

# زكرم ةم زحل ي ددرت لا قاطن لا ةرادا ني وكت لا ثم VPN 3000

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الرسم التخطيطي للشبكة](#)

[الاصطلاحات](#)

[تكوين سياسة النطاق الترددي الافتراضية على مركز VPN 3000](#)

[تكوين إدارة النطاق الترددي لأنفاق الموقع إلى الموقع](#)

[تكوين إدارة النطاق الترددي لأنفاق شبكات VPN البعيدة](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

## المقدمة

يصف هذا المستند الخطوات الضرورية المستخدمة لتكوين ميزة إدارة النطاق الترددي على مركز VPN 3000 من Cisco J:

• [أنفاق شبكة VPN من موقع إلى موقع \(LAN-to-LAN\)](#)

• [أنفاق شبكة VPN للوصول عن بعد](#)

**ملاحظة:** قبل تكوين أنفاق الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد أو الوصول من موقع إلى موقع، يجب عليك أولاً [تكوين سياسة عرض النطاق الترددي الافتراضية على مركز VPN 3000](#).

هناك عنصران لإدارة النطاق الترددي:

• **تنظيم عرض النطاق الترددي** — يحد من الحد الأقصى لمعدل حركة المرور النفقي. يرسل مركز VPN حركة

مرور يستلم هو أقل من هذا معدل ويخفض حركة مرور أن يتجاوز هذا معدل.

• **حجز النطاق الترددي** - قم بتخصيص الحد الأدنى لمعدل النطاق الترددي لحركة المرور النفقي. تسمح لك إدارة

النطاق الترددي العريض بتخصيص النطاق الترددي للمجموعات والمستخدمين بشكل منصف. وهذا يمنع

مجموعات معينة أو مستخدمين معينين من إستهلاك معظم عرض النطاق الترددي.

لا تنطبق إدارة النطاق الترددي إلا على حركة المرور النفقي (بروتوكول نفق الطبقة 2 [L2TP]، وبروتوكول الاتصال

النفقي من نقطة إلى نقطة [PPTP]، و IPsec) ويتم تطبيقها بشكل شائع على الواجهة العامة.

توفر ميزة "إدارة النطاق الترددي العريض" ميزات إدارية للوصول عن بعد واتصالات الشبكة الخاصة الظاهرية (VPN)

من موقع إلى موقع. تستخدم أنفاق الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد تنظيم النطاق الترددي

العريض حتى لا يستخدم مستخدمو النطاق الترددي العريض جميع النطاق الترددي. وعلى العكس، يمكن للمسؤول

تكوين "حجز النطاق الترددي" لأنفاق الموقع إلى الموقع لضمان الحد الأدنى من عرض النطاق الترددي لكل موقع

بعيد.

