Configuración de un túnel IPSec entre un concentrador VPN 3000 de Cisco y un firewall NG de punto de control

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Convenciones Diagrama de la red Configuraciones Configurar el concentrador VPN 3000 Configuración del punto de control NG Verificación Verificar la comunicación de red Ver el estado del túnel en el punto de control NG Ver el estado del túnel en el concentrador VPN Troubleshoot Resumen de la red Depuración del punto de control NG Depuración del concentrador de VPN Información Relacionada

Introducción

Este documento muestra cómo configurar un túnel IPsec con claves previamente compartidas para comunicarse entre dos redes privadas. En este ejemplo, las redes comunicantes son la red privada 192.168.10.x dentro del Cisco VPN 3000 Concentrator y la red privada 10.32.x.x dentro del firewall Checkpoint Next Generation (NG).

Prerequisites

Requirements

- El tráfico desde el interior del concentrador VPN y dentro del punto de control NG a Internet —representado aquí por las redes 172.18.124.x— debe fluir antes de comenzar esta configuración.
- Los usuarios deben estar familiarizados con la negociación IPSec. Este proceso se puede

dividir en cinco pasos, incluidas dos fases de intercambio de claves de Internet (IKE).Un túnel IPSec es iniciado por un tráfico interesado. Se considera que el tráfico es interesante cuando se transmite entre los pares IPSec.En la Fase 1 IKE, las entidades pares IPSec negocian la política establecida de la Asociación de seguridad (SA) IKE. Una vez que se autentican los pares, se crea un túnel seguro con la Asociación de seguridad de Internet y el protocolo de administración de claves (ISAKMP).En la Fase 2 de IKE, los peers IPSec utilizan el túnel autenticado y seguro para negociar las transformaciones de SA IPSec. La negociación de la política compartida determina el modo en que se establece el túnel IPSec.Se crea el túnel IPSec y los datos se transfieren entre los pares IPSec según los parámetros IPSec configurados en los conjuntos de transformación IPSec.El túnel IPSec termina cuando los IPSec SAs son borrados o cuando caduca su vigencia.

Componentes Utilizados

Esta configuración se desarrolló y aprobó con las siguientes versiones de software y hardware:

- Concentrador de la serie VPN 3000 3.5.2
- Firewall NG de punto de control

Convenciones

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

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: El esquema de direccionamiento IP utilizado en esta configuración no es legalmente enrutable en Internet. Son direcciones RFC 1918, que se han utilizado en un entorno de laboratorio.

Configuraciones

Configurar el concentrador VPN 3000

Complete estos pasos para configurar el VPN 3000 Concentrator:

1. Vaya a **Configuration > System > Tunneling Protocols > IPSec LAN a LAN** para configurar la sesión LAN a LAN. Establezca las opciones para los algoritmos de autenticación e IKE,

clave previamente compartida, dirección IP de peer y parámetros de red local y remota. Haga clic en Apply (Aplicar).En esta configuración, la autenticación se configuró como ESP-MD5-HMAC y el cifrado se configuró como 3DES

Configuration System Tunneling Protocols IPSec LAN-to-LAN Modify		
Modify an IPSec LAN-to-LAN connection.		
Name Checkpoint	Enter the name for this LAN-to-LAN connection.	
Interface Ethernet 2 (Public) (172.18.124.131)	Select the interface to put this LAN-to-LAN connection on.	
Peer 172.18.124.157	Enter the IP address of the remote peer for this LAN-to-LAN connection.	
Digital None (Use Preshared Keys) *	Select the Digital Certificate to use.	
Certificate Entire certificate chain Transmission Identity certificate only	Choose how to send the digital certificate to the IKE peer.	
Preshared Key ciscontprules	Enter the preshared key for this LAN-to-LAN connection.	
Authentication ESP/MD5/HMAC-128 •	Specify the packet authentication mechanism to use.	
Encryption 3DES-168 -	Specify the encryption mechanism to use.	
IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.	
Routing None 💌	Choose the routing mechanism to use.Parameters below are ignored if Network Autodiscovery is chosen.	
Local Network		
Network List Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.	
IP Address 192.168.10.0	Note: Enter a wildcard mark, which is the reverse of a subnet mark. A	
Wildcard Mask 0.0.0.255	wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.	
Remote Network		
Network List Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.	
IP Address 10.32.0.0 Wildcard Mask 0.0.127.255	Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match.	
Apply Cancel	For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.	

