

Exemplo de configuração de gerenciamento de largura de banda do VPN 3000 Concentrator

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Conventions](#)

[Configurar uma política de largura de banda padrão no VPN 3000 Concentrator](#)

[Configurar o gerenciamento de largura de banda para túneis site a site](#)

[Configurar o gerenciamento de largura de banda para túneis VPN remotos](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve as etapas necessárias usadas para configurar o recurso de gerenciamento de largura de banda no Cisco VPN 3000 Concentrator para:

- [Túneis VPN de site a site \(LAN a LAN\)](#)
- [Túneis VPN de acesso remoto](#)

Observação: antes de configurar o acesso remoto ou túneis VPN site a site, primeiro é necessário [configurar uma política de largura de banda padrão no VPN 3000 Concentrator](#).

Há dois elementos de gerenciamento de largura de banda:

- **Política de largura de banda** — limita a taxa máxima de tráfego em túnel. O VPN Concentrator transmite o tráfego que recebe abaixo dessa taxa e descarta o tráfego que excede essa taxa.
- **Reserva de largura de banda**—Define uma taxa de largura de banda mínima para o tráfego em túnel. O gerenciamento de largura de banda permite alocar a largura de banda de forma equitativa para grupos e usuários. Isso impede que determinados grupos ou usuários consumam a maior parte da largura de banda.

O gerenciamento de largura de banda se aplica somente ao tráfego em túnel (Layer 2 Tunnel Protocol [L2TP], Point to Point Tunneling Protocol [PPTP], IPSec) e é mais comumente aplicado à interface pública.

O recurso Gerenciamento de largura de banda oferece benefícios administrativos para acesso remoto e conexões VPN site a site. Os túneis VPN de acesso remoto utilizam a política de largura

de banda para que os usuários de banda larga não utilizem toda a largura de banda. Por outro lado, o administrador pode configurar a Reserva de Largura de Banda para túneis site a site para garantir uma quantidade mínima de largura de banda para cada local remoto.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

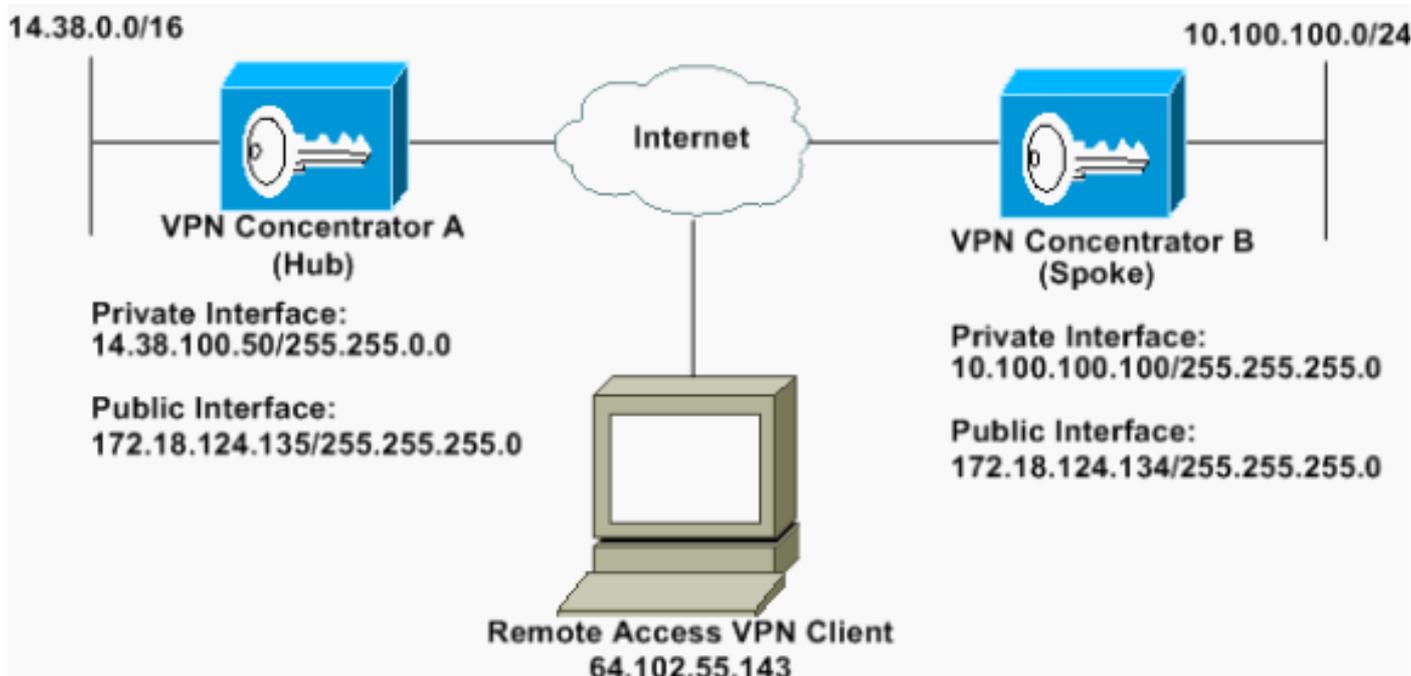
- Cisco VPN 3000 Concentrator com Software Releases 4.1.x e posteriores

