

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](#)

[トラブルシューティング](#)

[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](#)

概要

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、[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ださい](#)。

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、『[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、『[PIX 7.x と VPN 3000 コンセントレータの間の IPsec トンネルの設定例](#)』を参照してください。

前提条件

要件

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、『[IP Security \(IPsec \) 暗号化の概要](#)』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。

表記法

ドキュメント表記の詳細については、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

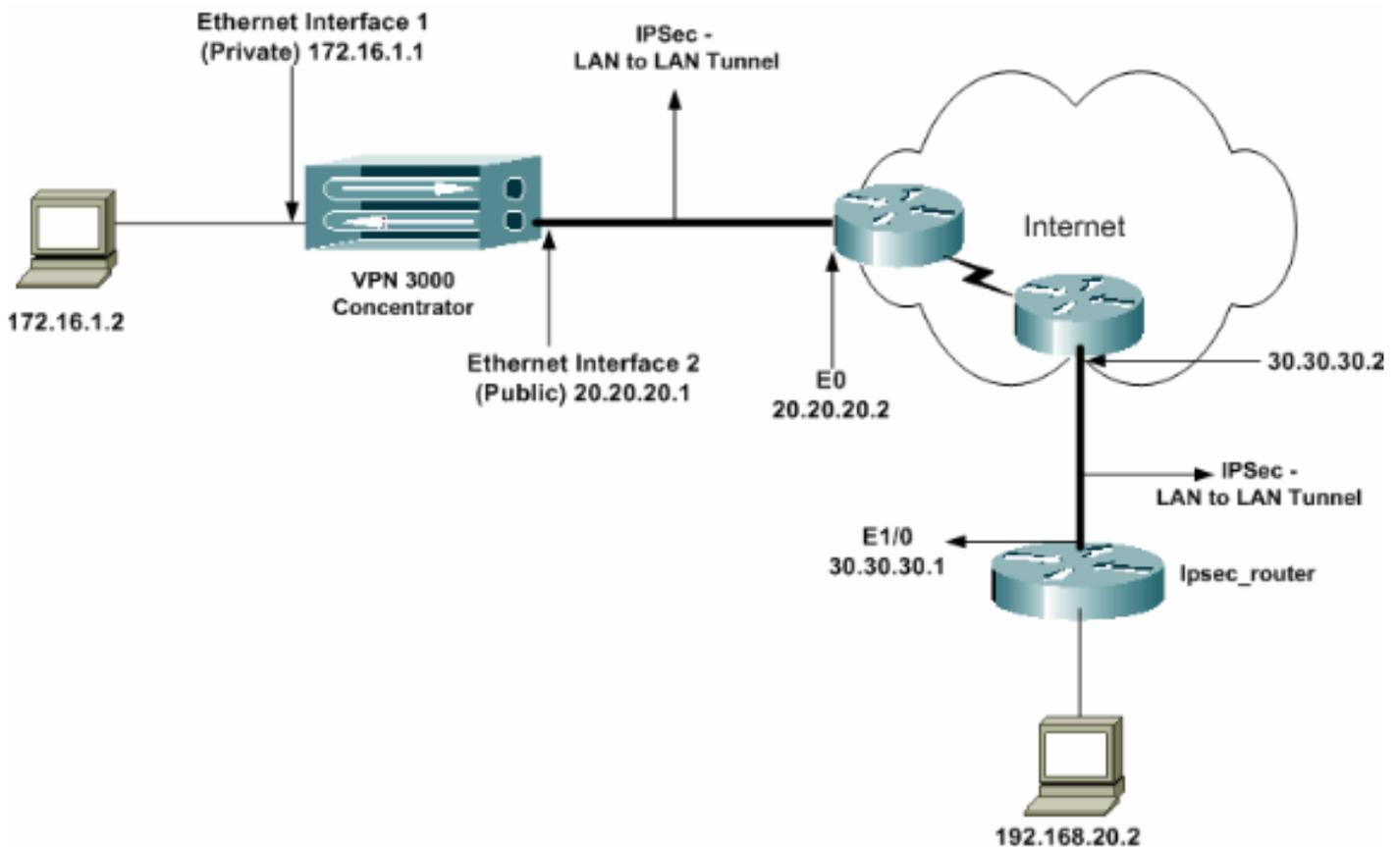
設定

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。

ネットワーク図

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。



設定

このドキュメントでは、次の構成を使用します。

- [IPSec ルータ](#)
- [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
