AES を使用した Cisco VPN 3000 コンセントレ ータとルータの間の LAN-to-LAN IPSec トンネ ルの設定例

内容

概要 前提条件 要件 使用するコンポーネント 表記法 設定 ネットワーク図 設定 VPN コンセントレータの設定 確認 ルータの設定の確認 VPN コンセントレータの設定の確認 トラブルシュート ルータのトラブルシューティング VPN コンセントレータのトラブルシューティング 関連情報

<u>概要</u>

このドキュメントでは、Advanced Encryption Standard(AES; 高度暗号化規格)を暗号化アルゴ リズムとして使用する、Cisco VPN 3000 コンセントレータと Cisco ルータの間の IPsec トンネ ルの設定方法について説明します。

AES は、National Institute of Standards and Technology (NIST; 国立標準技術研究所)により暗 号化方式として使用されるよう作成された、Federal Information Processing Standard (FIPS: 連 邦情報処理標準)公示による新しい標準方式です。この標準では、Data Encryption Standard (DES; データ暗号規格)を置き換える AES 対称暗号化アルゴリズムを、IPsec と Internet Key Exchange (IKE; インターネット キー エクスチェンジ)両方のプライバシー トラン スフォームとして指定しています。AES には、128 ビット キー (デフォルト)、192 ビット キ ー、256 ビット キーの 3 つの異なるキー長があります。Cisco IOS(R) での AES 機能には、新し い暗号化標準である AES のサポートと Cipher Block Chaining (CBC) モードが IPsec に追加さ れています。

AESの詳細については、<u>NISTコンピュータセキュリティリソースセンターのサイトを参照してく</u> <u>ださい</u> 。 VPN 3000 コンセントレータと PIX Firewall の間の LAN-to-LAN トンネル設定の詳細については 、『<u>Cisco VPN 3000 コンセントレータと PIX ファイアウォール の間の LAN-to-LAN IPSec トン</u> ネルの設定例』を参照してください。

PIX がソフトウェア バージョン 7.1 を使用している場合の詳細については、『<u>PIX 7.x と VPN</u> <u>3000 コンセントレータの間の IPsec トンネルの設定例</u>』を参照してください。

<u>前提条件</u>

<u>要件</u>

このドキュメントは、IPSec プロトコルに関する基本的知識を前提とします。IPsec に関する知 識を深めるには、『<u>IP Security(IPSec)暗号化の概要</u>』を参照してください。

この設定を行う前に、次の要件が満たされていることを確認します。

- ・ルータの要件 AES 機能は、Cisco IOS ソフトウェア リリース 12.2(13)T で導入されています。AES を有効にするには、ルータは IPsec をサポートしていて、「k9」の長さのキーをサポートする IOS イメージが稼働している必要があります(「k9」サブシステム)。注:AESのハードウェアは、Cisco 2600XM、2691、3725、および3745 AESアクセラレーションVPNモジュールでもサポートされています。この機能には設定上の考慮事項はなく、両方が使用可能である場合はハードウェア モジュールが自動的に選択されます。
- VPNコンセントレータの要件:AES機能のソフトウェアサポートは、リリース3.6で導入されました。ハードウェアのサポートは、新しい拡張スケーラブル暗号化プロセッサ(SEP-E)によって提供されます。この機能には設定上の考慮事項はありません。注: Cisco VPN 3000コンセントレータリリース3.6.3では、Cisco Bug ID CSCdy88797(登録ユーザ専用)により、トンネルはAESとネゴシエートしません。この問題は、リリース 3.6.4 以降では解決されています。注: Cisco VPN 3000コンセントレータでは、SEPモジュールとSEP-Eモジュールの両方を使用するのではなく、SEPモジュールまたはSEP-Eモジュールを使用します。同じデバイスに両方のモジュールをインストールしないでください。すでに SEP モジュールが含まれている VPN コンセントレータに SEP-E モジュールをインストールすると、VPN コンセントレータでは SEP モジュールが無効になり、SEP-E モジュールのみが使用されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ・Cisco IOS ソフトウェア リリース 12.3(5) が稼働する Cisco 3600 シリーズ ルータ
- ・ソフトウェア リリース 4.0.3 が稼働する Cisco VPN 3060 コンセントレータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