Observação: o recurso de gerenciamento de largura de banda foi apresentado na versão 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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Conventions

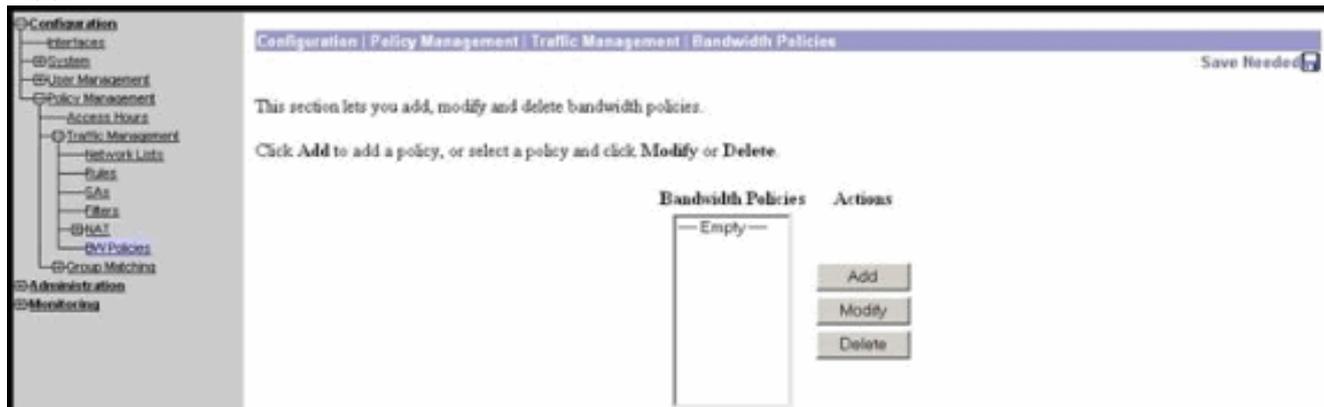
Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Configurar uma política de largura de banda padrão no VPN

