Ejemplo de Configuración de Túnel IPsec de LAN a LAN entre un Cisco VPN 3000 Concentrator y un Router con AES

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Convenciones Configurar Diagrama de la red Configuraciones Configuración del concentrador VPN Verificación Verifique la configuración del router Verifique la configuración del concentrador VPN Troubleshoot Resolución de Problemas en el Router Solución de problemas del concentrador VPN Información Relacionada

Introducción

Este documento muestra cómo configurar un túnel IPsec entre un Cisco VPN 3000 Concentrator y un router Cisco con Advance Encryption Standard (AES) como algoritmo de cifrado.

AES es una nueva publicación de la Norma Federal de Procesamiento de la Información (FIPS) creada por el Instituto Nacional de Normas y Tecnología (NIST) para ser utilizada como método de encriptación. Este estándar especifica un algoritmo de cifrado simétrico AES que reemplaza el estándar de cifrado de datos (DES) como transformación de la privacidad tanto para IPsec como para el intercambio de claves de Internet (IKE). AES tiene tres longitudes de clave diferentes, una clave de 128 bits (la predeterminada), una clave de 192 bits y una clave de 256 bits. La función AES de Cisco IOS® añade compatibilidad con el nuevo estándar de cifrado AES, con el modo de encadenamiento de bloques de cifrado (CBC), a IPsec.

Refiérase al <u>sitio</u> <u>del Centro</u> de Recursos de Seguridad Informática de NIST para obtener más información sobre AES.

Consulte <u>Ejemplo de Configuración de IPsec de LAN a LAN entre el Concentrador VPN 3000 de</u> <u>Cisco y el Firewall PIX</u> para obtener más información sobre la configuración de túnel de LAN a LAN entre un concentrador VPN 3000 y un Firewall PIX.

Consulte Ejemplo de Configuración del Túnel IPSec entre PIX 7.x y VPN 3000 Concentrator para obtener más información cuando el PIX tiene la versión de software 7.1.

Prerequisites

Requirements

Este documento requiere una comprensión básica del protocolo IPSec Consulte <u>Introducción al</u> <u>Cifrado IPSec</u> para obtener más información sobre IPsec.

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Requisitos del router: la función AES se introdujo en la versión 12.2(13)T del software del IOS de Cisco. Para habilitar AES, el router debe soportar IPsec y ejecutar una imagen IOS con claves largas "k9" (el subsistema "k9").Nota: El soporte de hardware para AES también está disponible en los módulos VPN de aceleración AES 2600XM, 2691, 3725 y 3745 de Cisco. Esta función no tiene implicaciones de configuración y el módulo de hardware se selecciona automáticamente si ambos están disponibles.
- Requisitos del concentrador VPN El soporte de software para la función AES se introdujo en la versión 3.6. El nuevo procesador de cifrado mejorado y escalable (SEP-E) proporciona soporte de hardware. Esta función no tiene implicaciones para la configuración.Nota: En Cisco VPN 3000 Concentrator versión 3.6.3, los túneles no negocian con AES debido al ID de bug de Cisco <u>CSCdy88797</u> (sólo para clientes registrados). Esto se ha resuelto desde la versión 3.6.4.Nota: El Cisco VPN 3000 Concentrator utiliza módulos SEP o SEP-E, no ambos. No instale ambos en el mismo dispositivo. Si instala un módulo SEP-E en un concentrador VPN que ya contiene un módulo SEP, el concentrador VPN inhabilita el módulo SEP y utiliza solamente el módulo SEP-E.

Componentes Utilizados

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

- Cisco 3600 Series Router con Cisco IOS Software Release 12.3(5)
- Concentrador VPN 3060 de Cisco con versión de software 4.0.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

<u>Configurar</u>

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

documento.

