Ejemplo de Configuración de SDM: VPN IPsec de Sitio a Sitio entre ASA/PIX y un Router IOS

Contenido

Introducción **Prerequisites Requirements Componentes Utilizados Productos Relacionados** Convenciones Configuración Diagrama de la red Configuración de ASDM del túnel VPN Configuración de SDM del router Configuración CLI ASA Configuración CLI del router Verificación Dispositivo de seguridad ASA/PIX - Comandos show Router IOS remoto - Comandos show Troubleshoot Información Relacionada

Introducción

Este documento proporciona una configuración de ejemplo del túnel IPsec de LAN a LAN (sitio a sitio) entre Cisco Security Appliances (ASA/PIX) y un router Cisco IOS. Las rutas estáticas se utilizan para simplificar.

Consulte <u>Ejemplo de Configuración de Túnel IPSec de LAN a LAN de PIX/ASA 7.x Security</u> <u>Appliance a un Router IOS</u> para obtener más información sobre el mismo escenario en el que el Dispositivo de Seguridad PIX/ASA ejecuta la versión de software 7.x.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

• Se debe establecer una conectividad IP de extremo a extremo antes de iniciar esta configuración.

• La licencia del dispositivo de seguridad debe estar habilitada para el cifrado del estándar de cifrado de datos (DES) (con un nivel de cifrado mínimo).

Componentes Utilizados

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

- · Cisco Adaptive Security Appliance (ASA) con versión 8.x y posteriores
- ASDM versión 6.x y posteriores
- Router Cisco 1812 con software Cisco IOS® versión 12.3
- Cisco Security Device Manager (SDM) versión 2.5

Nota: Consulte <u>Cómo Permitir el Acceso HTTPS para ASDM</u> para permitir que el ASA sea configurado por el ASDM.

Nota: Consulte <u>Configuración Básica del Router mediante SDM</u> para permitir que SDM configure el router.

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). If your network is live, make sure that you understand the potential impact of any command.

Nota: Refiérase a <u>Ejemplo de Configuración de VPN IPSec de Sitio a Sitio entre ASA/PIX y un</u> <u>Router IOS</u> para una configuración similar utilizando Cisco Configuration Professional en el router.

Productos Relacionados

Esta configuración también se puede utilizar con Cisco PIX 500 Series Security Appliance, que ejecuta la versión 7.x y posteriores.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configuración

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918 que se han utilizado en un entorno de laboratorio.

- Configuración de ASDM del túnel VPN
- Configuración de SDM del router
- <u>Configuración CLI ASA</u>
- Configuración CLI del router

Configuración de ASDM del túnel VPN

Complete estos pasos para crear el túnel VPN:

1. Abra su navegador e ingrese https://<IP_Address de la interfaz de ASA que se ha configurado para el acceso ASDM> para acceder al ASDM en el ASA.

Asegúrese de autorizar cualquier advertencia que le proporcione su navegador en relación con la autenticidad del certificado SSL. El nombre de usuario y la contraseña predeterminados están en blanco.

ASA presenta esta ventana para permitir la descarga de la aplicación ASDM. En este ejemplo se carga la aplicación en el equipo local y no se ejecuta en un subprograma Java.

Cisco ASDM 6.1))
Cisco ASDM 6.1(3) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.	
Cisco ASDM runs as either a local application or Java Web Start.	
 When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages: You can invoke ASDM from desktop shortcuts. No browser is required. One desktop shortcut allows you to connect to <i>multiple</i> Security Appliances. 	1
Running Cisco ASDM as Java Web Start You can run Cisco ASDM as Java Web Start that is dynamically downloaded from the device	
 Click <i>Run ASDM</i> to run Cisco ASDM. Click <i>Run Startup Wizard</i> to run Startup Wizard.Startup Wizard walks you through, step by step, the initial configuration of your security appliance. 	
Run ASDM Run Startup Wizard	

- 2. Haga clic en Download ASDM Launcher and Start ASDM para descargar el instalador para la aplicación ASDM.
- 3. Una vez que se haya descargado el punto de ejecución de ASDM, complete los pasos indicados en las indicaciones para instalar el software y ejecutar el punto de ejecución de ASDM de Cisco.
- 4. Ingrese la dirección IP para la interfaz que configuró con el comando http -, y un nombre de usuario y contraseña si especificó uno.

