

VPN 3000 Concentrator Bandwidth Management Configuration Example

Document ID: 60329

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

Configure a Default Bandwidth Policy on the VPN 3000 Concentrator

Configure Bandwidth Management for Site-to-Site Tunnels

Configure Bandwidth Management for Remote VPN Tunnels

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes the necessary steps used to configure the Bandwidth Management feature on the Cisco VPN 3000 Concentrator for:

- Site-to-site (LAN-to-LAN) VPN tunnels
- Remote access VPN tunnels

Note: Before you configure remote access or site-to-site VPN tunnels, you must first configure a default bandwidth policy on the VPN 3000 Concentrator.

There are two elements of Bandwidth Management:

- **Bandwidth Policing** Limits the maximum rate of tunneled traffic. The VPN Concentrator transmits traffic it receives below this rate and drops traffic that exceeds this rate.
- **Bandwidth Reservation** Sets aside a minimum bandwidth rate for tunneled traffic. Bandwidth Management allows you to allocate bandwidth to groups and users equitably. This prevents certain groups or users from consuming a majority of the bandwidth.

Bandwidth Management applies only to tunneled traffic (Layer 2 Tunnel Protocol [L2TP], Point to Point Tunneling Protocol [PPTP], IPSec) and is most commonly applied to the public interface.

The Bandwidth Management feature provides administrative benefits to remote access and site-to-site VPN connections. The remote access VPN tunnels utilize Bandwidth Policing so that broadband users do not utilize all the bandwidth. Conversely, the administrator can configure Bandwidth Reservation for site-to-site tunnels to guarantee a minimum amount of bandwidth to each remote site.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

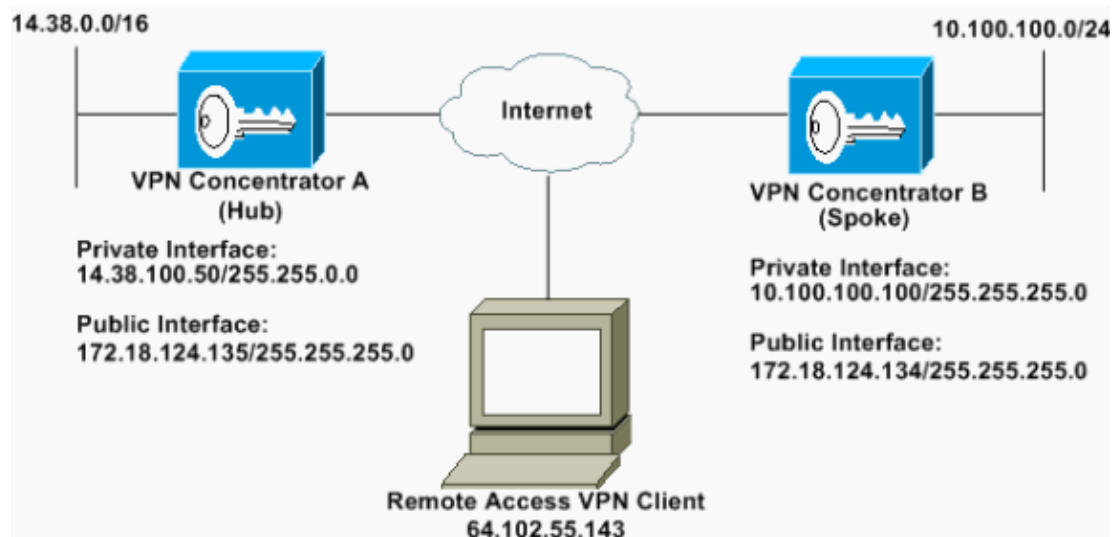
- Cisco VPN 3000 Concentrator with Software Releases 4.1.x and later

Note: The Bandwidth Management feature was introduced in release 3.6.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This document uses this network setup:



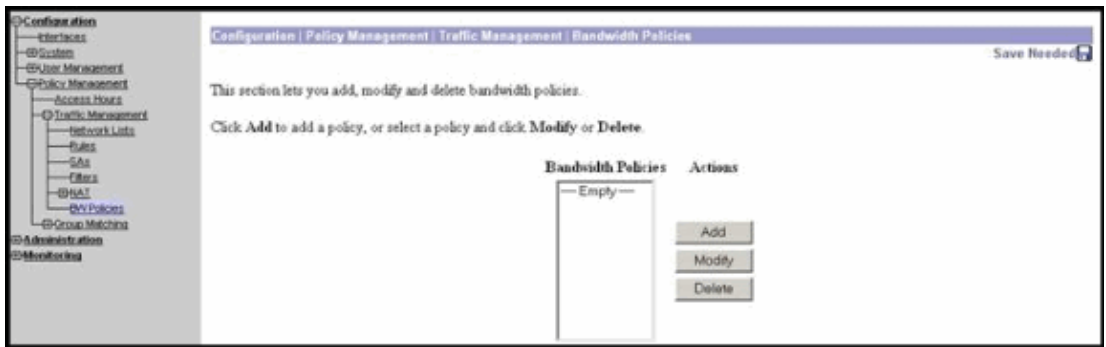
Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

