ASA/PIX: Servidor VPN remoto con el NAT entrante para el tráfico del cliente VPN con el CLI y el ejemplo de la Configuración de ASDM

Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados Productos Relacionados Convenciones Antecedentes Configuraciones Configure ASA/PIX como servidor VPN remoto con el ASDM Configure ASA/PIX al tráfico entrada de NAT del cliente VPN con el ASDM Configure ASA/PIX al tráfico entrada de NAT del cliente VPN con el ASDM Configure ASA/PIX como servidor VPN remoto y para el NAT entrante con el CLI Verificación ASA/PIX dispositivo de seguridad - comandos show Troubleshooting Información Relacionada

Introducción

Este documento describe cómo configurar Cisco 5500 Series Adaptive Security Appliance (ASA) para que actúe como servidor VPN remoto mediante el Adaptive Security Device Manager (ASDM) o la CLI y NAT el tráfico entrante del cliente VPN. 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 a través del Cliente Cisco VPN.

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. El ASA también se asume para ser configurado para el NAT saliente. Refiérase <u>no prohiben a host interiores el acceso a las redes externas con el uso de la PALMADITA</u> para más información sobre cómo configurar el NAT saliente.

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.

- Versión de software adaptante 7.x del dispositivo de seguridad de Cisco y posterior
- Versión 5.x y posterior adaptante del Administrador de dispositivos de seguridad
- Cliente VPN de Cisco versión 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 se puede también utilizar con la versión 7.x y posterior del dispositivo de seguridad del Cisco PIX.

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. Refiera a las <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 directiva del grupo para las conexiones específicas. Si usted no asigna una directiva del grupo determinado a los usuarios, la directiva 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 expedientes identifican los servidores a los cuales autentican a los usuarios del túnel, así como a los servidores de contabilidad, eventualmente, a quienes se envía la información de conexión. 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 pertenezcan a la creación del túnel sí mismo. Los grupos de túnel incluyen un indicador a una política del grupo que define los atributos orientados hacia el usuario.

Configuraciones

Configure ASA/PIX como servidor VPN remoto con el ASDM

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

 Abra su hojeador y ingrese los <IP_Address de https:// de la interfaz del ASA que se ha configurado para el ASDM Access> para acceder el ASDM en el ASA.Aseegurese autorizar cualquier advertencia que su navegador le dé relacionado con la autenticidad de certificados SSL. Nombre de usuario predeterminado y la contraseña son ambos espacio en blanco.El ASA presenta esta ventana para permitir la descarga de la aplicación ASDM. Este ejemplo carga la aplicación sobre la computadora local y no se ejecuta en los subprogramas java.



- 2. Haga clic el **activador de ASDM de la descarga y comience el ASDM** para descargar el instalador para la aplicación ASDM.
- 3. Una vez que el activador de ASDM descarga, complete los pasos ordenados por los prompts para instalar el software y funcionar con el Cisco ASDM launcher.

4. Ingrese el IP Address para la interfaz que usted configuró con el **HTTP -** ordene, y un nombre de usuario y contraseña si usted especificó uno.Este ejemplo utiliza el **cisco123** como el nombre de usuario y el **cisco123** como la

	🕵 Cisco ASDM Launch	er v1.5(30)			
	🤏 Cisco AS	cisco			
	Device IP Address / Name:	10.77.241.111	v		
	Username:	cisco123			
	Password:	****			
	🔄 Run in Demo Mode				
		OK Close			
contraseña			🗊 👙 🔒		

5. Seleccione los Asisitente > al Asisitente del IPSec VPN de la ventana

	🖆 Cisco ASDM 6.1 for ASA - 10.77.241.111								
	File View Tools				ards	Window	Help		
					Star	rtup Wizard	l		1
				IPsec VPN Wizard					
	Device List			SSL	VPN Wizar	d	ŀĜ	-	
	🗣 A	🖶 Add 📋 Delete			Liak	. من جا جا الله	u and c	a shiibo waxa	
				nıyı	T AValiability	y anu b	Calability Wizaru		
casera.	· · · · ·	10.7	7.241.1		Pack	ket Capture	e Wizar	·d	

6. Seleccione el tipo de túnel del **VPN de acceso remoto** y asegúrese de que la interfaz del túnel VPN está fijada según lo deseado, y haga clic **después** como se muestra aquí.

