Túnel IPsec LAN a LAN entre um Cisco VPN 3000 Concentrator e um roteador com exemplo de configuração AES

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados Conventions** Configurar Diagrama de Rede Configurações **Configurar o VPN Concentrator** Verificar Verifique a configuração do roteador Verifique a configuração do VPN Concentrator **Troubleshoot** Solucionar problemas do roteador Solucionar problemas do VPN Concentrator Informações Relacionadas

Introduction

Este documento mostra como configurar um túnel de IPsec entre um concentrador Cisco VPN 3000 e um roteador Cisco com padrão de codificação avançado (AES) como o algoritmo de criptografia.

O AES é uma nova publicação do Federal Information Processing Standard (FIPS) criada pelo National Institute of Standards and Technology (NIST) para ser usada como método de criptografia. Este padrão especifica um algoritmo de criptografia simétrica AES que substitui o DES (Data Encryption Standard, Padrão de Criptografia de Dados) como uma transformação de privacidade para IPsec e Internet Key Exchange (IKE). O AES tem três comprimentos de chave diferentes, uma chave de 128 bits (o padrão), uma chave de 192 bits e uma chave de 256 bits. O recurso AES no Cisco IOS® adiciona suporte para o novo padrão de criptografia AES, com CBC (Cipher Block Chaining, encadeamento de bloco de cifra) modo, ao IPsec.

Consulte o <u>site NIST Computer Security Resource Center</u> para obter mais informações sobre AES.

Consulte Túnel IPsec LAN a LAN entre o Cisco VPN 3000 Concentrator e o PIX Firewall Exemplo

para obter mais informações sobre a configuração do túnel LAN a LAN entre um VPN 3000 Concentrator e o PIX Firewall.

Consulte o <u>Exemplo de Configuração de Túnel IPsec Entre PIX 7.x e VPN 3000 Concentrator</u> para obter mais informações quando o PIX tem a versão de software 7.1.

Prerequisites

Requirements

Este documento requer uma compreensão básica do protocolo de IPSec. Consulte <u>Uma</u> <u>Introdução à Criptografia IPSec</u> para saber mais sobre o IPsec.

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Requisitos do roteador O recurso AES foi introduzido no Cisco IOS Software Release 12.2(13)T. Para habilitar o AES, seu roteador deve suportar IPsec e executar uma imagem do IOS com "k9" longas keys (o subsistema "k9").Observação: o suporte de hardware para AES também está disponível nos módulos VPN de aceleração AES Cisco 2600XM, 2691, 3725 e 3745. Este recurso não tem implicações de configuração e o módulo de hardware é selecionado automaticamente se ambos estiverem disponíveis.
- Requisitos do VPN Concentrator O suporte de software para o recurso AES foi introduzido na versão 3.6. O suporte de hardware é fornecido pelo novo processador de criptografia aprimorado e escalável (SEP-E). Este recurso não tem implicações de configuração.Observação: no Cisco VPN 3000 Concentrator versão 3.6.3, os túneis não negociam com AES devido à ID de bug da Cisco <u>CSCdy88797</u> (somente clientes <u>registrados</u>)
 . Isso foi resolvido na versão 3.6.4.Observação: o Cisco VPN 3000 Concentrator usa módulos SEP ou SEP-E, não ambos. Não instale ambos no mesmo dispositivo. Se você instalar um módulo SEP-E em um VPN Concentrator que já contenha um módulo SEP, o VPN Concentrator desabilitará o módulo SEP e usará somente o módulo SEP-E.

Componentes Utilizados

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

- Cisco 3600 Series Router com Cisco IOS Software Release 12.3(5)
- Cisco VPN 3060 Concentrator com Software Release 4.0.3

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</u> <u>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 nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Roteador IPsec
- <u>Concentrador de VPN</u>