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

### المكونات المستخدمة

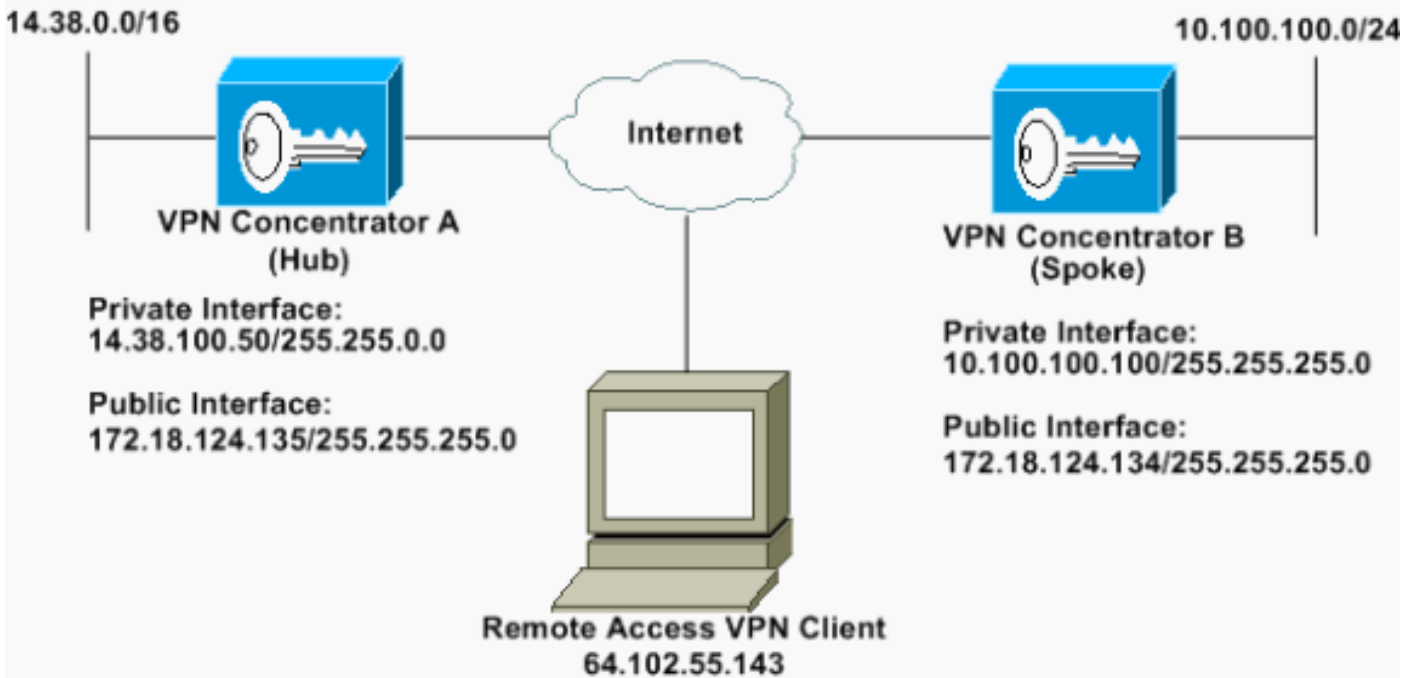
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- مركز VPN 3000 من Cisco مع إصدارات البرامج x.4.1 والإصدارات الأحدث
- ملاحظة: تم إدخال ميزة إدارة النطاق الترددي في الإصدار 3.6.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

### الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



### الاصطلاحات

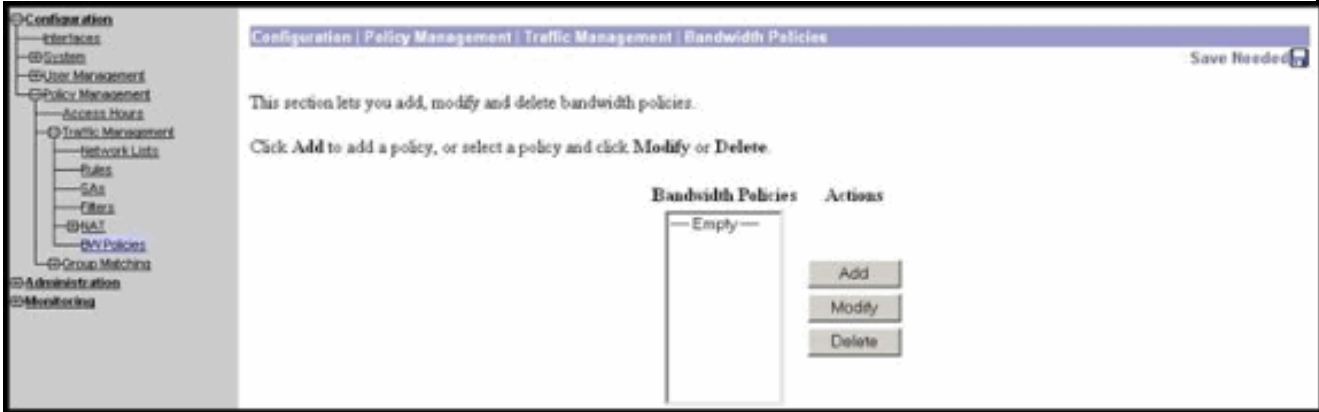
للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى [اصطلاحات تلميحات Cisco التقنية](#).

