# Configurando um túnel IPSec - Cisco VPN 3000 Concentrator para Checkpoint 4.1 Firewall

## Contents

Introduction Prerequisites Requirements Componentes Utilizados Diagrama de Rede Conventions Configurar o VPN 3000 Concentrator Configurar o firewall do ponto de verificação 4.1 Verificar Troubleshoot Sumarização de rede Debug de VPN 3000 Concentrator Debug de VPN 3000 Concentrator Debug de Checkpoint 4.1 Firewall Exemplo de saída de depuração Informações Relacionadas

## **Introduction**

Esse documento demonstra como formar um túnel de IPsec com chaves pré-compartilhadas para unir duas redes privadas:

- Uma rede privada dentro do Cisco VPN 3000 Concentrator (192.168.1.x).
- Uma rede privada dentro do firewall do ponto de controle 4.1 (10.32.50.x).

Pressupõe-se que o tráfego de dentro do VPN Concentrator e de dentro do Checkpoint para a Internet (representado neste documento pelas redes 172.18.124.x) flua antes que essa configuração comece.

## **Prerequisites**

### **Requirements**

Não existem requisitos específicos para este documento.

### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- VPN 3000 Concentrator
- Software VPN 3000 Concentrator versão 2.5.2.F
- Checkpoint 4.1 Firewall

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.

### Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



### **Conventions**

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

## Configurar o VPN 3000 Concentrator

Conclua estes passos para configurar o VPN 3000 Concentrator.

 Selecione Configuration > System > Tunneling Protocols > IPSec > IKE Proposal > Modify para criar uma proposta de Internet Key Exchange (IKE) chamada "des-sha" com hashing Secure Hash Algorithm (SHA), Data Encryption Standard (DES) e Diffie-Hellman Group 1. Mantenha o Time Lifetime padrão em 86400 segundos.Observação: o intervalo válido para o tempo de vida do IKE do VPN Concentrator é de 60 a 2147483647 segundos.

X Cisco Systems, Inc. VPN 3000	Concentrator Series (192.168.1.	1] - Netscape	
Elle Edit View Go Communicator	Help		
Back For Reload	Home Search Netscape F	int Security	N
📲 😻 Bookmarks 🎄 Location	hittp://172.18.124.35/access.hitml		🚽 🎧 What's Related
🔒 Instant Message 🔲 WebMai	🗏 Contact 関 People 関 Yel	low Pages 🖳 Download 📹 Cha	wels
VPN	3000		Main   Help   Support   Logout
Conc	entrator Series Mana	loer	Logged in: admin
Cone	entrator series Man	iger	Configuration   Administration   Monitoring
-@ <u>Configuration</u>	Configuration   System   Tur	upeline Protocols ( IPSec ) IKI	Proposale   MacBly
Interfaces	configuration   System   Tur	ineting Protocols   in Sec   inc	r roposais   wrouny
	Modify a configured IKE Pro	posal	
Address Management			
Tunneling Protocols	Proposal Name	des-sha	Specify the name of this IKE Proposal
	rioposaritanie		opecity are name of any first rioposa.
- GIPSes	Authentication Mode	Preshared Keys 🔹	Select the authentication mode to use.
LAN-to-LAN			Select the packet authentication algorithm to
E Proposate	Authentication Algorithm	SHA/HMAC-160	use.
Management Protocols	Encremtion Algorithm	DES.66	Select the encruption algorithm to use
Eventr	Encryption Augorithm	00000	Select the encryption algorithm to use.
	Diffie-Hellman Group	Group 1 (768-bits) 💌	Select the Diffie Hellman Group to use.
Policy Management			Select the lifetime measurement of the IKE
Access Hours	Lifetime Measurement	Time 💌	keys.
Network Lists	Data Lifetima	10000	Consider the data Materia in Islahatas (VD)
Ruler	Data Lifetime	10000	Specify the data menne in knooytes (R.B).
SAF	Time Lifetime	86400	Specify the time lifetime in seconds.
E INAT	Apply Cascal		
-EI-Administration	- oppiny Concer		
- Monitoring			
Cisco Systems			
A 4			
and I I I to an a filling a			
Docume Docume	nt: Done		

 Selecione Configuration (Configuração) > System (Sistema) > Tunneling Protocols (Protocolos de Tunelamento) > IPSec > IKE Proposals (Propostas IKE). Selecione "des-sha" e clique em Activate para ativar a proposta IKE.



3. Selecione Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add (Configuração > Sistema > Protocolos de Canalização > IPSec LAN para LAN > Adicionar).Configure um túnel IPsec chamado "to\_checkpoint" com o endereço de Checkpoint como Peer. Para a chave pré-compartilhadas, insira a chave real. Em Authentication (Autenticação), selecione ESP/SHA/HMAC-160 e selecione DES-56 para Encryption (Criptografia). Insira a proposta IKE ("des-sha" neste exemplo) e as redes local e remota.

🔆 Cisco Systems, Inc. VPN 3000	Concentrator Series [192.1	68.1.1] - Netscape	_ C ×
Ele Edit View Go Communicator	r <u>H</u> elp		
Back Forward Reload	Home Search Netscape	Print Security Floor	N
Bookmarks 🥻 Location	http://172.18.124.35/access.htm	ni	💌 🌎 🧊 What's Related
🕺 🧏 Instant Message 🖳 WebMai	I 🖳 Contact 🛄 People 📱	🖞 Yellow Pages 🖳 Download 📑 Channels	
VPN	3000		Main Help Support Logout
Con	ontrator Social M		
Conc	entrator series M	anager	Logged in: admin
El Cardio antiso	-		Configuration   Administration   Monitoring
Interfaces	Configuration   System	Tunneling Protocols   IPSec LAN-to-L	AN   Modify
	Modify an IPSec LAN-	to-LAN connection.	
DIUNNEIIng Protocols PPTP L2TP	Name [	to_checkpoint	Enter the name for this LAN-to-LAN connection.
LAN-to-LAN EXE Proposals	Interface [	Ethemet 2 (Public) (172.18.124.35)	Select the interface to put this LAN-to-LAN connection on.
Hanagement Protocols	Peer [	172.18.124.157	Enter the IP address of the remote peer for this LAN-to-LAN connection.
E 2 sosral	Digital Certificate	None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
Police Management	Preshared Key	ciscorules	Enter the preshared key for this LAN-to-LAN connection.
Nation Lists	Authentication [	ESP/SHA/HMAC-160 -	Specify the packet authentication mechanism to use.
	Encryption [	DES-56 👱	Specify the encryption mechanism to use.
- CD- <u>Administration</u> - CD-Manitering	IKE Proposal [	des-sha 💌	Select the IKE Proposal to use for this LAN-to-LAN connection.
Cisco Systems	Network Autodiscovery		Check to automatically discover networks. Parameters below are ignored if checked.
ADCESS	TION F ORUNDS		

