

SecureFirst

Bandwidth Management of Site to Site VPN Traffic (Pre SonicOS 5.8.1 firmware)

KNOWLEDGE DATABASE



Bandwidth Management of Site to Site VPN Traffic (Pre SonicOS 5.8.1 firmware)

DESCRIPTION:

SonicOS Enhanced offers an integrated traffic shaping mechanism through its Egress (outbound) and Ingress (inbound) bandwidth management (BWM) interfaces. Outbound BWM can be applied to traffic sourced from Trusted and Public Zones (such as LAN and DMZ) destined to Untrusted and Encrypted Zones (such as WAN and VPN). Inbound BWM can be applied to traffic sourced from Untrusted and Encrypted Zones destined to Trusted and Public Zones.

This scenario based article describes how to configure bandwidth management on a site-tosite VPN Policy. In this scenario, the site-to-site VPN has been configured on both sides and the tunnel is up.

Sett	ing	S						
🚱 Ad	cept	Cancel						
VPN G	ilobal	Settings						
🗹 Ena Unique I	ible VF Firewal	*N I Identifier: 0017	- et = 163					
VPN P	olicie	5						
Г	#	Name	Gateway		Destinations	Crypto Suite	Enable	Configure
П	1	WAN GroupVPN				ESP: 3DES/HMAC SHA1 (IKE)		Ø0±
1	2	WLAN GroupVPN				ESP: 3DES/HMAC SHA1 (IKE)		001
	з	To Site A	2.2.2.2		192.168.168.0 - 192.168.168.255	ESP: 3DES/HMAC SHA1 (IKE)	v	Ø×
	4	To Main Office	3,3.3.3	0	10.10.10.15 - 10.10.10.15	ESP: 3DES/HMAC SHA1 (IKE)	5	

RESOLUTION:

Enabling Bandwidth Management Settings on the WAN Interface | Advancedtab

Note: Once BWM has been enabled on an interface, and a link speed has been defined, traffic traversing that link will be throttled—both inbound and outbound-to the declared values, even if no Access Rules are configured with BWM settings.

BWM configurations begin by enabling BWM on the relevant **WAN** interface, and declaring the interface's available bandwidth in Kbps (Kilobits

per second). This is performed from the **Network** | Interfaces page by selecting the Configure icon for the **WAN** interface, and navigating to the **Advanced** tab:

Figure 1: Network | (WAN) Interface | Advanced Tab

General	Advanced	
Advanced Settir	igs	
ink Speed:	Auto N	legotiate 👻
Ose Default MA	C Address: 00:17:	C5:27:B2:DD
) Override Defau	It MAC Address:	
Enable Multicas	t Support	
Enable 802.1p	tagging 1	
nterface MTU:	1500	
Eragment non-	VPN outbound packets	larger than this Interfa
🗌 Ignore Do	n't Fragment (DF) Bit	
Do not send IC Do not send IC	MP Fragmentation Need	led for outbound pack
andwidth Man	agement	
🗹 Enable Egress (Jandwidth Management	
Available Inter Kbps):	rface Egress Bandwidth	1500.00000
🗹 Enable Ingress	Bandwidth Managemen	t
Available Inter	rface Incress Bandwidth	1

Egress and Ingress BWM can be enabled jointly or separately on WAN interfaces. Different bandwidth values may be entered for outbound and inbound bandwidth to support asymmetric links. Link rates up to 100,000 Kbps (100Mbit) may be declared on Fast Ethernet interfaces, while Gigabit Ethernet interfaces will support link rates up to 1,000,000 Kbps (Gigabit). The speed declared should reflect the actual bandwidth available for the link. Oversubscribing the link (i.e. declaring a value greater than the available bandwidth) is not recommended.

(Kbps):

Note: Once BWM has been enabled on an interface, and a link speed has been defined, traffic traversing that link will be throttled—both inbound and outbound—to the declared values, even if no Access Rules are configured with BWM settings.

Once one or both BWM settings are enabled on the WAN interface and the available bandwidth has been declared, a Bandwidth tab will appear on Access Rules. Bandwidth The tab will present either Inbound settings, Outbound settings, or both, depending on what was enabled on the WAN interface:



1000.000000



Bandwidth Management on a Site to Site VPN Policy

When a site to site VPN policy is created, a number of rules are created depending on the zones in the Local Network specified in the VPN Policy. For example, if the Local Networks consist of the LAN & DMZ zones, the following four rules are created:1) LAN | VPN 2) DMZ | VPN 3) VPN | LAN 4) VPN | DMZ.

Bandwidth Management can be configured on these rules depending on the direction of the traffic:

For traffic initiated from the LAN / DMZ to the VPN Tunnel

- Navigate to the Firewall | Access Rules page
- Select LAN | VPN (or DMZ | VPN as the case may be)
 Click on the edit button on the following auto-
- created VPN rule and configure BWM.

