PIX/ASA como servidor VPN remoto con la autenticación ampliada usando el CLI y el ejemplo de la Configuración de ASDM

Contenido

Introducción prerrequisitos Requisitos **Componentes Utilizados Productos Relacionados Convenciones Antecedentes** Configuraciones Configuración de ASA/PIX como Servidor VPN Remoto Usando ASDM Configuración de ASA/PIX como Servidor VPN Remoto Usando CLI Configuración de Almacenamiento de Contraseña de Cisco VPN Client Inhabilite la Autenticación Ampliada Verificación Troubleshooting **Crypto ACL Incorrecto** Información Relacionada

Introducción

Este documento describe cómo configurar el Cisco 5500 Series Adaptive Security Appliance (ASA) para que funcione como servidor VPN remoto usando el Adaptive Security Device Manager (ASDM) o 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 Cisco ASA es completa, puede ser verificada usando el Cisco VPN Client.

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 remoto de VPN Client se autentica contra el Active Directory usando un servidor RADIUS de Internet Authentication Service de Microsoft Windows 2003 (IAS).

Consulte el Ejemplo de Configuración de Autenticación de <u>PIX/ASA 7.x y al Cisco VPN Client 4.x</u> <u>para Cisco Secure ACS</u> para configurar una conexión VPN de acceso remoto entre un Cisco VPN Client (4.x para Windows) y el PIX 500 Series Security Appliance 7.x usando un Cisco Secure Access Control Server (ACS versión 3.2) para la 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.

Antecedentes

Las configuraciones del acceso remoto proporcionan el acceso remoto seguro para los clientes de Cisco VPN, tales como usuarios móviles. Una VPN de acceso remoto permite que los usuarios remotos accedan de forma segura a los recursos de red centralizada. El Cisco VPN Client cumple con el Protocolo IPSec y se está diseñado específicamente para funcionar con el dispositivo de seguridad. Sin embargo, el dispositivo de seguridad puede establecer las conexiones de IPSec con muchos clientes compatibles con el protocolo. Consulte <u>Guías de configuración ASA</u> para más información sobre el IPSec.

Los grupos y los usuarios son conceptos fundamentales en la administración de seguridad de los VPN y en la configuración del dispositivo de seguridad. Especifican los atributos que determinan el acceso de los usuarios y el uso de VPN. Un grupo es un conjunto de usuarios considerado una sola entidad. Los usuarios consiguen sus atributos de las políticas del grupo. Los grupos de túnel identifican la política del grupo para las conexiones específicas. Si no asigna una política del

grupo determinado al los usuarios, la política del grupo predeterminado para la conexión se aplica.

Un grupo de túnel consiste en un conjunto de registros que determina las políticas de conexión del túnel. Estos registros identifican los servidores para los que los usuarios del túnel son autenticados, y los servidores de contabilidad, de haber alguno, a los que se envía la información de las conexiones. Ellos también identifican una política de grupo predeterminada para las conexiones, y contienen los parámetros de la conexión específicos del protocolo. Los grupos de túnel incluyen una pequeña cantidad de atributos que pertenece a la creación del túnel mismo. Los grupos de túnel incluyen un indicador a una política del grupo que define los atributos orientados hacia el usuario.

Nota: En el ejemplo de configuración de este documento, las cuentas de usuario local se utilizan para la autenticación. Si desea utilizar otro servicio, tal como LDAP y RADIUS, consulte <u>Configuración de Servidor RADIUS externo para la Autorización y la Autenticación</u>.

La Internet Security Association y Key Management Protocol (ISAKMP), también denominada IKE, es el protocolo de negociación que los hosts acuerdan para crear una IPSec Security Association. Cada negociación ISAKMP se divide en dos secciones, Fase 1 y Fase 2. La Fase 1 crea el primer túnel para proteger mensajes posteriores de la negociación ISAKMP. La Fase 2 crea el túnel que protege los datos que viajan a través de la conexión segura. Consulte Palabras clave de la <u>Política ISAKMP para los comandos CLI</u> para más información sobre el ISAKMP.

