在Cisco VPN 3000集中器和路由器之间的LAN到 LAN IPSec隧道有AES的配置示例的

目录

简介 先决条件 要求 使用的组件 规则 配置 网络图 配置 配置 VPN 集中器 验证 检验路由器配置 验证VPN集中器配置 故障排除 排除路由器故障 排除VPN集中器故障 相关信息

<u>简介</u>

本文说明如何将Cisco VPN 3000集中器和带有新一代加密标准(AES)的Cisco路由器之间的IPSec隧 道配置为加密算法。

AES是美国标准技术研究所(NIST)新发布的联邦信息处理标准(FIPS),将用作加密方法。此标准规定AES对称加密算法(替换数据加密标准)需进行保密转换,供IPSec和互联网密钥交换(IKE)使用。 AES有三个不同的密钥长度、一个128位密钥(默认值),一个192位密钥和一个256位密钥。Cisco IOS®中的AES在IPSec中支持新的加密标准AES,同时提供密码链块(CBC)模式。

有关AES的详细信息,请参阅NIST计 算机安全资源中心站点。

有关VPN 3000集中器和PIX防火墙之间的LAN到LAN隧道配置的详细信息,请参阅<u>Cisco VPN</u> 3000集中器和PIX防火墙之间的LAN到LAN IPsec隧道配置示例。

当PIX具有软件版本7.1时,有关详细信息,请参阅<u>PIX 7.x和VPN 3000集中器之间的IPsec隧道配置</u> <u>示例</u>。

<u>先决条件</u>

<u>要求</u>

本文档需要对 IPSec 协议拥有基本的了解。要了解有关 IPsec 的详细信息,请参阅 <u>IPsec 加密简介</u> <u>。</u>

尝试进行此配置之前,请确保满足以下要求:

- 路由器要求 AES功能在Cisco IOS软件版本12.2(13)T中引入。要启用AES,您的路由器必须 支持IPsec并运行带有"k9"长密钥("k9"子系统)的IOS映像。注意:Cisco 2600XM、2691、 3725和3745 AES加速VPN模块也提供AES硬件支持。此功能没有配置暗示,并且如果两个都 可用,硬件模块自动地选择。
- VPN集中器要求 版本3.6中引入了对AES功能的软件支持。新的增强的可扩展加密处理器 (SEP-E)提供了硬件支持。此功能不涉及配置。注意:在Cisco VPN 3000集中器版本3.6.3中 ,由于Cisco Bug ID <u>CSCdy88797(仅限注册</u>客户),隧道不会协商到AES。这已从版本3.6.4中 解决。注意:Cisco VPN 3000集中器使用SEP或SEP-E模块,而不同时使用这两个模块。请勿 在同一设备上同时安装两者。如果您将SEP-E模块安装在包含一个SEP模块的VPN集中器上 .那么VPN集中器就禁用SEP模块,只使用SEP-E模块。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •带Cisco IOS软件版本12.3(5)的Cisco 3600系列路由器
- 带软件版本4.0.3的思科VPN 3060集中器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

<u>配置</u>

本部分提供有关如何配置本文档所述功能的信息。

注意:使用命<u>令查找工</u>具(<u>仅</u>限注册客户)可获取有关本节中使用的命令的详细信息。

<u>网络图</u>

本文档使用以下网络设置:



配置

本文档使用以下配置:

- IPsec路由器
- <u>VPN 集中器</u>

ipsec_router配置

-
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
!
<pre>! Configuration for IKE policies. crypto isakmp</pre>
policy 1
<pre>! Enables the IKE policy configuration (config-</pre>
isakmp) command mode, ! where you can specify the
parameters to be used during ! an IKE negotiation.
encryption aes 256
<pre>! Specifies the encryption algorithm as AES with a</pre>
256 ! bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
<pre>! Specifies the preshared key "cisco123" which !</pre>

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 espaes 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 ipsecisakmp !--- 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 ! 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 н 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 1 line con 0 line aux 0 line vty 0 4 login

注意:虽然ACL语法保持不变,但加密ACL的含义稍有不同。在加密ACL中,permit指定应加密匹 配的数据包,而deny 指定不需要加密匹配的数据包。

配置 VPN 集中器

end

VPN集中器在他们的出厂设置中没有预编程序设置IP地址。您必须使用控制台端口配置基于菜单的 命令行界面(CLI)的初始配置。 有关如何通过控制台进行配置的信息,请参阅<u>通过控制台配置 VPN</u> <u>集中器。</u>