Configuração do ipsec_router				
version 12.3				
service timestamps debug uptime				
service timestamps log datetime msec				
no service password-encryption				
!				
hostname ipsec_router				
!				
memory-size iomem 10				
no aaa new-model				
ip subnet-zero				
1				

```
!--- Configuration for IKE policies. crypto isakmp
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
I
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
```

```
configuration exempts !--- the LAN-to-LAN traffic from
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

Observação: embora a sintaxe da ACL seja inalterada, os significados são ligeiramente diferentes para ACLs criptografadas. Em ACLs criptografadas, **permit** especifica que os pacotes correspondentes devem ser criptografados, enquanto **deny** especifica que os pacotes correspondentes não precisam ser criptografados.

Configurar o VPN Concentrator

Os VPN Concentrators não são pré-programados com endereços IP em suas configurações de fábrica. Você precisa usar a porta de console para configurar as configurações iniciais que são uma interface de linha de comando (CLI) baseada em menu. Consulte <u>Configurando</u> <u>Concentradores VPN através do Console</u> para obter informações sobre como configurar através do console.

Depois que o endereço IP na interface Ethernet 1 (privada) é configurado, o restante pode ser configurado usando a CLI ou através da interface do navegador. A interface do navegador suporta HTTP e HTTP sobre SSL (Secure Socket Layer).

Esses parâmetros são configurados através do console:

- Hora/Data A hora e a data corretas são muito importantes. Eles ajudam a garantir que os registros e registros contabilísticos sejam precisos e que o sistema possa criar um certificado de segurança válido.
- Interface Ethernet 1 (privada) O endereço IP e a máscara (da nossa topologia de rede 172.16.1.1/24).

Neste ponto, o VPN Concentrator é acessível por meio de um navegador HTML da rede interna. Para obter informações sobre como configurar o VPN Concentrator no modo CLI, consulte <u>Configuração rápida usando CLI</u>.

 Digite o endereço IP da interface privada a partir do navegador da Web para ativar a interface GUI.Clique no ícone save required para salvar as alterações na memória. O nome de usuário e a senha padrão de fábrica são "admin", que diferencia maiúsculas de minúsculas.

	VPN 3000	Main Help Support Logout
	Concentrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
⊞Conflouration ∰Administration ∰Manifarina	Main Welcome to the VFN 3000 Concentrator Manager. In the left frame or the analyzitich burdway, click the function you want • Configuration - to configure all flattance of this davine. • Montoning - to configure all flattance of this davine. • Montoning - to reacted administrative functions on this davine. • Montoning - to view status, statistics, and logs on this davine. The base at the top right has: • Montoning - to serve status, statistics, and logs on this device. The base at the top right has: • Montoning - to serve status, statistics, and logs on this device. • Main - to neture to this screen • Montoning - to serve status, statistics, and logs on this device. • Montoning - to serve status, statistics for support and documentation. • Montoning - to serve status, statistics for support and documentation. • Montoning - to serve status, statistics for support and documentation. • Lagont - to log out of this screen and return to the Monager logits screen. Under the location bar in the upper right, there icons may appear. Click to: • Serve in serve the active configuration and make it the boot configuration. • Serve in screen is active configuration and make it the boot configuration. • Serve is active configuration and make it the boot configuration. • Reacter - to requerely ne	

2. Depois de exibir a GUI, selecione **Configuration > Interfaces > Ethernet 2 (Public)** para configurar a interface Ethernet

2.						
Configuration	nfigu	uration Interfaces	: Ethernet 2			
EPUiser Management Com	Configuring Ethernet Interface 2 (Public).					
Administration Ge	enera	al RIP OSPF B	andwidth			
			Gener	ral Parameters		
Se	el	Attribute	Value		Description	
	ΩĽ	Disabled			Select to disable this interface.	
	сı	DHCP Client			Select to obtain the IP Address, Subnet Mask and Default Geteway via DHCP.	