!
!--- 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
!
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
```

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トिंग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、『[CLI を使用したクイックコンフィギュレーション](#)』を参照してください。

1. 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 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration Administration Monitoring

Main

Welcome to the VPN 3000 Concentrator Manager.

In the left frame or the navigation bar above, click the function you want:

- **Configuration** -- to configure all features of this device.
- **Administration** -- to control administrative functions on this device.
- **Monitoring** -- to view status, statistics, and logs on this device.

The bar at the top right has:

- **Main** -- to return to this screen.
- **Help** -- to get help for the current screen.
- **Support** -- to access VPN 3000 Concentrator support and documentation.
- **Logout** -- to log out of this session and return to the Manager login screen.

Under the location bar in the upper right, these icons may appear. Click to:

- **Save** -- save the active configuration and make it the boot configuration.
- **Save Needed** -- as above, indicating you have changed the active configuration.
- **Reset** -- to temporarily reset statistics to zero.
- **Restore** -- to restore statistics from their real values.
- **Refresh** -- to refresh 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 | Interfaces | Ethernet 2

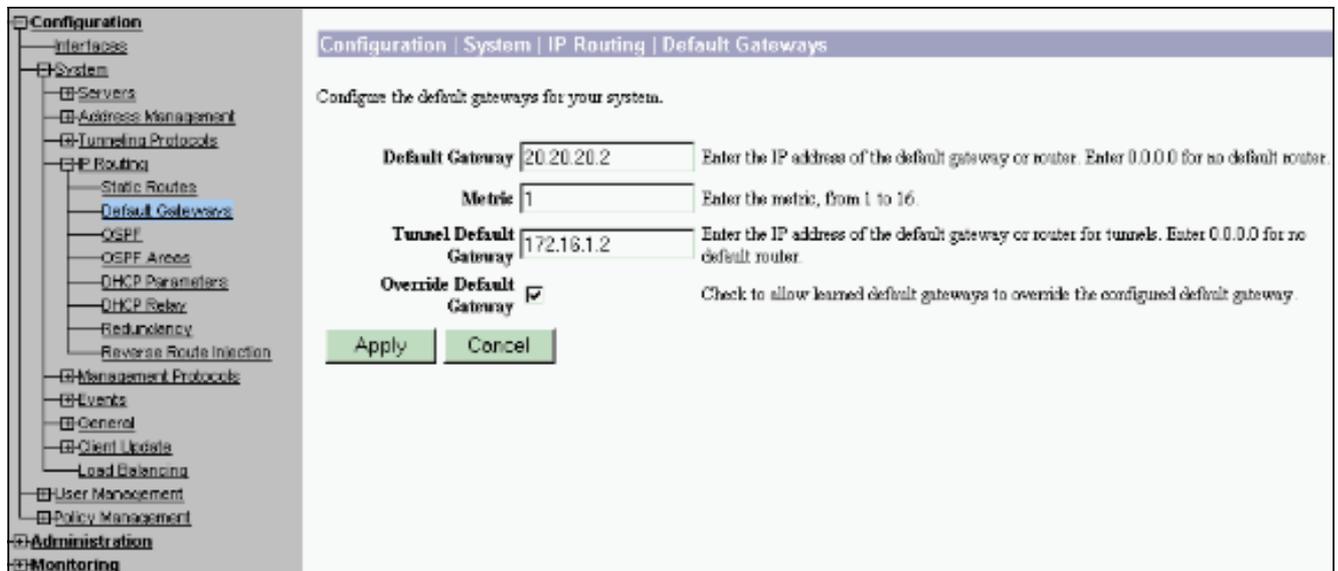
Configuring Ethernet Interface 2 (Public).

General RIP OSPF Bandwidth

General Parameters			
Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	20.20.20.1	
	Subnet Mask	255.255.255.0	
	Public Interface	<input checked="" type="checkbox"/>	Check to make this interface a "public" interface.