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

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Router IPsec
- <u>Concentrador VPN</u>

Configuración de IPSec_Router
version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
!
! Configuration for IKE policies. crypto isakmp

```
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
!
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
1
ip nat pool mypool 30.30.30.3 30.30.30.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
configuration exempts !--- the LAN-to-LAN traffic from
```

```
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

Nota: Aunque la sintaxis de ACL no se modifica, los significados son ligeramente diferentes para las ACL crypto. En las ACL crypto, **permit** especifica que los paquetes coincidentes deben ser cifrados, mientras que **deny** especifica que los paquetes coincidentes no necesitan ser cifrados.

Configuración del concentrador VPN

Los concentradores VPN no están preprogramados con direcciones IP en sus configuraciones de fábrica. Debe utilizar el puerto de la consola para configurar las configuraciones iniciales que son una interfaz de línea de comandos (CLI) basada en menús. Consulte <u>Configuración de</u> <u>Concentradores VPN a través de la Consola</u> para obtener información sobre cómo configurar a través de la consola.

Después de configurar la dirección IP en la interfaz Ethernet 1 (privada), el resto se puede configurar mediante la CLI o a través de la interfaz del explorador. La interfaz del explorador admite HTTP y HTTP a través de Secure Socket Layer (SSL).

Estos parámetros se configuran a través de la consola:

- Hora/Fecha: la hora y la fecha correctas son muy importantes. Ayudan a garantizar que las entradas de registro y de contabilidad sean exactas y que el sistema pueda crear un certificado de seguridad válido.
- Interfaz Ethernet 1 (privada): dirección IP y máscara (de nuestra topología de red 172.16.1.1/24).

En este momento, el VPN Concentrator es accesible a través de un navegador HTML desde la red interna. Para obtener información sobre la configuración del concentrador VPN en modo CLI, refiérase a <u>Configuración Rápida con CLI</u>.

 Escriba la dirección IP de la interfaz privada desde el navegador web para habilitar la interfaz GUI.Haga clic en el icono guardar los cambios necesarios para guardar la memoria. El nombre de usuario y la contraseña predeterminados de fábrica son "admin", que distingue entre mayúsculas y minúsculas.

	VPN 3000	Main Help Support Logout
	Concentrator Series Manager	Looned in: admin
		Configuration Administration Monitoring
⊞Conflouration ⊞Administration ⊞Mentiorine	Main Welcome to the VFH 3000 Concentrator Manager. In the left frame or the an-significe bar whove, click the function, you want: • Configuration - to configure all Sectures of this device. • Administration - to configure all Sectures of this device. • Montoning to continue administrative functions on this device. • Montoning to relate a status status and logs on this device. • Main to return to this scenen. • Main to so get help for the orment scene. • Main to so get help for the orment scene. • Main to so get or this scenen. • Main to so get or this scenen. • Main to so get or this scene Media • Main to so get or this scene media • Main to so get or this scene media • Main to so get or this scene media • Main to so get while the scene media • Main to so get while the scene media • Main to so get while the scene media • Main to so get while the scene media • Main to so get help for the scene media • Main to so get help for the scene media • Main to so get help for the scene media • Main to get or this scene media • Main to get or this scene media • Main to get or the scene scene media	

2. Después de activar la GUI, seleccione **Configuration > Interfaces > Ethernet 2 (Public)** para configurar la interfaz Ethernet

2.						
Configuration			I Ethnored 3			
Configuration Interfaces Ethernet 2						
EHUser Management Co	autica	uring Ethernet Interfa	ce 2 (Public).			
Policy Management	-	•	,			
- Administration	Gene	ral RIP OSPF B	andwidth			
			Gener	ral Parameters		
1	Sel	Attribute	Value		Description	
	0	Disabled			Select to disable this interface.	
	c	DHCP Client			Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.	
	6	Static IP Addressing				
		IP Address	20.20.20.1		Select to compute the IP Address and Subnet Mask.	
		Subnet Mask	255.255.255.0		Intelable.	
		Public Interface	N		Check to make this interface a "public" interface.	
		MAC Address 00.90 A4.00.41 F9 7		The MAC address for this interface.		
		Filter	Filter 2. Public (Defoult)		Select the filter for this interface.	
		Speed	10/100 auto 💌		Select the speed for this interface.	
		Duplex	Auto 💌		Select the duplex mode for this interface.	
