Configuración de IPSec entre un servidor Microsoft Windows 2000 y un dispositivo Cisco

Contenido

Introducción Antes de comenzar Convenciones **Prerequisites Componentes Utilizados** Diagrama de la red Configuración de Microsoft Windows 2000 Server para que funcione con dispositivos Cisco Tareas realizadas **Step-by-Step Instructions** Configuración de los dispositivos de Cisco Configuración del router Cisco 3640 Configuración de PIX Configuración del concentrador VPN 3000 Configuración del concentrador VPN 5000 Verificación **Troubleshoot** Comandos para resolución de problemas Información Relacionada

Introducción

Este documento muestra cómo formar un túnel IPSec con claves previamente compartidas para incorporar dos redes privadas: una red privada (192.168.I.X) dentro de un dispositivo Cisco y una red privada (10.32.50.X) dentro de Microsoft 2000 Server. Suponemos que el tráfico desde dentro del dispositivo Cisco y dentro del servidor 2000 a Internet (representado aquí por las redes 172.18.124.X) se encuentra fluyendo desde antes de comenzar esta configuración.

Puede encontrar información detallada sobre la configuración del servidor de Microsoft Windows 2000 en el sitio Web de Microsoft: <u>http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP</u>

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte <u>Convenciones de</u> <u>Consejos Técnicos de Cisco</u>.

Prerequisites

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Estas configuraciones fueron desarrolladas y probadas mediante las versiones de software y hardware indicadas a continuación.

- Microsoft Windows 2000 Server 5.00.2195
- Router 3640 de Cisco con la versión c3640-ik2o3s-mz.121-5.T.bin de software del IOS de Cisco.
- Secure PIX Firewall de Cisco con software PIX versión 5.2.1
- Concentrador Cisco VPN 3000 con versión 2.5.2F del software del concentrador VPN 3000
- Concentrador VPN 5000 de Cisco con la Versión 5.2.19 del software del concentrador VPN 5000

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Diagrama de la red

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



Configuración de Microsoft Windows 2000 Server para que funcione con dispositivos Cisco

Tareas realizadas

Este diagrama muestra las tareas realizadas en la configuración de Microsoft Windows 2000 Server:



Step-by-Step Instructions

Una vez que haya seguido las <u>instrucciones</u> de configuración<u>en el sitio Web de Microsoft, siga</u> <u>estos pasos para verificar que su configuración pueda funcionar con los dispositivos de Cisco.</u> Los comentarios y cambios se anotan junto a las capturas de pantalla.

 Haga clic en Start (Inicio) > Run (Ejecutar) > secpol.msc en Microsoft Windows 2000 Server y verifique la información de las siguientes pantallas.Después de utilizar las instrucciones del sitio Web de Microsoft para configurar un servidor 2000, se mostró la siguiente información de túnel.Nota: La regla de ejemplo se denomina "to_cisco".

Local Security Settings				_ 🗆 ×
Action ⊻iew ← →	- 🗈 📧 🗙 🕾 🛛	🔮 🛯 🏦 📄 🖺 🗕		
Tree	Name 🔺	Description	Policy Assigned	
Tree Security Settings Account Policies Dublic Key Policies Dublic Key Policies IP Security Policies on	Name Client (Respond Only) Secure Server (Requir Server (Request Secu to_cisco	Description Communicate normally (uns For all IP traffic, always req For all IP traffic, always req	Policy Assigned No No Yes	
	,			