## تكوين سياسة النطاق الترددي الافتراضية على مركز VPN 3000

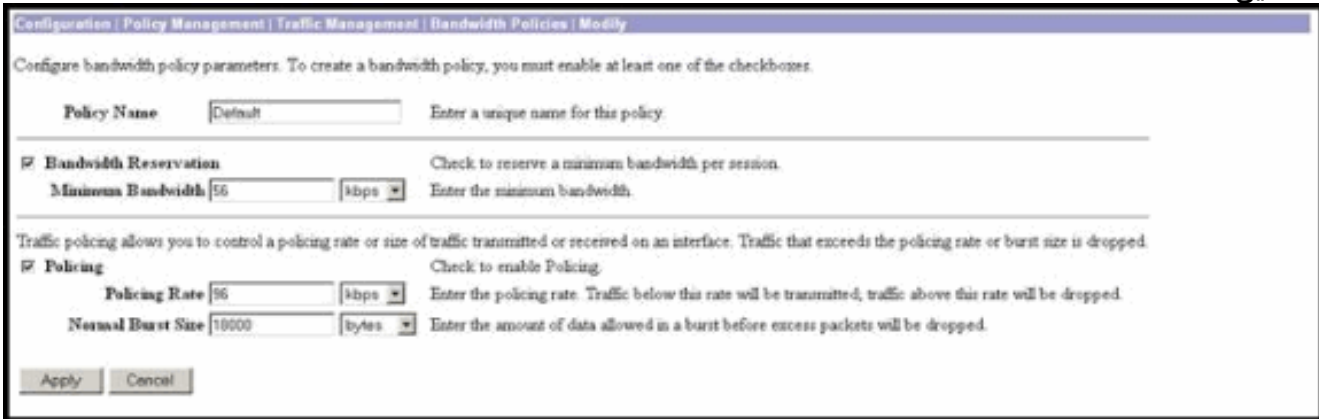
قبل تكوين إدارة النطاق الترددي على أنفاق الشبكة المحلية (LAN) إلى الشبكة المحلية (LAN) أو على أنفاق الوصول عن بعد، يجب تمكين إدارة النطاق الترددي على الواجهة العامة. في نموذج التكوين هذا، يتم تكوين سياسة عرض النطاق الترددي الافتراضي. يتم تطبيق هذا النهج الافتراضي على المستخدمين/الأنفاق التي لا تحتوي على نهج إدارة

النطاق الترددي المطبق على المجموعة التي ينتمون إليها في مركز الشبكة الخاصة الظاهرية (VPN).

1. لتكوين سياسة، حدد تكوين < إدارة السياسة > إدارة حركة مرور البيانات < سياسات النطاق الترددي، وانقر فوق إضافة.



بعد أن تنقر إضافة، تظهر نافذة التعديل.



2. قم بتعيين هذه المعلمات في نافذة "تعديل". اسم النهج—أدخل اسم نهج فريد يمكن أن يساعدك في تذكر النهج. الحد الأقصى للطول هو 32 حرفاً. في هذا المثال، يتم تكوين الاسم 'Default' كاسم النهج. حجز النطاق الترددي— حدد خانة الاختيار **حجز النطاق الترددي** لحجز حد أدنى من النطاق الترددي لكل جلسة عمل. في هذا المثال، يتم تخصيص 56 كيلوبت في الثانية من النطاق الترددي لجميع مستخدمي شبكة VPN الذين لا يندرجون ضمن مجموعة تم تكوين إدارة النطاق الترددي عليها. **السياسة**— حدد خانة الاختيار **السياسة** لتمكين السياسة. قم بإدخال قيمة للتحديد المعدل وحدد وحدة القياس. يرسل مركز الشبكة الخاصة الظاهرية (VPN) حركة المرور التي تنتقل إلى أقل من معدل الشرطة وتسقط جميع حركة المرور التي تنتقل إلى أعلى من معدل الشرطة. تم تكوين 96 كيلوبت في الثانية لضبط النطاق الترددي. الحجم العادي للاندفاع هو مقدار الاندفاع الفوري الذي يمكن أن يرسله مركز VPN في أي وقت معين. لتعيين حجم الاندفاع، أستخدم هذه الصيغة:  
$$\text{Policing Rate} / 8 * 1.5$$
 باستخدام هذه الصيغة، يكون معدل الاندفاع 18000 بايت.

3. طغطة يطبق.

