# ASDM del PIX/ASA 7.x: Restrinja el acceso a la red de los usuarios del VPN de acceso remoto

## Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados Productos Relacionados Diagrama de la red Convenciones Acceso de la configuración vía el ASDM Acceso de la configuración vía el CLI Verificación Troubleshooting Información Relacionada

## **Introducción**

Este documento proporciona una configuración de ejemplo mediante Cisco Adaptive Security Device Manager (ASDM) para restringir a lo que pueden acceder los usuarios VPN de acceso remoto de las redes internas detrás de PIX Security Appliance o Adaptive Security Appliance (ASA). Puede limitar los usuarios VPN de acceso remoto a solamente las áreas de la red a las que desea que accedan cuando:

- 1. Cree las Listas de acceso.
- 2. Asocíelas a las directivas del grupo.
- 3. Asocie esas directivas del grupo a los grupos de túnel.

Refiera a <u>configurar el Cisco VPN 3000 Concentrator para bloquear con los filtros y la asignación</u> <u>de filtro RADIUS</u> para aprender más sobre el escenario donde el concentrador VPN bloquea el acceso de los usuarios de VPN.

## prerrequisitos

### **Requisitos**

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El PIX se puede configurar usando el ASDM.**Nota:** Refiera a <u>permitir el acceso HTTPS para el</u> <u>ASDM</u> para permitir que el PIX sea configurado por el ASDM.
- Usted tiene por lo menos una buena configuración sabida del VPN de acceso remoto. Nota:

Si usted no tiene tales configuraciones, refiera al <u>ASA como servidor VPN remoto que usa el</u> <u>ejemplo de la Configuración de ASDM</u> para la información sobre cómo configurar una buena configuración del VPN de acceso remoto.

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 7.1(1) del dispositivo de seguridad de las 500 Series del Secure PIX de Cisco**Nota:** El PIX 501 y los dispositivos de seguridad 506E no soportan la versión 7.x.
- Versión 5.1(1) del Cisco Adaptive Security Device Manager**Nota:** El ASDM está solamente disponible en PIX o ASA 7.x.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

#### **Productos Relacionados**

Esta configuración también se puede utilizar con las siguientes versiones de hardware y software:

• Versión 7.1(1) adaptante del dispositivo de seguridad de las 5500 Series de Cisco ASA

#### Diagrama de la red

En este documento, se utiliza esta configuración de red:



En este ejemplo de configuración, una pequeña red corporativa con tres subredes es supuesta. Este diagrama ilustra la topología. Las tres subredes son Intranet, ingeniería, y nómina de pago. La meta de este ejemplo de configuración es permitir el Acceso Remoto del personal asalariado al Intranet y a las subredes de planillas de sueldos y evitar que accedan la subred de la ingeniería. También, los ingenieros deben poder acceder remotamente las subredes del Intranet y de la ingeniería, pero no la subred de planillas de sueldos. El usuario de nómina en este ejemplo es el "controller1". El usuario de la ingeniería en este ejemplo es el "engineer1".

#### **Convenciones**

Consulte <u>Convenciones de Consejos Técnicos de Cisco</u> para obtener más información sobre las convenciones sobre documentos.

## Configure el acceso vía el ASDM

Complete estos pasos para configurar el dispositivo de seguridad PIX usando el ASDM:

1. Seleccione la **configuración > el VPN > la directiva del general > del grupo**.

Gisco ASDM 5.1 for PIX - 10.89.129.147 File Rules Search Options Tools Wize	ds Help			<u>_0×</u>
Home Configuration Monitoring	Back Forward Sea	ch Refresh Save	<b>?</b> Help	CISCO SYSTEMS
Interfaces         Interfaces         Security Policy         NAT         Image: Security Policy         NAT         Image: Security Policy         Image: Security Policy	ral = Group Policy Group Policy Manage VPN group policy Manage VPN group policy pairs that may be store policy information is re Name payroll engineering DftGrpPolicy (System D.)	licies. A VPN group policy is ed internally on the device or ferenced by VPN tunnel grou Type Tunneling Internal - Inherited Internal - Inherited Internal IPSec	a collection of user-oriented attribu externally on a RADIUS server. The ups and user accounts. Protocol AAA Server Group - N/A - N/A - N/A	uteivalue e group Add • Edit Delete
		Apply	Reset	2 2.07-54 DM UTO

2. De acuerdo con qué medidas fueron tomadas para configurar a los grupos de túnel en el PIX, las directivas del grupo pudieron existir ya para esos grupos de túnel cuyos usuarios usted desea restringir. Si existe una política de grupo apropiada ya, elíjala y el tecleo edita. Si no, haga clic agregan y eligen el Internal group policy (política grupal interna)....