	MAC 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.
	MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	Public Interface IPsec Fragmentation Policy	<input checked="" type="radio"/> Do not fragment prior to IPsec encapsulation, fragment prior to interface transmission	
		<input type="radio"/> Fragment prior to IPsec encapsulation with Path MTU Discovery (ICMP)	
		<input type="radio"/> Fragment prior to IPsec encapsulation without Path MTU Discovery (Clear DF bit)	

Apply Cancel

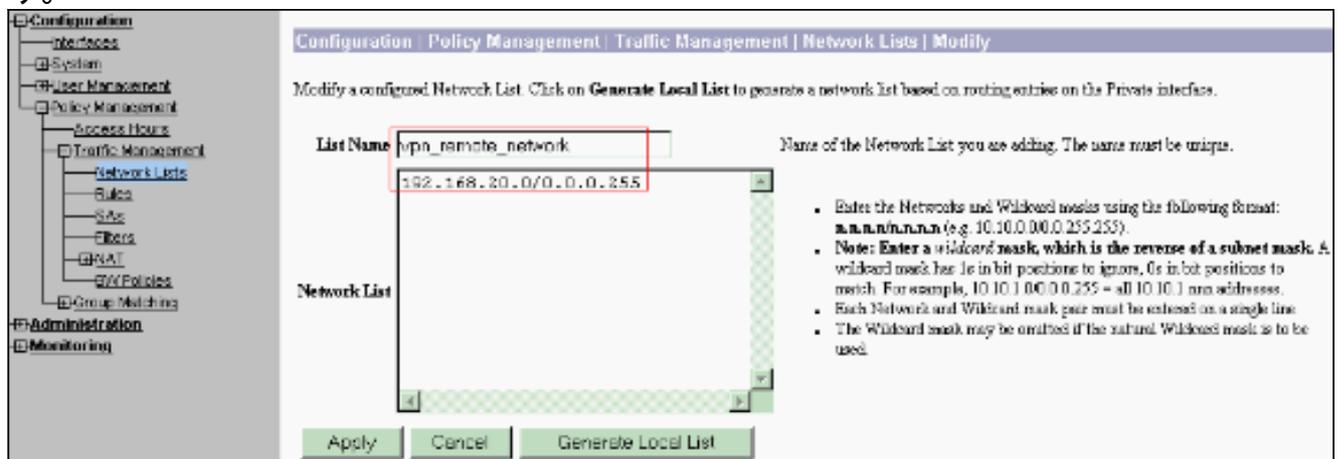
3. [Configuration] > [System] > [IP Routing] > [Default Gateways] を選択し、プライベートネットワーク内の他のサブネットに到達するために、IPSecのデフォルト（インターネット）ゲートウェイとトンネルデフォルト（内部）ゲートウェイを設定します。このシナリオでは、内部ネットワーク上では1つのサブネットのみ使用できます。



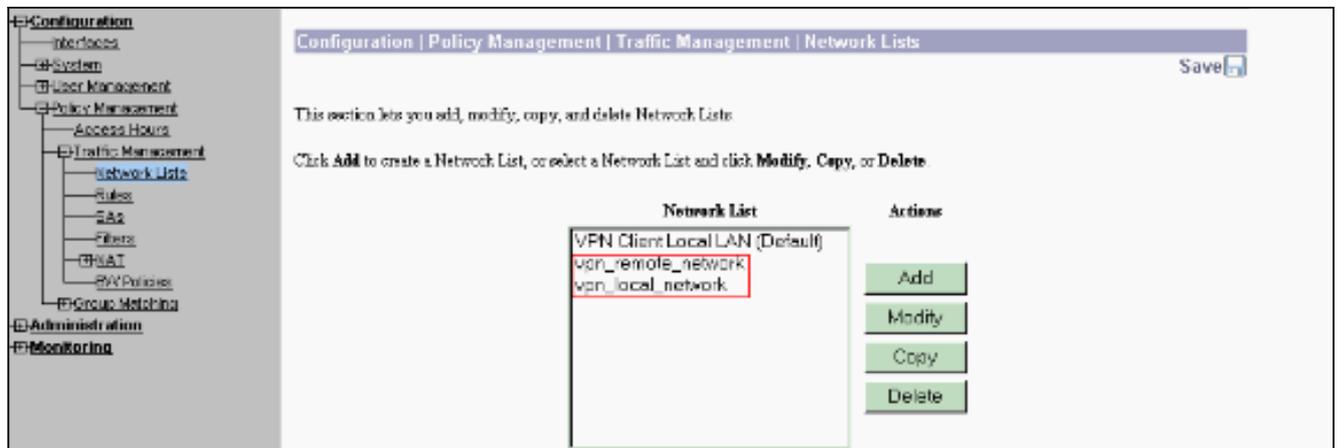
