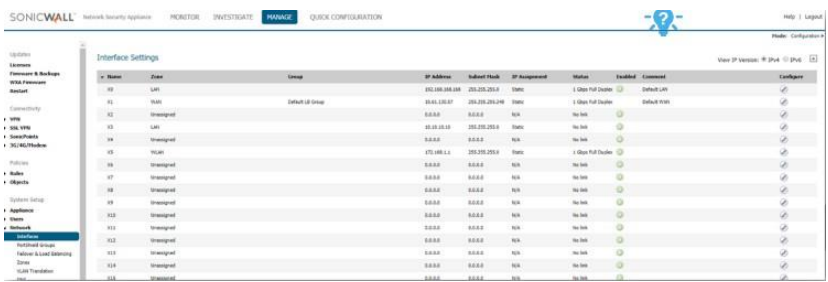




**How Can I Configure
Bandwidth
Management?**

**KNOWLEDGE
DATABASE**

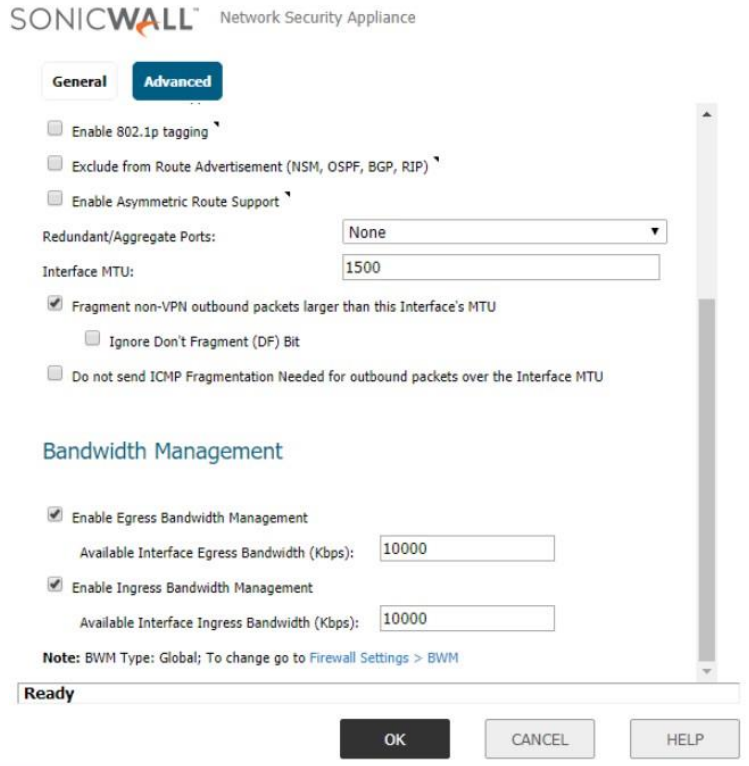
HOW CAN I CONFIGURE BANDWIDTH MANAGEMENT?



DESCRIPTION:

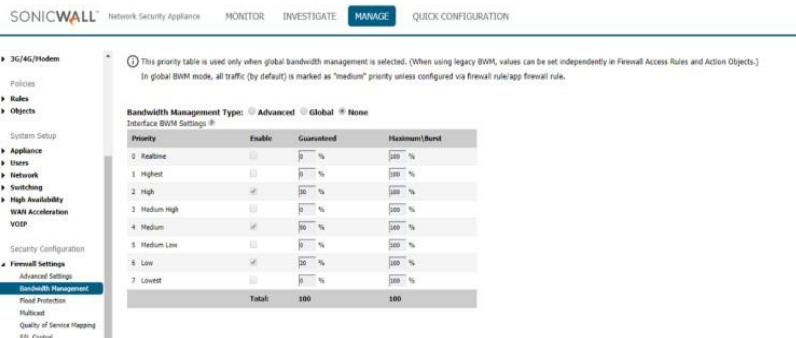
This article shows the steps needed to configure bandwidth management (BWM). SonicOS offers an integrated traffic shaping mechanism through its Interfaces, for both Egress (Outbound) and Ingress (Inbound) traffic. Outbound BWM can be applied to traffic sourced from **Trusted** and **Public Zones** (such 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.

1. Navigate to **Advanced** tab and Enable both the **Ingress** and **Egress Bandwidth Limitation** checkboxes.



Enabling Bandwidth Management (Either Advanced or Global)

1. Click **Manage** in the top navigation menu.
2. Navigate to **Firewall Settings | BWM**. Select either **Advanced** or **Global**, depending on your desired configuration.
3. Click **Accept**.



3. Input the Ingress and Egress Speeds of your WAN in Kbps. If you're unsure of these values, contact your ISP.
4. Click **OK**.

Creating Bandwidth Object (Only for Advanced BWM)

1. Click **Manage** in the top navigation menu.
2. Navigate to **Objects | Bandwidth Objects** and click **Add**.



Configure Bandwidth Management in WAN Interface

1. Navigate to **Network | Interfaces** and on the right side of the screen open the configure menu for the desired WAN Interface.

3. Add a Name, Guaranteed/Maximum Bandwidth, Traffic Priority, and Violation Action.

4. Click **OK**.

2. On the access rule creation/modification screen, select the **BWM** tab. On the BWM tab, enable **Egress or Ingress Bandwidth Management**, depending on which you wish to enforce and select the appropriate **Bandwidth Priority** (if Global BWM) or **Bandwidth Object** (if Advanced BWM).

3. Click **OK**.

Creating or Editing an Access Rule to apply Bandwidth Management

1. Navigate to **Rules | Access Rules** and find the access rule you'd like to apply BWM to. If a new access rule is required. Click configure on the relevant access rule or click **Add** and create the rule by entering the desired Source, Destination, Service, etc. into the fields.

#	From	To	Priority	Source	Destination	Service	Action	Status	Users Eval.	Enable (OP)	Flow report	Geo IP	Action	Enable (OP)	Enable (S2)	FR monitor
1	DMZ	DMZ	1	Any	Any	Any	allow	on	None							
2	DMZ	DMZ	2	Any	Any	Any	allow	on	None							
3	DMZ	LAN	2	Any	Any	Any	deny	on	None							
4	DMZ	VPN	1	SSL VPN RemoteAccess Networks	Any	Any	allow	on	None							
5	DMZ	VPN	2	SSL VPN RemoteAccess Networks	Any	Any	allow	on	None							
6	DMZ	WAN	1	Any	Any	Any	allow	on	None							
7	DMZ	WAN	2	Any	Any	Any	allow	on	None							
8	DMZ	WAN	1	Any	Any	Any	deny	on	None							
9	DMZ	LAN	2	Any	Any	Any	deny	on	None							
10	DMZ	LAN	1	Any	Any	Any	deny	on	None							
11	LAN	WAN	2	Any	Any	Any	allow	on	None							
12	LAN	DMZ	2	Any	Any	Any	allow	on	None							
13	LAN	LAN	2	Any	IP Management IP	HTTP Management	allow	on	None							
14	LAN	LAN	2	Any	IP Management IP	HTTP Management	allow	on	None							