

# Configuratievoorbeeld van VPN 3000 Concentrator-bandbreedtebeheer

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Conventies](#)

[Een standaard bandbreedtebeleid instellen op de VPN 3000-concentratie](#)

[Bandbreedtebeheer configureren voor site-to-site tunnels](#)

[Bandbreedtebeheer voor externe VPN-tunnels instellen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft de gewenste stappen die zijn gebruikt om de functie Bandbreedtebeheer te configureren in het Cisco VPN-centrator 3000 voor:

- [Site-to-site \(LAN-to-LAN\) VPN-tunnels](#)
- [Remote-toegang VPN-tunnels](#)

**Opmerking:** Voordat u externe toegang of site-to-site VPN-tunnels configureren moet u eerst [een standaard bandbreedte-beleid op VPN 3000 Concentrator](#) configureren.

Er zijn twee elementen van Bandbreedtebeheer:

- **Toezicht bandbreedte:** beperkt het maximale aantal tunnelverkeer. De VPN Concentrator zendt verkeer dat hij ontvangt toe onder dit tarief en druppelt verkeer af dat dit tarief overschrijdt.
- **Bandbreedtereservering-**Hiermee stelt u een minimum bandbreedte-tarief voor getunneerd verkeer in. Met Bandbreedtebeheer kunt u bandbreedte eerlijk toewijzen aan groepen en gebruikers. Dit voorkomt bepaalde groepen of gebruikers om een meerderheid van de bandbreedte te gebruiken.

Bandbreedtebeheer is alleen van toepassing op tunnelverkeer (Layer 2 Tunnel Protocol [L2TP], Point-to-Point Tunneling Protocol [PPTP], IPSec) en wordt het meest toegepast op de openbare interface.

De functie Bandbreedtebeheer biedt administratieve voordelen aan externe toegang en site-to-site VPN-verbindingen. De tunnels van de toegang op afstand VPN gebruiken Toezicht Bandbreedte

zodat breedbandgebruikers niet alle bandbreedte gebruiken. Omgekeerd kan de beheerder Bandbreedtereservering voor site-to-site tunnels configureren om een minimale bandbreedte voor elke externe site te garanderen.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

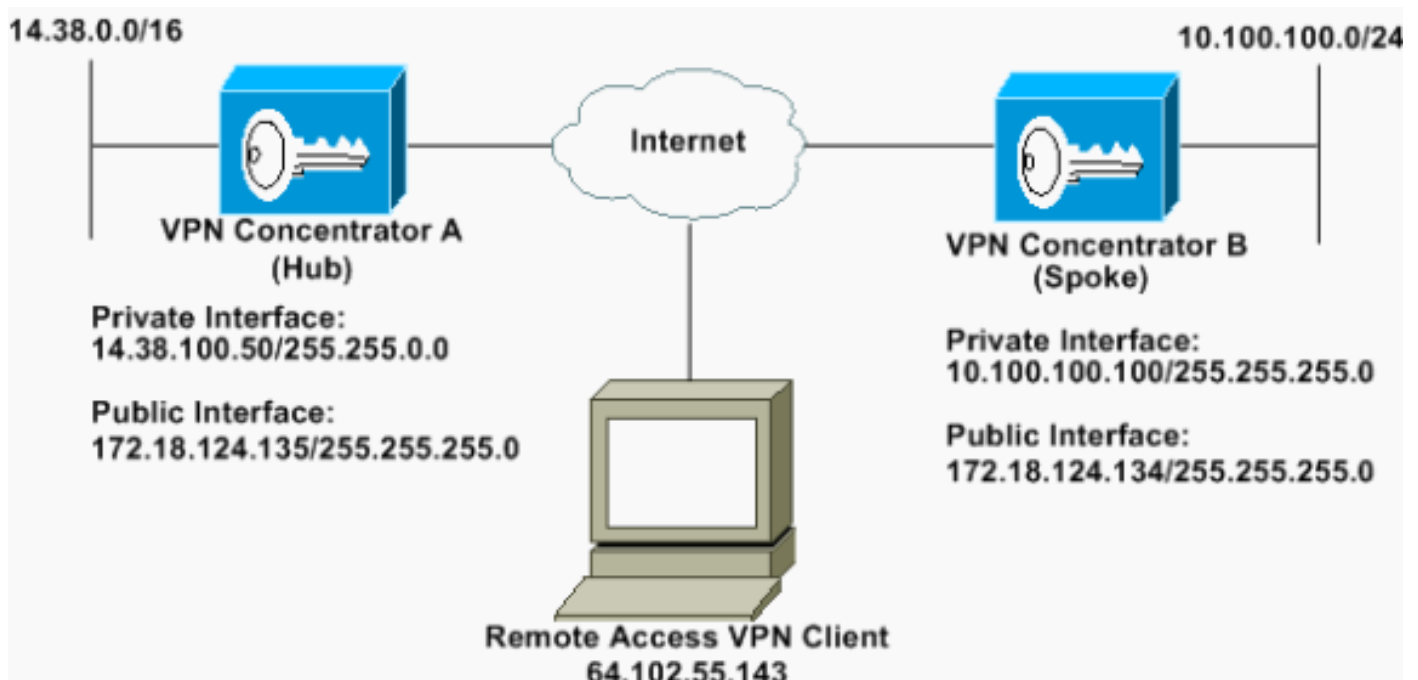
- Cisco VPN 3000 Concentrator met software-releases 4.1.x en hoger

**Opmerking:** De functie Bandbreedtebeheer is toegevoegd aan release 3.6.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

### Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



### Conventies

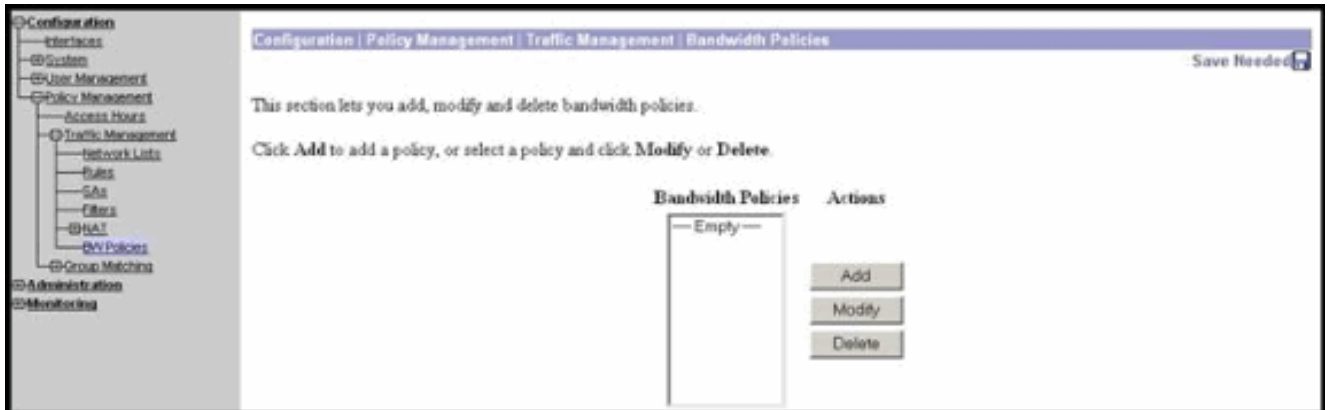
Raadpleeg voor meer informatie over documentconventies de [technische Tips](#) van [Cisco](#).

## Een standaard bandbreedtebeleid instellen op de VPN 3000-

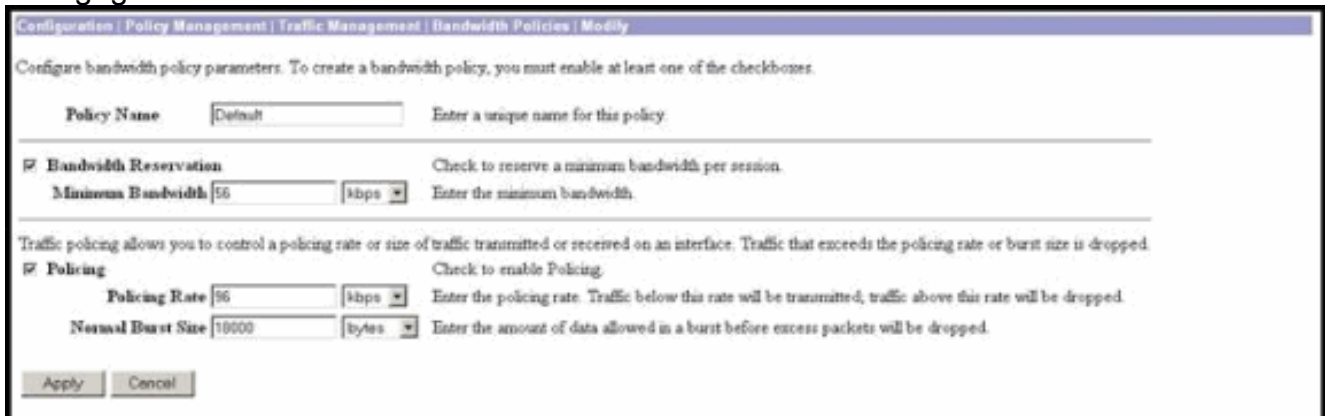
## concentratie

Voordat u Bandbreedtebeheer kunt configureren in de LAN-to-LAN tunnels of in de tunnels voor de toegang op afstand, moet u Bandbreedtebeheer op de openbare interface inschakelen. In deze voorbeeldconfiguratie wordt een standaard bandbreedtebeleid ingesteld. Dit standaardbeleid wordt toegepast op gebruikers/tunnels die geen beleid van het Bandbreedtebeheer hebben toegepast op de groep waartoe zij in de VPN-centrator behoren.

1. Om een beleid te configureren selecteert u **Configuration > Policy Management > Traffic Management > Bandbreedtebeleid** en klikt u op **Add**.



Nadat u op Add klikt, wordt het venster Wijzigen weergegeven.



2. Stel deze parameters in het venster Wijzigen in. **Beleidsnaam** - Voer een unieke beleidsnaam in die u kan helpen het beleid te onthouden. De maximale lengte is 32 tekens. In dit voorbeeld wordt de naam "Standaard" ingesteld als de beleidsnaam. **Bandbreedtereservering**-Controleer het vakje **Bandbreedtereservering** om een minimumhoeveelheid bandbreedte voor elke sessie te reserveren. In dit voorbeeld, wordt 56 kbps van bandbreedte gereserveerd voor alle gebruikers van VPN die niet onder een groep vallen die het Bandbreedtebeheer heeft geconfigureerd. **Toezicht**: controleer het aanvinkvakje **Toezicht** om toezicht mogelijk te maken. Geef een waarde op voor het instellen van de snelheid en selecteer de meeteenheid. De VPN Concentrator geeft verkeer door dat onder de politiekoers beweegt en laat al het verkeer vallen dat boven de politiesnelheid beweegt. 96 kbps wordt ingesteld voor Bandbreedteswitchtoezicht. De normale burst is de hoeveelheid momentane barst die de VPN Concentrator op een bepaald moment kan verzenden. Gebruik deze formule om de barstgrootte in te stellen:

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

Met deze formule is de Burst Rate 18000 bytes.

- Klik op **Apply** (Toepassen).
- Selecteer **Configuratie > Interfaces > Openbare interface** en klik op het tabblad **Bandbreedte** om het standaard bandbreedtebeleid op een interface toe te passen.
- De optie **Bandbreedtebeheer** inschakelen.
- Specificeer het koppelingstarief. De verbindingssnelheid is de snelheid van de netwerkverbinding door het internet. In dit voorbeeld wordt een T1-verbinding met internet gebruikt. Bijgevolg is 1544 kbps de geconfigureerde linksnelheid.
- Selecteer een beleid in de vervolgkeuzelijst **Bandbreedtebeleid**. Standaardbeleid wordt eerder ingesteld voor deze interface. Het beleid dat u hier toepast is een standaard bandbreedtebeleid voor alle gebruikers op deze interface. Dit beleid is van toepassing op gebruikers die geen **Bandbreedtebeheerbeleid** hebben dat op hun groep van toepassing is.

Configuration | Interfaces | Ethernet 2

**Configuring Ethernet Interface 2 (Public).**

General | IP | 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

## [Bandbreedtebeheer configureren voor site-to-site tunnels](#)

Voltooi deze stappen om **Bandbreedtebeheer** voor site-to-site tunnels te configureren.

- Selecteer **Configuration > Policy Management > Traffic Management > Bandbreedtebeleid** en klik op **Add** om een nieuw LAN-to-LAN bandbreedtebeleid te definiëren. In dit voorbeeld werd een beleid dat 'L2L\_tunnel' werd genoemd ingesteld met een bandbreedtereservering van 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: 10500 bytes Enter the amount of data allowed in a burst before excess packets will be dropped.

Apply Cancel

- Pas het bandbreedtebeleid op de bestaande LAN-to-LAN tunnel onder het vervolgkeuzemenu van het **Bandbreedtebeleid** toe.

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:

## [Bandbreedtebeheer voor externe VPN-tunnels instellen](#)

Voltooi deze stappen om Bandbreedtebeheer voor externe VPN-tunnels te configureren.

1. Selecteer **Configuration > Policy Management > Traffic Management > Bandbreedtebeleid** en klik op **Add** om een nieuw bandbreedtebeleid te maken. In dit voorbeeld wordt een beleid dat "RA\_tunnels" wordt genoemd ingesteld met een bandbreedtereservering van 8 kbps. Traffic Engineering is ingesteld met een politiesnelheid van 128 kbps en een barstgrootte van 2400 bytes.

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.

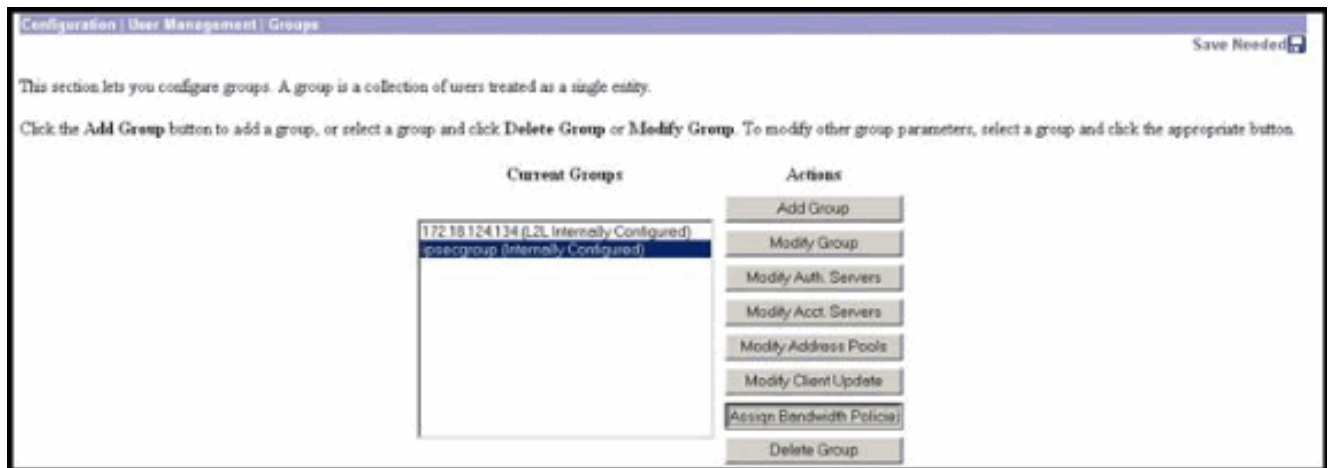
Traffic policing allows you to control a policing rate or size of traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped.

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.

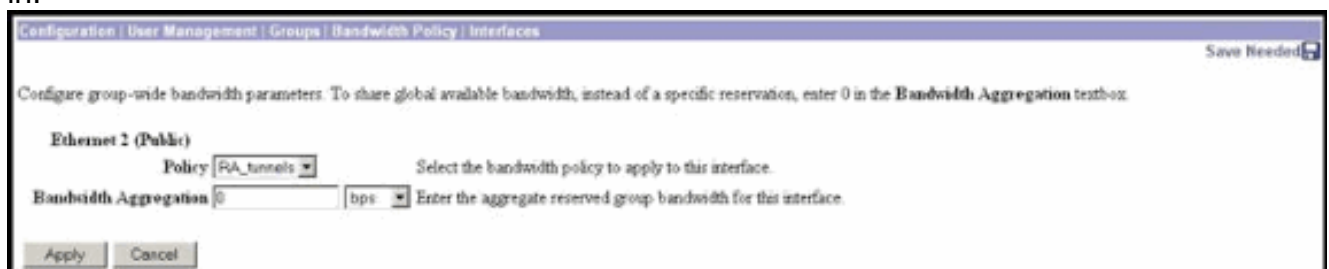
2. Als u het bandbreedtebeleid op een VPN-groep op afstand wilt toepassen, selecteert u **Configuration > User Management > Groepen**, selecteert u uw groep en klikt u op **Bandbreedtebeleid toewijzen**.



3. Klik op de interface waarop u het Bandbreedtebeheer voor deze groep wilt configureren. In dit voorbeeld is 'Ethernet2 (Public)' de geselecteerde interface voor de groep. Om een bandbreedtebeleid op een groep op een interface toe te passen, moet het Bandbreedtebeheer op die interface worden geactiveerd. Als u een interface kiest waarop het Bandbreedtebeheer is uitgeschakeld, verschijnt er een waarschuwingsbericht.



4. Selecteer het bandbreedtebeleid voor de groep van VPN voor deze interface. Het RA\_tunnels beleid, dat eerder werd gedefinieerd, wordt geselecteerd voor deze groep. Voer een waarde in voor de minimale bandbreedte die u voor deze groep wilt reserveren. De standaardwaarde van Bandwidth Aggregation is 0. De standaard meeteenheid is bps. Als u wilt dat de groep in de beschikbare bandbreedte op de interface deelt, voer 0 in.



Selecteer **Monitoring > Statistieken > Bandbreedtebeheer** in de VPN 3000-Concentrator om Bandbreedtebeheer te controleren.

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	1321526	74700
to_spoke (In)	Ethernet 2 (Public)	1539	237	206952492	23059658
to_spoke (Out)	Ethernet 2 (Public)	1539	588	206952492	118751970

## Problemen oplossen

Als u problemen wilt oplossen terwijl Bandbreedtebeheer is geïmplementeerd op de VPN 3000 Concentrator, schakelt u deze twee Event Classes in **Configuration > System > Events > Classes**:

- **BMGT** (met ernst aan logboek: 1-9)
- **BMGTDBG** (met ernst aan loggen: 1-9)

Dit zijn een paar van de meest voorkomende log berichten:

- De foutmelding `Aggregate Reservation` wordt in het logbestand overschreden wanneer een Bandbreedtebeleid wordt gewijzigd.

```
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.
```

Als deze foutmelding wordt weergegeven, zet u de groepsinstellingen terug en past u het RA\_tunnel beleid niet toe van de groep. Bewerk de "RA\_tunnel" met de juiste waarden en pas het beleid vervolgens opnieuw toe op de specifieke groep.

- Kan interfacebandbreedte niet vinden.

```
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.
```

U kunt deze fout ontvangen als het bandbreedtebeleid niet op de interface is ingeschakeld en u probeert deze op de LAN-to-LAN tunnel toe te passen. Als dit zich voordoet, [past u een beleid op de openbare interface toe](#) zoals uitgelegd in het [gedeelte Default Bandwidth Policy op VPN 3000 Concentrator](#).

## Gerelateerde informatie

- [Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina](#)
- [Cisco VPN 3000 Series clientondersteuningspagina](#)
- [IPsec-ondersteuningspagina](#)
- [Technische ondersteuning - Cisco-systemen](#)