

VPN 3000 コンセントレータ帯域幅管理機能の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

[VPN 3000コンセントレータでのデフォルト帯域幅ポリシーの設定](#)

[サイト間トンネルの帯域幅管理の設定](#)

[リモートVPNトンネルの帯域幅管理の設定](#)

[確認](#)

[トラブルシュート](#)

[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 \(LAN間\) VPNトンネル](#)
- [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、[VPN 3000コンセントレータでデフォルトの帯域幅ポリシーを設定する必要があります](#)。

帯域幅管理には、次の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、受信したトラフィックをこのレート未満で送信し、このレートを超えるトラフィックをドロップします。
- **Bandwidth Reservation**：トンネルトラフィックの最小帯域幅レートを確保します。帯域幅管理を使用すると、グループとユーザに帯域幅を均等に割り当てることができます。これにより、特定のグループやユーザが帯域幅の大部分を消費することを防止できます。

帯域幅管理は、トンネリングされたトラフィック(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)にのみ適用され、最も一般的にパブリックインターフェイスに適用されます。

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もたらします。リモートアクセスVPNトンネルでは、帯域幅ポリシングを使用するため、ブロードバンドユーザはすべての帯域幅を使用しません。逆に、管理者はサイト間トンネルの帯域幅予約を設定して、

各リモートサイトへの最小帯域幅を保証できます。

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。

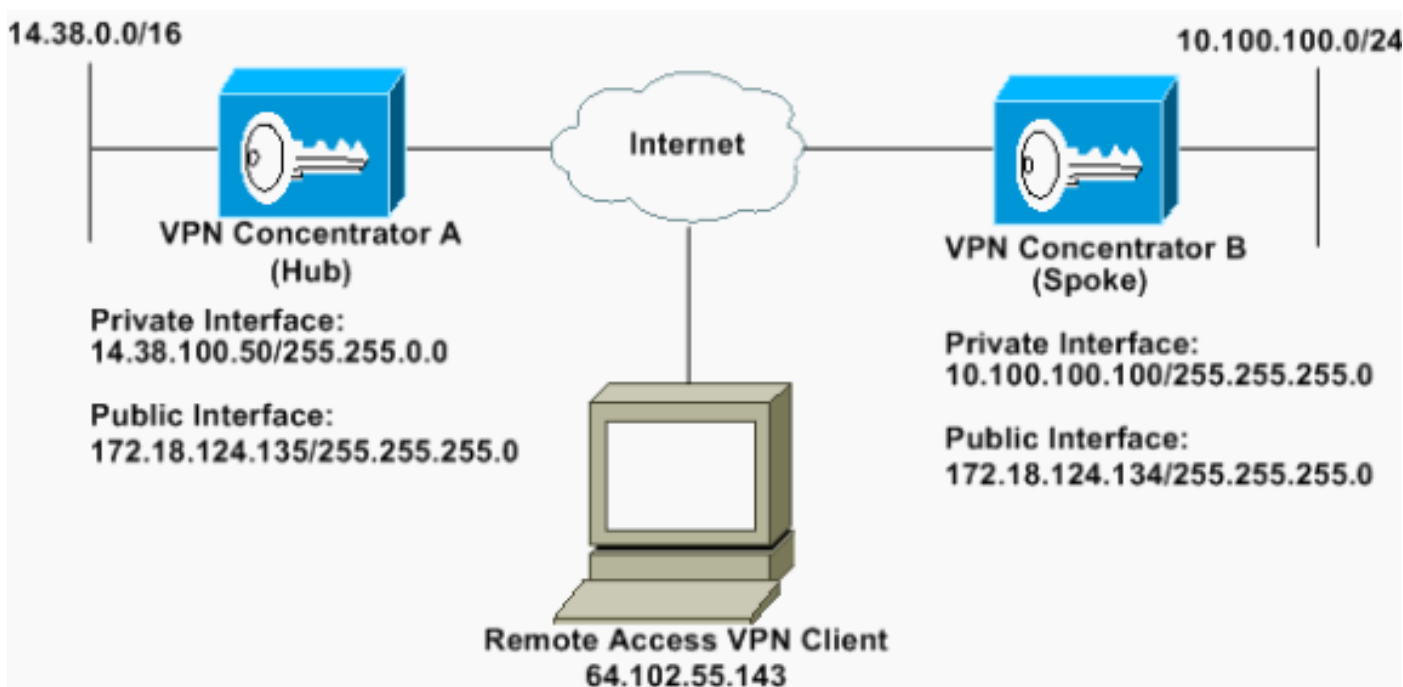
- ソフトウェアリリース4.1.x以降が稼働するCisco VPN 3000コンセントレータ