Configuraciones

Configuración de ASA/PIX como Servidor VPN Remoto Usando ASDM

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

1. Seleccione **Wizards > VPN Wizard** de la ventana principal.

🚰 Cisco ASDM 5.0 for ASA - 172.10	5.1.2				_ O ×
File Rules Search Options T	ools Wizards Help				
Home Configuration (Monitor	arch Refresh	Save Help		CISCO SYSTEMS
-Device Information		Interface Sta	tus		
General License		Interface	IP Address/Mask	Line Link	Current Kbps
Host Name: ciecosea e	ieco com	inside	172.16.1.2/24	Oup Oup	1
ACA Manajor: 7.0(4)	Davias Listino: 04 06 43m 25a	outside	10.10.10.2/24	😏 up 😲 up	0
ADDM (content 5.0(4)	Device Optime: do un 12m 355				
AsDM Version: 5.0(4)	Device Type: ASA5520				
Firewall Mode: Routed	Context Mode: Single				
Total Flash: 64 MB	Total Memory: 512 MB	Select an inter	face to view input and	output Kbps	
-VPN Status		Traffic Status	8		
IKE Tunnels: 0	IPSec Tunnels: 0	Connections	Per Second Usage		
-System Resources Status -		1			
CPU CPU Usage (per	roent)	0.5			
90******		2 mont			
0% 84		10.02.20	700.0	Total: D	
12.02.45		- 00PE 0		Tetat: 0	
15.02.20		outside' Inte	rface Traffic Usage (Kbps	0	
Memory Memory Usage	(MB)	1			
512 384		0.5			
60M9 200 128		13:02:20			
13.02.49 13:02:28		Input Kb	ps: 0 📕	Output Kbps: 0	
Latest ASDM Syslog Messa	jes			Configure At	SDM Syslog Filters
	Syslog Disabled				
Device configuration loaded succes	ssfully.	admin N	A (15)	12/22	2/05 1:02:46 PM UTC

 Seleccione el tipo de túnel Remote Access VPN y asegúrese de que la interfaz del Túnel VPN esté configurada según lo deseado.

📸 VPN Wizard		×
VPN Wizard	VPN Tunnel Type (Step 1 of)	
Branch Branch ISP Horns Corporate Network	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 telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM. VPN Tunnel Type:	
	C Site-to-Site	
	Remote Access	
	VPN Tunnel Interface: outside	
	Back Next Finish Cancel Hel	p

3. Ya ha sido seleccionado el único tipo de VPN Client disponible. Haga clic en Next (Siguiente).



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

📸 VPN Wizard						
VPN Wizard	VPN Client Tunnel Group Name and Authentication Method (Step 3 of)					
Branch Branch Branch Branch Branch Branch	The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the following screens. Use the same tunnel group name for the device and the remote client. Select the type of authentication: shared secret or certificate. If certificate, select the certificate name and the certificate signing algorithm.					
Corporate Network	Tunnel Group Name: hillvalleyvpn					
	Authentication Pre-shared Key					
	Certificate Signing Algorithm:					
	Trustpoint Name:					
	< Back Next > Finish Cancel Help					

Nota: No hay una manera de ocultar/cifrar la clave previamente compartida en el ASDM. La razón es es que el ASDM solamente debe ser utilizado por las personas que configuran el ASA o por las personas que ayudan 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: Consulte el Ejemplo Grupos de Servidores de Autenticación y Autorización de PIX/ASA 7.x para los usuarios de VPN a través de la Configuración de ASDM para la información sobre cómo configurar a un grupo de servidores AAA externo a través del ASDM.

