

Cisco ルータへの Cisco VPN 3000 コンセントレータの設定

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](#)

[インターフェイス設定です。](#)

[VPN コンセントレータ上で使用する場合](#)

[トラブルシュート](#)

[インターフェイス設定です。](#)

[問題：トンネルを開始できない](#)

[PFS](#)

[関連情報](#)

概要

この設定例では、Cisco IOS® ソフトウェアを実行するルータの背後にあるプライベート ネットワークを Cisco VPN 3000 コンセントレータの背後にあるプライベート ネットワークに接続する方法を示します。ネットワーク上のデバイスは、プライベート アドレスによって互いを認識します。

前提条件

要件

このドキュメントに特有の要件はありません。

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いています。

- Cisco IOSソフトウェアリリース12.3.(1)aが稼働するCisco 2611ルータ注：Cisco 2600シリー

ズルータに、VPN機能をサポートする暗号化IPsec VPN IOSイメージがインストールされていることを確認してください。

- Cisco VPN 3000コンセントレータ(4.0.1 B)

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。

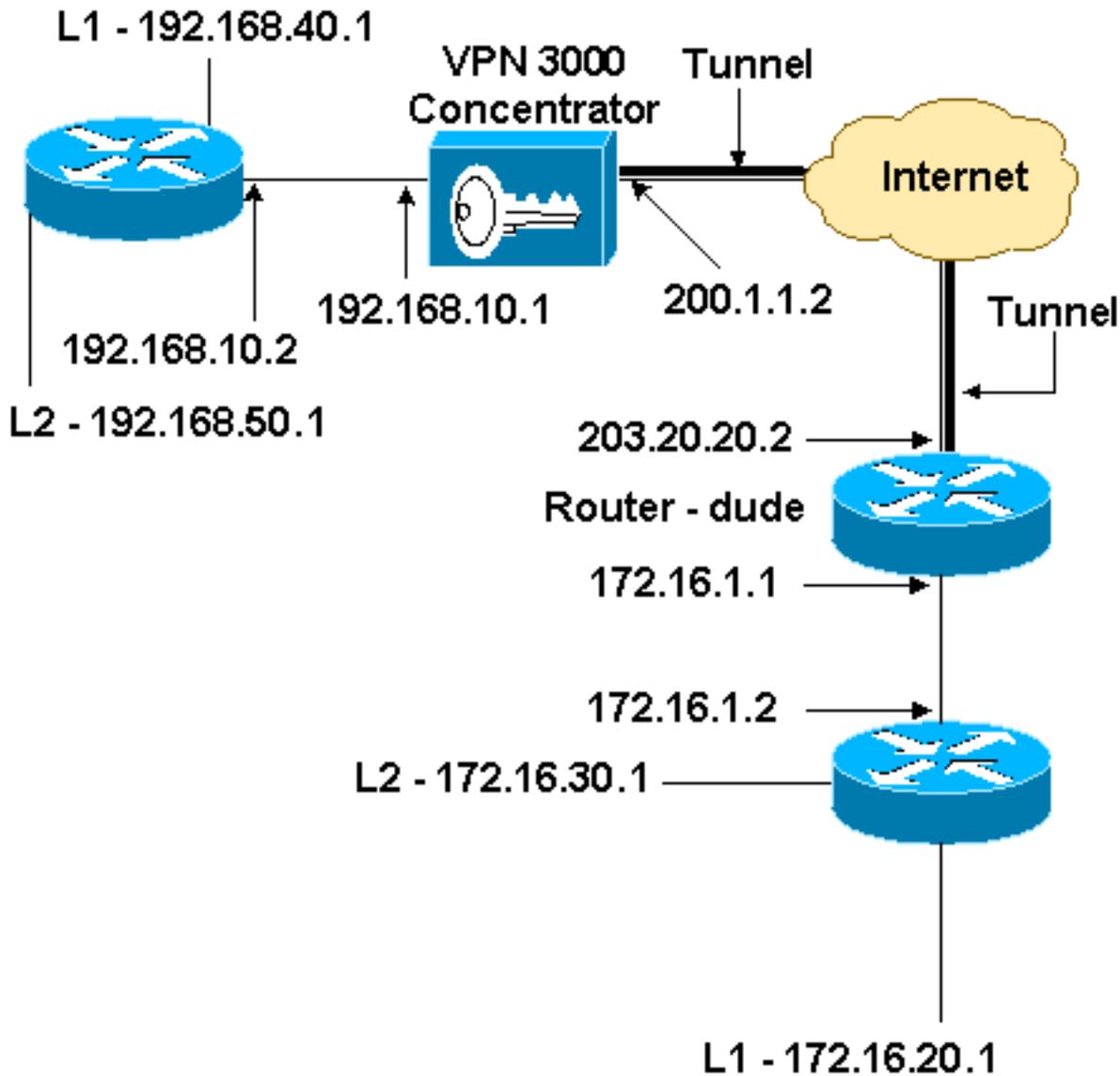
設定

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：このドキュメント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](#)) を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク設定を使用します。