🔆 Cisco Systems, Inc. VPN 3000	Concentrator Series [192.168.1.1] - Netscape	_ O ×
Eile Edit View Go Communicator	Help	
Back Former Reload	Home Search Netscape Print Security Story	N
Bookmarks & Location	http://172.18.124.35/access.html	Gil <sup>®</sup> What's Related
🦂 Instant Message 🔲 WebMail	🖳 Contact 🖳 People 🖳 Yellow Pages 🖳 Download 📩 Channels	
VPN	3000	Main Help Support Logout
Conc	antentos Sarias Managar	Lowerd in a dain
Conc	entrator series Manager	Logged in: admin
	Local Network	Configuration   Administration   Monitoring
Interfaces		Contraction of the strength of the
- D System	No	Specify the local network address list or
Servets	Network List Use IP Address/Wildcard-mask below	the IP address and wildcard mask for
- (i) Address Management		this LAN-to-LAN connection.
Tunneling Protocols		
	IP Address 192.168.1.0	Note: Enter a wildcard mask, which
E31PSec		is the reverse of a subnet mask. A
LAN-to-LAN		wildcard mask has 1s in bit positions to
IKE Proposals		ignore, 0s in bit positions to match. For
- III IP Reating	Wildcard Mask 0.0.0.255	example, 10.10.1.0/0.0.0.255 = all
- Management Protocols		10.10.1.nnn addresses.
- (i) Evante		
Tulicar Management	Ramata Network	
DPolicy Management	Nemote Network	
Access Hours		Specify the remote network address list
Traffic Management	Network List Use IP Address/Wildcard-mask below 🔳	or the IP address and wildcard mask.
Network Lists		for this LAN-to-LAN connection.
<u>SA</u>	TP Address 10.32.50.0	Note: Enter a wildcard mask, which
		is the reverse of a subnet mask. A
		wildcard mask has 1s in bit positions to
- T-Monitoring		ignore, 0s in bit positions to match. For
	Wildcard Mask 0.0.255	example, 10.10.1.0/0.0.0.255 = all
Cisco Systems		10.10.1.nnn addresses.
dis dis	Aprily Cancel	
Manager and Annual States of States and Stat	rappy cancer	L.
Docume	nt. Uone	

4. Selecione Configuração > Gerenciamento de Política > Gerenciamento de Tráfego > Associações de Segurança > Modificar. Verifique se o segredo de encaminhamento perfeito está desativado e deixe o tempo de vida útil do IPsec no padrão 28800 segundos.Observação: o intervalo válido para o tempo de vida do VPN Concentrator IPsec é de 60 a 2147483647 segundos.

💥 Cisco Systems, Inc. VPN 3000	Concentrator Series (192.168.1.	1] - Netscape	_ O ×
Elle Edit View Go Communicator	Help		
Back Reload	Home Search Netscape F	int Security	N
📲 🖋 Bookmarks 🎄 Location:	http://172.18.124.35/access.html		💌 🌏 🖓 🖉 What's Related
📜 🚴 Instant Message 🔲 WebMai	🖲 Contact 関 People 関 Yel	low Pages 😕 Download 📺 Channe	<b>.</b>
VPN	3000		Main   Help   Support   Logout
Conc	entrator Series Man	loer	Logged in: admin
Conc	entrator series wian	igei	Configuration   Administration   Monitoring
- Configuration	Configuration   Policy Mana	anmont   Traffic Mananamont   1	Security Associations   Madifu
interfaces	configuration ( Policy Mana	gement i franc management i s	Security Associations   Mourry
- Giluser Management	Modify a configured Security	Association	
Policy Management	/		
Access Hours			Specify the name of this Security
Nation Lists	SA Name	L2L: to_checkpoint	Association (SA).
	Tubovitonos	From Dida	Colort the encodering of this CA
SAI	Interitance	Fram Rule	Select the granuarity of this S.A.
GAdministration	IPSec Parameters		
Administer Sessions	Authentication Algorithm	ESP/SHA/HMAC-160	Select the packet authentication algorithm
Sintern Reboat	Automation Augoritant		to use
-Ping	Encrention Algorithm	DES-68	Select the ESP encryption algorithm to
Monitoring Refresh	Encryption Augoritan	020-00	use.
	Enconsulation Made	Turnel	Select the Encapsulation Mode for this
D-Certificate Management	Encapsulation Mode	runner	SA.
- 13 Monitoring	Destant Francis Courses	Disabled	Select the use of Perfect Forward
	Perfect Forward Secrecy	Disabled	Secrecy.
			Select the lifetime measurement of the
	Lifetime Measurement	Time 💌	IPSec keys.
Cisco Systems	Data Lifetime	10000	Specify the data lifetime in kilobutes (KB)
	L'ata Lifetine	10000	opecay are data meanic in anotytes (FLD).
and the set of the set	Time Lifetime	28800	Specify the time lifetime in seconds.
2 - Docume	nt: Done		

💥 Cisco Systems, Inc. VPN 3000	Concentrator Series (192.168.1.	1] - Netscape	_ O ×
Elle Edit View Go Communicator	Help		
Back Former Reload	Anne Search Netscape P	int Security	N
Bookmarks 🎄 Location:	http://172.18.124.35/access.html		
🗧 🚴 Instant Message 🔲 WebMail	🔄 Contact 🔄 People 🖳 Yel	low Pages 😕 Download 📑 Channels	
VPN	3000	200 77.7	Main   Help   Support   Logout
Conc	entrator Series Mana	iger	Logged in: admin
		-9	Configuration   Administration   Monitoring
Configuration Interfaces	Encryption Algorithm	DES-56 💌	Select the ESP encryption algorithm to use.
Diser Management     Officer Management     Access Hours	Encapsulation Mode	Tunnel	Select the Encapsulation Mode for this SA.
Traffic Management	Perfect Forward Secrecy	Disabled	Select the use of Perfect Forward Secrecy.
SAr ————————————————————————————————————	Lifetime Measurement	Time 💌	Select the lifetime measurement of the IPSec keys.
	Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Administer Sessions Software Update System Rebost	Time Lifetime	28800	Specify the time lifetime in seconds.
Ping Menitaring Refresh	IKE Parameters		
Officers Rights     Officers Management     Officers Management	IKE Peer	172.18.124.157	Specify the IKE Peer for a LAN-to-LAN IPSec connection.
- Monitoring	Negotiation Mode	Main 💌	Select the IKE Negotiation mode to use.
	Digital Certificate	None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
	IKE Proposal	des-sha 💌	Select the IKE Proposal to use.
Casco Systems	Apply Cancel		
Docume	nt: Done		

5. Salve a configuração.

## Configurar o firewall do ponto de verificação 4.1

Conclua estes passos para configurar o Firewall do Ponto de Verificação 4.1.

 Como a duração padrão de IKE e IPsec difere entre os fornecedores, selecione Propriedades > Criptografia para definir a duração do ponto de verificação de acordo com os padrões do VPN Concentrator.O tempo de vida IKE padrão do VPN Concentrator é de 86400 segundos (=1440 minutos).O tempo de vida padrão do VPN Concentrator IPsec é de 28800 segundos.