2. Esta regla de ejemplo contiene dos filtros: Microsoft-Cisco y Cisco-

Rules General Image: Security rules for communicating with other computers IP Security Rules: IP Filter List Filter Action Authentication T IM Microsoft-Cisco Permit IP Cisco-Microsoft Permit Image: Comparison of the second seco	Rules General Security rules for communicating with other computers IP Security Rules: IP Filter List Filter Action Authentication T Microsoft-Cisco Permit Preshared Key 1' Cisco-Microsoft Permit Preshared Key 1' Opnamic> Default Response Preshared Key N	to_cise	co Properties		
Security rules for communicating with other computers IP Security Rules: IP Filter List Filter Action Authentication T Microsoft-Cisco Permit Preshared Key 1 ^o Cisco-Microsoft Permit Cisco-Microsoft Default Response Opinamic> Default Response	Security rules for communicating with other computers IP Security Rules: IP Filter List Filter Action Microsoft-Cisco Permit Microsoft Permit Cisco-Microsoft Permit Cisco-Microsoft Default Response Volume Default Response	Rule	s General		
IP Security Rules: IP Filter List Filter Action Authentication T Image: Microsoft-Cisco Permit Preshared Key 1 Image: Cisco-Microsoft Permit Pershared Key 1 Image: Cisco-Microsoft Pershared Key 1 <td< th=""><th>IP Security Rules: IP Filter List Filter Action Authentication T ✓ Microsoft-Cisco Permit Preshared Key 1 ✓ Cisco-Microsoft Permit Preshared Key 1 ✓ Cynamic> Default Response Preshared Key N</th><th></th><th>Security rules f</th><th>or communicating with ot</th><th>her computers</th></td<>	IP Security Rules: IP Filter List Filter Action Authentication T ✓ Microsoft-Cisco Permit Preshared Key 1 ✓ Cisco-Microsoft Permit Preshared Key 1 ✓ Cynamic> Default Response Preshared Key N		Security rules f	or communicating with ot	her computers
IP Filter List Filter Action Authentication T ✓ Microsoft-Cisco Permit Preshared Key 1 ✓ Cisco-Microsoft Permit Preshared Key 1 ✓ Cynamic> Default Response Preshared Key N	IP Filter List Filter Action Authentication T ✓ Microsoft-Cisco Permit Preshared Key 1 ✓ Cisco-Microsoft Permit Preshared Key 1 ✓ Cisco-Microsoft Default Response Preshared Key N ✓ Opnamic> Default Response Preshared Key N	ĮP S	Security Rules:		
✓ Microsoft-Cisco Permit Preshared Key 1 ✓ Cisco-Microsoft Permit Preshared Key 1 ✓ Cisco-Microsoft Default Response Preshared Key N ✓ Oynamic> Default Response Preshared Key N	 ✓ Microsoft-Cisco ✓ Cisco-Microsoft ✓ Permit ✓ Preshared Key 1[°] ✓ Oynamic> ✓ Default Response ✓ Preshared Key N 	IF	P Filter List	Filter Action	Authentication
✓ Cisco-Microsoft Permit Preshared Key 1 ↓ Cisco-Microsoft Permit Preshared Key N Cisco-Microsoft Permit Preshared Key N Cisco-Microsoft Permit Permit Preshared Key N Cisco-Microsoft Permit Permit Preshared Key N	Cisco-Microsoft Permit Preshared Key 1 Cynamic> Default Response Preshared Key N		Microsoft-Cisco	Permit	Preshared Key
Compared Compare Compared Compared Comp Compared Compared Comp Compared	Comparison Comparison Preshared Key N		Cisco-Microsoft	Permit	Preshared Key
			(Dynamic)	Derault nesponse	riesnaleu Key
Add <u>E</u> dit <u>R</u> emove V se Add <u>W</u> izar				Class I G	Pausa di Anno

3. Seleccione la regla de seguridad IP de Cisco-Microsoft y, a continuación, haga clic en **Editar** para ver/agregar/editar las listas de filtros

Edit Rule Properties	? ×
Authentication Methods Tu IP Filter List	innel Setting Connection Type Filter Action
The selected IP filter lis secured with this rule.	st specifies which network traffic will be
IP Filter Lists:	
Name	Description
	Matches all ICMP packets betw
O Airie Hairic	Matches all IP packets from this
O Microsoft-Cisco	
Add Edit	Remove
0	K Cancel Apply

IP.
4. En la regla General > Advanced (Opciones avanzadas) se encuentra la vida útil de IKE (480 minutos = 28800

to_cisco Properties ?X
Rules General
Key Exchange Settings
Master key Perfect Forward Secrecy
Authenticate and generate a new key after every:
480 minutes
Authenticate and generate a new key after every:
0 session(s)
Protect identities with these security methods:
Methods
Internet Key Eyelennes (IKE) for 1) (indews 2000
Jointly developed by Microsoft and Cisco Systems, Inc.
OK Cancel
Advanced
OK Cancel Apply
segundos):

- 5. La ficha General > Advanced (Opciones avanzadas) > Method (Método) de la regla contiene el método de encripción IKE (DES), resumen IKE (SHA1) y el grupo Diffie-Helman