設定

このドキュメントでは次の設定を使用します。

ルータの設定

```

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 200.1.1.2

```

```
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
  set peer 200.1.1.2
  set transform-set to_vpn
!!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
  ip address 203.20.20.2 255.255.255.0
  ip nat outside
  half-duplex
  crypto map to_vpn
!
interface Ethernet0/1
  ip address 172.16.1.1 255.255.255.0
  ip nat inside
  half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 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 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!!--- Traffic to except from the NAT process. access-list
110 deny ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
```

```
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

VPN コンセントレータの設定

このラボ設定では、最初にコンソールポートからVPNコンセントレータにアクセスし、最小限の設定を追加して、さらに詳細な設定をグラフィカルユーザインターフェイス(GUI)で行うことができます。

[Administration] > [System Reboot] > [Schedule reboot] > [Reboot with Factory/Default Configuration] を選択して、VPNコンセントレータに既存の設定がないことを確認します。

VPNコンセントレータが[Quick Configuration]に表示され、リポート後に次の項目が設定されます。

- 時間/日付
- Configuration Interfaces (パブリックアドレス = 200.1.1.2/24、プライベートアドレス = 192.168.10.1/24) でのインターフェイス/マスク
- Configuration > System > IP routing > Default_Gateway (200.1.1.1) のデフォルトゲートウェイ

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を介してアクセスできません。

注：VPNコンセントレータは外部から管理されているため、次の項目も選択する必要があります。

- [Configuration] > [Interfaces] > 2-public > [Select IP Filter] > [1. Private (Default)]。
- [Administration] > [Access Rights] > [Access Control List] > [Add Manager Workstation] を選択して、外部マネージャのIPアドレスを追加します。

これは、外部からVPNコンセントレータを管理しない限り必要ありません。

1. GUIを起動した後にインターフェイスを再確認するには、[Configuration] > [Interfaces] を選択します。

Configuration | Interfaces Thursday, 03 July 2003 14:04:38
Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

| Interface | Status | IP Address | Subnet Mask | MAC Address | Default Gateway |
|-----------------------|---------------------------|--------------|---------------|-------------------|-----------------|
| Ethernet 1 (Private) | UP | 192.168.10.1 | 255.255.255.0 | 00.03.A0.88.00.7D | |
| Ethernet 2 (Public) | UP | 200.1.1.2 | 255.255.255.0 | 00.03.A0.88.00.7E | 200.1.1.1 |
| Ethernet 3 (External) | Not Configured | 0.0.0.0 | 0.0.0.0 | | |
| DNS Server(s) | DNS Server Not Configured | | | | |
| DNS Domain Name | | | | | |

• Power Supplies

2. [Configuration] > [System] > [IP Routing] > [Default Gateways] を選択し、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て、プライベートネットワーク内の他のサブネットに到達します。

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Tunnel Default Gateway Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.

Override Default Gateway Check to allow learned default gateways to override the configured default gateway.

3. [Configuration] > [Policy Management] > [Network Lists] 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。ローカルネットワークは次のとおりです。

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.

List Name Name of the Network List you are adding. The name must be unique.

Network List

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

リモートネットワークは次のとおりです。

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.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