Este ejemplo utiliza cisco123 para el nombre de usuario y cisco123 como la contraseña.

🖆 Cisco ASDM Launcher v1.5(30)		
Sisco ASDM Launcher		
10.77.241.111		
cisco123		

	solution of the second	

5. Ejecute el IPsec VPN Wizard una vez que la aplicación ASDM se conecte al ASA.

📧 Cisco ASDM 6.1 for ASA -	10.77.241.111				2	
File View Tools Wizards Wi	indow Help	Look For:			<u>.</u>	միս
Home 🖓 Cor Startup	Wizard	n 📿 Ba	ick 🌔 Fo	orward 🥝 Help 🚽	cis	ico
IPsec VF	PN Wizard					_
SSL VPN	l Wizard 🔊	ation 1				
High Av.	ailability and Scalability Wizard	nuun				
Device Informa Packet (Capture Wizard	Inte	rface Stat	us		
General License		Int	erface	IP Address/Mask	Line	u
Hech Viscou — discourse dal	fault domain invalid	dmz		10.77.241.111/26	🕤 սթ	0
ASA Version: 8.0(2) D	rauic.comain.invalio evice Untine: 14d 3h 1m 51c	insid	e	10.10.10.1/24	ւթ ար	0
ASDM Version: 6.1(3) D	evice Optime: 144 54 111 515	outs	ide	172.16.1.1/24	😈 up	0
Firewall Mode: Routed G	ontext Mode: Single					=
Total Flash: 64 MB To	otal Memory: 256 MB					
	r	Selec	t an interfa	ce to view input and o	utput Kbps	
VPN Tunnels	n una la con una churte di Data	Tran	ic Status			_
IKE: 0 IPSec: 0 Clientless 55	SE VPN: O SSE VPN Client: O Deca	us Cor	inections Pe	er Second Usage		
System Resources Status						
CPU CPU Usage (percent)	- 0				
100		-				
0% 5D			20:41	20:42	20:43 2	0:44
			UUP: 0	TCP: U Tota	#: U	<u>×</u>
	cisco123	15		🛃 📶 🗌	4/6/09 8:45:	42 PM UTC

6. Elija el tipo de túnel VPN IPsec de sitio a sitio y haga clic en Next como se muestra aquí.

🖆 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch Promote ISP Horne	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
Name	Site-to-Site
	Remote Access 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

7. Especifique la dirección IP externa del par remoto. Introduzca la información de autenticación que desea utilizar, que es la clave previamente compartida en este ejemplo. La clave previamente compartida utilizada en este ejemplo es cisco123. El nombre del grupo de túnel será su dirección IP externa de forma predeterminada si configura L2L VPN. Haga clic en Next (Siguiente).

🖆 VPN Wizard		<
VPN Wizard	Remote Site Peer (Step 2 of 6)	
Bronch	Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel. Peer IP Address: 172.17.1.1	
EST IN	Authentication Method	
Home	Pre-shared key	
Corporatu Network	Pre-Shared Key: disco123	
- F	Certificate	
The second	Certificate Signing Algorithm: rsa-sig	
	Certificate Name:	
THUM	Challenge/response authentication (CRACK)	
	Tunnel Group	
-6	For site-to-site connections with pre-shared key authentication, the tunnel group name must be the same as either the peer IP address or the peer hostname, whichever is used as the peer's identity.	
	Tunnel Group Name: 172.17.1.1	
	< Back Next > Finish Cancel Help	

8. Especifique los atributos que se utilizarán para IKE, también conocidos como fase 1. Estos atributos deben ser los mismos tanto en el ASA como en el router IOS. Haga clic en Next (Siguiente).

🖆 VPN Wizard		×
VPN Wizard	IKE Policy (Step 3 of 6)	
Branch Branch Fisp Fisp Hoene Corporate	Select the encryption algorithm, aut devices to use to negotiate an Inter them. Configurations on both sides (hentication algorithm, and Diffie-Hellman group for the net Key Exchange (IKE) security association between of the connection must match exactly.
Notwork	Encryption:	DES 🖌
	Authentication:	5HA
		< Back Next Finish Cancel Help

9. Especifique los atributos que se utilizarán para IPSec, también conocidos como fase 2. Estos atributos deben coincidir tanto en el ASA como en el router IOS. Haga clic en Next (Siguiente).