		MTU	1500		Enter the Maximum Transmit Unit for this interface (63 - 1500).	
	Public Interface IPSec Fragmentation Policy		C Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission			
			¹ C Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)		MTU Discovery (ICMP)	
			C Fragment prior to IPSec enc	opsulation without P	ath MTU Discovery (Clear DF bit)	
Ciera Svetsme						
the state of a state o	Ap	oply Cancel				

3. Seleccione Configuration > System > IP Routing > Default Gateways configure el gateway predeterminado (Internet) y el gateway predeterminado (interno) del túnel para IPsec para alcanzar las otras subredes en la red privada.En este escenario, sólo hay una subred disponible en la red interna.

<u>Configuration</u>		
	Configuration System IP Routing De	efault Gateways
- () System		
- Bervers	Configure the default sateways for your system.	
Address Management		
- El-Tunneting Protocols		
- CP Routing	Default Gateway 20.20.20.2	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for an default router.
Static Routes	Matrix 1	Enter the metric from 1 to 16
Default Gateways	Nor unit:	Enter the metric, from t to ro.
OSPE	Tunnel Default 172 16 1 2	Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no
OSPE Areas	Gateway Trainer	default router.
DHCP Parameters	Override Default	Check to allow bound default externance to councils the confirmed default externan
DHCP Relay	Gateway 🥙	Check to many learnes determ gareways to overtale the configures determ gareway.
Redunciancy	Annta Canad	
Reverse Route Injection	Appiy Concei	
- III-Management Protocols		
- Events		
General		
- El Client Lipdate		
Load Balancing		
El-User Management		
Policy Management		
+++Administration		
-E-Monitoring		

4. Seleccione Configuration > Policy Management > Traffic Management > Network Lists > Add para crear las listas de red que definen el tráfico que se cifrará.Las redes mencionadas en la lista son accesibles a la red remota. Las redes que se muestran en la siguiente lista son redes locales. También puede generar la lista de red local automáticamente a través de RIP al hacer clic en Generar lista

local.		
	Configurati	on Policy Management Traffic Management Network Lists Modify
- (I) System		
- Oser Management	Modify a confi	gued Network List, Click on Generate Local List to generate a network list based on routing entries on the Private interface.
Access Hours		
	List Name	vpn_locdl_network Name of the Network List you are acking. The name must be unaque.
Network Lists		172 . 16 . 0 . 0/0 . 0 . 255 . 255
Rules		Control by Chorness and Wildshift makes using the following Control by Physical Phys
<u>SAs</u>		 Note: Functional and the second second
Filters		• Index in the second s
-ENAT		ignore. Os in bit positions to match. For example,
BYV Policies	Network List	10 10.1 0/0.00 255 = all 10.10.1 reas addresses.
Group Matching	2 contraction maps	 Each Network and Wildcard mask pair must be entered on a
- Administration		single line.
- Monitoring		 The Wildrard mask may be omitted if the natural Wildrard
		weak is to be used.
		31 31 31 31 31 31 31 31 31 31 31 31 31 3
	Apply	Concel Generate Local List
	. 499	

5. Las redes de esta lista son redes remotas y deben configurarse manualmente. Para hacer esto, ingrese la red/comodín para cada subred

alcanzable.	Configuration Modify a configu	n – Policy Management – Trat red Network List Click on Generat	fic Management Network Lists Modily e Local List to generate a network list based on routing entries on the Private interface.
Diratic Monacement Getwork Lists Gidea SAs Giters Gidea G	Network List	192.168.20.0/0.0.0.255	 Enter the Network Like yea are saling. The barry must be during: Enter the Networks and Wildows' masks using the following format: ananan/manan (e.g. 10.10.0.00.0.255 253). Note: Enter a wildows' mask, which is the reverse of a subnet mask. A wildows' mask has it in bit positions to ignore, 0s in bit positions to metch. For example, 10.10.1.00.0.0.255 - all 10.10.1 nm addresses. Each Network and Wildows' mask pair must be extend on a single line. The Wildows' mask muy be omitted if the natural Wildows' must us to be used.
	Apply	Cancel Generate L	ocal List

Una vez terminado, estas son las dos listas de red:

El Configuration	Configuration Policy Managem	nent Traffic Management Netw	ork Lists	
				Save
Access Hours	This section lets you add, modify, copy, a	and delete Network Lists.		
Traffic Management	Click Add to create a Network List, or self	ect a Network List and click Modify, Copy	, or Delete.	
		Network List	Actions	
		VPN Client Local LAN (Defaulf) Vpn_remote_network		
Broup Matching		vpn_local_network	Add	
-@Administration -@MonKoring			Copy	
			Delete	