Properties Setup	×
High Availability   IP Pool NAT   Access Security Policy   Traffic Control   Services   Lo Authentication   SYNDefender   LDAP	s Lists Desktop Security og and Alert Security Servers Encryption ConnectControl
SKIP Enable Exportable SKIP Change SKIP Session Key :	Manual IPSEC SPI allocation range (hex):
Every 120 Seconds (0 for infinity) or Every 10485760 Dates (0 for infinity)	Erom 100
IKE Renegotiate I <u>K</u> E Security Associations every	440 minutes
Renegotiate I <u>P</u> SEC Security Associations every 2	8800 seconds
OK Cancel	Help

2. Selecione Gerenciar > Objetos de rede > Novo (ou Editar) > Rede para configurar o objeto para a rede interna ("cpinside") por trás do ponto de controle. Isso deve concordar com a "rede remota" no VPN

	Network Properties
	General NAT
	<u>N</u> ame: cpinside
	IP Address: 10.32.50.0 Get address
	Net <u>M</u> ask: 255.255.255.0
	Color:
	Location:     Broadcast:       Internal     External         Allowed     Disallowed
	OK Cancel Help
Concentrator.	

3. Selecione Gerenciar > Objetos de rede > Editar para editar o objeto do ponto de extremidade do gateway ("RTPCPVPN" Checkpoint) que o VPN Concentrator tem em seu parâmetro Peer.Em Local, selecione Interno. Para Tipo, selecione Gateway. Em Módulos instalados, verifique VPN-1 e FireWall-1 e verifique a Estação de

Workstation Properties	×
General Interfaces SNMP N	AT Certificates VPN Authe
	· · · —
Name: RTPCPVPN	
IP Address: 172.18.124.157	<u>G</u> et address
Comment: Firewalled gatew	ay to internet
Location:	Type:
⊙ Internal O External	© <u>H</u> ost ● Gate <u>w</u> ay
- Modules Installed	
VPN-1 & <u>F</u> ireWall-1	Version: 4.1 💌 Ge <u>t</u>
FloodGate-1	Version: 4.1
Compression	Version: 4.1
Management Station	Cojor:
ОК	Cancel Help

- gerenciamento.
- 4. Selecione Gerenciar > Objetos de rede > Novo (ou Editar) > Rede para configurar o objeto para a rede externa ("inside\_cisco") atrás do VPN Concentrator. Isso deve concordar com a rede "local" no VPN

	Network Properties
	General NAT
	<u>Name:</u> inside_cisco
	IP Address: 192.168.1.0 Get address
	Net <u>M</u> ask: 255.255.255.0
	Color:
	Location: Broadcast:
	<u>○ Internal</u> <u>○ Allowed</u> <u>○</u> isallowed
	OK Cancel Help
Concentrator.	

- 5. Selecione Gerenciar > Objetos de rede > Novo > Estação de trabalho para adicionar um objeto ao gateway do VPN Concentrator externo ("cisco\_endpoint"). Esta é a interface "Pública" do VPN Concentrator.Em Local, selecione Externo. Para Tipo, selecione Gateway.Observação: não marque a caixa de seleção VPN-1/FireWall-1.
- 6. Selecionar Manage > Network objetct > Edit para editar o ponto final do gateway do ponto de controle (chamado "RTPCPVPN") na guia VPN. Em Domain, selecione Other e, em seguida, selecione o lado interno da rede de ponto de controle (chamado "cpinside") a partir da lista suspensa. Sob esquemas de criptografia definidos, selecione IKE e clique em

Workstation Properties	×
General Interfaces SNMP NAT	Certificates VPN Authe
Domain: Disabled Valid Addresses(of Interfaces) Dther: Exportable for SecuRemote	Encryption schemes defined:
Traffic Control Logging	
Image: March M	19
OK Car	icel Help

Editar.

- 7. Altere as propriedades IKE da criptografia DES para concordar com o **DES-56** e o **algoritmo de criptografia** no VPN Concentrator.
- 8. Altere as propriedades de IKE para hashing SHA1 para concordar com o algoritmo SHA/HMAC-160 no VPN Concentrator.Desative o Modo assertivo.Verifique Suporta Sub-Redes.Marque Pre-Shared Secret em Authentication Method (Método de autenticação). Isso concorda com o Modo de autenticação do VPN Concentrator, Chaves pré-

General Interfaces	SNMP NAT	Certificates	VPN Authe	•
KE Properties				×
General				
– Key <u>N</u> egoti	ation Encryption M	vlethod(s): -	– <u>H</u> ash Method: –	
	ES		□ MD <u>5</u>	
	AST		SHA1	
	,ES			
_ <u>_</u>	ion Method:			
Pre-Sh	ared Secreț	Edit <u>S</u>	ecrets	
🗖 Public	<u>K</u> ey Signatures	<u>C</u> oni	igure	
	Addresive Mode		s Subnets	
		, ouppor		
ОК	Can	cel I	Help	
				_
compartilhadas.				

9. Clique em **Editar segredos** para definir a chave pré-compartilhada para concordar com a **chave pré-compartilhada** real do VPN Concentrator.**isakmp key key address address** 

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties
General
Shared Secret
Shared Secrets List:
Peer Name Shared Secret
<u>Edit</u>
OK Cancel
OK Cancel Help
OK Cancel Help

#### netmask netmask

10. Selecione Gerenciar > Objetos de rede > Editar para editar a guia VPN "cisco\_endpoint". Em Domain, selecione Other e, em seguida, selecione o interior da rede Cisco (chamado "inside\_cisco"). Sob esquemas de criptografia definidos, selecione IKE e clique em

Workstation Properties	
General Interfaces SNMP NAT	VPN
Domain:	Encryption schemes defined:
C Disabled	Manual IPSEC
○ <u>V</u> alid Addresses(of Interfaces)	
• <u>O</u> ther:	D 🕅 SKIP
inside_cisco 💌	
Exportable for SecuRemote	<u>E</u> dit
□ Traffic Control Logging □ Ium on Traffic Control Loggin	9
OK Can	cel Help

- 11. Altere a criptografia DES das propriedades IKE para concordar com o **DES-56, Encryption Algorithm** no VPN Concentrator.
- 12. Altere as propriedades de IKE para hashing SHA1 para concordar com o algoritmo SHA/HMAC-160 no VPN Concentrator.Altere estas configurações:Modo DeselectAggressive.Verifique Suporta Sub-Redes.Marque Pre-Shared Secret em Authentication Method (Método de autenticação). Isso concorda com o modo de autenticação do VPN Concentrator de chaves pré-

	General Interfaces SNMP NAT Certificates VPN Authe
	KE Properties
	General
	Key <u>N</u> egotiation Encryption Method(s): <u>H</u> ash Method:
	CAST
	Authentication Method:
	✓ Pre-Shared Secret Edit Secrets
	Public Key Signatures     Configure
	Supports Aggresive Mode 🔽 Supports Subnets
	OK Cancel Help
compartilhadas.	

13. Clique em **Editar segredos** para definir a chave pré-compartilhada para concordar com a chave pré-compartilhada real do VPN

	IKE Properties	×
	General	
	Shared Secret	] ا
	Shared Secrets List:	
	Peer Name Shared Secret	
	RTPCPVPN **** <u>E</u> dit	
	OK Cancel	
	OK Cancel Help	
Concentrator.		

