

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Diagramme du réseau](#)

[Conventions](#)

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

[Configurer la gestion de la bande passante pour les tunnels site à site](#)

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

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes nécessaires à la configuration de la fonctionnalité de gestion de la bande passante sur le concentrateur Cisco VPN 3000 pour :

- [Tunnels VPN site à site \(LAN à LAN\)](#)
- [Tunnels VPN d'accès distant](#)

Remarque : avant de configurer l'accès distant ou les tunnels VPN site à site, vous devez d'abord [configurer une stratégie de bande passante par défaut sur le concentrateur VPN 3000](#).

La gestion de la bande passante comporte deux éléments :

- **Bandwidth Policing** : limite le débit maximal du trafic tunnelisé. Le concentrateur VPN transmet le trafic qu'il reçoit en dessous de ce débit et abandonne le trafic qui dépasse ce débit.
- **Bandwidth Reservation** : définit un débit de bande passante minimal pour le trafic tunnelisé. La gestion de la bande passante vous permet d'allouer la bande passante aux groupes et aux utilisateurs de manière équitable. Cela empêche certains groupes ou utilisateurs de consommer la majorité de la bande passante.

La gestion de la bande passante s'applique uniquement au trafic tunnelisé (protocole L2TP [Layer 2 Tunnel Protocol], protocole PPTP [Point to Point Tunneling Protocol], IPSec) et est généralement appliquée à l'interface publique.

La fonctionnalité de gestion de la bande passante offre des avantages administratifs pour l'accès à distance et les connexions VPN de site à site. Les tunnels VPN d'accès à distance utilisent le

contrôle de bande passante pour que les utilisateurs à large bande n'utilisent pas toute la bande passante. Inversement, l'administrateur peut configurer la réservation de bande passante pour les tunnels de site à site afin de garantir une quantité minimale de bande passante à chaque site distant.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

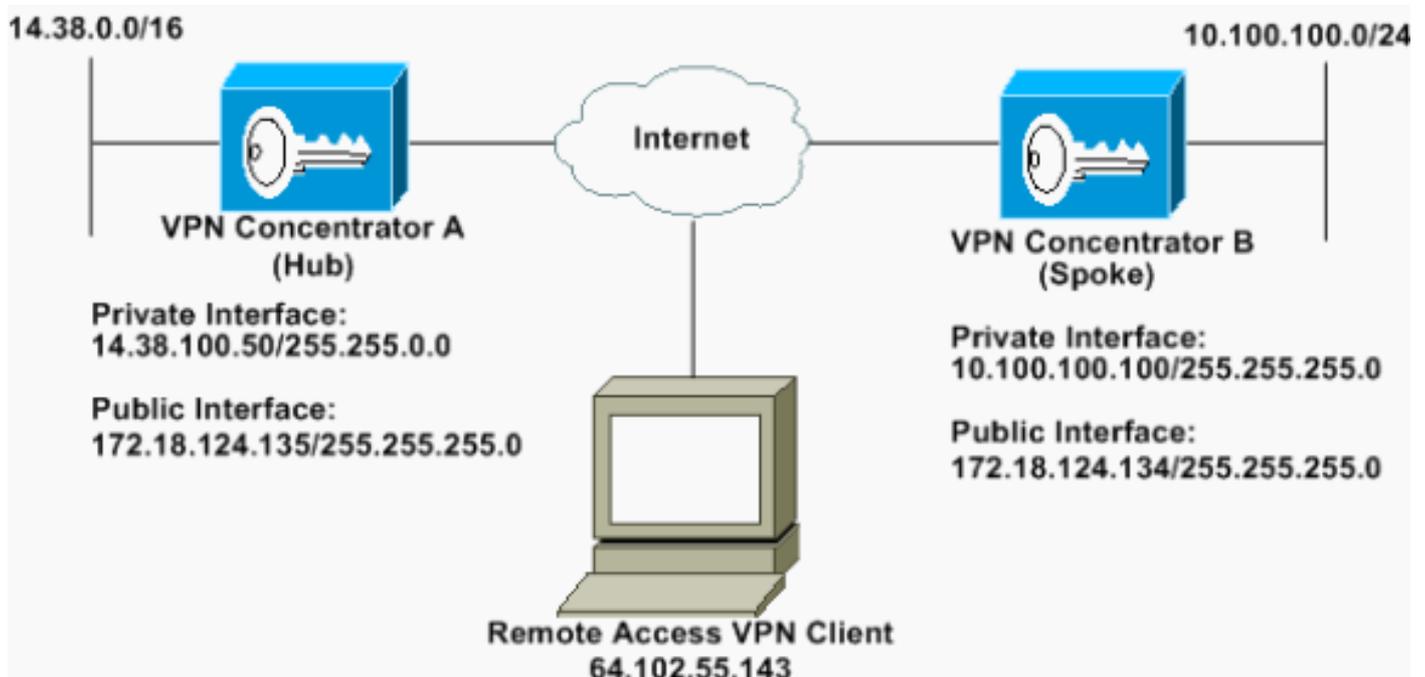
- Concentrateur Cisco VPN 3000 avec versions 4.1.x et ultérieures du logiciel