6. Cada filtro tiene 5 fichas: Métodos de autenticación (claves precompartidas para Internet Key Exchange

IF	PFilter List	1	Filter	Action
Authenticati	on Methods	Tunnel Se	tting	Connection Type
	The authentication between the com authentication me another computer	n method spe puters, Offer ethods when i t	cifies how tr and accept t negotiating s	ust is established hese ecurity with
Authentication	n Method preferer	nce order:		
Method	D	etails		Add
Preshared K	ey ci	sco123		
				E dit
				Remove
				Move up
				Move down
		OK	Cance	

IP	Filter List	1	Filter Actio	on
Authenticati	on Methods	Tunnel Set	ting Conn	ection Type
	This rule only app the selected type	olies to network	traffic over con	nections of
C All networ	k connections			
Cocal area	a network (LAN)			
O Remote a	ccess			

Katerroperces	ι τη
Authentication Methods Tu	nnel Setting Connection Type
The selected filter actio	n specifies whether this rule negotiates ic, and how it will secure the traffic.
Filter Actions:	
Name	Description
O Devel	Development and ID and take to
O Permit	Permit unsecured IP packets to
O Require Security	Accepts unsecured communicat
Add Edit	Remove 🛛 🗖 Use Add Wizard
0	K Cancel Apply

	Modify Security Method
	Security Method
	 High (ESP) Data will be encrypted, authentic and unmodified
	Medium (AH) Data will be authentic and unmodified, but will not be encrypted
	Custom (for expert users) Settings
onalizar:	OK Cancel Apply Ha

ga clic en Settings (Configuración) - IPSec transforms (Transformaciones IPSec) e IPSec lifetime (Duración

Custom Security Method Settings	? ×
Specify the settings for this custom secu	urity method.
Data and address integrity without e Integrity algorithm:	ncryption (AH) :
MD5 💌	
 Data integrity and encryption (ESP): Integrity algorithm: MD5 	
Encryption algorithm:	
Session Key Settings:	
🗖 Generate a new key every:	🔽 Generate a new key every
100000 Kbytes	3600 seconds
	OK Cancel

filtros IP: redes de origen y destino que se cifrarán:Para Cisco-Microsoft:

🖥 IP Filter I	list						?
	An IP filter list is compo addresses and protoco	osed of multiple filte ols can be combine	rs. In this way multiple sub d into one IP filter.	inets, IP			
Name:							
Cisco-Micr	rosoft						
Description	κ						Add
			A				Edit
			V				Remove
Filters:						$\overline{\mathbf{v}}$	Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address	Source Ma
Yes		ANY	ANY	ANY	<a ip="" specific="" sub<="" td=""><td>192.168.1.0</td><td>255.255.25</td>	192.168.1.0	255.255.25
•							Þ
						OK	Cancel



Cisco:

IP Filter l	ist					? ×
	An IP filter list is comp addresses and protoc	osed of multiple filters. I ols can be combined in	in this way multiple subn to one IP filter.	ets, IP		
Name:						
Microsoft-0	Cisco					
Description	r.					Add
			*			Edit
			v			Remove
Filters:					T	Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address
Yes		ANY	ANY	ANY	<a ip="" specific="" sub<="" td=""><td>10.32.50.0</td>	10.32.50.0
•						Þ
					OK	Cancel

Configuración del túnel - pares de encripción: Para Cisco-

 IP Filter List Authentication Methods Tunnel Setting Connection Type The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel. This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP Address: 172.18.124.157 	 IP Filter List Filter Action Authentication Methods Tunnel Setting Connection Type The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel. This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP Address: 172.18.124.157 	Edi	it Rule Pro	operties		?				
 The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel. This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP Address: 172.18.124.157 	 The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel. This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP Address: 172.18.124.157 	6	Authenti	IP Filter List cation Methods	Tunnel Setting	Filter Action Connection Type				
 This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP Address: 172.18.124.157 	 This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP Address: 172.18.124.157 			The tunnel endp IP traffic destina List. It takes two	point is the tunneling tion, as specified by prules to describe an	computer closest to the the associated IP Filter IPSec Tunnel.				
 The tunnel endpoint is specified by this IP Address: 172.18.124.157 	Image: The tunnel endpoint is specified by this IP Address: I72.18.124.157 OK Cancel		C This ru	ule does not specify	an IPSec tunnel.					
	OK Cancel Apply		The tunnel endpoint is specified by this IP Address: 172.18.124.157							
	OK Cancel Apply									
	OK Cancel Apply									
	OK Cancel Apply									
					ок	Cancel Apply				