- 3. En caso necesario, ingresa o cambia el nombre de la directiva del grupo en la cima de la ventana que se abre.
- 4. En la ficha general desmarque el cuadro de la **herencia** al lado del filtro y después haga clic **manejan**.

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

5. El tecleo **agrega el ACL** para crear una nueva lista de acceso en la ventana del ACL Manager que aparece.

1	ACL Ma	nager										×
С	onfigure	e ACLs.										
Γ	#	Rule Enabled	Action	Source Host/Networ	ĸ	Destination Host/Network	k	Service	Log Lo Interva	evel al	Time Range	Add ACL
												Add ACE
												EditACE
												Delete
												Move Up
												Move Down
	1										•	1
	🖌 Allo	ow traffic	<b>Q</b> (	Deny traffic								
					0K	c	ancel	1	Help	1		
										1		

6. Elija un número para la nueva lista de acceso y haga clic la

	🚰 Add New ACL	×
	ACL ID: 10	
AUTORIZACIÓN.	ок 🔓 с	ancel

- 7. Con su nuevo ACL seleccionado a la izquierda, el tecleo agrega ACE para agregar una nueva entrada de control de acceso a la lista.

<b>1</b>	ACL Mai	nager							×
C	onfigure	ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	10								Add ACE
									EditACE
									Delete
									Move Up
									Move Down
Ŀ	L							•	
	🖌 🎸	w traffic	<b>(3</b> C	)eny traffic					
				0	Cancel		Help		

8. Defina la Entrada de control de acceso (ACE) que usted desea agregar. En este ejemplo, primer ACE en ACL 10 permite el IP Access a la subred de planillas de sueldos de cualquier fuente. Nota: Por abandono, el ASDM selecciona solamente el TCP como el protocolo. Usted debe elegir el IP si usted desea al IP Access completo de los usuarios del permit or deny. Haga Click en OK cuando le acaban.

id 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: 0.0.0.0	IP address: 10.8.28.0
Mask 0.0.0.0	Mack: 255 255 255 0
Protocol and Service	
CICP CUDP CICMP CP	Manage Service Groups
IP Protocol	
IP protocol: any	
lease enter the description below (optional):	
ermit IP access from ANY source to the payroll sub	net (10.8.28.0 /24)
3	

9. ACE que usted ahora acaba de agregar aparece en la lista. Elija **agregan ACE** otra vez para agregar cualquier línea adicional a la lista de acceso.

1	ACL Ma	anager							×
С	onfigu	re ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
	3 10								Add ACE
ŀ	1		1	🧇 any	<b>10.8.28.0/24</b>	🕩 ip		Not Applied	Edit ACE
									Delete
									Move Up
									Move Down
4								•	
	🖌 🗸	ow traffic	<b>Q</b> (	Deny traffic					
				0	K Cance	el	Help		

En este ejemplo, un segundo ACE se agrega a ACL 10 para permitir el acceso a la subred de

Intranet.

ia Extendea Access List	Rule		
Action		Time Range	
		Time Range: Not Applied Ne	3₩
Permit	Deny	Syslog	
		Default Syslog More Options	
Source Host/Network		Destination Host/Network	
IP Address C N	ame 🔿 Group		up
IP address: 0.0.0.0		IP address: 10.8.27.0	
Mask: 0.0.0.0	*	Mask: 255.255.255.0 💌	
Protocol and Service CTCP CUDP IP Protocol	CICMP CIP	Manage Service Group	S
IP protocol: any			
lease enter the descripti	on below (optional):		
ermit IP access from AN	/ source to the subnet us	sed by all employees (10.8.27.0/24)	
1			Þ
	-		