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。

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。



表記法

ドキュメントの表記法の詳細は、「[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コンセントレータでのデフォルト帯域幅ポリシーの設

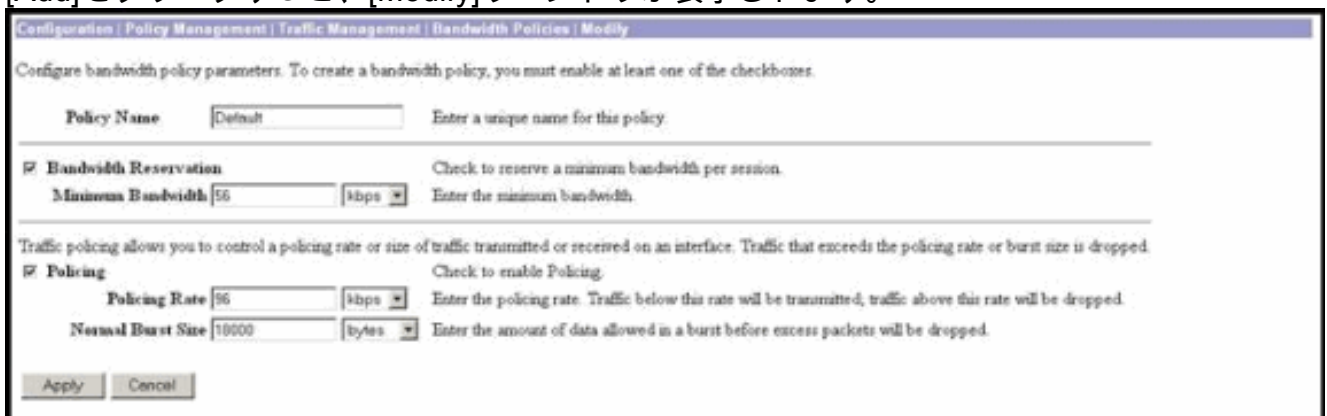
定

LAN-to-LANトンネルまたはリモートアクセストンネルで帯域幅管理を設定する前に、パブリックインターフェイスで帯域幅管理を有効にする必要があります。この設定例では、デフォルトの帯域幅ポリシーが設定されています。このデフォルトポリシーは、VPNコンセントレータに属するグループに帯域幅管理ポリシーが適用されていないユーザ/トンネルに適用されます。

1. ポリシーを構成するには、[Configuration] > [Policy Management] > [Traffic Management] > [Bandwidth Policies]を選択し、[Add]をクリックします。



[Add]をクリックすると、[Modify]ウィンドウが表示されます。



2. これらのパラメータは、[修正]ウィンドウで設定します。**Policy Name**：ポリシーの記憶に役立つ一意のポリシー名を入力します。最大長は 32 文字です。この例では、ポリシー名として「Default」という名前が設定されています。**Bandwidth Reservation**:[Bandwidth Reservation]チェックボックスをオンにして、各セッションの最小帯域幅を予約します。この例では、56 kbpsの帯域幅が、帯域幅管理が設定されているグループに属していないすべてのVPNユーザ用に予約されています。**ポリシング**：ポリシングを有効にするには、ポリシングチェックボックスをオンにします。ポリシングレートの値を入力し、計測単位を選択します。VPNコンセントレータは、ポリシングレートを下回るトラフィックを送信し、ポリシングレートを越えるトラフィックをすべてドロップします。帯域幅ポリシング用に96 kbpsが設定されています。通常のバーストサイズは、VPNコンセントレータが任意の時点で送信できる瞬間的なバーストの量です。バーストサイズを設定するには、次の式を使用します。

$$(\text{Policing Rate}/8) * 1.5$$

この式では、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. [Configuration] > [Interfaces] > [Public Interface]を選択し、[Bandwidth]タブをクリックして、デフォルトの帯域幅ポリシーをインターフェイスに適用します。
5. 帯域幅管理オプションを有効にします。

- リンクレートを指定します。リンクレートは、インターネットを介したネットワーク接続の速度です。この例では、インターネットへのT1接続が使用されます。したがって、設定されたリンクレートは1544 kbpsです。
- [帯域幅ポリシー(Bandwidth Policy)]ドロップダウンリストからポリシーを選択します。デフォルトポリシーは、このインターフェイスに対して以前に設定されています。ここで適用するポリシーは、このインターフェイスのすべてのユーザに対するデフォルトの帯域幅ポリシーです。このポリシーは、グループに帯域幅管理ポリシーが適用されていないユーザに適用されます。

Configuration | Interfaces | Ethernet 2

Configuring Ethernet Interface 2 (Public).

General | RIP | OSPF | Bandwidth

Bandwidth Management Parameters		
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.