Remarque : La fonctionnalité Gestion de la bande passante a été introduite dans la version 3.6.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



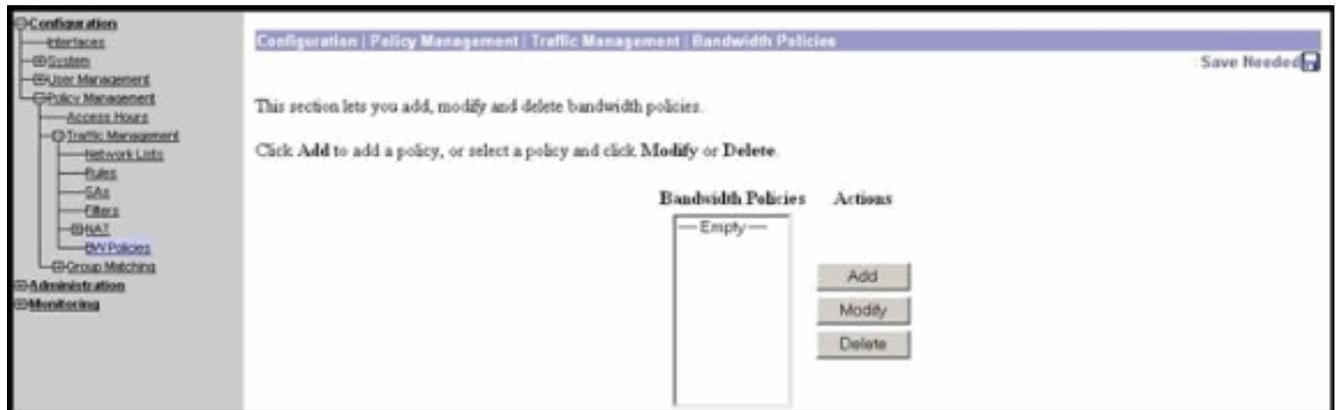
Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

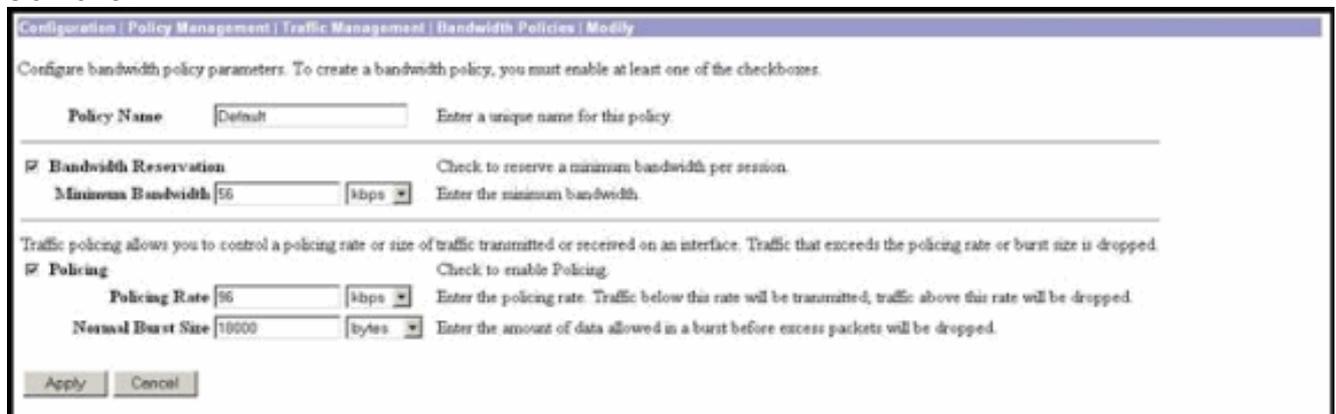
[Configurer une stratégie de bande passante par défaut sur le concentrateur VPN 3000](#)

