Watchguard Traffic Management and QoS

In a network with many computers, the volume of data that moves through the firewall can be very large. You can use Traffic Management and Quality of Service (QoS) actions to prevent data loss for important business applications, and to make sure mission-critical applications take priority over other traffic.

Traffic Management and QoS provide a number of benefits. You can:

- Guarantee or limit bandwidth
- Control the rate at which the XTM device sends packets to the network
- Prioritize when to send packets to the network

To apply traffic management to policies, you define a Traffic Management Action. A Traffic Management Action is a collection of settings that you can apply to one or more policy definitions. You do not need to configure the traffic management settings separately in each policy. If you use Application Control, you can also apply Traffic Management Actions to specific applications and application categories. You can define additional Traffic Management Actions if you want to apply different settings to different policies or applications.

Enable Traffic Management and QoS

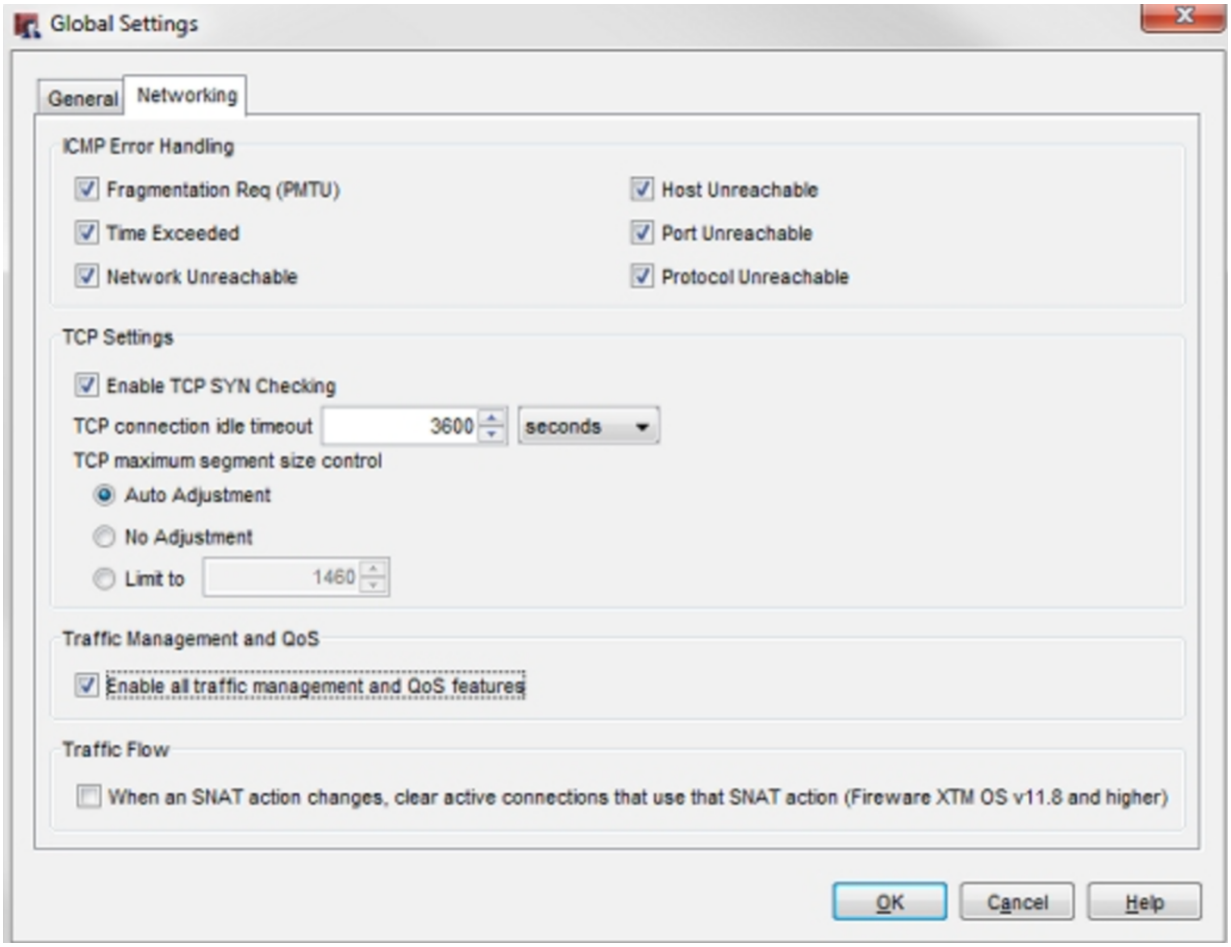
For performance reasons, all Traffic Management and QoS features are disabled by default. You must enable these features in Global Settings before you can use them.