	Edit Rule Pro	perties			? ×
	Authentic	IP Filter List ation Methods	Í Tunnel Settir	Filter Act	ion nection Type
		The tunnel endp IP traffic destina List. It takes two	point is the tunne ation, as specified a rules to describe	ling computer o I by the associa e an IPSec Tur	closest to the ated IP Filter nnel.
	C This rul C The tur	e does not specify nnel endpoint is sp	an IPSec tunnel ecified by this IP /	Address:	
	173	2.18.124.	35		
Microsoft-Cisco:			ОК	Cancel	Apply

Configuración de los dispositivos de Cisco

Configure el router de Cisco, PIX y los concentradores VPN como se muestra en los siguientes

Configure el router de Cisco, PIX y los concentradores VPN como se muestra en los siguiente ejemplos.

- <u>Cisco 3640 Router</u>
- <u>PIX</u>
- <u>VPN 3000 Concentrator</u>
- <u>Concentrador VPN 5000</u>

Configuración del router Cisco 3640

Cisco 3640 Router

```
Current configuration : 1840 bytes
```

```
!
version 12.1
no service single-slot-reload-enable
```

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname moss
!
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
ip audit notify log
ip audit po max-events 100
crypto isakmp policy 1
!--- The following are IOS defaults so they do not
appear: !--- IKE encryption method encryption des !---
IKE hashing hash sha !--- Diffie-Hellman group group 1
!--- Authentication method authentication pre-share
!--- IKE lifetime lifetime 28800
!--- encryption peer crypto isakmp key cisco123 address
172.18.124.157
!--- The following is the IOS default so it does not
appear: !--- IPSec lifetime crypto ipsec security-
association lifetime seconds 3600 ! !--- IPSec
transforms crypto ipsec transform-set rtpset esp-des
esp-md5-hmac
crypto map rtp 1 ipsec-isakmp
!--- Encryption peer set peer 172.18.124.157
set transform-set rtpset
!--- Source/Destination networks defined match address
115
!
call rsvp-sync
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
interface Ethernet0/1
ip address 172.18.124.35 255.255.255.240
ip nat outside
half-duplex
crypto map rtp
1
ip nat pool INTERNET 172.18.124.35 172.18.124.35 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.36
no ip http server
1
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
!--- Source/Destination networks defined access-list 115
permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
```

```
!
line con 0
transport input none
line 65 94
line aux 0
line vty 0 4
!
end
```

Configuración de PIX

PIX					
PIX Version 5.2(1)					
nameif ethernet0 outside security0					
nameif ethernet1 inside security100					
enable password 8Ry2YjIyt7RRXU24 encrypted					
passwd 2KFOnbNIdI.2KYOU encrypted					
hostname pixfirewall					
fixup protocol ftp 21					
fixup protocol http 80					
fixup protocol h323 1720					
fixup protocol rsh 514					
fixup protocol smtp 25					
fixup protocol sqlnet 1521					
fixup protocol sip 5060					
names					
<pre>! Source/Destination networks defined access-list 115</pre>					
permit ip 192.168.1.0 255.255.255.0 10.32.50.0					
255.255.255.0					
access-list 115 deny ip 192.168.1.0 255.255.255.0 any					
pager lines 24					
logging on					
no logging timestamp					
no logging standby					
no logging console					
no logging monitor					
no logging buffered					
no logging trap					
no logging history					
logging facility 20					
logging queue 512					
interface ethernet0 auto					
interface ethernet1 10baset					
mtu outside 1500					
mtu inside 1500					
ip address outside 172.18.124.35 255.255.255.240					
ip address inside 192.168.1.1 255.255.255.0					
ip audit info action alarm					
ip audit attack action alarm					
no failover					
Tallover timeout 0:00:00					
Tallover poll 15					
Tallover ip address outside 0.0.0.0					
Tallover 1p address inside U.U.U.U					
arp timeout 14400					
! Except Source/Destination from Network Address					
Translation (NAT): nat (inside) 0 access-list 115					
$\begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 $					
timeout conn 1:00:00 half-closed 0:10:00 udn 0:02:00 rng					
cimeout comi 1.00.00 maii-ciosed 0.10.00 uap 0.02.00 rpc					

0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable sysopt connection permit-ipsec no sysopt route dnat !--- IPSec transforms crypto ipsec transform-set myset esp-des esp-md5-hmac !--- IPSec lifetime crypto ipsec security-association lifetime seconds 3600 crypto map rtpmap 10 ipsec-isakmp !--- Source/Destination networks crypto map rtpmap 10 match address 115 !--- Encryption peer crypto map rtpmap 10 set peer 172.18.124.157 crypto map rtpmap 10 set transform-set myset crypto map rtpmap interface outside isakmp enable outside !--- Encryption peer isakmp key ******* address 172.18.124.157 netmask 255.255.255.240 isakmp identity address !--- Authentication method isakmp policy 10 authentication pre-share !--- IKE encryption method isakmp policy 10 encryption des !--- IKE hashing isakmp policy 10 hash sha !--- Diffie-Hellman group isakmp policy 10 group 1 !--- IKE lifetime isakmp policy 10 lifetime 28800 telnet timeout 5 ssh timeout 5 terminal width 80 Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08 : end

Configuración del concentrador VPN 3000

Utilice las opciones de menú y los parámetros que se muestran a continuación para configurar el concentrador VPN según sea necesario.

 Para agregar una propuesta IKE, seleccione Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec > IKE Proposals (Propuestas IKE) > Add a proposal (Agregar una propuesta).