 Na janela Policy Editor, insira uma regra com Source e Destination como "inside\_cisco" e "cpinside" (bidirecional). Ajustar Serviço=Qualquer, Ação=Criptografar e Rastreio=Longo.

T	'RTP(	CPVPN - Check Po	oint Policy Editor				- 🗆 🗡
Ei	e <u>E</u> di	t <u>V</u> iew <u>M</u> anage	Policy Window <u>H</u>	elp			
6	] 🖨	🖪 🕹 🕻	E 💁 🕉 🕉	B.   🐬 🌆 🖆	🗏 🖀 🖷 🖷	T. 🔫 🖝 🛃	🐻 🎹 🚯
ž	Seci	urity Policy - Standard	🕂 🖶 Address Trans	slation - Standard 🛛 😿	Bandwidth Policy - S	tandard	
	No.	Source	Destination	Service	Action	Track	In
Ì	1	🚆 inside_cisco	👷 cpinside 👷 inside_cisco	Any	Encrypt	Long	
							•
Fo	r Help,	press F1		RTPC	PVPN Rea	d/Write	

15. No título Ação, clique no ícone **Criptografar** verde e selecione **Editar propriedades** para configurar políticas de criptografia

cripiografia.				
urity Policy - Standard	💼 Address Translation	- Standard 🛛 😿 Band	dwidth Policy - Standard	^
∼ FVV1 Host	∼ Ldap-Servers	😰 Idap	accept	
∼ FVV1 Host	∼ Logical-Servers	∼ load_agent	accept	
nside_cisco	cpinside	Any	dit properties	ng .
		dest-unreach	Edit Encryption	
		icmp echo-request	accept	am -
		icmp info-reply	drop	
Any	Any	icmp mask-reply	🚺 🦲 reject	
•				

16. Selecione IKE e, em seguida, clique em

	Encryption Properties	×
	General  Encryption schemes defined:  C Reference Manual IPSEC  R Reference SKIP  R Reference SKIP  Edit	
itar	OK Cancel Help	

17. Na janela Propriedades de IKE, altere essas propriedades para concordar com as transformações IPsec do VPN Concentrator.Em Transform, selecione Encryption + Data Integrity (ESP). O Encryption Algorithm deve ser DES, Data Integrity deve ser SHA1 e o Allowed Peer Gateway deve ser o gateway Cisco externo (denominado "cisco\_endpoint").

IKE Properties	>
General	
- Transform:	
Encryption + Data Integrity (ESP)	
C Data Integrity Only (AH)	
Encryption Algorithm: DES	
Data Integrity SHA1	
Allowed Peer Gateway:	
Use Perfect Forward Secrecy	
OK Cancel Help	

- Click OK
- Depois de configurar o ponto de verificação, selecione Política > Instalar no menu Ponto de verificação para que as alterações entrem em vigor.

## **Verificar**

No momento, não há procedimento de verificação disponível para esta configuração.

## **Troubleshoot**

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

### Sumarização de rede

Quando várias redes internas adjacentes são configuradas no domínio de criptografia no ponto de verificação, o dispositivo pode resumi-las automaticamente em relação ao tráfego interessante. Se o VPN Concentrator não estiver configurado para corresponder, o túnel provavelmente falhará. Por exemplo, se as redes internas de 10.0.0.0 /24 e 10.0.1.0 /24 estiverem configuradas para serem incluídas no túnel, elas podem ser resumidas em 10.0.0.0 /23.

### Debug de VPN 3000 Concentrator

As possíveis depurações do VPN Concentrator incluem IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE. É configurado em Configuration > System > Events > Classes.





Épossível exibir depurações em Monitoring > Event log > Get Log.



Selecione Monitoring > Sessions para monitorar o tráfego do túnel de LAN para LAN.

Cisco Systems, Inc.	VPN 3000 C	oncentrator Seri	es [192.168.1.1	1] - Micro	soft Interr	net Explo	rer				_ O ×
Ele Edit View Go	Fgvorites	Яер									<b>e</b>
Back Formati	- O Stop	Refresh Home	Search	Favorites	(3) History	Q Channels	Fulscree	n Mai	en e		
Address Address Address	8.124.35/acce	ss.html									👻 🗌 Links
	VPN 3	000							Main H	elp   Sup	port   Logout
N. 77	Concer	ntrator Ser	ies Mana	ger						Log	ged in: admir
								Configur	ation   Admir	nistration	h   Monitoring
	-	LAN Sessions	Access Sessions	Mana See	gement sions	Acti Sessi	Active Con Sessions Ses		ssions Limit		alative <u>*</u> sions
-OSessions		1	0		1	2		3	10000		17
SEPs 		LAN-to-L	AN Sessio	ns			Remote	Access Ses	sions   Manag	ement S	essions ]
EPTP L2TP	_	Connectio Name	Connection Name         IP Address         Protocol         Encryption         Login Time         Dur						Duration	Bytes Tx	Bytes Rx
HITP Events		to checkpoi	int 172.18.1	IPSec/L/ to-LAN	LAN- DES-56 Feb 13 14:21:3		Feb 13 14:21:31	0:44:25	1664	1664	
Isinet         Otsi         Authentication         Authentication         Authentication         Authentication         Image: Second price         Image: Second price         Image: Second price         Output         Authentication         Image: Second price         Image: Second print         Image: Second print									essions ]		
at house the	İ.	Username	Public IP Address	Assign Add	ed IP ress	rotocol	Encrypt	ion Login Time	Duration	Bytes Tx	Bytes Rx
		11								nternet zon	e [ ],

Selecione Administration > Administer Sessions > LAN-to-LAN sessions > Actions - Logout para limpar o túnel.

#### Debug de Checkpoint 4.1 Firewall

**Observação:** esta foi uma instalação do Microsoft Windows NT. Como o rastreamento foi definido para Long na janela Policy Editor, o tráfego negado deve aparecer em vermelho em Log Viewer. É possível obter mais depuração detalhada com:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
e em outra janela:
```

C:\WINNT\FW1\4.1\fwstart Emita estes comandos para limpar SAs no ponto de verificação:

fw tab -t IKE\_SA\_table -x
fw tab -t ISAKMP\_ESP\_table -x
fw tab -t inbound\_SPI -x
fw tab -t ISAKMP\_AH\_table -x

Responda sim na janela Tem certeza? prompt.

#### Exemplo de saída de depuração

#### Cisco VPN 3000 Concentrator