10. Haga Click en OK una vez que le hacen que agrega los ACE.

n 📷	CL Ma	nager							×
Co	nfigur	e ACLs.							
	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range	Add ACL
G	10								Add ACE
	1	V	<b>~</b>	🧼 any	A 10.5.28.0/24	😕 ip		Not Applied	EditACE
	2		1	🧇 any	g <sup>a</sup> 10.8.27.0/24	💌 ip		Not Applied	<u></u>
									Delete
									Move Up
									Move Down
1	2 011	oustraffic	0.1	Domutraffic				•	
	80	owname	<b>U</b>	Jeny trainic					
				0	K Cance	. 1	Heln		
						<u> </u>	i ieih		

11. Seleccione el ACL que usted definió y pobló en los pasos más recientes para ser el filtro para su directiva del grupo. Haga Click en OK cuando le hacen.

check an innent checkbo	x to let the com	esponding setting take it	is value from the default group policy
Tunneling Protocols:	🔽 Inherit	F IPSec	
Filter:	🗖 Inherit	10	Manage
Connection Settings		None 10	
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		

12. El tecleo **se aplica** para enviar los cambios al PIX.

Fisco ASDM 5.1 for PIX - 10.89.129.147 File Rules Search Options Tools Wizards Help		
Home Configuration Monitoring Back Forward Search	Refresh Save Help	Cisco Systems
Image: Configuration > VPN > General > Group Policy   Image: VPN Wizard   Image: VPN Glop   Image: VPN System Option   Image: VPN System Option <td>es. A VPN group policy is a collection of nternally on the device or externally on enced by VPN tunnel groups and user Type Tunneting Protocol Internal - Inherited Internal IPSec Apply Reset</td> <td>of user-oriented attribute/value a RADIUS server. The group accounts. AAA Berver Group Add ▼ - N/A - N/A - N/A - N/A Delete</td>	es. A VPN group policy is a collection of nternally on the device or externally on enced by VPN tunnel groups and user Type Tunneting Protocol Internal - Inherited Internal IPSec Apply Reset	of user-oriented attribute/value a RADIUS server. The group accounts. AAA Berver Group Add ▼ - N/A - N/A - N/A - N/A Delete

13. Si usted lo hace configurar para hacer tan bajo las **opciones > preferencias**, el ASDM ve los comandos de antemano que está a punto de enviar al PIX. El tecleo **envía**.

🗯 Preview CLI Commands		×
The following CLI commands and send the commands to the PIX, of changes in ASDM, click Cancel.	e generated based on the changes you made in ASI click Send. To not send the commands and continu	DM. To e making
access-list 10 line 1 remark access-list 10 line 2 extende access-list 10 line 3 remark access-list 10 line 4 extende group-policy payroll attributes vpn-filter value 10	permit IP access from ANY source to the payroll sub d permit ip any 10.8.28.0 255.255.255.0 permit IP access from ANY source to the subnet use d permit ip any 10.8.27.0 255.255.255.0 s	net (10.8.28.0 /24 <u>)</u> ed by all employee
<b>   </b>	Send Cancel	

14. Aplique la directiva del grupo acaba de modificaa que fue creada o al grupo de túnel correcto. Haga clic al **grupo de túnel** en la trama izquierda.

🚰 Cisco ASDM 5	.1 for PIX - 10.89.129.147				
File Rules Se	earch Options Tools Wizards	Help			
Since (	Configuration Monitoring	Back Forward Sea	rch Refresh S	🗐 🧖 Save Help	Cisco Systems
Interfaces Security Policy NAT Security Policy NAT Clobal Objects Clobal Objects Properties	Configuration > VPN > General Configuration > VPN Wizard Client Update Client Upda	Tunnel Group     Manage VPN tunnel gr IPSec or WebVPN con     Name     Payroll     engineering     DefaultRAGroup     DefaultRAGroup     DefaultRAGroup     Group Delimiter:	oups. A VPN tunnel gr nection. Type Ipsec-ra ipsec-ra ipsec-ra ipsec-l2l	roup represents a connection s Group Policy Payroll engineering DftGrpPolicy DftGrpPolicy ng tunnel group names from th ted. Reset	e user name that
Configuration ch	anges saved successfully.		cisco NA	(2)	🗄 3/1 3/06 3:22:11 PM UTC

