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

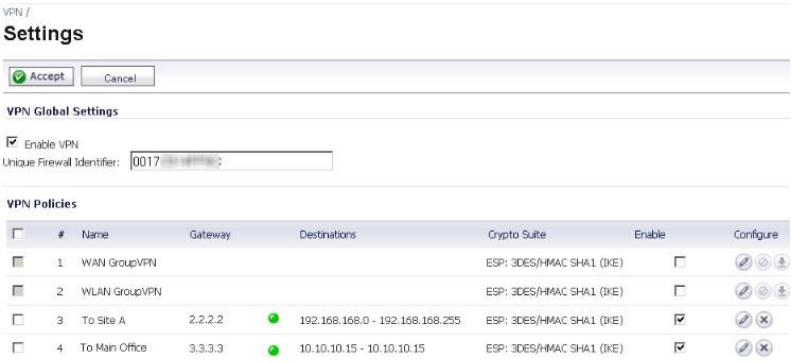
KNOWLEDGE DATABASE

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-to-site VPN Policy. In this scenario, the site-to-site VPN has been configured on both sides and the tunnel is up.



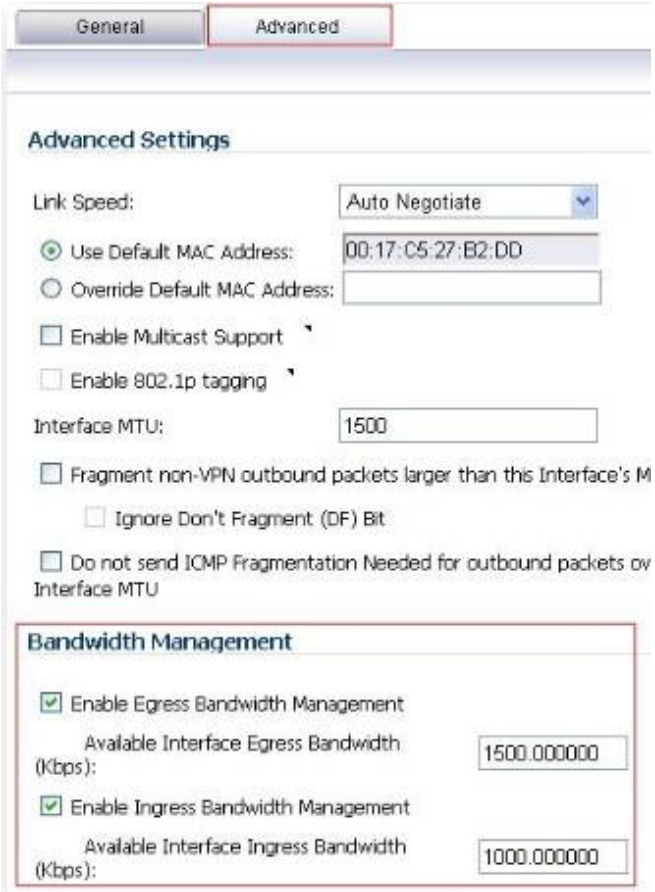
RESOLUTION:

Enabling Bandwidth Management Settings on the WAN Interface | Advanced tab

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



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.

***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**. The **Bandwidth** tab will present either **Inbound** settings, **Outbound** settings, or both, depending on what was enabled on the WAN interface:*

Calle 140 #11-45. Bogotá D.C. Colombia
+57 1 368 0290 / +57 318 4914652
sales@itclatam.com / tss@itclatam.com