在Ethernet 1(专用)接口上配置IP地址后,可以使用CLI或浏览器界面配置其余地址。浏览器界面 支持 HTTP 和使用安全套接字层 (SSL) 的 HTTP。

以下参数通过控制台进行配置:

• 时间/日期 — 正确的时间和日期非常重要。他们帮助保证记录和记帐条目是准确的,并且系统 能创建一个有效安全证书。

•以太网1(专用)接口 — IP地址和掩码(来自我们的网络拓扑172.16.1.1/24)。

此时,VPN集中器可通过HTML浏览器从内部网络访问。欲了解在CLI模式下配置VPN集中器的信息 ,使用CLI参见快速配置。

 从Web浏览器键入专用接口的IP地址以启用GUI界面。单击"保存**所需**"图标将更改保存到内存 。出厂默认用户名和密码为"admin",区分大小写。

	VPN 3000	Main Help Support Logout
	Concentrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
#:- <u>Configuration</u> #:- <u>Administration</u> #:Monitoring	Main Welcome to the VEN 3000 Concentrator Manager.	
	In the left forme or the contextual bar above, click the function you want	
	 <u>Configuration</u> - to configure all flectures of this device. <u>Administration</u> - to control administrative functions on this device. <u>Monitoring</u> to view status, statistics, and logs on this device. 	
	The bar at the top right has:	
	 Main - to return to this screen <u>Help</u> - to get help for the current screen. <u>Support</u> - to essees VPN 300D Concentrator support and documentation. <u>Logent</u> to log out of this section, and actum to the Manager logis screen. 	
	Under the location bar in the upper right, these icons may appear. Click to:	
	 Save	

2. 在启动GUI后,选择Configuration > Interfaces > Ethernet 2(Public)以配置Ethernet 2接口。

Configuration	Config	guration Interfaces	s Ethernet 2			
EPUser Management	Config	uring Ethernet Interfa	ce 2 (Public).			
• Monitoring	Gene	eral RIP OSPF B	andwidth			
			Genes	ral Parameters		
	Sel	Attribute	Value		Description	
	0	Disabled			Select to disable this interface.	
	0	DHCP Client			Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.	
	6	Static IP Addressing				
		IP Address	20.20.20.1		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this	
		Subnet Mask	255.255.255.0		mteriboe.	
		Public Interface	R		Check to make this interface a "public" interface.	
		MAC Address	00.90 A4.00.4L F9		The MAC address for this interface.	
		Filter	2. Public (Default)	•	Select the filter for this interface.	
		Speed	10/100 suto 💌		Select the speed for this interface.	
		Duplex	Auto 💌		Select the duplex mode for this interface.	
		MTU	1500		Enter the Maximum Transmit Unit for this interface (63 - 1500).	
			C Do not flagment prior to IPSec encapsulation; flagment prior to interface transmission			
		Public Interface IPSec Fragmentation Policy	C Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)		MTU Discovery (ICMP)	
			C Fragment prior to IPSec enc	upsulation without P	ath MTU Discovery (Clear DF bit)	
Cisco Systems	Aş	oply Cancel				

3. 选择**Configuration > System > IP Routing > Default Gateways** 配置IPsec的默认(Internet)网关 和隧道默认(内部)网关,以到达专用网络中的其他子网。在此场景中,内部网络中只有一个 子网可用

丁四月元。		
Configuration		
	Configuration System IP Routing D)efault Gateways
- BServers	Configure the default gateways for your system.	
- G-Tunneling Protocols	Default Catanan 20.20.20.2	Pater the IR address of the default mission or sector. Pater 0.0.0.0 for we default sector.
- G-P Routing	Detailuit Gatearay [20.20.20.2	Ealer the IP address of the default gas way or rother. Ealer 0.0.0.0 for an default rother.
Static Routes	Metric 1	Eater the metric, from 1 to 16.
Default Galeways	T 10.6 h	
	Cotomar 172.16.1.2	Enter the IP address of the default gateway or fouter for funnels. Enter 0.0.0.0 for no default market
DHCD Development	Galenay.	General to dien.
OHCP Paratieters	Override Default	Check to allow learned default gateways to override the configured default gateway.
Part rolen ov	Gatemay	
Reverse Route Intertion	Apply Concel	
-REvents		
- I General		
- Gient Update		
Load Balancing		
- E-User Management		
Policy Management		
Administration		
E Monitoring		

