PIX/ASA y cliente VPN para el Internet pública VPN en un ejemplo de configuración del palillo

Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados **Productos Relacionados Convenciones Antecedentes** Hairpinning o giro de 180 grados Configuraciones Diagrama de la red Configuración CLI del PIX/ASA Configure ASA/PIX con el ASDM Configuración de cliente VPN Verificación Verificación del cliente VPN Troubleshooting Información Relacionada

Introducción

Este documento describe cómo configurar un dispositivo de seguridad 7.2 ASA y posterior para realizar el IPSec en un palillo. Esta configuración se aplica a un caso específico, cuando ASA no permite la tunelización dividida y los usuarios se conectan directamente al ASA antes de que se les permita entrar a Internet.

Nota: En la versión 7.2 y posterior del PIX/ASA, la palabra clave de la intra-*interfaz* permite que todo el tráfico ingrese y salga la misma interfaz, y no apenas el tráfico IPSec.

Refiera al <u>router y al cliente VPN para el Internet pública en un ejemplo de configuración del palillo</u> para completar una configuración similar en un router del sitio central.

Refiera al Spoke-a-<u>cliente aumentado 7.x VPN del PIX/ASA con autenticación de TACACS+ el</u> <u>ejemplo de configuración</u> para aprender más sobre el escenario donde el eje de conexión PIX reorienta el tráfico del cliente VPN al spoke PIX.

Nota: Para evitar una coincidencia de los IP Addresses en la red, asigne un pool totalmente diverso de los IP Addresses al cliente VPN (por ejemplo, 10.x.x.x, 172.16.x.x, y 192.168.x.x). Este esquema de IP Addressing es útil para resolver problemas su red.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El dispositivo de seguridad del PIX/ASA del concentrador necesita funcionar con la versión 7.2 o posterior
- Cliente VPN de Cisco versión 5.x

Componentes Utilizados

La información en este documento se basa en versión 8.0.2 y Cliente VPN de Cisco versión 5.0 del dispositivo de seguridad PIX o ASA.

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 se puede también utilizar con la versión 7.2 y posterior del dispositivo de seguridad del Cisco PIX.

Convenciones

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

Antecedentes

Hairpinning o giro de 180 grados

Esta característica es útil para el tráfico VPN que ingrese una interfaz pero después se rutea fuera de esa misma interfaz. Por ejemplo, si usted tiene una red VPN del hub-and-spoke, donde está el concentrador el dispositivo de seguridad, y las redes VPN remotas es spokes, para que uno habló para comunicar con otro spoke, trafica debe salir en el dispositivo de seguridad y entonces otra vez al otro spoke.

Utilice el **comando same-security-traffic** de permitir que el tráfico ingrese y que salga la misma interfaz.

securityappliance(config)#same-security-traffic permit intra-interface

Nota: El hairpinning o el giro de 180 grados es aplicable para el cliente VPN a la comunicación del cliente VPN, también.

Configuraciones

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta <u>Command Lookup Tool</u> (<u>clientes registrados solamente</u>) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Public Internet

Configuración CLI del PIX/ASA

• <u>PIX/ASA</u>

Configuración de ejecución en el 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
1
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
1
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 !--- Configuration of group parameters for the VPN Clients. tunnel-group rtptacvpn general-attributes address-pool vpnpool

```
!--- Disable user authentication. authentication-server-
group none
!--- Bind group-policy parameters to the tunnel-group
for VPN Clients. default-group-policy clientgroup
tunnel-group rtptacvpn ipsec-attributes
pre-shared-key *
1
class-map inspection_default
match default-inspection-traffic
1
policy-map global_policy
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 esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
service-policy global_policy global
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0
: end
```

Configure ASA/PIX con el ASDM

Complete estos pasos para configurar Cisco ASA como servidor VPN remoto con el ASDM:

 Elija los Asisitente > al Asisitente del IPSec VPN de la ventana casera.

💏 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. Elija el tipo de túnel del **VPN de acceso remoto**, y asegúrese de que la interfaz del túnel VPN está fijada según lo

deseado.		
💏 VPN Wizard		×
VPN Wizard	VPN Tunnel Type (Step 1 of)	
a p	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 belecommuters is called remote access tunnel.	
Hor	This wizard creates basic tunnel configurations that you can edit later using the ASDM.	
Corporate	VPN Tunnel Type: Site to Site VPN	
THE H	C Site-to-Site	
	Remote Access Remote Access Remote Access	
R D	VPN Tunnel Interface:	
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-us authorization access lists still apply to the traffic.	ser
	≤Back Next> Einish Gancel	Help

3. Eligen al único tipo del cliente VPN disponible ya. Haga clic en Next

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.
	WPN Client Type:
(antipate)	Cisco VPN Client, Release 3.x or higher,
Network	or other Easy VPN Remote product
	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. PAP PC-CHAP PC MS-CHAP-V1 PC MS-CHAP-V2 PC EAP-PROXY
	Specify if the client will send tunnel group name as username@tunnelgroup;
- 1	Cient will send tunnel group name as username@turselgroup.
	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
	A Park Martha Cinich Cancel Hale

4. Ingrese un nombre para el Nombre de Grupo de Túnel. Suministre la información de autenticación que utilizará. La clave previamente compartida se elige en este ejemplo.

