# 使用AES的Cisco VPN 3000集中器和路由器之間 的LAN到LAN IPsec隧道配置示例

### 目錄

簡介 必要條件 需求 採用元件 慣例 設定 網路圖表 組態 配置VPN集中器 驗證 檢驗路由器配置 驗證VPN集中器配置 疑難排解 路由器故障排除 排除VPN集中器故障 相關資訊

# <u>簡介</u>

本文說明如何使用高級加密標準(AES)作為加密演算法,在Cisco VPN 3000集中器和思科路由器之 間配置IPsec隧道。

AES是由美國國家標準與技術研究所(NIST)建立的新聯邦資訊處理標準(FIPS)出版物,用於加密方法。此標準指定一個AES對稱加密演算法,該演算法取代資料加密標準(DES)作為IPsec和 Internet金鑰交換(IKE)的隱私轉換。AES有三種不同的金鑰長度,一個128位金鑰(預設),一個 192位金鑰和一個256位金鑰。Cisco IOS®中的AES功能新增了對IPsec對具有密碼塊連結(CBC)模式的新加密標準AES的支援。

有關AES的詳細資訊,請參閱<u>NIST電腦保安資源中心站點</u>。

有關VPN 3000集中器和PIX防火牆之間的LAN到LAN隧道配置的詳細資訊,請參閱<u>Cisco VPN</u> 3000集中器和PIX防火牆之間的LAN到LAN IPsec隧道配置示例。

有關PIX軟體版本7.1的詳細資訊,請參閱<u>PIX 7.x和VPN 3000集中器之間的IPsec隧道配置示例</u>。

# <u>必要條件</u>



本文檔需要對IPsec協定有基本的瞭解。請參閱<u>IPSec加密簡介</u>以瞭解有關IPsec的詳細資訊。

嘗試此組態之前,請確保符合以下要求:

- 路由器要求 AES功能是在Cisco IOS軟體版本12.2(13)T中匯入。為了啟用AES,您的路由器 必須支援IPsec並使用「k9」長金鑰運行IOS映像(「k9」子系統)。註:Cisco 2600XM、 2691、3725和3745 AES加速VPN模組也提供AES硬體支援。此功能沒有配置影響,如果兩個 模組都可用,將自動選擇硬體模組。
- VPN集中器要求 AES功能的軟體支援是在3.6版中引入的。硬體支援通過新的增強型可擴展加密處理器(SEP-E)提供。此功能不涉及配置。注意:在Cisco VPN 3000 Concentrator 3.6.3版中,由於Cisco錯誤ID <u>CSCdy88797</u>(僅限<u>註冊</u>客戶),通道不會與AES協商。 3.6.4版中已解決此問題。注意:Cisco VPN 3000 Concentrator使用SEP或SEP-E模組,而不是同時使用兩者。請勿將兩者安裝在同一裝置上。如果在已經包含SEP模組的VPN集中器上安裝SEP-E模組,則VPN集中器會禁用SEP模組並僅使用SEP-E模組。

### <u>採用元件</u>

本檔案中的資訊是根據軟體和硬體版本:

- 採用Cisco IOS軟體版本12.3(5)的Cisco 3600系列路由器
- 軟體版本4.0.3的Cisco VPN 3060集中器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

### <u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

### <u>設定</u>

本節提供用於設定本文件中所述功能的資訊。

註:使用<u>Command Lookup Tool</u>(僅<u>供</u>已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

#### 網路圖表

本檔案會使用以下網路設定:



### <u>組態</u>

本檔案會使用以下設定:

- IPsec路由器
- <u>VPN集中器</u>

### ipsec\_router組態

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 Ţ line con 0 line aux 0 line vty 0 4 login

注意:雖然ACL語法未更改,但加密ACL的含義略有不同。在加密ACL中,permit指定應加密匹配 的資料包,而deny指定不需要加密匹配的資料包。

### <u>配置VPN集中器</u>

VPN集中器出廠設定中未預先設定IP地址。必須使用控制檯埠來配置初始配置,這些配置是基於選 單的命令列介面(CLI)。 有關如何通過控制檯進行配置的資訊,請參閱<u>通過控制檯配置VPN集中器</u>。

在Ethernet 1(專用)介面上配置IP地址後,可以使用CLI或通過瀏覽器介面配置其餘地址。瀏覽器 介面同時支援HTTP和HTTP over Secure Socket Layer(SSL)。