	© 8	Static IP Addressing			Salash in and Gauss the 1D Address and Salash Mark	
		IP Address	20.20.20.1		Eater the IP Address and Subnet Mask for this	
		Subnet Mask	255.255.255.0		interface.	
		Public Interface	ic Interface 🔽		Check to make this interface a "publis" interface.	
		MAC Address	AC Address 00.90 A4.00.41 F9		The MAC address for this interface.	
	Filter 2. Public (Default)		•	Select the filter for this interface.		
		Speed	10/100 auto 💌		Select the speed for this interface.	
		Duplex	Auto 💌		Select the duplex mode for this interface.	
	мпе		1500		Enter the Maximum Transmit Unit for this interface (68 - 1500).	
	_		C Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission		agment prior to interface transmission	
	Public Interface IPSec		C Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)			
			C Fragment prior to IPSec enc	opsulation without P	ath MTU Discovery (Clear DF bit)	
Cisco Systems	Арр	dy Cancel				

 Selecione Configuration > System > IP Routing > Default Gateways configure o gateway padrão (Internet) e o gateway padrão de túnel (interno) para IPsec para acessar as outras sub-redes na rede privada.Neste cenário, há apenas uma sub-rede disponível na rede interna.

Configuration		
	Configuration System IP Routing De	fault Gateways
- (FSystem		
- Bervers	Configue the default gateways for your system.	
	n a 1 n	
- G-P Routing	Default Gateway 20.20.20.2	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.
Static Routes	Mateia 1	Enter the metric form 1 to 16
Default Gateways	Method 1	Ealer die metho, from 1 to 10.
OSPF	Tunnel Default 172 16 1 2	Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no
OSPF Areas	Gateway Control 10	default router.
<u>OHCP Parameters</u>	Override Default	Check to allow leaved default extension to convide the confirmed default extension
OHCP Relay	Gateway	CHER IS HOW BEINES GENER SHEWEYS IS SVEITHE THE CONSUMES GENER. SHEWEY.
Reduncionary	Apply Canaal	
Reverse Route Injection	Apply Concer	
- III- <u>Management Protocols</u>		
- E-Events		
General		
- Elebal trial - Elebal		
Load Balancing		
Huser Management		
+++Administration		

4. Selecione Configuration > Policy Management > Traffic Management > Network Lists > Add para criar as listas de rede que definem o tráfego a ser criptografado.As redes mencionadas na lista podem ser acessadas à rede remota. As redes mostradas na lista abaixo são redes locais. Você também pode gerar a lista de redes locais automaticamente via RIP quando clica em Gerar lista

ocal.				
-Configuration				
	configuration	n Policy Management Tra	ffic Manageme	nt Network Lists Modify
- T System				
- E-User Management [M	lodify a configu	ured Network List. Click on Genera	te Local List to gen	erate a network list based on routing entries on the Private interface.
Policy Management	_			
Access Hours	Läst Name	von local network		Name of the Network List you are adding. The name must be unious.
Network Lists		<pre>cpm_noca_motivoint</pre>		······································
Rules	1	172.16.0.0/0.0.255.255	*	. Eater the Networks and Wildcard masks using the following
SAS	T			format: n.n.n/n.n.n (e.g. 10.10.0.00.0.253.255).
Filters				Note: Enter a wildcard mask, which is the reverse of a
- ENAT				subnet mask. A widecard mask has is mult positions to
BAY Policies	a transfer List			10.10.100.0.0255 = all 10.10.1 yes addresses.
Group Matching	CEMPTH LIST			 Each Network and Wildcard mask pair must be entered on a
-Administration				single line.
Monitoring				 The Wildcard mask may be omitted if the natural Wildcard
			-	mask is to be used.
		4		
	Apply	Concel Generate	Lacal List	
Horsessen Hanagement Hanagement Geolegy Management Herseshors Horseshors Horseshor	List Name	wed Network List. Click on Genera vpn_local_network 172, 16, 0, 0/0, 0, 255, 255	te Local List to gen	 wrate a network list based on routing entries on the Private into Name of the Network List you are adding. The name must b Eater the Networks and Wildrard masks using the fifthermet: n.n.r.ndn.n.m.n (e.g. 10.100.000.255.225) Note: Enter a wildcard mask, which is the reven submet mask. A wildcard mask, no is in bit position ignore, 0s in bit positions to match. For example, 10.10.100.00.255 all 10.10.10.10 mas addresses. Each Network and Wildcard mask, pair must be ente single line. The Wildcard mask may be consisted if the natural W mask is to be used.