```
1 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=180 172.18.124.157
ISAKMP HEADER : (Version 1.0)
 Initiator Cookie(8): EF 61 3C 27 07 74 1B 25
 Responder Cookie(8): 00 00 00 00 00 00 00 00
 Next Payload : SA (1)
Exchange Type : Oakley Main Mode
 Flags
       :
                    0
                    0
 Message ID :
             :
                     164
 Length
7 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=406 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 164
9 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=407 172.18.124.157
processing SA payload
10 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=181 172.18.124.157
SA Payload Decode :
 DOI
      :
                     IPSEC (1)
 Situation
              :
                     Identity Only (1)
 Length
             :
                     92
13 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=182 172.18.124.157
Proposal Decode:
 Proposal # :
                     1
 Protocol ID :
                     ISAKMP (1)
 #of Transforms:
Length :
                     2
                     80
```

16 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=183 172.18.124.157 Transform # 1 Decode for Proposal # 1: Transform # : 1 Transform ID : IKE (1) : 36 Length 18 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=184 172.18.124.157 Phase 1 SA Attribute Decode for Transform # 1: Encryption Alg: DES-CBC (1) Hash Alg SHA (2) : Auth Method : Preshared Key (1) DH Group : Oakley Group 2 (2) Life Time : 86400 seconds 23 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=185 172.18.124.157 Transform # 2 Decode for Proposal # 1: Transform # : 2 Transform ID : IKE (1) Length : 36 25 02/13/2001 14:21:28.530 SEV=8 IKEDECODE/0 RPT=186 172.18.124.157 Phase 1 SA Attribute Decode for Transform # 2: Encryption Alg: DES-CBC (1) Hash Alg : SHA (2) Auth Method : Preshared Key (1) DH Group : Oakley Group 1 (1) 86400 seconds Life Time : 30 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=408 172.18.124.157 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 35 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=409 172.18.124.157 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 38 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=410 172.18.124.157 Phase 1 failure against global IKE proposal # 3: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 41 02/13/2001 14:21:28.530 SEV=7 IKEDBG/0 RPT=411 172.18.124.157 Oakley proposal is acceptable 42 02/13/2001 14:21:28.530 SEV=9 IKEDBG/1 RPT=107 172.18.124.157 processing vid payload 43 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=412 172.18.124.157 processing IKE SA 44 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=413 172.18.124.157 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2

Cfg'd: Oakley Group 1 49 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=414 172.18.124.157 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 52 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=415 172.18.124.157 Phase 1 failure against global IKE proposal # 3: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 55 02/13/2001 14:21:28.530 SEV=7 IKEDBG/28 RPT=3 172.18.124.157 IKE SA Proposal # 1, Transform # 2 acceptable Matches global IKE entry # 1 56 02/13/2001 14:21:28.530 SEV=9 IKEDBG/0 RPT=416 172.18.124.157 constructing ISA\_SA for isakmp 57 02/13/2001 14:21:28.530 SEV=8 IKEDBG/0 RPT=417 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + SA (1) ... total length : 8458 02/13/2001 14:21:28.630 SEV=8 IKEDECODE/0 RPT=187 172.18.124.157 ISAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): EF 61 3C 27 07 74 1B 25 Responder Cookie(8): 24 18 40 A1 3B E4 95 26 Next Payload : KE (4) Exchange Type : Oakley Main Mode Flags : 0 0 Message ID : Length : 152 64 02/13/2001 14:21:28.630 SEV=8 IKEDBG/0 RPT=418 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152 66 02/13/2001 14:21:28.630 SEV=8 IKEDBG/0 RPT=419 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152 68 02/13/2001 14:21:28.630 SEV=9 IKEDBG/0 RPT=420 172.18.124.157 processing ke payload 69 02/13/2001 14:21:28.630 SEV=9 IKEDBG/0 RPT=421 172.18.124.157 processing ISA\_KE 70 02/13/2001 14:21:28.630 SEV=9 IKEDBG/1 RPT=108 172.18.124.157 processing nonce payload 71 02/13/2001 14:21:28.650 SEV=9 IKEDBG/0 RPT=422 172.18.124.157 constructing ke payload 72 02/13/2001 14:21:28.650 SEV=9 IKEDBG/1 RPT=109 172.18.124.157 constructing nonce payload 73 02/13/2001 14:21:28.650 SEV=9 IKEDBG/38 RPT=7 172.18.124.157 Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabiliti es: 20000001) 75 02/13/2001 14:21:28.650 SEV=9 IKEDBG/1 RPT=110 172.18.124.157

constructing vid payload

76 02/13/2001 14:21:28.650 SEV=9 IKE/0 RPT=26 172.18.124.157 Generating keys for Responder... 77 02/13/2001 14:21:28.650 SEV=8 IKEDBG/0 RPT=423 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + KE (4) ... total length : 192 78 02/13/2001 14:21:28.770 SEV=8 IKEDECODE/0 RPT=188 172.18.124.157 ISAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): EF 61 3C 27 07 74 1B 25 Responder Cookie(8): 24 18 40 A1 3B E4 95 26 Next Payload : ID (5) Exchange Type : Oakley Main Mode Flags : 1 (ENCRYPT) Message ID : 0 : 68 Length 84 02/13/2001 14:21:28.770 SEV=8 IKEDBG/0 RPT=424 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64 86 02/13/2001 14:21:28.770 SEV=9 IKEDBG/1 RPT=111 172.18.124.157 Processing ID 87 02/13/2001 14:21:28.770 SEV=9 IKEDBG/0 RPT=425 172.18.124.157 processing hash 88 02/13/2001 14:21:28.770 SEV=9 IKEDBG/0 RPT=426 172.18.124.157 computing hash 89 02/13/2001 14:21:28.770 SEV=9 IKEDBG/23 RPT=7 172.18.124.157 Starting group lookup for peer 172.18.124.157 90 02/13/2001 14:21:28.870 SEV=7 IKEDBG/0 RPT=427 172.18.124.157 Found Phase 1 Group (172.18.124.157) 91 02/13/2001 14:21:28.870 SEV=7 IKEDBG/14 RPT=7 172.18.124.157 Authentication configured for Internal 92 02/13/2001 14:21:28.870 SEV=9 IKEDBG/1 RPT=112 172.18.124.157 constructing ID 93 02/13/2001 14:21:28.870 SEV=9 IKEDBG/0 RPT=428 construct hash payload 94 02/13/2001 14:21:28.870 SEV=9 IKEDBG/0 RPT=429 172.18.124.157 computing hash 95 02/13/2001 14:21:28.870 SEV=8 IKEDBG/0 RPT=430 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + ID (5) ... total length : 64 96 02/13/2001 14:21:28.870 SEV=7 IKEDBG/0 RPT=431 172.18.124.157 Starting phase 1 rekey timer 97 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=189 172.18.124.157 ISAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): EF 61 3C 27 07 74 1B 25 Responder Cookie(8): 24 18 40 A1 3B E4 95 26 Next Payload : HASH (8) Exchange Type : Oakley Quick Mode 1 (ENCRYPT) Flags :