💏 VPN Wizard	×
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Branch ISP United Voterson Network	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
a la state	Certificate Name:
JUI	C Challenge/response authentication (CRACK)
	Tunnel Group
the second	Tunnel Group Name: rtptacvpn
	<u>≤Back N</u> ext> Einish ⊆ancel <u>H</u> elp

Nota: No hay una manera de ocultar/cifrar la clave previamente compartida en el ASDM. La razón es que el ASDM se debe utilizar solamente por la gente que configura el ASA o por la gente que ayuda al cliente con esta configuración.

5. Elija si desea que los usuarios remotos sean autenticados en las bases de datos de usuarios locales o en un grupo de servidores AAA externo.Nota: Agrega a los usuarios a las bases de datos de usuarios locales en el paso 6.Nota: Refiera a los grupos de servidores de la autenticación y autorización del PIX/ASA 7.x para los usuarios de VPN vía el ejemplo de la Configuración de ASDM para la información sobre cómo configurar a un Grupo de servidores AAA externo con el ASDM.

🙀 VPN Wizard	×
VPN Wizard	Client Authentication (Step 4 of)
An and An	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.
Corpola	 Authenticate using the local user database
THE THE	C Authenticate using an AAA server group
	AAA Server Group Name:
	<u>≤Back</u> <u>N</u> ext> Einish <u>C</u> ancel <u>H</u> elp

6. Agregue a los usuarios a la base de datos local, en caso necesario.Nota: No quite a los Usuarios usuarios actuales de esta ventana. Elija la configuración > Device Administration (Administración del dispositivo) > la administración > las cuentas de usuario en la ventana ASDM principal para editar las entradas existentes en la base de datos o para quitarlas de la base de

datos.

🚰 VPN Wizard			×
VPN Wizard	User Accounts (Step 5 of 11)		
	Add new users into the user authenti or to remove them from the database Users/AAA > User Accounts in the ma	cation database. To edit existing entries in the database e, go to Configuration > Device Management > ain ASDM window.	
Home	User to Be Added		
Corporato Network	Username:	stick	
	Password (optional):	Delete	
	Confirm Password (optional):		
		_≤Back Next> Einish Cancel Help	

 Defina un pool de las direcciones locales que se asignarán dinámicamente a los clientes de VPN remotos cuando se conectan.

📸 VPN Wizard	\mathbf{x}
VPN Wizard	Address Pool (Step 6 of 11)
	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.
Corporate Network	Tunnel Group Name : rtptacvpn
The said	Pool Name: Vpnpool New
	Pool Settings
	Range Start Address: 192,168,10,1
	Range End Address: 192,168,10,254
	Subnet Mask: 255.255.255.0
	<u> < Back N</u> ext > <u>Einish</u> <u>Cancel</u> <u>H</u> elp

8. *Opcional:* Especifique la información de servidor DNS y WINS y un Nombre de Dominio Predeterminado que se avanzará a los clientes de VPN remotos.

🛃 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.
Comporte)	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></u> ancel <u>_</u>

 Especifique los parámetros para el IKE, también conocidos como fase 1. IKE.Las configuraciones a ambos lados del túnel deben hacer juego exactamente, pero el Cliente Cisco VPN elige automáticamente la configuración adecuada para sí mismo. No hay configuración IKE necesaria en PC del cliente.

💏 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	177-177 0-0-010
	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.	
Corporato	Encryption: 3DES Authentication: SHA	
	DH Group:	
		elp

10. Especifique los parámetros para el IPSec, también conocidos como fase 2 IKE.Las configuraciones a ambos lados del túnel deben hacer juego exactamente, pero el Cliente Cisco VPN elige automáticamente la configuración adecuada para sí mismo. No hay configuración IKE necesaria en PC del cliente.