5. As redes nesta lista são redes remotas e precisam ser configuradas manualmente. Para fazer isso, insira a rede/curinga de cada sub-rede

alcançável.	Configuration Modify a configu	n : Policy Management Trai	fic Management Network Lists Modify e Local List to generate a network list based on routing entries on the Private interface.
Access Hours Tratic Management Galess Galess	List Name (/pn_remote_network	 Name of the Network List you are adding. The name must be unique. Enter the Networks and Whileard masks using the following format: mann/mann (e.g. 10.10.0.00.0.255.253). Note: Enter a widecard mask, which is the reverse of a subnet mask. A widecard mask, and widecard mask, and the in bit positions to group. Os in bit positions to metch. For example, 10.10.1.000.0.255 - all 10.10.1 are addresses. Each Network and Wildowsh must be omitted if the natural Wildowsh mask to be used.
	Apply	Cancel Generate L	ocel List

Quando concluídas, estas são as duas listas de rede:

E)Configuration	Configuration Policy Management Traffic Management Network Lists	
GR <u>System</u> 	Save 🔜 This section lets you add, modify, copy, and delete Network Lists Click Add to create a Network List, or select a Network List and click Modify, Copy, or Delete. 	
Ellers O'Al D'Administration O'MonKoring	VPN Client Local LAN (Default) Vgn_remote_network Vpn_local_network Modity Copy Delete	

6. Selecione Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add e defina o túnel LAN-to-LAN.Esta janela tem três seções. A seção superior é para as informações de rede e as duas seções inferiores são para as listas de rede local e remota. Na seção Network Information (Informações da rede), selecione a criptografia AES, o tipo de autenticação, a proposta IKE e digite a chave pré-compartilhada. Nas seções inferiores, aponte para as listas de rede que você já criou, as listas Local e Remota, respectivamente.

- 				
	Configuration System Tunneling Protocols IPSec LAN-to-LAN Add			
- (#Servers	Add a new IPSec LAN-to-LAN connection			
 Address: Management 				
-CHTunnelino Protocols 	Enable 🗹	Check to enable this LAN-to-LAN connection.		
	Name test	Enter the name for this LAN-to-LAN connection.		
LANIto LAN	Interfare Ethernet 2 (Public) (20.20.20.1)	Select the interface for this LAN-to-LAN connection.		
<u>IKE Proceede</u> <u>NAT Transparency</u>	Connection Type Bi-directional	Choose the type of LAN to LAN connection. An $Originalo \ Only connection may have multiple peers specified below.$		
General G	50.30.30.1 ···	Enter the remote peer IP addresses for this LAN-to-LAN connection. Originate- Oxly connection may specify up to ten peer IP addresses. Boler one IP address per line.		
	Digini Narie (Use Preshared Keys) 💌	Select the digital certificate to use.		
-31 <u>Monitorina</u>	Certificate C Entire certificate chain. Transmission © Identity certificate only	Choose how to send the signal certificate to the DCE poor.		
	Preshared Key cisco123	Enter the prechared key for this LAN to LAN connection.		
	Authentication ESP/MD5/HMAC-128 -	Specify the packet authentication mechanism to use.		
Cisco Systems	Encryption AES-256 -	Specify the encryption mechanism to use.		
adhoadhoa	IKE Proposal KE-AES256-SHA	Select the IKE Proposal to use for this LAN-to-LAN connection.		

- Denfiguration Interfaces 		
- E-Servers		
- E-Address Management		
- E- <u>Tunneling Protocols</u>		
	Filter -None-	Choose the filter to apply to the traffic that is transled through this LAN-to-LAN
		convection.
<u></u>		Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN
Lonso Lon	IPSer NAT-T	rearer time through a NAT device. You must also enable IPSec over NAT-T under
MAT Transporter		NAT Transparency.
6 keeks	Bandwidth Policy -None-	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Walk to		Change the resting rescharging to use Personation helper are innered if Network
- Wanage pent Protocols	Rowting None	Autodisenvery is chosen.
- Exercise - Foreign - For		
-ff-General	Local Neurark: If a L6N-to-LAN N&T rule is used. Dis is the Transla	ted Network oddress
- El-Cient Update		Coordinates and antisent address for so the ID address and address aces. So this
Load Balancing	Network List vpn_local_network	[AN.to.] AN opposition
- Tolicy Management	IP Address	Note: Enter a wildcard mark, which is the ownerse of a submet mark. A
Access Hours		wildrand mask has 1s in bit positions to imore. Us in hit positions to match. For