<u>表記法</u>

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。



このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して います。

注:このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

<u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



<u>設定</u>

このドキュメントでは、次の構成を使用します。

- <u>IPSec ルータ</u>
- VPN コンセントレータ

```
ipsec_router の設定

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 (configisakmp) 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 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 ! 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 ! end

注:ACL構文は変更されませんが、暗号ACLの意味は若干異なります。暗号化 ACL では、permit は一致するパケットを暗号化する必要があることを指定しますが、一方 deny は一致するパケッ トを暗号化する必要がないことを指定します。

VPN コンセントレータの設定

VPN コンセントレータは、工場出荷時に IP アドレスが事前にプログラムされていません。コン ソール ポートを使用して、メニューベースの Command-Line Interface (CLI; コマンドライン イ ンターフェイス)である初期設定を行う必要があります。 コンソール経由で設定を行う方法の詳 細は、『コンソール経由での VPN コンセントレータの設定』を参照してください。

イーサネット 1(プライベート)インターフェイス上の IP アドレスが設定された後、残りの要素 は CLI を使用するか、ブラウザ インターフェイスを介して設定できます。ブラウザ インターフ ェイスでは HTTP と HTTP over Secure Socket Layer(SSL)の両方がサポートされています。

次のパラメータは、コンソールを使用して設定されます。

- Time/Date 正確な時刻と日付が非常に重要です。これによりロギングとアカウンティングの エントリが正確になり、システムが有効なセキュリティ認証を作成するのに役立ちます。
- Ethernet 1 (private) interface IP アドレスおよびマスク(このドキュメントのネットワーク トポロジでは 172.16.1.1/24)。

この段階で、VPN コンセントレータは、内部ネットワークから HTML ブラウザによってアクセ スできます。CLI モードでの VPN コンセントレータの設定の詳細は、『<u>CLI を使用したクイック</u> <u>コンフィギュレーション</u>』を参照してください。

Web ブラウザからプライベート インターフェイスの IP アドレスを入力し、GUI インターフェイスを有効にします。save needed アイコンをクリックして、変更をメモリに保存します。工場出荷時のデフォルトのユーザ名とパスワードは「admin」で、大文字と小文字が区別されます。

	VPN 3000	Main Help Support Logou
	Concentrator Series Manager	Logged in: admi Configuration Administration Monitoring
8:Conflouration 8:Administration €:Manifarina	Main Welcome to the VPN 3000 Concentrator Manager. In the left frame or the savigation bar above, click the function you wont: • <u>Configuration</u> - to configure all features of this device. • <u>Advantatedian</u> - to configure all features of this device. • <u>Advantatedian</u> - to configure all features of this device. • <u>Monitoring</u> to control advantatorization functions on this device. • <u>Monitoring</u> to view status, statistics, and logs on this device. The bar at the top right has: • <u>Monitoring</u> to notice to fais scenen. • <u>Monitoring</u> to age the dot the current screen. • <u>Monitoring</u> to age of this scenen. • <u>Monitoring</u> to age of this scenen. • <u>Monitoring</u> to go the dot the current screen. • <u>Monitoring</u> to go to of this scenen and veture. To the Manager login sceces. Under the location bar in the upper right, these icons may appear. Click to: • <u>Save to access</u> the active configuration and make it the boot configuration. • <u>Save Needed</u> as devey, industing you have sheaped the active configuration. • Restord to nontimely reset statistics to zero. • Restord to nontimely mean statistics to zero. • Restord to nontimely statistics.	

2. GUIを起動したら、[Configuration] > [Interfaces] > [Ethernet 2 (Public)] を選択して、 Ethernet 2インターフェイスを設定します。

Configuration	Configuration Interfaces Ethernet 2					
-BSystem -EHUser Management Co -BPolicy Management	Configuring Ethernet Interface 2 (Public).					
- Administration	General RIP OSPF Bandwidth					
		General Parameters				
	Sel	Attribute	Value		Description	
	0	Disabled			Select to disable this interface.	
	C	DHCP Client			Select to obtain the IP Address, Subnet Mask and Default Geteway via DHCP.	
	C.	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		mietikce.	
		Public Interface		Check to make this interface a "publis" interface.		
		MAC Address 00.90 A4.00.41 F9 T		The MAC address for this interface.		
	Filter 2. Public (Detault)		*	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.	