2. Vaya a Configuration > System > Tunneling Protocols > IPSec > IKE Proposale y establezca los parámetros requeridos.Seleccione la propuesta IKE IKE-3DES-MD5 y verifique los parámetros seleccionados para la propuesta. Haga clic en Aplicar para configurar la sesión de LAN a LAN.Estos son los parámetros para esta configuración:

Configuration System Tunneling Protocols IPSec IKE Proposals Modify			
Modify a configured IKE Proposal.			
Proposal Name IKE-3DES-MD5	Specify the name of this IKE Proposal.		
Authentication Mode Preshared Keys	 Select the authentication mode to use. 		
Authentication Algorithm MD5/HMAC-128 -	Select the packet authentication algorithm to use.		
Encryption Algorithm 3DES-168 -	Select the encryption algorithm to use.		
Diffie-Hellman Group Group 2 (1024-bits) -	Select the Diffie Hellman Group to use.		
Lifetime Measurement Time	Select the lifetime measurement of the IKE keys.		
Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).		
Time Lifetime 86400	Specify the time lifetime in seconds.		
Apply Cancel			

3. Vaya a Configuration > Policy Management > Traffic Management > Security Associations,

seleccione la SA IPSec creada para la sesión y verifique los parámetros SA IPSec elegidos para la sesión LAN a LAN.En esta configuración, el nombre de la sesión LAN a LAN era "Checkpoint", por lo que la SA IPSec se creó automáticamente como "L2L: Punto de control".



Estos son los parámetros para esta

<u>SA:</u>	
Configuration Policy Management Traffic Management 5	Security Associations Modify
Modify a configured Security Association.	
SA Name L2L: Checkpoint	Specify the name of this Security Association (SA).
Inheritance From Rule 💌	Select the granularity of this SA.
IPSec Parameters	
Authentication Algorithm ESP/MD5/HMAC-128 -	Select the packet authentication algorithm to use.
Encryption Algorithm 3DES-168 -	Select the ESP encryption algorithm to use.
Encapsulation Mode Tunnel 💌	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy Disabled	Select the use of Perfect Forward Secrecy.
Lifetime Measurement Time 💌	Select the lifetime measurement of the IPSec keys.
Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime 86400	Specify the time lifetime in seconds.
IKE Parameters	
IKE Peer 172.18.124.157	Specify the IKE Peer for a LAN-to-LAN IPSec connection.
Negotiation Mode Main 💌	Select the IKE Negotiation mode to use.
Digital Certificate None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
Certificate Transmission [©] Entire certificate chain [®] Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use as IKE initiator.
Apply Cancel	

Configuración del punto de control NG

Los objetos de red y las reglas se definen en el NG del punto de control para formar la política que pertenece a la configuración de VPN que se va a configurar. A continuación, esta política se instala con el Editor de políticas de NG de punto de control para completar el lado NG de punto de control de la configuración.

 Cree los dos objetos de red para la red NG de punto de control y la red VPN Concentrator que cifrarán el tráfico interesante.para crear objetos, seleccione Administrar > Objetos de red y, a continuación, seleccione Nuevo > Red. Introduzca la información de red adecuada y, a continuación, haga clic en Aceptar.Estos ejemplos muestran la configuración de los objetos de red denominados CP_inside (la red interna del punto de control NG) y CONC_INSIDE (la red interna del concentrador

Network Prope	rties - CP_inside		×
General NAT]		
<u>N</u> ame:	CP_inside		
IP <u>A</u> ddress	10.32.0.0		
Net <u>M</u> ask:	255.255.128.0		
<u>C</u> omment:	CPINSIDE		
Co <u>l</u> or:			
Broadcas	t address: ed <u>O No</u> t included		
	OK Cancel	Help	

Network Proper	ties - CONC_INSIDE	×
General NAT	1	
<u>N</u> ame:	CONC_INSIDE	
IP <u>A</u> ddress:	192.168.10.0	
Net <u>M</u> ask:	255.255.255.0	
<u>C</u> omment:	Concentrator network	
Color:		
Broadcast <u>I</u> nclude	address: ed <u>O No</u> t included	
	OK Cancel H	elp

2. Vaya a Manage > Network Objects y seleccione New > Workstation para crear objetos de estación de trabajo para los dispositivos VPN, Checkpoint NG y VPN Concentrator.Nota: Puede utilizar el objeto de estación de trabajo NG de punto de control creado durante la configuración inicial de NG de punto de control. Seleccione las opciones para configurar la estación de trabajo como Gateway y dispositivo VPN interoperable y, a continuación, haga clic en Aceptar.Estos ejemplos muestran la configuración de objetos llamados ciscocp (Checkpoint NG) y CISCO_CONC (VPN 3000 Concentrator):

Workstation Properties - c	iscocp	×
Workstation Properties - c	iscocp General Name: Ciscocp IP Address: 172.18.124.157 Genment: Checkpoint External IP Color:	×
	Type: C Host C Gateway Check Point Products ✓ Check Epint products installed: Version NG ✓ Get Version ✓VPN-1 & FireWall-1 ✓FloodGate-1 Policy Server ✓ Primary Management Station	
	Object Management Image: Managed by this Management Server (Internal) Image: Managed by another Management Server (External) Secure Internal Communication Image: Description of the transformation Image: Description of the transformation <td< td=""><td></td></td<>	
	OK Cancel He	alp