- E-Traffic Management	Wildcard Mask	szaruple, 10.10.1.000.0.0.255 = all 10.10.1 nrn addresses.
- E-Group Matching		
-33 <u>Administration</u>	Remote Network: If a LAN-to-LAN NAT rule is used, this is the Rem	ote Network address.
- Monitoring		Specify the remote network address list or the IP address and wildcard mask for
	Memory Last wpn_remote_network	this LAN-to-LAN connection.
	IP ildrer	
	n onnese	Note: Enter a wildowd mask, which is the reverse of a subnet mask. A
	Wildcaml Mask	wildcard mark has 1s in bit positions to ignore, 0s in bit positions to match. For
0		ransple, 10.10.1.00.0.0.255 = all 10.10.1 ann adáresses.
CISCO SPETEMS	Add Contel	
million and in the second		

7. Depois de clicar em Adicionar, se sua conexão estiver correta, você verá a janela Add-Done de LAN para LAN do IPSec.Essa janela apresenta uma sinopse das informações de configuração do túnel. Ele também configura automaticamente o nome do grupo, o nome SA e o nome do filtro. Você pode editar qualquer parâmetro nesta

tabela.	
Configuration	
	Configuration System Tunneling Protocols IPSec LAN to LAN Add Done
- Er <u>Systen</u>	Save Needed
- (3)-Address Management	An IPSet LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:
EPTP.	And an electric former lateral
L2TP	Auteenbrauen Serrer Institu
L –⊖ <u>PSeo</u>	Group 2020/2011
LANHO-LAN	Security Association 1.2.: test
KE Processis	where Parls 12L test Out
NAT Transparency	Plater Assess 1.22. test In
<u>eVerts</u>	
- It P Routing	Modifying any officers will effect the LAN-to-LAN configuration. The Grean is the same as your LAN-to-LAN rate. The Security Association and
	Filter Rules of start with "L2Ls" to indicate that they form a LAN-to-LAN configuration.
- CHEVarda	
- GK <u>General</u>	or (
- Client Update	
Load Balancing	
- E-User Management	
EPolicy Management	
Administration	
Monitoring	

Neste ponto, o túnel de LAN para LAN do IPsec foi configurado e você pode começar a trabalhar. Se, por algum motivo, o túnel não funcionar, você poderá verificar se há configurações incorretas.

8. Você pode visualizar ou modificar os parâmetros de IPsec LAN a LAN criados anteriormente ao selecionar Configuração > Sistema > Protocolos de tunelamento > IPSec LAN a LAN.Este gráfico mostra "teste" como o nome do túnel e a interface pública da extremidade remota é 30.30.30.1 conforme o cenário.

- Configuration					
	Configuration System	Tunneling Protocols IPSec LAN-to-LAN			
- G-System			Save		
- DServers					
	This section late you configure I	ESse LAN-to-LAN connections LAN-to-LAN connections are set	shlished with other VPN 3000 Concentrators		
	PIX frewalls, 7100/4000 series	The second set of the second second second second responses to configure a VEN 2002 and the mode access			
EPTP.	connection, go to User Managen	nent and configure a Group and User. To configure NAT over LAN	-to-LAN, go to LAN-to-LAN NAT Rules.		
L2TP		_ , , ,			
- EHEZeo	If you want to define a set of us	tworks on the local or remote side of the LAN-to-LAN connection.	configure the necessary Network Lists prior		
LAN-to-LAN	to creating the connection.				
IKE Proposals	5				
NAT Transparancy	Click the Add button to add a L $$	AN-to-LAN connection, or select a connection and click Modify or	Delete.		
<u>Alerts</u>		· · · ·			
- Cetter Mouting	(D) indicates a disabled LAN-to	LAN connection.			
HHManagement Protocols					
TE Case and		LAN-to-LAN			
		Connection	Actions		
L and Balancing		et /20 20 20 1) av Ethewaet 2 (Dublic)]]			
- All ber Management		st (30.30.30.1) on zenernet z (Public)			
GPolicy Management			Add		
Access Hours					
- Tratile Management			Modify		
Network Lists			Delete		
Rules			Delete		
<u>SAs</u>					
-EHAI					
E)V Policies					
- (1) Group Metching					
Administration					
-ta- <u>monicoring</u>					

9. Às vezes, seu túnel pode não aparecer se sua proposta de IKE estiver na lista de propostas inativas. Selecione Configuração > Sistema > Protocolos de tunelamento > IPSec > Propostas IKE para configurar a proposta IKE ativa.Se sua proposta de IKE estiver na lista "Propostas inativas", você poderá ativá-la quando selecionar a proposta de IKE e clicar no botão Ativar. Neste gráfico, a proposta selecionada "IKE-AES256-SHA" está na lista de propostas



 Selecione Configuration > Policy Management > Traffic Management > Security Associations para verificar se os parâmetros SA estão corretos.

