

Exemple de configuration de la gestion de la bande passante sur le concentrateur VPN 3000

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Conventions](#)

[Configurez une stratégie par défaut de bande passante sur le concentrateur VPN 3000](#)

[Configurez la gestion de la bande passante pour des tunnels de site à site](#)

[Configurez la gestion de la bande passante pour les tunnels VPN distants](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes nécessaires utilisées pour configurer la fonction de gestion de la bande passante sur le concentrateur de Cisco VPN 3000 pour :

- [Tunnels VPN de site à site \(entre réseaux locaux\)](#)
- [Tunnels VPN d'Accès à distance](#)

Remarque: Avant que vous configuriez des tunnels VPN d'Accès à distance ou de site à site, vous devez d'abord [configurer une stratégie par défaut de bande passante sur le concentrateur VPN 3000](#).

Il y a deux éléments de gestion de la bande passante :

- **Maintien de l'ordre de bande passante** — Limite le débit maximum du trafic percé un tunnel. Le concentrateur VPN transmet le trafic qu'il reçoit au-dessous de ce débit et les baisses trafiquent qui dépasse ce débit.
- **Réservation de bande passante** — Mettent de côté un débit de bande passante minimale pour le trafic percé un tunnel. La gestion de la bande passante te permet pour allouer la bande passante aux groupes et aux utilisateurs équitablement. Ceci empêche de certains groupes ou utilisateurs de consommer une majorité de la bande passante.

La gestion de la bande passante s'applique seulement au trafic percé un tunnel (tunnel Protocol [L2TP] de couche 2, perçage d'un tunnel point par point Protocol [PPTP], IPSec) et est le plus généralement appliquée à l'interface publique.

La fonction de gestion de la bande passante fournit les indemnités administratives aux connexions

VPN d'Accès à distance et de site à site. Les tunnels VPN d'Accès à distance utilisent la bande passante maintenant l'ordre de sorte que les utilisateurs de bande passante n'utilisent pas toute la bande passante. Réciproquement, l'administrateur peut configurer la réservation de bande passante pour que les tunnels de site à site garantissent un minimum de bande passante à chaque site distant.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

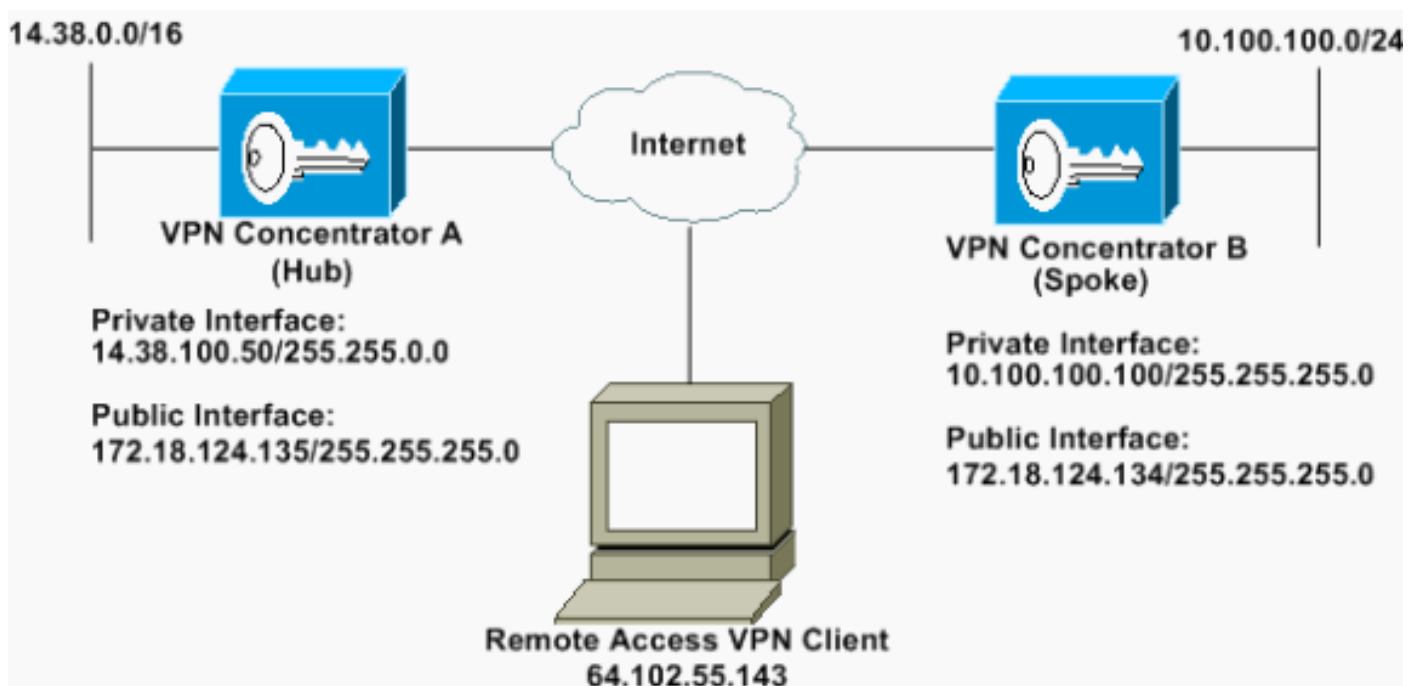
- Concentrateur de Cisco VPN 3000 avec des versions de logiciel 4.1.x et ultérieures