4. 选择Configuration > Policy Management > Traffic Management > Network Lists > Add以创建 定义要加密的流量的网络列表。列表中提到的网络可到达远程网络。以下列表中显示的网络是 本地网络。单击"生成本地列表"时,也可以通过RIP自动生成本地网络列表。

	Configuration	on Policy Management Tra	ffic Management	Network Lists Modify
- (#System				
-(*)-User Management	Madifera confi	nued Maturock List, Click on Camarat	a Local List to carend	a national list based on portion antrias on the Drivate interface
G-Policy Management	mouty a come	gard Herwork ESt. Carst da General	e nordi mire to Senergy	e herweite ist odsen off founde entries off the Fillene interiere.
Access Hours	List Name	von local setvork	Na	use of the Network List you are adding. The name point he unique
		<pre>ph_local_netroix</pre>		na n
Network Lists		122.16.0.0/0.0.255.255	A	Enter the Metamoles and 1956 and marks union the following
Rules				 Easer the Networks and Whotald masks doing his following Convertige a product of a product of the 10 to 0 conditions of the second second
				1019901: n.n.n.n.n.n.n.(e.g. 10.10.0.00.0.255.255).
Filters				. Note: Enter a wildcard mask, which is the reverse of a
TINAT				subnet mask. A wilcloard mask has 1s in bit positions to
Phil Delicion				ignore, 0s in bit positions to match. For example,
Ci Creare Materiae	Network List			10.10.1.0/0.0.0.255 = all 10.10.1 mm. addresses.
- GEPOrous Matching				 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.
				meak is to be used.
			7	
			ссоссосс <u>ь</u>	
	Apply	Concel Generate L	.acal List	

5. 此列表中的网络是远程网络,需要手动配置。为此,请为每个可到达子网输入网络/通配符。

-E-Configuration		
	Configuration Policy Management Traffic Management Network Lists Modily	
— <u>⊞System</u>		
	Modify a configured Network List. Click on Generate Local List to generate a network list based on routing entries on the Privete	interface.
Access Hours	The New York and a set of the New York Statement Statement of the Statement Statem	at her emission
Traffic Management	Las trans of the terretoria Las you are saining. The bank mark	n de unique.
Cietvers Lists Guides Guides	192.168.20.0/0.0.0.255 • Ehite the Networks and Wildowid masks using the non-nummeric (e.g. 10.10.0.00.0.255.253). • Network List • One of the state of the st	s following format: ense of a subnet mask. A is in bit positions to 10.1 nm addresses, attend on a single line. Whileard music is to be
	Apply Cancel Generate Local List	

完成后,以下是两个网络列表

E)Configuration Interfaces	Configuration Policy Managem	ent Traffic Management Netw	oork Lists	Saug
- GPSystem - GPSystem - GPSystem Management - GPSystem Management - Stratfic Management - Gettess - Galess -	This section lets you add, modify, copy, a Clink Add to create a Network List, or sele	ad delete Network Lists et a Network List and click Medilify, Cepy <u>Network List</u> VPN Client Local LAN (Default) vgn_remote_network	y, or Delete. Actiene	Save
Eren Huises Eren Heishna Eren Heishna Eren Heishna Eren Heishna		vpn_local_network	Modity Copy Delete	

6. 选择Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add并定义LAN到 LAN隧道。此窗口包含三个部分。上面的部分是网络信息,而下面的两部分是本地和远程网络 列表。在Network Information(网络信息)部分,选择AES加密、身份验证类型、IKE提议 ,并键入预共享密钥。在底部部分中,分别指向已创建的网络列表(本地和远程)。