15. Elija al grupo de túnel que usted desea aplicar la directiva del grupo a y el tecleo edita.

🚰 Cisco ASDM 5.	.1 for PIX - 10.89.129.147				
File Rules Se	arch Options Tools Wizards He	qle			
Home C	Configuration Montoring Bas	ck Forward Sear	ch Refresh Sa	ve Help	Cisco Systems
Interfaces Security Policy NAT Security Policy Security Poli	Configuration - VFN - General - Tu Configuration - VFN - General - Tu Configuration - VFN - General - Tu Configuration - Tu	Annel Group  Manage VPN tunnel group  Manage VPN tunnel group  Pace or WebVPN conr  Name  Payroll  engineering DefaultRAGroup DefaultL2LGroup  Specify the delimeter to are received when tunn Group Delimiter:	bups, A VPN tunnel grou ection. Type ipsec-ra ipsec-ra ipsec-ra ipsec-l2l be used when parsing els are being negotiate None V Apply	up represents a connection : Group Policy payroll engineering DritOrpPolicy DritOrpPolicy g tunnel group names from the	specific record for a Add ▼ Edit Delete ne user name that
Configuration cha	anges saved successivily.		CIBCO NA (2	2/ 😅 🛄	ST306 3:22:31 PM 010

16. Si su directiva del grupo fue creada automáticamente (véase el paso 2), verifican que la directiva del grupo que usted acaba de configurar está seleccionada en la casilla desplegable. Si su directiva del grupo no fue configurada automáticamente, selecciónela de la casilla desplegable. Haga Click en OK cuando le hacen.

🔂 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	
Group Policy: payroll	
Strip the realm from username before passing it on to the AWA server	
Strip the group from username before passing it on to the AAA server	
OK Cancel Help	

- 17. El tecleo **se aplica** y, si está indicado, el tecleo **envía** para agregar el cambio a la configuración PIX.Si la directiva del grupo fue seleccionada ya usted puede ser que reciba un mensaje que no dice "ningún cambio fue hecho." Haga clic en OK.
- 18. Relance los pasos 2 a 17 para cualquier grupo de túnel adicional a quien usted quisiera agregar las restricciones. En este ejemplo de configuración, es también necesario restringir el acceso de los ingenieros. Mientras que el procedimiento es lo mismo, éstas son algunas ventanas en las cuales las diferencias son notables: Nueva lista de acceso 20

<b>1</b>	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	Latrice
	20								Delete
	1	V	<b>~</b>	🧇 any	A 192.168.1.0/24	😕 ip		Not Applied	Maustin
	2		<ul> <li>Ø</li> </ul>	🧇 any	10.8.27.0/24	🕑 ip		Not Applied	Move Op
									Move Down
1								<u> </u>	
1	Allo	iw traffic	8	Denytraffic					
					1				
				0	Cance	el	Help		

Elija la **lista de acceso 20** como filtro en la directiva del grupo de ingeniería.

Check an innent checkbox	to let the com	esponding setting take	its value from the default group p	oncy.
Tunneling Protocols:	🔽 Inherit	F IP.Sec		
Filter:	🗖 Inherit	20	Manage	
Connection Settings				
Access Hours:	Inherit		Vew	
Simultaneous Logins:	🔽 Inherit			
Maximum Connect Time	e: 🔽 Inherit	🗖 Unlimited	minutes	
Idle Timeout:	🔽 Inherit	☐ Unlimited	minutes	
Servers				
DNS Servers:	🔽 Inherit	Primary:	Secondary:	
WINS Servers:	🔽 Inherit	Primary:	Secondary:	
DHCP Scope:	Inherit			

Verifique que la directiva del grupo de ingeniería esté fijada para el grupo de túnel que dirige.

🔂 Edit Tunnel Group	×
Name: engineering Type: jipsec-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 AVA server	
Strip the group from username before passing it on to the AAA server	
OK Cancel Help	

## Configure el acceso vía el CLI

Complete estos pasos para configurar el dispositivo de seguridad usando el CLI:

**Nota:** Algunos de los comandos mostrados en esta salida se derriban a una segunda línea debido a las razones espaciales.