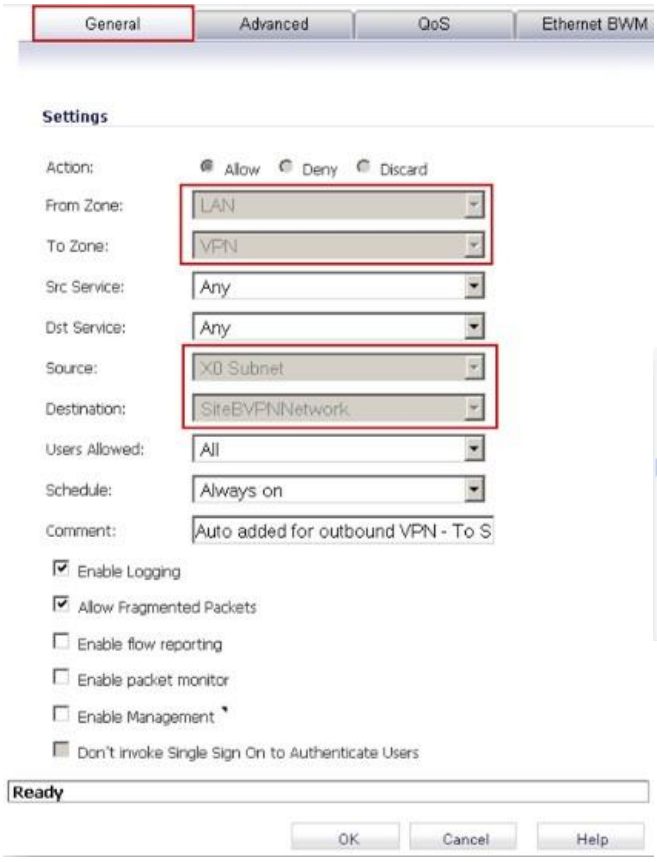
Bandwidth Management on a Site to Site VPN Policy

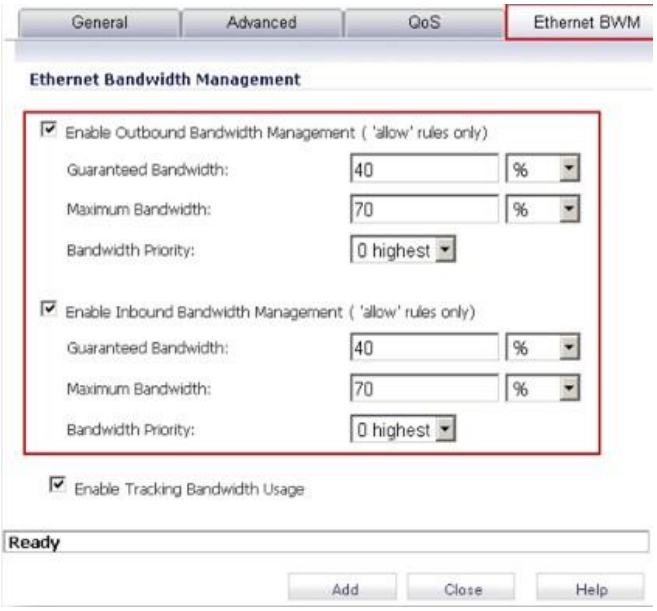
When a site to site VPN policy is created, a number of rules are created depending on the zones in the Local Network specified in the VPN Policy. For example, if the Local Networks consist of the LAN & DMZ zones, the following four rules are created: 1) LAN | VPN 2) DMZ | VPN 3) VPN | LAN 4) VPN | DMZ.

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

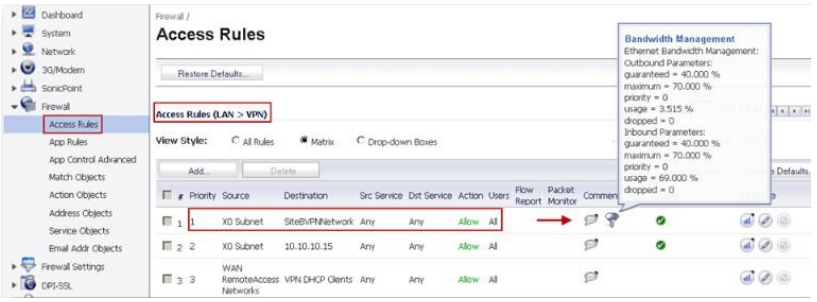
- Navigate to the **Firewall** | **Access Rules** page
- Select **LAN** | **VPN** (or **DMZ | VPN** as the case may be)
- Click on the edit button on the following auto-created VPN rule and configure BWM.





