# Configuração de um Túnel IPSec - Cisco VPN 5000 Concentrator to Checkpoint 4.1 Firewall

## Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Conventions Configurar Diagrama de Rede Configurações Checkpoint 4.1 Firewall Verificar Troubleshoot Comandos de Troubleshooting do VPN 5000 Concentrator Sumarização de rede 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. Ele une uma rede privada dentro do Cisco VPN 5000 Concentrator (192.168.1.x) a uma rede privada dentro do Checkpoint 4.1 Firewall (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 de você iniciar essa configuração.

## **Prerequisites**

## **Requirements**

Não existem requisitos específicos para este documento.

## **Componentes Utilizados**

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

- Cisco VPN 5000 Concentrator
- Software Cisco VPN 5000 Concentrator versão 5.2.19.0001
- 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.

## **Conventions**

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

# **Configurar**

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



#### **Configurações**

Este documento utiliza esta configuração.

#### Cisco VPN 5000 Concentrator

[ IP Ethernet 0:0 ] Mode SubnetMask IPAddress	= Routed = 255.255.255.0 = 192.168.1.1
[ General ] EthernetAddress DeviceType ConfiguredOn ConfiguredFrom DeviceName IPSecGateway	<pre>= 00:00:a5:e9:c8:00 = VPN 5002/8 Concentrator = Timeserver not configured = Command Line, from Console = "cisco_endpoint" = 172.18.124.34</pre>
[ IKE Policy ] Protection	= SHA_DES_G2
<pre>[ Tunnel Partner VPN 1 ] KeyLifeSecs LocalAccess Peer BindTo SharedKey KeyManage Transform Partner Mode [ IP VPN 1 ]</pre>	<pre>= 28800 = "192.168.1.0/24" = "10.32.50.0/24" = "ethernet 1:0" = "ciscorules" = Auto = esp(sha,des) = 172.18.124.157 = Main</pre>
Numbered Mode	= Off = Poutod
[ IP Ethernet 1:0 ] IPAddress SubnetMask Mode	= 172.18.124.35 = 255.255.255.240 = Routed
[ IP Static ] 10.32.50.0 255.255.255.0	VPN 1 1
Configuration size is 113	31 out of 65500 bytes.

## **Checkpoint 4.1 Firewall**

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

1. Selecione **Propriedades > Criptografia** para definir as vidas do ponto de verificação IPsec para concordar com o comando **KeyLifeSecs = 28800** VPN Concentrator.**Observação:** deixe a vida útil do IKE (Internet Key Exchange) do ponto de controle no

Properties Setup		
High Availability   IP Pool NAT   Access   Security Policy   Traffic Control   Services   Log Authentication   SYNDefender   LDAP = E	Lists g and Alert incryption	Desktop Security Security Servers ConnectControl
SKIP Enable Exportable SKIP Change SKIP Session Key :	- Manual IF SPI allo	PSEC cation range (hex):
Every 120 Seconds (0 for infinity)	Erom	100
or E⊻ery 10485760 Bytes (0 for infinity)	<u>Ι</u> ο	ffff
Renegotiate IKE Security Associations every       14         Renegotiate IPSEC Security Associations every       28	800	minutes seconds
		1
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 o comando VPN Concentrator **Peer =** 

	Network Properties
	General NAT
	Name: cpinside
	IP Address: 10.32.50.0
	Net <u>M</u> ask: 255.255.255.0
	Color:
	Location:
	Internal O External
"10.32.50.0/24"	OK Cancel Help

3. Selecione Gerenciar > Objetos de rede > Editar para editar o objeto do ponto de extremidade do gateway ("RTPCPVPN" Checkpoint) para o qual o VPN Concentrator aponta no comando Partner = <ip>.Selecione Interno em Local.Selecione Gateway para Tipo.Verifique VPN-1 e FireWall-1 e Management Station em Modules Installed (Módulos