		MTU	1500		Enter the Maximum Transmit Unit for this interface (62 - 1500).	
	Public Interface IPSec		C Do not flagment prior to IPSec encapsulation; flagment prior to interface transmission			
			¹ C Fragment prior to IPSec encepsulation, with Path MTU Discovery (ICMP)		MTU Discovery (ICMP)	
			C Frigment prior to IPSec enc	opsulation without P	ath MTU Discovery (Clear DF bit)	
CISCO SYSTEMS	Ap	oply Cancel				

3. [Configuration] > [System] > [IP Routing] > [Default Gateways] を選択し、プライベートネッ トワーク内の他のサブネットに到達するために、IPSecのデフォルト(インターネット)ゲ ートウェイとトンネルデフォルト(内部)ゲートウェイを設定します。このシナリオでは、 内部ネットワーク上では1つのサブネットのみ使用できます。

Configuration		
	Configuration System IP Routing De	fault Gateways
- (FSystem		
- Bervers	Configue the default gateways for your system.	
	B A B A B B B B B B B B B B	
- G-IP 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	Metrie 1	Enter the metric form 1 to 16
Default Gateways	and the late	Lanet the metho, from t to to.
OSPE	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
OSPE Areas	Gateway	default router.
OHCP Parameters	Override Default	Check to allow leaved default asternary to coveride the configured default asternary
OHCP Relay	Gateway	CHECK ID HIDW MILLING GENER SHEWHYN ID OVERLEE DIE GENERGENES GENERE SHEWHY.
Redunciancy	Apply Cancel	
Reverse Route Injection	Apply Concer	
- III Management Protocols		
- Huents		
General		
- El Client Lipdate		
Load Balancing		
-Heronitoring		

[Configuration] > [Policy Management] > [Traffic Management] > [Network Lists] > [Add] を選択し、暗号化するトラフィックを定義するネットワークリストを作成します。このリストに記載されているネットワークは、リモートネットワークに到達できます。次のリストに示されているネットワークが Local ネットワークです。Generate Local List をクリックすると、RIP を介して Local ネットワーク リストを自動的に生成することもできます。

· - · · · · · · · · · · · · · · · · · ·			
	Confirment	an I Dallas Managament I Tar	47 - Manuar and I Materia II Set I Mar 196 -
ntertaces	Configurati	on Policy Management Tra	nic management network Lists modity
- O System			
- E-User Management	Modify a confi	gured Network List. Click on Genera	te Local List to generate a network list based on routing entries on the Private interface.
Access Hours	List Name	von local actwork	Name of the Network List you are adding. The name possible priors
		whuTingerTigework	that of the Heriteria carry of the table in the set of angle.
	Network List	172.16.0.0/0.0.255.255	 Ealer the Networks and Wildrard masks using the following former: n.n.n.n/n.n.n.n (e.g. 10.10.0.000.255.255). Note: Enter a wildcard mask, which is the reverse of a submet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.000.0255 = all 10.10.1 mas addresses. Each bitrard and Wildcard mask match as atomic to a standard mask.
		<u>a</u>	Destructive and without since pair most of statements of a single line. The Wildcard mask may be omitted if the natural Wildcard mask is to be used.
	Apply	Concel Generate I	local List

5. このリストのネットワークはリモート ネットワークであり、手動で設定する必要がありま す。これを行うには、到達可能な各サブネットのネットワーク/ワイルドカードを入力しま

す。		
Configuration Interfaces Configuration Interfaces	Configuration Policy Management Traffic Management Network Lists Modify	
- CRUser Management	Modify a configured Network List. Click on Generate Local List to generate a network list based on routing entries on the Private interface.	
profic Monseement	List Name wpn_remote_network Name of the Network List you are adding. The same must be unique.	
- Cietvork Lists - Guida - SAs - Citaria - Cita	 192.168.20.0/0.0.0.255 Exter the Networks and Wildowid masks using the following format: a.m.n/n.n.n. (e.g. 10.10.0.00.0.255 253). Note: Exter a wildowid mask, which is the reverse of a subnet mask. wildowid mask has 16 in bit positions to ignore, 06 in bit positions to meth. For example, 10 10 10 00 0.0255 = all 10 10.1 non addresses. Each Network and Wildowid anak pair must be entered on a single line. The Wildowid must may be omitted if the natural Wildowid must is to be used. 	4
