

# VPN 3000 コンセントレータ帯域幅管理機能の設定例

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

[VPN 3000 コンセントレータのデフォルト帯域幅 ポリシーを設定して下さい](#)

[サイト間のトンネルのための帯域幅管理を設定して下さい](#)

[リモート VPN トンネルのための帯域幅管理を設定して下さい](#)

[確認](#)

[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、Cisco VPN 3000 コンセントレータで帯域幅管理機能を設定するために必要な手順を説明します。

- [サイト間の \( LAN-to-LAN な \) VPN はトンネル伝送します](#)
- [リモートアクセス VPN トンネル](#)

注: リモートアクセスまたはサイト間VPN トンネルを設定する前に、最初に [VPN 3000 コンセントレータのデフォルト帯域幅 ポリシーを設定して下さい](#)。

帯域幅管理の 2 つの要素があります:

- **帯域幅 ポリシング**—トンネルトラフィックの最大レートを制限します。VPN コンセントレータはこの比率を超過するこの比率の下で受信する送信し、トラフィックを廃棄しますトラフィックを。
- **帯域予約**—トンネルトラフィックのために最小帯域幅 比率を確保します。帯域幅管理はグループおよびユーザに帯域幅を公正に割り当てることを可能にします。これはある特定のグループかユーザが帯域幅の大半を消費することを防ぎます。

帯域幅管理はトンネルトラフィック ( レイヤ2 トンネルプロトコル [L2TP]、ポイント ツー ポイント トンネリング プロトコル [PPTP]、IPSec ) にだけ適用し、パブリックインターフェイスに最も一般に適用します。

帯域幅管理機能はリモートアクセスおよびサイト間VPN 接続に管理上の利点を提供します。リモートアクセス VPN トンネルはブロードバンド ユーザがすべての帯域幅を利用しないように帯域幅 ポリシングを利用します。逆に、管理者は各リモートサイトに最低限の帯域幅を保証するた

めにサイト間のトンネルのための帯域予約を設定できます。

## 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

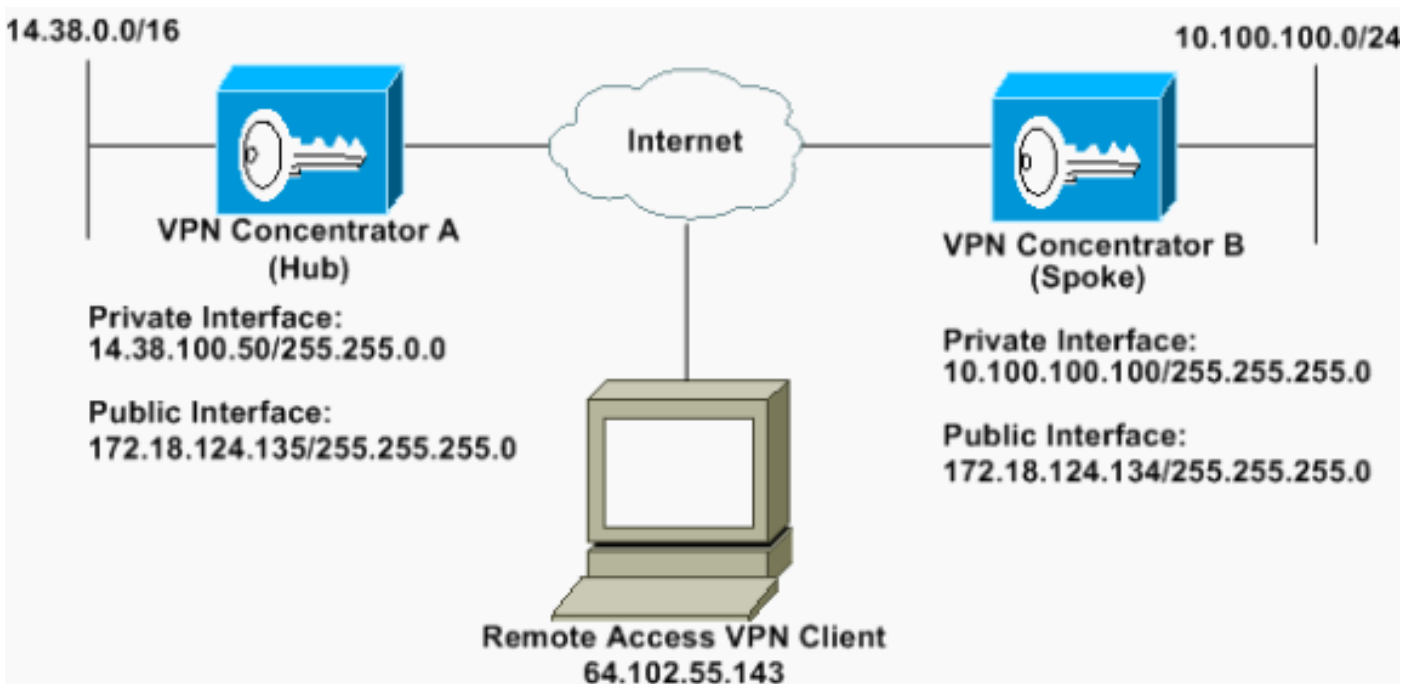
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェアリリース 4.1.x およびそれ以降が付いている Cisco VPN 3000 コンセントレータ
- 注: 帯域幅管理機能はリリース 3.6 で導入されました。