4. حدد تكوين < واجهات > واجهة عامة وانقر فوق علامة التبويب النطاق الترددي لتطبيق سياسة النطاق الترددي الافتراضية على واجهة.

5. قم بتمكين خيار إدارة النطاق الترددي.

6. حدد معدل الارتباط. معدل الارتباط هو سرعة اتصال الشبكة من خلال الإنترنت. في هذا المثال، يتم استخدام اتصال T1 بالإنترنت. بالتالي، 1544 كيلوبت/ثانية هو معدل الارتباط الذي تم تكوينه.

7. حدد سياسة من القائمة المنسدلة "نهج النطاق الترددي". تم تكوين النهج الافتراضي مسبقاً لهذه الواجهة. النهج الذي تقوم بتطبيقه هنا هو نهج النطاق الترددي الافتراضي لجميع المستخدمين على هذه الواجهة. يتم تطبيق هذا النهج على المستخدمين الذين ليس لديهم نهج إدارة النطاق الترددي المطبق على مجموعتهم.

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

## تكوين إدارة النطاق الترددي لأنفاق الموقع إلى الموقع

أكمل هذه الخطوات لتكوين إدارة النطاق الترددي لأنفاق من موقع إلى موقع.

- حدد تكوين < إدارة السياسة > إدارة حركة مرور البيانات < سياسات النطاق الترددي وانقر فوق إضافة لتحديد سياسة نطاق ترددي جديد من شبكة LAN إلى شبكة LAN. في هذا المثال، تم تكوين سياسة تسمى 'L2L\_tunnel' باستخدام حجز النطاق الترددي بسرعة 256 كيلوبت في الثانية.

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: 10530 bytes Enter the amount of data allowed in a burst before excess packets will be dropped.

Apply Cancel

- تطبيق سياسة النطاق الترددي على نفق الاتصال من شبكة LAN الموجود ضمن القائمة المنسدلة "نهج النطاق الترددي العريض".

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, 10.10.1.0/0.0.255 = all 10.10.1.rmn 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, 10.10.1.0/0.0.255 = all 10.10.1.rmn addresses.

Wildcard Mask:

## تكوين إدارة النطاق الترددي لأنفاق شبكات VPN البعيدة

أكمل هذه الخطوات لتكوين إدارة النطاق الترددي لأنفاق شبكات VPN البعيدة.

- حدد تكوين < إدارة السياسة > إدارة حركة المرور < سياسات النطاق الترددي وانقر فوق إضافة لإنشاء سياسة عرض نطاق ترددي جديدة. في هذا المثال، تم تكوين سياسة تسمى 'RA\_Tunnels' باستخدام حجز عرض نطاق ترددي يبلغ 8 كيلوبت في الثانية. يتم تكوين تنظيم حركة المرور بمعدل تنظيم يبلغ 128 كيلوبت في الثانية وحجم اندفاع يبلغ 24000 بايت.

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.

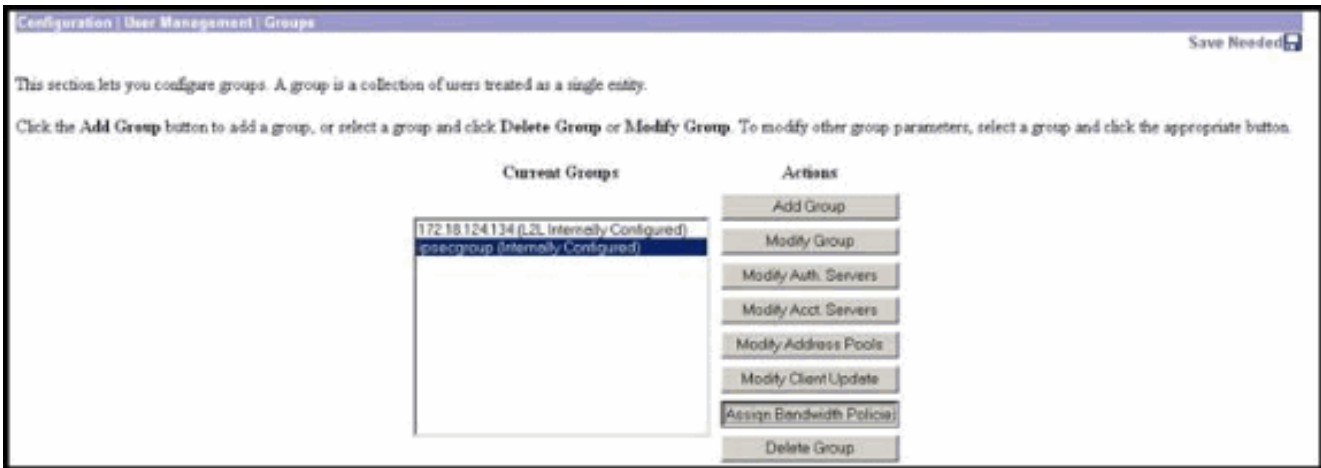
Policy Name:  Enter a unique name for this policy.