	Apply Cancel Generate Local List	

完了時の2つのネットワークリストは次のとおりです。

544	
Or User Management This section lets you add, modify, copy, and delete Network Lists Access Hours Click Add to create a Network List, or select a Network List and click Modify. Copy, or Delete. Hates Network List Access Hours VPN Client Local LAN (Default) Place Methods VPN Client Local LAN (Default) Place Methods VPN Client Local LAN (Default) Price Methods Vpn_local_network Add Modify Copy Delete	

 [Configuration] > [System] > [Tunneling Protocols] > [IPSec LAN-to-LAN] > [Add]を選択し、 LAN-to-LANトンネルを定義します。このウィンドウには3つのセクションがあります。上 部のセクションはネットワーク情報用で、下部の2つのセクションは Local および Remote ネットワーク リスト用です。Network Information セクションで、AES 暗号化、認証タイプ 、IKE プロポーザルを選択し、事前共有キーを入力します。下部のセクションで、すでに作 成した Network リスト (それぞれ Local リストと Remote リストの両方)を指定します。

- G Configuration				
	Configuration System Tunneling Protocols IPSec LAN-to-LAN Add			
- (#Servers	Add a new IPSec LAN-to-LAN connection			
Address Management				
PPTP	Enable 🗹	Check to enable this LAN-to-LAN connection.		
	Name best	Enter the name for this LAN-to-LAN connection.		
- ANIto LAN	Interface Ethernet 2 (Public) (20.20.20.1)	Select the interface for this LAN-to-LAN connection.		
<u></u>	Connection Type Bi-directional	Choose the type of LAN-to LAN connection. An Originate-Only connection may have multiple peers specified below.		
Akria 	30.30.30.1	Enter the remote peer IP addresses for this LAN-to-LAN connection. Originate- Days connection may specify up to ten peer IP addresses. Boter one IP address per line		
	Digini None (Use Preshared Keys) 💌	Subset the digital cartificate to use.		
-3-Monitoring	Certificate C Entire certificate clain. Transmission © Identity certificate only	Choose how to send the digital certificate to the DCE poor.		
	Preshared Key cisco123	Enter the preshared key for this LAN-to-LAN connection.		
	Authentication ESP/MD5/HMA0-128 -	Specify the packet authentication mechanism to use.		
Cisco Systems	Encryption AES-256 -	Specify the corryptica methanism to use.		
	IKE Proposal KE-AES256-SHA	Select the IKE Proposal to use for this LAN-to-LAN connection.		

- Denfiguration Interfaces - Distant		
-E-Servers		
E-Acidress Management		
- E- <u>Tunneling Protocols</u>		
	Filter -None-	Choose the filter to apply to the traffic that is transled through this L&N-to-LAN
		convection.
AN MARK		Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN
HE Processie	IPSer DAT-T	roaneritza ihaouga a NAT device. You noist also enable IFSec over NAT-T under
NAT Transporency		HAT I taisparancy.
Akris	Bandwidth Policy —None— 💌	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
- E-P Routing	Territor Manager	Choose the routing mechanism to use Parameters below are ignored if Network
- El-Management Protocols	Komag None	Autodiscovery is chosen.
- Events		-
- E-General	Local Network: If a LAN-to-LAN NAT rule is used, this is the Translat	led Network address.
-E-Client Update	Natural List was local actuask	Specify the local network address list or the IP address and wildcard mask for this
Lead Balancing	THE WARK DATE OF COLOR OF A DECK	LAN-to-LAN congestion.
- 99- <u>User Manaciement</u>	IF Address	
- Histov Manacement		Nois: Enter a wildcard mask, which is the ownerse of a submet mask. A
Access Hours	Wildcard Mask	wikirard mesk has 1s in bit positions to ignore, 0s is bit positions to realth. For
Weige states Materials		szaruple, 10.10.1.000.0.0.255 = all 10.10.1 mm addresses.
-Thûdministration		
Monitoring	Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remo	ite Network address.
	Network List vpn_remote_notwork	Specify the tenote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
	IP Address	