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

### ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



### 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。

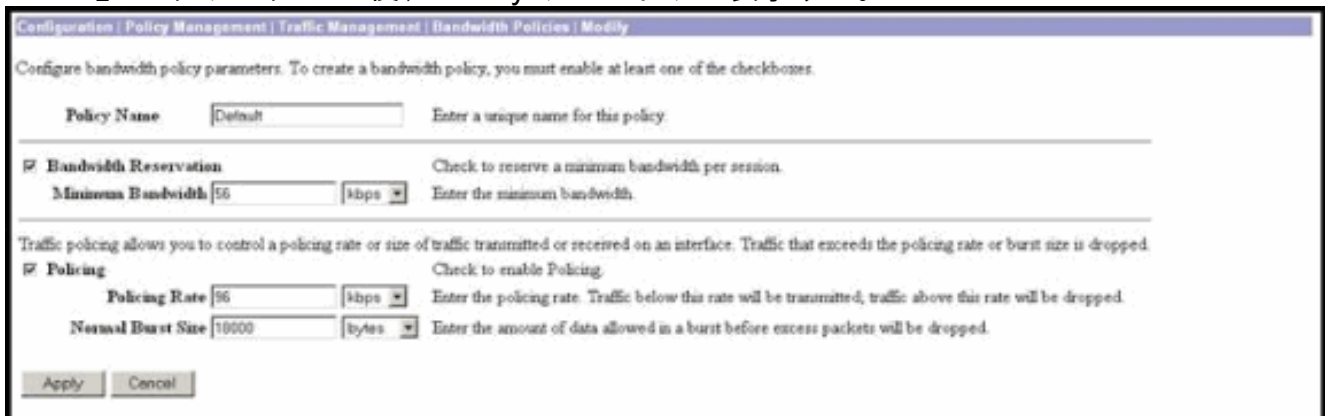
## VPN 3000 コンセントレータのデフォルト帯域幅ポリシーを設定して下さい

LAN-to-LAN トンネルまたはリモートアクセストンネルの帯域幅管理を設定できる前にパブリックインターフェイスの帯域幅管理を有効にしなければなりません。この設定例では、デフォルト帯域幅ポリシーは設定されます。このデフォルトポリシーはそれらによってが VPN コンセントレータでに属するグループに適用される帯域幅管理ポリシーがないトンネル/ユーザに適用されます。