這些引數是通過控制檯配置的:

• 時間/日期 — 正確的時間和日期非常重要。它們有助於確保日誌記錄和會計分錄準確無誤,並 且系統可以建立有效的安全證書。

• Ethernet 1(private)interface - IP地址和掩碼(來自我們的網路拓撲172.16.1.1/24)。

此時,可從內部網路通過HTML瀏覽器訪問VPN集中器。有關在CLI模式下配置VPN集中器的資訊 ,請參閱<u>使用CLI快速配置</u>。

 2. 從Web瀏覽器鍵入專用介面的IP地址以啟用GUI介面。按一下save needed圖示將更改儲存到 記憶體。出廠預設使用者名稱和密碼是「admin」,區分大小寫。

	VPN 3000	Main   Help   Support   Logout
	Concentrator Series Manager	Logged in: admir
		Configuration   Administration   Monitoring
<del>40-<u>Configuration</u> ∰-<u>Administration</u> ∰Manitacina</del>	Main         Welcome to the VFN 3000 Concentrator Manager.         In the left forme or the conjugate all features of this device.         • Configuration - to configure all features of this device.         • Administration - to control administrative functions use this device.         • Monitoring - to very status, statistica, and logs on this device.         The bar at the top right has:         • Main - to return to this across         • Main - to return to this across         • Main - to some VPN 3000 Concentrator support and documentation.         • Lagrat - to log out of this section and return to the Manager login access.         Under the knoticu bar in the upper right, these icons may appear. Click to:         • Section - to expland the active configuration and make it the boot configuration.         • Section - to active configuration and make it the boot configuration.	Configuration   Administration   Monitoring
	<ul> <li>Result #* to temporarily result statistics to zero.</li> <li>Restors ** to restore statistics from their result values.</li> </ul>	
	🔹 Rafaala 🕸 to adrach statistica.	

2. 啟動GUI後,選擇Configuration > Interfaces > Ethernet 2(Public)以設定Ethernet 2介面。

Configuration	Config	guration   Interfaces	s   Ethernet 2			
EPUser Management	Config	uring Ethernet Interfa	ce 2 (Public).			
Content General RIP OSPF Bandwidth						
			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		<b>N</b>		Check to make this interface a "public" interface.		
	MAC Address		00.90 A4.00.4L F9		The MAC address for this interface.	
	Filter Speed		2. Public (Default)	•	Select the filter for this interface.	
			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		agreent prior to interface transmission	
	Public Interface IPSec		C Fragment prior to IPSec encepsulation 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. 選擇Configuration > System > IP Routing > Default Gateways,為IPsec配置預設(Internet)網 關和隧道預設(內部)網關,以到達專用網路中的其他子網。在此場景中,內部網路中只有一 個可用的子網

<u> Configuration</u>		
	Configuration   System   IP Routing   De	fault Gateways
- O'System		
- Bervers	Configure the default gateways for your system.	
Tunneting Protocols	Dofinalit Cotomore 20.20.20.2	Fater the IR address of the default minimum or souther. Fater 0.0.0.0 for an default souther
GPRouting	Detailint Gateway [20.20.20.2	Zaher the 1P address of the default geleway of Rother. Earler 0.0000 for an default rother.
Static Routes	Metric 1	Enter the metric, from 1 to 16.
Default Gateways		
<u>GGPT</u>	Catagoria 172.16.1.2	Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default marker
OSPF Arees	cananaà .	- General router.
UHCP Paratieters	Override Default	Check to allow learned default gateways to override the configured default gateway.
	Gateway	
Redunciency Results Foundation	Apply Concel	
Fielder and Anterstein	· + + + · · ·	
- International Proceeds		
- Concept		
Client Indate		
Load Balancing		
-FFLUser Management		
Policy Management		
Administration		
THMonitoring		

4. 選擇Configuration > Policy Management > Traffic Management > Network Lists > Add以建立 定義要加密的流量的網路清單。清單中提到的網路可以到達遠端網路。以下清單顯示的網路是 本地網路。按一下Generate Local List時,還可以通過RIP自動生成本地網路清單。