Remarque: La fonction de gestion de la bande passante a été introduite dans la version 3.6.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux [Conventions relatives aux conseils techniques Cisco](#).

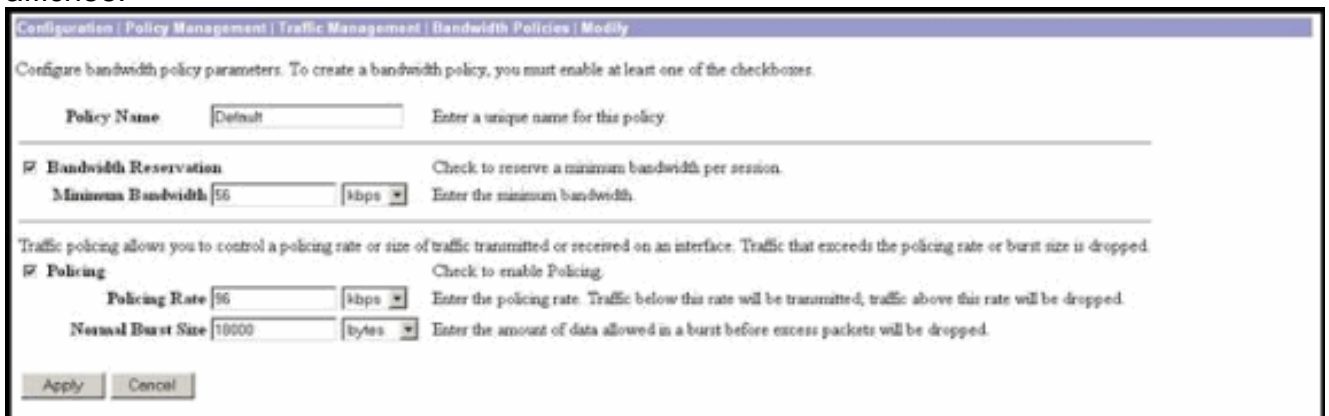
[Configurez une stratégie par défaut de bande passante sur le concentrateur VPN 3000](#)

Avant que vous puissiez configurer la gestion de la bande passante sur les tunnels entre réseaux locaux ou sur les tunnels d'Accès à distance, vous devez activer la gestion de la bande passante sur l'interface publique. Dans cette configuration d'échantillon, une stratégie par défaut de bande passante est configurée. Cette stratégie par défaut est appliquée aux utilisateurs/aux tunnels qui n'ont pas une stratégie de gestion de la bande passante appliquée au groupe qu'ils appartiennent à dans le concentrateur VPN.

1. Pour configurer une stratégie, sélectionnez les **stratégies de configuration > de Gestion des stratégies > de gestion de trafic > de bande passante**, et cliquez sur Add.



Après que vous cliquez sur Add, la fenêtre de modifier est affichée.