6. Seleccione Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add y defina el túnel de LAN a LAN.Esta ventana tiene tres secciones. La sección superior es para la información de red y las dos secciones inferiores son para las listas de red local y remota. En la sección Network Information (Información de red), seleccione el cifrado AES, el tipo de autenticación, la propuesta IKE y escriba la clave previamente compartida. En las secciones inferiores, señale las listas de red que ya ha creado, tanto las listas Local como Remota, respectivamente.

- 				
	Configuration System Tunneling Protocols IPSec LAN-to-LAN Add			
- (T) Servers	Add a new IPSec LAN-to-LAN connection			
-CP-Tunnelino Protocols 	Enable 🖻	Check to earlie this LAN-to-LAN connection.		
	Name test	Enter the name for this LAN-to-LAN connection.		
LAN-to-LAN	Interface Ethernet 2 (Public) (20.20.20.1)	Select the interface for this LAN-to-LAN connection.		
<u>NAT Transparency</u>	Connection Type Bi-directional	Choose the type of LAN-to-LAN connection. An <i>Originato-Only</i> connection may have multiple poors opecified below.		
	30.30.30.1 · · ·	Inter the tenacte peer IP addresses for this LAN-to-LAN connection. Originate $\Omega(p)$ connection may specify up to ten peer IP addresses. Enter one IP address per line.		
	Digini Certificate None (Use Preshared Keys) 💌	Solect the digital contificate to use.		
-39- <u>Moniforina</u>	Certificate C Entire certificate chain. Transmission (*) Identity certificate only	Choose how to send the digital certificate to the DCE peer.		
	Preshared Key cisco123	Enter the preshared key for this LAN-to-LAN connection.		
	Authentication ESP/MD5/HMAC-128 -	Specify the packet authentication mechanism to use.		
Cisco Systems	Encryption AES-256	Specify the encryptica methanism to use.		
	IKE Proposal KE-AES256-SHA	Select the IKE Proposal to use for this LAN-to-LAN connection.		

-Denfiguration Interfaces		
- E-Sarvaris		
- El-Ackress Management		
E-Tunneling Protocols		
PPTP		Channe the filter to another to the traffic that is translad through this 1 kM to 1 kM
L2TP	Filter -None-	consistent and the appropriate and a reasonable through the bence-to-bence
E-PSsc		Plank to M MST T concertified 195cs many establish this 1.610 to 1.630
LAN-20-LAN	IDSAN NATIT.	consisting thereads a M.6 T charing. Vice parts also availed This Likewise M.8 T. T under
HE Proposals	I Ber Dell-1	NAT Transmerer
NAT Transparency		ters ranopunky.
Abrix	Bandwidth Policy None-	Discose the bandwidth policy to apply to this LAN-to-LAN connection.
-E-P Routing	Provident Islam	Choose the routing mechanism to use Parameters helow are ignored if Network
El-Management Protocols	Komag None	Autodiscovery is chosen.
- Events		-
- E General	Local Neissark: If a LAN-to-LAN NAT rule is used, this is the Translat	ted Network address.
- El-Client Update		Specify the local network address list or the IP address and wildcard reask for this
Load Balancing	Network List Vpn_local_network	LAN-to-LAN connection.
	IP Address	Note: Enter a wildcard mark, which is the program of a submet mark. A
Access Hours		wildrand mask has 1s in bit positions to imore. Us is bit positions to match. For
- E-Traffic Management	Wildcard Maste	szample, 10.10.1.00.0.0.255 = all 10.10.1 mm addresses.
E-Broup Matching		
-33 <u>Administration</u>	Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remo	te Network address.
- Monitoring		I Specify the senate returnsk address list or the IP address and address have for
	Network List vpn_remote_network	this LAN-to-LAN connection.
	T (1)	
	II' Address	Note: Enter a widdoord mask, which is the process of a submet mask. A
		wildcard mask has is in bit positions to ignore. Us in bit positions to match. For
	Willicard Mark	ransple, 10.10.1 0.0.0.0.255 = al 10.10.1 ann adáresses.
Cisco Sestems		•
- A	Add Concel	
- منا التسط التس		

7. Después de hacer clic en **Agregar**, si la conexión es correcta, aparecerá la ventana IPSec LAN-to-LAN-Add-Done (IPSec LAN a LAN-Add-Done).Esta ventana presenta una sinopsis de la información de configuración del túnel. También configura automáticamente el nombre de grupo, el nombre SA y el nombre de filtro. Puede editar cualquier parámetro de esta tabla

Configuration	
	Configuration System Tunneling Protocols IPSec LAN-to-LAN Add Done
- Existen	Save Needed
- I Servers	
- Charlese Management	An IPSet LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:
Tunneling Protocols	
	Authentication Server Internal
	Group 20:20:20.1
LANHO-LAN	Security Association 1.21. test
KE Processis	en a 124 test Out
NAT Transportency	Pilter Rules 1.2. had In
- OP Routing	Modifying any of these iters will effect the LAN-Io-LAN configuration. The Group is the same as your LAN-Io-LAN peer. The Security Association and
- CHManagement Protocols	Filler Rules all start with "L2L2" to indicate that they form a LAN-to-LAN configuration.