Message ID : 7755aa11 Length 164 : 104 02/13/2001 14:21:29.030 SEV=8 IKEDBG/0 RPT=432 172.18.124.157 RECEIVED Message (msgid=7755aal1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng th : 160 107 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=433 172.18.124.157 processing hash 108 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=434 172.18.124.157 processing SA payload 109 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=190 172.18.124.157 SA Payload Decode : DOI IPSEC (1) : Situation : Identity Only (1) Length : 52 112 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=191 172.18.124.157 Proposal Decode: Proposal # : 1 Protocol ID : ESP (3) #of Transforms: 1 DA 16 3F E3 Spi : Length : 40 116 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=192 172.18.124.157 Transform # 1 Decode for Proposal # 1: Transform # : 1 DES-CBC (2) Transform ID : Length 28 : 118 02/13/2001 14:21:29.030 SEV=8 IKEDECODE/0 RPT=193 172.18.124.157 Phase 2 SA Attribute Decode for Transform # 1: Life Time : 28800 seconds HMAC Algorithm: SHA (2) Tunnel (1) Encapsulation : 121 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=113 172.18.124.157 processing nonce payload 122 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=114 172.18.124.157 Processing ID 123 02/13/2001 14:21:29.030 SEV=5 IKE/35 RPT=14 172.18.124.157 Received remote IP Proxy Subnet data in ID Payload: Address 10.32.50.0, Mask 255.255.255.0, Protocol 0, Port 0 125 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=115 172.18.124.157 Processing ID 126 02/13/2001 14:21:29.030 SEV=5 IKE/34 RPT=14 172.18.124.157 Received local IP Proxy Subnet data in ID Payload: Address 192.168.1.0, Mask 255.255.255.0, Protocol 0, Port 0 128 02/13/2001 14:21:29.030 SEV=5 IKE/66 RPT=4 172.18.124.157 IKE Remote Peer configured for SA: L2L: to\_checkpoint 129 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=435 172.18.124.157 processing IPSEC SA 130 02/13/2001 14:21:29.030 SEV=7 IKEDBG/27 RPT=1 172.18.124.157

IPSec SA Proposal # 1, Transform # 1 acceptable 131 02/13/2001 14:21:29.030 SEV=7 IKEDBG/0 RPT=436 172.18.124.157 IKE: requesting SPI! 132 02/13/2001 14:21:29.030 SEV=8 IKEDBG/6 RPT=6 IKE got SPI from key engine: SPI = 0x4d6e483f 133 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=437 172.18.124.157 oakley constucting quick mode 134 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=438 172.18.124.157 constructing blank hash 135 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=439 172.18.124.157 constructing ISA\_SA for ipsec 136 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=116 172.18.124.157 constructing ipsec nonce payload 137 02/13/2001 14:21:29.030 SEV=9 IKEDBG/1 RPT=117 172.18.124.157 constructing proxy ID 138 02/13/2001 14:21:29.030 SEV=7 IKEDBG/0 RPT=440 172.18.124.157 Transmitting Proxy Id: Remote subnet: 10.32.50.0 Mask 255.255.255.0 Protocol 0 Port 0 Local subnet: 192.168.1.0 mask 255.255.255.0 Protocol 0 Port 0 141 02/13/2001 14:21:29.030 SEV=9 IKEDBG/0 RPT=441 172.18.124.157 constructing qm hash 142 02/13/2001 14:21:29.030 SEV=8 IKEDBG/0 RPT=442 172.18.124.157 SENDING Message (msgid=7755aa11) with payloads : HDR + HASH (8) ... total length : 156 144 02/13/2001 14:21:29.270 SEV=8 IKEDECODE/0 RPT=194 172.18.124.157 ISAKMP HEADER : (Version 1.0) Initiator Cookie(8): EF 61 3C 27 07 74 1B 25 Responder Cookie(8): 24 18 40 A1 3B E4 95 26 Next Payload : HASH (8) Exchange Type : Oakley Quick Mode : 1 (ENCRYPT) Flags 7755aa11 Message ID : Length : 60 151 02/13/2001 14:21:29.270 SEV=8 IKEDBG/0 RPT=443 172.18.124.157 RECEIVED Message (msgid=7755aal1) with payloads : HDR + HASH (8) + NONE (0) ... total length : 52 153 02/13/2001 14:21:29.270 SEV=9 IKEDBG/0 RPT=444 172.18.124.157 processing hash 154 02/13/2001 14:21:29.270 SEV=9 IKEDBG/0 RPT=445 172.18.124.157 loading all IPSEC SAs 155 02/13/2001 14:21:29.270 SEV=9 IKEDBG/1 RPT=118 172.18.124.157 Generating Quick Mode Key! 156 02/13/2001 14:21:29.270 SEV=9 IKEDBG/1 RPT=119 172.18.124.157 Generating Quick Mode Key! 157 02/13/2001 14:21:29.270 SEV=7 IKEDBG/0 RPT=446 172.18.124.157 Loading subnet:

Dst: 192.168.1.0 mask: 255.255.255.0

Src: 10.32.50.0 mask: 255.255.255.0

constructing delete payload

159 02/13/2001 14:21:29.270 SEV=4 IKE/49 RPT=6 172.18.124.157 Security negotiation complete for LAN-to-LAN Group (172.18.124.157) Responder, Inbound SPI = 0x4d6e483f, Outbound SPI = 0xda163fe3 161 02/13/2001 14:21:29.270 SEV=8 IKEDBG/7 RPT=6 IKE got a KEY\_ADD msg for SA: SPI = 0xda163fe3 162 02/13/2001 14:21:29.270 SEV=8 IKEDBG/0 RPT=447 pitcher: rcv KEY\_UPDATE, spi 0x4d6e483f 163 02/13/2001 14:21:29.670 SEV=8 IKEDECODE/0 RPT=195 172.18.124.157 ISAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): EF 61 3C 27 07 74 1B 25 Responder Cookie(8): 24 18 40 A1 3B E4 95 26 HASH (8) Next Payload : Oakley Quick Mode Exchange Type : Flags : 1 (ENCRYPT) Message ID : 7755aa11 : Length 60 170 02/13/2001 14:21:29.670 SEV=6 IKE/0 RPT=27 172.18.124.157 Duplicate Phase 2 packet detected! 171 02/13/2001 14:21:29.760 SEV=8 IKEDECODE/0 RPT=196 172.18.124.157 ISAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): EF 61 3C 27 07 74 1B 25 Responder Cookie(8): 24 18 40 A1 3B E4 95 26 Next Payload : HASH (8) Exchange Type : Oakley Quick Mode Flags : 1 (ENCRYPT) Message ID : 7755aa11 Length : 60 178 02/13/2001 14:21:29.760 SEV=6 IKE/0 RPT=28 172.18.124.157 Duplicate Phase 2 packet detected! 179 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=448 pitcher: recv KEY\_SA\_ACTIVE spi 0x4d6e483f 180 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=449 KEY\_SA\_ACTIVE old rekey centry found with new spi 0x4d6e483f 181 02/13/2001 14:21:29.880 SEV=7 IKEDBG/9 RPT=5 172.18.124.157 IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0 182 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=450 172.18.124.157 IKE SA MM:f2ea8e68 rcv'd Terminate: state MM\_ACTIVE\_REKEY flags 0x000000e6, refcnt 1, tuncnt 0 184 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=451 172.18.124.157 IKE SA MM:f2ea8e68 terminating: flags 0x000000a6, refcnt 0, tuncnt 0 185 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=452 sending delete message 186 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=453 172.18.124.157 constructing blank hash 187 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=454

