# Configurando um túnel IPSec entre um Cisco VPN 3000 Concentrator e um Checkpoint NG Firewall

## Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados Conventions** Diagrama de Rede Configurações Configurar o VPN 3000 Concentrator Configurar o ponto de verificação NG Verificar Verificar a comunicação de rede Exibir status do túnel no ponto de controle NG Exibir o status do túnel no VPN Concentrator Troubleshoot Sumarização de rede Depurações para ponto de controle NG Debugs para concentrador de VPN Informações Relacionadas

## **Introduction**

Este documento demonstra como configurar um túnel IPSec com chaves pré-compartilhadas para comunicação entre duas redes privadas. Neste exemplo, as redes de comunicação são a rede privada 192.168.10.x dentro do Cisco VPN 3000 Concentrator e a rede privada 10.32.x.x dentro do firewall Checkpoint Next Generation (NG).

# **Prerequisites**

## **Requirements**

- O tráfego de dentro do VPN Concentrator e de dentro do Checkpoint NG para a Internet representado aqui pelas redes 172.18.124.x deve fluir antes de iniciar essa configuração.
- Os usuários devem estar familiarizados com a negociação de IPSec. Esse processo pode ser dividido em cinco etapas, incluindo duas fases de Internet Key Exchange (IKE).Um túnel de

IPSec é iniciado por um tráfego interessante. O tráfego é considerado interessante quando ele é transmitido entre os peers IPSec.Na Fase 1 IKE, os correspondentes IPSec negociam a política de Associação de segurança (SA) IKE estabelecida. Quando os correspondentes são autenticados, um túnel seguro é criado com o ISAKMP (Internet Security Association and Key Management Protocol).Na Fase 2 da IKE, os peers de IPSec usam o túnel autenticado e seguro para negociar transformações de SA do IPSec. A negociação da política compartilhada determina como o túnel de IPSec é estabelecido.O túnel IPSec é criado e os dados são transferidos entre os peers IPSec com base nos parâmetros de IPSec configurados nos conjuntos de transformação de IPSec.O túnel de IPSec finaliza quando os IPSec SAs são excluídos ou quando sua vida útil expira.

### **Componentes Utilizados**

Essa configuração foi desenvolvida e testada com estas versões de software e hardware:

- VPN 3000 Series Concentrator 3.5.2
- Firewall NG de ponto de verificação

### **Conventions**

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

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



**Observação:** o esquema de endereçamento IP usado nesta configuração não é legalmente roteável na Internet. Eles são endereços RFC 1918, que foram usados em um ambiente de laboratório.

# **Configurações**

### Configurar o VPN 3000 Concentrator

Conclua estes passos para configurar o VPN 3000 Concentrator:

1. Vá para **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** para configurar a sessão de LAN para LAN. Defina as opções para autenticação e algoritmos IKE, chave pré-compartilhada, endereço IP do peer e parâmetros de rede local e remota. Clique em Apply.Nesta configuração, a autenticação foi definida como ESP-MD5-HMAC e a criptografia foi definida como

#### 3DES.

Configuration   System   Tunneling Protocols   IPSec LAN-to	o-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  C Entire certificate chain Transmission  F Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key ciscortprules	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 reserve of a subnet mark A
Wildcard Mask 0.0.0.256	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 <i>wildcard</i> 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. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nn addresses.
Apply Cancel	

2. Vá para Configuration > System > Tunneling Protocols > IPSec > IKE Proposal e defina os parâmetros necessários.Selecione a proposta IKE-3DES-MD5 e verifique os parâmetros selecionados para a proposta. Clique em Apply para configurar a sessão LAN-to-LAN.Estes são os parâmetros para esta configuração:

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. Vá para Configuration > Policy Management > Traffic Management > Security Associations, selecione o SA de IPSec criado para a sessão e verifique os parâmetros de SA de IPSec

escolhidos para a sessão LAN a LAN.Nesta configuração, o nome da sessão LAN a LAN era "Checkpoint", de modo que o SA do IPSec foi criado automaticamente como "L2L:

#### Checkpoint."

Configuration   Policy Management   Traffic Manag	ement   Security Associatio	ns	en Honerland 🗖
		2.84	ie weeden
This section lets you add, configure, modify, and onegotiate IKE parameters.	delete IPSec Security Assoc	iations (SAs). Security Associations use <u>IKE Prop</u>	osals to
Click Add to add an SA, or select an SA and click	k Modify or Delete.		
	IPSec SAs	Actions	
	ESP-DES-MD5 ESP-3DES-MD5		
	ESP/IKE-3DES-MD5 ESP-3DES-NONE	Add	
	ESP-L2TP-TRANSPORT ESP-3DES-MD5-DH7	Modify	
	L2L: Checkpoint	Delete	

# Estes são os parâmetros para esta SA:

Configuration   Policy Manag	gement   Traffic Management   S	Security Associations   Modify
Modify a configured Securi	ty 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	<ul> <li>Entire certificate chain</li> <li>Identity certificate only</li> </ul>	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		

### Configurar o ponto de verificação NG

Os objetos e as regras de rede são definidos no ponto de verificação NG para compor a política relacionada à configuração de VPN a ser configurada. Essa política é então instalada com o Editor de política NG do ponto de verificação para concluir o lado NG do ponto de verificação da configuração.

1. Crie os dois objetos de rede para a rede Checkpoint NG e a rede VPN Concentrator que

criptografarão o tráfego interessante.para criar objetos, selecione **Gerenciar > Objetos de Rede** e selecione **Novo > Rede**. Insira as informações de rede apropriadas e clique em OK.Esses exemplos mostram a configuração de objetos de rede chamados CP\_inside (a rede interna do Checkpoint NG) e CONC\_INSIDE (a rede interna do VPN

·	Network Proper	ties - CP_insio	le		×	
	General NAT	1				
	<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		]		
	Color:	-				
	- Broadcast	address: ed Ot	N <u>o</u> t included	]		
ator)		ОК	Cancel	Help	]	

Network Prope	ties - CONC_INSIDE		×
General NAT			
<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:	<b></b>		
Broadcas <u>I</u> nclud	address: ed <u>O No</u> t included		
	OK Cancel	Help	

2. Vá para Gerenciar > Objetos de Rede e selecione Novo > Estação de Trabalho para criar objetos de estação de trabalho para os dispositivos VPN, Checkpoint NG e VPN Concentrator.Observação: você pode usar o objeto de estação de trabalho Checkpoint NG criado durante a configuração inicial de NG do ponto de verificação. Selecione as opções para definir a estação de trabalho como Gateway and Interoperable VPN Device e clique em OK.Estes exemplos mostram a configuração de objetos chamados ciscocp (Checkpoint NG) e 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

Workstati	on Properties -	ISCO_CONC	×
Gene	ral	General	
- NAT	logy	Name: CISCO_CONC	
	nced	IP Address: 172.18.124.131	<u>G</u> et address
		Comment: VPN Concentrator	
		Cojor:	
		Type: C <u>H</u> ost CGate <u>w</u> ay	
		Check Point Products	<u></u>
		Check Point products installed: Version	G 💌 Get Version
		□VPN-1 & FireWall-1 □ FloodGate-1 □ Policy Server □ Management Station	-
		Object Management	
		C Managed by this Management Server (Inter	nel)
		C Managed by another Management Server (E	[xternal]
		Interoperable ⊻PN Device	
1		OK	Cancel Help

3. Vá para Gerenciar > Objetos de Rede > Editar para abrir a janela Propriedades da Estação de Trabalho para a estação de trabalho Checkpoint NG (ciscocp neste exemplo). Selecione Topologia nas opções no lado esquerdo da janela e selecione a rede a ser criptografada. Clique em Editar para definir as propriedades da interface.Neste exemplo, CP\_inside é a rede interna do ponto de verificação NG.

Vorkstation Properties - c	iscocp				x
General Topology	Topology Get Interfaces	1			
- VPN - Authentication - Management	Name E100B0 E100B1	IP Address 10.32.50.50 172.18.124.157	Network Mask 255.255.128.0 255.255.255.0	IP Addresses behind CP_inside External	
. Advanced					
	I ■	Edit	Remove	Show	
	Show all IPs bet	hind Gateway		2,000	
	VPN Domain	es <u>b</u> ehind Gateway b	ased on Topology	Show	
	C <u>M</u> anually Defin	ned	7	Sho <u>w</u>	
	Exportable for	SecuRemote			
			ОК	Cancel Help	

