco accessi 20** come filtro in Criteri di gruppo di Engineering.

Check an innent checkbo	x to let the com	esponding setting take	its value from the default group poli
Tunneling Protocols:	🗹 Inherit	F IPBec	
Filter:	🗖 Inherit	20	Manage
Connection Settings			
Access Hours:	I∕ Inherit		New
Simultaneous Logins:	🔽 Inherit		
Maximum Connect Tim	e: 🔽 Inherit	🗖 Unlimited	minutes
Idle Timeout:	🔽 Inherit	🗖 Unlimited	minutes
Servers			
DNS Servers:	🔽 Inherit	Primary:	Secondary:
WINS Servers:	🔽 Inherit	Primary:	Secondary:
DHCP Scope:	🔽 Inherit		

Verificare che i Criteri di gruppo di progettazione siano impostati per il gruppo di tunnel di progettazione.

🔂 Edit Tunnel Group	×
Name: engineering Type: ipsec-ra	
General IPSec	
Configure general access attributes from the following sub-tabs.	
Basic AAA Client Address Assignment Advanced	
Group Policy: engineering	
Strip the realm from username before passing it on to the AAA server	
Strip the group from username before passing it on to the AAA server	
OK Cancel Help	

## Configurazione dell'accesso tramite CLI

Completare la procedura seguente per configurare l'appliance di sicurezza tramite la CLI:

**Nota:** alcuni dei comandi mostrati in questo output sono riportati su una seconda riga per motivi di spazio.

1. Creare due diversi elenchi di controllo di accesso (15 e 20) da applicare agli utenti durante la connessione alla VPN di accesso remoto. L'elenco degli accessi verrà richiamato più avanti nella configurazione.

ASAwCSC-CLI(config)#access-list 15 remark permit IP access from ANY source to the payroll subnet (10.8.28.0/24)

ASAwCSC-CLI(config)#access-list 15 extended permit ip any 10.8.28.0 255.255.0

```
ASAwCSC-CLI(config)#access-list 15 remark Permit IP access from ANY
source to the subnet used by all employees (10.8.27.0)
ASAwCSC-CLI(config)#access-list 15 extended permit ip
any 10.8.27.0 255.255.255.0
ASAwCSC-CLI(config)#access-list 20 remark Permit IP access from ANY
source to the Engineering subnet (192.168.1.0/24)
ASAwCSC-CLI(config)#access-list 20 extended permit ip
any 192.168.1.0 255.255.255.0
ASAwCSC-CLI(config)#access-list 20 remark Permit IP access from ANY
source to the subnet used by all employees (10.8.27.0/24)
ASAwCSC-CLI(config)#access-list 20 extended permit ip
any 10.8.27.0 255.255.255.0
```

 Creare due pool di indirizzi VPN diversi. Crearne uno per il ciclo paghe e uno per gli utenti remoti del reparto tecnico.

ASAwCSC-CLI(config)#ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask 255.255.255.0

```
ASAwCSC-CLI(config)#ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask 255.255.255.0
```

3. Creare criteri per il ciclo paghe che si applicano solo a loro quando si connettono. ASAWCSC-CLI(config)#group-policy Payroll internal

ASAwCSC-CLI(config)#group-policy Payroll attributes

ASAwCSC-CLI(config-group-policy)#dns-server value 10.8.27.10

ASAwCSC-CLI(config-group-policy)#vpn-filter value 15

!--- Call the ACL created in step 1 for Payroll. ASAwCSC-CLI(config-group-policy)#vpntunnel-protocol IPSec

ASAwCSC-CLI(config-group-policy)#default-domain value payroll.corp.com

ASAwCSC-CLI(config-group-policy)#address-pools value Payroll-VPN

!--- Call the Payroll address space that you created in step 2.

4. Questo passo è uguale al passo 3, con la differenza che è per il gruppo Engineering. ASAWCSC-CLI(config)#group-policy Engineering internal

ASAwCSC-CLI(config)#group-policy Engineering attributes

ASAwCSC-CLI(config-group-policy)#dns-server value 10.8.27.10

ASAwCSC-CLI(config-group-policy)#vpn-filter value 20

!--- Call the ACL that you created in step 1 for Engineering. ASAwCSC-CLI(config-grouppolicy)#vpn-tunnel-protocol IPSec

ASAwCSC-CLI(config-group-policy)#default-domain value Engineer.corp.com

ASAwCSC-CLI(config-group-policy)#address-pools value Engineer-VPN

!--- Call the Engineering address space that you created in step 2.

