ASA/PIX: IP estático dirigiendo para el cliente del IPSec VPN con el CLI y el ejemplo de la Configuración de ASDM

Contenido

Introducción prerrequisitos Requisitos **Componentes Utilizados Productos Relacionados Convenciones** Configurar Diagrama de la red VPN de acceso remoto de la configuración (IPSec) Configurar ASA/PIX con la CLI Configuración de Cliente Cisco VPN Verificación Comandos show Troubleshooting Borre las asociaciones de seguridad Comandos para resolución de problemas Información Relacionada

Introducción

Este documento describe cómo configurar el dispositivo de seguridad adaptante de las Cisco 5500 Series (ASA) para proporcionar el IP Address estático al cliente VPN con el Administrador de dispositivos de seguridad adaptante (ASDM) o el CLI. El ASDM ofrece administración de seguridad de talla mundial y monitoreo a través de una Interfaz de administración basada en la Web intuitiva, fácil de utilizar. Una vez que la configuración de ASA de Cisco es completa, puede ser verificada con el Cliente Cisco VPN.

Consulte el Ejemplo de Configuración de Autenticación <u>PIX/ASA 7.x y Cisco VPN Client 4.x con</u> <u>Windows 2003 IAS RADIUS (en comparación con Active Directory)</u> para instalar la conexión VPN de acceso remoto entre Cisco VPN Client (4.x para Windows) y PIX 500 Series Security Appliance 7.x. El usuario de cliente VPN remoto autentica contra el Active Directory con un servidor de RADIUS del Internet Authentication Service de Microsoft Windows 2003 (IAS).

Refiera al <u>PIX/ASA 7.x y al Cliente Cisco VPN 4.x por el ejemplo de la configuración de</u> <u>autenticación del Cisco Secure ACS</u> para configurar una conexión VPN de acceso remoto entre un Cliente Cisco VPN (4.x para Windows) y el dispositivo de seguridad 7.x de la serie PIX 500 con un Cisco Secure Access Control Server (ACS versión 3.2) para el Autenticación ampliada (Xauth).

prerrequisitos

Requisitos

Este documento asume que el ASA está completamente operativo y está configurado para permitir que el ASDM de Cisco o el CLI realice los cambios de configuración.

Nota: Consulte <u>Cómo Permitir el Acceso HTTPS para el ASDM</u> o el <u>PIX/ASA 7.x: SSH en el</u> <u>Ejemplo de Configuración de las Interfaces Interiores y Exteriores</u> para permitir que el dispositivo sea configurado remotamente por el ASDM o el Secure Shell (SSH).

Componentes Utilizados

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

- Cisco Adaptive Security Appliance Software Version 7.x y posterior
- Adaptive Security Device Manager Version 5.x y posterior
- Cisco VPN Client Version 4.x y posterior

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 usar con Cisco PIX Security Appliance Version 7.x y posterior.

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco</u> para obtener más información sobre las convenciones del documento.

Configurar

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

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

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son los direccionamientos del RFC 1918, que fueron utilizados en un ambiente de laboratorio.

VPN de acceso remoto de la configuración (IPSec)

Procedimiento del ASDM

Complete estos pasos para configurar el VPN de acceso remoto:

 Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > IPSec > las políticas IKE > Add para crear una política isakmp.

🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111			
File View Tools Wizards Wi	ndow Help		
Home 🕞 Configuration	Monitoring 🔚 Save 🔇 Refi	resh 🚫 Back 🚫 Forwa	rd 💡 Help
Remote Access P X Introduction Network (Client) Access AnyConnect Connection IPsec Connection Profile Group Policies Dynamic Access Policie Address Assignment Advanced Schutz Advanced Schutz Advanced D Schutz Access Comto Mans	Configuration > Remote A Configure specific Internet	ccess VPN > Network (Key Exchange (IKE) algorith	Client) Access > Advance ms and parameters, within t Hash
IKE Policies			

2. Proporcione los detalles de la política isakmp.

🕵 Add IKE Polic	y			
Priority:	2	Authentication:	pre-share 🔽	
Encryption:	des 💌	D-H Group:	2 🗸	
Hash:	sha 💌	Lifetime:	Unlimited86400	seconds 💌
		Cancel	Help	

El Haga Click en OK y **se aplica**.

3. Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > IPSec > los parámetros IKE para habilitar el IKE en la interfaz

exterior.					
🚰 Cisco ASDM 6.1 for ASA -	🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111				
File View Tools Wizards Win	dow Help				
🚯 Home 🚳 Configuration 📴 N	fonitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help				
Remote Access d P ×	Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Parameters				
Introduction Network (Client) Access	Enable IKE NAT Transparency				
- AnyConnect Connection	Interface IKE Enabled Enable Enable IPsec over NAT-T				
Group Policies	draz No NAT Keepalive: 20 seconds				
Address Assignment	outside Yes Enable IPsec over TCP				
E-B Advanced	Enter up to 10 comma-separated TCP port				
B-BSSL VPN	values (1- 65535):				
Psec	10000				
-% IKE Policies					
IKE Parameters	Identity to Be Sent to Peer				
Psec Prefragme					
🖲 🗟 Certificate to Co	Identity: Automa M Key id String:				
Joint Content of					
System Options	Disable inbound aggressive mode connections				
- Manager					
AAA/Local Users	Alert peers before disconnecting				
Secure Desktop Manager	Wait for all active sessions to voluntarily terminate before rebooting				

4. Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > IPSec > IPSec transforman los conjuntos > Add para crear el ESP-DES-SHA transforman el conjunto, como se

1	🖆 Add Transform Set	×
	Set Name: ESP-DES-SHA	
	Properties	
	Mode: 💿 Tunnel 🔵 Transport	
	ESP Encryption: DES	
	ESP Authentication:	
	Cancel Help	

El Haga Click en OK y **se aplica**.

5. Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > avanzó > IPSec > las correspondencias de criptografía > Add para crear una correspondencia de criptografía con la directiva dinámica de la prioridad 1, como se muestra.

🖆 Create IPsec Rule	
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
Interface: outside 💙 Policy Type: dynamic 💙	Priority: 1
Transform Sets Transform Set to Be Added: ESP-DES-MD5	Move Up
Remove	
Peer Settings - Optional for Dynamic Crypto Map Entries The Connection Type is applicable to static tunnel policies only. Uni-directional connection for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may redundant peers.	n type policies are used specify up to 10
OK Cancel Help	

El Haga Click en OK y **se aplica**.

 Elija la configuración > el VPN de acceso remoto >AAA ponen > los usuarios locales > Add para crear la cuenta de usuario (por ejemplo, nombre de usuario - cisco123 y contraseña cisco123) para el acceso de cliente VPN.

🖆 Add User Account			
Identity			
-VPN Policy	Username:	cisco123	
	Password:	****	
	Confirm Password:	*****	
	User authentica	ated using MSCHAP	
	Access Restriction		
	Select one of the	options below to restrict ASDM, SSH, Telnet and Conso	ole access.
	Note: All users have network access, regardless of these settings.		
	 Full access(ASDM, SSH, Telnet and Console) 		
	Privilege level is used with command authorization.		
	Privilege Le	evel: 2	
	🚫 CLI login pron	mpt for SSH, Telnet and console (no ASDM access)	
	This setting	g is effective only if AAA authenticate console command	l is configured.
	🚫 No ASDM, SSI	H, Teinet or Console access	
	This setting	g is effective only if AAA authenticate console command	is configured.
Find:		🔘 Next 🛛 🔘 Previous	
	(OK Cancel Help	

7. Vaya a la **política del VPN** y agregue el **estático/dedicó la dirección IP** para el usuario el "cisco123," como

sigue.						
🖆 Cisco ASDA 6.1 for ASA	- 10.77	7.241.111				
File View Tools Wizards W	Vindow H	Help				
Home 🚱 Configuration 💆	Monitorin	ng 🔚 Save 💽 Refresh	🚱 Back 🔘 Forward 🦻 Help 🖉			
Remote Access	Config	uration > Remote Acces	s <u>VPN > AAA/Local Users > Local</u>	Users		
Network (Client) Access	Crea	add User Accour	1			
Prec Connection Profiles	Con	r -identity	Check an Inherit checkbox to let th	e correspond	ling setting take its value	from the
Dynamic Access Policies	AAA	Contraction of the second	Group Policy:	🖌 Inherit		
Address Assignment	Use	6	Tunneling Protocols:	🖌 Inherit	Clientiess SSL VPN	SSL
Address Pools Advanced	ena		Filter:	🗹 înherit		
- SL VPN Access - SL VPN Access			Tunnel Group Lock:	🗹 Inherit		
- AAA Server Groups - A LDAP Attribute Map			Store Password on Client System:	🖌 Inherit	Ves ONo	
- Clocal Users - A Secure Desktop Manager			Connection Settings			
Certificate Management			Access Hours:	🖌 înherit		
- Stoad Balancing			Simultaneous Logins:	🖌 Inherit		
- DNS			Maximum Connect Time:	🖌 Inherit	Unlimited	Minute
, agriatation			Idle Timeout:	🗹 înherit	Unlimited	Minute
			Dedicated IP Address (Optional)			-
			IP Address: 192.168.5.1	Subnet Mask	: 255.255.255.0	
			L)