🖆 VPN Wizard	2	×
VPN Wizard	PN Tunnel Type (Step 1 of)	
Branch Branch ISP Home	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.	
Corporate Network	VPN Tunnel Type: Site-to-Site VPN	
A A A A A A A A A A A A A A A A A A A	Site-to-Site	
	Remote Access	
	VPN Tunnel Interface: Outside	
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.	
	< Back Next > Finish Cancel Help	9

7. Eligen al tipo del cliente VPN, como se muestra. Eligen al **Cliente Cisco VPN** aquí. Haga clic en Next

(Siguiente).

🖆 VPN Wizard	2
VPN Wizard	Remote Access Client (Step 2 of)
Branch	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
	VPN Client Type:
Home	Cine WWI Clerk Deleges 2 v av history
Corporate Network	or other Eacy VIN Demote product
	or other Easy very Remote product
1	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.
- I STUTUT	PAP CHAP MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY
A THE	Specify if the client will send tunnel group name as - username@tunnelgroup.
- B-	Client will send tunnel group name as username@tunnelgroup.
	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
	< Back Next > Finish Cancel Help

8. Ingrese un nombre para el Nombre de Grupo de Túnel. Ingrese la información de autenticación para utilizar, que es la clave previamente compartida en este ejemplo. La clave previamente compartida usada en este ejemplo es cisco123. El nombre de grupo de túnel usado en este ejemplo es Cisco. Haga clic en Next (Siguiente).

🖆 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Branch Horne Horne	The ASA allows you to group remote access tunnel users based on common connection parameters and clent 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 clent. Authentication Method Pre-shared key Pre-Shared Key: Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Challenge/response authentication (CRACK)
	< Back Next > Finish Cancel Help

9. 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: Usted agrega a los usuarios a la base de datos de usuarios locales en el paso 10.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)	
Brandh Brandh Brandh Brandh Horno Corpor ato Notwork	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. Authenticate using the local user database AAA Server Group Name: New	
	< Back Next > Finish Cancel Hel	P

10. Proporcione un nombre de usuario y la contraseña y el tecleo opcionales agregan para agregar a los usuarios nuevos a la base de datos de autenticación de usuario. Haga clic en Next (Siguiente).Nota: No quite a los usuarios existentes de esta ventana. Seleccione la configuración > la Administración de dispositivos > Users/AAA > 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

🖆 VPN Wizard			×
VPN Wizard	User Accounts (Step 5 of 11)		
Brandh Brandh Brandh Brandh Brandh	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 a, go to Configuration > Device Management > ain ASDM window.	
Home	User to Be Added		
Corporate Network	Username:	cisco123	
	cisco Password (optional):	Add >>	
	Confirm Password (optional):		
		<back next=""> Finish Cancel Help</back>	

 Para definir un pool de las direcciones locales que se asignarán dinámicamente a los clientes VPN remotos, haga clic **nuevo** para crear a una nueva **agrupación** IP.

🖆 VPN Wizard		\mathbf{X}
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Branch ISP Ditto Horne Network	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients. Tunnel Group Name : CISCO	
THE THE	Pool Name:	
	Pool Settings	
THURHIN	Range Start Address:	
	Range End Address:	
making the stand when the	Subnet Mask:	
	< Back Next > Finish Cancel Help	2

12. En la nueva ventana titulada **agregue a la agrupación IP** proporcionan esta información, y hacen clic la AUTORIZACIÓN.Nombre de la agrupación IPComenzar la dirección IPTerminación de la dirección IPMáscara de

	Add IP Pool	
	Name:	vpnpool
	Starting IP Address:	192.168.1.1
	Ending IP Address:	192.168.1.254
	Subnet Mask:	255.255.255.0
net	OK R	Cancel Help

13. Después de que usted defina el pool de las direcciones locales que se asignarán dinámicamente a los clientes VPN remotos cuando conectan, haga clic **después.**

🖆 VPN Wizard		
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Branch ISP Home	Enter a pool of local addresses to be used for assigning dynamic IP ad clients.	idresses to remote VPN
Corporate Network	Tunnel Group Name : cisco	
THE THE	Pool Name: vpnpool	New
	Pool Settings	
	Range Start Address: 192.168.1.1	
- ICONTRA	Range End Address: 192.168.1.254	
- CAL	Subnet Mask: 255.255.255.0	
	< Back Next >	inish Cancel Help

14. *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)
Brandt Frankt	Attributes you configure below are push ASA. If you do not want an attribute pu	ed to the VPN client when the client connects to the shed to the client, leave the corresponding field blank.
Corporate	Tunnel Group:	disco
Territor 10	Primary DNS Server:	
	Secondary DNS Server:	
1111	Primary WINS Server:	
	Secondary WINS Server:	
	Default Domain Name:	
		< Back Next > Finish Cancel Help

15. 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.