-Configuration				
	Configuration	on   Policy Management   Tra	ffic Management   Netw	ork Lists   Modify
- <del>I Systen</del>				
	Modify a confi	gured Network List, Click on General	e Local List to generate a netw	ork list based on routing entries on the Private interface.
			•	· · · · · · · · · · · · · · · · · · ·
Access Hours ————————————————————————————————————	List Name	vpn_local_network	Name of th	te Network List you are adding. The name must be unique.
Croup Mathing Croup Mathing Croup Mathing Croup Mathing Croup Mathing Constantion Constantion Constantion	Network List	172.16.0.0/0.0.255.255	■ Ec fa N su ig 10 Ec aŭ . T m	ter the Networks and Wildrard masks using the following error: n.n.n.m.n.n (e.g. 10.10.0.00.0.255.255). de: Enter a wildcard mask, which is the reverse of a heter mask. A wildcard mask has 1s in bit positions to nore, 0s in bit positions to match. For example, 110.1.00.00.0.255 = all 10.10.1 rms addresses. sch Network and Wildcard mask pair must be entered on a ngle line. he Wildcard mask may be omitted if the natural Wildcard ask is to be used.
	Apply	Concel Generate L	lacal List	

5. 此清單中的網路是遠端網路,需要手動配置。為此,請為每個可到達子網輸入網路/萬用字元

0	
<u>Configuration</u> <u>interfaces</u>	Configuration   Policy Management   Traffic Management   Network Lists   Modify
	Modify a configured Network List. Click on Generate Local List to generate a network list based on routing entries on the Private interface.
Access Hours	List Nume vpn_nemote_network Name of the Network List you are adding. The same must be unique.
Catvork Lists	<ul> <li>192.168.20.0/0.0.0.255</li> <li>Enter the Networks and Wildowid masks using the following format: a.n.n.th.n.n.n (e.g. 10.10.0.00.0.255 253).</li> <li>Note: Enter a wildowid mask, which is the reverse of a subnet mask. A wildowid mask, here is in bit positions to impose, 0s in bit positions to meth. For example, 10.10.1.00.0.255 = all 10.10.1 nm addresses.</li> <li>Each Network and Wildowid mask pair must be extended on a single line. The Wildowid mask, may be omitted if the natural Wildowid mask is to be used.</li> </ul>
	Apply Cancel Generate Local List

完成後,以下是兩個網路清單

HConfiguration     Interlaces     GPSystem     GPUser Management     Paley Management     District Management     Vietwork Lists	Configuration   Policy Manager This section lets you add, modify, copy, Click Add to create a Network List, or se	nent   Traffic Management   Netw and data Network Lista last a Network List and click <b>Modify, Cap</b>	vork Lists y, or Delete.	Save
Eldes GA2 Official BY Publicies Official Administration Official Microsoft		Network List VPN Client Local LAN (Default) Vpn_remole_network vpn_local_network	Actiene Add Modity Copy Delete	

6. 選擇Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add, 然後定義 LAN到LAN隧道。此視窗有三個部分。頂部用於網路資訊,底部兩部分用於本地和遠端網路清 單。在Network Information(網路資訊)部分,選擇AES加密、身份驗證型別、IKE建議,然 後鍵入預共用金鑰。在底部部分中,分別指向您已建立的本地和遠端網路清單。