Bandwidth Reservation Check to reserve a minimum bandwidth per session.  
Minimum Bandwidth:  kbps Enter the minimum bandwidth.

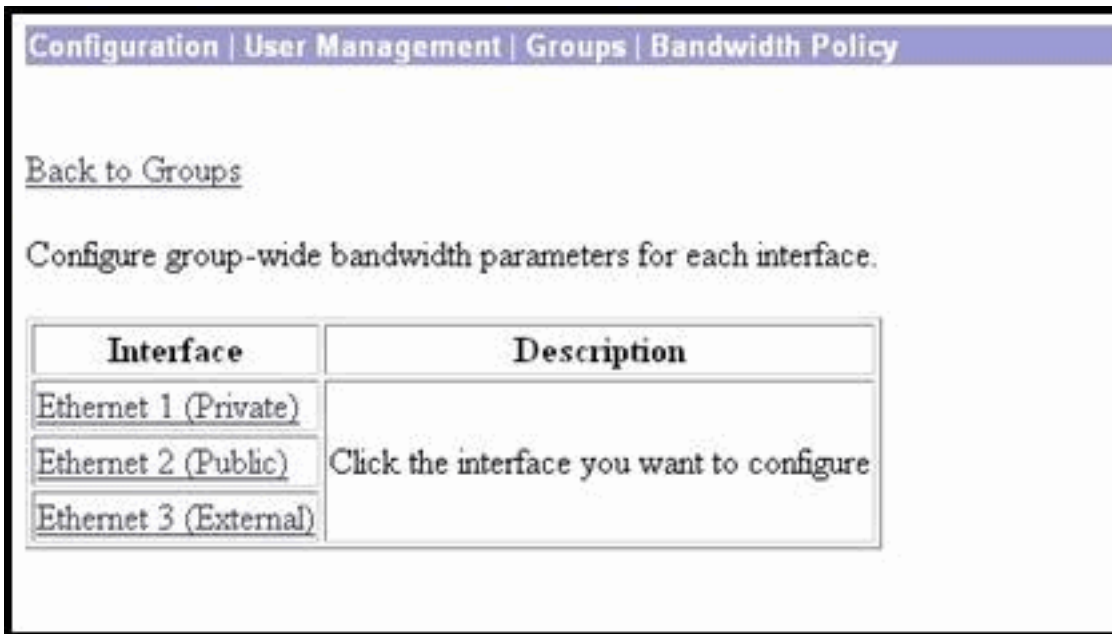
Traffic policing allows you to control a policing rate or size of traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped.

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.

- لتطبيق سياسة النطاق الترددي على مجموعة VPN للوصول عن بعد، حدد تكوين < إدارة المستخدم > مجموعات، وحدد مجموعتك، ثم انقر فوق تعيين سياسات النطاق الترددي.