🔂 VPN Wizard	
VPN Wizard	Client Authentication (Step 4 of)
Branch Branch Fise Long Home Network	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next screen. 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, use Configuration > Features > Properties > AAA Setup category in the main ASDM window.
	 Authenticate using the local user database Authenticate using an AAA server group AAA Server Group
	< Back Next > Finish Cancel Help

6. Agregue los usuarios a las bases de datos locales en caso necesario.Nota: No quite a los usuarios existentes de esta ventana. Seleccione Configuration > Device Administration > Administration > User Accounts en la ventana principal ASDM para editar las entradas existentes en la base de daros o quitarlas de la base de datos.

🔂 VPN Wizard	
VPN Wizard	User Accounts (Step 5 of 11)
Brench Free Charles Free Cha	Enter a new username/password into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Device Administration > Administration > User Accounts in the main ASDM window.
Corporate Network	Username: Add >> Password (optional): Delete Confirm Password (optional): biff
	< Back Next > Finish Cancel Help

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

📷 VPN Wizard		×
VPN Wizard	Address Pool (Step 6 of 11)	
Brench Fr	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.	
Corporato Network	Tunnel Group Name: hillvalleyvpn	
111 - I + M	Pool Name: vpnpool	
	Range Start Address: 172.16.1.100	
TTT	Range End Address: 172.16.1.199	
	Subnet Mask (Optional): 255.255.255.0	
	< Back Next > Finish Cancel Help	

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)
Branch Branch Branch Branch Branch	Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.
Home	Tunnel Group: hillvalleyvpn
Network he	Primary DNS Server:
	Secondary DNS Server:
	Primary WINS Server:
1 I III	Secondary WINS Server:
CR-	Default Domain Name:
	< Back Next > Finish Cancel Help

 Especifique los parámetros para el IKE, también conocidos como fase 1. IKE.Las configuraciones a ambos lados del túnel deben coincidir de manera exacta. Sin embargo, el Cisco VPN Client selecciona automáticamente la configuración adecuada para sí mismo. Por lo tanto, no hay configuración IKE necesaria en PC del cliente.

薩 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	
Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch	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.	
Corporate Network	Encryption: 3DES	
1 Alter	Authentication: SHA	
STATION .	DH Group: 2	
	< Back Next > Finish Cancel Help	

10. Especifique los parámetros para el IPSec, también conocidos como fase 2 IKE.Las configuraciones a ambos lados del túnel deben coincidir de manera exacta. Sin embargo, el Cisco VPN Client selecciona automáticamente la configuración adecuada para sí mismo. Por lo tanto, no hay configuración IKE necesaria en PC del cliente.

🚰 VPN Wizard	
VPN Wizard	IPSec Encryption and Authentication (Step 9 of 11)
Branch Branch Branch Home	Select the encryption and authentication algorithms for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly.
Corporate Network	Encryption: 3DES
	Authentication: SHA
	< Back Next > Finish Cancel Help

11. Especifique qué host internos (de haber alguno) o redes deben exponerse 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.

💼 VPN Wizard		X		
VPN Wizard	Address Translation Exemption and Split Tunnelin	ng (Optional) (Step 10 of 11)		
Network Address Translation (NAT) is used to hide the internal network from or users. You can make exceptions to NAT to expose the entire or part of the internetwork to authenticated remote users protected by VPN. To expose the entire network behind the most secure interface to remote VPN without NAT, leave the selection list blank.				
Corporate Network	Host/Network to Be Added	Selected Hosts/Networks:		
	Interface: inside	Add >>		
	IP address: 0.0.0.0	Delete		
THE C	Mask: 0.0.0.0 💌			
	Enable split tunneling to let remote users hav resources defined above, and unencrypted ac	ve simultaneous encrypted access to the ccess to the internet.		
	< Back	Next > Finish Cancel Help		

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



Configuración de ASA/PIX como Servidor VPN Remoto Usando CLI

Termina estos pasos para configurar un Servidor de Acceso VPN remoto de la línea de comando. Consulte <u>Configuración de VPN de Acceso Remoto</u> o Referencias de Comandos de <u>Cisco ASA</u> <u>5500 Series Adaptive Security Appliance</u> para obtener más información sobre cada uno de los comandos.