Avant de pouvoir configurer la gestion de la bande passante sur les tunnels LAN à LAN ou sur les tunnels d'accès distant, vous devez activer la gestion de la bande passante sur l'interface publique. Dans cet exemple de configuration, une stratégie de bande passante par défaut est configurée. Cette stratégie par défaut est appliquée aux utilisateurs/tunnels qui n'ont pas de stratégie de gestion de la bande passante appliquée au groupe auquel ils appartiennent dans le concentrateur VPN.

1. Pour configurer une stratégie, sélectionnez **Configuration > Policy Management > Traffic Management > Bandwidth Policies**, puis cliquez sur **Add**.



Après avoir cliqué sur Ajouter, la fenêtre Modifier s'affiche.



2. Définissez ces paramètres dans la fenêtre Modifier. **Policy Name** : saisissez un nom de stratégie unique qui peut vous aider à mémoriser la stratégie. La longueur maximale est de 32 caractères. Dans cet exemple, le nom 'Default' est configuré en tant que nom de stratégie. **Bandwidth Reservation** : cochez la case **Bandwidth Reservation** pour réserver une quantité minimale de bande passante pour chaque session. Dans cet exemple, 56 kbits/s de bande passante sont réservés à tous les utilisateurs VPN qui ne font pas partie d'un groupe dont la gestion de bande passante est configurée. **Policing** : cochez la case **Policing** pour activer la police. Saisissez une valeur pour le taux de réglementation et sélectionnez l'unité de mesure. Le concentrateur VPN transmet le trafic qui se déplace en dessous du taux de réglementation et abandonne tout trafic qui se déplace au-dessus du taux de réglementation. 96 kbits/s sont configurés pour la surveillance de la bande passante. La taille de rafale normale est la quantité de rafale instantanée que le concentrateur VPN peut envoyer à un moment donné. Pour définir la taille de rafale, utilisez la formule suivante :

(Policing Rate/8) * 1.5

Avec cette formule, le débit de rafale est de 18 000 octets.

3. Cliquez sur Apply.
4. Sélectionnez **Configuration > Interfaces > Public Interface** et cliquez sur l'onglet Bandwidth pour appliquer la stratégie de bande passante par défaut à une interface.
5. Activez l'option **Gestion de la bande passante**.
6. Spécifiez le débit de liaison. Le débit de liaison correspond à la vitesse de la connexion réseau via Internet. Dans cet exemple, une connexion T1 à Internet est utilisée. Par conséquent, 1 544 kbits/s est le débit de liaison configuré.
7. Sélectionnez une stratégie dans la liste déroulante Stratégie de bande passante. La stratégie par défaut est configurée précédemment pour cette interface. La stratégie que vous appliquez ici est une stratégie de bande passante par défaut pour tous les utilisateurs de cette interface. Cette stratégie s'applique aux utilisateurs qui n'ont pas de stratégie de gestion de la bande passante appliquée à leur groupe.

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.

[Configurer la gestion de la bande passante pour les tunnels site à site](#)

Complétez ces étapes pour configurer la gestion de la bande passante pour les tunnels de site à site.

1. Sélectionnez **Configuration > Policy Management > Traffic Management > Bandwidth Politiques** et cliquez sur **Add** pour définir une nouvelle stratégie de bande passante LAN à LAN. Dans cet exemple, une stratégie appelée 'L2L_tunnel' a été configurée avec une réservation de bande passante de 256 kbits/s.