8. Elija la configuración > el VPN de acceso remoto > el acceso > la asignación de dirección >

a las agrupaciones de direcciones de la red (cliente) y el tecleo agrega para agregar al cliente VPN para los usuarios de cliente

VPIN.		
😭 Cisco ASDM 6.1 for ASA	- 10.77.241.111	
File View Tools Wizards Wi	ndow Help	
🔥 Home 🔏 Configuration 📴 I	Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help	
Remote Access D P ×	Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Por Configure named IP Address pools.	oks
AnyConnect Connection Pr Psec Connection Profiles Group Policies	This parameter is enforced in either a VPN <u>Psec Connection Profiles</u> , <u>AnyConnect Connection Profiles</u> or <u>Group Pc</u>	
	Pool Name Star	es
Advanced Clientless SSL VPN Access AAA/Local Users AAA/Local Users	Starting IP Addre 192.168.5.10	
Certificate Management	Ending IP Address: 192.168.5.100	
- B DHCP Server - M DNS - Advanced	Subher Mask:	
	OK Cancel Help	

 Elija la configuración > el acceso del VPN de acceso remoto > de la red (cliente) > conexión IPSec perfila > Add para agregar a un grupo de túnel (por ejemplo, TunnelGroup1 y el preshared cierran como cisco123), como se

muestra.					
File View Tools Wizards Window He	dp.			Look For:	
Home 🆓 Configuration 🔯 Monitori	ng 🔚 Save 🔇 Refresh 🄇	🔁 Back 🔘 Forward 🧳 H	elp		
Remote Access VPN P ×	Configuration > Remote Acce Access Interfaces	ess VPN > Network (Client) Ar	cess > IPsec Conne	ction Profiles	
AnyConnect Connection Profiles	Enable interfaces for IPsec a	ccess.			
IPsec Connection Profiles	Interface	Alow A	ccess		
- Provide Prov	dmz				
Address Assignment	inside				
E-B Clentless SSL VPN Access					
De AAA/Local Users					
😐 👸 Secure Desktop Manager	Constanting Desides				
Certificate Management	Connection Profiles	un) matilian hau una is suthant	centred and other manage	akara	
- Load Balancing	Connection pronie (cunnel gro	up) specifies now user is auchenc	icated and other parali	ecers.	
- P DHCP Server	🕈 Add 📈 Edit 📋 Da	lete			
DNS Advanced	Name	IPsec Enabled	L2TP/IPsec	Enabled	Autentication
III ag novances	DefaultWEBVPNGroup	✓			LOCAL
	DefaultRAGroup	V	N N		LOCAL
Cal Remote Acress VPN					
Site-to-Site VPN					
🔯 ies					
Device Management					
»			Apply Re:	set	

Bajo lengueta **básica**, elija al grupo de servidores como **LOCAL** para el campo de la autenticación de usuario.Elija **vpnclient1** como los pools de la dirección cliente para los usuarios de cliente

VPN.

🐴 Home 🥵 Configuration 🔯 Monitoring 🔚 Save	🚱 Refresh 🚺 🚱 Back 🧯	Forward 🦓 Help	
Remote Access	emote Access VPN > Net	twork (Client) Access > IPsec Connection P	rofiles
? Introduction			
Network (Client) Access 🛛 🌆 Add IPsec Remo	te Access Connectio	n Profile	
- AnyConnect Connection			
IPsec Connection Profile	Name:	TunneiGroup1	
Group Policies		Torreid cope	
	IKE Peer & thentication		<u></u>
E-Sp Address Assignment		(
Assignment Policy	Pre-shared Key:	*****	
Address Pools		(-
B-B Advanced	Identity Certificate:	None Y	Manage
AAA/LOCAL OSETS	User Authentication —		
- Se LDAR Attribute Man	Server Group:	LOCAL	Manage
- Contract Users	Server Group:	Evone (1)	_ manage
	Falback:	Use LOCAL if Server Group fails	
	Client Address Assignm	nent	
P DHCP Server	DHCP Servers:		
	Client Address Pools	vonclient1	Select.
- 💀 Advanced		(iprenerice	Concert
	Default Crown Ballion		
	Default Group Folicy		
	Group Policy:	DfltGrpPolicy 💙	Manage
		(Following fields are attributed of the group polic	y selected a
			,
		Enable IPsec protocol	
		Enable L2TP over IPsec protocol	

Haga clic en OK.