- TROINT Under	OK I
Load Balancing	
FiUser Management	
EPplicy Management	
Administration	
Monitoring	

En este punto, el túnel de LAN a LAN IPSec se ha configurado y puede comenzar a funcionar. Si, por alguna razón, el túnel no funciona, puede verificar si hay configuraciones erróneas.

 Puede ver o modificar los parámetros IPsec de LAN a LAN creados anteriormente cuando seleccione Configuration > System > Tunneling Protocols > IPSec LAN a LAN.Este gráfico muestra "prueba" como el nombre del túnel y la interfaz pública del extremo remoto es 30.30.30.1 según el escenario.

-G-Configuration			
Interfaces	Configuration System Tunneling Pr	otocols IPSec LAN-to-LAN	
- G-System			Save
- DServers			
	This section lats you configure IPSec LAN-to-LA	N connections I AN-to-LAN connections are se-	shished with other VPN 3000 Concentrators
	PEX firewalls, 7100/4000 series contens and other	IPSec-compliant security gateways. To configure	e a VPN 3002 or other remote access
<u>PPTP</u>	connection, go to Uper Management and configure	a Group and User. To configure NAT over LAI	N-to-LAN, go to LAN-to-LAN NAT Rules.
L2TP			10
EHPSeo	If you want to define a set of networks on the loc	al or remote side of the LAN-to-LAN connection	, configue the necessary Network Lists prior
LAN-to-LAN	to creating the connection.		,
KE Proposals			
	Click the Add button to add a LAN-to-LAN core	action, or select a connection and click Modify a	: Delete.
<u>Nerts</u>		,,-	
	(D) indicates a disabled LAN-to-LAN connection	L.	
Hianagement Protocols	,_,		
- Events		TAN - TAN	
- D <u>General</u>		Comparation	A-+15
- Dient Update		Condection	Actions
Load Balancing	test (30.30.3	0.1) on Ethernet 2 (Public)	
- @- <u>User Manacement</u>			Add
- (=) Policy Management			7455
Access Hours			Modity
NEWOOK LESIS			Delete
Steel Steel			
<u>ons</u> Dime			
TELES S			
- Carrier Metriking			
- Administration			

9. A veces, es posible que su túnel no aparezca si su propuesta IKE está en la lista Propuestas inactivas. Seleccione Configuration > System > Tunneling Protocols > IPSec > IKE Proposale para configurar la propuesta IKE activa.Si su propuesta IKE está en la lista "Propuestas inactivas", puede activarla cuando seleccione la propuesta IKE y haga clic en el botón Activate. En este gráfico, la propuesta seleccionada "IKE-AES256-SHA" se encuentra en la lista de propuestas



 Seleccione Configuration > Policy Management > Traffic Management > Security Associations para verificar si los parámetros SA son correctos.



 Haga clic en el nombre SA (en este caso, L2L: test), y luego haga clic en Modify para verificar las SA.Si alguno de los parámetros no coincide con la configuración del par remoto, puede cambiarse

aqui.		
Configuration	Configuration Policy Management Traffic Managem	rent Security Associations Modify
	Modify a coafigured Security Association.	
Definition	S& Name L2L: test Inheritance From Bule	Specify the name of this Security Association (SA). Select the genularity of this SA.
CHPSec	IPSec Parameters	
NAT Transparency	Algorithm ESP/MD5/HMAC-128	Select the packet authentication algorithm to use.
<u>Alerts</u> EP Routing	Encryption Algorithm AES-256	Select the ESP encryption algorithm to use.
El-Management Protocols	Encapsulation Mode Tunnel 💌	Select the Encapsulation Mode for this SA.
-E-General -E-General	Servery Disabled	Select the use of Perfect Forward Secrecy.
	Lifetime Measurement	Select the lifetime measurement of the IPS+: heye
Policy Management	Data Lifetime 10000	Specify the data lifetime in kilobytes (ICB).
Access Hours	Time Lifetime 28800	Specify the time lifetime in seconda.
Rules	IKE Parameters	
Elters	Connection Type Hidrectional IKE Press 30 30 30.1	The Connection Type and IKE Force cannot be modified on IFSec SA that is part of a LAN-to-LAN Connection.
EV(Policies	Negatiation Mode Main 💌	Select the IKE Negotiation mode to use.
E-B-Group Matching	Digital Certificate None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
-E-Monitoring	Contificate C Entire contificate chain. Transmission @ Identity contificate only	Chooses how to send the digital cartificate to the $1\mathrm{K\Sigma}$ power.
	IKE Proposal IKE AES256 SHA	 Select the IKE Proposal to use as IKE initiator.
CISCO SUSTEMS	Apply Concel	

Verificación

Verifique la configuración del router

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta <u>Output Interpreter</u> (sólo para clientes registrados) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

 show crypto isakmp sa — Muestra todas las asociaciones actuales de seguridad (SA) IKE de un par. El estado QM_IDLE indica que la SA permanece autenticada con su peer y se puede utilizar para los intercambios de modo rápido subsiguientes. Está en estado de quietud. ipsec_router#show crypto isakmp sa