🖆 VPN Wizard]
VPN Wizard	IPsec Encryption and Authentication (Step 4 of 6)	
Branch Branch Branch Hanvo Corporato Network	Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.	
	< Back Next > Finish Cancel Help	

10. Especifique los hosts cuyo tráfico se debe permitir que pase a través del túnel VPN. En este paso, debe proporcionar las redes local y remota para el túnel VPN. Haga clic en el botón situado junto a Local Networks (Redes locales), como se muestra aquí, para elegir la dirección de red local en la lista desplegable.

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks (Step 5 of 6)	
Branch Franch	An IPsec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPsec tunnel.	
	Action: Protect Do not Protect	
Horne	Local Networks: any	
Network	Remote Networks: any	
	✓ Exempt ASA side host/network from address translation: inside	
	< Back Next > Finish Cancel	Help

11. Elija la dirección de red local y haga clic en OK como se muestra aquí.

🖆 Browse Local Netwo	orks			
🗣 Add 👻 📝 Edit 👔	Delete Q			
Filter:	· ·			Filter Clear
Name ^	1 IP Address	Netmask	Description	
Network Objects				
- 🏈 any	0.0.0.0	0.0.0		
dmz-network	10.77.241.64	255.255.255.192		
inside-network	10.10.10.0	255.255.255.0		
····· 📑 outside-networ	k 172.16.1.0	255.255.255.0		
Selected Local Networks -				
Local Networks ->	any			
				Lancel

12. Haga clic en el botón junto a Redes remotas, como se muestra aquí, para elegir la dirección de red remota en la lista desplegable.

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Brandh	An IPsec tunnel protect remote sites. Please ide	ts data exchanged by selected hosts and networks at the local and antify hosts and networks to be used in the IPsec tunnel.
	Action:	Protect O Do not Protect
Home	Local Networks:	inside-network/24
Corporate Network	Remote Networks:	any 🤤
	Exempt ASA side h	nost/network from address translation:
		< Back Next > Finish Cancel Help

13. Elija la dirección de Red remota y haga clic en Aceptar como se muestra aquí.

Nota: Si no tiene Red remota en la lista, deberá agregar la red a la lista haciendo clic en Agregar.

🖆 Browse Remote Net	works			
🗣 Add 🗸 🗹 Edit 👔	Delete 🔍			
Filter:				Filter Clear
Name ^	1 IP Address	Netmask	Description	
Network Objects				
	0.0.0.0	0.0.0.0		
dmz-network	10.77.241.64	255.255.255.192		
📑 inside-network	10.10.10.0	255.255.255.0		
- 🛃 outside-networ	k 172.16.1.0	255.255.255.0		
i 🔂 🔂 🔂 🕹 🕹 🗠	10.20.10.0	255.255.255.0		
Detected Remote Networks	s 			
Kemote Networks ->	any			
				K Cancel

 Marque la casilla de verificación Exención del host/red del lado ASA de la traducción de direcciones para evitar que el tráfico del túnel pase por la traducción de direcciones de red. A continuación, haga clic en Next.

🖆 VPN Wizard		
VPN Wizard	Hosts and Networks	(Step 5 of 6)
Branch	An IPsec tunnel protec remote sites. Please id	ts data exchanged by selected hosts and networks at the local and entify hosts and networks to be used in the IPsec tunnel.
	Action:	Protect O Do not Protect
Home	Local Networks:	inside-network/24
Corporate	Remote Networks:	10.20.10.0/24
	Exempt ASA side l	host/network from address translation:
		< Back Next > Finish Cancel Help

15. En este resumen se muestran los atributos definidos por el Asistente para VPN. Vuelva a comprobar la configuración y haga clic en Finish cuando esté satisfecho con la configuración correcta.



Configuración de SDM del router

Complete estos pasos para configurar el Túnel VPN Sitio a Sitio en el Router Cisco IOS:

1. Abra el explorador e introduzca https://<IP_Address of the interface of the Router that has been configured for SDM Access> para acceder a SDM en el router.

Asegúrese de autorizar cualquier advertencia que le proporcione su navegador en relación con la autenticidad del certificado SSL. El nombre de usuario y la contraseña predeterminados están en blanco.

El router presenta esta ventana para permitir la descarga de la aplicación SDM. En este ejemplo se carga la aplicación en el equipo local y no se ejecuta en un subprograma Java.