10. Elija avanzado > cliente que dirige y marque la casilla de verificación de la agrupación de direcciones del uso para asignar la dirección IP a los clientes VPN.Nota: Aseegurese desmarcar las casillas de verificación para el servidor de autenticación del uso y utilizar el DHCP.

🚰 Add IPsec Remote Acces	ess Connection Profile	
Global General General Authentication Authorization Accounting D-IPsec PPP	I Client Address Assignment Policy is policy affects all Network (Client) Access connections. The fol ler until an address is found. Use authentication server Use DHCP Use address pool ace-Specific Address Pools Add C Edit C Delete Interface Address Pools	llowing are tried in
Find:	OK Cancel Help	
	Con Cancer Help	

Haga clic en OK.

11. Habilite la **interfaz exterior** para el acceso del IPSec. El tecleo **se aplica** para proceder.

🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111			
File View Tools Wizards Wi	ndow Help		
Home 😪 Configuration 📝	Monitoring 🔚 Save 🔇 Refresh 🔇 B	ack 🚫 Forward 💡 Help	
Remote Access D P × Introduction Network (Client) Access AnyConnect Connection Profiles Connection Profiles Dynamic Access Policies Address Assignment Policy Address Pools Address Pools Address SSL VPN Access AAA/Local Users AAA/Local Users AAA/Local Users AAA/Local Users AAA/Local Users Certificate Management Cortificate Management Cartificate Management Cartificate Management Cartificate Management Cartificate Management DHCP Server DNS Advanced	Configuration > Remote Access VPN Access Interfaces Enable interfaces for IPsec access. Interface Allow outside annotation dmz inside Connection Profiles connection profile (tunnel group) specie	Network (Client) Access > IPsec Conne Access Access Fies how user is authenticated and other paramer IPsec Enabled V	

Configurar ASA/PIX con la CLI

Complete estos pasos para configurar al servidor DHCP para proporcionar los IP Addresses a los clientes VPN de la línea de comando. Consulte <u>Configuración de VPN de Acceso Remoto</u> o Referencias de Comandos de <u>Cisco ASA 5500 Series Adaptive Security Appliance</u> para obtener más información sobre cada uno de los comandos.

Configuración corriente en el dispositivo ASA
ASA# sh run
ASA Version 8.0(2)
!
<i>! Specify the hostname for the Security Appliance.</i>
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! ! Configure the outside and inside
<i>interfaces</i> . interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 ! Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1

--- Specify the location of the ASDM image for ASA to fetch the image for ASDM access. asdm image disk0:/asdm-613.bin no asdm history enable arp timeout 14400 global (outside) 1 192.168.1.5 nat (inside) 0 access-list 101 nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policyrecord DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto dynamic-map outside_dyn_map 1 set transform-set ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp dynamic outside_dyn_map !--- Specifies the interface to be used with !--- the settings defined in this configuration. crypto map outside_map interface outside !--- PHASE 1 CONFIGURATION ---! !--- This configuration uses ISAKMP policy 2. !---The configuration commands here define the Phase !--- 1 policy parameters that are used. crypto isakmp enable outside crypto isakmp policy 2 authentication pre-share encryption des hash sha group 2 lifetime 86400 no crypto isakmp nat-traversal !--- Specifies that the IP address to the vpn clients are assigned by the local and not by AAA or dhcp. The CLI vpn-addr-assign local for VPN address assignment through ASA is hidden in the CLI provided by show run command. no vpn-addr-assign aaa no vpn-addr-assign dhcp telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list 1 class-map inspection_default match default-inspection-traffic 1 policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map 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
1
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal
!--- In order to identify remote access users to the
Security Appliance, !--- you can also configure
usernames and passwords on the device. !--- specify the
IP address to assign to a particular user, use the vpn-
framed-ip-address command !--- in username mode
username cisco123 password ffIRPGpDSOJh9YLq encrypted
username cisco123 attributes
 vpn-framed-ip-address 192.168.5.1 255.255.255.0
!--- Create a new tunnel group and set the connection !-
-- type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

Configuración de Cliente Cisco VPN

Intente conectar con Cisco ASA con el Cliente Cisco VPN para verificar que el ASA está configurado con éxito.

- 1. Elija el Start (Inicio) > Programs (Programas) > Cisco Systems VPN Client (VPN Client de Cisco Systems) > al cliente VPN.
- 2. Tecleo nuevo iniciar la nueva ventana de entrada de la conexión VPN del



crear.