4. Na janela Propriedades da interface, selecione a opção para designar a estação de trabalho como interna e especifique o endereço IP apropriado. Click OK.As seleções de topologia mostradas designam a estação de trabalho como interna e especificam endereços IP por trás da interface

	Interface Properties	×	
	General Topology QoS		
	Topology		
	$\bigcirc$ External (leads out to the internet)		
	Internal (leads to the local network)		
	IP Addresses behind this interface:		
	O Not Defined		
	O Network defined by the interface IP and Net Mask		
	Anti-Spoofing		
	Perform Anti-Spoofing based on interface topology		
	Spoof Tracking: 🔿 N <u>o</u> ne 💿 <u>L</u> og 🔿 <u>A</u> lert		
<u>.</u>	OK Cancel Help		

5. Na janela Propriedades da estação de trabalho, selecione a interface externa no Ponto de verificação NG que sai para a Internet e clique em **Editar** para definir as propriedades da interface. Selecione a opção para designar a topologia como externa e clique em

Interface Properties
General Topology QoS
Topology
<ul> <li>External (leads out to the internet)</li> </ul>
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
Perform Anti-Spoofing based on interface topology
Spoof Tracking: 🔿 N <u>o</u> ne 💿 Log 🔿 <u>A</u> lert
OK Cancel Help

- OK.
- 6. Na janela Propriedades da estação de trabalho no Ponto de verificação NG, selecione VPN nas opções no lado esquerdo da janela e selecione os parâmetros IKE para algoritmos de criptografia e autenticação. Clique em Editar para configurar as propriedades de IKE.

Workstation Properties - o	iscocp X
General Topology NAT VPN Authentication Management T-Advanced	VPN     Encryption schemes     Image: Imag
	Nickname DN   Certificate Authority   Image: Certificate Authority   Add   Egit   Press Press Here

7. Defina as propriedades de IKE para corresponder às propriedades no VPN Concentrator.Neste exemplo, selecione a opção de criptografia para **3DES** e a opção de

IKE Properties General	×
Support key exchange encryptio	n with: Support data integrity with: MD <u>5</u>
Support authentication methods:     Image: Pre-Shared Secret     Image: Public Key Signatures     Image: VPN-1 & FireWall-1 authent	Edit <u>Secrets</u> Specify ication for SecuRemote (Hybrid Mode)
	<u>A</u> dvanced

hash para MD5.

 Selecione a opção de autenticação para Segredos pré-compartilhados e clique em Editar segredos para definir a chave pré-compartilhada como compatível com a chave précompartilhada no VPN Concentrator. Clique em Editar para inserir sua chave como mostrado e clique em Definir,

Sha	red Secret	×
ſ	- Shared Secrets List:	
	Peer Name Shared Secret CISCO_CONC ****	<u>E</u> dit <u>R</u> emove
	Enter secret: ciscortprules Set	
<b>&lt;</b> .	OK Cancel	<u>H</u> elp

 Na janela de propriedades de IKE, clique em Avançado... e alterar estas configurações:Desmarque a opção para o modo agressivo de suporte.Selecione a opção Support key exchange for subnets.Quando terminar, clique em OK,

Advanced IKE properties			×
Use UDP encapsulation			
	UDP. VPN1_IP	SEC_encapsu 💌	3
Support Diffie-Hellman groups			
	Group 1 (76	58 bit) 24 bit)	
	Group 5 (15	536 bit)	
Rekeying Parameters			
Renegotiate IKE security asso	ciations	1440	Minutes
Renegotiate IPSEC Security a	ssociations every	3600	Seconds
🔲 Renegotiate IPSEC Securi	ty associations eve	ery 50000	KBytes
Misc			
Support IP <u>c</u> ompression fo	r SecureClient		
Support aggresive mode			
Support key exchange for	subnets		
	Cancel	Help	1
	Cancer	<u> </u>	]

10. Vá para Gerenciar > Objetos de Rede > Editar para abrir a janela Propriedades da Estação de Trabalho do VPN Concentrator. Selecione Topologia nas opções no lado esquerdo da janela para definir manualmente o domínio VPN.Neste exemplo, CONC\_INSIDE (a rede interna do VPN Concentrator) é definida como o domínio VPN.