1. Cree dos diversas listas de control de acceso (15 y 20) que se apliquen a los usuarios mientras que conectan con el VPN de acceso remoto. Esta lista de acceso se invita más adelante en la configuración.

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
```

2. Cree a dos diversas agrupaciones de direcciones VPN. Cree uno para la nómina de pago y uno para los usuarios remotos de la ingeniería. ASAWCSC-CLI(config)#ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask 255.255.0

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

 Cree las directivas para la nómina de pago que se aplican solamente a ellas cuando conectan.

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. Este paso es lo mismo que el paso 3 a menos que esté para el grupo de ingeniería. 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. Cree a los usuarios locales y asigne los atributos que usted acaba de crear a esos usuarios para restringir su acceso a los recursos.

ASAwCSC-CLI(config)#username engineer password cisco123

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

 Cree a los grupos de túnel que contienen las directivas de la conexión para los usuarios de nómina.

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

 Cree a los grupos de túnel que contienen las directivas de la conexión para los usuarios de la ingeniería.

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

Una vez que le configuración ingresan, usted puede ver esta área resaltada en su configuración:

#### Nombre del 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
interface Ethernet0/1
nameif Engineer
security-level 100
ip address 192.168.1.1 255.255.255.0
1
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 esp-
sha-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
!
class-map inspection_default
match default-inspection-traffic
!
1
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)#
```

## **Verificación**

Utilice las capacidades de monitoreo del ASDM de verificar su configuración:

 Seleccione la supervisión > el VPN > los VPN statistics (Estadísticas de la VPN) > las sesiones.Usted ve a las sesiones de VPN activas en el PIX. Seleccione la sesión que usted está interesado adentro y haga clic los detalles.

Home Configuration Monitoring Ba	ack Forward S	Q Q iearch Refresh	🔜 🤶 Save Help	Cisco Systems
Moniforing > VPN > VPN Statistics	<ul> <li>Sessions</li> <li>Remote Access</li> </ul>	LAN-to-LAN	Total 0	Total Cumulative 1 3
Routing Sessions	Filter By: Remote A	ccess 💌 🗔 All Sess Group Policy	ions 💌	Filter Protocol Details
Properties	Username controller1	Tunnel Group DftGrpPolicy payroll	Public IP Address 10.8.27.50 172.22.1.165	Encryption IPSec 3DES Ping
	•   'o sait VPN sessions, Logout By: - All Se	right-click on the above ssions - •	Table and select Table	sort Order from popup menu. .ogout Sessions .ast Updated: 3/13/06 2:39:33 PM

 Seleccione la lengueta ACL.Los ACL hitcnt reflejan el tráfico que atraviesa el túnel del cliente a las redes permitidas.

Session Details					
Remote Detailed					
Usemame	Group Policy Tunnel Group	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Client Type Version
ontroller1	DfftGrpPolicy payroll	10.8.27.50 172.22.1.165	IPSec 3DES	20:35:08 UTC Mon Mar 13 2006 0h:09m:58s	WinNT 4.8.00.0440
The following a access-list 10, access-list 10 access-list 10 access-list 10 access-list 10 access-list 10	CL is being appli : 2 elements line 1 remark per line 2 extended p line 3 remark per line 4 extended p	ed to this session: mit IP access from ermit ip any 10.8.2 mit IP access from ermit ip any 10.8.2	ANY source to the j 8.0 255.255.255.0 ANY source to the : 7.0 255.255.255.0	payroll subnet (10.8.28.0 /2 (hitcnt=8) 0x25954260 subnet used by all employees (hitcnt=4) 0xd52617df	4) (10.8.27.0 /2
		Refresh	Close	Help	

## **Troubleshooting**

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## Información Relacionada

- Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 ASA como servidor VPN remoto que usa el ejemplo de la Configuración de ASDM
- Ejemplos de configuración y lista de notas técnicas del Dispositivos de seguridad Cisco PIX de la serie 500
- Ejemplos de configuración y lista de notas técnicas del Dispositivos de seguridad adaptable <u>Cisco ASA de la serie 5500</u>
- Ejemplos de configuración y lista de notas técnicas del Cliente Cisco VPN
- Soporte Técnico y Documentación Cisco Systems