1. ポリシーを設定するために、Configuration > Policy Management > Traffic Management > Bandwidth Policies の順に選択し、『Add』をクリックして下さい。



『Add』をクリックした後、Modify ウィンドウは表示する。



2. Modify ウィンドウのこれらのパラメータを設定して下さい。ポリシーは name — ポリシーを覚えるのを助けることができるユニークなポリシー名前を入力します。最大長は 32 文字です。この例では、ネーム「デフォルト」はポリシー名で設定されます。帯域予約—各セッションのために最低限の帯域幅を予約するために帯域予約 チェックボックスをチェックして下さい。この例では、56 キロビットの広帯域/秒はグループの下でころばないすべての VPN ユーザ向けに予約済みです設定される帯域幅管理がある。ポリシング—ポリシングを有効にするためにポリシング チェックボックスをチェックして下さい。ポリシングレートの値を入力し、測定単位を選択して下さい。ポリシングレートの下で移動する送信し、すべてのトラフィックを廃棄します VPN コンセントレータはトラフィックをポリシングレートの上で移動する。96 キロビット/秒は帯域幅 ポリシングのために設定されます。正常なバースト サイズは VPN コンセントレータがいつでも送信できる即時バーストの量です。バースト サイズを設定するために、この数式を使用して下さい: $(\text{Policing Rate}/8) * 1.5$ この数式によって、バースト レートは 18000 バイトです。
3. [Apply] をクリックします。
4. 帯域幅タブを Configuration > Interfaces > Public Interface の順に選択し、インターフェイスにデフォルト帯域幅ポリシーを適用するためにクリックして下さい。
5. 帯域幅管理 オプションを有効にして下さい。
6. リンク レートを規定して下さい。リンク レートはインターネットを通過してネットワーク接続の速度です。この例でインターネットへの T1 接続は使用されます。その結果、1544 キ

ロビット/秒は設定されたリンク比率です。

7. 帯域幅 ポリシー ドロップダウン リストからポリシーを選択して下さい。デフォルトポリシーはこのインターフェイスのために先に設定されます。ここにいるこのインターフェイスのすべてのユーザ向けのデフォルト帯域幅 ポリシー適用するポリシー。このポリシーはグループに適用される帯域幅管理 ポリシーがないユーザに適用されます。

Attribute	Value	Description
Bandwidth Management	<input checked="" type="checkbox"/>	Check to enable bandwidth management.
Link Rate	1544 kbps	Set the link rate that will be applied to all tunneled traffic. The defined link rate must be based on available Internet bandwidth and not the physical LAN connection rate.
Bandwidth Policy	Default	This policy is applied to all VPN tunnels that do not have a group based Bandwidth Management policy. Policies are configured at Configuration   Policy Management   Traffic Management   Bandwidth Policies.

## サイト間のトンネルのための設定 帯域幅管理

サイト間のトンネルのための帯域幅管理を設定するためにこれらのステップを完了して下さい。

1. Configuration > Policy Management > Traffic Management > Bandwidth Policies の順に選択し、新しく LAN-to-LAN な 帯域幅 ポリシーを定義するために『Add』をクリックして下さい。この例では、'L2L\_tunnel' と呼ばれたポリシーは 256 キロビット/秒の帯域予約で設定されました。

Configure bandwidth policy parameters. To create a bandwidth policy, you must enable at least one of the checkboxes.

Policy Name: L2L\_tunnel Enter a unique name for this policy.

Bandwidth Reservation Check to reserve a minimum bandwidth per session.  
Minimum Bandwidth: 256 kbps Enter the minimum bandwidth.

Traffic policing allows you to control a policing rate or size of traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped.

Policing Check to enable Policing.  
Policing Rate: 56 kbps Enter the policing rate. Traffic below this rate will be transmitted, traffic above this rate will be dropped.  
Normal Burst Size: 10500 bytes Enter the amount of data allowed in a burst before excess packets will be dropped.