188 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=455 172.18.124.157 constructing qm hash

189 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=456 172.18.124.157 SENDING Message (msgid=87b7c1a4) with payloads : HDR + HASH (8) ... total length : 80

191 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=457 172.18.124.157 IKE SA MM:241840al rcv'd Terminate: state MM\_REKEY\_DONE flags 0x00000082, refcnt 1, tuncnt 1

193 02/13/2001 14:21:29.880 SEV=6 IKE/0 RPT=29 172.18.124.157 Removing peer from peer table failed, no match!

194 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=458 sending delete message

195 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=459 172.18.124.157 constructing blank hash

196 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=460 constructing ipsec delete payload

197 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=461 172.18.124.157 constructing qm hash

198 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=462 172.18.124.157 SENDING Message (msgid=63f2abb8) with payloads : HDR + HASH (8) ... total length : 68

200 02/13/2001 14:21:29.880 SEV=7 IKEDBG/9 RPT=6 172.18.124.157 IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

201 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=463 172.18.124.157 IKE SA MM:241840al terminating: flags 0x00000082, refcnt 0, tuncnt 0

202 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=464 sending delete message

203 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=465 172.18.124.157 constructing blank hash

204 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=466 constructing delete payload

205 02/13/2001 14:21:29.880 SEV=9 IKEDBG/0 RPT=467 172.18.124.157 constructing qm hash

206 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=468 172.18.124.157 SENDING Message (msgid=d6a00071) with payloads : HDR + HASH (8) ... total length : 80

208 02/13/2001 14:21:29.880 SEV=4 AUTH/22 RPT=13 User 172.18.124.157 disconnected

209 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=469 pitcher: received key delete msg, spi 0x2962069b

210 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=470 pitcher: received key delete msg, spi 0xda163fe2

211 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=471 pitcher: received key delete msg, spi 0x4d6e483f

212 02/13/2001 14:21:29.880 SEV=8 IKEDBG/0 RPT=472 pitcher: received key delete msg, spi 0xda163fe3 213 02/13/2001 14:21:29.890 SEV=8 IKEDBG/0 RPT=473 pitcher: received a key acquire message! 214 02/13/2001 14:21:29.890 SEV=4 IKE/41 RPT=6 172.18.124.157 IKE Initiator: New Phase 1, Intf 2, IKE Peer 172.18.124.157 local Proxy Address 192.168.1.0, remote Proxy Address 10.32.50.0, SA (L2L: to\_checkpoint) 217 02/13/2001 14:21:29.890 SEV=9 IKEDBG/0 RPT=474 172.18.124.157 constructing ISA\_SA for isakmp 218 02/13/2001 14:21:29.890 SEV=8 IKEDBG/0 RPT=475 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + SA (1) ... total length : 84219 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=197 172.18.124.157 TSAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): FE 75 39 26 66 21 F6 F8 Responder Cookie(8): 67 1D 73 71 AE 2B 88 2E Next Payload : SA (1) Exchange Type : Oakley Main Mode Flags : 0 Message ID : 0 : 84 Length 225 02/13/2001 14:21:30.430 SEV=8 IKEDBG/0 RPT=476 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total length : 84 227 02/13/2001 14:21:30.430 SEV=8 IKEDBG/0 RPT=477 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total length : 84 229 02/13/2001 14:21:30.430 SEV=9 IKEDBG/0 RPT=478 172.18.124.157 processing SA payload 230 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=198 172.18.124.157 SA Payload Decode : DOI : IPSEC (1) Situation : Identity Only (1) Length : 56 233 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=199 172.18.124.157 Proposal Decode: Proposal # : 1 Protocol ID : ISAKMP (1) #of Transforms: 1 44 Length : 236 02/13/2001 14:21:30.430 SEV=8 IKEDECODE/0 RPT=200 172.18.124.157 Transform # 1 Decode for Proposal # 1: Transform # : 1 Transform ID : IKE (1) Length : 36 238 02/13/2001 14:21:30.440 SEV=8 IKEDECODE/0 RPT=201 172.18.124.157 Phase 1 SA Attribute Decode for Transform # 1: Encryption Alg: DES-CBC (1) : Hash Alg SHA (2) : DH Group Oakley Group 1 (1)

Auth Method : Preshared Key (1) Life Time 86400 seconds : 243 02/13/2001 14:21:30.440 SEV=7 IKEDBG/0 RPT=479 172.18.124.157 Oakley proposal is acceptable 244 02/13/2001 14:21:30.440 SEV=9 IKEDBG/0 RPT=480 172.18.124.157 constructing ke payload 245 02/13/2001 14:21:30.440 SEV=9 IKEDBG/1 RPT=120 172.18.124.157 constructing nonce payload 246 02/13/2001 14:21:30.440 SEV=9 IKEDBG/38 RPT=8 172.18.124.157 Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabiliti es: 20000001) 248 02/13/2001 14:21:30.440 SEV=9 IKEDBG/1 RPT=121 172.18.124.157 constructing vid payload 249 02/13/2001 14:21:30.440 SEV=8 IKEDBG/0 RPT=481 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + KE (4) ... total length : 192 250 02/13/2001 14:21:30.540 SEV=8 IKEDECODE/0 RPT=202 172.18.124.157 ISAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): FE 75 39 26 66 21 F6 F8 Responder Cookie(8): 67 1D 73 71 AE 2B 88 2E Next Payload : KE (4) Exchange Type : Oakley Main Mode Flags 0 : Message ID : 0 152 Length : 256 02/13/2001 14:21:30.540 SEV=8 IKEDBG/0 RPT=482 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152 258 02/13/2001 14:21:30.540 SEV=8 IKEDBG/0 RPT=483 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152 260 02/13/2001 14:21:30.540 SEV=9 IKEDBG/0 RPT=484 172.18.124.157 processing ke payload 261 02/13/2001 14:21:30.540 SEV=9 IKEDBG/0 RPT=485 172.18.124.157 processing ISA\_KE 262 02/13/2001 14:21:30.540 SEV=9 IKEDBG/1 RPT=122 172.18.124.157 processing nonce payload 263 02/13/2001 14:21:30.560 SEV=9 IKE/0 RPT=30 172.18.124.157 Generating keys for Initiator... 264 02/13/2001 14:21:30.570 SEV=9 IKEDBG/1 RPT=123 172.18.124.157 constructing ID 265 02/13/2001 14:21:30.570 SEV=9 IKEDBG/0 RPT=486 construct hash payload 266 02/13/2001 14:21:30.570 SEV=9 IKEDBG/0 RPT=487 172.18.124.157 computing hash 267 02/13/2001 14:21:30.570 SEV=8 IKEDBG/0 RPT=488 172.18.124.157