Apply Cancel

サイト間トンネルの帯域幅管理の設定

サイト間トンネルの帯域幅管理を設定するには、次の手順を実行します。

- [Configuration] > [Policy Management] > [Traffic Management] > [Bandwidth Policies]の順に選択し、[Add]をクリックして新しいLAN-to-LAN帯域幅ポリシーを定義します。この例では、「L2L_tunnel」というポリシーが256 kbpsの帯域幅予約で設定されています。

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: 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.

Apply Cancel

- [Bandwidth Policy]ドロップダウンメニューで、既存のLAN-to-LANトンネルに帯域幅ポリシーを適用します。

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 xxx 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 xxx addresses.

Wildcard Mask:

リモートVPNトンネルの帯域幅管理の設定

リモートVPNトンネルの帯域幅管理を設定するには、次の手順を実行します。

1. [Configuration] > [Policy Management] > [Traffic Management] > [Bandwidth Policies]を選択し、[Add]をクリックして新しい帯域幅ポリシーを作成します。この例では、「RA_tunnels」というポリシーが8 kbpsの帯域幅予約で設定されています。トラフィックポリシングは、ポリシングレートが128 kbps、バーストサイズが24000バイトで設定されます。

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 check-boxes.

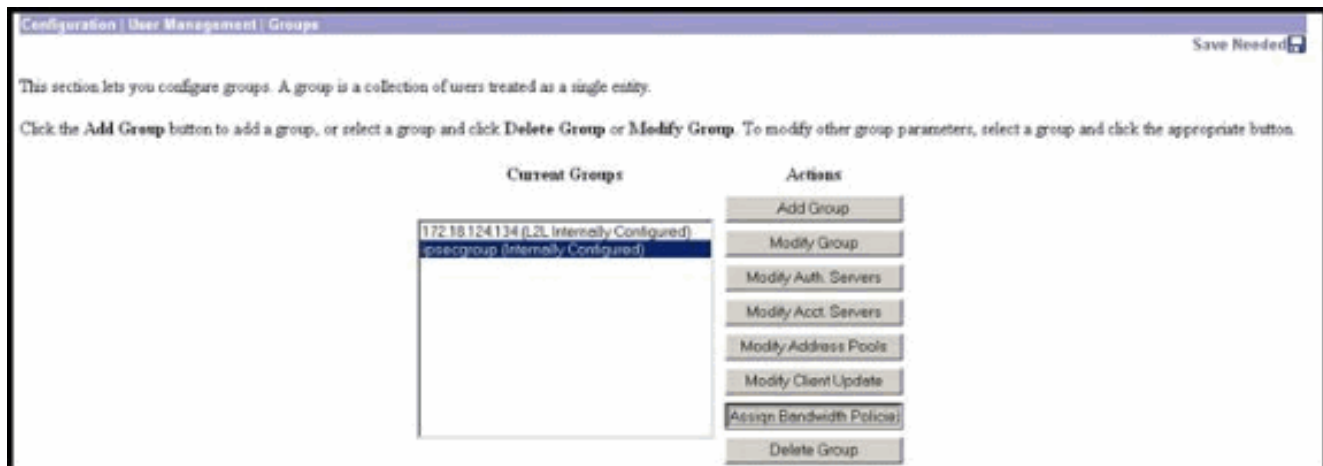
Policy Name: Enter a unique name for this policy.

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

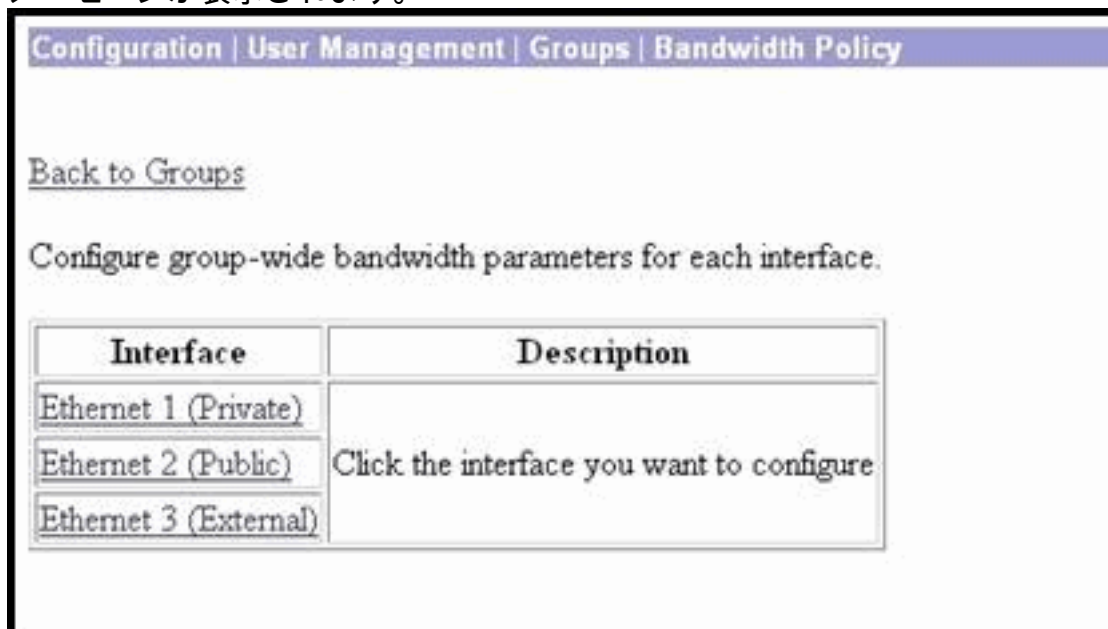
Traffic policing allows you to control a policing rate or size of traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped.