Workstation Properties -	CISCO_CONC	×
General	General	
- NAT	Name: CISCO_CONC	
	IP Address: 172.18.124.131 Get address	
	Comment: VPN Concentrator	
	Cojor:	
	Type: C Host C Gateway	
	Check Point Products	
	Check Point products installed: Version NG Cet Version	
	□VPN-1 & FireWall-1 □FloodGate-1 □Policy Server □Management Station	
	Object Management	
	Managed by this Management Server (Internal)	
	Managed by another Management Server (External)	
	Interoperable ⊻PN Device	
	OK Cancel H	elp

3. Vaya a Administrar > Objetos de Red > Editar para abrir la ventana Propiedades de la Estación de Trabajo para la estación de trabajo NG de punto de control (ciscocp en este ejemplo). Seleccione Topology en las opciones del lado izquierdo de la ventana y luego seleccione la red que desea cifrar. Haga clic en Editar para establecer las propiedades de la interfaz.En este ejemplo, CP_inside es la red interna del punto de control NG.

kstation Properties -	ciscocp			
General	Topology			
- Topology NAT	<u>G</u> et Interface	\$		
- VPN	Name	IP Address	Network Mask	IP Addresses behind
- Authentication	E100B0	10.32.50.50	255.255.128.0	CP_inside
- Management	E100B1	172.18.124.157	255.255.255.0	External
- Advanced				
	•			
	Add	Edit	Remove	Show
				2,1011
	Show all IPs b	ehind Gateway		
	VPN Domain			
	 All IP Address information 	sses <u>b</u> ehind Gateway b	based on Topology	Show
	information.			
	C <u>M</u> anually De	fined	*	Sho <u>w</u>
		1		
	Exportable f	or SecuRemote		
			04	Causal Halp

4. En la ventana Propiedades de la interfaz, seleccione la opción para designar la estación de trabajo como interna y, a continuación, especifique la dirección IP adecuada. Click OK.Las selecciones de topología mostradas designan la estación de trabajo como interna y especifican las direcciones IP detrás de la interfaz

Interface Properties
General Topology QoS
Topology
External (leads out to the internet)
Internal (leads to the local network)
IP Addresses behind this interface:
O <u>N</u> ot Defined
O Network defined by the interface IP and Net Mask
Anti-Spoofing
Perform Anti-Spoofing based on interface topology
Spoof Tracking: O None 💿 Log O Alert
OK Cancel Help

- CP_inside:
- 5. En la ventana Propiedades de la estación de trabajo, seleccione la interfaz exterior en el Checkpoint NG que lleva a Internet y luego haga clic en **Editar** para establecer las propiedades de la interfaz. Seleccione la opción para designar la topología como externa y luego haga clic en

Interface Properties X
General Topology QoS
Topology
• External (leads out to the internet)
Internal (leads to the local network)
IP Addresses behind this interface:
C Not Defined
C Network defined by the interface IP and Net Mask
O <u>S</u> pecific: ▼
Anti-Spoofing
Case (Tracking: C. N
OK Cancel Help

- Aceptar.
- 6. En la ventana Propiedades de la estación de trabajo en el Checkpoint NG, seleccione VPN de las opciones del lado izquierdo de la ventana y, a continuación, seleccione los parámetros IKE para los algoritmos de cifrado y autenticación. Haga clic en Edit para configurar las propiedades IKE.

Workstation Properties - o	iscocp	×
General Topology NAT VEN Authentication Management • Advanced	VPN Encryption schemes Image: Imag	
	Nickname DN Certificate Authority Add Edit PK	

7. Establezca las propiedades IKE para que coincidan con las propiedades del concentrador VPN.En este ejemplo, seleccione la opción de cifrado para **3DES** y la opción de hash para

IKE Properties	2
General	
Support key exchange encryption	with: T Support data integrity with:
DES	MD <u>5</u>
Support authentication methods: -	
I Pre-Shared Secret	Edit <u>S</u> ecrets
Public Key Signatures	Specify
VPN-1 & FireWall-1 authentio	cation for SecuRemote (Hybrid Mode)
	<u>A</u> dvanced
	Lancei Heip

8. Seleccione la opción de autenticación para **Secretos Previamente Compartidos** y luego haga clic en **Editar Secretos** para establecer la clave previamente compartida para que sea compatible con la clave previamente compartida en el concentrador VPN. Haga clic en **Editar** para ingresar la clave como se muestra, luego haga clic en **Establecer**,

-	Shared Secret				×
	Shared Secrets List:				1
	Peer Name	Shared Se	cret		
	LISCO_CONC	~~~~		<u>E</u> dit	
				Bemove	
	Enter secret: cisc	cortprules	Set		
ar.	ОК	Canc	el	<u>H</u> elp	

Aceptar.