	Configuration System Tunneling Protocols	IPSec LAN-to-LAN Add
	A 45	
	Add a new Lifeet LAN-to-LAN connection.	
- (3- <u>Tunneline Protocols</u>	Eashle 🔽	Check to enable this LAN to LAN connection.
	Name bast	Determine the same first his () is 1 () association.
- PEsec	Ivanie (98)	Enter the mane for this EPEN-00-EPEN connection.
LAN-to-LAN	Intexture Ethernet 2 (Public) (20.20.20.1	Select the interface for this LAN-to-LAN connection.
NAT Transparency	Connection Type Bi-directional	Choose the type of LAN-to-LAN connection. An Originate Only connection may have wellink more exactled below.
Alerta	20 20 20 1	ante multie teens etecnier cense.
- @4P Routing - @Management Environment	30.30.30.1	
	8	
	8	Enter the remote peer IP addresses for this LAM-to-LAN connection. Originate-
i ged Balancing	Poers	$\Omega_{N}(p)$ connection may specify up to ten peer IP addresses. Enter one IP address per line
- DUser Management		418-
Ender Wans gement	8	
Traffic Management	i i i i i i i i i i i i i i i i i i i	
- (7)-Orouo Matching	Digini Nano Il Iso Emakorad Karak	- Sabat the divided contification to use
- Administration	Certificate None (Ose Presnated Reys)	and a second the deposit contraction to use.
	Certificate C Entire certificate chain.	Choose how to send the digital certificate to the DCE peer.
	Transmission @ Identity certificate only	
	Preshared Key cisco123	Enter the possbared key for this LAN-to-LAN connection.
	Authentication ESP/MD5/HMAC-128	Specify the pathet authentication mechanism to use.
CISCO SYSTEMS	Enryption AES-256	Specify the entryptica mechanism to use.
ավիրումիրու	IKE Proposal KE-AES256-SHA	Select the IKE Proposal to use for this LAN-to-LAN connection.
-= Configuration		
E-Servers		
- El-Acidress Management - El-Tuppeling Protocols		
EETE	Witten Internet	Choose the filter to apply to the traffic that is transled through this LAN-to-LAN
	Puter - None-	connection.
LANZELAN	IPSer NAT-T	Check to let NAT-T competible IPSec peers establish this LAN-to-LAN connection theoryk a NAT device. You range also enable IPSec over NAT-T under
KE Proposelo		NAT Transparency.
Alerts	Baadwidth Policy -None- 💌	Choose the bandwidth policy to apply to this LAN-to-LAN connection
- E-P Routing - E-Management Protocols	Routing None -	Choose the routing mechanism to use Parameters below are ignored if Network Autodiscovery is chosen.
- Brents		
- E-General Clearl Lockston	Local Neiseark: If a LAN-to-LAN NAT rule is used, this is	the Translated Network address.
Lost Balancing	Network List vpn_local_network	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
Prolov Management	IP Address	Note: Enter a wildoord mask, which is the swarze of a subset mask. A
Access Hours	Wildcard Mask	wikinand eases has 1s in bit positions to ignore, 0s in bit positions to reatch. For
E-Group Matching		szaruple, 10.10.1.040.0.0.235 = all 10.10.1 mm addresses.
-31 <u>Administration</u>	Remote Network: If a LAN-to-LAN NAT rule is used, this	s is the Reporte Network address.
1.9 Monitoring	Network List vpn_remote_network	Specify the tenote network address list or the IP address and wildcard mask for this I by to 1 b M execution.
	IP Address	THE LEAST DELEVIT CONTROL OF
		Note: Enter a wildowd mask, which is the reverse of a submet mask. A wildowd mask has bein hit restitutes for india to state. For
	Wildcard Mask	ransple, 10.10.1 I0.0.0.255 = all 10.10.1 ann addresses.
CISCO SUSTEMS	Add Concel	

7. 单击Add后,如果连接正确,系统将显示"IPSec LAN-to-LAN-Add-Done"窗口。此窗口提供隧 道配置信息的概要。它还自动配置组名、SA名和过滤器名。可以编辑此表中的任何参数。

Configuration	
Cr <u>soniquianun</u>	
misriacas	Configuration System Tunneling Protocols IPSec LAN to-LAN Adu Done
- C Systen	Save Needed
- Alervers	
- Ch-Address Management	An IPSet LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:
	Authentisation Server Internal
Esec	Group 20.20.20.1
LANHO-LAN	Security Association 1.21.: test
KE Processis	Films Balas 121: test Out
NAT Transportney	L2. test in
<u>ellerts</u>	
- IP Routing	Modifying any of these tarsa will affect the LAN-to-LAN configuration. The Groun is the same as your LAN-to-LAN rose. The Security Association and
	Filter Rules all start with "L7L4" to indicate that they from a LAN to LAN configuration.
- CHEVanta	
- III General	
- (F) Client Lipciate	OK
Load Balancing	
User Management	
EPolicy Management	
Monitoring	