- 2. La descarga de SDM comienza ahora. Una vez que se haya descargado el iniciador de SDM, complete los pasos indicados en las indicaciones para instalar el software y ejecutar el iniciador de SDM de Cisco.
- 3. Ingrese el Nombre de usuario y la Contraseña si especificó uno y haga clic en Aceptar.

Este ejemplo utiliza el cisco123 para el nombre de usuario y el cisco123 como la contraseña.

Authenticati	on Required 🛛 🔀
Java ⁻	
Enter login det /10.77.241.10	ails to access level_15 or view_access on 9:
User name:	cisco123
Password:	•••••
🔄 Save this p	assword in your password list
	OK Cancel
Authentication	scheme: Basic

4. Elija Configuration->VPN->Site-to-Site VPN y haga clic en el botón de opción situado junto a Create a Site-to-Site VPN en la página de inicio de SDM. A continuación, haga clic en Iniciar la tarea seleccionada como se muestra aquí:



5. Elija Step by step wizard para continuar con la configuración:



6. En la siguiente ventana, proporcione la Información de Conexión VPN en los espacios respectivos. Seleccione la interfaz del túnel VPN en la lista desplegable. Aquí, se elige FastEthernet0. En la sección Identidad de Peer, elija Peer con dirección IP estática y proporcione la dirección IP de peer remoto. A continuación, proporcione la clave previamente compartida (cisco123 en este ejemplo) en la sección Autenticación como se muestra. A continuación, haga clic en Next.

Site-to-Site VPN Wizard		
VPN Wizard	VPN Connection Information Select the interface for this VPN connection:	FastEthernet0
	Peer Identity Select the type of peer(s) used for this VPN connection: Enter the IP address of the remote peer: Authentication Authentication ensures that each end of the V Pre-shared Keys pre-shared key: Re-enter Key:	Peer with static IP address 172.16.1.1 VPN connection uses the same secret key. C Digital Certificates
		<back next=""> Finish Cancel Help</back>

7. Haga clic en Agregar para agregar propuestas IKE que especifican el algoritmo de cifrado, el algoritmo de autenticación y el método de intercambio de claves.

Site-to-Site VPN Wizard							K
VPN Wizard IKE Proposals IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote					l key exchange he remote e remote		
	device should be configured with at least one of the policies listed below. Click the Add button to add more policies and the Edit button to edit an existing policy.						
	Priority	Encryption	Hash	D-H Group	Authentication	Туре	
	Add	Edit					
				« Back Next	s Finish C	ancel Help	1

8. Proporcione el algoritmo de cifrado, el algoritmo de autenticación y el método de intercambio de claves como se muestra aquí, luego haga clic en Aceptar. Los valores del algoritmo de cifrado, del algoritmo de autenticación y del método de intercambio de claves deben coincidir con los datos proporcionados en el ASA.

Add IKE Policy	
Configure IKE Policy	
Priority:	Authentication:
1	PRE_SHARE
Encryption:	D-H Group:
DES	group2
Hash:	Lifetime:
SHA_1	24 0 0 HH:MM:SS
QK	Cancel Help

9. Haga clic en Next como se muestra aquí.

Site-to-Site VPN Wizard

×

VPN Wizard

IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit.. button to edit an existing policy.

	Priority	Encryption	Hash	D-H Group	Authentication	Туре
	1	3DES	SHA_1	group2	PRE_SHARE	User Defined
	2	DES	SHA_1	group1	PRE_SHARE	User Defined
	Add	Edit				
- 1 / Con						
and the second						
				1	1 1	1
				< Back Next	t> Finish (Cancel Help

10. En esta nueva ventana se deben proporcionar detalles del conjunto de transformación. El conjunto de transformación especifica los algoritmos Encryption y Authentication utilizados para proteger los datos en el túnel VPN. A continuación, haga clic en Agregar para proporcionar estos detalles. Puede agregar cualquier número de conjuntos de transformación según sea necesario. Para ello, haga clic en Agregar y proporcione los detalles.