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.
Maximum 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.

2. Appliquez la stratégie de bande passante au tunnel LAN à LAN existant dans le menu

déroulant 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
 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:

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

Complétez ces étapes pour configurer la gestion de la bande passante pour les tunnels VPN distants.

1. Sélectionnez **Configuration > Policy Management > Traffic Management > Bandwidth Policies** et cliquez 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 kbits/s. La régulation du trafic est configurée avec un taux de régulation de 128 kbits/s et une taille de rafale de 24 000 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 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. Pour appliquer la stratégie de bande passante à un groupe VPN d'accès distant, sélectionnez **Configuration > User Management > Groups**, sélectionnez votre groupe, puis

cliquez sur **Affecter des stratégies de bande passante**.

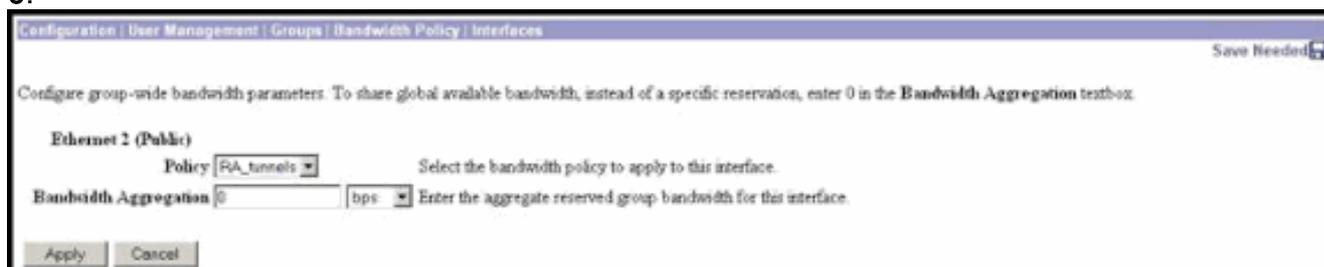


3. Cliquez sur l'interface sur laquelle vous voulez configurer la gestion de la bande passante pour ce groupe. Dans cet exemple, 'Ethernet2 (Public)' est l'interface sélectionnée pour le groupe. Pour appliquer une stratégie de bande passante à un groupe sur une interface, la gestion de bande passante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



apparaît.

4. Sélectionnez la stratégie de bande passante pour le groupe VPN de cette interface. La stratégie RA_tunnels, précédemment définie, est sélectionnée pour ce groupe. Entrez une valeur pour la bande passante minimale à réserver pour ce groupe. La valeur par défaut de l'agrégation de bande passante est 0. L'unité de mesure par défaut est le bit/s. Si vous souhaitez que le groupe partage la bande passante disponible sur l'interface, saisissez 0.



Vérification

Sélectionnez **Monitoring > Statistics > Bandwidth Management** sur le concentrateur VPN 3000 pour surveiller Bandwidth Management.

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	1321525	74700
to_spoke: (In)	Ethernet 2 (Public)	1539	237	206952492	23059658
to_spoke: (Out)	Ethernet 2 (Public)	1539	588	206952492	118751970

Dépannage

Pour résoudre des problèmes lors de la mise en oeuvre de la gestion de la bande passante sur le concentrateur VPN 3000, activez ces deux classes d'événements sous **Configuration > System > Events > Classes** :

- **BMGT** (avec gravité à consigner : 1-9)
- **BMGTDBG** (avec la gravité du journal : 1-9)

Voici quelques-uns des messages de journal des événements les plus courants :

- Le message d'erreur `Dépasse la réservation agrégée` est affiché dans les journaux lorsqu'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 s'affiche, revenez aux paramètres du groupe et annulez l'application de la stratégie 'RA_tunnel' à partir du groupe. Modifiez le 'tunnel_RA' avec les valeurs correctes, puis réappliquez la stratégie au groupe spécifique.

- Bande passante de l'interface introuvable.

```
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 que vous essayez de l'appliquer sur le tunnel LAN à LAN. Si c'est le cas,

[appliquez une stratégie à l'interface publique](#) comme expliqué dans la section [Configurer une stratégie de bande passante par défaut sur le 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](#)