		Note: Enter a wildowid mask, which is the reverse of a subnet mask. A
	Wildcard Mask	vicesto mens ass is to or positione to grow, us to on positions to match. For ransple, 10.10 1 000.0.0.255 = al 10.10 1 mm addresses.
cisco Sistems	Add Concel	

 Add をクリックした後、接続が正しい場合、IPSec LAN-to-LAN-Add-Done ウィンドウが表示されます。このウィンドウにはトンネル設定情報の概要が表示されます。また、Group Name、SA Name、および Filter Name が自動的に設定されます。この表では任意のパラメータを編集できます。

Configuration	
	Configuration System Tunneling Protocols IPSec LAN-to-LAN Add Done
- D Systen	Save Needed
	An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:
PPTP	And an Annal Internal
L2TP	Superior administration of the second s
	Group 2020301
LANHO-LAN	Security Association 1.2.: test
KE Processis	rates Parts 12L bet Out
NAT Transparency	PLDCT Males 1.22. test In
- <u>Alertz</u>	
- CHP Routing	ModPring one of Boso have will effect the LAN-INLEN configuration. The Grean is the same as your LAN-INLAN near The Security Association and
- GPManagement Protocols	Files Rules all start with "L2Ls" to indicate that they from a LAN-to-LAN configuration.
- Cleventa	
- Gl-General	or 1
- Client Update	
Load Balancing	
- T-User Management	
EPolicy Management	
Administration	
→ Monitoring	

この時点で IPsec LAN-to-LAN トンネルが設定され、作業を開始できます。何らかの理由で トンネルが機能しない場合は設定ミスをチェックできます。

 以前に作成したLAN-to-LAN IPsecパラメータは、[Configuration] > [System] > [Tunneling Protocols] > [IPSec LAN-to-LAN]の順に選択すると表示または変更できます。次の図ではト ンネルの名前として「test」が表示され、またリモート エンドのパブリック インターフェイ スはシナリオに従って 30.30.30.1 となっています。

GConfiguration		
Interfaces	Configuration System Tunneling Protocols IPSec LAN-to-LAN	
- G -System		Save
- DServers		
	This section late you configure IPSec LAN-to-LAN connections LAN-to-LAN connections are as	tablished with other VPN 3000 Concentrators
	PIX frewalls, 7100/4000 series contexs and other IPSec-compliant security gateways. To configure	a VPN 3002 or other remote acress
<u>EPTP</u>	connection, go to User Management and configure a Group and User. To configure NAT over LAN	I-to-LAN, go to LAN-to-LAN NAT Rules.
L2TP		1.5
EHPSec	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.	,
KE Proposals		
NAT Transparency	Click the Add button to add a LAN-to-LAN connection, or select a connection and click Modify or	Delete.
<u>Alerts</u>	·	
- D Routing	(D) indicates a disabled LAN-to-LAN connection.	
Hitelanagement Protocols		
- Events	TAN + TAN	
- D <u>General</u>	Lan-to-Lan Connection	A-tioner
- Dient Update	Connection	Actions
Load Balancing	test (30.30.30.1) on Ethernet 2 (Public)	
E-User Management		Add
		2400
Access Hours		Modity
References		Delete
SA0		
Eller v		
TWAT		
EVU Policies		
- E Croup Metching		
Administration		

9. IKE プロポーザルが Inactive Proposals リスト内にある場合、時としてトンネルがアップ状態にならない場合があります。[Configuration] > [System] > [Tunneling Protocols] > [IPSec] > [IKE Proposals]を選択して、アクティブなIKEプロポーザルを設定します。IKE プロポーザルが「Inactive Proposals」リスト内にある場合、その IKE プロポーザルを選択して Activate ボタンをクリックすると、それを有効にできます。次の図では、選択されたプロポーザル「IKE-AES256-SHA」が Active Proposals リスト内にあります。

-DConfiguration					
Interfaces	Configuration System Tunneling Protocol	ls IPSec IKE Proposi	als		
				Save 🗖	
- I Servers					
Haddress Management	Add, delete, prioritize, and configure IKE Proposals.				
- G- <u>Tunneling Protocols</u>					
<u></u>	Select an Inactive Proposal and click Artistate to make it Artists, or click Modify. Conv or Delete as an opportate.				
	Select as Active Proposal and click Deactivate to make it	t Inactive, or click Move Up	or Move Down to change its priority.		
	Click Add or Copy to add a new Inactive Proposal. IKE	Proposals are used by Security	ity Associations to specify IKE parameters.		
LAN-10-LAN					
THE PERSONNEL	Active		Inactive		
Alerts	Proposals	Actions	Proposals		
- THP Bouling	CiscoVPNClient3DES-MD5		IKE-3DES-SHA-DSA	1	
Management Protocols	IKE-3DES-MD5	<< Activate	IKE-3DES-MD5-BSA-DH1		
