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

<u>概要</u>

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。

- <u>サイト間(LAN間)VPNトンネル</u>
- <u>リモートアクセスVPNトンネル</u>

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、<u>VPN 3000コンセントレー</u> <u>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</u>。

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 0

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



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。

Configuration Heristes -@System	Configuration Policy Management Traffic Management Bandwidth Policies Save N	leeded
Organistration Organistration Organistration Organistration Organistration Organistration Organistration Official	Save h This section lets you add, modify and delete bandwidth policies. Click Add to add a policy, or select a policy and click Modify or Delete. Bandwidth Pelicies Actions Empty- Add Modify	leeded
	Delinte	

[Add]をクリックすると、[Modify]ウィンドウが表示されます。

Policy Name	Default	Enter a unique name for this policy
Bandwidth Reservation	an in the second se	Check to reserve a minimum bandwidth per session.
Minimum Bandwidth	56 kbps	 Enter the minimum bandwidth.
ffic policing allows you to	o control a policing rate or	ize of traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped
ffic policing allows you t Policing	o control a policing rate of	ize of tradfic transmitted or seceived on an interface. Tradfic that exceeds the policing rate or burst size is dropped Check to enable Policing.
ffic policing allows you t Policing Policing Rate	o control a policing rate of	 ize of traffic transmitted or seceived on an interface. Traffic that exceeds the policing rate or burst size is dropped. Check to enable Policing. Enter the policing rate. Traffic below this rate will be transmitted, traffic above this rate will be dropped.

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超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。

(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。
- 7. [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	
You are modifying the Configuring Ethernet	e interface you are using to connect Interface 2 (Public).	to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.
General RIP OSPF Da	ndwidth	Bandwidth Management Parameters
Attaibute	Value	Description
Bandwidth Management	2	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		

<u>サイト間トンネルの帯域幅管理の設定</u>

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。

1. [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 M	enagement Traffic	Management	Bandwidth Palicies Madity	
Configure bandwidth poli	cy parameters. To cr	reate a bandwid	th policy, you must enable at least one of the checkboxes.	
Policy Name	L2L_turnel	-	Enter a unique name for this policy.	
🕫 Bandwidth Reserv	ation		Check to reserve a minimum bandwidth per session.	
Minimum Bandwie	drh [256	kbps 💌	Enter the minimum bandwidth.	
Traffic poäcing allows yo	u to control a policin	g rate or size of	traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped	
Pelicing			Check to enable Policing	
Policing Ra	ute 56	kbps 💌	Enter the policing rate. Traffic below this rate will be transmitted, traffic above this rate will be dropped.	
Normal Burst S	ize 18500	bytes 💌	Enter the amount of data allowed in a burst before excess packets will be dropped.	
Apply Cancel	1			

2. [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	r LAN Add
Add a new IPSec LAN-to-LAN connection	
Name to socke	Enter the name for this LAN-to-LAN connection
Interface Ethomot 2 (Public) (172 18 124 1 %)	Select the interface for this LAN-to-LAN connection
Pear 12218124114	Enter the ID address of the remote neer for this LAN-to-LAN connection.
Digital Certificate None (Use Preshared Keys) *	Select the digital certificate to use.
Certificate C Entire certificate chain Transmission # Identity certificate only	Choose how to send the digital certificate to the IRE peer.
Preshared Key osco123	Enter the preshared key for this LAN-to-LAN connection.
Authentication ESP/MD5/HMAC-128 *	Specify the packet authentication mechanism to use.
Encryption 3DES-168	Specify the encryption mechanism to use.
IKE Proposal #E-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter -Nono-	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSer NAI-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 L2L_turnel *	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing None	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.
Local Network: If a LAN-to-LAN NAT role is used, this is	he Translated Network address
Network List Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address 1430.0.0	
Wildcard Mark 0.0.255 255	Note: Enter a wildcard mark, which is the reverse of a subnet mark. A wildcard mark has is n bit postions to ignore, Os in bit positions to match. For example, 10.10.1.0/0.0.255 = al. 10.10.1.mn addresses.
Remote Network: If a LAN-to-LAN NAT rule is used, this	is the Remote Network address.
Network List Use IP Address/Wildcard-mask below	Specify the remote network address hit or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address 10.100.100.0	Note: Fater a self-fored much which is the resource of a submatenach. A subfract much has been been been subscribed as
Wildcard Mask 0.0.0.255	Or in bit positions to match. For example, 10.10.1.000.0.255 = al 10.10.1.nn addresses.
Add Cancel	

<u>リモートVPNトンネルの帯域幅管理の設定</u>

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。

	[FIA_tunnels		Enter a unique name for this policy.
Z Bandwidth Reserv	ation		Check to reserve a minimum bandwidth per session.
Minimum Bandwi	dth (8	kbps 💌	Enter the minimum bandwidth.
raffic policing allows y	u to control a poão	ing rate or size of	traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped
7 Policing			Check to enable Policing
			Total description of Taffe balanchic and an initial second and soften down diverse with a descent
Policing R	ate 128	kbps 💌	inter the poacing rate. France octow this rate will be transmitted, traine above this rate 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。

Cenfiguration Buer Managament Groups		Save Needed
This section lets you configure groups. A group is a collection of users treated as a single entity.		
Click the Add Group button to add a group, or relect a group and click Delete Group or Medify Gro	mp . To modify other group p	arameters, select a group and click the appropriate button.
Current Groups	Actions	
	Add Group	
172.18.124.134 (L2L Internally Configured) operational (Configured)	Modily Group	
	Modily Auth. Servers	
	Modily Acct. Servers	
	Modily Address Pools	
	Modity Client Update	
	Assign Bandwidth Policie)	
	Delete Group	

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。

Configuration User	Management Groups Bandwidth Polic	cy
<u>Back to Groups</u> Configure group-wide	bandwidth parameters for each interface.	ŝ
Interface	Description	
Interface Ethernet 1 (Private)	Description	4
Interface Ethernet 1 (Private) Ethernet 2 (Public)	Description Click the interface you want to configure	

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。

Configuration User Management Groups Bandwidth Policy Interfaces	
	Save Needed
Configure group-wide bandwidth parameters: To share global available bandwidth, instead of a specific reservation, enter 0 in the Bandwidth Aggregation textbox.	
Ethernet 2 (Public)	
Policy RA_tunnels . Select the bandwidth policy to apply to this interface.	
Bandwidth Aggregation	
Apply Cancel	

<u>確認</u>

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

Monitoring Statistics Bandwidth M	lanagement			Wednesday	, 14 August 2002 14:16:
Dis street, shows bandwidth manage Group	ment information. To refresh the elaristics	, this Refresh. Select a Group (o filter the users.		Resenge Refresh
Here Manue	Terretore	Traffic Rate (chps)	Traffic Volume	(bytes)
User Name	Interface	Conformed	Throttled	Conformed	Throttled
ipsecriser (In)	Ethemet 2 (Public)	10	5	1/13/13/2	1004508
parcuse: (Out)	Ethernet 2 (Public)	11	2	1321326	74700
to_spoke (In)	Ethernet 2 (Public)	1539	237	206052492	23359858

<u>トラブルシュート</u>

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。

•帯域幅ポると、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 Interrface [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と表示されることがあります。このような場合は、「<u>VPN</u> <u>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</u>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

- <u>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</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
- IPSec に関するサポート ページ
- <u>テクニカルサポート Cisco Systems</u>