 En la ventana de propiedades IKE, haga clic en Avanzadas... y cambie estos parámetros:Anule la selección de la opción Support agresive mode.Seleccione la opción para el intercambio de claves Support para subredes.Cuando haya terminado, haga clic en Aceptar,

Advanced IKE properties			×
Use <u>U</u> DP encapsulation	UDP VPN1_IPSI	EC_encapsi 🔻	
Support Diffie-Hellman groups	,		
	Group 1 (768	bit)	
	Group 2 (102	4 bit)	
	Group 5 (153	6 bit)	
Rekeying Parameters			
Renegotiate IKE security assoc	iations	1440 🕂	Minutes
Renegotiate IPSEC Security as	sociations every	3600 ÷	Seconds
Renegotiate IPSEC Security	associations ever	, 50000 🕀	KBytes
	-	,	-
Misc			
Support IP compression for	SecureUlient		
Support Aggresive mode	ubnete		
I ■ Support Key excitatinge for s	ubriets		
Οκ	Cancel	Help	
		Пеф	

10. Vaya a Administrar > Objetos de Red > Editar para abrir la ventana Propiedades de la Estación de Trabajo para el Concentrador VPN. Seleccione Topology en las opciones del lado izquierdo de la ventana para definir manualmente el dominio VPN.En este ejemplo, CONC_INSIDE (la red interna del concentrador VPN) se define como el dominio VPN.

w	orkstation Properties - C	ISCO_CONC			×
	General	Topology			
	- Topology - NAT	<u>G</u> et Interfaces			
		Name	IP Address	Network Mask	
			······	· · · · · · · · · · · · · · · · · · ·	
		Add	<u>E</u> dt	<u>B</u> emove <u>S</u> how	y
		S <u>h</u> ow all IPs behi	nd Gateway		
		VPN Domain			
		C All IP Addresses information.	s <u>b</u> ehind Gateway b	ased on Topology	Shgw
		Manually Define		SIDE 💌	Show
		Egoortable for S	ecuRemote		
				OK Cano	el Help

11. Seleccione **VPN** de las opciones del lado izquierdo de la ventana y luego seleccione **IKE** como esquema de encriptación. Haga clic en **Edit** para configurar las propiedades IKE.

Workstation Properties -	CISCO_CONC			×
General Topology NAT Advanced	VPN Encryption schemes Image: Image			
		UK	Cancel	Help

12. Establezca las propiedades IKE para reflejar la configuración actual en el concentrador VPN.En este ejemplo, establezca la opción de encripción para **3DES** y la opción de

IKE Properties	
General	
Support key exchange encryption	n with:Support data integrity with:
Support authentication methods:	Edit <u>S</u> ecrets
Public Key Signatures VEN-1 & EireWall-1 authenti	Matching Criteria
	A duran and
	<u>A</u> dvanced

hashing para MD5.

13. Seleccione la opción de autenticación para Secretos Previamente Compartidos y luego haga clic en Editar Secretos para establecer la clave previamente compartida. Haga clic en Editar para ingresar la clave como se muestra, luego haga clic en Establecer,

·	Sha	ared Secret			-	×
	[- Shared Secrets	List:			1
		Peer Name	Shared S	iecret		
		ciscocp			<u>E</u> dit	
					<u>R</u> emove	
					-	
		Enter secret:	ciscortprules	Set		
	L	ПК	L Car	ncel I	Help	1
Aceptar.						

14. En la ventana de propiedades IKE, haga clic en **Avanzadas...** y cambie estos parámetros:Seleccione el grupo Diffie-Hellman adecuado para las propiedades IKE.Anule la selección de la opción **Support agresive mode**.Seleccione la opción para el **intercambio de claves Support para subredes**.Cuando haya terminado, haga clic en **Aceptar**,

Advanced IKE properties			×
Use UDP encapsulation			
	UDP VPN1_IPS	EC_encapsi 💌	
Support Diffie-Hellman groups			
	Group 1 (768	3 bit) M Hay	
	Group 2 (102	24 Dit) 36 bit)	
		,	
Rekeying Parameters			
Renegotiate IKE security assoc	ations	1440 🛨	Minutes
Renegotiate IPSEC Security as:	sociations every	3600 🛨	Seconds
🔲 Renegotiate IPSEC Security	associations ever	y 50000 🚊	KBytes
Miss			
Support IP compression for	SecureClient		
Support aggresive mode			
Support key exchange for <u>s</u>	ubnets		
OK	Cancel	<u>H</u> elp	

15. Seleccione Reglas > Agregar reglas > Arriba para configurar las reglas de cifrado para la política. En la ventana Policy Editor, inserte una regla con el origen como CP_inside (red interna del punto de control NG) y el destino como CONC_INSIDE (red interna del concentrador VPN). Establecer valores para Servicio = Any, Action = Encrypt y Track = Log. Cuando haya agregado la sección Acción de cifrado de la regla, haga clic con el botón derecho en Acción y seleccione Editar propiedades.

CISCOCP - Check Point Policy Editor	- Standard				anarorora)a	
File Edit View Manage Rules Policy	Topology Search Window	Help				
■ ● 苯吗 晰	A] 🗉 🖳 🗗 🏜	■ 및 ↔ ♥	54 🛛 🖄 🚠			
1 °% 🛄 📰 🖓 🖓 84 🗛 🤇	1 Q Q 🖸 💊 🍈	6				
\$ € 4 @ 8 8 0 %	🗱 Security - Standard 🗮	Address Translation - St	andard 🙀 QoS - S	tandard 🛄 Desktop Se	scurity - Standard	
E-St Network Objects	NO SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL
Workstation	Ho. Sounce	DESTIMATION	SERVICE	PACTION	THEFT	INSTRUCT
- CISCO_CONC	1 부 CP_inside 부 CONC_INSIDE	부 CONC_NSIDE 부 CP_inside	* Any	Edit propert	ies	Gateway:
-+ CONC_INSIDE	2 44 CP_inside	* Any	* Any	Add Encryp	.on	Gateway
Orgendae Orgendae	Name CISCO_CONC ciscocp	IP 172.18. 172.18.	Comment 124.131 VPN Conc 124.157 Checkpoil	Auth Auth Client Auth Client Auth Client Auth Client Auth Client Auth Client Client Client Encrypt Client Encrypt Client Client Clien	ypt	1

16. Seleccione IKE y haga clic en

	Encryption Properties	×
	General Encryption schemes defined: Image: Region of the scheme	
Edit	OK Cancel Help	

17. En la ventana IKE Properties, cambie las propiedades para coincidir con la transformación del concentrador VPN.Establezca la opción Transformar en Cifrado + Integridad de datos (ESP).Establezca el algoritmo de cifrado en 3DES.Establezca la integridad de los datos en MD5.Establezca la puerta de enlace de par permitida para que coincida con el concentrador VPN (CISCO_CONC).Cuando haya finalizado, haga clic en OK

1	(KE Properties	
	General	
	Transform	_
	Encryption + Data Integrity (ESP)	
	🔘 Data Integrity Only (AH)	
	Encryption Algorithm: 3DES	
	Data Integrity MD5	
	Compression method: None	
	Allowed Peer Gateway:	
	Use Perfect Forward Secrecy	
	Use DH <u>G</u> roup: Group 1 (768 bit)	
	Perform IP <u>P</u> ool NAT	
	OK Cancel Help	
		l

18. Después de configurar el punto de control NG, guarde la política y seleccione **Policy** > **Install** para

habilitarla.						
CISCOCP - Check Point Policy	Editor - Standard					
File Edit View Manage Rules	Policy Topology Search Window	Help				
🖬 🕘 🐰 🔁 🛍 💑	Verify Instal	°e ≞ ≪ ∣ ¶	V 🛔 🐉 🛛 😡			
) 🎦 🔲 😂 🌮 🕹 💱	Uninstall					
<u>କ୍ରାର୍ଦ୍ଧାତା ଅନାତା</u>	Access Lists	ddress Translation - St	andard 🔛 QoS - S	Standard 🛅 Desktop	Security - Standard	
E-X+ Network Objects	Install Users Database	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON
B-B Workstation	Management High Availability					
ciscocp	Global Properties	+ CONC_NSDE + CP_inside	🗙 Any	Encrypt	🔳 Log	Gateways
Network			The second second		B	In other
	- CP_mase	A werk	A ACTY	C accept	Log	Conterwarys
CP_Inside						
OSE Device						
Embedded Device						
-III Group						
Ungical Server						
- R Address Range						
- E Gateway Cluster						<u> </u>
Dynamic Object	Name	IP	Comment			
	CISCO_CONC	172.18.1	124.131 VPN Conc	centrator		
	discocp	172.18.1	124.157 Checkpoi	nt External IP		
	11					

La ventana de instalación muestra las notas de progreso a medida que se compila la política.



o la ventana de instalación indique que la instalación de la política ha finalizado, haga clic en **Cerrar** para finalizar el

procedimiento.	
Install Policy	×
Standard.W: Security Policy Script generated into Standard.pf Standard: Compiled OK.	4
Installing VPN-1/FireWall-1 policy On: ciscocp	
VPN-1/FireWall-1 policy installed successfully on ciscocp	
VPN-1/FireWall-1 policy Installation for all modules was successful	
	T
<u>Close</u>	