Site-to-Site VPN Wizard		×
VPN Wizard	Transform Set A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below. Click the Add button to add a new transform set and the Edit button to edit the specified transform set. Select Transform Set Default Transform Set Details of the specified transform set	
IDA	Name ESP Encryption ESP Integrity AH Integrity ESP-3DES-SHA ESP_3DES ESP_SHA_HMAC	
	Ada Edit	

11. Proporcione los detalles de Transform Set (Encryption and Authentication Algorithm) y haga clic en OK como se muestra.

Ad	d Tran	sform Set		
Na	ame:	ASA-IPSEC		
		ata integrity with	encryption (ES	P)
	Integri	ty Algorithm:	ESP_SHA_H	MAC 🔽
	Encryp	tion Algorithm:	ESP_DES	-
1				Show Advanced >>
		ок	Cancel	Help

12. Elija el conjunto de transformación que se utilizará en la lista desplegable, como se muestra.

Site-to-Site VPN Wizard		×
VPN Wizard	Transform Set A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below. Click the Add button to add a new transform set and the Edit button to edit the specified transform set. Select Transform Set SDM Default Transform Set PtasA-IPSEC	
	Name ESP Encryption ESP Integrity AH Integrity ESP-3DES-SHA ESP_3DES ESP_SHA_HMAC Add Edit	
	< Back Next > Finish Cancel Hel	p

13. Haga clic en Next (Siguiente).

Site-to-Site VPN Wizard					×
VPN Wizard	Transform Set A transform set specifies the e data in the VPN tunnel. Since t communicate, the remote devi one selected below. Click the Add button to add a transform set. Select Transform Set ASA-IPSEC Details of the specified transform	ncryption and aut he two devices mo ce must be config new transform se	nentication algorithm ust use the same alg ured with the same t t and the Edit butto	ns used to protect the gorithms to transform set as the in to edit the specified	
	ASA-IPSEC	ESP Encryption ESP_DES	ESP Integrity ESP_SHA_HMAC	AH Integrity	
		« (Back Next > Fini	sh Cancel Hel	р

14. En la siguiente ventana, proporcione los detalles sobre el tráfico que debe protegerse a través del túnel VPN. Proporcione las redes de origen y de destino del tráfico que se va a proteger para que el tráfico entre las redes de origen y de destino especificadas esté protegido. En este ejemplo, la red de origen es 10.20.10.0 y la red de destino es 10.10.10.0. A continuación, haga clic en Next.

Site-to-Site VPN Wizard		
Site-to-Site VPN Wizard VPN Wizard	Traffic to protect IPSec rules define the traffic, such as file transferrences protected by this VPN connection. Other data tradevice. You can protect all traffic between a part specify an IPSec rule that defines the traffic type Protect all traffic between the following subnet Local Network Enter the IP address and subnet mask of the network where IPSec traffic originates. IP Address:	ers (FTP) and e-mail (SMTP) that will be affic will be sent unprotected to the remote icular source and destination subnet, or is to be protected. ts Remote Network Enter the IP Address and Subnet Mask of the destination Network. IP Address:
	10.20.10.0 Subnet Mask: 255.255.255.0 or 24	10.10.10.0 Subnet Mask: 255.255.255.0 or 24
	C Create/Select an access-list for IPSec traffic	V
		Back Next > Finish Cancel Help

15. Esta ventana muestra el resumen de la configuración VPN de sitio a sitio realizada. Marque la casilla de verificación Test VPN Connectivity after configuration si desea probar la conectividad VPN. Aquí, la casilla está marcada, ya que la conectividad debe estar marcada. A continuación, haga clic en Finalizar.

Site-to-Site VPN Wizard		X
VPN Wizard	Summary of the Configuration	
VPN WIZARD	Click Finish to deliver the configuration to the router.	tication Encryption HARE DES HARE 3DES
	Test VPN connectivity after configuring.	
	< Back	Next > Finish Cancel Help

16. Haga clic en Start como se muestra para verificar la conectividad VPN.

VPN Troubleshooting	2
Tunnel Details	
Interface: FastEthernet0 Peer: 172.16.1.1	
🔲 Summ	nany 🖳 Details
Activity	Status
Failure Reason(s) Recommended Action(s)	
Start Save Report Close	Help

17. En la siguiente ventana se proporciona el resultado de la prueba de conectividad VPN. Aquí puede ver si el túnel está activo o inactivo. En este ejemplo de configuración, el túnel es Up como se muestra en verde.