General	Advanced	QoS	Ethernet BW
Settings			
Action:	@ Allow @ Deny @	Discard	
From Zone:	LAN	¥	
To Zone:	VPN	*	
Src Service:	Any	•	
Dst Service:	Any	•	
Source:	X8 Subnet	¥	
Destination:	SiteBVPNNetwork	÷	
Users Allowed:	All	•	
Schedule:	Always on	•	
Comment:	Auto added for outbo	und VPN - To S	
🗹 Enable Loggin	ng		
I Allow Fragme	nted Packets		
Enable flow r	eporting		
🗌 Enable packe	t monitor		
🗌 Enable Manaç	ement *		
🔲 Don't invoke	Single Sign On to Authentica	te Users	
ady			
	OK	Cancel	Help

Enable Outbound B	andwidth Manager	ment ('allow' rules	only)	
Guaranteed Bandw	idth:	40	96 -	
Maximum Bandwidt	h:	70	96 -	3
Bandwidth Priority:		0 highest 💌]	
Enable Inbound Bar	ndwidth Manageme	ent ('allow' rules o	nly)	
Guaranteed Bandw	idth:	40	%	3
Maximum Bandwidt	h:	70	%	3
Bandwidth Priority:		0 highest 💌	1	

In the above access rule, any traffic from the LAN (Trusted) Zone's LAN Subnets destined to the remote VPN subnet (Encrypted) will be guaranteed 40% of the declared bandwidth (40% of 1500Kbps = 600Kbps), but it will not be permitted to exceed 70% (70% of 1500 Kbps = 1050 Kbps).

Add

Close

Help

Here is a BWM usage status when a file is being downloaded from a remote site FTP Server ovre VPN.

	Dashboard	Frewall /								-		-
	System Network	Access Rules								Bandwidth Management Ethernet Bandwidth Manage	ment:	
	3G/Modern	Restore Defaults								Outbound Parameters: guaranteed = 40.000 %		
ę	SonicPoint Firewal Access Rules	Access Rules (LAN > VPN)								maxmum = 70.000 % priority = 0 usage = 3.515 % dropped = 0		
	App Rules App Control Advanced	View Style: C All Rules	Matrix	C Drop-dov	vn Baxes					Inbound Parameters: guaranteed = 40.000 % maximum = 70.000 %		
	Match Objects Action Objects	Add.	Destination	Src Service	Dst Service	Action	Users Flo	w Packet	Comme	usage = 69.000 % dropped = 0		a Defaults
	Address Objects Service Objects	I 1 X0 Subnet	SiteBVPNNetwork	Any	Any	Allow	Al		29	0		00
	Email Addr Objects	E 2 2 X0 Subnet	10.10.10.15	Any	Any	Alow	Al		ø	0		00
100	Firewall Settings DPI-SSI.	III 3 3 WAN RemoteAcces Networks	s VPN DHCP Clients	Any	Any	Alow	AI		ø			00

For traffic initiated from the other side of the VPN Tunnel

- Navigate to the Firewall | Access Rules
- Select VPN |LAN
- Click on the edit button on the following auto-created VPN rule and configure BWM.