- I Events	IKE-3DES-MD5-DH1	Departi vote a a	IKE-DES-MD5-DH7		
- II-General	IKE-DES-MD5	Descrivere vv	CiscoVPNClienF3DES-MD5-RSA		
- Client Update	IKE-3DES-MD5-DH7	Mave Up	CiscoVPNClient-3DES-SHA-DSA		
Load Balancing	CiscoVPNClient3DES-MD5-DH5		CiscoVPNClient-3DES-MD5-RSA-DH5		
	CiscoVPNClient-AES128-SHA	Move Down	CiscoVPNCliant-3DES-SHA-DSA-DH5		
	IKE-AES128-SHA	لماماد	CiscoVPNCliant-AES256-SHA		
Administration	IKE-3DES-MD5-RSA	Add			
• Monitoring	RE-AES256-SHA	Modify			
		Coov			
		Delete			
			1		

10. [Configuration] > [Policy Management] > [Traffic Management] > [Security Associations] の 順に選択し、SAパラメータが正しいことを確認します。



11. SA名をクリックします(この場合はL2L:test)を選択し、[Modify]をクリックしてSAを確認し ます。パラメータの一部がリモート ピアの設定と一致しない場合、ここで変更できます。

Configuration	Configuration Policy Management Traffic Manager	ment Security Associations Modify
	Modify a configured Security Association.	
- ED-Servers	, , , ,	
Address Management		
- DTurneling Protocols	SA Name L2L: test	Specify the more of this Security Association (SA).
EETE	Inheritance From Bule	Select the groundwite of this SA.
910-		
LAN-ID-LAN	IPSec Parameters	
HC Proposals	Authentication ESP/MD5/HMAC-128	Select the packet authentication elemithm to use
NAT Transparency	Algorithm	creet the period contraction appointed to dee.
<u>Alerts</u>	Encryption Algorithm AES-256	Select the ESP encryption algorithm to use.
- DP Routing		
EPManagement Protocols	Encapsulation Mode Tunnel	Select the Encapsulation Mode for this SA.
- Events	Perfect Forward	
- El-General	Serrecy Unsabled	solid the us of Polici Forward Sichery.
- Elent Update	Lifetime	
Losd Balancing	Measurement	Select the lifetime measurement of the IPSec Neys
- (Huser Management	Det. 146 days 10000	Const. C. A. 2011 (2011)
	Data Emetimie	aperny the data methos in succyses (into).
Access Hours	Time Lifetime 28800	Specify the time lifetime in seconds.
	20000	-{
Rideo	WITH D	
	IKE Parameters	
	Connection Type Hidrectional	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of
ran at	IKE Preus 30.30.30.1	a LAN-to-LAN Connection.
EX(Policies	Negotiation Mode Main	Select the IKE Negotiation mode to use
Group Matching ₩0 designation	Digital Certificate None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
E Maritanian		
E-manual and	Certificate C Batus certificate cham	Choose how to send the digital cartificate to the IKE coser.
	Transmission @ Identity certificate only	
	IKE Proposal IKE: AES256-SHA	 Select the IKE Proposal to use as IKE initiator.
CISCO SYSTEMS	Apply Concel	

<u>確認</u>

<u>ルータの設定の確認</u>

この項では、設定が正常に動作しているかどうかを確認する際に役立つ情報を紹介しています。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています(登録ユーザ専用)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

show crypto isakmp sa:現在ピアにあるすべての IKE SA を表示します。状態 QM_IDLE は、SA がピアと認証された状態であり、後続のクイック モードの交換に使用できることを示します。そのため、現在はアイドル状態にあります。
 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:現在の SA で使用されている設定を表示します。ピア IP アドレス、ローカルとリモートの両端のアクセスが可能なネットワーク、および使用されている変換セットをチェックします。2 つの ESP SA が、各方向に 1 つずつあります。AH 変換セットは使用されているため、空の状態です。
ipsec_router#show crypto ipsec sa

Ω

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: すべての暗号化エンジンの現在アクティブな暗号化 セッション接続を表示します。接続 ID はそれぞれ固有のものです。暗号化および復号化され るパケットの数が最後の2つのカラムに表示されます。

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>VPN コンセントレータの設定の確認</u>

VPN コンセントレータの設定を確認するには、次の手順を実行します。

 ルータ上のshow crypto ipsec saおよびshow crypto isakmp saコマンドと同様に、VPNコン セントレータでMonitoring > Statistics > IPSecを選択すると、IPSecおよびIKE統計情報を表 示できます。

	Monitoring Statistics IPSec		Thursday	.01 Ja	anuary 2004 19:32:36	
	mennennig Faranases fin and				Reset @ Refresh®	
	IKE (Phase 1) Statistics	IPSec (Phase 2) Statistics				
- Policy Management	Active Tunnels	L	Active Tunnels	1		
Access Hours	Total Tunnels	2	Total Tunnels	2		