2. Placez ces paramètres dans la fenêtre de modifier. **Nom de stratégie** — Écrivez un seul nom de stratégie qui peut vous aider à se souvenir la stratégie. La longueur maximale est 32 caractères. Dans cet exemple, le nom « par défaut » est configuré comme nom de stratégie. **Réservation de bande passante** — Cochez la case de **réserve** **de bande passante** pour réserver un minimum de bande passante pour chaque session. Dans cet exemple, 56 Kbps de bande passante est réservé pour tous les utilisateurs VPN qui ne tombent pas sous un groupe qui fait configurer la gestion de la bande passante. **Maintien de l'ordre** — Cochez la case de **maintien de l'ordre** pour activer le maintien de l'ordre. Écrivez une valeur pour maintenir l'ordre le débit et sélectionnez l'unité de la mesure. Le concentrateur VPN transmet le trafic que les mouvements au-dessous du débit de maintien

de l'ordre et relâche tout le trafic qui se déplace au-dessus du débit de maintien de l'ordre. 96 Kbps est configurés pour le maintien de l'ordre de bande passante. La taille de rafale normale est la quantité de rafale instantanée que le concentrateur VPN peut envoyer à un moment donné. Pour fixer la taille de rafale, utilisez cette formule : $(\text{Policing Rate}/8) * 1.5$ Avec cette formule, le débit de rafales est de 18000 octets.

3. Cliquez sur **Apply**.
4. Le **Configuration > Interfaces** choisi > **interface publique** et cliquent sur en fonction l'onglet de bande passante pour s'appliquer la stratégie par défaut de bande passante à une interface.
5. Activez l'option de **gestion de la bande passante**.
6. Spécifiez le débit de la liaison. Le débit de la liaison est la vitesse de la connexion réseau par l'Internet. Dans cet exemple une connexion à Internet de t1 est utilisée. En conséquence, 1544 Kbps est le débit de la liaison configuré.
7. Sélectionnez une stratégie de la liste déroulante de stratégie de bande passante. La stratégie par défaut est configurée plus tôt pour cette interface. La stratégie que vous vous appliquez voici une stratégie par défaut de bande passante pour tous les utilisateurs sur cette interface. Cette stratégie est appliquée aux utilisateurs qui n'ont pas une stratégie de gestion de la bande passante appliquée à leur groupe.

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

[Configurez la gestion de la bande passante pour des tunnels de site à site](#)

Terminez-vous ces étapes pour configurer la gestion de la bande passante pour des tunnels de site à site.

1. Les **stratégies** choisies de **configuration > de Gestion des stratégies > de gestion de trafic > de bande passante** et cliquent sur Add pour définir une nouvelle stratégie de bande passante d'entre réseaux locaux. Dans cet exemple, une stratégie appelée le 'L2L_tunnel' a été configurée avec une réservation de bande passante de 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: Enter a unique name for this policy.

Bandwidth Reservation Check to reserve a minimum bandwidth per session.

Minimum Bandwidth: 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: Enter the policing rate. Traffic below this rate will be transmitted, traffic above this rate will be dropped.

Normal Burst Size: Enter the amount of data allowed in a burst before excess packets will be dropped.

- Appliquez la stratégie de bande passante au tunnel entre réseaux locaux existant sous le menu déroulant de stratégie de bande passante.

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: 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.mnn 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.mnn addresses.

Wildcard Mask:

[Configurez la gestion de la bande passante pour les tunnels VPN distants](#)

Terminez-vous ces étapes pour configurer la gestion de la bande passante pour les tunnels VPN distants.

- Les stratégies choisies de configuration > de Gestion des stratégies > de gestion de trafic > de bande passante et cliquent sur Add pour créer une nouvelle stratégie de bande passante. Dans cet exemple, une stratégie appelée « RA_tunnels » est configurée avec une réservation de bande passante de 8 Kbps. La Réglementation du trafic est configurée avec du débit de maintien de l'ordre de 128 Kbps et d'une taille de rafale de 24000 octets.

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. Pour s'appliquer la stratégie de bande passante à un groupe VPN d'Accès à distance, le **Configuration > User Management > Groups** choisi, sélectionner votre groupe, et le clic **assignent des stratégies de bande passante**.