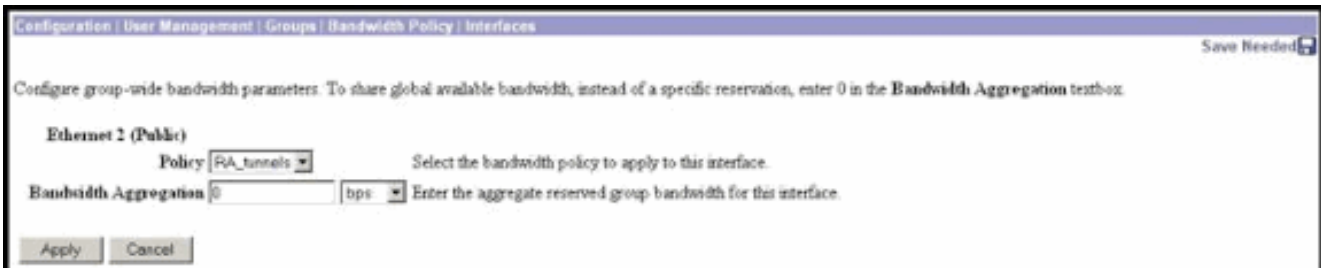


3. انقر فوق الواجهة التي تريد تكوين "إدارة النطاق الترددي" عليها لهذه المجموعة. في هذا المثال، يقصد ب (Ethernet2 (Public)' الواجهة المحددة للمجموعة. لتطبيق سياسة النطاق الترددي على مجموعة على واجهة، يجب تمكين إدارة النطاق الترددي على هذه الواجهة. إذا اخترت واجهة تم فيها تعطيل إدارة النطاق الترددي، تظهر رسالة



تحذير.

4. حدد سياسة النطاق الترددي لمجموعة VPN لهذه الواجهة. يتم تحديد سياسة RA\_Tunnels، التي تم تعريفها من قبل، لهذه المجموعة. أدخل قيمة للحد الأدنى من عرض النطاق الترددي لحجزه لهذه المجموعة. القيمة الافتراضية لتجميع النطاق الترددي هي 0. وحدة القياس الافتراضية هي bps. إذا كنت تريد أن تشارك المجموعة في النطاق الترددي المتاح على الواجهة، فأدخل 0.



## [التحقق من الصحة](#)

حدد المراقبة < الإحصائيات > إدارة النطاق الترددي على مركز VPN 3000 لمراقبة إدارة النطاق الترددي.

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)	11	5	143342	1001508
ipsecgw: (Out)	Ethernet 2 (Public)	11	5	1321526	74700
vo_spoke: (In)	Ethernet 2 (Public)	1539	237	206052492	23069858
vo_spoke: (Out)	Ethernet 2 (Public)	1539	588	206052492	118751970

## استكشاف الأخطاء وإصلاحها

لاستكشاف أخطاء أي مشكلة وإصلاحها أثناء تنفيذ إدارة النطاق الترددي على مركز VPN 3000، قم بتمكين فتي الأحداث هاتين تحت التكوين < النظام < الأحداث < الفئات:

- BMGT (مع خطوة التسجيل: 9-1)
  - BMGTDBG (مع خطوة السجل: 9-1)
- هذه بعض من أكثر رسائل سجل الأحداث شيوعاً:

• تظهر رسالة خطأ على السجلات عند تعديل نهج النطاق الترددي.

SEV=4 BMGT/47 RPT=2 10:03:10.840 08/14/2002 1

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

في حالة عرض رسالة الخطأ هذه، ارجع إلى إعدادات المجموعة وقم بإلغاء تطبيق نهج 'RA\_Tunnel' من المجموعة. قم بتحرير 'RA\_Tunnel' بالقيم الصحيحة ثم أعد تطبيق النهج مرة أخرى على المجموعة المحددة. تعذر العثور على النطاق الترددي للواجهة.

SEV=4 BMGTDBG/56 RPT=1 13:03:58.040 08/14/2002 11

.Could not find interface bandwidth policy 0 for group 1 interface 2

قد تتلقى رسالة الخطأ هذه إذا لم يتم تمكين سياسة النطاق الترددي على الواجهة وتحاول تطبيقها على نفق من شبكة LAN إلى شبكة LAN. إذا كان هذا هو الحال، فقم بتطبيق سياسة على الواجهة العامة كما هو موضح في قسم تكوين سياسة عرض النطاق الترددي الافتراضي على مركز VPN 3000.

## معلومات ذات صلة

- [صفحة دعم مركز Cisco VPN 3000 Series](#)
- [صفحة دعم عميل Cisco VPN 3000 Series](#)
- [صفحة دعم IPSec](#)
- [الدعم الفني - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتمة مچرت مء مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل