

Konfigurationsbeispiel für die Bandbreitenverwaltung des VPN 3000 Concentrator

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdigramm](#)

[Konventionen](#)

[Konfigurieren einer Standard-Bandbreitenrichtlinie für den VPN 3000-Konzentrator](#)

[Konfigurieren der Bandbreitenverwaltung für Site-to-Site-Tunnel](#)

[Konfigurieren der Bandbreitenverwaltung für Remote-VPN-Tunnel](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden die erforderlichen Schritte zur Konfiguration der Bandbreitenmanagementfunktion im Cisco VPN 3000 Concentrator für folgende Aufgaben beschrieben:

- [Site-to-Site \(LAN-to-LAN\)-VPN-Tunnel](#)
- [VPN-Tunnel für Remote-Zugriff](#)

Hinweis: Bevor Sie Remote-Zugriff oder Site-to-Site-VPN-Tunnel konfigurieren, müssen Sie zuerst [eine Standardbandbreitenrichtlinie für den VPN 3000-Concentrator konfigurieren](#).

Es gibt zwei Elemente des Bandbreitenmanagements:

- **Bandwidth Policing** (Bandbreitenüberwachung): Limitiert die maximale Rate für getunnelten Datenverkehr. Der VPN Concentrator überträgt den eingehenden Datenverkehr unter diese Rate und verwirft den Datenverkehr, der diese Rate überschreitet.
- **Bandbreitenreservierung** - Legt eine Mindestbandbreite für getunnelten Datenverkehr beiseite. Mit dem Bandbreitenmanagement können Sie Gruppen und Benutzern Bandbreite gerecht zuweisen. Dadurch wird verhindert, dass bestimmte Gruppen oder Benutzer den Großteil der Bandbreite beanspruchen.

Das Bandbreitenmanagement gilt nur für getunnelten Datenverkehr (Layer 2 Tunnel Protocol [L2TP], Point to Point Tunneling Protocol [PPTP], IPSec) und wird meist auf die öffentliche Schnittstelle angewendet.

Die Funktion Bandbreitenmanagement bietet administrative Vorteile für den Remote-Zugriff und Site-to-Site-VPN-Verbindungen. Die VPN-Tunnel für den Remote-Zugriff verwenden Bandwidth Policing, sodass Breitbandbenutzer nicht die gesamte Bandbreite nutzen. Umgekehrt kann der Administrator die Bandbreitenreservierung für Site-to-Site-Tunnel konfigurieren, um jedem Remote-Standort eine Mindestbandbreite zu garantieren.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

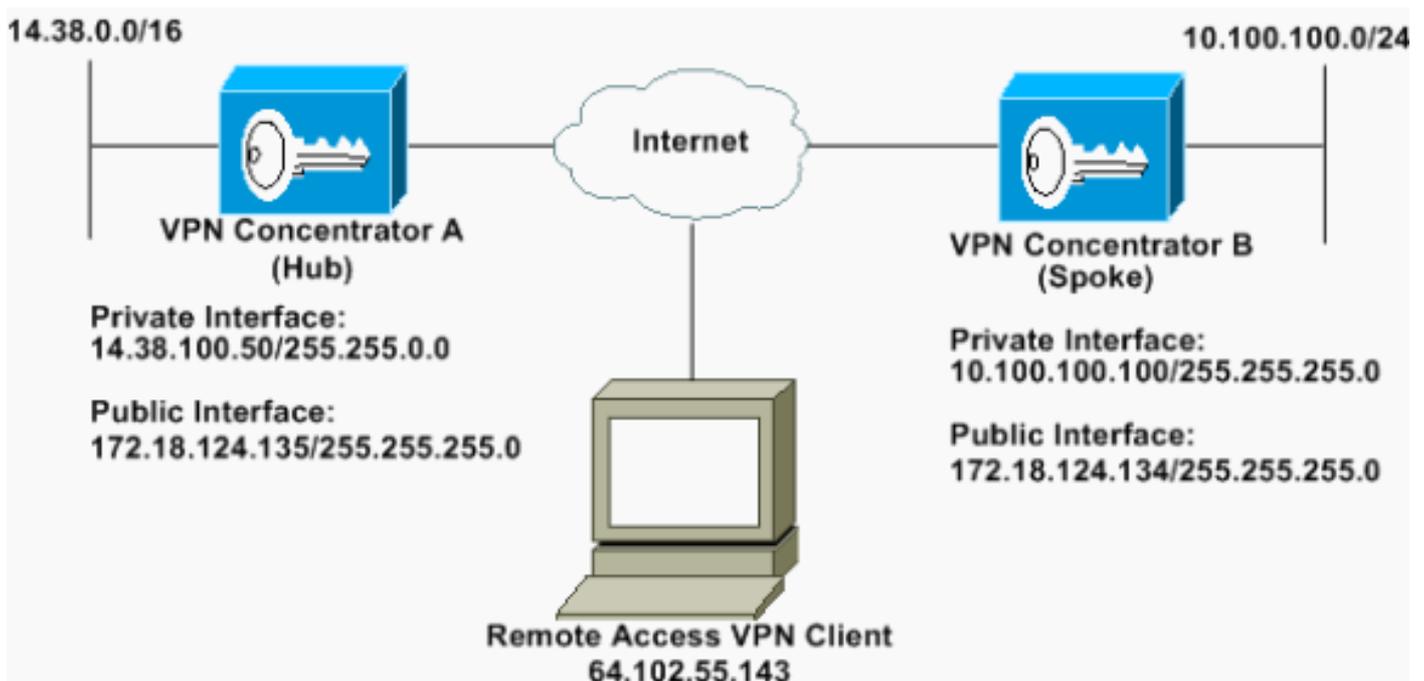
- Cisco VPN 3000 Concentrator mit Software-Versionen 4.1.x und höher

Hinweis: Die Funktion Bandbreitenmanagement wurde in Version 3.6 eingeführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdigramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#).

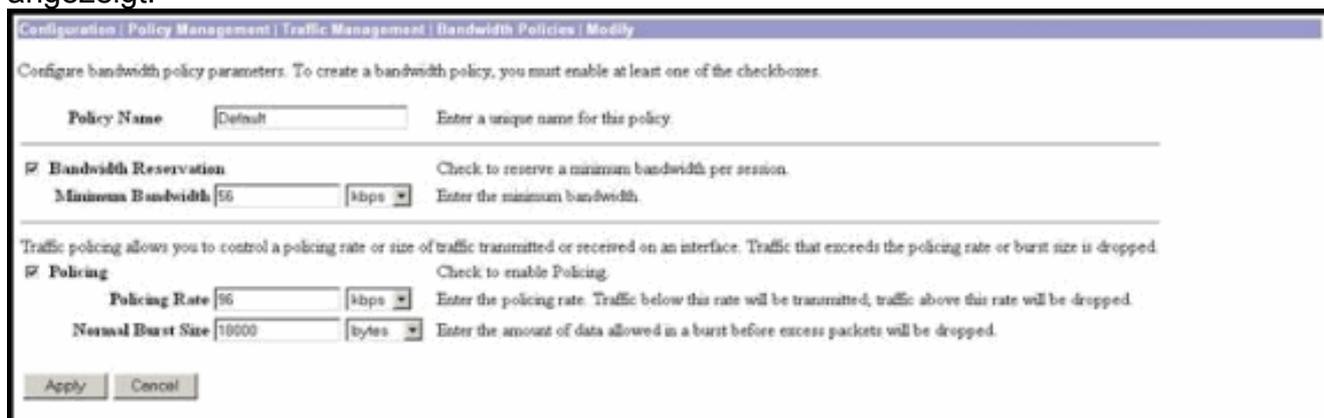
Konfigurieren einer Standard-Bandbreitenrichtlinie für den VPN 3000-Konzentrator

Bevor Sie die Bandbreitenverwaltung in den LAN-zu-LAN-Tunneln oder in den Remote-Zugriffstunneln konfigurieren können, müssen Sie die Bandbreitenverwaltung auf der öffentlichen Schnittstelle aktivieren. In dieser Beispielkonfiguration wird eine Standardbandbreitenrichtlinie konfiguriert. Diese Standardrichtlinie wird auf Benutzer/Tunnel angewendet, für die keine Bandbreitenmanagementrichtlinie auf die Gruppe angewendet wurde, der sie im VPN-Concentrator angehören.

1. Um eine Richtlinie zu konfigurieren, wählen Sie **Konfiguration > Richtlinienmanagement > Datenverkehrsmanagement > Bandbreitenrichtlinien** aus, und klicken Sie auf **Hinzufügen**.



Nachdem Sie auf Hinzufügen geklickt haben, wird das Fenster **Ändern** angezeigt.



2. Legen Sie diese Parameter im Fenster **Ändern** fest. **Policy Name** (Richtliniennamen): Geben Sie einen eindeutigen Richtliniennamen ein, mit dem Sie sich die Richtlinie merken können. Die maximale Länge beträgt 32 Zeichen. In diesem Beispiel wird der Name 'Default' als Richtliniennamen konfiguriert. **Bandbreitenreservierung** - Aktivieren Sie das Kontrollkästchen **Bandbreitenreservierung**, um eine Mindestbandbreite für jede Sitzung zu reservieren. In diesem Beispiel ist 56 Kbit/s Bandbreite für alle VPN-Benutzer reserviert, die nicht zu einer Gruppe gehören, für die das Bandbreitenmanagement konfiguriert ist. **Policing**: Aktivieren Sie das Kontrollkästchen **Policing**, um die Richtlinienvergabe zu aktivieren. Geben Sie einen Wert für die Policing-Rate ein, und wählen Sie die Maßeinheit aus. Der VPN Concentrator überträgt Datenverkehr, der sich unterhalb der Regelungsrate bewegt, und verwirft den

gesamten Datenverkehr, der über die Regelungsrate hinausgeht. 96 Kbit/s sind für das Bandwidth Policing konfiguriert. Die normale Burst-Größe ist die Menge an momentanem Burst, die der VPN Concentrator jederzeit senden kann. Verwenden Sie folgende Formel, um die Burst-Größe festzulegen:

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

Mit dieser Formel beträgt die Burst Rate 18.000 Byte.

3. Klicken Sie auf **Übernehmen**.
4. Wählen Sie **Konfiguration > Schnittstellen > Öffentliche Schnittstelle**, und klicken Sie auf die Registerkarte Bandbreite, um die Standardbandbreitenrichtlinie auf eine Schnittstelle anzuwenden.
5. Aktivieren Sie die Option **Bandbreitenverwaltung**.
6. Geben Sie die Verbindungsrate an. Die Verbindungsrate ist die Geschwindigkeit der Netzwerkverbindung über das Internet. In diesem Beispiel wird eine T1-Verbindung zum Internet verwendet. Folglich ist 1544 Kbit/s die konfigurierte Verbindungsrate.
7. Wählen Sie eine Richtlinie aus der Dropdown-Liste Bandbreitenrichtlinie aus. Die Standardrichtlinie wurde für diese Schnittstelle zuvor konfiguriert. Die hier angewendete Richtlinie ist eine Standardbandbreitenrichtlinie für alle Benutzer dieser Schnittstelle. Diese Richtlinie wird auf Benutzer angewendet, für die keine Bandbreitenmanagementrichtlinie auf ihre Gruppe angewendet wurde.

The screenshot shows the configuration page for Ethernet Interface 2 (Public). It features a warning icon and text: "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." Below this, the page is titled "Configuring Ethernet Interface 2 (Public)." and has tabs for "General", "RIP", "OSPF", and "Bandwidth". The "Bandwidth" tab is active, displaying a table of "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.

At the bottom of the form are "Apply" and "Cancel" buttons.

[Konfigurieren der Bandbreitenverwaltung für Site-to-Site-Tunnel](#)

Führen Sie diese Schritte aus, um die Bandbreitenverwaltung für Site-to-Site-Tunnel zu konfigurieren.

1. Wählen Sie **Konfiguration > Richtlinienmanagement > Datenverkehrsmanagement > Bandbreitenrichtlinien aus**, und klicken Sie auf **Hinzufügen**, um eine neue LAN-zu-LAN-Bandbreitenrichtlinie zu definieren. In diesem Beispiel wurde eine Richtlinie namens "L2L_tunnel" mit einer Bandbreitenreservierung von 256 Kbit/s konfiguriert.

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. Wenden Sie die Bandbreitenrichtlinie auf den vorhandenen LAN-to-LAN-Tunnel im Dropdown-Menü Bandwidth Policy (Bandbreitenrichtlinie) an.

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 Choose how to send the digital certificate to the IKE peer.
 Identity certificate only
 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:
 Wildcard Mask: 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.

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:
 Wildcard Mask: 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.

[Konfigurieren der Bandbreitenverwaltung für Remote-VPN-Tunnel](#)

Führen Sie diese Schritte aus, um die Bandbreitenverwaltung für Remote-VPN-Tunnel zu konfigurieren.

1. Wählen Sie **Konfiguration > Richtlinienmanagement > Datenverkehrsmanagement > Bandbreitenrichtlinien aus**, und klicken Sie auf **Hinzufügen**, um eine neue Bandbreitenrichtlinie zu erstellen. In diesem Beispiel wird eine Richtlinie mit dem Namen "RA_tunnels" mit einer Bandbreitenreservierung von 8 Kbit/s konfiguriert. Das Traffic-Policing wird mit einer Regelungsrate von 128 Kbit/s und einer Burst-Größe von 24.000 Byte konfiguriert.

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.

- Um die Bandbreitenrichtlinie auf eine VPN-Gruppe für den Remote-Zugriff anzuwenden, wählen Sie **Konfiguration > Benutzerverwaltung > Gruppen aus**, wählen Sie Ihre Gruppe aus, und klicken Sie auf **Bandbreitenrichtlinien zuweisen**.

Configuration | User Management | 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 select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, select a group and click the appropriate button.

Current Groups	Actions
<input type="checkbox"/> 172.18.124.134 (L2L Internally Configured) <input checked="" type="checkbox"/> ipsecgroup (Internally Configured)	<input type="button" value="Add Group"/> <input type="button" value="Modify Group"/> <input type="button" value="Modify Auth. Servers"/> <input type="button" value="Modify Acct. Servers"/> <input type="button" value="Modify Address Pools"/> <input type="button" value="Modify Client Update"/> <input type="button" value="Assign Bandwidth Policy"/> <input type="button" value="Delete Group"/>

- Klicken Sie auf die Schnittstelle, auf der Sie die Bandbreitenverwaltung für diese Gruppe konfigurieren möchten. In diesem Beispiel ist "Ethernet2 (Public)" die ausgewählte Schnittstelle für die Gruppe. Um eine Bandbreitenrichtlinie auf eine Gruppe einer Schnittstelle anzuwenden, muss die Bandbreitenverwaltung auf dieser Schnittstelle aktiviert sein. Wenn Sie eine Schnittstelle auswählen, auf der die Bandbreitenverwaltung deaktiviert ist, wird eine Warnmeldung

Configuration | User Management | Groups | Bandwidth Policy

[Back to Groups](#)

Configure group-wide bandwidth parameters for each interface.

Interface	Description
Ethernet 1 (Private)	Click the interface you want to configure
Ethernet 2 (Public)	
Ethernet 3 (External)	

angezeigt.

- Wählen Sie die Bandbreitenrichtlinie für die VPN-Gruppe für diese Schnittstelle aus. Die zuvor definierte RA_tunnels-Richtlinie wird für diese Gruppe ausgewählt. Geben Sie einen

Wert für die Mindestbandbreite ein, die für diese Gruppe reserviert werden soll. Der Standardwert für die Bandbreitenaggregation ist 0. Die Standardmesseinheit ist bps. Wenn die Gruppe die verfügbare Bandbreite der Schnittstelle gemeinsam nutzen soll, geben Sie 0 ein.

Überprüfen

Wählen Sie **Monitoring > Statistics > Bandwidth Management** im VPN 3000 Concentrator aus, um das Bandbreitenmanagement zu überwachen.

User Name	Interface	Traffic Rate (kbps)		Traffic Volume (bytes)	
		Conformed	Throttled	Conformed	Throttled
ipsecsec: (In)	Ethernet 2 (Public)	10	5	143342	1004508
ipsecsec: (Out)	Ethernet 2 (Public)	11	0	1331526	74700
po_spoke: (In)	Ethernet 2 (Public)	1539	237	206952492	23069658
po_spoke: (Out)	Ethernet 2 (Public)	1539	588	206952492	118751970

Fehlerbehebung

Um Probleme zu beheben, während die Bandbreitenverwaltung im VPN 3000-Konzentrator implementiert ist, aktivieren Sie die folgenden beiden Ereignisklassen unter **Configuration > System > Events > Classes**:

- **BMGT** (mit "Severity to Log" (Zu protokollierender Schweregrad): 1-9)
- **BMGTDBG** (Protokollschweregrad: 1-9)

Dies sind einige der häufigsten Ereignisprotokollmeldungen:

- Die Fehlermeldung `Aggregate Reservation` wird bei Änderung einer Bandbreitenrichtlinie in den Protokollen angezeigt.

```
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.
```

Wenn diese Fehlermeldung angezeigt wird, kehren Sie zu den Gruppeneinstellungen zurück, und deaktivieren Sie die Anwendung der Richtlinie 'RA_tunnel' aus der Gruppe. Bearbeiten Sie den 'RA_tunnel' mit den richtigen Werten, und wenden Sie die Richtlinie dann wieder auf die spezifische Gruppe an.

- Schnittstellenbandbreite kann nicht gefunden werden.

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.

Sie erhalten diesen Fehler möglicherweise, wenn die Bandbreitenrichtlinie auf der Schnittstelle nicht aktiviert ist und Sie versuchen, sie auf den LAN-to-LAN-Tunnel anzuwenden. In diesem Fall [wenden Sie eine Richtlinie auf die öffentliche Schnittstelle an](#), wie im Abschnitt [Konfigurieren einer Standard-Bandbreitenrichtlinie für den VPN 3000-Konzentrator](#) beschrieben.

Zugehörige Informationen

- [Support-Seite für Cisco VPN Konzentratoren der Serie 3000](#)
- [Cisco VPN Client Support-Seite der Serie 3000](#)
- [IPSec-Support-Seite](#)
- [Technischer Support - Cisco Systems](#)