```
Proposal Name = DES-SHA

!--- Authentication method Authentication Mode = Preshared Keys !--- IKE hashing

Authentication Algorithm = SHA/HMAC-160 !--- IKE encryption method Encryption Algorithm =

DES-56 !--- Diffie-Hellman group Diffie Hellman Group = Group 1 (768-bits) Lifetime

Measurement = Time Date Lifetime = 10000 !--- IKE lifetime Time Lifetime = 28800
```

 Para definir el túnel de LAN a LAN, seleccione Configuration > System > Tunneling Protocols > IPSec LAN a LAN.

```
Name = to_2000
Interface = Ethernet 2 (Public) 172.18.124.35/28
!--- Encryption peer Peer = 172.18.124.157 !--- Authentication method Digital Certs = none
(Use Pre-shared Keys) Pre-shared key = ciscol23 !--- IPSec transforms Authentication =
ESP/MD5/HMAC-128 Encryption = DES-56 !--- Use the IKE proposal IKE Proposal = DES-SHA
```

Autodiscovery = off !--- Source network defined Local Network Network List = Use IP Address/Wildcard-mask below IP Address 192.168.1.0 Wildcard Mask = 0.0.0.255 !---Destination network defined Remote Network Network List = Use IP Address/Wildcard-mask below IP Address 10.32.50.0 Wildcard Mask 0.0.0.255

 Para modificar la asociación de seguridad, seleccione Configuration > Policy Management > Traffic Management > Security Associations > Modify.

SA Name = L2L-to_2000 Inheritance = From Rule IPSec Parameters /--- IPSec transforms Authentication Algorithm = ESP/MD5/HMAC-128 Encryption Algorithm = DES-56 Encapsulation Mode = Tunnel PFS = Disabled Lifetime Measurement = Time Data Lifetime = 10000 /--- IPSec lifetime Time Lifetime = 3600 Ike Parameters /--- Encryption peer IKE Peer = 172.18.124.157 Negotiation Mode = Main /--- Authentication method Digital Certificate = None (Use Preshared Keys) /--- Use the IKE proposal IKE Proposal DES-SHA

Configuración del concentrador VPN 5000

Concentrador VPN 5000 [IP Ethernet 1:0] Mode = RoutedSubnetMask = 255.255.255.240IPAddress = 172.18.124.35[General] IPSecGateway = 172.18.124.36DeviceName = "cisco" EthernetAddress = 00:00:a5:f0:c8:00DeviceType = VPN 5002/8 Concentrator ConfiguredOn = Timeserver not configured ConfiguredFrom = Command Line, from Console [IP Ethernet 0:0] Mode = RoutedSubnetMask = 255.255.255.0 IPAddress = 192.168.1.1 [Tunnel Partner VPN 1] *!--- Encryption peer* Partner = 172.18.124.157 *!---*IPSec lifetime KeyLifeSecs = 3600 BindTo = "ethernet 1:0" !--- Authentication method SharedKey = "ciscol23" KeyManage = Auto !--- IPSec transforms Transform = esp(md5,des) Mode = Main !--- Destination network defined Peer = "10.32.50.0/24" !--- Source network defined LocalAccess = "192.168.1.0/24" [IP Static] 10.32.50.0 255.255.255.0 VPN 1 1 [IP VPN 1] Mode = Routed Numbered = Off [IKE Policy] !--- IKE hashing, encryption, Diffie-Hellman group Protection = SHA_DES_G1 Configuration size is 1088 out of 65500 bytes.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Esta sección proporciona información que puede utilizar para resolver problemas de sus

configuraciones.

Comandos para resolución de problemas

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

Nota: Antes de ejecutar comandos debug, consulte <u>Información Importante sobre Comandos</u> <u>Debug</u>.

Cisco 3640 Router