4. [Configuration] > [Policy Management] > [Traffic Management] > [Network Lists] > [Add] を選択し、暗号化するトラフィックを定義するネットワークリストを作成します。このリストに記載されているネットワークは、リモートネットワークに到達できます。次のリストに示されているネットワークが Local ネットワークです。Generate Local List をクリックすると、RIP を介して Local ネットワーク リストを自動的に生成することもできます。



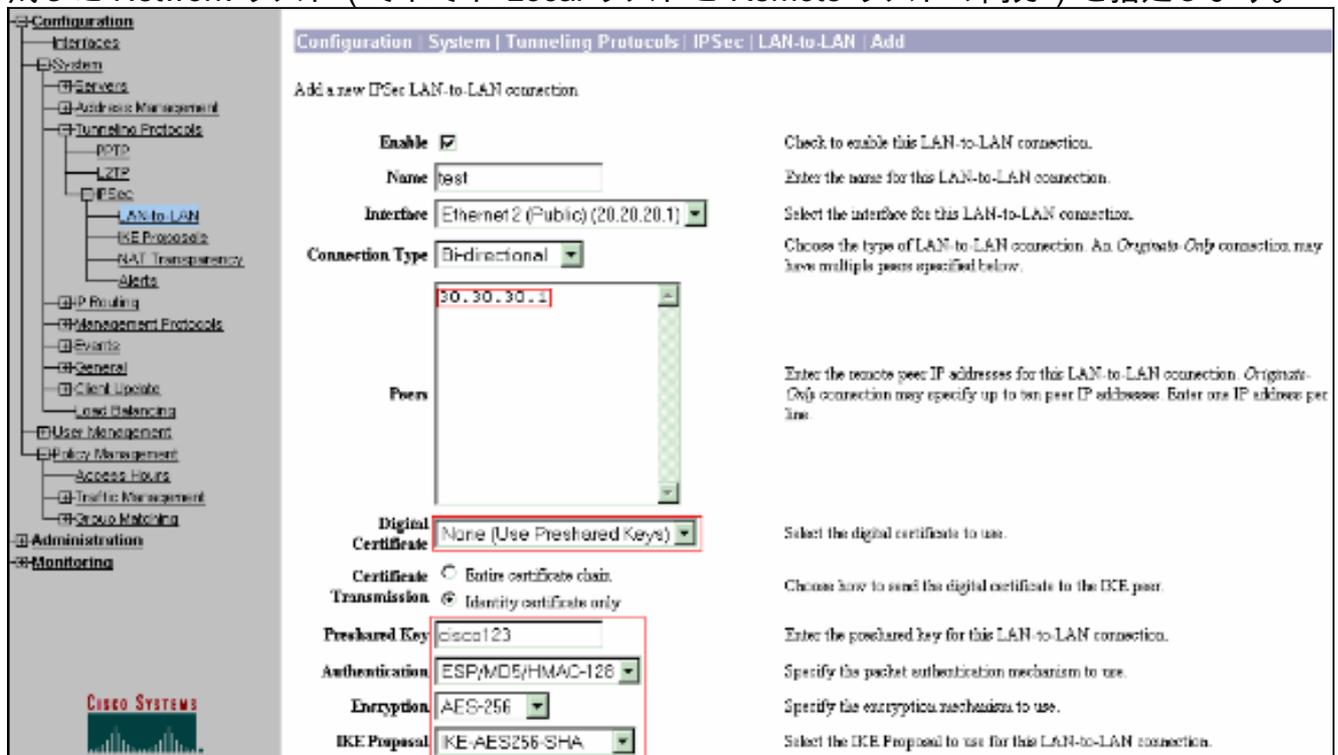
5. このリストのネットワークはリモートネットワークであり、手動で設定する必要があります。これを行うには、到達可能な各サブネットのネットワーク/ワイルドカードを入力します。

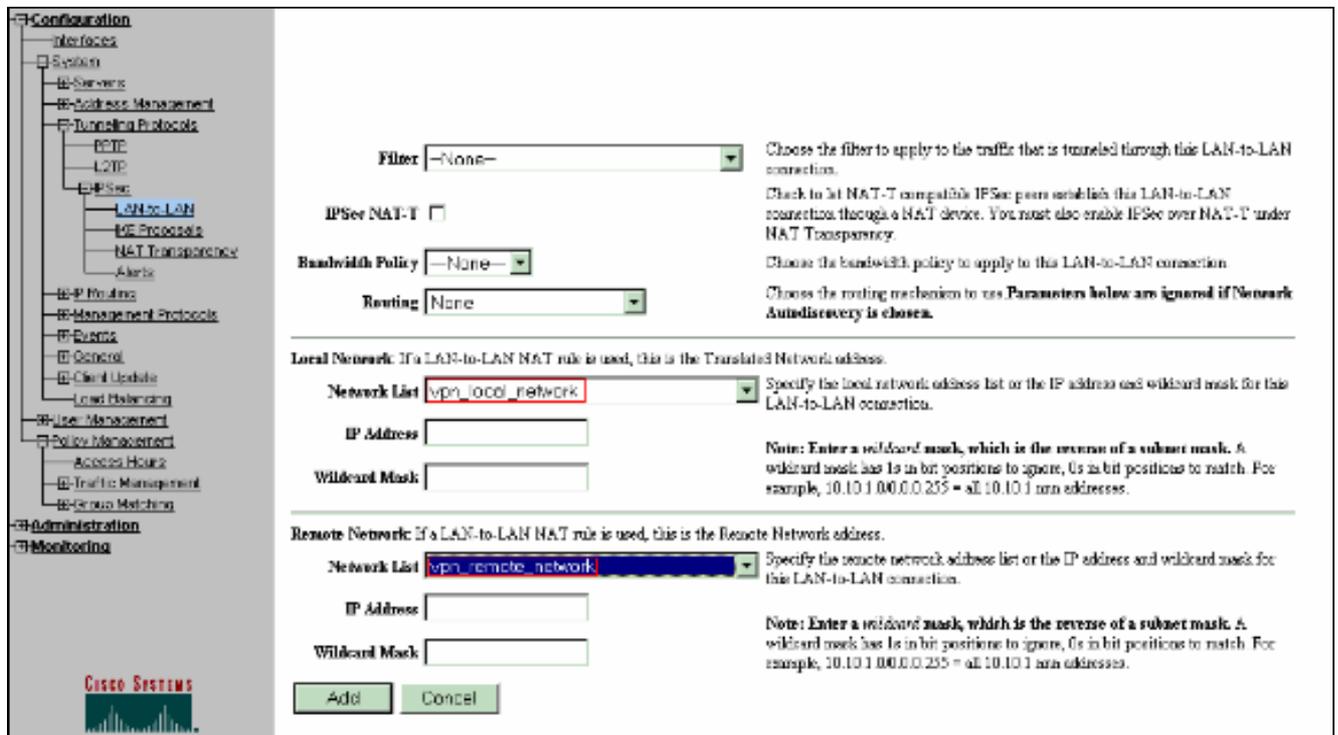


完了時の2つのネットワークリストは次のとおりです。

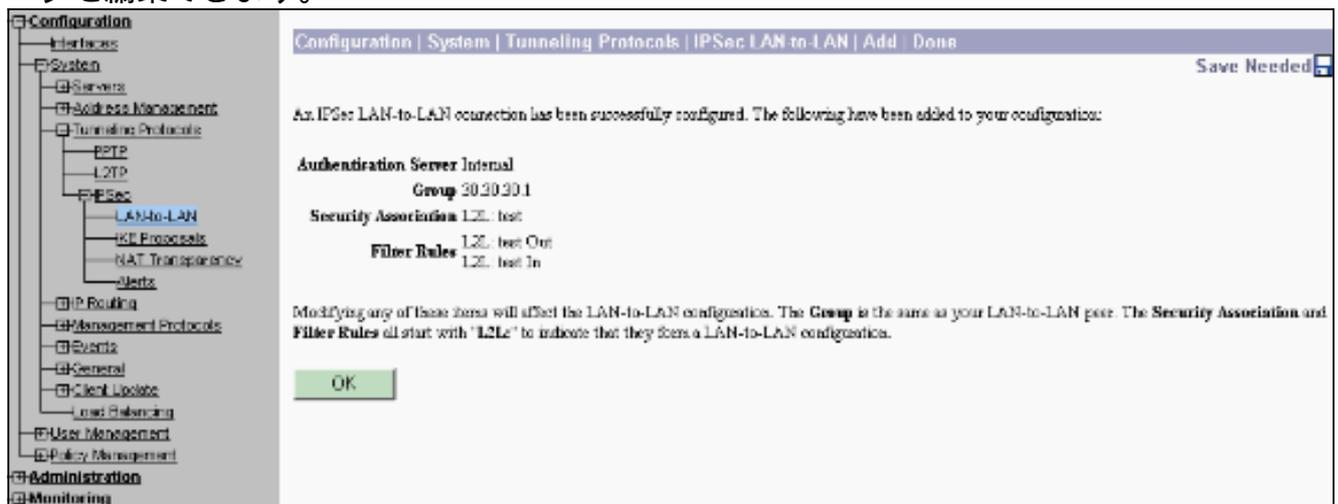


6. [Configuration] > [System] > [Tunneling Protocols] > [IPSec LAN-to-LAN] > [Add]を選択し、LAN-to-LANトンネルを定義します。このウィンドウには3つのセクションがあります。上部のセクションはネットワーク情報用で、下部の2つのセクションは Local および Remote ネットワーク リスト用です。Network Information セクションで、AES 暗号化、認証タイプ、IKE プロポーザルを選択し、事前共有キーを入力します。下部のセクションで、すでに作成した Network リスト (それぞれ Local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



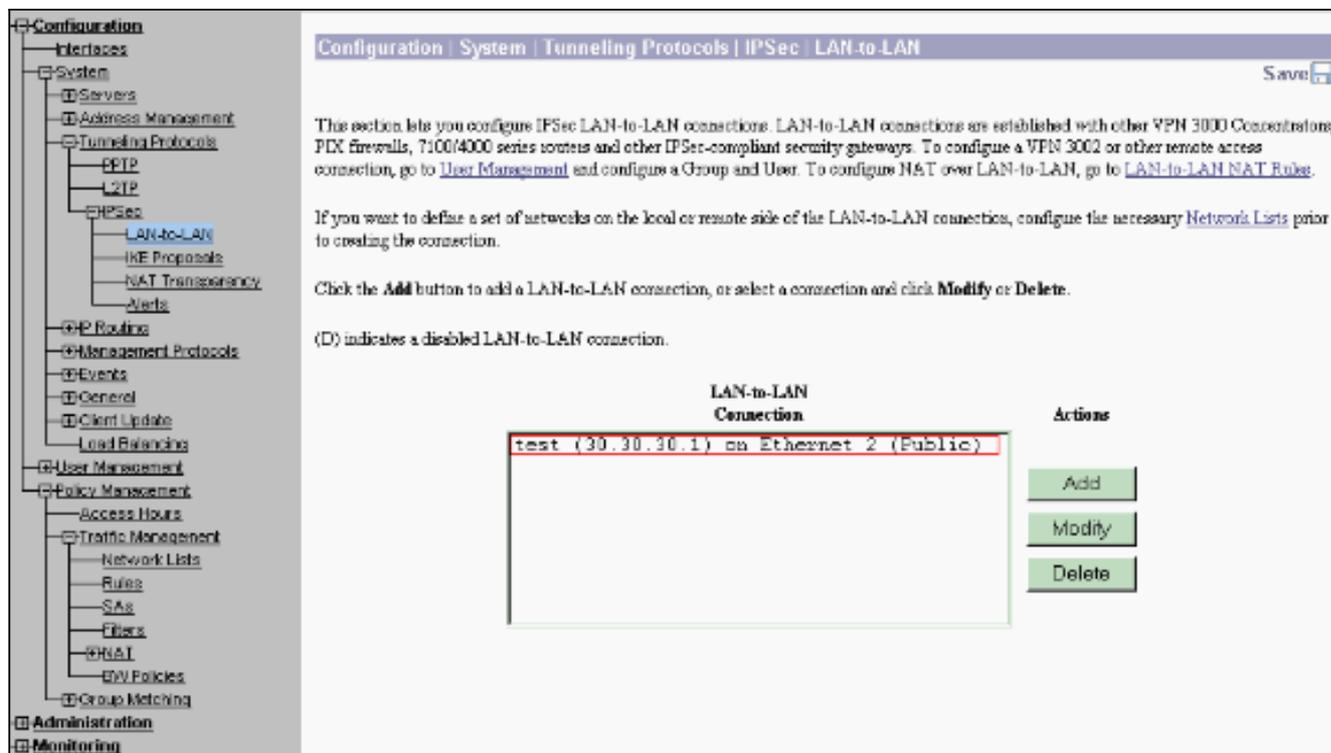


7. Add をクリックした後、接続が正しい場合、IPsec LAN-to-LAN-Add-Done ウィンドウが表示されます。このウィンドウにはトンネル設定情報の概要が表示されます。また、Group Name、SA Name、および Filter Name が自動的に設定されます。この表では任意のパラメータを編集できます。