Network Lists	Received Bytes	3545268	Received Bytes	36.02		
Rules	Sent Bytes	5553204	Sent Bytes	5376		
<u>SAs</u>	Received Packets	60187	Received Packets	145		
Eitera Eitera	Sent Packets	60299	Sent Packets	51		
BA/ Policies	Received Parkets Dropped	0	Received Parkets Dropped	0		
Group Matching	Sent Parkets Dropped	D	Received Parkets Dropped (Anti-Replay)	U		
- C-Administration	Received Notifies	60084	Sent Packets Dropped	0		
EKSoftware Undete	Seat Notifies	120172	Inhound Authentirations	145		
Consentrator	Received Phase-2 Eachanges	2	Failed Inbound Authentications	0		
Clients Surface Reheat	Sent Phase-2 Exchanges	49	Outhound Authentirations	St		
-Reboot Status	Invalid Phase-2 Exchanges Received	D	Failed Outbound Authentications	0		
Elba	Invalid Phase 2 Eachanges Sent	0	Decryptions	145		
Monitoring Retresh	Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0		
- Ele 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		
XML Export	Initiated Tunnels	0	No-SA Failures	0		
El Certificate Management	Failed initiated Tuanels	0	Protocol Use Failures	0		
Encolinient	Failed Remote Tunnels	0				
- Monitoring	Authentication Failures	0				
	Decryption Failures	D				
Dynamic Filtero	Hash Validation Failures	0				
Cisco Systems	System Capability Failures	0				
thuthu	No-SA Failures	0				

2. ルータ上の show crypto engine connections active コマンドと同じように、VPN コンセント レータ上の Administration-Sessions ウィンドウを使用すると、すべてのアクティブな IPsec LAN-to-LAN 接続またはトンネルのパラメータと統計を表示できます。

Configuration Interfaces DS225cn DUser Management Officier Management	Administration Ad	Iminister Ses	sions To refiect	the statistic	s dick Refresh	Selector G	innum ba fülter t	Thursday	y, 01 Janu Ri	uary 21 eset 🏑	104-19:30:2 Refresh@
- Actions Hours - Charlis Management - Name - Sag - Class - Sag - Class - Charl - Class - Charl - Class - Charles - Class - C	ca that season's name. T Group [-All- Legout All: <u>PPTP User</u> Session Summary	io log out a seast I L2TP User IP	on, chick Le Sec User [gent in the	tabla below. To to- <u>LAN</u>	test the net	work connecti	on to a seasion, cl	ick Ping.		a secondo vido
	Active LAN-to-	Active Remo	ie Acti	te Manage	ment Total	Artive H	Peak Concure	ent Conru	rrent	Total C	unsulative
	LAN SCRIPTS	and Access Sessions Session		Sessions	Sessions		Sessions	Session	S LINEIT	Sessions	
Concentrator											
Ciente	LAN-to-LAN Sessions [Reacto Access Sessions Management										
System Reboot Reboot Status	Connection Name	IP Address	Pro	iorel	Encryption	Lagia T	ine Dura	tion Bytes Tx	Bytes Rx		Sections
Ping	test	30.30.30.1	IPSecLA	N-to-LAN	AES-256	Jan 1 19:	57:29 0:02	:51 2128	2128	(Les	ant [Pilog]
Hontorina Setresti EAccess Martis EFile Management EContribute Management	ana Serest sa futz anazarat Brenete Arcess Sessions [LAN-20-LAN									nolocar	nt Sessions (
-Monitoring	Username	Assigned IP Ad Public IP Add	ddress Iress	Group	Protocol Encryptio	a Lo	gin Time Juration	Client Type Version	Bytes Bytes	: Tx : Rx	Artions
	No Remote Access Sessious										
Management Sessions [LAN-to-LAN See								aione Rema	ne [Remote Access Sessions]		
	Administrator	IP Addre	tas I	Protocol	Encryption	L	Login Time	Duratio	ian 🗌	Arti	0845
	admin.	172.161.2	нт	TP	None	Jan Ol	19:17:42	0:12:38	[100	out Pir	c)

<u>トラブルシュート</u>

ここでは、設定のトラブルシューティングに使用できる情報を示します。

<u>ルータのトラブルシューティング</u>

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

注: debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

- debug crypto engine 暗号化されたトラフィックを表示します。
 暗号化エンジンは、暗号化と復号化を実行する実際のメカニズムです。
 暗号化エンジンは、ソフトウェアであることも
 、あるいはハードウェア アクセラレータであることも可能です。
- **debug crypto isakmp**:IKEフェーズ1のInternet Security Association and Key Management Protocol(ISAKMP)ネゴシエーションを表示します。
- debug crypto ipsec:IKEフェーズ2のIPSecネゴシエーションを表示します。

詳細情報とサンプル出力については、『<u>IPSec のトラブルシューティング - debug コマンドの理</u> <u>解と使用</u>』を参照してください。