3. Complete la información de su nueva conexión.Ingrese el nombre del Entrada de conexión junto con una descripción. Ingrese el IP Address externo del ASA en el rectángulo del host. Entonces ingrese el nombre de grupo de túnel VPN (TunnelGroup1) y la contraseña (clave previamente compartida - cisco123) como está configurado en el ASA. Haga clic en Save

VPN Client Create New VPN Connect	tion Entry	X
Connection Entry: ASA		
Description: vpntunnel		cisco
Host: 192.168.1.1		
Authentication Transport Backup Servers	Dial-Up	
Group Authentication	C Mutual Group	Authentication
Name: TunnelGroup1		
Password: ******		
Confirm Password: ******		
C Certificate Authentication Name: Send CA Certificate Chain		
Erase User Password	Save	Cancel

(Guardar).

4. Haga clic la conexión que usted quiere utilizar, y el tecleo **conecta de la** ventana principal del cliente

status: Connected VPN Client - Version	ersion 5.0.03.0530		
Connection Entries Status Certificates Log	Options Help		
Connect New Import Mo	adiy Delete	ili Cis	ulu sco
Connection Entries Certificates Log	Host	Transport	
			and the second second
) ASA	192.168.1.1	IPSec/UDP	
ASA	192.168.1.1	IPSec/UDP	

5. Cuando se le pregunte, ingrese el **nombre de usuario: cisco123** y **contraseña: cisco123** como está configurado en el ASA para el Xauth, y **AUTORIZACIÓN del** tecleo a conectar

VPN Client 1	User Authentication for "ASA"
The server has reques authentication.	sted the following information to complete the user
	cisco123
cisco Password:	*******

6. El cliente VPN está conectado con el ASA en el sitio

central.				
🥔 statu	is: Connected VPN Client - Version	5.0.03.0530		
Connecti	on Entries Status Certificates Log Options	Help		
Disconn	nect New Import Modity	Delete		diada cisco
Connect	ion Entries Certificates Log			
	Connection Entry	Host	Transport	
8	ASA	192.168.1.1	IPSec/UDP	
1				
Connecte	ed to "ASA".	C	onnected Time: 0 day(s), 00:01.18	•

 Una vez que la conexión se establece con éxito, elija las estadísticas del menú Status (Estado) para verificar los detalles del túnel.

🥔 statu	s: Connected VPN Client - Version	5.0.03.0530	
Connectio	n Entries Status Certificates Log Options	Help	
Disconne Connectio	ect N Reset Stats	Delete	cisco
	Connection Entry	Host	Transport
0	ASA	192.168.1.1	IPSec/UDP

Verificación

Comandos show

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 todas las asociaciones actuales de seguridad IKE (SA) de un par.
- muestre IPSec crypto sa Muestra las configuraciones usadas por los SA actuales.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración. También se muestra un ejemplo de salida del debug .

Nota: Para más información sobre el IPSec VPN del Acceso Remoto del troubleshooting refiera la mayoría del IPSec VPN común L2L y del Acceso Remoto que resuelve problemas las soluciones.

Borre las asociaciones de seguridad

Cuando usted resuelve problemas, aseegurese borrar las asociaciones de seguridad existentes después de que usted realice un cambio. En el modo privilegiado del PIX, utilice estos comandos:

- clear [crypto] ipsec sa Borra el IPSec activo SA. La palabra clave crypto es opcional.
- clear [crypto] isakmp sa Borra el IKE activo SA. La palabra clave crypto es opcional.

Comandos para resolución de problemas

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.

Nota: Consulte <u>Información Importante sobre Comandos de Debug</u> antes de usar un **comando debug**.

- debug crypto ipsec 7 Muestra negociaciones IPsec de la Fase 2.
- debug crypto isakmp 7 Muestra negociaciones ISAKMP de la Fase 1.

Información Relacionada

- Página de Soporte de Cisco ASA 5500 Series Adaptive Security Appliances
- Referencias de comandos del Dispositivos de seguridad adaptable Cisco ASA de la serie
 <u>5500</u>
- Página de Soporte de Cisco PIX 500 Series Security Appliances
- Referencia de comandos del Dispositivos de seguridad Cisco PIX de la serie 500

- <u>Cisco Adaptive Security Device Manager</u>
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Página de soporte para cliente Cisco VPN
- <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>Solicitudes de Comentarios (RFC)</u>
- Soporte Técnico y Documentación Cisco Systems