```
dst src state conn-id slot
20.20.20.1 30.30.30.1 QM_IDLE 1 0
```

show crypto ipsec sa — Muestra la configuración actual utilizada por las SA actuales
 Verifique la dirección IP par, las redes accesibles en los extremos remotos y locales y la
 transformación fijada que se utiliza. Hay dos ESP SA, uno en cada dirección. Dado que se
 utilizan conjuntos de transformación AH, está vacío.
 ipsec_router#show crypto ipsec sa

```
interface: Ethernet1/0
```

Crypto map tag: vpn, local addr. 30.30.30.1

protected vrf:

```
local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
```

remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

current_peer: 20.20.20.1:500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145

#pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 6, #recv errors 0

local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1

path mtu 1500, media mtu 1500

current outbound spi: 54FA9805

inbound esp sas:

spi: 0x4091292(67703442)

transform: esp-256-aes esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn

sa timing: remaining key lifetime (k/sec): (4471883/28110)

```
IV size: 16 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x54FA9805(1425709061)
transform: esp-256-aes esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4471883/28110)
IV size: 16 bytes
replay detection support: Y
outbound ah sas:
```

outbound pcp sas:

 show crypto engine connections active: muestra las conexiones de sesión cifradas activas actuales para todos los motores criptográficos. Cada ID de conexión es único. El número de paquetes cifrados y descifrados se muestra en las dos últimas columnas.
 ipsec router#show crypto engine connections active

psec_rou	acer#Bilow crypt	to engrine com	leccroms	accive		
ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	Ethernet1/0	30.30.30.1	set	HMAC_SHA+AES_256_C	0	0
2000	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	0	19
2001	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	19	0

Verifique la configuración del concentrador VPN

Complete estos pasos para verificar la configuración del VPN Concentrator.

 De manera similar a los comandos show crypto ipsec sa y show crypto isakmp sa en los routers, puede ver las estadísticas de IPsec e IKE cuando selecciona Monitoring > Statistics > IPSec en los concentradores VPN.

-= Configuration	Monitoring Statistics II	PSec		Thursday	, U1 Ja	muary 2004 19:32:36
Cierioces						Reset 🥔 Refresh 🔞
- FiUser Management		IKE (Phase 1) Statistics	IPSec (Phase 2) Statistics			
- ⊕Policy Management		Active Tunnels	L	Active Tunnels	l	
Access Hours		Total Tunnels	2	Total Tunnels	2	
Network Lists		Received Bytes	3545268	Received Bytes	3602	
Fules		Sent Bytes	5553204	Sent Bytes	5376	
<u>SAs</u>		Received Packets	60187	Received Packets	145	
Eitera Gibist		Sent Packets	60299	Sent Packets	-51	
BAY Policies		Received Packets Dropped	0	Received Parkets Dropped	0	
		Sent Packets Dropped	D	Received Parkets Dropped (Anti-Replay)	0	
GAdministration		Received Notifies	60084	Sent Packets Dropped	0	
E:Software Undete		Seat Notifies	120172	Inbound Authentirations	145	
Concentrator		Received Phase-2 Exchanges	2	Failed Inbound Authentications	0	
Cients Custos Dabast		Sent Phase-2 Exchanges	49	Outbound Authentirations	St	
	Inc	ulid Phase-2 Exchanges Received	D	Failed Outbound Authentications	U	
Elba	Б	invalid Phase-2 Exchanges Sent	0	Decryptions	145	
Monitoring Retresh	Reje	erted Received Phase-2 Exchanges	0	Failed Decryptions	0	
EFAccess Hams	R	ejected Sent Phase-2 Exchanges	0	Encryptions	51	
Swap Confio File	Pha	se-2 SA Delete Requests Received	0	Failed Encryptions	0	