🖆 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	
Branch Branch F F F F F F F F F F F F F F F F F F F	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.	
Network	Encryption: DES	
	Authentication:	
	Diffie-Helman Group: 2	
	< Back Next Finish Cancel He	dp.

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



Configure ASA/PIX al tráfico entrada de NAT del cliente VPN con el ASDM

Complete estos pasos para configurar Cisco ASA al tráfico entrada de NAT del cliente VPN con el ASDM:

1. Elija la **configuración > el Firewall > las reglas nacionales**, y el haga click en Add En la lista desplegable, selecta **agregue la regla dinámica**



NAT.

2. En la ventana **dinámica de la regla del agregar NAT**, elija el **exterior** como la interfaz, y haga clic el botón Browse al lado del cuadro de la **fuente**.

🖾 Add	Dyna	mic NAT Rule		\mathbf{X}
Original Interf Sourc Translat Select	face: [:e: [ted — t a gloi	Outside bal pool for dynamic tr	anslation.	
Poo 0	l ID	Interface (outbound) (inbound)	Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
Conn	ectior	Settings	OK Cancel Help	*

3. En la ventana de la fuente de la ojeada, seleccione los objetos de red adecuada y también elija la **fuente** bajo sección seleccionada de la fuente, y haga clic la **AUTORIZACIÓN**. Aquí el objeto de red de 192.168.1.0 se elige.

🖆 Browse Source				
🗣 Add 🗹 Edit 📋 D	elete 🔍			
Filter:				Filter Clear
Name	↑ 1 IP Address	Netmask	Description	
Network Objects				
🔷 🔷 any	0.0.0	0.0.0		
inside-networ	k 172.16.1.0	255.255.255.0		
- 🚮 Outside-netw	ork 10.10.10.0	255.255.255.0		
i- 🛃 192.168.1.0	192.168.1.0	255.255.255.0		
Selected Source				
	.168.1.0/24			
				K Cancel

4. El tecleo maneja.

C	Add Dyna	amic NAT Rule		
OI Tr	iginal Interface: Source: anslated — Select a glo Pool ID 0 0	Outside 192.168.0.0 bal pool for dynamic Interface (outbound) (inbound)	translation. Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
	Connection	n Settings	OK Cancel Help	*

5. En la ventana de la agrupación global del manejo, haga click en

R	Manage Glo	obal Pool		×
	🔁 Add 🗹 E	dit 💼 Delete		
	Pool ID	Interface	Addresses Pool	
				_
				-
L				
		ОК	Cancel Help	
d				

6. En la ventana de la agrupación global de direcciones del agregar, elija el interior como la interfaz y 2 como el pool ID. También aseegurese que el botón de radio al lado de la PALMADITA usando la dirección IP de la interfaz está seleccionado. Haga clic Add>>, y después haga clic la AUTORIZACIÓN.

🞼 Add Global Address Pool		X
Interface: inside Pool ID: 2		
IP Addresses to Add Range Starting IP Address: Ending IP Address: Netmask (optional): IP Address Translation (PAT) IP Address: Netmask (optional):	Add >> << Delete	Addresses Pool inside
Port Address Translation (PAT) using IP Address of the interface OK OK	Cancel	Help

7. Haga Click en OK después de que usted seleccione a la agrupación global con el **pool ID 2** configurado en el paso anterior.

🕵 Add Dyn	amic NAT Rule		
Original			
Interface:	Outside	~	
Source:	192.168.1.0/24		
Translated — Select a glo	bal pool for dynamic t	ranslation.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
	(inbound)	Same as original address (identity)	
2	Inside	inside	Manage
Connectio	n Settings		۲
		Cancel Help	

8. Ahora el tecleo **se aplica** para aplicar la configuración al ASA. This complete la configuración.

Type Source Destination Service Interface Addr Outside (1 Dynamic rules) Inside (1 Exempt rules, 1 Dynamic rules) Inside (1 Exempt rules, 1 Dynamic rules) Inside (1 Exempt rules, 1 Dynamic rules) Image: Control of the second rule of the s			Original			Translated	
Outside (1 Dynamic rules) inside inside inside (1 Exempt rules, 1 Dynamic rules) inside inside 1 Exempt any if 192.168.1.0/24 (outbound) 2 Dynamic any Outside if 0	#	Туре	Source	Destination	Service	Interface	Addr
1 Inside Inside Inside Inside (1 Exempt rules, 1 Dynamic rules) any Image: 192.168.1.0/24 (outbound) 2 Image: Dynamic any Image: 192.168.1.0/24 Outside	l Outsi	de (1 Dynamic rules)					
1 Exempt any # 192.168.1.0/24 (outbound) 2 Dynamic any Outside Image: Outside	1	Dynamic	192.168.1.0)/24		inside	an in
1 Exempt any Image: 192.168.1.0/24 (outbound) 2 Image: 192.168.1.0/24 Outside Image: 192.168.1.0/24	inside	(1 Exempt rules, 1 D	ynamic rules)				
2 Outside any Outside O	1	🔁 Exempt	🌍 any	192.168.1.0/24		(outbound)	
	2	Dynamic	🌍 any			Outside	🎫 O(