Workstation Properties	×
General Interfaces SNMP NAT Certificates VPN Authe	Þ
Name: RTPCPVPN	
IP Address: 172.18.124.157 Get address	
Comment: Firewalled gateway to internet	
Location:       Type:         ⊙ Internal       ⊆ External         ○ Host       ⊙ Gateway	
Modules Installed VPN-1 & <u>Fi</u> reWall-1 Version: 4.1 <u>Get</u>	
FloodGate-1 Version: 4.1	
Compression Version: 4.1	
Management Station Color:	
OK Cancel Help	

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 o comando LocalAccess = <192.168.1.0/24> VPN

General NAT
<u>N</u> ame: inside_cisco
IP Address: 192.168.1.0 Get address
Net <u>Mask:</u> 255.255.255.0
Color: Color:
Location: Broadcast:
○ Internal ● External ● Allowed ○ Disallowed
OK Cancel Help

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 "externa" do VPN Concentrator com conectividade com o Checkpoint (neste documento, 172.18.124.35 é o endereço IP no comando IPAaddress = <ip>).Selecione Externo em Local. Selecione Gateway para Tipo.Observação: não verifique VPN-1/FireWall-

Workstation Properties	×
General Interfaces SNMP 1	NAT VPN
Name: cisco endpoint	
IP Address: 172.18.124.35	Get address
Location:	– Туре: –
O <u>I</u> nternal ⊙ <u>E</u> xternal	⊂ <u>H</u> ost
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	Color:
	Cancel Help

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) Dither: Exportable for SecuRemote	- Encryption <u>s</u> chemes defined:
Traffic Control Logging	<u>E</u> dit
Ium on Traffic Control Loggin	g
OK Car	ool Holp

7. Altere as propriedades de IKE para a criptografia DES e o hashing SHA1 para concordar com o comando do VPN Concentrator SHA\_DES\_G2.Nota: O "G2" refere-se ao grupo Diffie-Hellman 1 ou 2. No teste, descobriu-se que o Checkpoint aceita "G2" ou "G1".Altere estas configurações:Desative o Modo assertivo.Verifique Suporta Sub-Redes.Marque Pre-Shared Secret em Authentication Method (Método de

General Interfaces SNMP NAT Certificates VPN Authe
KE Properties 📐 🔹 💌
General
Key <u>N</u> egotiation Encryption Method(s): <u>H</u> ash Method:
□ 🖾 3DES 🔽 SHA <u>1</u>
Authentication Method:
Pre-Shared Secret Edit Secrets
Public Key Signatures <u>Configure</u>
Supports Aggresive <u>M</u> ode 🔽 Supports Su <u>b</u> nets
OK Cancel Help
itenticação).

8. Clique em **Editar segredos** para definir a chave pré-compartilhada de acordo com o comando **SharedKey = <key>** VPN

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

#### Concentrator.

 Selecione Gerenciar > Objetos de rede > Editar para editar a guia VPN "cisco\_endpoint". Em Domain, selecione Other e selecione o interior da rede VPN Concentrator (chamada "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
○ Valid 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
 	cel Help

10. Altere as propriedades de IKE para a criptografia DES e o hashing SHA1 para concordar com o comando do VPN Concentrator SHA\_DES\_G2.Nota: O "G2" refere-se ao grupo Diffie-Hellman 1 ou 2. No teste, descobriu-se que o ponto de verificação aceita "G2" ou "G1".Altere estas configurações:Desative o Modo assertivo.Verifique Suporta Sub-Redes.Marque Pre-Shared Secret em Authentication Method (Método de

	General	Interfaces	SNMP NAT	Certificates	VPN	Authe 🔸 🕨	-
	KE Prope	erties 📐					×
	General						
		Key <u>N</u> egotia <b>D</b> S C <b>D</b> S C <b>D</b> S 30	ation Encryption ES AST DES	Method(s): -	Hash M □ M ☑ S	Method: ID <u>5</u> HA <u>1</u>	
	[	Authenticati	ion Method:	Edit	Secrets	1	
		Public	<u>K</u> ey Signatures		nfigure		
	☐ Supports Aggresive <u>M</u> ode						
		ОК	Ca	ncel	Help		
autenticação).							

11. Clique em **Editar segredos** para definir a chave pré-compartilhada de acordo com o comando **SharedKey = <key>** VPN

	IKE Properties	×
	General	
	Shared Secret X	
	Shared Secrets List:	
	Peer Name Shared Secret	
	RTPCFVPN **** <u>E</u> dit	
	Bemove	
	OK Cancel	
		5
	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.