💏 VPN Wizard	×
VPN Wizard	IPsec Encryption and Authentication (Step 9 of 11)
	Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.
Carbonnin (Encryption: SDES Authentication: SHA:

11. Especifique cuál, eventualmente, se pueden exponer los host internos o las redes a los usuarios de VPN remotos. Si deja esta lista vacía, permita que los usuarios de VPN remotos acceden a la red interna completa del ASA. Puede también habilitar la tunelización dividida en esta ventana. La tunelización dividida encripta el tráfico a los recursos definidos anteriormente en este procedimiento y proporciona el acceso no cifrado a Internet en general al no tunelizar ese tráfico. Si la tunelización dividida no se habilita, todo el tráfico de los usuarios de VPN remotos se tuneliza al ASA. Éste puede convertirse en un gran ancho de banda y hacer un uso intensivo del procesador, sobre la base de su configuración.

PN Wizard	Address Translation Exemption and Split Tur	ineling (Optional) (Step 10 of 11)
	Network Address Translation (NAT) is used to hide make exceptions to NAT to expose the entire or p users protected by VPN. To expose the entire network behind the most se leave the selection list blank.	e the internal network from outside users. You car art of the internal network to authenticated remo cure interface to remote VPN users without NAT,
(Network	Host/Network	Selected Hosts/Networks: any
	Interface: Inside	Add
The state	Address: Jany:	Delete
C.A	Enable split tunneling to let remote users hav defined above, and unencrypted access to the	e simultaneous encrypted access to the resources te internet.

12. Esta ventana muestra un resumen de las acciones que ha realizado. Haga clic en **Finalizar** si está satisfecho con la configuración.



13. Configure el comando same-security-traffic de habilitar el tráfico entre dos o más host conectados con la misma interfaz cuando usted hace clic el checkbox como se muestra:

Home Configuration	Monitoring	resh G Back	C) Forwe	rd 🦻 H	elp	1	cisco
)evice Setup 🗇 ਦ 兴	Configuration > Device !	Setup > Interfa	ces				۵
Startup Wizard	Interface	Name	Enabled	Security Level	IP Address	Si	Add 👻
O Davida Nama/Darbursed	Ethernet0	outside	Yes	0	172.18.124.98	255.2	Edt.
Suctan Time	Ethernet1	inside	Yes	100	172.16.3.101	255.2	EOU.
e 🕓 System nine	Ethernet2		No	1		1.1.	Contration
	Ethernet3		No	-			rania
	Ethernet4		No			1	
	Ethernet5		No	1.		1.1	
3 Device Setup							
Device Setup	Image: Section 1.1 Image: Section 1.1 Image: Section						
Device Setup Firewall							
Device Setup Firewall Remote Access VPN Ste-to-Site VPN	■ I Enable traffic between	two or more interf	faces which a	are configure	ed with same secu	rity levels	

 Elija las reglas de la configuración > del Firewall >NAT, y el tecleo agrega la regla dinámica NAT para crear esta traducción dinámica con el uso del 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 1 Delete Ø 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 s
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. Elija el **interior** como la interfaz de origen, y ingrese los direccionamientos que usted quiere al NAT. Para el direccionamiento Translate en la interfaz, elija **afuera** y haga clic la **AUTORIZACIÓN**.

terface:	inside	•	
urce:	0.0.0.0	_	
slated -			
lect a glo	obal pool for dynamic translatio	n.	
Pool II) Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
1	outside	172.18.124.166	Manage
nnectio	n Settings		
meeco	n secongs		

16. Elija el **exterior** como la interfaz de origen, y ingrese los direccionamientos que usted quiere al NAT. Para el direccionamiento Translate en la interfaz, elija **afuera** y haga clic la

AUTORIZACIÓN.

ource:	192.168.10.0	-	
nslated -			
elect a gl	obal pool for dynamic translation	h.	
Pool I	D Interface	Addresses Pool	
0	(outbound) (inbound)	Same as original address (identity) Same as original address (identity)	
1	outside	172.18.124.166	Manage
1	putsite	j函 1/2.10.124.100	

17. La traducción aparece en las Reglas de traducción en las **reglas de la configuración > del Firewall**

>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> i	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 🛉 🗲 👗	Ba 🚓 - Q. Find	E Diagram	: Trace
📇 10.77.241.143 🔝 172.16.3.101	Filter: Ori	ginal Source	• 6 •	n	- File	Clear 🔀
				Original		Translated
	#	Туре	Source	Destination Se	ervice Interface	Address
	🖂 inside			In the second second second		
	1	Dynamic	🔜 0.0.0.0		outside	172.18.124.
	2	Dynamic	192.168.10.0		outside	172.18.124
-tga Objects - 🛃 Advanced						
Device Setup						
💑 Firewall	•					Þ
Remote Access VPN			.0 0000	172 18 124	166	×
Site-to-Site VPN	Est	Laffie Manual II		Dynamic	Destination Ad	dress
Device Management) Enable	e tranfic through th	e nrewali without address b	ansiación		
*			Ap	ply Reset		

Nota 1: El comando de permiso-<u>VPN de la conexión del sysopt</u> necesita ser configurado. <u>El</u> <u>comando show running-config sysopt</u> verifica si se configura.