1. Ingrese el comando ip local pool en el modo de configuración global para configurar los pools de dirección IP para usar en los túneles de acceso remoto VPN Para eliminar los pools de direcciones, ingrese la forma no de este comando.El dispositivo de seguridad utiliza los pools de direcciones basadas en el grupo de túnel para la conexión. Si configura más de un pool de direcciones para un grupo de túnel, el dispositivo de seguridad los utiliza en el orden en el están configurados. Emita este comando para crear un pool de las direcciones locales que pueden ser utilizadas para asignar a las direcciones dinámicas a los clientes de VPN del acceso remoto:

ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0

- 2. Ejecutar este comando: ASA-AIP-CLI(config)#username marty password 12345678
- 3. Emita este conjunto de comandos para configurar el túnel específico:ASA-AIP-CLI(config)#isakmp policy 1 authentication pre-shareASA-AIP-CLI(config)#isakmp policy 1 encryption 3desASA-AIP-CLI(config)#isakmp policy 1 hash shaASA-AIP-CLI(config)#isakmp policy 1 group 2ASA-AIP-CLI(config)#isakmp policy 1 lifetime 43200ASA-AIP-

CLI(config)#isakmp enable outsideASA-AIP-CLI(config)#crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmacASA-AIP-CLI(config)#crypto dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-SHAReverso-ruta determinada del outside_dyn_map 10 del mapa dinámico ASA-AIP-CLI(config)#cryptoASA-AIP-CLI(config)#crypto dynamic-map outside_dyn_map 10 set security-association lifetime seconds 288000Outside_dyn_map dinámico IPSec-ISAKMP del outside_map 10 de la correspondencia ASA-AIP-CLI(config)#cryptoASA-AIP-CLI(config)#crypto map outside_map interface outsideASA-AIP-CLI(config)#crypto isakmp nat-traversal

4. *Opcional:* Si desea que la conexión omita la lista de acceso que se aplica a la interfaz, emita este comando:

ASA-AIP-CLI(config) **#sysopt connection permit-ipsec**

Nota: Este comando funciona en las imágenes 7.x anteriores a 7.2(2). Si usa una imagen 7.2(2), emita el comando ASA-AIP-CLI(config)#sysopt connection permit-vpn .

- 5. Ejecutar este comando: ASA-AIP-CLI(config)#group-policy hillvalleyvpn internal
- 6. Emita estos comandos para configurar las configuraciones de la conexión cliente:ASA-AIP-CLI(config)#group-policy hillvalleyvpn attributesASA-AIP-CLI(config)#(config-grouppolicy)#dns-server value 172.16.1.11ASA-AIP-CLI(config)#(config-group-policy)#vpn-tunnelprotocol IPSecASA-AIP-CLI(config)#(config-group-policy)#default-domain value test.com
- 7. Ejecutar este comando: ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn ipsec-ra
- 8. Ejecutar este comando: ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn ipsec-attributes
- 9. Ejecutar este comando: ASA-AIP-CLI(config-tunnel-ipsec)#pre-shared-key cisco123
- 10. Ejecutar este comando:

ASA-AIP-CLI(config) #tunnel-group hillvalleyvpn general-attributes

- 11. Emita este comando para consultar la base de datos de usuario local para la autenticación. ASA-AIP-CLI(config-tunnel-general)#authentication-server-group LOCAL
- 12. Asocie la política del grupo al grupo de túnel ASA-AIP-CLI(config-tunnel-ipsec)# default-group-policy hillvalleyvpn
- 13. Emita este comando en el modo atributos generales de hillvalleyvpn tunnel-group para asignar el vpnpool creado en el paso 1 al grupo hillvalleyvpn. ASA-AIP-CLI(config-tunnel-general)#address-pool vpnpool