다. GConfiguration		
	Configuration Policy Management Traffic Management Security Association	ons
		Save
- EServers		
- El-Address Management	This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security if	Associations use <u>IRE Proposals</u> to negotiate IRE
PPTP	parameters.	v
	Click Add to add an SA, or select an SA and click Modify or Delete.	
LAN-ID-LAN KE Protocols	IPSec SAs Artions	
NAT Transparency	ESP-3DES-MD5	
Alerts	ESP-3DES-MD5-DH5	
- EHP Routing	ESP-3DES-MD5-DH7	1
FHManagement Protocols	ESP-3DES-NONE Add	
EPEvents	ESP-AES128-SHA	_
- D General	ESP-DES-MD5 Modity	
- Elient Update	ESPI-2TP-TRANSPORT Delate	
Load Balancing	ESP/KE-3DES-MD5	
- ERUser Management	L2L:test	
Policy Management		
Access Hours		
-EFIraffic Management		
Network Lists		
- Foulies		
- E-NAT		
BAY Policies		
Group Matching		
- Administration		
Monitoring		
(@Monitoring		

11. Clique no nome SA (neste caso, L2L: teste) e clique em Modificar para verificar as SAs.Se algum dos parâmetros não corresponder à configuração de peer remoto, ele poderá ser alterado

ลด	U	L
~ 9	~	•••

D Conformation	Conferencies I Deline Management I Tariffe Manageme	and Convite Americation (Madife			
E configuration	Configuration Policy Management Traffic Management Security Associations Modify				
- Feystein	Modify a configured Security Association				
EDServers					
Address Management	P 4 Marca I (Calendar	Consider the survey of this Consultant because in the ACA (
	SA Phane LZL 1981	specify the name of this sectionly Association (Sec).			
ELE CELE	Inheritance From Bula	Select the consularity of this SA			
91121-		a check the generation of the second			
- CHPSec					
LAN-ID-LAN	IPSec Parameters				
HE Proposals	Authentication ERD/ADD/HMAC-128	School the second standing time in a second terms			
	Algorithm	anset us peaks substitueion aground to use.			
<u>Alerts</u>	Formation Algorithm AFS, 255	Select the VSE accountion elementhes to use			
- DP Routing	HESTER I	and the say point againer to see.			
EP-Management Protocols	Encapsulation Mode Tunnel 💌	Select the Encapsulation Mode for this SA.			
- Events	Perfect Forward				
- El-General	Serrer Disabled	Salect the use of Profect Forward Secrecy.			
- Elent Update	10.000				
Losd Balancing	Time •	Select the lifetime measurement of the IPSec keys.			
	Australian				
- Policy Management	Data Lifetime 10000	Specify the data lifetime in kilobytes (ICB).			
Access Hours					
- DTraffic Management	Time Lifetime 28800	Specify the time lifetime in seconds.			
Network Lists					
	IKE Parameters				
<u></u>	Connection Two Bidaceticael	The Converties Trees and UEE Descentions are dified as 195 of 5 h that is read of			
Elbers	Connection 1 pper connection in	a local section in the section of th			
GRAT	IKE PEER SU SU SU	a England Constantion.			
EX/Policies	Negatiation Mode Main	Select the IKE Negotiation mode to use.			
- El-Group Matching	Divised Contificate Diano (Los Deach aread Kerse)	Salant das Thinksl Cashiffants de con			
Administration	Dignal Centukale (None (Ose Presnared Neys)	Select the English Certificate to use.			
Monitoring	Certificate 🗢 Entire certificate chain				
	Transmission & Identify and State	Choose how to send the digital cartificate to the IKE peer.			
	 Identity centrate only 				
	IKE Proposal IKE AES256 SHA	 Select the IKE Proposal to use as IKE initiator. 			
Cisco Systems					
de de	Apply Concel				
at the second second second					

Verificar

Verifique a configuração do roteador

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

A <u>Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados</u> <u>comandos show, o que permite exibir uma análise da saída do comando show.</u>

 show crypto isakmp sa — Exibe todas as SAs IKE atuais em um peer. O estado QM_IDLE indica que o SA permanece autenticado com seu par e pode ser usado para trocas de modo rápido subsequentes. Está em um estado silencioso. ipsec_router#show crypto isakmp sa

dst src state conn-id slot 20.20.20.1 30.30.1 **QM IDLE** 1 0

 show crypto ipsec sa —Exibe as configurações usadas pelas SAs atuais. Verifique os endereços IP dos pares, as redes acessíveis nas extremidades local e remota e o conjunto de transformações usado. Há duas SAs ESP, uma em cada direção. Como os conjuntos de transformação AH são usados, ele está vazio.
 ipsec_router#show crypto ipsec sa