VPN Troubleshooting		×
Tunnel Details		1
Interface: FastEthernet0	Peer: 172.16.1.1	
	🔲 Summary 🛛 📓 Details	
Activity	Status	
Checking the tunnel status	O Up	
Failure Reason(s)	Recommended Action(s)	
]
Start Save Report	Close Help	

Esto completa la configuración en el router Cisco IOS.

Configuración CLI ASA

<#root>	
ASA#	
show run	
: Saved ASA Version 8.0(2) ! hostname ASA	

enable password 8Ry2YjIyt7RRXU24 encrypted names I !--- Configure the outside interface. ! interface Ethernet0/1 nameif outside security-level 0 ip address 172.16.1.1 255.255.255.0 !--- Configure the inside interface. ! interface Ethernet0/2 nameif inside security-level 100 ip address 10.10.10.1 255.255.255.0 !-- Output suppressed ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-group DefaultDNS domain-name default.domain.invalid access-list 100 extended permit ip any any access-list inside_nat0_outbound extended permit ip 10.10.10.0 255.255.255.0 10.20.10.0 255.255.255.0 !--- This access list (inside_nat0_outbound) is used !--- with the nat zero command. This prevents traffic which !--- matches the access list from undergoing network address tra (outside_1_cryptomap) . !--- Two separate access lists should always be used in this configuration. access-list outside_1_cryptomap extended permit ip 10.10.10.0 255.255.255.0 10.20.10.0 255.255.255.0 !--- This access list (outside_cryptomap) is used !--- with the crypto map outside_map !--- to determine which traffic should be encrypted and sent !--- across the tunnel. !--- This ACL is (inside_nat0_outbound)

. !--- Two separate access lists should always be used in this configuration.

pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm-613.bin asdm history enable arp timeout 14400 global (outside) 1 interface nat (inside) 1 10.10.10.0 255.255.255.0 nat (inside) 0 access-list inside_nat0_outbound !--- NAT 0 prevents NAT for networks specified in !--- the ACL inside_nat0_outbound access-group 100 in interface outside route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute http server enable http 0.0.0.0 0.0.0.0 dmz no snmp-server location no snmp-server contact !--- PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac !--- Define the transform set for Phase 2. crypto map outside_map 1 match address outside_1_cryptomap !--- Define which traffic should be sent to the IPsec peer. crypto map outside_map 1 set peer 172.17.1.1 !--- Sets the IPsec peer crypto map outside_map 1 set transform-set ESP-DES-SHA

!--- Sets the IPsec transform set "ESP-AES-256-SHA" !--- to be used with the crypto map entry "outside

crypto map outside_map interface outside

!--- Specifies the interface to be used with !--- the settings defined in this configuration.

!--- PHASE 1 CONFIGURATION ---! !--- This configuration uses isakmp policy 10. !--- The configuration

```
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption des
hash sha
group 1
lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
I
tunnel-group 172.17.1.1 type ipsec-121
!--- In order to create and manage the database of connection-specific !--- records for ipsec-121-IPse
tunnel-group
in global configuration mode. !--- For L2L connections the name of the tunnel group
MUST
be the IP !--- address of the IPsec peer.
tunnel-group 172.17.1.1 ipsec-attributes
pre-shared-key *
!--- Enter the pre-shared-key in order to configure the !--- authentication method.
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
ļ
```

```
class-map inspection_default
  match default-inspection-traffic
!
!
!
!
username cisco123 password ffIRPGpDS0Jh9YLq encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d
: end
```