w	orkstation Properties - C	ISCO_CONC			×
	Garand	Topology			
	Topology	n opology	1		
	- NAT	Liet Interfaces			
	- VPN 	Name	IP Address	Network Mask	
			· · · · · · · · · · · · · · · · · · ·		······································
		Add	Edt.	Bemove Show	1
			2000	100000 2000	
		5how all IPs beh	nd laateway		
		VPN Domain			
		<ul> <li>All IP Addresse: information.</li> </ul>	s <u>b</u> ehind Gateway b	ased on Topology	Show
		Manuallu Defini	ed LL cours av		Show
		<u>M</u> andaly Dank		SDE 🔟	
		Europetable for 9	eou Remote		
			repuniennote		
			_		
				OK Cance	Help

11. Selecione VPN nas opções no lado esquerdo da janela e selecione IKE como esquema de criptografia. Clique em Editar para configurar as propriedades de IKE.

Workstation Properties -	CISCO_CONC			×
General Topology NAT Advanced	VPN Encryption schemes			
		OK	Cancel	Help

12. Defina as propriedades de IKE para refletir a configuração atual no VPN Concentrator.Neste exemplo, defina a opção de criptografia para **3DES** e a opção de hash

General	
Support key exchange encryption with: Support data integrity with:	
□ S DES I MD <u>5</u>	
I I I I I I I I I I I I I I I I I I I	
Support authentication methods:	
✓ Pre-Shared Secret Edit Secrets	
Public Key Signatures <u>Matching Criteria</u>	
Advanced	
<u>Advanced</u>	
OK Cancel Help	

para MD5.

13. Selecione a opção de autenticação para **Segredos pré-compartilhados** e clique em **Editar segredos** para definir a chave pré-compartilhada. Clique em **Editar** para inserir sua chave como mostrado e clique em **Definir**,

Share	ed Secret				×
<u>ح</u>	Shared Secrets List:				1
	Peer Name	Shared Sec	aret 🛛		
	ciscocp	****		<u>E</u> dit	
				Remove	
	Enter secret: ciso	cortprules	Set		
	ОК	Cance	el	<u>H</u> elp	

14. Na janela de propriedades de IKE, clique em Avançado... e alterar estas configurações:Selecione o grupo Diffie-Hellman apropriado para as propriedades IKE.Desmarque a opção para o modo agressivo de suporte.Selecione a opção Support key exchange for subnets.Quando terminar, clique em OK,

Ad	vanced IKE properties			×
	Z Use UDP encapsulation			
		UDP VPN1_IPS	SEC_encapsi 💌	
9	Support Diffie-Hellman groups			
		Group 1 (76	8 bit)	
		Group 2 (10	124 Dit) (36 bit)	
F	Rekeying Parameters			
	Renegotiate IKE security assoc	iations	1440 🚊	Minutes
	Renegotiate IPSEC Security as	sociations every	3600 🕂	Seconds
	🔲 Renegotiate IPSEC Securit	y associations eve	ery 50000 🚊	KBytes
h	Misc			
	Support IP compression for	SecureClient		
	Support aggresive mode			
	🔽 Support key exchange for §	ubnets		
	ОК	Cancel	<u>H</u> elp	

15. Selecione Regras > Adicionar Regras > Topo para configurar as regras de criptografia para a política. Na janela Editor de políticas, insira uma regra com origem como CP\_inside (rede interna do ponto de controle NG) e destino como CONC\_INSIDE (rede interna do VPN Concentrator). Defina valores para Serviço = Qualquer , Ação = Criptografia e Rastreamento = Log. Quando tiver adicionado a seção Criptografar ação da regra, clique com o botão direito do mouse em Ação e selecione Editar propriedades.