```
interface: Ethernet1/0
```

Crypto map tag: vpn, local addr. 30.30.30.1

protected vrf:

```
local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
```

remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

current_peer: 20.20.20.1:500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145

#pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 6, #recv errors 0

local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1

path mtu 1500, media mtu 1500

current outbound spi: 54FA9805

inbound esp sas:

spi: 0x4091292(67703442)

transform: esp-256-aes esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn

sa timing: remaining key lifetime (k/sec): (4471883/28110)

```
IV size: 16 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x54FA9805(1425709061)
transform: esp-256-aes esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4471883/28110)
IV size: 16 bytes
replay detection support: Y
outbound ah sas:
```

outbound pcp sas:

 show crypto engine connections ative — Exibe as conexões de sessão criptografada ativas atuais para todos os mecanismos de criptografia. Cada ID de conexão é exclusiva. O número de pacotes criptografados e descriptografados é exibido nas duas últimas colunas. ipsec_router#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	Ethernet1/0	30.30.30.1	set	HMAC_SHA+AES_256_C	. 0	0
2000	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	. 0	19
2001	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	19	0

Verifique a configuração do VPN Concentrator

Conclua estes passos para verificar a configuração do VPN Concentrator.

 Semelhante aos comandos show crypto ipsec sa e show crypto isakmp sa nos roteadores, você pode exibir as estatísticas de IPsec e IKE quando seleciona Monitoring > Statistics > IPSec nos VPN Concentrators.

-=- <u>Configuration</u>	Monitoring Statistics IPSec Thursday,	U1 Ja	inuary 2004 19:32:36
ElStaten			Reset 🥔 Refresh 🔞
-FiUser Management	IKE (Phase 1) Statistics IPSec (Phase 2) Statistics		
EPfolicy Management	Active Tunnels 1 Active Tunnels	l	
Access Hours	Total Tunnels 2 Total Tunnels	2	
Network Lists	Received Bytes 3545260 Received Bytes	3632	
Bulez	Sent Bytes 5553204 Sent Bytes	5376	
<u>SAs</u>	Received Packets 60187 Received Packets	145	
Eller2	Sent Packets 60299 Sent Packets	-51	
Bit Policies	Received Parkets Dropped 0 Received Parkets Dropped	0	
Group Matching	Sent Parkets Dropped O Received Parkets Dropped (Anti-Replay)	0	
	Received Notifies 60084 Sent Packets Dropped	0	
-ErSoftware Undete	Sent Notifies 120172 Inhound Authentirations	145	
Concentrator	Received Phase-2 Eachanges 2 Failed Inbound Authentications	0	
Clients Surface Robert	Sent Phase-2 Exchanges 45 Outhound Authentirations	St	
	Invalid Phase-2 Exchanges Received 0 Failed Outbound Authentications	0	
Eina	Invalid Phase 2 Exchanges Sent 0 Decryptions	145	
Monitoring Refresh	Bejerted Received Phase-2 Exchanges 0 Failed Derryptions	0	
- DF is Management	Rejected Sent Phase-2 Exchanges 0 Encryptions	-51	
Swap Config File	Phase-2 SA Delete Requests Received 0 Failed Encryptions	0	
TFTP Transfor	Phase-2 SA Delete Requests Sent 30 System Capability Failures	0	
XM_ Export	Initiated Tunnels 0 No. SA Failures	0	
EPCertificate Management	Failed indifated Tunnels 0 Protocol Use Failures	0	
Enroliment	Failed Benute Tunnels 0		
	Authentization Failures 0		
	Decryption Failures 0		
Dynamic Filters	Hash Validation Failures 0		
Cisco Systems	System Capability Failures 0		
thusthus	No-SA Failures 0		

2. Semelhante ao comando **show crypto engine connections ative** em roteadores, você pode usar a janela Administration-Sessions no VPN Concentrator para exibir os parâmetros e as estatísticas de todas as conexões LAN para LAN IPsec ativas ou

tuneis.											
Configuration Interfaces: FrSysten	Administration Ad	iminister Ses	sions					Thursday	, 01 Janu R	uary 2004-19:30:20 eset 🖉 Refresh®	
Characterial Characteriant Characte	This error shows statis on that session's name. T Group —AII- Legout AII: <u>PPTP User</u> Session Summary	tice for sessions. To log out a session (1277 User 127	To refiech the stati or, click Legent in Sec User <u>IPSec LA</u>	stios, click R the table belo <u>N-to-LAN</u>	efnesik, Sel w. To test	ect a Group b the astwork o	a filter the se canection to	ssions. For n a seasion, chi	tore informe its Ping ,	rtion on a session, clici	
BN Policies 	Active LAN-to- LAN Sessions	Active Remot Access Sessio	e Active Man Is Sessie	igement	Fotal Activ Sessions	e Peak C	oncurrent ssions	Conrus	vent Limit	Total Cumulative Sessions	
Administer Sessions	1	0	0 1		2 3		3	4000		19	
Concentrator Clientz System Reboot	LAN-10-LAN Sessio	115					[Rea	cte Access S	essions Mi	unegement Sessions]	