Configure ASA/PIX como servidor VPN remoto y para el NAT entrante con el CLI

Configuración que se está ejecutando en el Dispositivo ASA
ciscoasa# show running-config
: Saved
ASA Version 8.0(3)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif Outside
security-level 0
ip address 10.10.10.2 255.255.255.0

interface Ethernet0/1 nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 1 passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside_nat0_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2 192.168.1.0 255.255.255.0 outside nat (inside) 0 access-list inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0 route Outside 0.0.0.0 0.0.0.0 10.10.10.3 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-policy-record DfltAccessPolicy http server enable no snmp-server location no snmp-server contact !--- Configuration for IPsec policies. !--- Enables the crypto transform configuration mode, !--- where you can specify the transform sets that are used !--- during an IPsec negotiation. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5hmac crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group1 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map interface Outside crypto isakmp enable Outside !--- Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are

used during an IKE negotiation. Encryption and !-Policy details are hidden as the default values are chosen. crypto isakmp policy 10 authentication pre-share encryption des hash sha group 2 lifetime 86400 crypto isakmp policy 30 authentication pre-share encryption des hash md5 group 2 lifetime 86400 telnet timeout 5 ssh timeout 60 console timeout 0 management-access inside threat-detection basic-threat threat-detection statistics access-list group-policy cisco internal group-policy cisco attributes vpn-tunnel-protocol IPSec !--- Specifies the username and password with their !--respective privilege levels username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0 username cisco attributes vpn-group-policy cisco tunnel-group cisco type remote-access tunnel-group cisco general-attributes address-pool vpnpool default-group-policy cisco !--- Specifies the pre-shared key "cisco123" which must !--- be identical at both peers. This is a global !--configuration mode command. tunnel-group cisco ipsecattributes pre-shared-key * ! class-map inspection_default match default-inspection-traffic ! policy-map type inspect dns migrated_dns_map_1 parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns migrated_dns_map_1 inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp

```
inspect sip
inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3
: end
ciscoasa#
```

Verificación

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

1. Haga clic en

New.			
VPN Client - Version 5.0.03.0530			
Connection Entries Status Certificates Log Options	; Help		
Connect News Import Modify) Delete		ahaha cisco
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
Not connected.			

 Complete la información de su nueva conexión.El campo del host debe contener la dirección IP o el nombre de host de Cisco previamente configurado ASA. La información de autenticación del grupo debe corresponder a eso usado en la salvaguardia del tecleo del paso 4. cuando le

Connection Entry: MyVPNClient Description: Host: 10.10.10.2 Authentication Transport Backup Servers Dial-Up Group Authentication Name: Cisco Password: ******** Confirm Password: ******** Confirm Password: ******** Confirm Password: ******* Confirm Password: ******* Confirm Password: ******* Confirm Password: ******* Confirm Password: Cancel	VPN Client Create New VPN Connection Entry	×
Description: Host: 10.10.10.2 Authentication Transport Backup Servers Dial-Up Group Authentication Mutual Group Authentication Name: cisco Password: ******** Confirm Password: ******** Confirm Password: ******** Confirm Password: ******** Confirm Cancel Save Cancel	Connection Entry: MyVPNClient]
Host: 10.10.10.2 Authentication Transport Backup Servers Dial-Up Group Authentication Mutual Group Authentication Name: cisco Password: ******** Confirm Password: ******* Confirm Password: ******* Send CA Certificate Chain Transport Erase User Password Save Cancel	Description:	
Authentication Transport Backup Servers Dial-Up Image: Group Authentication Image: Mutual Group Authentication Name: cisco Password: Image: Mutual Group Authentication Confirm Password: Image: Mutual Group Authentication Name: Image: Mutual Group Authentication Name: Image: Mutual Group Authentication Image: Mutual Group Authentication Image: Mutual Group Authentication Image: Mutual Group Authentica	Host: 10.10.10.2	
Group Authentication Name: Confirm Password: ********* Confirm Password: ************************************	Authentication Transport Backup Servers Dial-Up	
Name: cisco Password: ******* Confirm Password: ******* Confirm Password: ********	Group Authentication	p Authentication
Password: ****** Confirm Password: ******* Certificate Authentication Name: Send CA Certificate Chain Erase User Password Save Cancel	Name: cisco	
Confirm Password: ****** Certificate Authentication Name: Send CA Certificate Chain Erase User Password Cancel	Password: ******	
 Certificate Authentication Name: Send CA Certificate Chain Erase User Password Save Cancel 	Confirm Password: *******	
Name: Send CA Certificate Chain Erase User Password Save Cancel	Certificate Authentication	
Send CA Certificate Chain Erase User Password Save Cancel	Name:	
Erase User Password Cancel	🔽 Send CA Certificate Chain	
Erase User Password Save Cancel		
	Erase User Password Save	Cancel