2. Continuention		
-s- <u>compuration</u> 	Configuration   System   Tunneling Protocols   IPSec	LAN-to-LAN   Add
	Add a new IPSet LAN-to-LAN connection	
	5-11-E	01 - 3
<u>porp</u>	Enable 🗠	Check to enable thus LAN-to-LAN connection.
-pesec	Name test	Enter the name for this LAN-to-LAN connection.
LANto-LAN	Interface Ethernet 2 (Public) (20.20.20.1)	Select the interface for this LAM-to-LAN connection.
NAT Transparency	Connection Type Bi-directional	Choose the type of LAN-to-LAN connection. An Originate Only connection may have multiple passes exactled below.
Alerta	30.30.30.1	
- (3) Management Protocols	8	
		Total de constructor 10 addresses for deis I M to I AN accession. Accesses
- Client Upclate	Peers	Enter the reduces peer IP addresses for this LAP-to-LAP connection. Originam- Dely connection may specify up to ten peer IP addresses. Enter one IP address per
Load Balancing		lne
PEdicy Management		
Access Hours —@-Traffic Management		
- (7) Group Matching	Digini	Salari the district cartificate to use
- Administration - Administration	Certificate	and the open contracts to see.
	Certificate C Estire certificate chain. Transmission (*) Linguitzenet/Cente anter	Choose how to send the digital certificate to the DKE peer.
	Prechand Key circo123	Fater the needbard bar for this I & Nata I & Nata and
	Anthentication ESDA(DE)(4)(40-128	Search the presented any for the Least to Least to make that
Corro Sveteme	Exercise AEC.2EC	Specify the parameter machines to use
ali ali	INF Remarked INF A ESTIMATION	Salari the D'E Base and to use for this I AM to 1 AM assumption
additional inter-	INE Proposal INE AES250-SHA	ander the type Puppen to the for the type-to-take connection.
hterfoces		
-EE-Acidress Management		
- E-Tunneling Protocols		Choose the filter to early to the traffic that is transled through this LAN-to-LAN
L2TP	Filter -None-	consection.
LAN-to-LAN	IPSer NAT-T	Check to let NAT-T competible IPSec peers establish this LAN-to-LAN respective, theorem & NAT device. You reast also enable IPSec over NAT-T under
KE Proposelo NAT Transporter		NAT Transparency.
Akriz	Bandwidth Policy None-	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
	Routing None 🔹	Choose the routing mechanism to use Parameters below are ignored if Network Autodiscovery is chosen.
-E-Client Update	Local Network: If a LAN-to-LAN NAT rule is used, this is the Transk	ated Network address. Sectify the local network address list or the IP address and wildowid musk for this
Lost Balancing	Newwork Last Vpn_locol_network	LAN-to-LAN occurrentico.
Policy Management	IP Address	Noin: Enter a wildcard mask, which is the ownerse of a valuet nearly. A
Access Hours ————————————————————————————————————	Wildcard Mask	wiking mask has 1s in bit positions to gnore, 0s is bit positions to match. For severals, 10,10,1,00,0,0,055 = -0,10,10,1 are addressed
El-Group Matching	•	sample, 10.103 00000205 - al 10.103 min ancresses.
-3- <u>Administration</u> -3-Monitoring	Remote Network: If a LAN-to-LAN NAT rule is used, this is the Rem	ate Network address.
	Network List Mpn_remote_network	Specify the senate network address list or the D' address and wildcard mask for this LAN-to-LAN connection.
	IP Address	Note: Index a wildowd mask, which is the reserve of a subner mask. 4
	Wildcaml Mask	wildrard marks has Is in bit positions to ignore, 0s in bit positions to match. For
Cisco Sestews		raarapie, 10.10 1.00.0.0.235 = al. 10.10 1 ann addresses.
do als	Add Concel	

7. 按一下Add後,如果連線正確,系統將顯示一個IPSec LAN-to-LAN-Add-Done視窗。此視窗顯示隧道配置資訊的概要。它還自動配置組名、SA名和過濾器名。可以編輯此表中的任何引數

o

G-Configuration	
	Confluencellan   Contain   Truncallan Destavala   IDCon   AM as I AM   Add   Davis
risriaces	Configuration   System   Tutineting Protocols   PSec LAN-to-LAN   Adu   Done
- <del>D</del> Systen	Save Needed
- Alervera	
- Ch-Address Management	An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:
<u>PPTP</u>	Authentication Server Internal
	Group 2020201
LANHO-LAN	Security Association 1.21. (test
KE Proposals	man 1.22. test Out
NAT Transporency	Planet Aules 1.24, but In
- CHP Routing	Modiffust any of these trens will affect the LAN-to-LAN configuration. The Group is the same as your LAN-to-LAN cost. The Security Association and
	Filter Rules all start with "L7L4" to indicate that they from a LANADAN configuration.
- CTEventa	
- (I) Client Lipclate	
Load Balancing	
- E-User Management	
EPolicy Management	
Monitoring	

此時已設定IPsec LAN到LAN隧道,您可以開始工作。如果由於某種原因,通道無法正常工作,您可以檢查是否配置錯誤。

 選擇Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN時,您可以檢視或修 改先前建立的LAN到LAN IPsec引數。此圖顯示「測試」為通道名稱,依照案例,遠端的公共 介面為30.30.30.1。