1	RTPO	PVPN - Check P	oint Policy Editor				_ 🗆 🗵
Ē	jie <u>E</u> di	t <u>V</u> iew <u>M</u> anage	Policy Window <u>H</u>	elp			
	- 8	🖪 🔍 👗 🖻	🖻 🚇 😽 🦻	B.   🕫 🗽   🖆	l 🖳 🖀 🖷 🖷	T. 🔫   🖦   🛃	🐻 🎹 🚯
	Secu	urity Policy - Standard	📩 📥 Address Trans	slation - Standard 🛛 😿	Bandwidth Policy - S	tandard	
	No.	Source	Destination	Service	Action	Track	In
ļ	1	🚆 inside_cisco	👷 cpinside 👷 inside_cisco	Any	Encrypt	Long	
l	•						•
F	or Help,	press F1		RTPC	PVPN Rea	d/Write	

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

criptografia.				
rrity Policy - Standard 🛛	Address Translation ·	Standard 🛛 👬 Band	width Policy - Standard	
∼ FVV1 Host	∼ Ldap-Servers	10 Idap	accept	
∼ FW1 Host	∼ Logical-Servers	∼ load_agent	accept	5
nside_cisco	cpinside	Any	dit properties	ng .
		icmp dest-unreach	Edit Encryption	
		icmp echo-request	accept	am .
		icmp info-reply	drop	
	Any	icmp mask-reply	🚺 😑 reject	
4				•

14. Selecione IKE e clique em

E	Encryption Properties	×
	General Encryption schemes defined:	
ditar	OK Cancel Help	

15. Na janela Propriedades de IKE, altere essas propriedades para concordar com o comando Transform = esp(sha,des) VPN Concentrator.Em Transform, selecione Encryption + Data Integrity (ESP). O algoritmo de criptografia deve ser DES, a integridade dos dados deve ser SHA1, e o gateway de peer permitido deve ser o gateway do VPN Concentrator externo (chamado "cisco\_endpoint"). Click

m: ption + Data Integrity (ESP) Integrity Only (AH)
n Algorithm: DES
grity SHA1 💌
eer Gateway:
Perfect Forward Secrecy
Perfect Forward Secrecy

16. 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**

## Comandos de Troubleshooting do VPN 5000 Concentrator

A <u>Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados</u> <u>comandos show.</u> Use a OIT para exibir uma análise da saída do comando show.

# Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- vpn trace dump all Mostra informações sobre todas as conexões VPN correspondentes, incluindo informações sobre a hora, o número VPN, o endereço IP real do peer, quais scripts foram executados e, em caso de erro, o número de linha e de rotina do código de software em que ocorreu o erro.
- show system log buffer Mostra o conteúdo do buffer de log interno.
- show vpn statistics Mostra essas informações para usuários, parceiros e o total para ambos. (Para modelos modulares, a tela inclui uma seção para cada slot de módulo. Consulte a seção <u>Exemplo de Saída de Depuração</u>.)Ativo Atual As conexões ativas atuais.<sub>Em Negot</sub> As conexões em negociação no momento.<sub>High Water</sub> O maior número de conexões ativas simultâneas desde a última reinicialização.<sub>Total</sub> em execução O número de total de conexões bem-sucedidas desde a última reinicialização.<sub>Túnel</sub> ok O número de túneis para os quais não houve erros.<sub>Túnel</sub> é iniciado O número de túneis é iniciado.<sub>Erro</sub> de túnel O número de túneis com erros.
- show vpn statistics verbose Mostra as estatísticas de negociação de ISAKMP e muitas outras estatísticas de conexão ativas.