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。

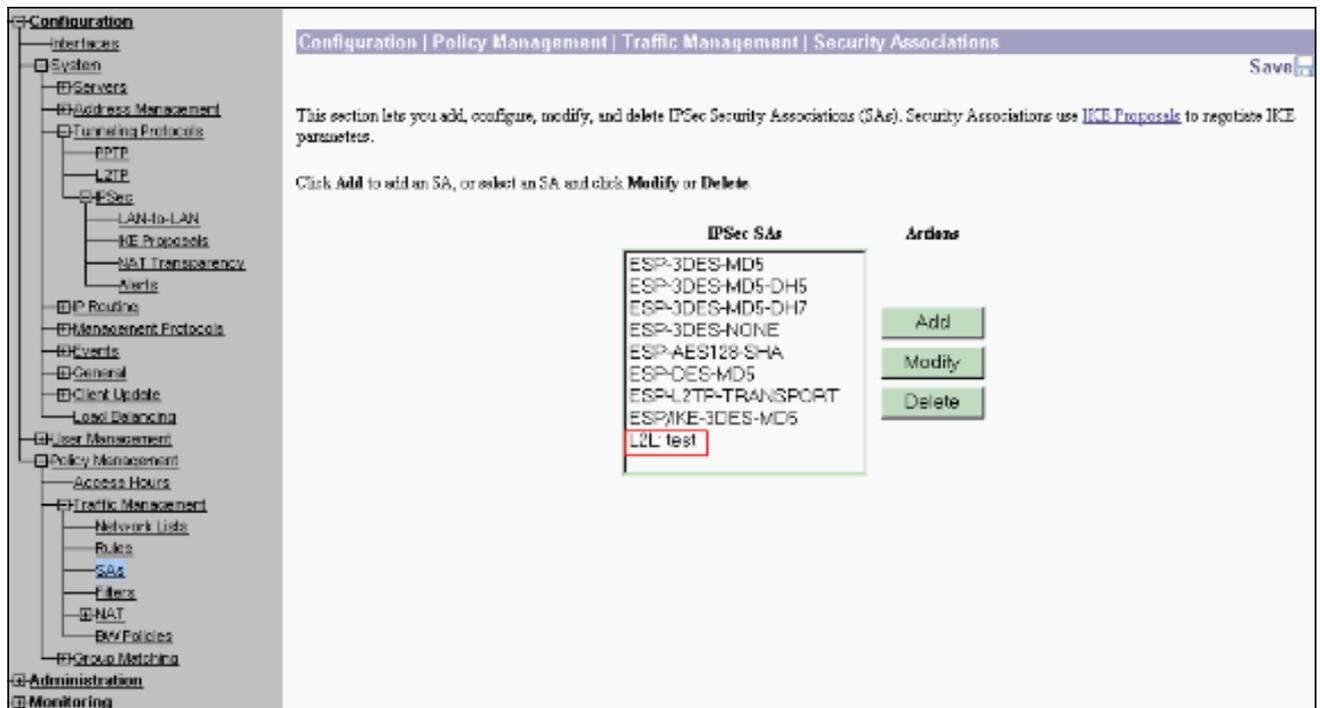
8. 以前に作成した LAN-to-LAN IPsec パラメータは、[Configuration] > [System] > [Tunneling Protocols] > [IPsec LAN-to-LAN] の順に選択すると表示または変更できます。次の図ではトンネルの名前として「test」が表示され、またリモートエンドのパブリックインターフェイスはシナリオに従って 30.30.30.1 となっています。



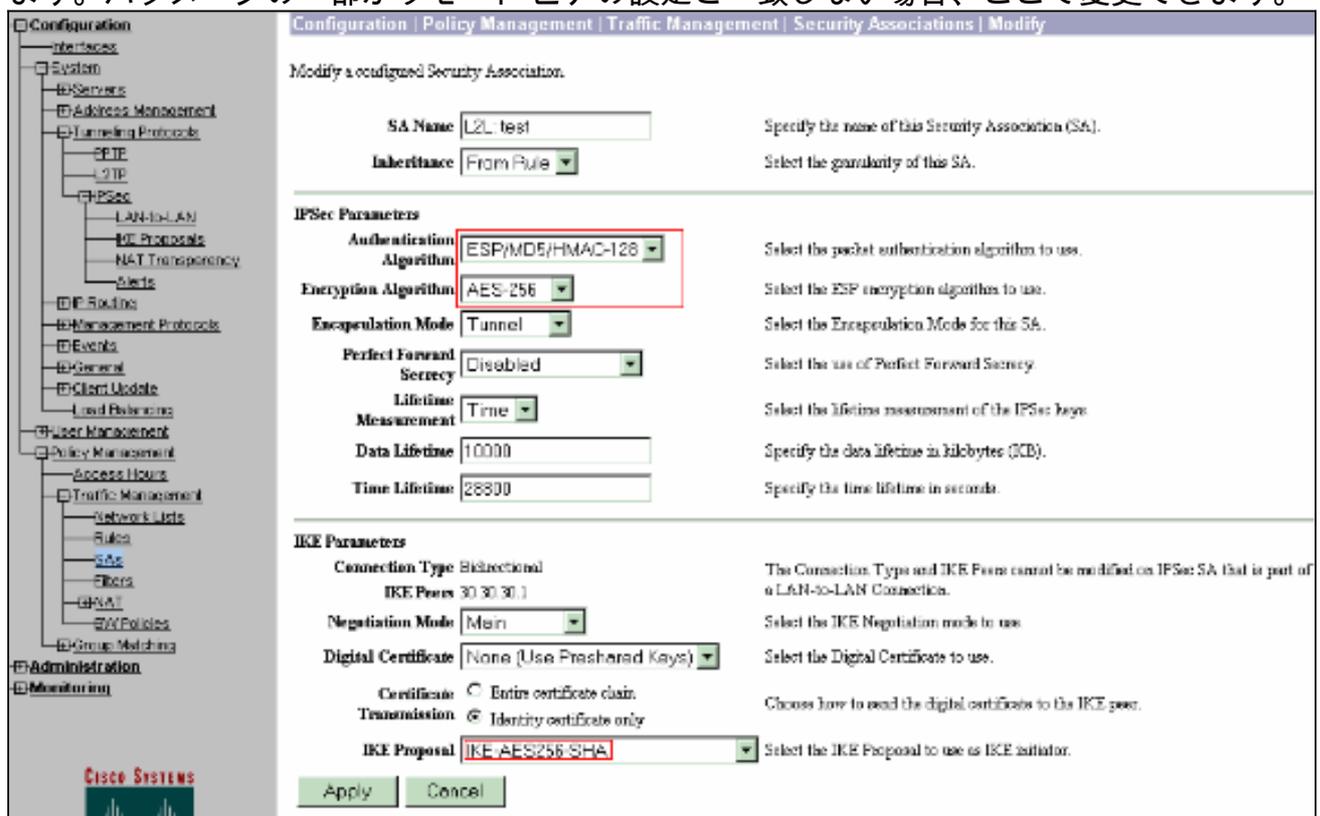
9. IKE プロポーザルが Inactive Proposals リスト内にある場合、時としてトンネルがアップ状態にならない場合があります。[Configuration] > [System] > [Tunneling Protocols] > [IPSec] > [IKE Proposals]を選択して、アクティブなIKEプロポーザルを設定します。IKE プロポーザルが「Inactive Proposals」リスト内にある場合、その IKE プロポーザルを選択して Activate ボタンをクリックすると、それを有効にできます。次の図では、選択されたプロポーザル「IKE-AES256-SHA」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



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。



確認

ルータの設定の確認

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          0
```