Nota 2: Agregue esta salida para el transporte opcional UDP:

group-policy clientgroup attributes vpn-idle-timeout 20 **ipsec-udp enable ipsec-udp-port 10000**

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

Nota 3: Configure este comando en la configuración global del Dispositivo de PIX para que los clientes VPN conecten vía el IPSec sobre el TCP:

isakmp ipsec-over-tcp port 10000

Nota: Refiera a la <u>Conexión mediante pines en el</u> vídeo de <u>Cisco</u> ASA para más información sobre diversos escenarios donde la conexión mediante pines puede ser utilizada.

Configuración de cliente VPN

Complete estos pasos para configurar al cliente VPN:

1. Elija

status: Disco	nnected VP	N Client - Versi	on 5.0.03.0530	
Connection Entries	Status Certific	ates Log Options	s Help	
Connect N	ew Impo	a 🏹 rt Modify	Delete	cisco
Connection Entries	Certificates	Log		
Con	nection Entry /	<u>(</u>	Host	Transport

2. Ingrese el nombre del IP Address y de grupo de túnel de la interfaz exterior PIX junto con la contraseña para autenticación.

VPN Client	Create New VPN Connec	tion Entry	
Connection Entry: pix	1		
Description: pix	on stick for internet access		ululu cisco
Host: 17.	18.124.98		
Authentication T	ransport Backup Servers	Dial-Up	
Group Authentic	ation	Mutual Group.	Authentication
Name:	rtptacvpn		
Password:	*****		
Confirm Password	. ******		
C Certificate Authe Name:	ntication Ticate Chain		
Erase User Password	ł	Save	Cancel

3. (*Opcional*) haga clic el **Tunelización transparente del permiso** bajo transporte cuadro (esto es opcional y requiere la configuración adicional del PIX/ASA mencionada en la <u>nota</u>

				(
Connection Entry:	pix1			
Description:	pix on a stick f	for internet connecti	on	CISCO
Host:	172.18.124.98	}		
Authentication	Transport	Backup Servers	Dial-Up	
Enable Trans	parent Tunnel	ing		
IPSec over	UDP (NAT /	PAT)		
C IPSec over	r TCP	TCP Port: 10000		
Allow Local L	AN Access			
Peer response tin	neout (second	s): 90		
F 11 P	.l			1
Erase User Passy	vord		Save	Cancel

4. Salve el perfil.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- show crypto isakmp sa: muestra las asociaciones de seguridad IKE (SAs) actuales en una par.
- <u>muestre IPSec crypto sa</u> Visualiza todos los SA actuales. Look for cifra y desencripta los paquetes en el SA que definen el tráfico del cliente VPN.

Intente hacer ping u hojear a un IP Address público del cliente (por ejemplo, www.cisco.com).

Nota: La interfaz interior del PIX no se puede hacer ping para la formación de un túnel a menos que el comando del <u>Acceso de administración</u> se configure en el modo de configuración global.

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

Verificación del cliente VPN

Complete estos pasos para verificar al cliente VPN.

- 1. Haga clic con el botón derecho del ratón en el icono del bloqueo del cliente VPN presente en la bandeja del sistema después de una conexión satisfactoria y elija la opción para estadísticas de ver cifra y desencripta.
- 2. Haga clic en la lengueta de los detalles de la ruta para no verificar la ninguna lista de túnel dividido pasajera abajo de la aplicación.

Troubleshooting

Nota: Para más información sobre cómo resolver problemas los problemas VPN, refiera a las soluciones del troubleshooting VPN.

Información Relacionada

- Ejemplo aumentado de la configuración VPN del Spoke-a-cliente para la versión 7.0 del dispositivo de seguridad PIX
- <u>Cliente de Cisco VPN</u>
- <u>Negociación IPSec/Protocolos IKE</u>
- <u>Cisco PIX Firewall Software</u>
- <u>Referencias de Comandos de Cisco Secure PIX Firewall</u>
- Avisos de campos de productos de seguridad (incluido PIX)
- <u>Conexión mediante pines en Cisco ASA</u>
- <u>Solicitudes de Comentarios (RFC)</u>
- Soporte Técnico y Documentación Cisco Systems