Ejemplo de Configuración de Administración de Ancho de Banda del Concentrador VPN 3000

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Diagrama de la red Convenciones Configuración de una Política de Ancho de Banda Predeterminada en el Concentrador VPN 3000 Configuración de la administración del ancho de banda para túneles de sitio a sitio Configuración de la Administración de Ancho de Banda para los Túneles VPN Remotos Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe los pasos necesarios para configurar la función de Administración del Ancho de Banda en el Cisco VPN 3000 Concentrator para:

- Túneles VPN de sitio a sitio (de LAN a LAN)
- Túneles VPN de acceso remoto

Nota: Antes de configurar el acceso remoto o los túneles VPN de sitio a sitio, primero debe configurar una política de ancho de banda predeterminada en el VPN 3000 Concentrator.

Hay dos elementos de la gestión del ancho de banda:

- Regulación del ancho de banda: limita la velocidad máxima del tráfico tunelizado. El concentrador VPN transmite el tráfico que recibe por debajo de esta velocidad y descarta el tráfico que excede esta velocidad.
- Reserva de ancho de banda: reserva una velocidad de ancho de banda mínima para el tráfico tunelizado. La administración del ancho de banda permite asignar el ancho de banda de forma equitativa a grupos y usuarios. Esto evita que determinados grupos o usuarios consuman la mayor parte del ancho de banda.

La gestión del ancho de banda se aplica solamente al tráfico tunelizado (protocolo de túnel de capa 2 [L2TP], protocolo de túnel de punto a punto [PPTP], IPSec) y se aplica con mayor frecuencia a la interfaz pública.

La función Bandwidth Management proporciona ventajas administrativas para el acceso remoto y las conexiones VPN de sitio a sitio. Los túneles VPN de acceso remoto utilizan la regulación del

ancho de banda para que los usuarios de banda ancha no utilicen todo el ancho de banda. Por el contrario, el administrador puede configurar la reserva de ancho de banda para los túneles de sitio para garantizar una cantidad mínima de ancho de banda a cada sitio remoto.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

• Concentrador Cisco VPN 3000 con versiones de software 4.1.x y posteriores **Nota:** La función Bandwidth Management se introdujo en la versión 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 la red

En este documento, se utiliza esta configuración de red:



Convenciones

Para obtener más información sobre las convenciones del documento, consulte <u>Convenciones de</u> <u>Consejos Técnicos de Cisco</u>.

Configuración de una Política de Ancho de Banda Predeterminada en el Concentrador VPN 3000

Antes de configurar la Administración del Ancho de Banda en los túneles de LAN a LAN o en los túneles de acceso remoto, debe habilitar la Administración del Ancho de Banda en la interfaz pública. En esta configuración de ejemplo, se configura una política de ancho de banda predeterminada. Esta política predeterminada se aplica a los usuarios/túneles que no tienen una política de Administración de ancho de banda aplicada al grupo al que pertenecen en el VPN Concentrator.

 Para configurar una política, seleccione Configuration > Policy Management > Traffic Management > Bandwidth Policies y haga clic en

Add.		
Configuration - theritons - Distance -	Configuration Policy Management Traffic Management Bandwidth Policies This section lets you add, modify and delete bandwidth policies. Circk Add to add a policy, or select a policy and circk Modify or Delete. Bandwidth Policies Actions Empty- Add Modity Delete	Save Needec

Después de hacer clic en Agregar, se muestra la ventana Modificar

nfigare bandwidth policy parameters. 1	To create a bandwi	th policy, you must enable at least one of the checkboxes.
Policy Name Default		Enter a unique name for this policy
🕫 Bandwidth Reservation		Check to reserve a minimum bandwidth per session.
Minimum Bandwidth 56	kbps *	Enter the minimum bandwidth
	and the second	feedfor to construct a construct on an interaction. The first second attack of the contract sectors of the const
Traffic policing allows you to control a po	shiring rate or size o	t danie transmise or received on an invitace, traine that excreds the policing face or own size is dropped.
Traffic policing allows you to control a po Policing	shiring rate or size o	t name manimums or receives on an interface. Traine that encrean the posteng rate or ourst size is gropped. Check to enable Policing.
Traffic policing allows you to control a po Policing Policing Rate 96	sbring rate or size o	chanc trainmine or receives on an interface. Trainc that encrean the policing rate or burn nize is gropped. Check to enable Policing. Enter the policing rate. Traffic below this rate will be transmitted, traffic above this rate will be dropped.