此时,IPsec LAN到LAN隧道已设置,您可以开始工作。如果由于某种原因隧道不工作,您可 以检查配置错误。

8. 选择Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN时,可以查看或修改 之前创建的LAN到LAN IPsec参数。此图显示隧道名称为"test",根据场景,远程端的公共接口 为30 30 30 1

//00.00.00.18		
GConfiguration		
Interfaces	Configuration System Tunneling Protocols IPSec LAN-to-LAN	
-G-System		Save
- D <u>Servers</u>		
	This section lsts you configure IPSec LAN-to-LAN connections. LAN-to-LAN connections are se	tablished with other VPN 3000 Concentrators,
-EF <u>Tunneting Protocols</u>	PIX firewalls, 7100/4000 series contens and other IPSec-compliant security gateways. To configure	a VPN 3002 or other remote access
1.272	connection, go to User Management and configure a Group and User. To configure NAT over LAN	I-to-LAN, go to <u>LAN-to-LAN NAT Rules</u> .
	If you want to define a set of astworks on the local or remote side of the LAN-to-LAN connection	, configure the necessary <u>Network Lists</u> prior
KE Proposals	to creating the connection.	
NAT Transparancy	Click the Add button to add a LAN-to-LAN connection, or select a connection and click Modify or	Delete.
<u>-Verts</u>	· · · ·	
- College and Performing	(D) indicates a disabled LAN-to-LAN connection.	
TOEucoto		
- ECeneral	LAN-to-LAN	
- @Client Update	Connection	Actions
Load Balancing	test (30.30.30.1) on Ethernet 2 (Public)	
		Add
GPolicy Management		7455
		Modify
Network Lists		
Rules		Delete
-SA8		
THAL		
ENV Policies		
- (E) Croup Metching		
- Administration		
111 (MUNICOLINI)		

9. 有时,如果IKE提议在Inactive Proposals列表中,则隧道可能无法打开。选择Configuration > **System** > Tunneling Protocols > **IPSec** > IKE Proposals以配置活动IKE建议。如果您的IKE建议在"非活动建议"列表中,则在选择IKE建议并单击"激活"按钮时可以启**用该**建议。在此图中,所选建议"IKE-AES256-SHA"在"活动建议"列表中。



10. 选择Configuration > Policy Management > Traffic Management > Security Associations以验 证SA参数是否正确。



11. 单击SA名称(在本例中为L2L:test),然后单击Modify以验证SA。如果任何参数与远程对等体 配置不匹配,可在此处更改。

Configuration	Configuration Policy Management Traffic Manageme	ent Security Associations Modify
	Modify a configured Security Association.	
Address Management Durneling Protocols	SA Name L2L: test	Specify the name of this Security Association (SA).
	Inheritance From Pule 💌	Select the granularity of this SA.
LAN-ID-LAN	IPSec Parameters	
NAT Transporancy	Audie atication Algorithm ESP/MD5/HMAC-128	Select the packet authentication algorithm to use.
Alerts	Encryption Algorithm AES-256	Select the ESP encryption algorithm to use.
EH-Management Protocols	Encapsulation Mode Tunnel 💌	Select the Encapsulation Mode for this SA.
	Serrecy Disabled	Select the use of Perfect Forward Secrecy.
Losd Balancing	Lifetime Measurement	Select the lifetime measurement of the IPS+: keys
	Data Lifetime 10000	Specify the data lifetime in kilobytes (ICB).
Access Hours	Time Lifetime 28800	Specify the time lifetime in seconds.
Rules	IKE Parameters	
	Connection Type Bidrectional IKE Press 30 30 30 1	The Consection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
EXCPolicies	Negatiation Mode Main	Select the IKE Negotiation mode to use
Group Metching Group Metching Group Metching	Digital Certificate None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
-E <u>Monitoring</u>	Contilicate C Entire certificate chain. Transmission © Identity certificate only	Choose how to used the digital cartificate to the IRE post.
	IKE Proposal IKE AES256 SHA	Select the IKE Proposal to use as IKE initiator.
CISCO SYSTEMS	Apply Concel	