	Advanced	000	Emerier	BW
Settings				
Action:	@ Alow @ De	ny 🐔 Discard		
From Zone:	VPN		2	
To Zone:	LAN		-	
Src Service:	Any		•	
Dst Service:	Any		-	
Source:	SiteBVPNNetw	ork	-	
Destination:	X0 Subnet		-	
Users Allowed:	All		•	
Schedule:	Always on	1	•	
Comment:	Auto added for i	nbound VPN - To S	Site	
🗹 Enable Loggin	9			
Allow Fragmer	nted Packets			
Enable flow re	eporting			
🗆 Enable packet	monitor			
Enable packet Enable Magaze	: monitor			
Enable packet Enable Manage	: monitor ement			
Enable packet Enable Manage Don't invoke S	: monitor ement Single Sign On to Auth	enticate Users		
Enable packet Enable Manage Don't invoke S dy	: monitor ement [*] Single Sign On to Auth	enticate Users		
Enable packet Enable Manage Don't invoke S	monitor ement [•] Single Sign On to Auth	enticate Users		
Enable packet Enable Manage Don't Invoke S	: monitor ement [•] Single Sign On to Auth	enticate Users OK Cano	cel He	lp
Enable packet Enable Manag Don't invoke \$ dy General	: monitor ement [•] Single Sign On to Auth	OK Can	cel He	lp 3WI
Enable packet Enable Manag Don't invoke S dy General	: monitor ement [•] Single Sign On to Auth Advanced	OK Cano	cel He Ethernet 8	lp 3WI
Enable packet Enable Manag Don't Invoke S dy General	monitor ement Single Sign On to Auth Advanced th Management	OK Cano QoS	cel He Ethernet 8	lp 3WI
Enable packet Enable Manag Don't invoke S dy General hernet Bandwidt	monitor ement [•] Single Sign On to Auth Advanced th Management	OK Can	cel He Ethernet B	lp 3VVI
Enable packet Enable Manag Don't invoke \$ dy General hernet Bandwidt Enable Outboun	monitor ement ¹ Single Sign On to Auth Advanced th Management d Bandwidth Managem	OK Cano OK Cano QoS nent ('allow' rules only	cel He Ethernet B	lp 3VVI
Enable packet Enable Manag Don't invoke { dy General Fernet Bandwidt Enable Outboun Guaranteed Ban	monitor ement ¹ Single Sign On to Auth Advanced th Management d Bandwidth Managem dwidth:	OK Can OK Can QoS nent ('allow' rules only 40	Ethernet E	lp 3WI
Enable packet Enable Manag Don't invoke § dy General Fernet Bandwidt Enable Outboun Guaranteed Ban Maximum Bandw	monitor ement ¹ Single Sign On to Auth Advanced th Management d Bandwidth Managerr dwidth: ridth:	OK Cano OK Cano QoS nent ('allow' rules only 40 70	cel He Ethernet 8	lp 3VVI
Enable packet Enable Manag Don't invoke § dy General Fernet Bandwidth Enable Outboun Guaranteed Ban Maximum Bandwidth Priori	monitor ement Single Sign On to Auth Advanced Management d Bandwidth Managem dwidth: adth: ty:	OK Can OK Can QoS nent ('allow' rules only 40 70 0 highest	cel He Ethernet £	lp 3VVI
Enable packet Enable Manag Don't invoke § dy General Fernet Bandwidt Enable Outboun Guaranteed Ban Maximum Bandw Bandwidth Priori Enable Inbound	monitor ement ¹ Single Sign On to Auth Advanced Advanced th Management d Bandwidth Manageme dwidth: ridth: ty: Bandwidth Manageme	enticate Users OK Cano QoS nent ('allow' rules only 40 70 0 highest • nt ('allow' rules only)	cel He Ethernet B	lp 3VVI
Enable packet Enable Manag Don't invoke § dy General Fernet Bandwidth Enable Outboun Guaranteed Ban Maximum Bandwidth Priori Enable Inbound Guaranteed Ban	monitor ement Single Sign On to Auth Advanced Management d Bandwidth Management dwidth: high: ty: Bandwidth Management dwidth:	enticate Users OK Cano QoS nent ('allow' rules only 40 70 0 highest T nt ('allow' rules only) 40	cel He Ethernet 0) % ▼ % ▼	Ip BWVI
Enable packet Enable Manag Don't invoke § dy General Fernet Bandwidt Enable Outboun Guaranteed Ban Maximum Bandw Bandwidth Priori Enable Inbound Guaranteed Ban Maximum Bandw	monitor ement Single Sign On to Auth Advanced Management d Bandwidth Managerre dwidth: http: Bandwidth Managerre dwidth: http:	enticate Users OK Cano QoS ent ('allow' rules only 40 70 0 highest • ent ('allow' rules only) 40 70	cel He Ethernet B	1p 3VVI
Enable packet Enable Manag Don't invoke § dy General Fernet Bandwidth Enable Outboun Guaranteed Ban Maximum Bandwidth Priori Enable Inbound Guaranteed Ban Maximum Bandw Bandwidth Priori Antipication Bandwidth Priori Bandwidth Priori Bandwidth Priori Comparison C	monitor ement Single Sign On to Auth Single Sign On to Auth Advanced Advanced Management dwidth: dwidth: dwidth: dwidth: dwidth: dwidth: dwidth: ty:	enticate Users OK Cano QoS nent ('allow' rules only 40 70 0 highest 140 70 10 highest 140 70 10 highest 1	cel He Ethernet 6) % % % %	lp 3WI
Enable packet Enable Manag Don't invoke § dy General Fernet Bandwidth Enable Outboun Guaranteed Ban Maximum Bandwidth Priori Enable Inbound I Guaranteed Ban Maximum Bandw Bandwidth Priori Z Enable Inbound I Guaranteed Ban Maximum Bandw Bandwidth Priori Z Enable Inbound I Guaranteed Ban Maximum Bandw Bandwidth Priori Z Enable Inbound I Guaranteed Ban Maximum Bandw Bandwidth Priori	monitor ement Single Sign On to Auth Advanced Management dwidth: didth: ty: Bandwidth Manageme dwidth: idth: ty:	enticate Users OK Can QoS ent ('allow' rules only 40 70 0 highest 70 70 70 0 highest 70 70	cel He Ethernet E) 96 ▼ 96 ▼ 96 ▼	lp 3VVI

Add Close Help



Calle 140 #11-45. Bogotá D.C. Colombia +57 1 368 0290 / +57 3184914652 sales@itclatam.com / tss@itclatam.com REV 1.01