```
172.16.1.0/0.0.0.255
172.16.20.0/0.0.0.255
172.16.30.0/0.0.0.255
```

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Apply Cancel Generate Local List

4. 完了時の2つのネットワークリストは次のとおりです。注：IPSecトンネルがアップしない場合は、対象トラフィックが両側で一致するかどうかを確認します。対象トラフィックは、ルータとPIXボックスのアクセスリストによって定義されます。これらは、VPNコンセントレータのネットワークリストによって定義されます。

Configuration | Policy Management | Traffic Management | Network Lists

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

| Network List | Actions |
|--------------------------------|---|
| VPN Client Local LAN (Default) | <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/> |
| vpn_local_subnet | |
| router_subnet | |

5. [Configuration] > [System] > [Tunneling Protocols] > [IPSec LAN-to-LAN]の順に選択し、LAN-to-LANトンネルを定義します。

Add a new IPSec LAN-to-LAN connection.

| | |
|--|--|
| <p>Enable <input checked="" type="checkbox"/></p> <p>Name <input type="text" value="to_router"/></p> <p>Interface <input type="text" value="Ethernet2 (Public) (200.1.1.2)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> <p>203.20.20.2</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate <input type="radio"/> Entire certificate chain</p> <p>Transmission <input checked="" type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text" value="cisco123"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p> | <p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p> |
| <p>Filter <input type="text" value="-None-"/></p> <p>IPSec NAT-T <input type="checkbox"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="None"/></p> | <p>Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.</p> <p>Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.</p> |
| <p>Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p>Network List <input type="text" value="vpn_local_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p> | |
| <p>Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p>Network List <input type="text" value="router_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p> | |
| <p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p> | |

6. [Apply] をクリックすると、LAN-to-LANトンネル設定の結果として自動的に作成される他の

設定が表示されます。

Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN | Add | Done Save Needed

An IPsec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:

Authentication Server Internal
Group 203.20.20.2
Security Association L2L: to_router
Filter Rules L2L: to_router Out
L2L: to_router In

Modifying any of these items will affect the LAN-to-LAN configuration. The **Group** is the same as your LAN-to-LAN peer. The **Security Association** and **Filter Rules** all start with "L2L:" to indicate that they form a LAN-to-LAN configuration.

OK

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]で表示または変更できます。

Configuration | System | Tunneling Protocols | IPsec | LAN-to-LAN Save Needed

This section lets you configure IPsec LAN-to-LAN connections. LAN-to-LAN connections are established with other VPN 3000 Concentrators, PIX firewalls, 7100/4000 series routers and other IPsec-compliant security gateways. To configure a VPN 3002 or other remote access connection, go to [User Management](#) and configure a Group and User. To configure NAT over LAN-to-LAN, go to [LAN-to-LAN NAT Rules](#).

If you want to define a set of networks on the local or remote side of the LAN-to-LAN connection, configure the necessary [Network Lists](#) prior to creating the connection.

Click the **Add** button to add a LAN-to-LAN connection, or select a connection and click **Modify** or **Delete**.

(D) indicates a disabled LAN-to-LAN connection.

| LAN-to-LAN Connection | Actions |
|--|--|
| to_router (203.20.20.2) on Ethernet 2 (Public) | <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> |

- [Configuration] > [System] > [Tunneling Protocols] > [IPsec] > [IKE Proposals] を選択して、アクティブなIKEプロポーザルを確認します。

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **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 Associations](#) to specify IKE parameters.

| Active Proposals | Actions | Inactive Proposals |
|-----------------------------|---------------|---------------------------------|
| CiscoVPNClient-3DES-MD5 | << Activate | IKE-3DES-SHA-DSA |
| IKE-3DES-MD5 | Deactivate >> | IKE-3DES-MD5-RSA-DH1 |
| IKE-3DES-MD5-DH1 | Move Up | IKE-DES-MD5-DH7 |
| IKE-DES-MD5 | Move Down | CiscoVPNClient-3DES-MD5-RSA |
| IKE-3DES-MD5-DH7 | Add | CiscoVPNClient-3DES-SHA-DSA |
| IKE-3DES-MD5-RSA | Modify | CiscoVPNClient-3DES-MD5-RSA-DH5 |
| CiscoVPNClient-3DES-MD5-DH5 | Copy | CiscoVPNClient-3DES-SHA-DSA-DH5 |
| CiscoVPNClient-AES128-SHA | Delete | CiscoVPNClient-AES256-SHA |