<u>验证</u>

检验路由器配置

本部分提供的信息可帮助您确认您的配置是否可正常运行。

<u>命令输出解释程序工具(仅限注册用户)支持某些</u> show <mark>命令,使用此工具可以查看</mark>对 show 命令 输出的分析。

• show crypto isakmp sa - 显示对等体上的所有当前 IKE SA。状态QM_IDLE表示SA保持与其对 等体的身份验证,并可用于后续快速模式交换。它处于静止状态。 ipsec_router#show crypto isakmp sa

dst src state conn-id slot

20.20.20.1 30.30.30.1 **QM_IDLE** 1 0

 show crypto ipsec sa - 显示当前 SA 使用的设置。检查对等 IP 地址、本地和远程端都可访问的 网络,以及所使用的转换集。有两个 ESP SA,每个方向一个。由于使用AH转换集,因此它为 空。

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 active — 显示所有加密引擎的当前活动加密会话连接。每个连接ID都是唯一的。加密和解密信息包的数量在前二列中显示。 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

<u>验证VPN集中器配置</u>

完成以下步骤以验证VPN集中器配置。

1. 与在路由器上显示crypto ipsec sa和**show crypto isakmp sa命令类似,在VPN集中器上选择** Monitoring > Statistics > IPSec时,可以查看IPsec和IKE统计信息。

-Configuration	Monitoring Statistics IPSec		Thursday	, U1 Ja	nuary 2004-19:32:36	
- E-System					Reset 🥔 Refresh 🔞	
-FiUser Management	IKE (Phase 1) Statistics	IPSec (Phase 2) Statistics				
Pelicy Management	Active Tunnels	L	Active Tunnels	l		
Access Hours	Total Tunnels	2	Total Tunnels	2		
Network Lists	Received Bytes	1545262	Received Bytes	3602		
Rules	Sent Bytes	5553204	Sent Bytes	5376		
<u>SAs</u>	Received Packets	60187	Received Packets	145		
EIND T	Sent Packets	60299	Sent Packets	51		
DAY Policies	Received Parkets Dropped	0	Received Parkets Dropped	0		
Group Matching	Sent Parkets Dropped	U	Received Parkets Dropped (Anti-Replay)	U		
- Administration	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		
Susteen Rehort	Sent Phase-2 Exchanges	49	Outhound Authentirations	St		
-Reboot Status	Invalid Phase-2 Exchanges Received	D	Failed Outbound Authentications	0		
Eina	Invalid Phase 2 Exchanges Sent	0	Decryptions	145		
Monitoring Retresh	Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0		
-DFile Management	Rejected Sent Phase-2 Exchanges	0	Encryptions	51		
Swap Confid File	Phase-2 SA Delote Requests Received	0	Failed Encryptions	0		
	Phase-2 SA Delete Requests Sent	50	System Capability Failures	0		
XML Export	Initiated Tunnels	0	No-SA Failures	0		
EFCertificate Management	Failed Indifated Tunnels	0	Protocol Use Failures	0		
Enrollment	Failed Benute Tunnels	0				
	Authentication Failures	0				
	Decryption Failures	D				
Dynamic Filters	Hash Validation Failures	0				
Cisco Systems	System Capability Failures	0				
adhoadhoa	No-SA Failures	0				

2. 与路由器上的show crypto engine connections active命令相似,您可以使用VPN集中器上的管理会话窗口查看所有IPSec LAN-到-LAN有效连接或隧道参数和统计数据。