2. Establezca estos parámetros en la ventana Modificar. Nombre de política: introduzca un nombre de política único que le ayude a recordar la política. La longitud máxima es de 32 caracteres. En este ejemplo, el nombre 'Default' se configura como Policy Name. Reserva de ancho de banda: active la casilla de verificación Reserva de ancho de banda para reservar una cantidad mínima de ancho de banda para cada sesión. En este ejemplo, se reservan 56 kbps de ancho de banda para todos los usuarios de VPN que no pertenecen a un grupo que tiene configurada la Administración del ancho de banda. Regulación de tráfico: active la casilla de verificación Regulación de tráfico para habilitar la regulación de tráfico. Introduzca un valor para Velocidad de regulación y seleccione la unidad de medida. El concentrador VPN transmite el tráfico que se mueve por debajo de la velocidad de regulación y descarta todo el tráfico que se mueve por encima de la velocidad de regulación. 96 kbps está configurado para la regulación del ancho de banda. El tamaño normal de ráfaga es la cantidad de ráfaga instantánea que el VPN Concentrator puede enviar en cualquier

momento. Para establecer el tamaño de ráfaga, utilice esta fórmula: (Policing Rate/8) * 1.5

Con esta fórmula, la Velocidad de ráfaga es de 18000 bytes.

3. Haga clic en Apply (Aplicar).

م مر ما را

- 4. Seleccione **Configuration > Interfaces > Public Interface** y haga clic en la pestaña Bandwidth para aplicar la política de ancho de banda predeterminada a una interfaz.
- 5. Active la opción Administración del ancho de banda.
- Especifique la velocidad del link.La velocidad del link es la velocidad de la conexión de red a través de Internet. En este ejemplo se utiliza una conexión T1 a Internet. En consecuencia, 1544 kbps es la velocidad de link configurada.
- 7. Seleccione una política en la lista desplegable Política de ancho de banda.La política predeterminada se ha configurado anteriormente para esta interfaz. La política que aplica aquí es una política de ancho de banda predeterminada para todos los usuarios de esta interfaz. Esta política se aplica a los usuarios que no tienen una política de administración de ancho de banda aplicada a su

grupo. 🛕 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).** ral RIP OSPF Dendwidth **Bandwidth Management Parameters** Value Attribute Description Bandwidth Management 🗟 Check to enable bandwidth management. htps Set the link rate that will be applied to all tunneled traffic. The defined link rate must be based on available Internet bandwidth Link Rate 1544 and not the physical LAN connection rate. This policy is applied to all VPN tunnels that do not have a group based Bandwidth Management policy. Policies are Bandwidth Policy Detaut onfigured at Configuration | Policy Management | Traffic Management | Bandwidth Policies. Apply Cancel

Configuración de la administración del ancho de banda para túneles de sitio a sitio

Complete estos pasos para configurar la Administración del Ancho de Banda para los túneles de sitio a sitio.

 Seleccione Configuration > Policy Management > Traffic Management > Bandwidth Policies y haga clic en Add para definir una nueva política de ancho de banda de LAN a LAN.En este ejemplo, se configuró una política llamada 'L2L_tunnel' con una reserva de ancho de banda de 256

onfigure bandwidth poli	cy parameters. To cre	ate a bandwi	th policy, you must enable at least one of the checkbones.
Policy Name	L2L_turnel	-	Enter a unique name for this policy.
Bandwidth Reserv	ation		Check to reserve a minimum bandwidth per session.
Minimun Bandwi	dth [256	kbps 💌	Enter the minimum bandwidth
raffic poäcing allows yo	u to control a policing	rate or size of	f traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped
Policing			Check to enable Policing
Policing R	ate 56	kbps 💌	Enter the policing rate. Traffic below this rate will be transmitted, traffic above this rate will be dropped.
			We cannot show a water as the second state of the second state of the second state of the