<b><u></u></b>					
GConfiguration					
	Configuration   Syste	em   Tunneling Protocols   IPSec   LAN-to-LAN			
- <del>G</del> -System			Save		
- @Servers					
	This section lats you config	pure IFSec LAN-to-LAN connections, LAN-to-LAN connections are set	ablished with other VPN 3000 Concentrators,		
	PEX firewalls, 7100/4000 series conters and other IPSec-compliant security gateways. To configure a VPM 3002 or other remote access				
<u> - 9919</u>	connection, go to User Mar	ragement and configure a Group and User. To configure NAT over LAN	-to-LAN, go to LAN-to-LAN NAT Rules.		
L2IP					
-EHPSeo	If you want to define a set	of actworks 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					
NAT Transparency	Click the Add button to add	d a LAN-to-LAN connection, or select a connection and click Modify or	Delete.		
<u>Averts</u>					
	(D) indicates a disabled LA	N-to-LAN connection.			
Hiteragement Protocols					
- the venus		LAN-to-LAN			
- <u>WGeneral</u>		Connection	Actions		
Load Gelencies		Anna (22, 28, 28, 15, av. Ethermore, 2, (Ethelic)			
Cost Salariana		test (30.30.30.1) on Ethernet 2 (Fublic)			
CEpticy Management			Add		
Bocess Hours					
-Entratific Management			Modity		
Network Lists					
Rules			Delete		
-SA8					
Eitters					
- ENAL					
ENV Policies					
□ ① Croup Metching					
Administration					
C Monitoring					

9. 有時,如果您的IKE建議在「非活動建議」清單中,則通道可能無法啟動。選擇Configuration > System > Tunneling Protocols > IPSec > IKE Proposals以配置活動的IKE提議。如果您的 IKE建議位於「非活動建議」清單中,則可以在選擇IKE建議並按一下啟用按鈕時啟用它。在此 圖中,選定的建議「IKE-AES256-SHA」位於活動建議清單中。



10. 選擇Configuration > Policy Management > Traffic Management > Security Associations以驗 證SA引數是否正確。



11. 按一下SA名稱(在本例中為L2L:test),然後按一下Modify以驗證SA。如果任何引數與遠端對 等配置不匹配,可以在此處對其進行更改。

Configuration	Configuration   Policy Management   Traffic Managem	ent   Security Associations   Modify
	Modify a configured Security Association.	
Address Management     Evanueling Protocols	SA Name L2L: test	Specify the name of this Security Association (SA).
	Inheritance From Bule 💌	Select the granukarity of this SA.
LAN-10-LAN	IPSec Parameters	
NAT Transporency	Authentication Algorithm ESP/MD5/HMAC-128	Select the packet authentication algorithm to use.
DE Boutog	Encryption Algorithm AES-256	Select the ESP encryption algorithm to use.
-EP-Management Protocols	Encapsulation Mode Tunnel 💌	Select the Encapsulation Mode for this SA.
- Events - El-General	Servey Disabled	Select the use of Perfect Forward Secrecy.
Losd Balancing	Lifetime Time 💌	Select the lifetime measurement of the IPSe: heye
Policy Management	Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).
Access Hours	Time Lifetime 28800	Specify the time lifetime in seconds.
	IKE Parameters	
Elters	Connection Type Hidrectional IKE Press 30 30 30 J	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
EX(Policies	Negatiation Mode Main	Select the IKE Negotiation mode to use
E Group Matching	Digital Certificate None (Use Preshared Keys)	Select the Digital Certificate to use.
-E-Monitoring	Certificate C Entire certificate clain. Transmission © Identity certificate only	Chooses how to read the digital cartificate to the IKE poor.
	IKE Proposal IKE AES256 SHA	Select the IKE Proposal to use as IKE initiator.
CISCO SYSTEMS	Apply Concel	



### 檢驗路由器配置

本節提供的資訊可用於確認您的組態是否正常運作。

<u>輸出直譯器工具(僅供註冊</u>客戶使用)支援某些show命令,此工具可讓您檢視<u>show</u>命令輸出的分析。

• show crypto isakmp sa — 顯示對等體上的所有當前IKE SA。狀態QM\_IDLE表示SA保持其對等 體的身份驗證,可用於後續的快速模式交換。它處於靜止狀態。 ipsec\_router#show crypto isakmp sa

dst src state conn-id slot

20.20.20.1 30.30.30.1 **QM\_IDLE** 1

 show crypto ipsec sa — 顯示當前SA使用的設定。檢查對等IP地址、可在本地和遠端端訪問的 網路,以及使用的轉換集。有兩個ESP SA,每個方向一個。由於使用了AH轉換集,因此它是 空的。