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"/>

3. Cliquez sur l'interface sur laquelle vous voulez configurer la gestion de la bande passante pour ce groupe. Dans cet exemple, 'Ethernet2 (public)' est l'interface sélectionnée pour le groupe. Pour s'appliquer une stratégie de bande passante à un groupe sur une interface, la gestion de la bande passante doit être activée sur cette interface. Si vous choisissez une interface sur laquelle la gestion de la bande passante est désactivée, un message d'avertissement

Configuration | User Management | Groups | Bandwidth Policy

[Back to Groups](#)

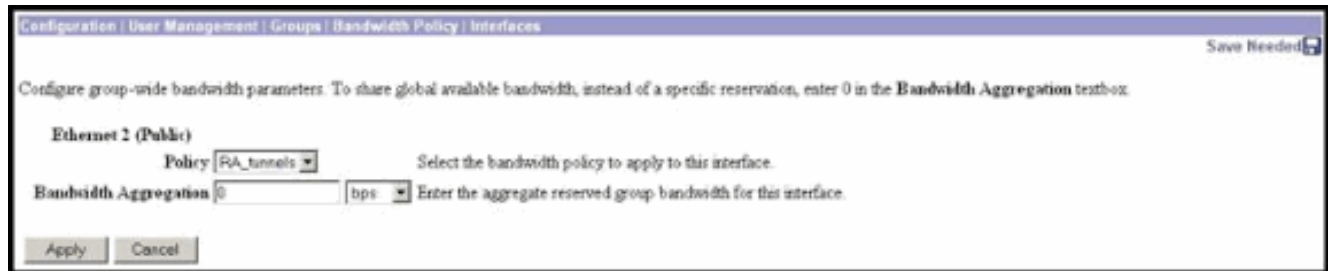
Configure group-wide bandwidth parameters for each interface.

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

apparaît.

4. Sélectionnez la stratégie de bande passante pour le groupe VPN pour cette interface. La stratégie de RA_tunnels, qui a été précédemment définie, est sélectionnée pour ce groupe.

Écrivez une valeur pour que la bande passante minimale réserve à ce groupe. La valeur par défaut de l'agrégation de bande passante est 0. L'unité de la mesure par défaut est des bps. Si vous voulez que le groupe partage dans la bande passante disponible sur l'interface, écrivez 0.



Vérifiez

Surveillance > statistiques > gestion de la bande passante choisies sur le concentrateur VPN 3000 pour surveiller la gestion de la bande passante.

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
ipseccuser (In)	Ethernet 2 (Public)	13	5	1437342	1001508
ipseccuser (Out)	Ethernet 2 (Public)	11	9	1321526	74700
no_spoke (In)	Ethernet 2 (Public)	1539	237	206052492	23069858
no_spoke (Out)	Ethernet 2 (Public)	1539	588	206052492	118751970

Dépannez

Pour dépanner tous les problèmes tandis que la gestion de la bande passante est mise en application sur le concentrateur VPN 3000, activez ces deux classes d'événement sous la configuration > le système > les événements > les classes :

- **BMGT** (avec la sévérité à se connecter : 1-9)
- **BMGTDBG** (avec la sévérité à se connecter : 1-9)

Ce sont certains des messages de journal d'événements les plus communs :

- Dépasse le message d'erreur d'agrégat de réservation est vu sur les logs quand une stratégie de bande passante est modifiée.

```
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.
```

 Si ce message d'erreur est affiché, revenez aux configurations de groupe et ONU-appliquez la stratégie de « RA_tunnel » à partir du groupe. Éditez le « RA_tunnel » avec les valeurs correctes et puis réappliquez la stratégie de nouveau au groupe spécifique.
- Incapable de trouver la bande passante d'interface.

```
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. Vous pouvez recevoir cette erreur si la stratégie de bande passante n'est pas activée sur l'interface et vous essayez pour l'appliquer sur le tunnel entre réseaux locaux. Si c'est le cas, [appliquez-vous une stratégie à l'interface publique](#) comme expliqué dans le [configurer une stratégie par défaut de bande passante sur la](#) section de [concentrateur VPN 3000](#).

Informations connexes

- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Page d'assistance du Client VPN 3000 Series Cisco](#)
- [Page d'assistance IPsec](#)
- [Support technique - Cisco Systems](#)