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.

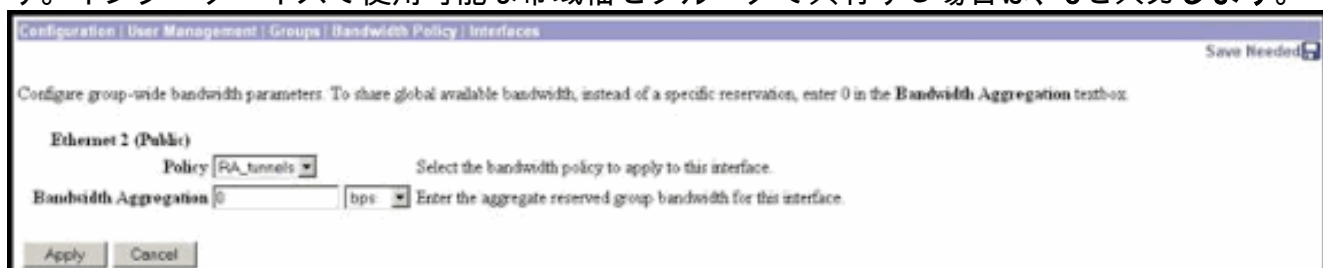
2. 帯域幅ポリシーをリモートアクセスVPNグループに適用するには、[Configuration] > [User Management] > [Groups]を選択して、グループを選択し、[Assign Bandwidth Policies]をクリックします。



3. このグループの帯域幅管理を設定するインターフェイスをクリックします。この例では、「Ethernet2 (Public)」がグループに選択されているインターフェイスです。インターフェイスのグループに帯域幅ポリシーを適用するには、そのインターフェイスで帯域幅管理を有効にする必要があります。帯域幅管理が無効になっているインターフェイスを選択すると、警告メッセージが表示されます。



4. このインターフェイスのVPNグループの帯域幅ポリシーを選択します。以前に定義した RA_tunnelsポリシーがこのグループに対して選択されます。このグループに予約する最小帯域幅の値を入力します。帯域幅集約のデフォルト値は0です。デフォルトの測定単位はbpsです。インターフェイスで使用可能な帯域幅をグループで共有する場合は、0を入力します。



確認

VPN 3000コンソントレータでMonitoring > Statistics > Bandwidth Managementの順に選択し、帯域幅管理を監視します。

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: [All]					
User Name	Interface	Traffic Rate (kbps)		Traffic Volume (bytes)	
		Conformed	Throttled	Conformed	Throttled
ipseccgr (In)	Ethernet 1 (Public)	11	5	143342	1001508
ipseccgr (Out)	Ethernet 2 (Public)	11	9	1321526	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

VPN 3000 コンセントレータに帯域幅管理が実装されている間に問題をトラブルシューティングするには、[Configuration] > [System] > [Events] > [Classes] で次の2つのイベントクラスを有効にします。

- **BMGT**(Severity to Log:1-9)
- **BMGTDBG**(ログの重大度 : 1-9)

最も一般的なイベントログメッセージの一部を次に示します。

- 帯域幅が超過すると、ログに「Exceeds the Aggregate Reservation」エラーメッセージが表示されます。

```
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された場合は、グループ設定に戻り、グループから「RA_tunnel」ポリシーを適用し直します。正しい値で「RA_tunnel」を編集し、ポリシーを特定のグループに再適用します。

- インターフェイス帯域幅が見つかりません。

```
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.
```

このエラーは、インターフェイスで帯域幅ポリシーが有効になっていない場合に、LAN-to-LANトンネルに適用しようとする则表示されることがあります。このような場合は、「[VPN 3000 コンセントレータのデフォルト帯域幅ポリシーの設定](#)」の項で説明するように、ポリシーをパブリックインターフェイスに適用します。

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](#)