2. Aplique la política de ancho de banda al túnel LAN a LAN existente en el menú desplegable Bandwidth Policy (Política de ancho de

banda)).
Sanaa	

hytos

Configuration System	1 Tunneling Protoco	ils IPSec LAN to L	AN A44
Add a new IPSec LAN	I-to-LAN connection	é.	
Name	to_spoke		Enter the name for this LAN-to-LAN connection.
Interface	Ethemet 2 (Public) (1	72.18.124.135) *	Select the interface for this LAN-to-LAN connection.
Peer	17218124134		Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate	None (Use Preshare	ad Keys) *	Select the dupial certificate to use.
Certificate Transmission	C Entire certificate # Identity certificate	chain e only	Choose how to send the digital certificate to the IKE peer.
Preshared Key	cisco123		Enter the preshared key for this LAN-to-LAN connection.
Authentic ation	ESP/MD5/HMAC-12	8 -	Specify the packet authentication mechanism to use.
Encryption	3DES-168 .		Specify the encryption mechanism to use.
IKE Proposal	IKE-3DES-MD5	-	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter	-None-	*	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T	E .		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	L2L_tunnel ·		Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing	None		Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.
Local Network: If a L	AN-to-LAN NAT n	ale is used, this is the	Translated Network address.
Network List	Use IP Address/Wild	dcard-mask below 💌	Specify the local network address hit or the IP address and wildcard mark for this LAN-to-LAN connection.
IP Address	14.38.0.0		neger gener hennen weren en der einen einen eine weren einen eine einen einen einen einen der eine eine einen Weren Weren Stratten und eine Bereichte der einen weren Stratten eine Bertreten einen eine Bertreten Stratten St
Wildcard Mark	0.0.255.255		Note: Enter a wildcard mask, which is the reverse of a subset mask. A valor of dimark has is in or pormons to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1 mm addresses.
Remote Network: If a	ALAN-to-LAN NAT	l'rule is used, this is t	he Remote Network address
Network List	Use IP Address/Wik	dcard-mask below 💌	Specify the remote network address hit or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address	10.100.100.0		Note: Process will develop the which is the second of a submet work. A will be advect by a bit which is the second
Wildcard Mask	0.0.0.255		Fore: Enter a wank of a statistic state reverse of a submer mask. A whole if of miss, and its in on positions to ignore, Os in bit positions to match. For example, 10.10.1.000.0.255 = al 10.10.1.nn addresses.
Add Cancel	t i		

Configuración de la Administración de Ancho de Banda para los Túneles VPN Remotos

Complete estos pasos para configurar la Administración del Ancho de Banda para los túneles VPN remotos.

 Seleccione Configuration > Policy Management > Traffic Management > Bandwidth Policies y haga clic en Add para crear una nueva política de ancho de banda.En este ejemplo, se configura una política llamada 'RA_tunnels' con una reserva de ancho de banda de 8 kbps. La regulación del tráfico se configura con una velocidad de regulación de tráfico de 128 kbps y un tamaño de ráfaga de 24000

onfigure bandwidth pol	cy parameters. To o	create a bandwi	ith policy, you must enable at least one of the checkboxes.
Policy Name	RA_tunnels		Enter a unique name for this policy.
🕫 Bandwidth Reserv	ation		Check to reserve a minimum bandwidth per session.
Mininean Bandwi	dala (3	kbps 💌	Enter the minimum bandwidth.
Traffic policing allows yo	u to control a polici	ing rate or size o	f traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped.
Policing			Check to enable Policing
Policing R	ate 128	kbps -	Enter the policing rate. Traffic below this rate will be transmitted, traffic above this rate will be dropped.
Normal Burst S	are 24000	bytes *	Enter the amount of data allowed in a burst before excess packets will be dropped.

2. Para aplicar la política de ancho de banda a un grupo VPN de acceso remoto, seleccione

Configuration > User Management > Groups, seleccione su grupo y haga clic en **Assign Bandwidth**

Policies.