2. 帯域幅 ポリシー ドロップダウン メニューの下で既存の LAN-to-LAN トンネルに帯域幅 ポリシーを適用して下さい。

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Name  Enter the name for this LAN-to-LAN connection.

Interface  Select the interface for this LAN-to-LAN connection.

Peer  Enter the IP address of the remote peer for this LAN-to-LAN connection.

Digital Certificate  Select the digital certificate to use.

Certificate  Entire certificate chain  
Transmission  Identity certificate only  
Choose how to send the digital certificate to the IKE peer.

Preshared Key  Enter the preshared key for this LAN-to-LAN connection.

Authentication  Specify the packet authentication mechanism to use.

Encryption  Specify the encryption mechanism to use.

IKE Proposal  Select the IKE Proposal to use for this LAN-to-LAN connection.

Filter  Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.

IPSec NAT-T  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.

Bandwidth Policy  Choose the bandwidth policy to apply to this LAN-to-LAN connection.

Routing  Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.

---

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List  Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address  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.mnn addresses.

Wildcard Mask

---

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List  Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address  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.mnn addresses.

Wildcard Mask

## リモート VPN トンネルのための帯域幅管理を設定して下さい

リモート VPN トンネルのための帯域幅管理を設定するためにこれらのステップを完了して下さい。

1. Configuration > Policy Management > Traffic Management > Bandwidth Policies の順に選択し、新しい帯域幅 ポリシーを作成するために『Add』をクリックして下さい。この例では、「RA\_tunnels」と呼ばれるポリシーは 8 キロビット/秒の帯域予約で設定されます。トラフィック ポリシングは 24000 バイトの 128 キロビット/秒およびバースト サイズのポリシングレートで設定されます。

Configuration | Policy Management | Traffic Management | Bandwidth Policies | Modify

Configure bandwidth policy parameters. To create a bandwidth policy, you must enable at least one of the checkboxes.

Policy Name  Enter a unique name for this policy.

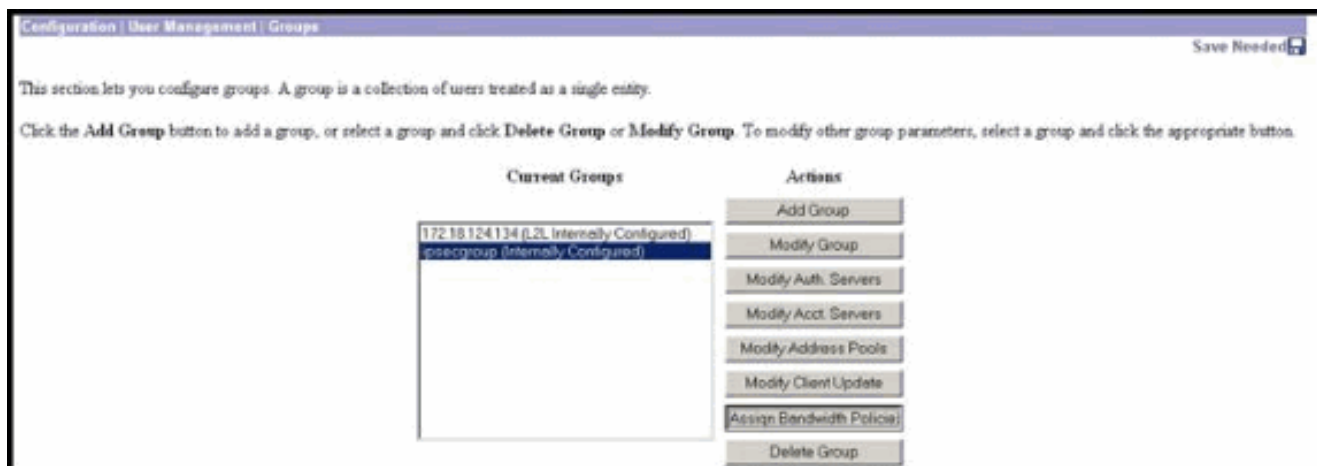
Bandwidth Reservation Check to reserve a minimum bandwidth per session.  
Minimum Bandwidth  kbps Enter the minimum bandwidth.

Traffic policing allows you to control a policing rate or size of traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped.

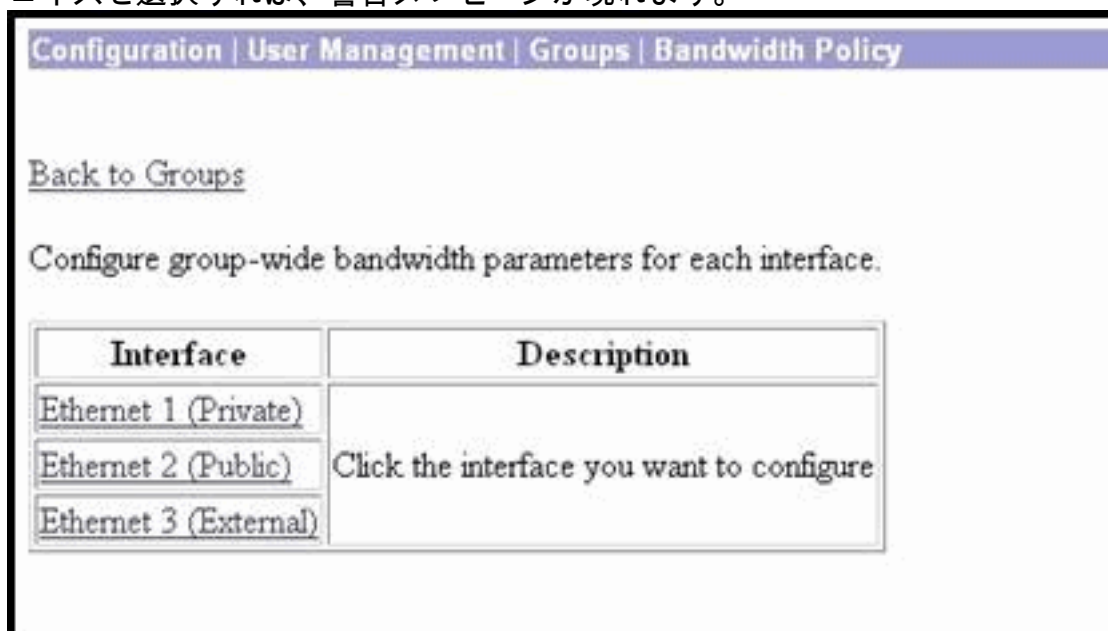
Policing Check to enable Policing.  
Policing Rate  kbps Enter the policing rate. Traffic below this rate will be transmitted, traffic above this rate will be dropped.  
Normal Burst Size  bytes Enter the amount of data allowed in a burst before excess packets will be dropped.

2. 帯域幅 ポリシーをリモートアクセス VPN グループに適用するために、Configuration > User Management > Groups の順に選択し、グループを選択し、『Assign Bandwidth Policies』をクリックして下さい。