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Verificar la comunicación de red

Para probar la comunicación entre las dos redes privadas, puede iniciar un ping desde una de las redes privadas a la otra red privada. En esta configuración, se envió un ping desde el lado NG del punto de control (10.32.50.51) a la red del concentrador VPN (192.168.10.2).

```
C:\WINNT\System32\cmd.exe
```

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=10ms TTL=253
Reply from 192.168.10.2: bytes=32 time=10ms TTL=253
Reply from 192.168.10.2: bytes=32 time<10ms TTL=253
Reply from 192.168.10.2: bytes=32 time<10ms TTL=253
Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = Oms, Maximum = 10ms, Average =
                                                5ms
C:\>
C:\>
C:\>
C:\>
```

Ver el estado del túnel en el punto de control NG

Para ver el estado del túnel, vaya al Editor de directivas y seleccione **Ventana > Estado del sistema**.

CISCOCP - Check Point System Status								
Ele View Modules Products Tools Window Help								
🗩 🔍 🖻 🗛 🛄 🔦 🎫 🇞 💷 🗳 🛠	54							
Modules IP Address	VPN-1 Details							
	Status:	ок						
E-Ciscocp 172.18.124.157	Packets							
FireWal-1	Encrypted:	19						
FloodGate-1	Decrypted:	18						
Management	Errors							
SVN Foundation	Encryption errors:	0						
	Decryption errors:	0						
	IKE events errors:	3						
	Hardware							
	HW Vendor Name:	none						
	HW Status:	none						
For Help, press F1			Last updated:09:34:14 PM					

Ver el estado del túnel en el concentrador VPN

Para verificar el estado del túnel en el VPN Concentrator, vaya a Administración > Administrar sesiones.

his screen shows st aformation on a sess onnection to a sessi	atistics for sessions.' ion, click on that sess on, click Ping .	To refresh the statis sion's name. To log	tics, click Refre out a session, cl	sh. Sel ick Log	ect a Group gout in the tal	to filter ble belo	the sessions w. To test th	s. For more he network
roupAll ogout All: <u>PPTP U</u>	ser L2TP User IPS	ec User L2TP/IPSe	ec User IPSec/U	JDP Us	er IPSec/TC	<u>P User</u>	PSec LAN	I-to-LAN
Session Summa	ry							
Session Summa Active LAN-to- LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak S	Concurrent essions	Con Sessio	current ons Limit	Total Cumulative Sessions
Session Summa Active LAN-to- LAN Sessions 1	Active Remote Access Sessions	Active Management Sessions 3	Total Active Sessions	Peak S	Concurrent essions 4	Con Sessio	current ons Limit	Total Cumulative Sessions 17
Session Summa Active LAN-to- LAN Sessions 1 LAN-to-LAN S	Active Remote Access Sessions 0 essions	Active Management Sessions 3	Total Active Sessions 4	Peak S	Concurrent essions 4 [Remote Acc	Con Sessio 1	current ons Limit 1500 ssions Man	Total Cumulative Sessions 17 agement Sessions
Session Summa Active LAN-to- LAN Sessions 1 LAN-to-LAN S Connection Nam	Active Remote Access Sessions 0 essions 1P Address	Active Management Sessions 3 Protoco	Total Active Sessions 4	Peak S	Concurrent essions 4 [<u>Remote Acc</u> Login T	Con Sessio 1 cess Ses Time	current ons Limit 1500 ssions Man Duration	Total Cumulative Sessions 17 agement Sessions

En Sesiones de LAN a LAN, seleccione el nombre de conexión para el punto de control para ver los detalles de las SA creadas y el número de paquetes transmitidos/recibidos.

Connection Name	IP Add	tress	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	
Checkpoint	172.18.12	4.157 IF	Sec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	25	
a ore oreanoner i			IK	E Session		(an mar)			
1	Session ID	1			Encryption Algorith	m 3DES-1	68		
Hashing	Algorithm	MD5		1	Diffie-Hellman Gro	up Group 2	Group 2 (1024-bit)		
Authentica	tion Mode	Pre-Share	d Keys	I	KE Negotiation Mo	de Main			
Rekey Tin	e Interval	86400 sec	onds						
			IPS	ec Session					
:	2			ss 10.32.0.	10.32.0.0/0.0.127.255				
Loc	al Address	192.168.1	0.0/0.0.0.255		Encryption Algorith	m 3DES-1	3DES-168		
Hashing	Algorithm	MD5			SI	2P 1	1		
Encapsula	tion Mode	Tunnel			Rekey Time Interv	al 28800 s	28800 seconds		
		386			Desta Translati	1 286			

Troubleshoot

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

Nota: El tráfico no debe ser PATed a través del túnel IPSec usando la dirección IP pública del concentrador VPN (interfaz externa). De lo contrario, el túnel falla. Por lo tanto, la dirección IP utilizada para PATing debe ser una dirección distinta a la configurada en la interfaz externa.

Resumen de la red

Cuando se configuran varias redes adyacentes dentro del dominio de cifrado en el punto de control, el dispositivo puede resumir automáticamente las redes con respecto al tráfico interesante. Si el concentrador VPN no está configurado para coincidir, es probable que el túnel falle. Por ejemplo, si las redes internas de 10.0.0.0 /24 y 10.0.1.0 /24 están configuradas para ser incluidas en el túnel, estas redes se pueden resumir en 10.0.0.0 /23.

Depuración del punto de control NG

Para ver los registros, seleccione Window > Log Viewer.

-	CISCOCP - C	heck Poi	nt Log Vie	wer - [fv	log]			1 100000								×
Ek	e Mode Edi	Selecti	on yew	Iools ¥	(indow H	elp	1.11	a financia a se	2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		1 12					1 - 1 ¹
6	9 🍊 🖷	Log	-	= 0	1 ±	6 1	B B	r 🔲 🎫 🖫	8 🖽 "	880		1.1.1.1.1	1000			11
	Date	Time	Product	1999) 1997 - J.	Inter.	Orig	Туре	Action	Source	Destinati	Pr.,	Rule	S_Port	SrcKeyID	DstKeyID	×
1	13Aug2002	21:32:	VPN-1	& FireN.	💽 dae	ciscoop	log	0- key install	ciscoop	CISCO_CONC						
2	13Aug2002	21:32:	VPN-1	& FirekV	. 🕒 dee	. ciscocp	log	Over key install	ciscocp	CISCO_CONC				0x5879f30d	0xt1351129	

Para habilitar los debugs en el VPN Concentrator, vaya a **Configuration > System > Events > Classes**. Habilite AUTH, AUTHDBG, IKE, IKEDBG, IPSEC e IPSECDBG para que la gravedad se registre como 1 - 13. Para ver las depuraciones, seleccione **Monitoring > Filterable Event Log**.