0

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 — 顯示所有加密引擎的當前活動加密會話連線。每個連 線ID都是唯一的。加密和解密的資料包數量顯示在最後兩列中。 ipsec\_router#show crypto engine connections active

Interface IP-Address State Algorithm ТD

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>驗證VPN集中器配置</u>

完成以下步驟以驗證VPN集中器配置。

1. 與路由器上的show crypto ipsec sa和**show crypto isakmp sa**命令類似,在VPN集中器上選擇 **Monitoring > Statistics > IPSec**時,可以檢視IPsec和IKE統計資訊。

Configuration	Monitoring   Statistic	s   IPSec		Thursday,	. U1 Ja	muary 2004-19:32:36 Report & Refresh
- El System		IKE (Phase 1) Statistics		IPSec (Phase 2) Statistics		racaci@ racinesing
EPUser Management	i	Active Tunnels	1	Active Tannels		
Access Hours		Total Tunnels		Tatal Tunnels		
Traffic Management		Possing Rates	1545062	Reached Bying	2012	
Network Lists		Sant Brins	5552204	Cant Brates	\$174	
Sha		Beacherd Deckers	40102	Bracke J Drahats	2310	
Elter2		Received Packets	epts)	Recented Packets	140	
-EPAULT		Sent Packets	60299	Sent Packets	51	
EN/ Policies		Received Parkets Dropped	0	Received Parkets Dropped	0	
		Sent Packets Dropped	0	Received Parkets Dropped (Anti-Replay)	0	
Administer Selectors		Received Notifies	60084	Sent Packets Dropped	0	
-ErSoftware Undete		Sent Notifies	120172	Inhound Authentirations	145	
Concentrater		Received Phase-2 Eachanges	2	Failed Inbound Authentications	0	
<u>Cients</u>		Sent Phase-2 Exchanges	49	Outbound Authentirations	SL	
		Invalid Phase-2 Exchanges Received	0	Failed Outbound Authentications	0	
Eins		Invalid Phase 2 Exchanges Sent	0	Decryptions	145	
Monitoring Refresh		Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0	
-DFile Management		Rejected Sent Phase-2 Exchanges	0	Encryptions	51	
Swap Config File		Phase-2 SA Delete Requests Received	0	Failed Encryptions	0	
TFTP Transfer		Phase-2 SA Delete Requests Sent	50	System Capability Failures	0	
XML Export		Initiated Tunnels	0	No-SA Failures		
El Certificate Management		Failed Initiated Tunnels	0	Protocol Use Failures	0	
Enrollment		Failed Remote Tunnels	0			
		Authentication Failures	0			
-Routing Table		Decryption Failures	D			
Dynamic Filters		Hash Validation Failures	0			
Cisco Systems		System Capability Failures	0			
ամիտավիտ		No-SA Failures	0			

2. 與路由器上的**show crypto engine connections active**命令類似,可以使用VPN集中器上的 Administration-Sessions視窗檢視所有活動IPsec LAN到LAN連線或通道的引數和統計資訊。