Reboot Status	Connection Name	IP Address	Protocol	Encry	tion L	agin Tinus	Duration	Bynes Tx	Byles Rx	Actions	
Hins Honitorina Setresh Honitorina Setresh Honitorina Management Si Cellina Management	Remote Access Sea	1 30.30.30.1	INSECTION OF THE	.0 0.22-	200 70	B1190729		N-to-LAN S	essions M	ingenent Sessions)	
	Username	Assigned IP Add	Miress Gra	ng Ent	rincol Aprilan	Login Ti Duratio	me <u>C</u> m	<u>lient Type</u> <u>Version</u>	Bytes Bytes	Tx Artions	
	No Remote Access Sessions										
	Management Sessio	88					[LAN-	to-LAN See	cione Barna	da Access Sessions]	
	Administrator	IP Addre	ss Protocol	Enr	Encryption		Legin Time		3h	Ardeas	
	admir.	172.161.2	HTTP	None		Jan.01 19:17	42	0:12:38	[1.00	out [Ping]	

Troubleshoot

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

Solucionar problemas do roteador

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.

- debug crypto engine Exibe o tráfego que está criptografado. O mecanismo de criptografia é o mecanismo real que executa criptografia e descriptografia. Um mecanismo de criptografia pode ser um software ou um acelerador de hardware.
- debug crypto isakmp Exibe as negociações de Internet Security Association and Key Management Protocol (ISAKMP) da fase 1 do IKE.
- debug crypto ipsec Exibe as negociações de IPsec da fase 2 do IKE.

Consulte <u>Solução de problemas de IPSec - Entendendo e usando comandos **debug** para obter informações mais detalhadas e saída de exemplo.</u>

Solucionar problemas do VPN Concentrator

Semelhante aos comandos **debug** nos roteadores Cisco, você pode configurar classes de evento para exibir todos os alarmes.

1. Selecione Configuration > System > Events > Classes > Add para ativar o registro de classes de evento.Essas classes estão disponíveis para

IPsec:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE

Configuration	
	Configuration System Events Classes
	Save Needed
- ERServers	
Aderess Management	This section lets you configure special handling of specific event classes.
EPTunneling Protocols	
Entrement On the set	Click the Add button to add an event class, or select an event class and click Modify or Delete.
EX-File lactement of 000 (2015	
Ceneral	Click here to configure general event parametera.
ETP Backup	
Classes	Cenfigured
Trap Destinations	Erent Classes Actions
	IKEDECCCE
SMIP Servers	IPSECDEG
	MB2TRAP Add
- Ciert Unida	
Load Balancing	Modity
- Illeer Monacement	
	Celete
Administration	
#H <u>Monitoring</u>	

2. Ao adicionar, você também pode selecionar o nível de Gravidade para cada classe, com base no nível de Gravidade que o alarme é enviado.Os alarmes podem ser tratados por um destes métodos:Por logExibido no consoleEnviado para o servidor Syslog UNIXEnviado como e-mailEnviado como armadilha para um servidor de Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol)



3. Selecione Monitoring > Filterable Event Log para monitorar os alarmes

ativados. -Configuration Monitoring | Filterable Event Log -Interfaces Oystem - THEerwers Select Filter Options - Address Management Severifies Erent Class Al Classes ALL 🔺 -31-Tunneling Protocols AUTH - THP Routing AUTHDBG - El-Management Protocols AUTHDECODE etnex#0 -General Client IP Address 0.0.0.0 Erents/Page 100 💌 -FTP Backup -All-٠ Direction Oldest to Newest -Group -Cheeses -Trap Destinations 144 44 ►► ►► GetLog SaveLog ClearLog -Syslog Servers -SMTP Servers Email Regiptents - General -(#) Client Upplate 37992 01/02/2004 11:58:24.540 SEV-8 IKEDECODE/0 RPT-61097 30.30.30.1 Style of the style of the style style in the style of the style o -Load Balancing ERUser Management Delicy Management Administration Honitoring Flags : 1 (BUCDYPT) Berrage ID : a3905ced Length : 92 -Routing Table Dynamic Filters Length -EFilterable Event Log -Live Event Log 37355 01/02/2004 11:58:28.540 SEV-8 INEDECODE/0 RFT-61098 30.30.30.1 System Status Notify Fayload Decode : : IPSEC (1) : IBAKKP (1) DOT EKSessions Protocol - Statistics : DPD R-O-THEDI-ACK (96137) : AD AG OC 63 05 CA 53 25 6D B2 65 02 66 0D 12 6C : 32 Berrage 591 Length 38005 01/02/2004 11:58:48.540 SEV-8 INEBECODE/0 89T-61099 30.30.1 ISACHP HEADER : | Version 1.0) Initiator Dooble(9): AS AS SC 63 09 CA 55 25 Cisco Systems Responder Coobie(8): 68 B2 66 02 86 0D 12 60 Best Dayload : HASH (8) ath Exchance Type : Dakley Informations

Informações Relacionadas

- Advanced Encryption Standard (AES)
- <u>Módulo de criptografia DES/3DES/AES VPN</u>
- <u>Configurações de exemplo de IPSec</u>
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de Suporte de Negociação IPSec/Protocolos IKE

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.