- **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
```

```
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、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

[VPN コンセントレータの設定の確認](#)

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。

1. 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。

IKE (Phase 1) Statistics		IPSec (Phase 2) Statistics	
Active Tunnels	1	Active Tunnels	1
Total Tunnels	2	Total Tunnels	2
Received Bytes	5545268	Received Bytes	5038
Sent Bytes	5553204	Sent Bytes	5376
Received Packets	60187	Received Packets	145
Sent Packets	60295	Sent Packets	51
Received Packets Dropped	0	Received Packets Dropped	0
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notifies	60084	Sent Packets Dropped	0
Sent Notifies	120172	Inbound Authentications	145
Received Phase-2 Exchanges	2	Failed Inbound Authentications	0
Sent Phase-2 Exchanges	49	Outbound Authentications	51
Invalid Phase-2 Exchanges Received	0	Failed Outbound Authentications	0
Invalid Phase-2 Exchanges Sent	0	Decryptions	145
Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0
Rejected Sent Phase-2 Exchanges	0	Encryptions	51
Phase-2 SA Delete Requests Received	0	Failed Encryptions	0
Phase-2 SA Delete Requests Sent	90	System Capability Failures	0
Initiated Tunnels	0	No SA Failures	0
Failed Initiated Tunnels	0	Protocol Use Failures	0
Failed Remote Tunnels	0		
Authentication Failures	0		
Decryption Failures	0		
Hash Validation Failures	0		
System Capability Failures	0		
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。