Cerliguration User Management Groups	Save Needed
This section.lets you configure groups. A group is a collection of users treated as a single	atity.
Click the Add Group button to add a group, or select a group and click Delete Group	r Modify Group. To modify other group parameters, select a group and click the appropriate button.
Current Group	Actions
	Add Group
17218124134 (J2L Intervely insectory Untervely Conto	Configured) Modify Group
	Modily Auth. Servers
	Modey Acct Servers
	Modily Address Pools
	Modity Client Update
	Assign Bendwidth Policie)
	Delete Group

3. Haga clic en la interfaz en la que desea configurar la Administración de ancho de banda para este grupo.En este ejemplo, 'Ethernet2 (Public)' es la interfaz seleccionada para el grupo. Para aplicar una política de ancho de banda a un grupo en una interfaz, la Administración de ancho de banda debe estar habilitada en esa interfaz. Si elige una interfaz en la que se inhabilita la Administración de ancho de banda, aparecerá un mensaje de

an and an all the second states and		
Sack to Groups		
Configure group-wide	bandwidth parameters for each interface.	
	. C. 1997 (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1	
Interface	Description	
Interface Ethernet 1 (Private)	Description	
Interface Ethernet 1 (Private) Ethernet 2 (Public)	Description Click the interface you want to configure	= =

advertencia.

4. Seleccione la política de ancho de banda para el grupo VPN para esta interfaz.La política RA_tunnels, que se definió previamente, se selecciona para este grupo. Introduzca un valor para el ancho de banda mínimo que se reservará para este grupo. El valor predeterminado de la agregación de ancho de banda es 0. La unidad de medida predeterminada es bps. Si desea que el grupo comparta el ancho de banda disponible en la interfaz, ingrese

0.	
Configuration User Management Groups Bandwidth Policy Interfaces	
	Save Needed
Configure group-wide bandwidth parameters. To share global available bandwidth, instead of a specific reservation, enter 0 in the Bandwidth Aggregation textbox.	
Ethernet 2 (Public)	
Policy RA_tunnels	
Baudwidth Aggregation 0 bps 💌 Enter the aggregate reserved group bandwidth for this interface.	
Apply Cancel	

Verificación

Seleccione **Monitoring > Statistics > Bandwidth Management** en el VPN 3000 Concentrator para monitorear Bandwidth Management .

Monitoring Statistics Bandwidth W	anagement			Wednesday	, 14 August 2002 14:15: Reset @ Refresh	
This screer, shows bandwidth manager	ment information. To refresh the statistics.	, the's Refresh. Select a Group t	o filter the users.			
Group -/J-						
	Transform	Traffic Rate (kbps)		Traffic Volume	Traffic Volume (bytes)	
User Name	Interface	Conformed	Throttled	Cordormed	Throttled	
ipsecriser (In)	Ethemet 2 (Public)	10	5	1/13/13/2	1004508	
		1 2.54		2011-011-01		
quarcuser (Out)	Ethemat 2 (Public)	11	2	1321326	74700	
gancase (Out) to_spoke (In)	Ethernet 2 (Public) Ethernet 2 (Public)	11	237	1321326 206052492	74700 23369858	

Troubleshoot

Para resolver cualquier problema mientras se implementa la Administración del Ancho de Banda en el VPN 3000 Concentrator, habilite estas dos Clases de Evento en **Configuración > Sistema > Eventos > Clases**:

- BMGT (con gravedad para registrar: 1-9)
- BMGTDBG (con Gravedad para Registrar: 1-9)

Estos son algunos de los mensajes de registro de eventos más comunes:

• El mensaje de error Excedes the Aggregate Reservation se ve en los registros cuando se modifica una política de ancho de banda.

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 Interrface [2] exceeds the Aggregate Reservation [0 bps] configured for that group.

Si se muestra este mensaje de error, vuelva a la configuración del grupo y anule la aplicación de la política 'RA_tunnel' del grupo. Edite 'RA_tunnel' con los valores correctos y, a continuación, vuelva a aplicar la política al grupo específico.

No se puede encontrar el ancho de banda de la interfaz.

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. Puede recibir este error si la política de ancho de banda no está habilitada en la interfaz e intenta aplicarla en el túnel de LAN a LAN. Si este es el caso, <u>aplique una política a la interfaz</u> <u>pública</u> como se explica en la sección <u>Configure una Política de Ancho de Banda</u> <u>Predeterminada en el VPN 3000 Concentrator</u>.

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de soporte de IPSec

<u>Soporte Técnico - Cisco Systems</u>