

# VPN 3000集中器頻寬管理配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[慣例](#)

[在VPN 3000集中器上配置預設頻寬策略](#)

[為站點到站點隧道配置頻寬管理](#)

[為遠端VPN隧道配置頻寬管理](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本文檔介紹在思科VPN 3000集中器上配置頻寬管理功能所需的步驟，用於：

- [站點到站點 \( LAN到LAN \) VPN隧道](#)
- [遠端訪問VPN隧道](#)

**注意：**在配置遠端訪問或站點到站點VPN隧道之前，必須首先在[VPN 3000集中器上配置預設頻寬策略](#)。

頻寬管理有兩個要素：

- **頻寬管制** — 限制隧道傳輸流量的最大速率。VPN集中器傳輸它接收的低於此速率的流量，並丟棄超過此速率的流量。
- **頻寬預留(Bandwidth Reservation)** — 為通過隧道傳輸的流量預留最小頻寬速率。「頻寬管理」允許您為組和使用者公平分配頻寬。這可防止某些組或使用者佔用大部分頻寬。

頻寬管理僅適用於隧道流量（第2層隧道協定[L2TP]、點對點隧道協定[PPTP]、IPSec），通常應用於公共介面。

頻寬管理功能為遠端訪問和站點到站點VPN連線提供了管理優勢。遠端訪問VPN隧道使用頻寬策略，以便寬頻使用者不會使用所有頻寬。反之，管理員可以為站點到站點隧道配置頻寬保留，以保證每個遠端站點有最低頻寬量。

## 必要條件

### 需求

本文件沒有特定需求。

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

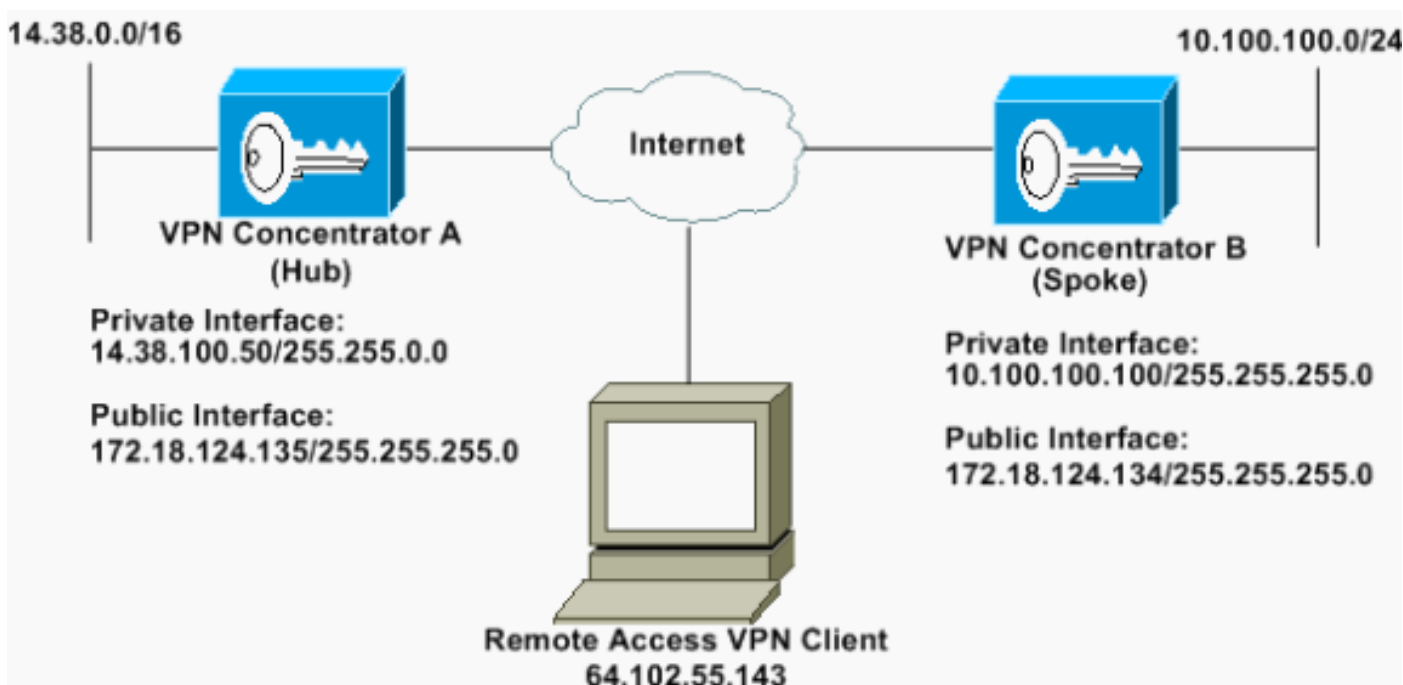
- Cisco VPN 3000 Concentrator ( 軟體版本4.1.x及更高版本 )

註：3.6版引入了頻寬管理功能。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 網路圖表

本檔案會使用以下網路設定：



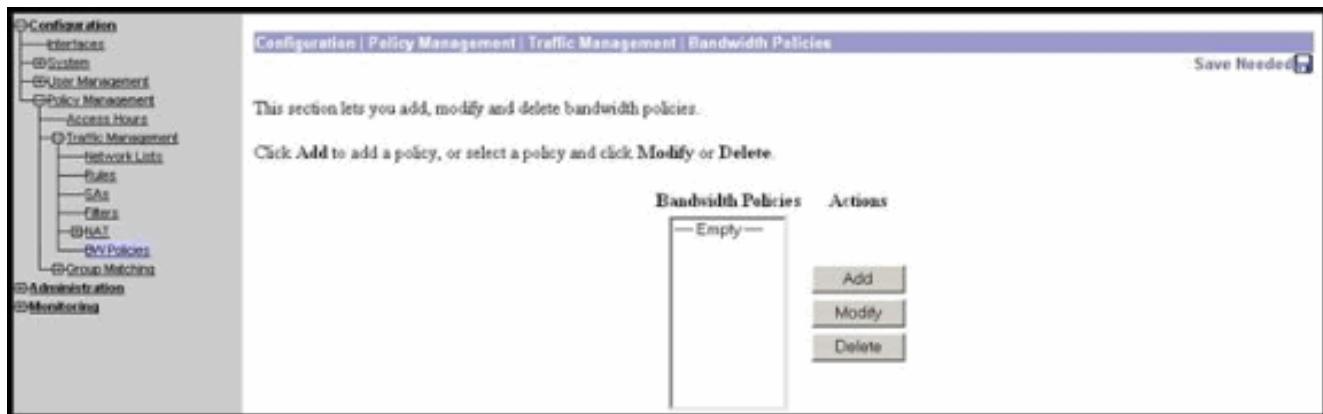
## 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

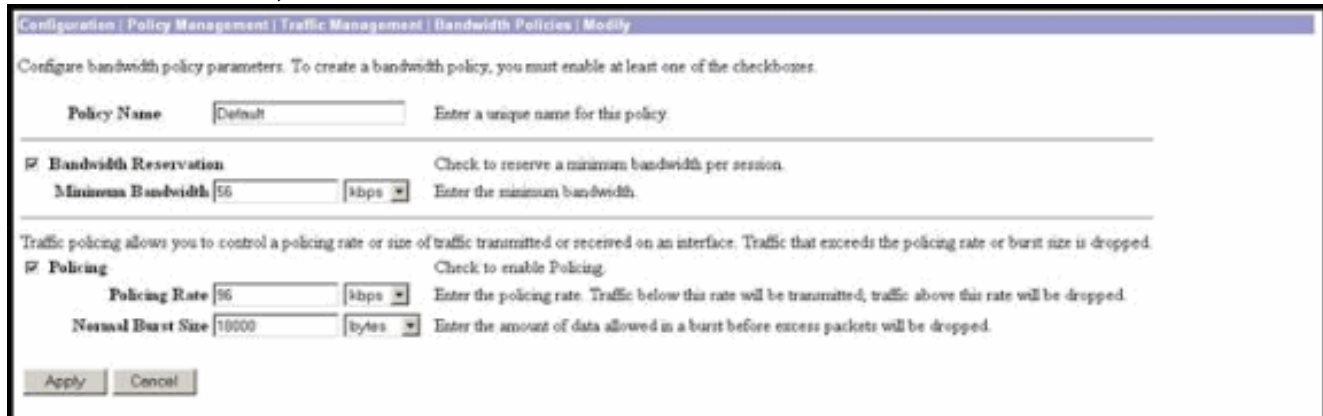
## 在VPN 3000集中器上配置預設頻寬策略

必須先在公共介面上啟用頻寬管理，然後才能在LAN到LAN隧道或遠端訪問隧道上配置頻寬管理。在此示例配置中，配置了預設頻寬策略。此預設策略應用於未將頻寬管理策略應用於其在VPN集中器中所屬組的使用者/隧道。

1. 要配置策略，請選擇Configuration > Policy Management > Traffic Management > Bandwidth Policies，然後點選Add。



按一下「新增」後，將顯示「修改」視窗。



2. 在「修改」視窗中設定這些引數。**Policy Name** — 輸入可以幫助您記住策略的唯一策略名稱。最大長度為32個字元。在本示例中，名稱「Default」被配置為策略名稱。**Bandwidth Reservation** — 選中**Bandwidth Reservation**復選框，為每個會話保留最小頻寬量。在本示例中，為不屬於已配置頻寬管理的組的所有VPN使用者保留56 kbps頻寬。**Policing** — 選中**Policing**覈取方塊以啟用管制。為Policing Rate輸入值，並選擇度量單位。VPN集中器傳輸低於管制速率的流量，並丟棄高於管制速率的所有流量。為頻寬策略配置了96 kbps。正常突發量大小是VPN集中器可在任何給定時間傳送的即時突發量。要設定突發大小，請使用以下公式：
 
$$(\text{Policing Rate}/8) * 1.5$$
 使用此公式，突發速率是18000位元組。
3. 按一下「Apply」。
4. 選擇**Configuration > Interfaces > Public Interface**，然後按一下Bandwidth頁籤將預設頻寬策略應用到介面。
5. 啟用**Bandwidth Management**選項。
6. 指定鏈路速率。鏈路速率是通過Internet進行網路連線的速度。在本示例中，使用到Internet的T1連線。因此，1544 kbps是配置的鏈路速率。
7. 從Bandwidth Policy下拉選單中選擇一個策略。在此介面之前配置了預設策略。您在此應用的策略是此介面上所有使用者的預設頻寬策略。此策略將應用於沒有對其組應用頻寬管理策略的使用者。

Configuration | Interfaces | Ethernet 2

You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

**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

## 為站點到站點隧道配置頻寬管理

完成以下步驟，為站點到站點隧道配置頻寬管理。

1. 選擇 Configuration > Policy Management > Traffic Management > Bandwidth Policies，然後按一下 Add 以定義新的 LAN 到 LAN 頻寬策略。在本示例中，名為「L2L\_tunnel」的策略配置了 256 kbps 的頻寬保留。

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: 50 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

2. 在 Bandwidth Policy 下拉選單下，將頻寬策略應用於現有的 LAN 到 LAN 隧道。

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 Transmission:  Entire certificate chain  
 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:

## 為遠端VPN隧道配置頻寬管理

完成以下步驟，為遠端VPN隧道配置頻寬管理。

1. 選擇 Configuration > Policy Management > Traffic Management > Bandwidth Policies，然後點選 Add 以建立新的頻寬策略。在本示例中，名為「RA\_tunnels」的策略配置了 8 kbps 的頻寬保留。流量管制配置為管制速率 128 kbps，突發大小 24000 位元組。

Configurations | 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.

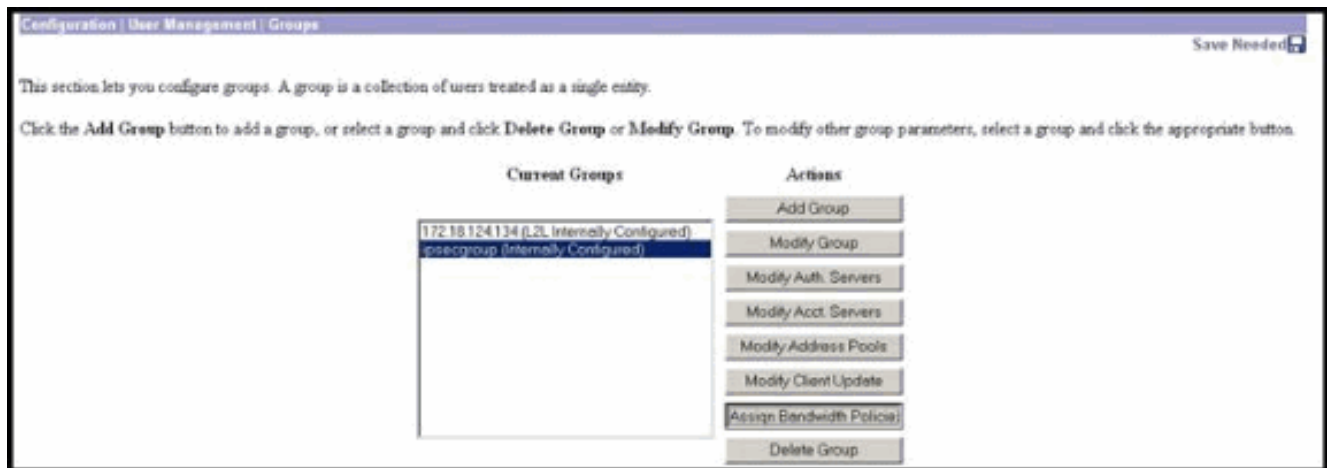
Policy Name:  Enter a unique name for this policy.

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.

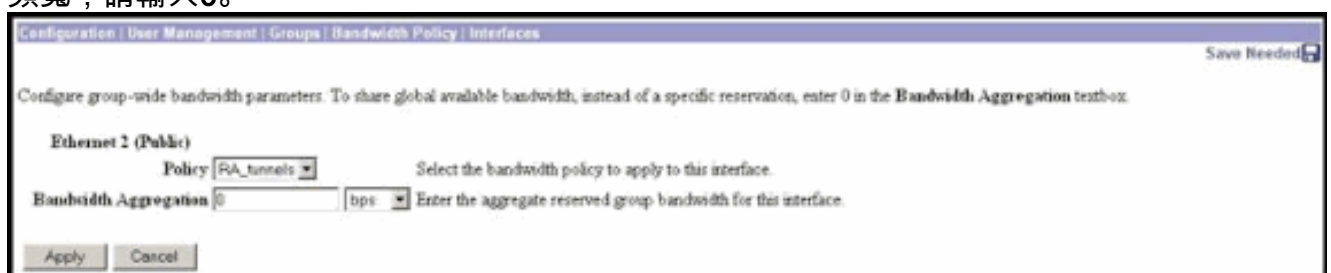
2. 要將頻寬策略應用於遠端訪問VPN組，請選擇 Configuration > User Management > Groups，選擇您的組，然後按一下 Assign Bandwidth Policies。



3. 按一下要為其配置頻寬管理的介面。在本示例中，「Ethernet2(Public)」是組的選定介面。要將頻寬策略應用於介面上的組，必須在該介面上啟用頻寬管理。如果選擇禁用頻寬管理的介面，則會顯示一條警告消息。



4. 為此介面的VPN組選擇頻寬策略。為此組選擇RA\_tunnels策略（以前已定義）。輸入要為此組保留的最小頻寬值。頻寬聚合的預設值為0。預設度量單位為bps。如果希望組共用介面的可用頻寬，請輸入0。



## 驗證

在VPN 3000 Concentrator上選擇Monitoring > Statistics > Bandwidth Management以監控Bandwidth Management。



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
ipsecgw (In)	Ethernet 2 (Public)	10	5	143342	1001508
ipsecgw (Out)	Ethernet 2 (Public)	11	9	1321526	74900
co_spoke (In)	Ethernet 2 (Public)	1539	237	206052492	23069858
co_spoke (Out)	Ethernet 2 (Public)	1539	588	206052492	118751970

## 疑難排解

要在VPN 3000集中器上實施頻寬管理時排除任何問題，請在**Configuration > System > Events > Classes**下啟用這兩個事件類：

- **BMGT**(嚴重性為日誌：1-9)
- **BMGTDBG**(嚴重性為日誌：1-9)

以下是一些最常見的事件日誌消息：

- 修改頻寬策略時，在日誌上顯示Exceeded the Aggregate Reservation錯誤消息。

**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.

如果顯示此錯誤消息，請返回到組設定並從組中取消應用「RA\_tunnel」策略。使用正確的值編輯「RA\_tunnel」，然後將策略重新應用到特定組。

- 無法找到介面頻寬。

**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.

如果在介面上未啟用頻寬策略，並嘗試將其應用於LAN到LAN隧道，則可能會收到此錯誤。如果是這種情況，請按照[在VPN 3000集中器上配置預設頻寬策略](#)一節中的說明，將策略應用到公共介面。

## 相關資訊

- [Cisco VPN 3000系列集中器支援頁面](#)
- [Cisco VPN 3000系列使用者端支援頁面](#)
- [IPSec支援頁面](#)
- [技術支援 - Cisco Systems](#)