Administration Administer Sessions																							
<p>This screen shows statistics for sessions. To refresh the statistics, click Refresh. Select a Group to filter the sessions. For more information on a session, click on that session's name. To log out a session, click Logout in the table below. To test the network's connection to a session, click Ping.</p> <p>Group: <input type="text" value="-All-"/></p> <p>Logout All: PPTP User L2TP User IPSec User IPSec LAN-to-LAN</p>																							
<p>Session Summary</p> <table border="1"> <thead> <tr> <th>Active LAN-to-LAN Sessions</th> <th>Active Remote Access Sessions</th> <th>Active Management Sessions</th> <th>Total Active Sessions</th> <th>Peak Concurrent Sessions</th> <th>Concurrent Sessions Limit</th> <th>Total Cumulative Sessions</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0</td> <td>1</td> <td>2</td> <td>3</td> <td>400</td> <td>19</td> </tr> </tbody> </table>		Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions	1	0	1	2	3	400	19								
Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions																	
1	0	1	2	3	400	19																	
<p>LAN-to-LAN Sessions [Remove Access Sessions Management Sessions]</p> <table border="1"> <thead> <tr> <th>Connection Name</th> <th>IP Address</th> <th>Protocol</th> <th>Encryption</th> <th>Login Time</th> <th>Duration</th> <th>Bytes Tx</th> <th>Bytes Rx</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>test</td> <td>30.30.30.1</td> <td>IPSec:LAN-to-LAN</td> <td>AES-256</td> <td>Jan 1 19:37:29</td> <td>0:02:51</td> <td>2128</td> <td>2128</td> <td>[Logout] [Ping]</td> </tr> </tbody> </table>		Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	Actions	test	30.30.30.1	IPSec:LAN-to-LAN	AES-256	Jan 1 19:37:29	0:02:51	2128	2128	[Logout] [Ping]				
Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx	Actions															
test	30.30.30.1	IPSec:LAN-to-LAN	AES-256	Jan 1 19:37:29	0:02:51	2128	2128	[Logout] [Ping]															
<p>Remote Access Sessions [LAN-to-LAN Sessions Management Sessions]</p> <table border="1"> <thead> <tr> <th>Username</th> <th>Assigned IP Address</th> <th>Group</th> <th>Protocol</th> <th>Encryption</th> <th>Login Time</th> <th>Duration</th> <th>Client Type</th> <th>Bytes Tx</th> <th>Bytes Rx</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td colspan="11" style="text-align: center;">No Remote Access Sessions</td> </tr> </tbody> </table>		Username	Assigned IP Address	Group	Protocol	Encryption	Login Time	Duration	Client Type	Bytes Tx	Bytes Rx	Actions	No Remote Access Sessions										
Username	Assigned IP Address	Group	Protocol	Encryption	Login Time	Duration	Client Type	Bytes Tx	Bytes Rx	Actions													
No Remote Access Sessions																							
<p>Management Sessions [LAN-to-LAN Sessions Remote Access Sessions]</p> <table border="1"> <thead> <tr> <th>Administrator</th> <th>IP Address</th> <th>Protocol</th> <th>Encryption</th> <th>Login Time</th> <th>Duration</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>admin</td> <td>172.16.1.2</td> <td>HTTP</td> <td>None</td> <td>Jan 01 19:17:42</td> <td>0:12:38</td> <td>[Logout] [Ping]</td> </tr> </tbody> </table>		Administrator	IP Address	Protocol	Encryption	Login Time	Duration	Actions	admin	172.16.1.2	HTTP	None	Jan 01 19:17:42	0:12:38	[Logout] [Ping]								
Administrator	IP Address	Protocol	Encryption	Login Time	Duration	Actions																	
admin	172.16.1.2	HTTP	None	Jan 01 19:17:42	0:12:38	[Logout] [Ping]																	

トラブルシューティング

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。

ルータのトラブルシューティング

[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 コマンドをサポートします。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、『[IPsec のトラブルシューティング - debug コマンドの理解と使用](#)』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

Configured Event Classes	Actions
IKEDECODE	Add Modify Delete
IPSECDEBG	
MIB2TRAP	

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) サーバへトラップとして送信

Configuration | System | Events | Classes | Add

This screen lets you add and configure an event class for special handling.

Class Name: Select the event class to configure.

Enable: Check to enable special handling of this class.

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.
Changing a value set to Use Event List will override the sections of the Event List referring to this event class.

Events to Log: Select the events to enter in the log.

Events to Console: Select the events to display on the console.

Events to Syslog: Select the events to send to a Syslog Server.

Events to Email: Select the events to send to an Email Recipient.

Events to Trap: Select the events to send to an SNMP Trap Destination.

3. [Monitoring] > [Filterable Event Log] を選択して、有効なアラームを監視します。

Monitoring | Filterable Event Log

Select Filter Options

Event Class: Severities:

Client IP Address: Events/Page:

Group: Direction:

```

37992 01/02/2004 11:58:28.540 SEV=F IKEDECODE/0 RPT=61037 30.30.30.1
ISAKMP HEADER : ( Version 1.0 )
Initiator Cookie(S):  A8 A8 8C 63 09 CA 55 25
Responder Cookie(S):  C8 B2 66 02 86 CD 12 6C
Next Payload :  HASH (8)
Exchange Type :  Oakley Informational
Flags :  1 (REQRYP1)
Message ID :  a3980cad
Length :  92

37999 01/02/2004 11:58:28.540 SEV=F IKEDECODE/0 RPT=61037 30.30.30.1
Notify Payload Decode :
DOT :  TP88C (1)
Protocol :  ISAKMP (1)
Message :  DPD 3-U-THEERE-ACK (96137)
Spi :  A8 A8 8C 63 09 CA 55 25 C8 B2 66 02 86 CD 12 6C
Length :  32

38005 01/02/2004 11:58:48.540 SEV=F IKEDECODE/0 RPT=61037 30.30.30.1
ISAKMP HEADER : ( Version 1.0 )
Initiator Cookie(S):  A8 A8 8C 63 09 CA 55 25
Responder Cookie(S):  C8 B2 66 02 86 CD 12 6C
Next Payload :  HASH (8)
Exchange Type :  Oakley Informational

```

関連情報

- [Advanced Encryption Standard \(AES \)](#)
- [DES/3DES/AES VPN 暗号化モジュール](#)
- [IPSec の設定例](#)
- [Cisco VPN 3000 シリーズ クライアントに関するサポート ページ](#)
- [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](#)