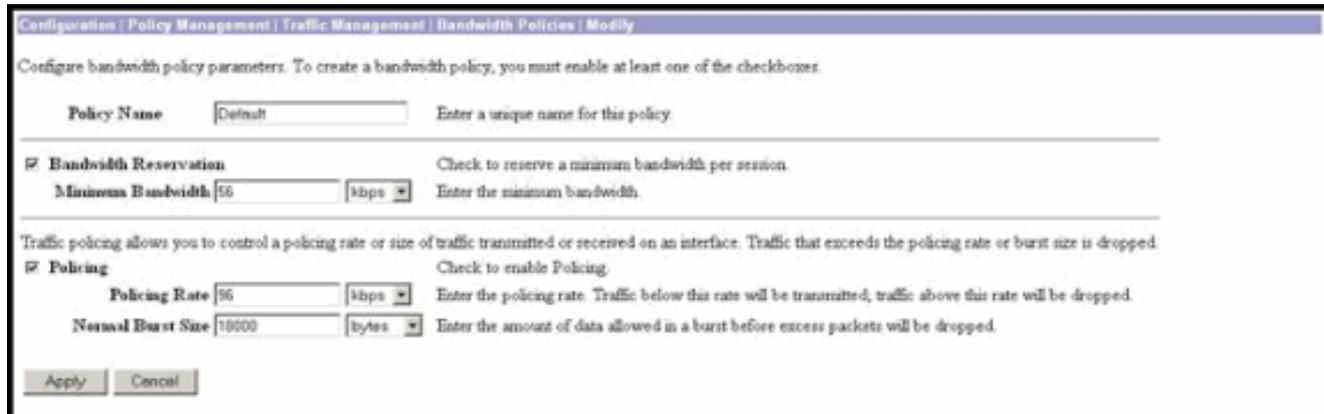
3000 Concentrator

Antes de configurar o Gerenciamento de largura de banda nos túneis de LAN para LAN ou nos túneis de acesso remoto, você deve ativar o Gerenciamento de largura de banda na interface pública. Nesta configuração de exemplo, uma política de largura de banda padrão é configurada. Essa política padrão é aplicada a usuários/túneis que não têm uma política de Gerenciamento de largura de banda aplicada ao grupo ao qual pertencem no VPN Concentrator.

1. Para configurar uma política, selecione **Configuration > Policy Management > Traffic Management > Bandwidth Policies** e clique em **Add**.



Depois de clicar em Adicionar, a janela Modificar é exibida.



2. Defina esses parâmetros na janela Modificar. **Nome da política** — Insira um nome de política exclusivo que pode ajudá-lo a lembrar-se da diretiva. O comprimento máximo é de 32 caracteres. Neste exemplo, o nome 'Default' é configurado como o Nome da política. **Reserva de largura de banda**—Marque a caixa de seleção **Reserva de largura de banda** para reservar uma quantidade mínima de largura de banda para cada sessão. Neste exemplo, 56 kbps de largura de banda são reservados para todos os usuários de VPN que não se enquadram em um grupo que tem o Gerenciamento de largura de banda configurado. **Policimento**—Marque a caixa de seleção **Policimento** para ativar a vigilância. Insira um valor para Taxa de vigilância e selecione a unidade de medida. O VPN Concentrator transmite o tráfego que se move abaixo da taxa de vigilância e descarta todo o tráfego que se move acima da taxa de vigilância. 96 kbps é configurado para o policimento de largura de banda. O tamanho normal da intermitência é a quantidade de intermitência instantânea que o VPN Concentrator pode enviar a qualquer momento. Para definir o tamanho da intermitência, use esta fórmula:

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

Com esta fórmula, a taxa de intermitência é de 18.000 bytes.

3. Clique em Apply.
4. Selecione **Configuration > Interfaces > Public Interface** e clique na guia Bandwidth para aplicar a política de largura de banda padrão a uma interface.
5. Ative a opção **Bandwidth Management (Gerenciamento de largura de banda)**.
6. Especifique a taxa de link. A taxa de link é a velocidade da conexão de rede através da Internet. Neste exemplo, uma conexão T1 com a Internet é usada. Conseqüentemente, 1544 kbps é a taxa de link configurada.
7. Selecione uma diretiva na lista suspensa Diretiva de largura de banda. A política padrão é configurada anteriormente para esta interface. A política que você aplica aqui é uma política de largura de banda padrão para todos os usuários nesta interface. Essa política é aplicada aos usuários que não têm uma política de gerenciamento de largura de banda aplicada ao seu grupo.

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.

[Configurar o gerenciamento de largura de banda para túneis site a site](#)

Conclua estes passos para configurar o Gerenciamento de largura de banda para túneis site a site.

1. Selecione **Configuration > Policy Management > Traffic Management > Bandwidth Policies** e clique em **Add** para definir uma nova política de largura de banda de LAN para LAN. Neste exemplo, uma política chamada 'L2L_tunnel' foi configurada com uma reserva de largura de banda de 256 kbps.

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: 50 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. Aplique a política de largura de banda ao túnel LAN para LAN existente no menu suspenso Diretiva de largura de

banda.

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 Entire certificate chain
Transmission 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.mn 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.mn addresses.

Wildcard Mask

[Configurar o gerenciamento de largura de banda para túneis VPN remotos](#)

Conclua estes passos para configurar o Gerenciamento de largura de banda para túneis VPN remotos.

1. Selecione **Configuration > Policy Management > Traffic Management > Bandwidth Policies** e clique em **Add** para criar uma nova política de largura de banda. Neste exemplo, uma política chamada 'RA_túneis' é configurada com uma reserva de largura de banda de 8 kbps. A Política de Tráfego é configurada com uma taxa de vigilância de 128 kbps e um tamanho de intermitência de 24.000 bytes.

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.