Configuración que se está ejecutando en el Dispositivo ASA

```
ASA-AIP-CLI(config)#show running-config
ASA Version 7.2(2)
!
hostname ASAwAIP-CLI
domain-name corp.com
```

```
enable password WwXYvtKrnjXqGbu1 encrypted
names
interface Ethernet0/0
nameif outside
security-level 0
ip address 10.10.10.2 255.255.255.0
1
interface Ethernet0/1
nameif inside
security-level 100
ip address 172.16.1.2 255.255.255.0
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
1
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
interface Management0/0
shutdown
no nameif
no security-level
no ip address
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name corp.com
pager lines 24
mtu outside 1500
mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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 hillvalleyvpn1 internal
group-policy hillvalleyvpn1 attributes
dns-server value 172.16.1.11
vpn-tunnel-protocol IPSec
default-domain value test.com
username marty password 6XmYwQ009tiYnUDN encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
```

```
crypto dynamic-map outside_dyn_map 10 set transform-set
ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 10 set security-
association lifetime seconds 288000
crypto map outside_map 10 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
crypto isakmp nat-traversal 20
tunnel-group hillvalleyvpn type ipsec-ra
tunnel-group hillvalleyvpn general-attributes
address-pool vpnpool
default-group-policy hillvalleyvpn
tunnel-group hillvalleyvpn ipsec-attributes
pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
class-map inspection_default
match default-inspection-traffic
!
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
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192
: end
ASA-AIP-CLI(config)#
```

Configuración de Almacenamiento de Contraseña de Cisco VPN Client

Si tiene los clientes numerosos del Cisco VPN, es muy difícil recordar todos los nombres de usuario y contraseña del cliente de VPN. Para almacenar las contraseñas en el equipo de VPN Client, configure ASA/PIX y VPN Client como se describe en esta sección.

ASA/PIX

Use el comando group-policy attributes en el modo de configuración global:

```
group-policy VPNusers attributes
password-storage enable
Cliente de Cisco VPN
```

Edite el archivo .pcf y modifique estos parámetros:

SaveUserPassword=1 UserPassword= <type your password>

Inhabilite la Autenticación Ampliada

En el modo de grupo de túnel, ingrese este comando para inhabilitar la autenticación ampliada, que está habilitada de forma predeterminada, en PIX/ASA 7.x:

```
asa(config)#tunnel-group client ipsec-attributes
asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

Después de inhabilitar la autenticación ampliada, los clientes de VPN no solicita nombre de usuario/ contraseña para la autenticación (Xauth). Por lo tanto, ASA/PIX no requiere la configuración del nombre de usuario y contraseña para autenticar a los clientes de VPN.

Verificación

Intente conectarse con Cisco ASA usando el Cisco VPN Client para verificar que el ASA esté configurado con éxito.

1. Seleccione Connection Entries > New.

¥PN Client - Version 4.0.5 (Rel)			
Connection Entries Status Certificates Log	Options	Help	
Connect to my_remote_vpn Ctrl+O Disconnect Ctrl+D	F		CISCO SYSTEMS
Create Shortcut Modify			
Delete		Host	Transport 🔺
Dyplicate			
Set as Default Connection Entry			
<u>N</u> ew			
Import 1/2			
Exit VPN Client Ctrl+Q			
			-
▲			>
Not connected.			

 Complete la información de su nueva conexión.El campo del host debe contener la dirección IP o el nombre de la computadora principal de Cisco previamente configurado ASA. La información de autenticación del grupo debe coincidir con la usada en el <u>paso 4.</u> Haga clic en **Guardar** cuando

	👌 VPN Client Cr	eate New VPN Connection	Entry	×
	Connection Entry:	_remote_vpn		
	Description:			
	<u>H</u> ost: 10	.10.10.2		
	Authentication 1	Fransport Backup Servers	Dial-Up	
	• Group Authentic	ation	C <u>M</u> utual G	roup Authentication
	<u>N</u> ame:	hillvalleyvpn		
	Password:	*****		
	Confirm Password	d: [********		
	C Certificate Author	entication	1	
	Send CA Cer	tificate Chain	J	
fiinalice.	Erase <u>U</u> ser Passwor	d	<u>S</u> ave	Cancel

3. Seleccione la conexión creada recientemente, y el haga clic en **Conectar**.

VPN Client - Version 4.0.5 (Rel)		
Connection Entries Status Certificates	Log Options <u>H</u> elp	
Connect New Import	Modify Delete	CISCO SYSTEMS
Connection Entries Certificates Lo	g	
Connection Entry	Host	Transport 🔺
my_remote_vpn	10.10.10.2	IPSec/UDP
		_
		-
Not connected.		

4. Ingrese un nombre de usuario y contraseña para la autenticación ampliada. Esta información debe coincidir con la especificada en los <u>pasos 5 y</u>

	👌 VPN Client U	ser Authen	ntication for "my_remote_vpn" 🛛 🗙
	Enter Username and CISCO SYSTEMS	d Password. <u>U</u> sername: <u>P</u> assword:	marty
6.			OK Cancel

5. Una vez que la conexión está **establecida satisfactoriamente seleccione** Estadísticas del menú Estado para verificar los detalles del túnel.Esta ventana muestra el tráfico y la información

etails ess Infoi ent: erver:	Route Details mation 172.16.1.100 10.10.10.2	Fire	wall nnection Informa Entry: Time:	ation m	y_remote_vpn	
ess Infor ent: erver:	r mation 172.16.1.100 10.10.10.2	Co	nnection Informa Entry: Time:	ation m	y_remote_vpn	
			rime:	0	day(s), 00:01.31	
eceived: ent:	240 46816	Cry	ypto Encryption: Authentication:	11 H	68-bit 3-DES MAC-SHA1	
ets acrypted: acrypted: scarded: passed:	332 4 137 61	Тта	ansport Transparent Tunne Local LAN: Compression:	eling: Ir D N	active isabled one	
					Reset	
	ts crypted: crypted: carded: bassed:	nt: 46816 ts crypted: 332 crypted: 4 carded: 137 wassed: 61	nt: 46816 ts Tra crypted: 332 crypted: 4 carded: 137 passed: 61	at: 46816 Authentication: ts Transport crypted: 332 Transparent Tunne crypted: 4 Local LAN: carded: 137 Compression: bassed: 61	at: 46816 Authentication: H ts Transparent Tunneling: In crypted: 332 Transparent Tunneling: In crypted: 4 Local LAN: D carded: 137 Compression: N bassed: 61	at: 46816 Authentication: HMAC-SHA1 ts Transport trypted: 332 Transparent Tunneling: Inactive crypted: 4 Local LAN: Disabled carded: 137 Compression: None Reset Close

sta ventana muestra la información de la tunelización

Jecured Houles
Network Subnet M
0.0.0.0 0.0.0.0

Troubleshooting

Use esta sección para resolver problemas de configuración.

Crypto ACL Incorrecto

El ASDM 5.0(2) crea y aplica una lista de control de acceso crypto (ACL) que puede causar los problemas para los clientes de VPN que utilizan la tunelización dividida, así como para los hardwares cliente en el modo de la red-extensión. Use ASDM version 5.0(4.3) o posterior para evitar este problema. ConsulteCisco bug ID <u>CSCsc10806</u> (clientes registrados solamente) para más detalles.

Información Relacionada

- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- La mayoría del IPSec VPN común L2L y del Acceso Remoto que resuelve problemas las soluciones
- Alertas y Troubleshooting de Cisco ASA 5500 Series Adaptive Security Appliances
- Soporte Técnico y Documentación Cisco Systems