- **debug crypto engine** Muestra mensajes de depuración sobre los motores criptográficos, que realizan el cifrado y el descifrado.
- debug crypto isakmp Muestra mensajes sobre eventos IKE.
- debug crypto ipsec: Muestra eventos de IPSec.
- show crypto isakmp sa: muestra todas las asociaciones actuales de seguridad IKE (SA) de un par.
- show crypto ipsec sa Muestra las configuraciones usadas por las asociaciones de seguridad actuales.
- clear crypto isakmp (del modo de configuración) Borra todas las conexiones IKE activas.
- clear crypto sa (en el modo de configuración) Borra todas las asociaciones de seguridad de IPSec.

<u>PIX</u>

- debug crypto ipsec Muestra los IPSec Negotiations de la fase 2.
- debug crypto isakmp: muestra las negociaciones de fase 1 del protocolo Asociación de seguridad en Internet y administración de claves (ISAKMP).
- debug crypto engine Muestra el tráfico cifrado.
- show crypto ipsec sa Muestra las asociaciones de seguridad de la fase 2.
- show crypto isakmp sa Muestra las asociaciones de seguridad de la Fase 1.
- clear crypto isakmp (del modo configuración) Limpia las asociaciones de seguridad de Intercambio de clave de Internet (IKE).
- clear crypto ipsec sa (from configuration mode) Borra las asociaciones de seguridad IPSec.

VPN 3000 Concentrator

- Inicie la depuración del Concentrador VPN 3000 seleccionando Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases) > Modify (Modificar) (Gravedad en el registro=1-13, Gravedad en la consola=1-3): IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- El registro de eventos puede borrarse o recuperarse seleccionando Monitoring (Monitoreo) > Event Log (Registro de eventos).
- El tráfico de túnel de LAN a LAN puede supervisarse en Monitoring (Supervisión) > Sessions (Sesiones).
- - El túnel se puede borrar en Administración > Administración > Sesiones > Sesiones LAN a

LAN > Acciones - Cierre de sesión.

Concentrador VPN 5000

- vpn trace dump all Muestra información acerca de todas las conexiones de VPN concordantes, incluida la información acerca de la hora, el número VPN, la dirección IP real del par, las secuencias de comandos que se ejecutaron y, en caso de algún error, la rutina y el número de línea del código de software en el que se produjo el error.
- show vpn statistics: Muestra la siguiente información para usuarios, socios y el total para ambos. (En el caso de los modelos modulares, la pantalla incluye una sección para cada ranura del módulo.) Activas actualmente: Las conexiones que están activas actualmente. In Negot – Las conexiones que están siendo negociadas actualmente. Agua alta - Cantidad máxima de conexiones activas al mismo tiempo desde el último reinicio. Total en ejecución -Cantidad total de conexiones correctas desde el último reinicio. Comienzo del túnel - El número de túneles comienza. Túneles correctos – Cantidad de túneles que no presentan errores. Error de túnel – El número de túneles con errores.
- show vpn statistics verbose Muestra las estadísticas de negociación ISAKMP y muchas otras estadísticas de conexión activa.

Información Relacionada

- Anuncio de fin de venta de los concentradores Serie VPN 5000 de Cisco
- <u>Configuración de seguridad de red IPSec</u>
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- <u>Soporte Técnico Cisco Systems</u>