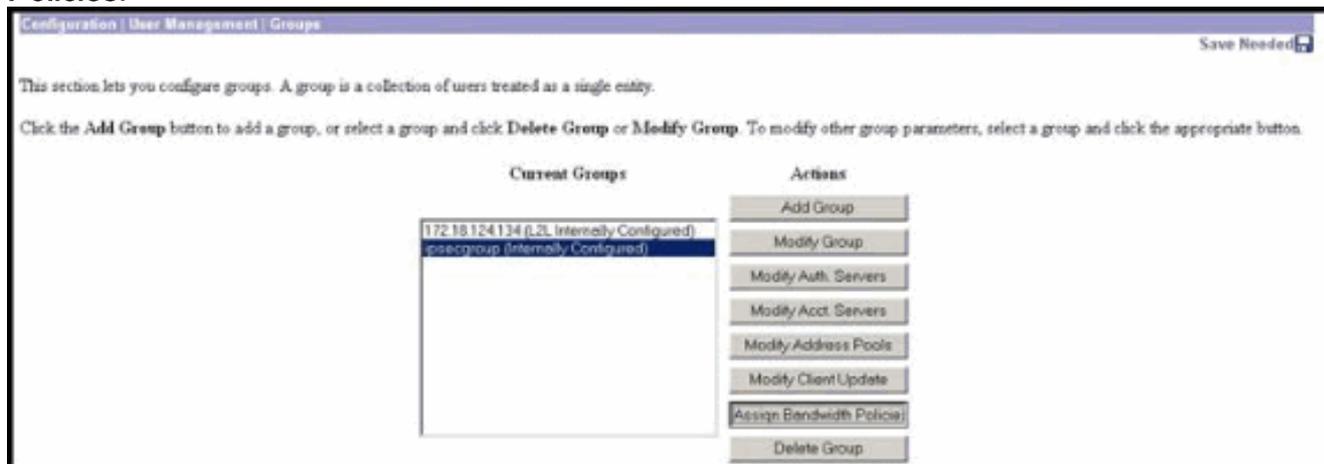
Bandwidth Reservation Check to reserve a minimum bandwidth per session.
Minimum Bandwidth kbps Enter the minimum bandwidth.

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.

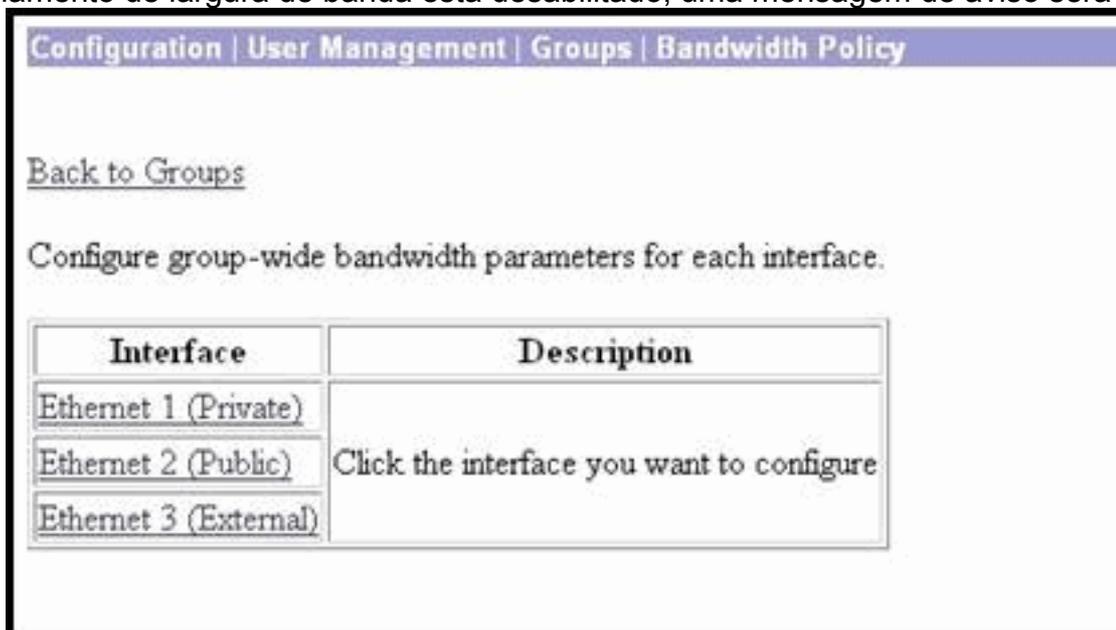
Policing Check to enable Policing.
Policing Rate kbps Enter the policing rate. Traffic below this rate will be transmitted, traffic above this rate will be dropped.
Normal Burst Size bytes Enter the amount of data allowed in a burst before excess packets will be dropped.