```
VPN コンセントレータのトラブルシューティング
```

Cisco ルータの debug コマンドと同様に、イベント クラスを設定してすべてのアラームを表示できます。

1. [Configuration] > [System] > [Events] > [Classes] > [Add] を選択して、イベントクラスのロ ギングをオンにします。IPsec に使用可能なクラスは次のとおりです。 IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE

Configuration						
<u>interfaces</u>	Configuration System Events Classes					
	Save Needed					
-ED <u>Servers</u>						
E Address Monogement	This section lets you configure special handling of specific event classes.					
EFTurneling Protocols						
EHP Routing	Click the Add button to add as event class, or select as event class and thick Modiffy or Delete.					
EPManacement Protocols	, -					
- DEvents	Click here to configure superal event parameters.					
General						
ETP Beckulo	Configurad					
	Consignment Provide Classes Actions					
- Irap Desgnaporis						
GVTD Servers	IKEDECODE					
Empl Recipionio	IPSEQUES					
The second	MB2TRAP Add					
-Fi-Client Undate						
Load Balancing	Modily					
- CHPolicy Management	Detete					
12:Monitoring						

 2. 上記のクラスを追加する際、アラームが送信される Severity レベルに基づいて、各クラスの Severity レベルを選択することもできます。アラームは、次のいずれかの方式により処理で きます。ログコンソール上での表示UNIX Syslog サーバへの送信電子メールとして送信 Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル)サーバ ヘトラップとして送信



<u>関連情報</u>

- Advanced Encryption Standard (AES)
- DES/3DES/AES VPN 暗号化モジュール
- ・<u>IPSec の設定例</u>
- <u>Cisco VPN 3000 シリーズ クライアントに関するサポート ページ</u>
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