Configuration	Administration   Ad	iminister Ses	sions					Thursday	. 01 Janu	uary 2004-19:30:20
ElSystem									R	eset 🥔 Refresh 🕲
Eliter Management     Eliter Management     Ansee Hours     Firstlic Management     Mathematical State     Eliters     Eliters	This screen shows statist on that essentiate name. T Group —Alt– Legout All: <u>PTP User</u>	tics for sessions. 10 log out a session 127F User   12	To refiech ti m, chick <b>Leg</b> <u>lec User</u>   <u>D</u> i	he statistics part in the t Sec LAN-ty	s, click <b>Refresh</b> able below. To b a <u>-LAN</u>	Select a <b>Group</b> est the astwork	to filter the se connection to	ssions. For n a sension, chi	uore informas ek <b>Ping</b> .	tion on a session, click
ENAL ENV Policies	Session Summary	Lather Barrie			Total 4	artes De de	r	Constant		Fair I Consecutive
Group Matching	LAN Sessions	Active Kemin Access Sessio	e Acito Isi	e Managen Sessions	Sessi	nove Peak ous S	concurrent essions	Sessions	Linit	Sessions
Administer Sessions	1	1 0		L			3			19
Concentrator Cliente System Reboot Reboot Status	LAN-to-LAN Sessio	ns IP Address	Proto	col	Encryption	Lagin Time	[Real	ete Access Se Bytes Tx	essione   Mr Bytes Rx	Actions
Ping Magina bu Padasah	test	30.30.30.1	IPSecLAN	-to-LAN	AES-256	Jan 1 19:57:29	0:02:51	2128	2128	[Logent   Ping]
Biologia Referance Biologia Statis D'Ele Nonsecont Bi-Qertificate Management GMontioring	Remote Access Sess	ions Assigned IP Ai Public IP Aid	id <u>ress</u> ress	Group	Protocol Encryption	Login' Dura	[L6 Sime	N-10-LAN Se <u>lient Type</u> Version	satone   Ma <u>Bytes</u> Bytes	Integrment Sessions ] Tx Rx Artions
	No Remote Access Sessions									
	Management Sessions [LAN-to-LAN Sessions   Baracle Access Session							de Access Sessions ]		
	Administrator	IP Addre	ss Pr	wincol	Encryption	Logi	n Time	Duratio	n 🗌	Ardens
	admin.	172.161.3	нтт	P	None	Jan.01 19:1	7.42	0:12:38	[1.00	xit [ Ping ]

## <u>疑難排解</u>

本節提供的資訊可用於對組態進行疑難排解。

### <u>路由器故障排除</u>

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊</u>。

- debug crypto engine 顯示加密的流量。加密引擎是執行加密和解密的實際機制。加密引擎可以是軟體或硬體加速器。
- debug crypto isakmp 顯示IKE第1階段的網際網路安全關聯和金鑰管理協定(ISAKMP)協商。
- debug crypto ipsec 顯示IKE第2階段的IPsec協商。

如需更多詳細資訊和範例輸出,請參閱<u>IPSec疑難排解 — 瞭解和使用</u>debug命令。

### 排除VPN集中器故障

與Cisco路由器上的debug命令類似,您可以配置事件類以檢視所有警報。

1. 選擇Configuration > System > Events > Classes > Add以開啟事件類的日誌記錄。以下類可用 於

IPsec:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



 新增時,您還可以根據警報傳送的嚴重性級別選擇每個類的嚴重性級別。可通過以下方法之一 處理警報:按日誌顯示在控制檯上傳送到UNIX系統日誌伺服器作為電子郵件傳送以陷阱形式 傳送到簡單網路管理協定(SNMP)伺服器

-E+Configuration							
	Configuration   System   Events   Classes   Add						
- El Servers	This screen lets you add and configure an event class for special handling.						
Address Management							
Tunneling Protocols	Class Name IVEDBG	Calast the sumst class to assistment					
- EHP Routing	Cass Halle   NEDBG	Select the event tass to contigue.					
Management Protocols	Enable 🖂	Check to enable special bandling of this class.					
General	If one of the following values has been set to the Event List, the Event List can be even by viewing Configuration   System   Events   General,						
ETP Backup	a service service and the service s						
Classes Trans Continuitions	Changing a value set to Use Sweet List will override the sections of the Event List referring to this event class.						
Inab Usstmations	Frants to Log Councilion 1-F	Calant the execute to exten in the law					
SVEIDE SELVERE	Theorem on the Second es 1-2	select the events to enter in the tog.					
Broat Registers	Events to Console Severities 1-3 💌	Select the events to display on the consols.					
- El-Geografi	Events & Surlas Mana	Falast the second to a Secolar Second					
-Elicit Undate	Theiring in Silvering Mone	select the events to send to a systog server.					
Loed Balancing	Events to Email None	Select the events to send to an Email Recipient.					
- EUser Management		The first second data and the second s					
- EPolicy Management	Theire in Trab None	Select the events to send to an SMMIP 1 sap Destination.					
Administration	Add Dancel						
- Monitoring	- Contact						

3. 選擇Monitoring > Filterable Event Log以監視已啟用的警報。



# 相關資訊

- <u>進階加密標準(AES)</u>
- DES/3DES/AES VPN加密模組
- IPSec示例配置
- <u>Cisco VPN 3000系列使用者端支援頁面</u>
- IPSec協商/IKE通訊協定支援頁面