5. Creare utenti locali e assegnare gli attributi appena creati a tali utenti per limitarne l'accesso

#### alle risorse.

ASAwCSC-CLI(config)#username engineer password ciscol23 ASAwCSC-CLI(config)#username engineer attributes ASAwCSC-CLI(config-username)#vpn-group-policy Engineering ASAwCSC-CLI(config-username)#vpn-filter value 20 ASAwCSC-CLI(config)#username marty password cisco456 ASAwCSC-CLI(config)#username marty attributes ASAwCSC-CLI(config)username)#vpn-group-policy Payroll ASAwCSC-CLI(config-username)#vpn-filter value 15

6. Creare gruppi di tunnel contenenti criteri di connessione per gli utenti del ciclo paghe. ASAwCSC-CLI(config)#tunnel-group Payroll type ipsec-ra

ASAwCSC-CLI(config)#tunnel-group Payroll general-attributes

ASAwCSC-CLI(config-tunnel-general)#address-pool Payroll-VPN

ASAwCSC-CLI(config-tunnel-general)#default-group-policy Payroll

ASAwCSC-CLI(config)#tunnel-group Payroll ipsec-attributes

ASAwCSC-CLI(config-tunnel-ipsec)#pre-shared-key time1234

7. Creare gruppi di tunnel contenenti criteri di connessione per gli utenti del reparto tecnico. ASAWCSC-CLI(config)#tunnel-group Engineering type ipsec-ra

ASAwCSC-CLI(config)#tunnel-group Engineering general-attributes

ASAwCSC-CLI(config-tunnel-general)#address-pool Engineer-VPN

ASAwCSC-CLI(config-tunnel-general)#default-group-policy Engineering

ASAwCSC-CLI(config)#tunnel-group Engineering ipsec-attributes

ASAwCSC-CLI(config-tunnel-ipsec)#pre-shared-key Engine123

Dopo aver immesso la configurazione, è possibile visualizzare questa area evidenziata nella configurazione:

#### Nome dispositivo 1

```
ASA-AIP-CLI(config)#show running-config

ASA Version 7.2(2)

!

hostname ASAwCSC-ASDM

domain-name corp.com

enable password 9jNfZuG3TC5tCVH0 encrypted

names

!

interface Ethernet0/0

nameif Intranet

security-level 0
```

```
ip address 10.8.27.2 255.255.255.0
1
interface Ethernet0/1
nameif Engineer
security-level 100
ip address 192.168.1.1 255.255.255.0
interface Ethernet0/2
nameif Payroll
security-level 100
ip address 10.8.28.0
1
interface Ethernet0/3
no nameif
no security-level
no ip address
interface Management0/0
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name corp.com
access-list Inside_nat0_outbound extended permit ip any
172.10.1.0 255.255.255.0
access-list Inside_nat0_outbound extended permit ip any
172.16.2.0 255.255.255.0
access-list 15 remark permit IP access from ANY source
to the
  Payroll subnet (10.8.28.0/24)
access-list 15 extended permit ip any 10.8.28.0
255.255.255.0
access-list 15 remark Permit IP access from ANY source
to the subnet
  used by all employees (10.8.27.0)
access-list 15 extended permit ip any 10.8.27.0
255.255.255.0
access-list 20 remark Permit IP access from Any source
to the Engineering
  subnet (192.168.1.0/24)
access-list 20 extended permit ip any 192.168.1.0
255,255,255,0
access-list 20 remark Permit IP access from Any source
to the subnet used
  by all employees (10.8.27.0/24)
access-list 20 extended permit ip any 10.8.27.0
255.255.255.0
pager lines 24
mtu MAN 1500
mtu Outside 1500
mtu Inside 1500
ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask
255.255.255.0
ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400
global (Intranet) 1 interface
```