2. Para aplicar a política de largura de banda a um grupo VPN de acesso remoto, selecione **Configuration > User Management > Groups**, selecione seu grupo e clique em **Assign Bandwidth**

Policies.

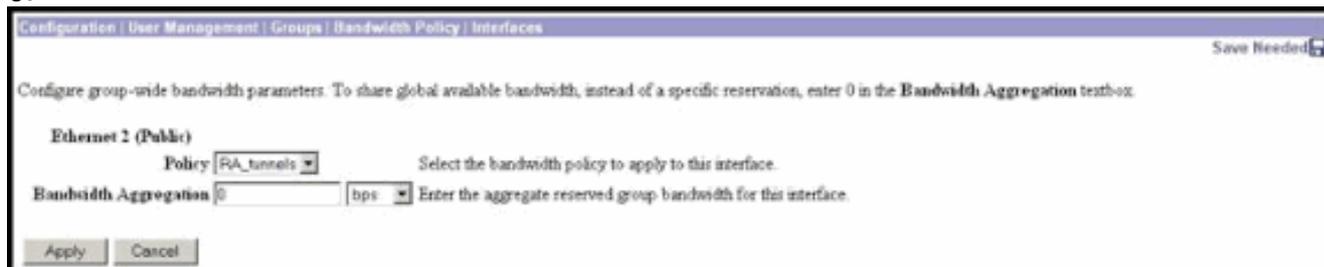


3. Clique na interface na qual deseja configurar o Gerenciamento de largura de banda para este grupo. Neste exemplo, 'Ethernet2 (Public)' é a interface selecionada para o grupo. Para aplicar uma política de largura de banda a um grupo em uma interface, o Gerenciamento de largura de banda deve ser ativado nessa interface. Se você escolher uma interface na qual o Gerenciamento de largura de banda está desabilitado, uma mensagem de aviso será



exibida.

4. Selecione a política de largura de banda para o grupo VPN para esta interface. A política RA_túneis, que foi definida anteriormente, é selecionada para este grupo. Insira um valor para a largura de banda mínima a ser reservada para esse grupo. O valor padrão da agregação de largura de banda é 0. A unidade de medida padrão é bps. Se desejar que o grupo compartilhe na largura de banda disponível na interface, digite 0.



[Verificar](#)

Selecione **Monitoring > Statistics > Bandwidth Management** no VPN 3000 Concentrator para monitorar o Bandwidth Management.

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: ipsec

User Name	Interface	Traffic Rate (kbps)		Traffic Volume (bytes)	
		Conformed	Throttled	Conformed	Throttled
ipsec: (In)	Ethernet 2 (Public)	10	5	143342	1004508
ipsec: (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

Troubleshoot

Para solucionar qualquer problema enquanto o Gerenciamento de largura de banda é implementado no VPN 3000 Concentrator, ative estas duas classes de evento em **Configuration > System > Events > Classes**:

- **BMGT** (com severidade para registro: 1-9)
- **BMGTDBG** (com severidade para registro: 1-9)

Estas são algumas das mensagens de log de eventos mais comuns:

- A mensagem de erro `Excede a Reserva Agregada` é exibida nos registros quando uma Política de Largura de Banda é modificada.

```
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.
```

Se esta mensagem de erro for exibida, retorne às configurações do grupo e desaplique a política 'RA_tunnel' do grupo. Edite o 'RA_tunnel' com os valores corretos e, em seguida, reaplique a política ao grupo específico.

- Não é possível localizar a largura de banda da 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.
```

Você pode receber esse erro se a política de largura de banda não estiver habilitada na interface e tentar aplicá-la no túnel LAN a LAN. Se esse for o caso, [aplique uma política à interface pública](#) conforme explicado na seção [Configurar uma política de largura de banda padrão no VPN 3000 Concentrator](#).

Informações Relacionadas

- [Página de suporte do Cisco VPN 3000 Series Concentrator](#)
- [Página de suporte ao cliente do Cisco VPN 3000 Series](#)
- [Página de suporte do IPSec](#)
- [Suporte Técnico - Cisco Systems](#)