| IKE-AES128-SHA | | IKE-AES256-SHA |

8. [Configuration] > [Policy Management] > [Traffic Management] > [Security Associations] の順に選択して、セキュリティアソシエーションのリストを表示します。

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

| IPSec SAs | Actions |
|--------------------|-------------------------|
| ESP-3DES-MD5 | Add Modify Delete |
| ESP-3DES-MD5-DH5 | |
| ESP-3DES-MD5-DH7 | |
| ESP-3DES-NONE | |
| ESP-AES128-SHA | |
| ESP-DES-MD5 | |
| ESP-L2TP-TRANSPORT | |
| ESP/IKE-3DES-MD5 | |
| L2L: to_router | |

9. セキュリティアソシエーション名をクリックし、次に[Modify]をクリックしてセキュリティアソシエーションを確認します。

| | | |
|---------------------------------|--|---|
| SA Name | <input type="text" value="L2L: to_router"/> | Specify the name of this Security Association (SA). |
| Inheritance | <input type="text" value="From Rule"/> | Select the granularity of this SA. |
| IPSec Parameters | | |
| Authentication Algorithm | <input type="text" value="ESP/MD5/HMAC-128"/> | Select the packet authentication algorithm to use. |
| Encryption Algorithm | <input type="text" value="3DES-168"/> | Select the ESP encryption algorithm to use. |
| Encapsulation Mode | <input type="text" value="Tunnel"/> | Select the Encapsulation Mode for this SA. |
| Perfect Forward Secrecy | <input type="text" value="Disabled"/> | Select the use of Perfect Forward Secrecy. |
| Lifetime Measurement | <input type="text" value="Time"/> | Select the lifetime measurement of the IPSec keys. |
| Data Lifetime | <input type="text" value="10000"/> | Specify the data lifetime in kilobytes (KB). |
| Time Lifetime | <input type="text" value="28800"/> | Specify the time lifetime in seconds. |
| IKE Parameters | | |
| Connection Type | Bidirectional | The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection. |
| IKE Peers | 203.20.20.2 | |
| Negotiation Mode | <input type="text" value="Main"/> | Select the IKE Negotiation mode to use. |
| Digital Certificate | <input type="text" value="None (Use Preshared Keys)"/> | Select the Digital Certificate to use. |
| Certificate Transmission | <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only | Choose how to send the digital certificate to the IKE peer. |
| IKE Proposal | <input type="text" value="IKE-3DES-MD5"/> | Select the IKE Proposal to use as IKE initiator. |

確認

このセクションでは、この設定で使用されるshowコマンドをリストします。

インターフェイス設定です。

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。

[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。

- **show crypto ipsec sa** : 現在のセキュリティアソシエーションで使用されている設定を表示します。
- **show crypto isakmp sa** : ピアにおける現在のInternet Key Exchange (IKE ; インターネット鍵交換) セキュリティアソシエーション(SA)をすべて表示します。
- **show crypto engine connection 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。

[IOS Command Lookup Tool \(登録ユーザ専用\)](#) を使用して、特定の[コマンドに関する](#)詳細情報を確認できます。

VPN コンセントレータ上で使用する場合

[Configuration] > [System] > [Events] > [Classes] > [Modify]の順に選択して、ロギングをオンにし

ます。次のオプションを使用できます。

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

ログに対する重大度 = 1 ~ 13

コンソールに対する重大度 = 1 ~ 3

[Monitoring] > [Event Log]を選択し、イベントログを取得します。

トラブルシュート

インターフェイス設定です。

debugコマンドを試す前に、『[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。
- debug crypto ipsec : フェーズ 2 の IPsec ネゴシエーションを表示します。
- debug crypto isakmp : フェーズ 1 の ISAKMP ネゴシエーションを表示します。

問題：トンネルを開始できない

エラー メッセージ

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

解決方法

このSAに対して必要な同時ログイン数を設定するか、同時ログイン数を5に設定するには、次の操作を実行します。

[Configuration] > [User Management] > [Groups] > [Modify 10.19.187.229] > [General] > [Simultaneous Logins]に移動し、ログイン数を5に変更します。

PFS

IPSec のネゴシエーションでは、Perfect Forward Secrecy (PFS; 完全転送秘密) によって、それぞれの新しい暗号鍵が以前の鍵とは独立したものであることが保証されます。両方のトンネルピアでPFSを有効または無効にします。そうでない場合、LAN-to-LAN(L2L)IPsecトンネルはルータで確立されません。

この暗号マップエントリに対して新しいセキュリティアソシエーション(SA)が要求されたときに、IPSecがPFSを要求するように指定するには、暗号マップ設定モードでset pfsコマンドを使用し

ます。IPSecがPFSを要求しないように指定するには、このコマンドのno形式を使用します。

```
set pfs [group1 | group2]
```

```
no set pfs
```

set pfs コマンドについて：

- *group1*：新しいDiffie-Hellman交換の実行時に、IPSecで768ビットのDiffie-Hellmanプライムモジュラスグループを使用するように指定します。
- *group2*：新しいDiffie-Hellman交換の実行時に、IPSecが1024ビットのDiffie-Hellmanプライムモジュラスグループを使用することを指定します。

デフォルトでは、PFSは要求されません。このコマンドでグループが指定されていない場合は、*group1*がデフォルトとして使用されます。

例：

```
Router(config)#crypto map map 10 ipsec-isakmp
```

```
Router(config-crypto-map)#set pfs group2
```

set pfsコマンドの詳細については、『Cisco IOS [Security](#) Command Reference』を参照してください。

[関連情報](#)

- [一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について](#)
- [Cisco VPN 3000 シリーズ コンセントレータ](#)
- [Cisco VPN 3002 Hardware Client](#)
- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)