SENDING Message (msgid=0) with payloads :

HDR + ID (5) ... total length : 64 268 02/13/2001 14:21:30.740 SEV=8 IKEDECODE/0 RPT=203 172.18.124.157 ISAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): FE 75 39 26 66 21 F6 F8 Responder Cookie(8): 67 1D 73 71 AE 2B 88 2E ID (5) Next Payload : Exchange Type : Oakley Main Mode 1 (ENCRYPT) Flags : Message ID : 0 Length : 68 274 02/13/2001 14:21:30.740 SEV=8 IKEDBG/0 RPT=489 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64 276 02/13/2001 14:21:30.740 SEV=9 IKEDBG/1 RPT=124 172.18.124.157 Processing ID 277 02/13/2001 14:21:30.740 SEV=9 IKEDBG/0 RPT=490 172.18.124.157 processing hash 278 02/13/2001 14:21:30.740 SEV=9 IKEDBG/0 RPT=491 172.18.124.157 computing hash 279 02/13/2001 14:21:30.740 SEV=9 IKEDBG/23 RPT=8 172.18.124.157 Starting group lookup for peer 172.18.124.157 280 02/13/2001 14:21:30.830 SEV=8 IKEDECODE/0 RPT=204 172.18.124.157 TSAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): FE 75 39 26 66 21 F6 F8 Responder Cookie(8): 67 1D 73 71 AE 2B 88 2E Next Payload : ID (5) Exchange Type : Oakley Main Mode 1 (ENCRYPT) Flags : : 0 Message ID Length : 68 286 02/13/2001 14:21:30.830 SEV=6 IKE/0 RPT=31 172.18.124.157 Duplicate Phase 1 packet detected! 287 02/13/2001 14:21:30.830 SEV=6 IKE/0 RPT=32 MM received unexpected event EV\_RESEND\_MSG in state MM\_I\_DONE 288 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=492 172.18.124.157 Found Phase 1 Group (172.18.124.157) 289 02/13/2001 14:21:30.840 SEV=7 IKEDBG/14 RPT=8 172.18.124.157 Authentication configured for Internal 290 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=493 172.18.124.157 Oakley begin quick mode 291 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=494 172.18.124.157 Starting phase 1 rekey timer 292 02/13/2001 14:21:30.840 SEV=4 AUTH/21 RPT=15 User 172.18.124.157 connected 293 02/13/2001 14:21:30.840 SEV=8 IKEDBG/6 RPT=7 IKE got SPI from key engine: SPI = 0x08201539 294 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=495 172.18.124.157

oakley constucting quick mode

295 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=496 172.18.124.157 constructing blank hash 296 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=497 172.18.124.157 constructing ISA\_SA for ipsec 297 02/13/2001 14:21:30.840 SEV=9 IKEDBG/1 RPT=125 172.18.124.157 constructing ipsec nonce payload 298 02/13/2001 14:21:30.840 SEV=9 IKEDBG/1 RPT=126 172.18.124.157 constructing proxy ID 299 02/13/2001 14:21:30.840 SEV=7 IKEDBG/0 RPT=498 172.18.124.157 Transmitting Proxy Id: Local subnet: 192.168.1.0 mask 255.255.255.0 Protocol 0 Port 0 Remote subnet: 10.32.50.0 Mask 255.255.255.0 Protocol 0 Port 0 302 02/13/2001 14:21:30.840 SEV=9 IKEDBG/0 RPT=499 172.18.124.157 constructing qm hash 303 02/13/2001 14:21:30.840 SEV=8 IKEDBG/0 RPT=500 172.18.124.157 SENDING Message (msgid=23bc1709) with payloads : HDR + HASH (8) ... total length : 184 305 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=205 172.18.124.157 ISAKMP HEADER : ( Version 1.0 ) Initiator Cookie(8): FE 75 39 26 66 21 F6 F8 Responder Cookie(8): 67 1D 73 71 AE 2B 88 2E Next Payload : HASH (8) Exchange Type : Oakley Quick Mode Flags : 1 (ENCRYPT) Message ID : 23bc1709 Length : 164 312 02/13/2001 14:21:31.000 SEV=8 IKEDBG/0 RPT=501 172.18.124.157 RECEIVED Message (msgid=23bc1709) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng th : 156 315 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=502 172.18.124.157 processing hash 316 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=503 172.18.124.157 processing SA payload 317 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=206 172.18.124.157 SA Payload Decode : : IPSEC (1) DOT : Situation Identity Only (1) Length : 48 320 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=207 172.18.124.157 Proposal Decode: Proposal # : 1 Protocol ID : ESP (3) #of Transforms: 1 DA 16 3F E4 Spi : Length : 36 324 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=208 172.18.124.157 Transform # 1 Decode for Proposal # 1: Transform # : 1 Transform ID : DES-CBC (2)

326 02/13/2001 14:21:31.000 SEV=8 IKEDECODE/0 RPT=209 172.18.124.157 Phase 2 SA Attribute Decode for Transform # 1: Life Time : 28800 seconds Encapsulation : Tunnel (1) SHA (2) HMAC Algorithm: 329 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=127 172.18.124.157 processing nonce payload 330 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=128 172.18.124.157 Processing ID 331 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=129 172.18.124.157 Processing ID 332 02/13/2001 14:21:31.000 SEV=9 IKEDBG/0 RPT=504 172.18.124.157 loading all IPSEC SAs 333 02/13/2001 14:21:31.000 SEV=9 IKEDBG/1 RPT=130 172.18.124.157 Generating Quick Mode Key! 334 02/13/2001 14:21:31.010 SEV=9 IKEDBG/1 RPT=131 172.18.124.157 Generating Quick Mode Key! 335 02/13/2001 14:21:31.010 SEV=7 IKEDBG/0 RPT=505 172.18.124.157 Loading subnet: Dst: 10.32.50.0 mask: 255.255.255.0 Src: 192.168.1.0 mask: 255.255.255.0 337 02/13/2001 14:21:31.010 SEV=4 IKE/49 RPT=7 172.18.124.157 Security negotiation complete for LAN-to-LAN Group (172.18.124.157) Initiator, Inbound SPI = 0x08201539, Outbound SPI = 0xda163fe4 339 02/13/2001 14:21:31.010 SEV=9 IKEDBG/0 RPT=506 172.18.124.157 oakley constructing final quick mode 340 02/13/2001 14:21:31.010 SEV=8 IKEDBG/0 RPT=507 172.18.124.157 SENDING Message (msgid=23bc1709) with payloads : HDR + HASH (8) ... total length : 76 342 02/13/2001 14:21:31.010 SEV=8 IKEDBG/7 RPT=7 IKE got a KEY\_ADD msg for SA: SPI = 0xda163fe4 343 02/13/2001 14:21:31.010 SEV=8 IKEDBG/0 RPT=508 pitcher: rcv KEY\_UPDATE, spi 0x8201539 344 02/13/2001 14:21:31.890 SEV=8 IKEDBG/0 RPT=509 pitcher: recv KEY\_SA\_ACTIVE spi 0x8201539 345 02/13/2001 14:21:31.890 SEV=8 IKEDBG/0 RPT=510 KEY\_SA\_ACTIVE no old rekey centry found with new spi 0x8201539, mess\_id 0x0

### Informações Relacionadas

Length

:

24

- <u>Negociação IPsec/Protocolos IKE</u>
- Suporte Técnico e Documentação Cisco Systems