Configuration											
Interfaces	Administration Ad	iminister Sea	sions						Thursday	, 01 Jan	uary 2004-19:30:2
- Er Systen										R	eset 🥔 Refresh 🖗
- E-User Management											
- EPPolicy Management	This other shows static	tios for sessions	To reflect	the statistics	dick Refresh	Select	Group to	filter the sec	stione Form	or infano	ation on a session , di
Actease Hours	and sources source assists for example, to private the sources, that we need to be a source of the sources of the source of the										
EFTraffic Management	Victorial Proposition and the second	0.0500.0000	ond once we	Barry	ALE CLENT. 20	0001100	and the task of	A CONTRACTOR OF CONTRACTOR	a source of the	a sug	
Network Lists											
	Group [=/\]E	-									
SA2	Logout All: PPTP User	12TP User IP	Sec User 1	PSec LAN-b	o-LAN						
Eliters											
- E NAI	Session Summary										
BAV Policies	Authors 3 AIN to	Author Berry	4		and Tratel	A contract	Desite 43		C		Testal disease laders
- Circus Matching	LAN Sossions	Active Kenni Accore Specia	ne Aet	Sections	nent Total	dane	Pear C	sions	Conrun	Linde	Ford Culturative
- Administration	List actions			DC SS MILS			00		3033443	Lantin	3030100
Administer Sessions				L 2		2	3		4000		19
Software Update											
<u>Concentrator</u>											
<u>Cients</u>	LAN-ta-LAN Sessions [Remote Access Sessions Management Sess								anogement Sessions]		
System Reboot	Connection Name	IP Address	Pro	iorel	Encryption	Lagi	a Tinus	Duration	Bytes Tx	Bytes Ra	Actions
Ping	test	30.30.30.1	IPSec/LA	N-to-LAN	AES-256	Jai	19:57:29	0:02:51	2128	212	8 [Logant Ping]
Monitorine Refresh											
- EM poess Matte											
File Management	Remate Areess See	lions						LT AT	NUMBER OF	ariona I M	anorment Sessions 1
- E-Certificate Management											
Monitoring	Username	Assigned IP A	ddress	Group	Pretecol		Login Th	me <u>C</u>	licat Type	<u>Byte</u>	Artions
	Public IP Address Encryption Duration Version Bytes Rz No Remote Access Sessions										
	Management Sessions [LAN-to-LAN Sessions]										
	Administrator	IP Addr	HI 1	Protocol	Encryption		Legin	Time	Duration	h	Actions
	admir.	172161.1	HT	TP	None	Jan	0119:17	42	0:12:38	[Lee	out Ping]
		1	1			10.00				11.000	

<u>故障排除</u>

本部分提供的信息可用于对配置进行故障排除。

<u>排除路由器故障</u>

<u>命令输出解释程序(仅限注册用户)(OIT) 支持某些 show 命令。</u>使用 OIT 可查看对 show 命令输 出的分析。

注意:在使用debug<u>命令之前,请参</u>阅有关Debug命**令的**重要信息。

- debug crypto engine 显示已加密的流量。加密引擎是执行加密和解密的实际机制。加密引擎可以是软件或硬件加速器。
- debug crypto isakmp 显示IKE第1阶段的互联网安全关联和密钥管理协议(ISAKMP)协商。

• debug crypto ipsec - 显示 IKE 第 2 阶段的 IPsec 协商。

有关详细信息和输出示例,请参阅IPSec故障排除— 了解和使用debug命令。

排除VPN集中器故障

类似于Cisco路由器的debug命令,您能配置事件类型,以查看所有告警。

- 1. 选择Configuration > **System >** Events > **Classes** > Add以启用事件类的日志记录。IPsec可使 用以下类
 - : IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



2. 当添加时,您还能为每个组选择严重级别,警告是根据根据这些安全级别发送的。警报可以通过以下方法之一处理:按日志显示在控制台上发送到UNIX系统日志服务器作为电子邮件发送 作为陷阱发送到简单网络管理协议(SNMP)服务器

	· · · · · · · · · · · · · · · · · · ·					
	Configuration Sustan Events Class	on LAdd				
Interneties	Configuration System Events Classes Ann					
- El Servers	This screen lets you add and configure an event class for special handling.					
- El-Adoltess Management	······································					
EFTunneling Protocols						
- EHP Bouting	Class Name KEDBG	 Select the event class to configure. 				
	Enable 🖂	Check to enable special handling of this class.				
General						
FTP Backup	If one of the following values has been set to Use Event List, the Event List can be seen by viewing Configuration System Events General.					
Classes	Changing a value set to Use Sweet List will overcide the sections of the Event List reflecting to this event class.					
<u>——Trao Destinations</u>						
	Events to Log Severities 1–5	Select the events to enter in the log.				
	Frents in Console Severities 1-3	Select the events to display on the controls				
Email Recipients	Erena a compression activities 1.5	built he state to deputy of the content.				
- @General	Events to Syslog None	Select the events to send to a Syslog Server.				
- ElClient Update						
Load Balancing	Events to Email None	Select the events to send to an Enail Recipient.				
-BUser Management	Events to Tran None	Select the events to card to an SNMP Trap Destination				
Policy Management	There is ride labele	control the electric of electric of an electric distribution.				
- Administration - Monitoring	Add Cancel					

3. 选择Monitoring > Filterable Event Log 以监控已启用的警报。



相关信息

- <u>高级加密标准 (AES)</u>
- DES/3DES/AES VPN加密模块
- IPSec配置示例
- Cisco VPN 3000 系列客户端支持页
- IPsec 协商/IKE 协议支持页