TFTP Transfer	PI	hase-2 SA Delete Requests Sent	50	System Capability Failures	0	
XML Export		Initiated Tunnels	0	No. SA Failures	0	
EPCertricate Management		Failed Initiated Tunnels	0	Protocol Use Failures	U U	
Enrollment		Failed Bemote Tunnels	0			
		Authentication Failures	0			
Routing Table		Decryption Failures	D			
Dynamic Fiftero		Hash Validation Failures	0			
Cisco Systems		System Capability Failures	0			
ալիթացիթա		No-SA Failures	0			

2. Al igual que el comando **show crypto engine connections active** en los routers, puede utilizar la ventana Administration-Sessions en el VPN Concentrator para ver los parámetros y estadísticas de todas las conexiones o túneles IPsec LAN a LAN

activos.										
Configuration	Administration I Ad	Iminister Ses	sions					Thursday	. 01.Jan	Lary 2004 19:30:2
- Er Systen									R	eset 🥔 Refresh 🔞
E-Lister Management										
Actes Hours	This screen shows statis on that session's name. T	tios for sessions. In log out a sessio	To refleck the statis or chick Lagrant in th	tias, click Refr e w table below: "	sla Selett In test the	a Group to network o	r filter the se connection to	ssions. For m a session, chi	uore informa ck Pine	rtion on a session, clid
- EFIraffic Management	Co. Har book on b band. 1	o segundadores	of other page at the	N 0000 00071.	0.0001.000	20111012.0	current of		arme.	
Network Lists	Group -AI-	-								
SA2	Legout All: PPTP User	12TP User IP	lec User IPSec LA1	I-to-LAN						
ENAL	Session Summary									
	Active LAN-ta- LAN Sessions	Active Remat Access Sessio	e Active Mana IS Session	gement Tot 15 S	d Artive ssions	Peak C Set	oncurrent ssions	Concurrent Total Cumula Sessions Limit Sessions		Total Cumulative Sessions
Administer Sessions	1	0	L	1 2 3		3	4000 19		19	
<u>Concentrator</u> <u>Clientz</u>	LAN-ta-LAN Sessions [Remote Access Sessions Management Sessions]									
System Reboot Reboot Status	Connection Name	IP Address	Protocol	Encryptio	a Log	in Tinus	Duration	Bytes Tx	Byles Rx	Actions
Ping	test	30.30.30.1	IPSeo/LAN-to-LAN	AES-256	Just	19:57:29	0:02:51	2128	2128	[Logent Ping]
Monitorine; Retreph										
E Fle Management	Remote Access Sessions [LAN-to-LAN Sessons [Management Sessions]									
Hardenhouse Management	Usemane	Assigned IP Ai Public IP Add	dress <u>Gran</u>	p. Proto- Encryp	ol ion	Login Ti Duratio	me <u>C</u> n	lient Type Version	Bytes Bytes	Tx Artions
	No Remote Access Sessions									
	Management Sessions [LAN-to-LAN Sessions Bernote Access Sessions]									
	Administrator	IP Addre	ss Protocol	Encrypt	-	Legin	Time	Duratie	h	Artiens
	admin.	172.161.2	HTTP	None	Ja	a 01 19:17	42	0:12:38	Log	of [Ping]

Troubleshoot

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

Resolución de Problemas en el Router

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> antes de utilizar los comandos **debug**.

- debug crypto engine: muestra el tráfico cifrado. El motor criptográfico es el mecanismo real que realiza el cifrado y el descifrado. Un motor criptográfico puede ser un software o un acelerador de hardware.
- debug crypto isakmp: muestra las negociaciones ISAKMP (del inglés Internet Security Association and Key Management Protocol, Asociación de seguridad de Internet y protocolo de administración de claves) de la fase IKE 1.
- debug crypto ipsec: muestra las negociaciones IPSec de la fase IKE 2.

Refiérase a <u>Resolución de Problemas de IPSec - Comprensión y Uso de Comandos **debug** para obtener información más detallada y salida de ejemplo.</u>

Solución de problemas del concentrador VPN

Al igual que los comandos **debug** en los routers Cisco, puede configurar las clases Event para ver todas las alarmas.