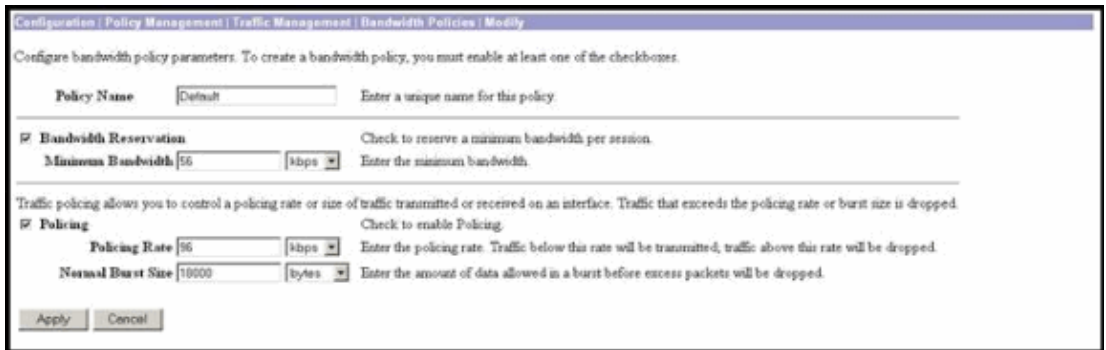
Configure a Default Bandwidth Policy on the VPN 3000 Concentrator

Before you can configure Bandwidth Management on the LAN-to-LAN tunnels or on the remote access tunnels, you have to enable Bandwidth Management on the public interface. In this sample configuration, a default bandwidth policy is configured. This default policy is applied to users/tunnels that do not have a Bandwidth Management policy applied to the group they belong to in the VPN Concentrator.

1. To configure a policy, select **Configuration > Policy Management > Traffic Management > Bandwidth Policies**, and click **Add**.



After you click Add, the Modify window is displayed.



2. Set these parameters in the Modify window.

- ◆ **Policy Name** Enter a unique policy name that can help you remember the policy. The maximum length is 32 characters. In this example, the name 'Default' is configured as the Policy Name.
- ◆ **Bandwidth Reservation** Check the **Bandwidth Reservation** check box to reserve a minimum amount of bandwidth for each session. In this example, 56 kbps of bandwidth is reserved for all the VPN users who do not fall under a group that has Bandwidth Management configured.
- ◆ **Policing** Check the **Policing** check box to enable policing. Enter a value for Policing Rate and select the unit of measurement. The VPN Concentrator transmits traffic that moves below the policing rate and drops all traffic that moves above the policing rate. 96 kbps is configured for Bandwidth Policing. The normal burst size is the amount of instantaneous burst that the VPN Concentrator can send at any given time. To set the burst size, use this formula:

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

With this formula, the Burst Rate is 18000 bytes.

3. Click **Apply**.
4. Select **Configuration > Interfaces > Public Interface** and click on the Bandwidth tab to apply the default bandwidth policy to an interface.
5. Enable the **Bandwidth Management** option.
6. Specify the link rate.

The link rate is the speed of the network connection through the Internet. In this example a T1 connection to the Internet is used. Consequently, 1544 kbps is the configured link rate.

7. Select a policy from the Bandwidth Policy drop-down list.

Default policy is configured earlier for this interface. The policy you apply here is a default bandwidth policy for all users on this interface. This policy is applied to users who do not have a Bandwidth Management policy applied to their group.

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

Configure Bandwidth Management for Site-to-Site Tunnels

Complete these steps to configure Bandwidth Management for site-to-site tunnels.

1. Select **Configuration > Policy Management > Traffic Management > Bandwidth Policies** and click **Add** to define a new LAN-to-LAN bandwidth policy.

In this example, a policy called 'L2L_tunnel' was configured with a bandwidth reservation of 256 kbps.

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: 10510 bytes Enter the amount of data allowed in a burst before excess packets will be dropped.

Apply Cancel

2. Apply the bandwidth policy to the existing LAN-to-LAN tunnel under the Bandwidth Policy drop-down menu.

Configuration | System | Tunneling Protocols | IPsec | LAN to LAN | Add

Add a new IPsec LAN-to-LAN connection.

Name	<input type="text" value="to_spoke"/>	Enter the name for this LAN-to-LAN connection.
Interface	<input type="text" value="Ethernet2 (Public) (172.18.124.135)"/>	Select the interface for this LAN-to-LAN connection.
Peer	<input type="text" value="172.18.124.134"/>	Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate	<input type="text" value="None (Use Freshshared Keys)"/>	Select the digital certificate to use.
Certificate	<input type="radio"/> Entire certificate chain	Choose how to send the digital certificate to the IKE peer.
Transmission	<input checked="" type="radio"/> Identity certificate only	
Freshshared Key	<input type="text" value="josco123"/>	Enter the preshared key for this LAN-to-LAN connection.
Authentication	<input type="text" value="ESP/MO5/HMAC-128"/>	Specify the packet authentication mechanism to use.
Encryption	<input type="text" value="3DES-168"/>	Specify the encryption mechanism to use.
IKE Proposal	<input type="text" value="IKE-3DES-MO5"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter	<input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPsec NAT-T	<input type="checkbox"/>	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	<input type="text" value="LAN_tunnel"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing	<input type="text" value="None"/>	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	<input type="text" value="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	<input type="text" value="14.30.0.0"/>	
Wildcard Mask	<input type="text" value="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.

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

Network List	<input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address	<input type="text" value="10.100.100.0"/>	
Wildcard Mask	<input type="text" value="0.0.255"/>	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.

Configure Bandwidth Management for Remote VPN Tunnels

Complete these steps to configure Bandwidth Management for remote VPN tunnels.

1. Select **Configuration > Policy Management > Traffic Management > Bandwidth Policies** and click **Add** to create a new bandwidth policy.

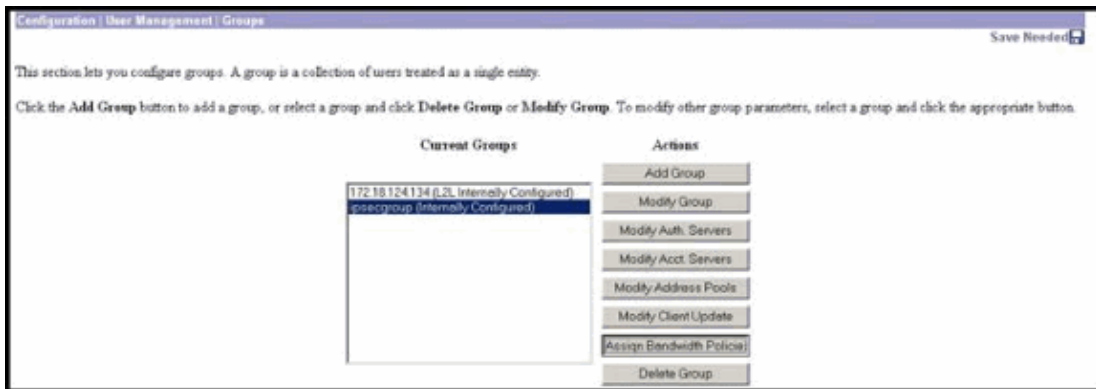
In this example, a policy called 'RA_tunnels' is configured with a bandwidth reservation of 8 kbps. Traffic Policing is configured with a policing rate of 128 kbps and a burst size of 24000 bytes.

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.

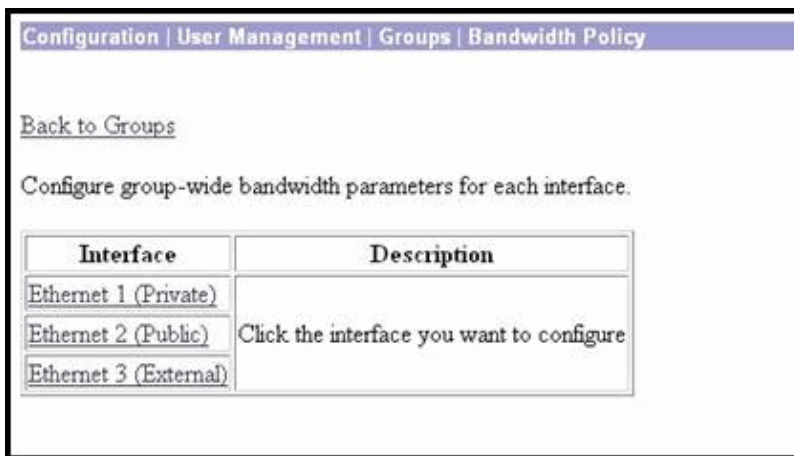
Policy Name	<input type="text" value="RA_tunnels"/>	Enter a unique name for this policy.
<input checked="" type="checkbox"/> Bandwidth Reservation		Check to reserve a minimum bandwidth per session.
Minimum Bandwidth	<input type="text" value="8"/> <input type="text" value="kbps"/>	Enter the minimum bandwidth.
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.		
<input checked="" type="checkbox"/> Policing		Check to enable Policing.
Policing Rate	<input type="text" value="128"/> <input type="text" value="kbps"/>	Enter the policing rate. Traffic below this rate will be transmitted, traffic above this rate will be dropped.
Normal Burst Size	<input type="text" value="24000"/> <input type="text" value="bytes"/>	Enter the amount of data allowed in a burst before excess packets will be dropped.

2. To apply the bandwidth policy to a remote access VPN group, select **Configuration > User Management > Groups**, select your group, and click **Assign Bandwidth Policies**.



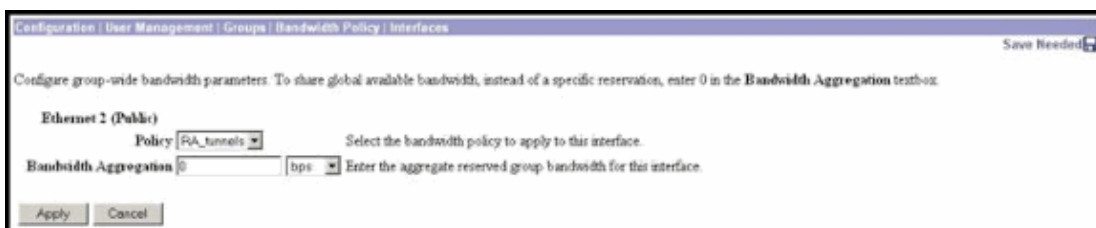
3. Click the interface on which you want to configure Bandwidth Management for this group.

In this example, 'Ethernet2 (Public)' is the selected interface for the group. To apply a bandwidth policy to a group on an interface, Bandwidth Management must be enabled on that interface. If you choose an interface on which Bandwidth Management is disabled, a warning message appears.



4. Select the bandwidth policy for the VPN group for this interface.

The RA_tunnels policy, which was previously defined, is selected for this group. Enter a value for the minimum bandwidth to reserve for this group. The default value of Bandwidth Aggregation is 0. The default unit of measurement is bps. If you want the group to share in the available bandwidth on the interface, enter **0**.



Verify

Select **Monitoring > Statistics > Bandwidth Management** on the VPN 3000 Concentrator to monitor Bandwidth Management.

Monitoring Statistics Bandwidth Management		Wednesday, 14 August 2002 14:56:33			
		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
ipseccgroup (In)	Ethernet 2 (Public)	10	5	143342	1004508
ipseccgroup (Out)	Ethernet 2 (Public)	11	3	1321526	749700
no_spoke (In)	Ethernet 2 (Public)	1539	237	206052492	23069858
no_spoke (Out)	Ethernet 2 (Public)	1539	593	206052492	118751970

Troubleshoot

To troubleshoot any problems while Bandwidth Management is implemented on the VPN 3000 Concentrator, enable these two Event Classes under **Configuration > System > Events > Classes**:

- **BMGT** (with Severity to Log: 1–9)
- **BMGTDBG** (with Severity to Log: 1–9)

These are some of the most common event log messages:

- The Exceeds the Aggregate Reservation error message is seen on the logs when a Bandwidth Policy is modified.

```
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.
```

If this error message is displayed, return to the group settings and un-apply the 'RA_tunnel' policy from the group. Edit the 'RA_tunnel' with the correct values and then re-apply the policy back to the specific group.

- Unable to find interface bandwidth.

```
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.
```

You may receive this error if the bandwidth policy is not enabled on the interface and you try to apply it on the LAN-to-LAN tunnel. If this is the case, apply a policy to the public interface as explained in the Configure a Default Bandwidth Policy on the VPN 3000 Concentrator section.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
 - [Cisco VPN 3000 Series Client Support Page](#)
 - [IPSec Support Page](#)
 - [Technical Support – Cisco Systems](#)
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 19, 2007

Document ID: 60329