### 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 Checkpoint 4.1 Firewall

Esta foi uma instalação do Microsoft Windows NT. Como o rastreamento foi definido como Longo na janela do Editor de políticas (conforme visto na <u>Etapa 12</u>), o tráfego negado deve aparecer em vermelho no Visualizador de registros. Uma depuração mais detalhada pode ser obtida por:

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 as Associações de Segurança (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_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
   new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing 121p_do_negotiation, (0 @ 0)
   new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing 121p_start_phase_2, (0 @ 0)
   new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing 121p_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
```

#### cisco\_endpoint#**show vpn stat**

	Current	In	High	Running	Tunnel	Tunnel	Tunnel
	Active	Negot	Water	Total	Starts	OK	Error
Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0

#### IOP slot 1:

	Current	In	High	Running	Tunnel	Tunnel	Tunnel
	Active	Negot	Water	Total	Starts	OK	Error
Users	0	0	0	0	0	0	0
Partners	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0

#### cisco\_endpoint#**show vpn stat verb**

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0

Stats	VPN0:1
Wrapped	13
Unwrapped	9
BadEncap	0
BadAuth	0
BadEncrypt	0
rx IP	9
rx IPX	0
rx Other	0
tx IP	13
tx IPX	0
tx Other	0
IKE rekey	0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries:  $\ensuremath{\textbf{0}}$ 

ISAKMP Negotiation stats	5
Admin packets in	4
Fastswitch packets in	0
No cookie found	0
Can't insert cookie	0
Inserted cookie(L)	1
Inserted cookie(R)	0
Cookie not inserted(L)	0
Cookie not inserted(R)	0
Cookie conn changed	0
Cookie already inserted	0
Deleted cookie(L)	0
Deleted cookie(R)	0
Cookie not deleted(L)	0
Cookie not deleted(R)	0
Forwarded to RP	0
Forwarded to IOP	0
Bad UDP checksum	0
Not fastswitched	0
Bad Initiator cookie	0
Bad Responder cookie	0
Has Responder cookie	0
No Responder cookie	0
No SA	0
Bad find conn	0
Admin queue full	0
Priority queue full	0
Bad IKE packet	0

No memory	0
Bad Admin Put	0
IKE pkt dropped	0
No UDP PBuf	0
No Manager	0
Mgr w/ no cookie	0
Cookie Scavenge Add	1
Cookie Scavenge Rem	0
Cookie Scavenged	0
Cookie has mgr err	0
New conn limited	0

IOP slot 1:

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0
Stats							
Wrapped							
Unwrapped	L						
BadEncap							
BadAuth							
BadEncryp	t						
rx IP							
rx IPX							
rx Other							
tx IP							
ty Other							
IKE rekev							
1112 101101							
Input VPN	pkts dro	pped due	to no SA	: 0			
Input VPN	pkts dro	pped due	to no fr	ee queue e	entries: (	)	
ISAKMP Ne	gotiation	stats					
Admin pac	kets in	0					
Fastswitc	h packets	in 3					
No cookie	found	0					
Can't ins	ert cooki	.e 0					
Inserted	cookie(L)	0					
Inserted	cookie(R)	1					
Cookie no	t inserte	ed(L) 0					
Cookie no	t inserte	ed(R) U					
Cookie co	nn change						
COOKIE al	ready ins	serled U					
Deleted d	ookie(L)	0					
Cookie no	t deleted	U(T.) 0					
Cookie no	t deleted	$I(\mathbf{R}) = 0$					
Forwarded	to RP	0					
Forwarded	to TOP	° 3					
Bad UDP c	hecksum	0					
Not fasts	witched	0					
Bad Initi	ator cook	tie 0					
Bad Respo	nder cook	ie O					
Has Respo	nder cook	ie O					
No Respon	der cooki	.e 0					
No SA		0					
Bad find	conn	0					

Admin queue full	0
Priority queue full	0
Bad IKE packet	0
No memory	0
Bad Admin Put	0
IKE pkt dropped	0
No UDP PBuf	0
No Manager	0
Mgr w/ no cookie	0
Cookie Scavenge Add	1
Cookie Scavenge Rem	0
Cookie Scavenged	0
Cookie has mgr err	0
New conn limited	0
	0

# Informações Relacionadas

- Anúncio do fim do ciclo de comercialização dos concentradores Cisco VPN 5000 Series
- <u>Negociação IPsec/Protocolos IKE</u>
- <u>Suporte Técnico e Documentação Cisco Systems</u>