CISCOCP - Check Point Policy Editor -	Standar	d				a and a second second	
File Edit View Manage Rules Policy	Topology	Search Window H	ielp				
」■●業品館 疊盤液	#	•	≝ "L ↔ 🛛 🛡	54 🛛 🖄 🏦			
1 📬 📰 📰 🖓 24 84   🗛 C	190	۵ 🖸 🔪 🍈 🗍	9				
<u>♀ &lt; &lt; @ 8 8 0 %</u>	EE Sec	unity - Standard 🔠	Address Translation - St	andard 💭 QoS - S	itandard 🛄 Desktop S	ecurity - Standard	
E St Network Objects	NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL
Workstation		300//62	DESTIMATION	SERVICE	ALTION	THACK	INSTALL
- CISCO_CONC	1	부 CP_inside 부 CONC_INSIDE	부 CONC_INSIDE 부 CP_inside	* Any	Edt propert	ties	Gateway:
-++ CONC_INSIDE	2	++ CP_inside	* Any	* Any	Add Encryp	tion Som	Gateway
- Domain - OSE Device - ME Embedded Device - ME Group - WE Logical Server - ME Address Range					accept     accept     drop     reject     User Auth     Client Auth     Section 8	n h	
Gateway Ouster						wari	
- M Change Carlos		NE CO_CONC ocp	IP 172.18.1 172.18.1	24.131 VPN Cond 24.157 Checkpoi	centrator nt Externa Query Colu	rypt	
					Clear Query	1	

### 16. Selecione IKE e clique em

Encryptic	n Properties		×
General	]		
End	ryption <u>s</u> chemes defined: —		
	₩E ₩ FWZ		
	<u>E</u> dit		
	OK Ca	ncel   ł	 

17. Na janela Propriedades de IKE, altere as propriedades para concordar com a transformação do VPN Concentrator.Defina a opção Transform como Encryption + Data Integrity (ESP).Defina o algoritmo de criptografia como 3DES.Defina Data Integrity (Integridade dos dados) como MD5.Defina o Gateway de peer permitido para corresponder ao VPN Concentrator (CISCO\_CONC).Quando terminar, clique em

IKE Properties	
General	
Transform	
Encryption + Data Integ	nity (ESP)
C Data Integrity Only (AH)	
Encryption Algorithm:	3DES 🔽
<u>D</u> ata Integrity	MD5
Compression method:	None
	INGINE .
Allowed Peer Gateway:	
Use Perfect Forward Secreo	
Use DH Group:	Group 1 (768 bit) 🔽
Perform IP Pool NAT	
	Cancel Help

18. Depois que o NG do ponto de verificação estiver configurado, salve a política e selecione **Política > Instalar** para ativá-



A janela de instalação exibe notas de progresso à medida que a política é compilada.



o a janela de instalação indicar que a instalação da diretiva está concluída, clique em **Fechar** para concluir o

 Install Policy

 Standard.W: Security Policy Script generated into Standard.pf

 Standard:

 Compiled OK.

 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

# **Verificar**

Use esta seção para confirmar se a sua configuração funciona corretamente.