1. Seleccione Configuration > System > Events > Classes > Add para activar el registro de clases de evento.Estas clases están disponibles para

IPSec:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE

Configuration							
	Configuration System Events Classes						
- C System	Save Needed						
E)Address Management	This section late two sevents have there of execute sevent abases						
EPTunneling Protocols	The second its you configure shown instantifier shown endows.						
-EHE Routing	Click for Add better to odd or struct store president or struct shore and ship. Maddle or Dallate						
E Management Protopols	Care are sum out on the design of seven and seven and seven and seven these water the seven and seven and seven						
- Events	Citizh han in an Sana an an I ann an Anna an						
General	Cark new to complete generativent parameters.						
ETP Backup							
Characters	Canfigured						
Trap Destinations	Erent Classes Actions						
	IKEDECODE						
<u>SMIP Servers</u>	IPSECDEG						
Ernal Recipients	MB2TRAP						
- ED-General	Add						
-E-Client Update	Monity						
Load Balancing	Mobily						
	Delete						
Administration							
Him Monitoring							

2. Al agregar, también puede seleccionar el nivel de gravedad para cada clase, en función del nivel de gravedad que se envía la alarma.Las alarmas pueden manejarse mediante uno de estos métodos:Por registroSe muestra en la consolaEnviado al servidor UNIX SyslogEnviado como correo electrónicoEnviado como trampa a un servidor SNMP



3. Seleccione **Monitoring > Filterable Event Log** para monitorear las alarmas

activadas.

- PConfiguration								
	Monitoring Filterable Event Log							
- (I) Servers	Select Filter Ontions							
	Farmi Close Disclosure Servicies (1)							
	AI Closses ALLA							
- IP Routing								
	AUTHORG 2							
- C) Events	AOTHDEOGDE M 3 M							
General	Client IP Address 0.0.0.0 Erents@age 100 v							
ETP Backup								
<u>Classes</u>	Group -All- Direction Oldest to Newest 💌							
Trap Destinations								
Systog Servers	GetLog SaveLog GearLog							
SMTP Servers								
Enell Recipients								
- (3) Client Lipolate	37992 01/02/2004 11:58:29.540 SEV-8 TKEDECODE/0 RFT-61097 30.30.30.1							
Load Balancing	IBARND HIADED : (Version 1.0)							
- FEH <u>User Management</u>	Initiator Cookie(8): AS AS 80 63 09 CA 55 25							
EPolicy Management	Responder Cookie(0): CD BZ 66 02 06 0D 12 60							
-3:Administration	Sext Payload : HASH (8)							
- Monitoring	Exchange Type : Dakley Informational							
Routing Table	Figs : 1 (DUPY); Berger ID : a3900ed							
Dynamic Filters	Leverage LD : adduced							
- Filerable Event Log	Jengun 76							
Live Event Log	37999 01/02/2004 11:58:28.540 SEV-# IKEBECODE/0 BUT-61098 30.30.1							
System Status	Rotify Fayload Decode :							
-EK <u>Sessions</u>	DOI : IPSEC (1)							
- En Statistics	Protocal : ISANY (1)							
	Berrage : DPD 1-0-THER1-ACK (36137)							
	Spi : AD AD CC 63 CD CA 53 25 6D 12 66 02 16 CD 12 6C							
	lengta : de							
	38885 01/02/2004 11:58:48.540 SEV-8 INEDECODE/0 80T-61039 30.30.1							
	ISACHP HIADER : Version 1.0)							
Caseo Systems	Initiator Cookie(8): A0 A0 SC 53 09 CA 55 25							
	Responder Coohie(8): 68 82 66 02 86 0D 12 60							
ومتاليت متاليت	Sext Jayload : HASH (8)							
	Erchange Type : Dakley Informational							

Información Relacionada

- Advanced Encryption Standard (AES)
- <u>Módulo de cifrado VPN DES/3DES/AES</u>
- <u>Configuraciones de ejemplo de IPSec</u>
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de Soporte de IPSec Negotiation/IKE Protocols