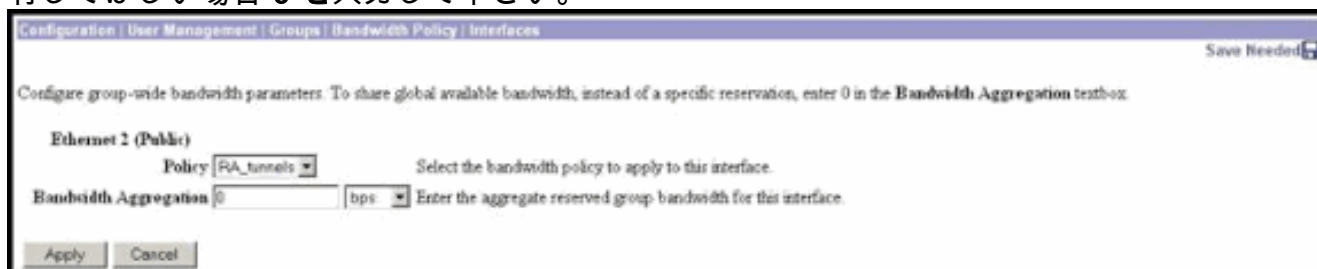




3. このグループのための帯域幅管理を設定したいと思うインターフェイスをクリックして下さい。この例では、'Ethernet2 (パブリック)' は「グループのための選択したインターフェイスです。帯域幅 ポリシーをインターフェイスのグループに適用するために、帯域幅管理はそのインターフェイスで有効にする必要があります。帯域幅管理が無効であるインターフェイスを選択すれば、警告メッセージが現れます。



4. このインターフェイスの VPNグループに帯域幅 ポリシーを選択して下さい。RA\_tunnels ポリシーはこのグループに、以前に定義された、選択されます。このグループのために予約するために最小帯域幅の値を入力して下さい。帯域幅集約のデフォルト値は 0 です。測定単位の既定の単位はビット/秒です。グループにインターフェイスの利用可能な帯域幅で共有してほしい場合 0 を入力して下さい。



## 確認

帯域幅管理を監視するために VPN 3000 コンセントレータで Monitoring > Statistics > Bandwidth Management の順に選択して下さい。

Monitoring Statistics Bandwidth Management		Wednesday, 14 August 2002 14:16:33			
		Reset Refresh			
This screen shows bandwidth management information. To refresh the statistics, click Refresh. Select a Group to filter the users.					
Group: <input type="text" value="-All-"/>					
User Name	Interface	Traffic Rate (kbps)		Traffic Volume (bytes)	
		Conformed	Throttled	Conformed	Throttled
ipseccgr (In)	Ethernet 2 (Public)	11	5	1433342	1001508
ipseccgr (Out)	Ethernet 2 (Public)	11	5	1331526	74900
no_spoke (In)	Ethernet 2 (Public)	1539	237	206052492	23959858
no_spoke (Out)	Ethernet 2 (Public)	1539	588	206052492	118751970

## トラブルシューティング

帯域幅管理が VPN 3000 コンセントレータで設定される間、問題を解決するために、**Configuration > System > Events > Classes** の下でこれら二つのイベント クラスを有効にしてください:

- **BMGT** (記録すべき重大度と: 1-9)
- **BMGTDBG** (記録すべき重大度と: 1-9)

これらはいくつかのもっとも一般的な イベントログメッセージです:

- 帯域幅 ポリシーが修正されるとき エラーメッセージを見られますログで。

```
1 08/14/2002 10:03:10.840 SEV=4 BMGT/47 RPT=2
```

```
The Policy [ RA_tunnels ] with Reservation [ 8000 bps ] being applied to Group [ ipsecgroup ] on Interface [ 2 ] exceeds
```

```
the Aggregate Reservation [ 0 bps ] configured for that group. このエラーメッセージが表示する場合、グループ設定に戻し、グループから「RA_tunnel」ポリシーを非適用して下さい。正しい値を用いる「RA_tunnel」を編集し、次に特定のグループに戻ってポリシーを再適用して下さい。
```

- インターフェイス 帯域幅を見つけることが不可能。

```
11 08/14/2002 13:03:58.040 SEV=4 BMGTDBG/56 RPT=1
```

```
Could not find interface bandwidth policy 0 for group 1 interface 2. 帯域幅 ポリシーがインターフェイスで有効にならないし、LAN-to-LAN トンネルでそれを加えることを試みれば場合このエラーを受け取ることができます。これが事実である場合、設定で説明されているように パブリックインターフェイスにポリシーを VPN 3000 コンセントレータ セクションのデフォルト帯域幅 ポリシー適用して下さい。
```

## 関連情報

- [Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ](#)
- [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 に関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)