Configuración CLI del router

```
<#root>
Building configuration...
Current configuration : 2403 bytes
I
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname R3
I
boot-start-marker
boot-end-marker
ļ
no logging buffered
1
username cisco123 privilege 15 password 7 1511021F07257A767B
no aaa new-model
ip subnet-zero
ļ
ļ
ip cef
1
1
ip ips po max-events 100
no ftp-server write-enable
I
crypto isakmp policy 2
authentication pre-share
!--- Specifies the pre-shared key "cisco123" which should !--- be identical at both peers. This is a g
```

```
crypto isakmp key ciscol23 address 172.16.1.1
ï
I
!--- Configuration for IPsec policies. !--- Enables the crypto transform configuration mode, !--- wher
crypto ipsec transform-set ASA-IPSEC esp-des esp-sha-hmac
ï
!--- !--- Indicates that IKE is used to establish !--- the IPsec Security Association for protecting t
crypto map SDM_CMAP_1 1 ipsec-isakmp
description Tunnel to172.16.1.1
!--- Sets the IP address of the remote end.
set peer 172.16.1.1
!--- !--- Configures IPsec to use the transform-set !--- "ASA-IPSEC" defined earlier in this configura
set transform-set ASA-IPSEC
!--- !--- Specifies the interesting traffic to be encrypted.
match address 100
i
!
ļ
!--- Configures the interface to use the !--- crypto map "SDM_CMAP_1" for IPsec.
interface FastEthernet0
ip address 172.17.1.1 255.255.255.0
duplex auto
speed auto
crypto map SDM_CMAP_1
interface FastEthernet1
ip address 10.20.10.2 255.255.255.0
duplex auto
```

```
speed auto
I
interface FastEthernet2
no ip address
ļ
interface Vlan1
ip address 10.77.241.109 255.255.255.192
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
I
I
ip nat inside source route-map nonat interface FastEthernetO overload
ļ
ip http server
ip http authentication local
ip http secure-server
I
!--- Configure the access-lists and map them to the Crypto map configured.
access-list 100 remark SDM_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
I
ļ
ļ
!--- This ACL 110 identifies the traffic flows using route map
access-list 110 deny ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
match ip address 110
I
control-plane
I
line con 0
login local
line aux 0
line vty 0 4
privilege level 15
login local
transport input telnet ssh
I
end
```

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.

- PIX Security Appliance Comandos show
- Router IOS remoto Comandos show

Dispositivo de seguridad ASA/PIX - Comandos show

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

<#root>
ASA#
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: 172.17.1.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE

show crypto ipsec sa—Muestra todas las SA IPSec actuales en un par.

```
<#root>
```

ASA#

show crypto ipsec sa

interface: outside Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)

current_peer: 172.17.1.1

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
 #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 9, #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.: 172.16.1.1, remote crypto endpt.: 172.17.1.1
      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: 434C4A7F
    inbound esp sas:
      spi: 0xB7C1948E (3082917006)
        transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x434C4A7F (1129073279)
         transform: esp-des esp-sha-hmac none
         in use settings ={L2L, Tunnel, PFS Group 2, }
        slot: 0, conn_id: 12288, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4274999/3588)
         IV size: 8 bytes
         replay detection support: Y
```

Router IOS remoto - Comandos show

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

show crypto ipsec sa—Muestra todas las SA IPSec actuales en un par.

```
local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  current peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
#pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)
     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
        transform: esp-des esp-sha-hmac,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
     outbound ah sas:
     outbound pcp sas:
```

 show crypto engine connections active: muestra las conexiones actuales y la información sobre los paquetes cifrados y descifrados (solo router).

<#root>

Router#

show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
3	FastEthernet0	172.17.1.1	set	HMAC_SHA+DES_56_CB	0	0
2001	FastEthernet0	172.17.1.1	set	DES+SHA	0	59
2002	FastEthernet0	172.17.1.1	set	DES+SHA	59	0

Troubleshoot

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.

Nota: Consulte <u>Información Importante sobre Comandos Debug</u> y <u>Solución de Problemas de</u> <u>Seguridad IP - Comprensión y Uso de Comandos debug</u> antes de utilizar los comandos debug.

• debug crypto ipsec 7 — Muestra negociaciones IPsec de la Fase 2.

debug crypto isakmp 7 — Muestra negociaciones ISAKMP de la Fase 1.

• debug crypto ipsec — Muestra los IPSec Negotiations de la Fase 2.

debug crypto isakmp — Muestra las negociaciones ISAKMP para la fase 1.

Consulte <u>Soluciones de Troubleshooting de VPN IPSec de Acceso Remoto y L2L Más Comunes</u> para obtener más información sobre cómo resolver problemas de VPN de Sitio-Sitio.

Información Relacionada

- <u>Cisco PIX Firewall Software</u>
- <u>Cisco Adaptive Security Device Manager</u>
- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>Ejemplo de Configuración Profesional: VPN IPsec de Sitio a Sitio entre ASA/PIX y un Router</u>
 <u>IOS</u>
- <u>Referencias de Comandos de Cisco Secure PIX Firewall</u>
- <u>Cisco Router and Security Device Manager</u>
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).