nat (Inside) 0 access-list Inside nat0 outbound nat (Inside) 1 192.168.1.0 255.255.255.0 nat (Inside) 1 10.8.27.0 255.255.255.0 nat (Inside) 1 10.8.28.0 255.255.255.0 route Intranet 0.0.0.0 0.0.0.0 10.8.27.2 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 group-policy Payroll internal group-policy Payroll attributes dns-server value 10.8.27.10 vpn-filter value 15 vpn-tunnel-protocol IPSec default-domain value payroll.corp.com address-pools value Payroll-VPN group-policy Engineering internal group-policy Engineering attributes dns-server value 10.8.27.10 vpn-filter value 20 vpn-tunnel-protocol IPSec default-domain value Engineer.corp.com address-pools value Engineer-VPN username engineer password LCaPXI.4Xtvclaca encrypted username engineer attributes vpn-group-policy Engineering vpn-filter value 20 username marty password 6XmYwQ009tiYnUDN encrypted privilege 0 username marty attributes vpn-group-policy Payroll vpn-filter value 15 no snmp-server location no snmp-server contact crypto ipsec transform-set ESP-3DES-SHA esp-3des espsha-hmac crypto dynamic-map Outside\_dyn\_map 20 set pfs crypto dynamic-map Outside\_dyn\_map 20 set transform-set ESP-3DES-SHA crypto map Outside\_map 65535 ipsec-isakmp dynamic Outside\_dyn\_map crypto map Outside\_map interface Outside crypto isakmp enable Outside crypto isakmp policy 10 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 tunnel-group Payroll type ipsec-ra tunnel-group Payroll general-attributes address-pool vpnpool default-group-policy Payroll tunnel-group Payroll ipsec-attributes pre-shared-key \* tunnel-group Engineering type ipsec-ra tunnel-group Engineering general-attributes address-pool Engineer-VPN default-group-policy Engineering tunnel-group Engineering ipsec-attributes

```
pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
1
class-map inspection_default
match default-inspection-traffic
!
!
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:0e579c85004dcfb4071cb561514a392b
: end
ASA-AIP-CLI(config)#
```

# **Verifica**

Utilizzare le funzionalità di monitoraggio di ASDM per verificare la configurazione:

 Selezionare Monitoraggio > VPN > Statistiche VPN > Sessioni.Si vedono le sessioni VPN attive sul PIX. Selezionare la sessione desiderata e fare clic su Dettagli.

Cisco ASDM 5.1 for PIX - 10.89.129.14 File Rules Search Options Tools	7 Wizards Help			
📸 🦓 🤯 Home Configuration Monitor	ing Back Forward Se	orch Refresh Sa	ve Help	Cisco Systems
Monitoring > VPN > VP  Interfaces  Interfaces  VPN  Image: Statistics  Image: Statistics	N Statistics > Sessions a Grapi els stics statistic PSec 8	LAN-to-LAN 1 0	Total	Total Cumulative 1 3
Routing Cessions	Filter By: Remote Ad Username controllert D	Cress I All Sessions Group Policy As: Tunnel Group Pul MIGrpPolicy 10.9 avroll 172	s  signed IP Address blic IP Address 8.27.50 IPS .22.1.165 3D	Filter Protocol Encryption Bec ES Bing
Logging	To sort VPN sessions, r Logout By: - All Ses	ight-click on the above tab sions - I	le and select Table So Logo effesh	It Order from popup menu. but Sessions
Data Refreshed Successfully.		cisco NA (2	Last 2)   🍰 🔂	Updated: 3/13/06 2:39:33 PM

2. Selezionare la scheda ACL.Gli accessi riflettono il traffico che attraversa il tunnel tra il client e le reti consentite.

🔁 Session Details					×		
Remote Detailed							
Usemame	Group Policy Tunnel Group	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Client Type Version		
controller1	DfttGrpPolicy payroll	10.8.27.50 172.22.1.165	IPSec 3DES	20:35:08 UTC Non Mar 13 2006 0h:08m:58s	WinNT 4.8.00.0440		
Username         Group Policy         Assigned IP Address         Encryption         Login Time         Client Type           controlleri         DrttGrpPolicy         10.8.27.50         IPSec         20.35.00 UTC Mon Mar 13.2006         WinNT           controlleri         DrttGrpPolicy         10.8.27.50         IPSec         20.35.00 UTC Mon Mar 13.2006         WinNT           controlleri         DrttGrpPolicy         10.8.27.50         IPSec         20.35.00 UTC Mon Mar 13.2006         WinNT           controlleri         The following ACL is being applied to this session:         ************************************							
				Last Update	d: 3/13/06 2:47:17 PM		

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

## Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance ASA come server VPN remoto con</u>
   <u>esempio di configurazione ASDM</u>
- Esempi di configurazione di appliance di sicurezza Cisco PIX serie 500 e note tecniche
- Esempi di configurazione di appliance Cisco ASA serie 5500 Adaptive Security e note tecniche
- Esempi di configurazione di Cisco VPN Client e note tecniche
- Documentazione e supporto tecnico Cisco Systems