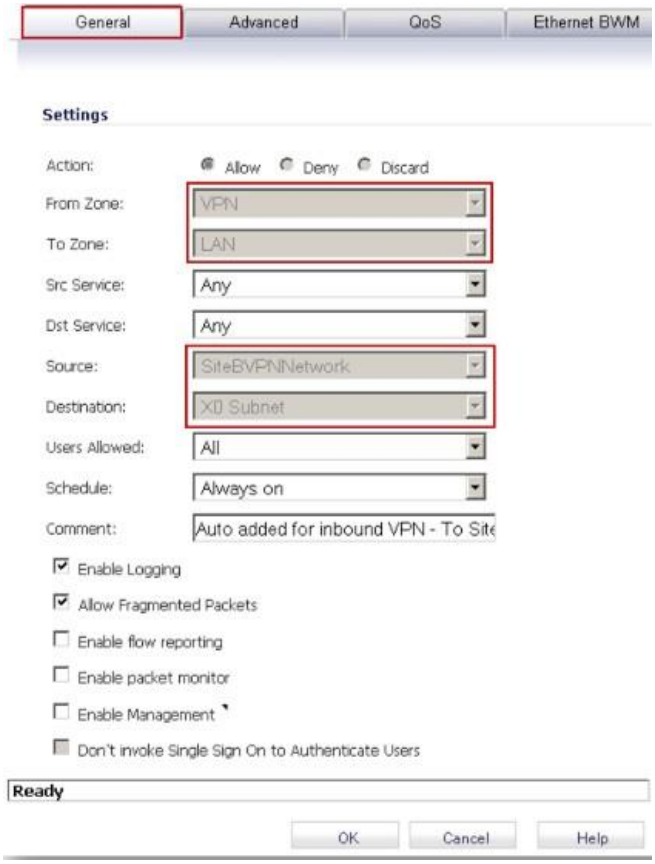
In the above access rule, any traffic from the LAN (Trusted) Zone's **LAN Subnets** destined to the remote VPN subnet (Encrypted) will be guaranteed 40% of the declared bandwidth (40% of 1500Kbps = 600Kbps), but it will not be permitted to exceed 70% (70% of 1500 Kbps = 1050 Kbps).

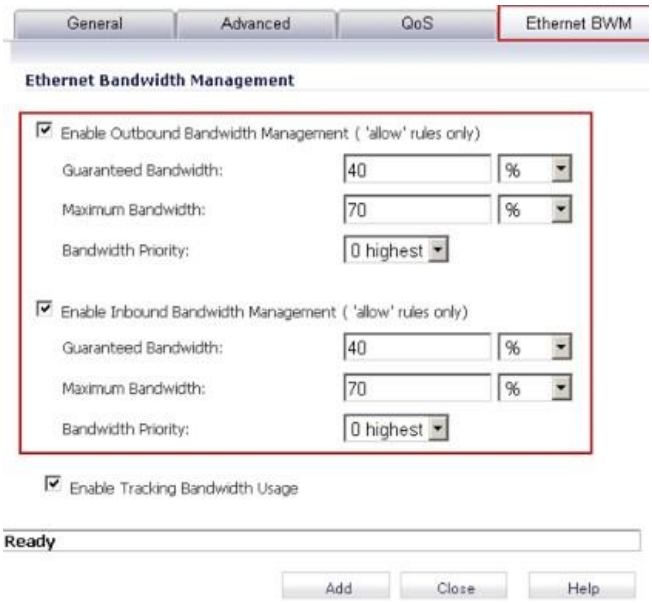
Here is a BWM usage status when a file is being downloaded from a remote site FTP Server ovre VPN.



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.





Calle 140 #11-45. Bogotá D.C. Colombia
+57 1 368 0290 / +57 318 4914652
sales@itclatam.com / tss@itclatam.com