1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128 3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157 processing SA payload 4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class Auth Method: Rcv'd: Preshared Key Cfg'd: XAUTH with Preshared Key (Initiator authenticated) 10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157 Oakley proposal is acceptable 14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157 processing VID payload 15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157 processing IKE SA 16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class Auth Method: Rcv'd: Preshared Key Cfg'd: XAUTH with Preshared Key (Initiator authenticated) 22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157 IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 3 26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157 constructing ISA_SA for isakmp 27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total length : 84 29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157 RECEIVED Message (msgid=0) with payloads :

HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157 processing ke payload 34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157 processing ISA_KE 35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157 processing nonce payload 36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157 constructing ke payload 37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157 constructing nonce payload 38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157 constructing Cisco Unity VID payload 39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157 constructing xauth V6 VID payload 40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157 Send IOS VID 41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157 Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 2000001) 43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157 constructing VID payload 44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157 Send Altiga GW VID 45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157 Generating keys for Responder... 46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) ... total length : 256 48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60 50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157 Group [172.18.124.157] Processing ID 51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157 Group [172.18.124.157] processing hash 52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157 Group [172.18.124.157] computing hash 53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157 Group [172.18.124.157]

Starting group lookup for peer 172.18.124.157

54 09/11/2002 20:36:03.690 SEV=8 AUTHDEG/1 RPT=10 AUTH_Open() returns 9

55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10 Authentication session opened: handle = 9

56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10 AUTH_PutAttrTable(9, 748174)

57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10 AUTH_GroupAuthenticate(9, 2f1b19c, 49c648)

58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10 AUTH_BindServer(51a6b48, 0, 0)

59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10 Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1

60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10 AUTH_CreateTimer(51a6b48, 0, 0)

61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10 Reply timer created: handle = 4B0018

62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10 AUTH_BuildMsg(51a6b48, 0, 0)

63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10 AUTH_StartTimer(51a6b48, 0, 0)

64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10 Reply timer started: handle = 4B0018, timestamp = 1163319, timeout = 30000

65 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10 AUTH_SndRequest(51a6b48, 0, 0)

66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19 IntDB_Decode(3825300, 156)

67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19 IntDB_Xmt(51a6b48)

68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10 xmit_cnt = 1

69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20 IntDB_Xmt(51a6b48)

70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10 IntDB_Match(51a6b48, 3eb7ab0)

71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10 AUTH_RcvReply(51a6b48, 0, 0)

72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20 IntDB_Decode(3eb7ab0, 298)

73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10 IntDB_Rcv(51a6b48)

74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10

AUTH_DeleteTimer(51a6b48, 0, 0) 75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10 Reply timer stopped: handle = 4B0018, timestamp = 1163329 76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10 AUTH_Callback(51a6b48, 0, 0) 77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157 Authentication successful: handle = 9, server = Internal, group = 172.18.124.15778 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157 Group [172.18.124.157] Found Phase 1 Group (172.18.124.157) 79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10 AUTH_GetAttrTable(9, 748420) 80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157 Group [172.18.124.157] Authentication configured for Internal 81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: IP Compression = disabled 82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: Split Tunneling Policy = Disabled 83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10 AUTH_Close(9) 84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157 Group [172.18.124.157] constructing ID 85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527 Group [172.18.124.157] construct hash payload 86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157 Group [172.18.124.157] computing hash 87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157 Group [172.18.124.157] constructing dpd vid payload 88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) ... total length : 80 90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157 Group [172.18.124.157] PHASE 1 COMPLETED 91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157 Keep-alive type for this connection: None 92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157

Keep-alives configured on but peer does not

support keep-alives (type = None)