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

Status: Disconnected VPN Client - Version	5.0.03.0530		
Connection Entries Status Certificates Log Options Hi	эlp		
Connection Entries Certificates Log	Delete		cisco
Connection Entry	Host	Transport	
MyVPNClient	10.10.10.2	IPSec/UDP	
Not connected.			1

4. Ingrese un nombre de usuario y contraseña para la autenticación ampliada. Esta información debe hacer juego eso especificada en los **pasos 5 y**

	VPN Client User Authentication for "MyVPNClient"
	The server has requested the following information to complete the user authentication.
	Username: cisco123 CISCO Password: *******
6.	OK Cancel

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

🥔 status: Connected VI	PN Client - Version 5.0.	03.0530		
Connection Entries Status Ce	ertificates Log Options Hel	p		
Disconnect N	tics Ctrl+S cations Ctrl+N	X elete	cise	()., CO
Connection Entries Reset	Stats			
Connection Entry	Δ	Host	Transport	
MyVPNClient		10.10.10.2	IPSec/UDP	
Connected to "MyVPNClient".		Connect	ed Time: 0 day(s), 00:00.36	•

Esta ventana muestra el tráfico y la información

Tunnel Details Route Details	Firewall	
Address Information Client: 192.168.1.1 Server: 10.10.10.2	Connection Information Entry: Time:	n MyVPNClient 0 day(s), 00:01.13
Bytes Received: 5412 Sent: 5416	Crypto Encryption: Authentication:	56-bit DES HMAC-MD5
Packets Encrypted: 39 Decrypted: 31 Discarded: 8 Bypassed: 22	Transport Transparent Tunneling Local LAN: Compression:	Inactive Disabled None
		Reset
		Close

ventana muestra la información de la tunelización

E	VPN Client	Statistics		
	Tunnel Details	Route Details Fir	ewall	
	Local LAN Rout	es	Secured Re	outes
	Network	Subnet Mask	Network	Subnet Mask
			0.0.0.0	0.0.0

ASA/PIX dispositivo de seguridad - comandos show

• show crypto isakmp sa — Muestra todas las IKE SAs actuales en un par. ASA#show crypto isakmp sa

```
Active SA: 1
     Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
 Total IKE SA: 1
     IKE Peer: 10.10.10.1
 1
                               Role : responder
     Type : user
     Rekey
             : no
                               State
                                       : AM_ACTIVE
• muestre IPSec crypto sa — Muestra todo el SA de IPSec actual en un par.
 ASA#show crypto ipsec sa
 interface: Outside
     Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10
 .10.2
       local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
       current_peer: 10.10.10.1, username: cisco123
       dynamic allocated peer ip: 192.168.1.1
       #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
       #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0
       #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
       #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1
```

```
path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: F49F954C
    inbound esp sas:
      spi: 0x3C10F9DD (1007745501)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
        slot: 0, conn id: 24576, crypto-map: SYSTEM DEFAULT CRYPTO MAP
         sa timing: remaining key lifetime (sec): 27255
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0xF49F954C (4104099148)
         transform: esp-des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
        sa timing: remaining key lifetime (sec): 27255
        IV size: 8 bytes
        replay detection support: Y
ciscoasa(config)#debug icmp trace
!--- Inbound Nat Translation is shown below for Outside to Inside ICMP echo request
translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3
2
!--- Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply
untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192
len=32
ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1
ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3
ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32
ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32
ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32
```

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

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.

Refiera a <u>la mayoría del IPSec VPN común L2L y del Acceso Remoto que resuelve problemas las</u> <u>soluciones</u> para más información sobre cómo resolver problemas el Sitio-sitio VPN.

Información Relacionada

- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>Cisco Adaptive Security Device Manager</u>
- Alertas y Troubleshooting de Cisco ASA 5500 Series Adaptive Security Appliances
- Soporte Técnico y Documentación Cisco Systems