### Verificar a comunicação de rede

Para testar a comunicação entre as duas redes privadas, você pode iniciar um ping de uma das redes privadas para a outra rede privada. Nessa configuração, um ping foi enviado do lado de NG do ponto de verificação (10.32.50.51) para a rede do VPN Concentrator (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:\>
```

### Exibir status do túnel no ponto de controle NG

Para visualizar o status do túnel, vá para o Editor de políticas e selecione **Janela > Status do** sistema.

😰 CISCOCP - Check Point System Status						
Ele View Modules Products Tools Window Help						
) 2 🗉 🖂 🛄 🔌 🎫 🇞 🟭 🚅 🎯 😤	<b>₽</b> ?					
Modules IP Address	VPN-1 Details					
	Status:	ок				
E-Ciscocp 172.18.124.157	Packets					
FireWall-1	Encrypted:	19				
FloodGate-1	Decrypted:	18				
Management	Errors					
SVN Foundation	Encryption errors:	0				
ALM-1	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			

## Exibir o status do túnel no VPN Concentrator

Para verificar o status do túnel no VPN Concentrator, vá para Administration > Administer Sessions.

This screen shows st nformation on a sess onnection to a sessi	inister Sessions atistics for sessions. ion, click on that sess on, click <b>Ping</b> .	To refresh the statis sion's name. To log	tics, click Refro out a session, cl	sh. Sel ick Log	ect a Group gout in the tal	Wedness to filter ble belo	day, 11 Sept the sessions w. To test th	ember 2002 20:37 to Reset @ Refresh a. For more he network	
Group [All .ogout All: <u>PPTP U</u> Session Summa	ser   L2TP User   IPS	ec User   L2TP/IPSe	ec User   IPSec/U	JDP Us	er   IPSec/TC	<u>P User</u>	IPSec LAN	-to-LAN	
[		Active	Total Active Peak Concurren Sessions Sessions		Concurrent	t Concurrent Sessions Limit		Total Cumulative Sessions	
Active LAN-to- LAN Sessions	Active Remote Access Sessions	Management Sessions	Sessions	S	essions	Sessio	ons Limit	Sessions	
Active LAN-to- LAN Sessions	Active Remote Access Sessions 0	Management Sessions 3	Sessions 4	S	essions 4	Sessio	ons Limit	Sessions 17	
Active LAN-to- LAN Sessions	Active Remote Access Sessions 0 essions	Management Sessions 3	Sessions 4	S	4 [ Remote Act	Session 1 cess Ses	500 Man	agement Sessions ]	
Active LAN-to- LAN Sessions 1 LAN-to-LAN S Connection Nan	Active Remote Access Sessions 0 essions ne IP Address	Management Sessions 3 Protoco	4 Encr	Syption	4 [ Remote Acc	Sessio	500 Sions   Man	agement Sessions ]	

Em Sessões LAN a LAN, selecione o nome da conexão do Ponto de verificação para ver os detalhes das SAs criadas e o número de pacotes transmitidos/recebidos.

Connection Name IP Ad		iress	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Ro		
heckpoint 172.18.124.1			IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	256		
	Session ID	1	IK	E Session	Encryption Algorith	m 3DES-1	68			
	c 1 10	1	IK	E Session	T	277720 1	60			
Hashing	Algorithm	MDS		_	Diffie Hellman Gray	m Group 2	Group 2 (1024-bit)			
riasining	Algorithm	D. OL	12		Dime-neuman Gro	the cuords a	Main Main			
Authentica	tion Mode	Pre-Sh	ared Keys	1	KE Negotiation Mo	le Main				
Rekey Tin	ie Interval	86400	seconds							
			IPS	ec Session						
	Session ID	2			Remote Addre	ss 10.32.0.	10.32.0.0/0.0.127.255			
	al Address	192.16	8.10.0/0.0.0.255		Encryption Algorith	m 3DES-1	3DES-168			
Loc	at Auturess						1			
Loc Hashing	Algorithm	MD5			SE	P 1				
Loc Hashing Encapsula	Algorithm tion Mode	MD5 Tunnel			SE Rekey Time Interv	P 1 al 28800 s	econds			

# **Troubleshoot**

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

**Observação:** o tráfego não deve ser PATed pelo túnel IPSec usando o endereço IP público do VPN Concentrator (interface externa). Caso contrário, o túnel falhará. Portanto, o endereço IP usado para PATing deve ser um endereço diferente do configurado na interface externa.

### Sumarização de rede

Quando várias redes adjacentes são configuradas no domínio de criptografia no ponto de verificação, o dispositivo pode resumir automaticamente as redes 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, essas redes podem ser resumidas em 10.0.0.0 /23.

### Depurações para ponto de controle NG

Para visualizar os registros, selecione Janela > Visualizador de registros.

a l	ISCOCP - C	heck Poi	int Log Vie	wer - [fv	v.log]			10000								X
Ele	Elle Mode Edit Selection View Iools Window Help													1.1		
60	f / f / Log · 本 A ▼ ± g = 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1											11				
	Date	Time	Product	1949	Inter.	Orig., 1	fype	Action	Source	Destinati	Pr., R	ule	S_Port	SrcKeyID	DstKeyID	×
1	13Aug2002	21:32:	VPN-1	& FireN.	💽 dae	ciscocp	log	0- key instali	ciscoop	CISCO_CONC						
2	13Aug2002	21:32:	VPN-1	& FireW.	🔄 🔄	. ciscocp	log	Ore key instal	ciscocp	CISCO_CONC				0x5879f30d	0xt1351129	
1																

Para habilitar depurações no VPN Concentrator, vá para **Configuration > System > Events > Classes**. Ative AUTH, AUTHDBG, IKE, IKEDBG, IPSEC e IPSECDBG para que a gravidade seja registrada como 1 - 13. Para visualizar as depurações, selecione **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 TOS 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 AUTHDBG/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 = 3000065 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] processing IPSEC SA

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 00000000, 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 SPI 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

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 0000000, 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\_msghdr2secassoc(): 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)

## Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de suporte do IPSec
- <u>Suporte Técnico Cisco Systems</u>