93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157 Group [172.18.124.157] Starting phase 1 rekey timer: 64800000 (ms) 94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16 User 172.18.124.157 connected 95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10 AUTH_UnbindServer(51a6b48, 0, 0) 96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10 Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0 97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10 AUTH_Int_FreeAuthCB(51a6b48) 98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10 Authentication session closed: handle = 9 99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 156 102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157 Group [172.18.124.157] processing hash 103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157 Group [172.18.124.157] processing SA payload 104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157 Group [172.18.124.157] processing nonce payload 105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157 Group [172.18.124.157] Processing ID 106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157 Group [172.18.124.157] Received remote IP Proxy Subnet data in ID Payload: Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0 109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157 Group [172.18.124.157] Processing ID 110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157 Group [172.18.124.157] Received local IP Proxy Subnet data in ID Payload: Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0 113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534 QM IsRekeyed old sa not found by addr 114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157 Group [172.18.124.157] IKE Remote Peer configured for SA: L2L: Checkpoint

115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157 Group [172.18.124.157]

116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157 Group [172.18.124.157] IPSec SA Proposal # 1, Transform # 1 acceptable 117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157 Group [172.18.124.157] IKE: requesting SPI! 118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39 IPSEC key message parse - msgtype 6, len 200, vers 1, pid 0000000, seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300 122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139 Processing KEY_GETSPI msg! 123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10 Reserved SPT 305440147 124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10 IKE got SPI from key engine: SPI = 0x1234a593 125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157 Group [172.18.124.157] oakley constucting quick mode 126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157 Group [172.18.124.157] constructing blank hash 127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157 Group [172.18.124.157] constructing ISA_SA for ipsec 128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157 Group [172.18.124.157] constructing ipsec nonce payload 129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157 Group [172.18.124.157] constructing proxy ID 130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157 Group [172.18.124.157] Transmitting Proxy Id: Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0 Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0 134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157 Group [172.18.124.157] constructing qm hash 135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157 SENDING Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) ... total length : 152 137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + NONE (0) ... total length : 48

processing IPSEC SA

139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157

Group [172.18.124.157] processing hash 140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157 Group [172.18.124.157] loading all IPSEC SAs 141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157 Group [172.18.124.157] Loading subnet: Dst: 192.168.10.0 mask: 255.255.255.0 Src: 10.32.0.0 mask: 255.255.128.0 146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157 Group [172.18.124.157] Security negotiation complete for LAN-to-LAN Group (172.18.124.157) Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959 149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40 IPSEC key message parse - msgtype 1, len 606, vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0, spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140 Processing KEY_ADD msg! 154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141 key_msqhdr2secassoc(): Enter 155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142 No USER filter configured 156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143 KeyProcessAdd: Enter 157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144 KeyProcessAdd: Adding outbound SA 158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145 KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255, dst 10.32.0.0 mask 0.0.127.255 159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146 KeyProcessAdd: FilterIpsecAddIkeSa success 160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41 IPSEC key message parse - msgtype 3, len 327, vers 1, pid 0000000, seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0, spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147

Processing KEY_UPDATE msg!

165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148

Update inbound SA addresses

166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149
key_msghdr2secassoc(): Enter

167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150 No USER filter configured

168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151 KeyProcessUpdate: Enter

169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152 KeyProcessUpdate: success

170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7 IKE got a KEY_ADD msg for SA: SPI = 0x0df37959

171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547 pitcher: rcv KEY_UPDATE, spi 0x1234a593

172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157 Group [172.18.124.157] PHASE 2 COMPLETED (msgid=54796f76)

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de soporte de IPSec
- Soporte Técnico Cisco Systems