When you enable all traffic management and QoS feature in the Global Settings, the Firebox or XTM device must make additional decisions about traffic, even if you don't configure Traffic Management or QoS in any policies. This can cause a noticeable reduction in overall throughput, especially on smaller devices that have less processing power. Do not enable Traffic Management and QoS in the global settings unless you are going to use these features.

To enable Traffic Management and QoS features.

- Select Setup > Global Settings.
  The Global Settings window appears.

- Select the Networking tab.



- Select the Enable all traffic management and QoS features check box.
- Click OK.
- Save the Configuration File.

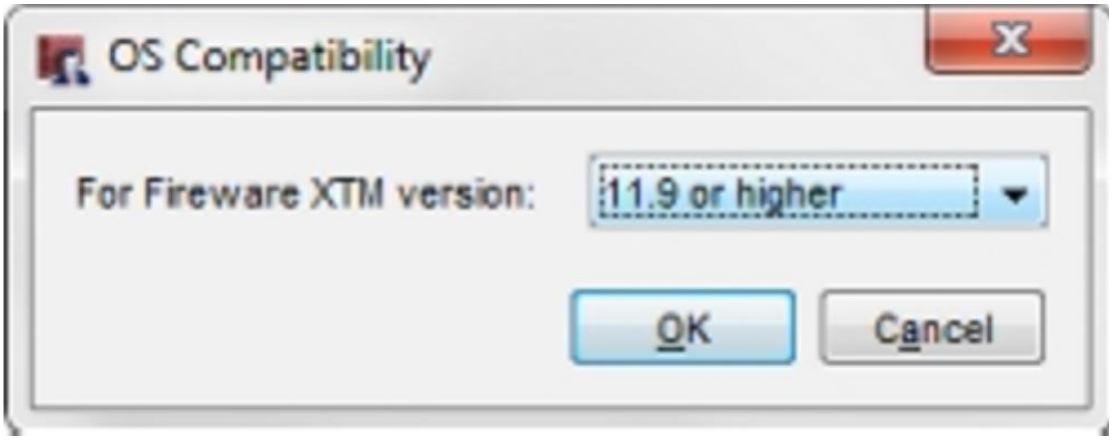
OS Compatibility

Traffic Management Actions operate differently in Fireware XTM v11.9 and higher than in previous versions. Because Policy Manager can manage devices that use different versions of Fireware XTM OS, you must set the OS Compatibility version before you add a Traffic Management Action.

To set the OS compatibility version:

- Select Setup > OS Compatibility.

The OS Compatibility dialog box appears.



- In the For Fireware XTM version text box, select the OS version that the XTM device uses.
- Click OK.

The available Traffic Management configuration options depend on the version of Fireware XTM OS your device uses.

Guarantee Bandwidth

Bandwidth reservations can prevent connection timeouts. A traffic management queue with reserved bandwidth and low priority can give bandwidth to real-time applications with higher priority when necessary without disconnecting. Other traffic management queues can take advantage of unused reserved bandwidth when it becomes available.

The Guaranteed Bandwidth setting in a Traffic Management Action enables you to set a minimum bandwidth that you want to allocate to traffic controlled by the Traffic Management Action.

For example, suppose your company has an FTP server on the external network and you want to guarantee that FTP uploads always get at least 200 Kilobytes per second (Kbps) through the external interface. You might also want to set a guaranteed bandwidth for FTP downloads to make sure that the connection has end-to-end guaranteed bandwidth. To do this, you create a Traffic Management Action that guarantees a minimum of 200 Kbps, and then use this as the Forward action in the FTP policy that handles traffic from the trusted network to the external network. This will allow ftp put at 200 Kbps. If you want to allow ftp get at 200 Kbps, you must configure a second Traffic Management Action that guarantees 200 Kbps and use it as the Reverse action in the FTP policy. To separately guarantee traffic in each direction you must use two different Traffic Management Actions, because if a policy uses the same Traffic Management Action for forward and reverse traffic, the action applies to the combined bandwidth of traffic in both directions.

Restrict Bandwidth

To preserve the bandwidth that is available for other applications, you can restrict the amount of bandwidth for certain traffic types or applications. A bandwidth restriction can discourage the use of certain applications when users find that the speed of the application's performance is significantly degraded.

The Maximum Bandwidth setting in a Traffic Management Action enables you to set a limit on the amount of traffic allowed by the Traffic Management Action.

For example, suppose that you want to allow FTP downloads but you want to limit the speed at which users can download files. You can add a Traffic Management Action that has the Maximum Bandwidth set to a low amount, such as 100 Kbps. Then you can use this as the Reverse Action in the Traffic Management settings in the outbound FTP policy. This can help discourage large FTP downloads when users on the trusted network find the FTP experience is unsatisfactory.

QoS Marking

QoS marking creates different types of service for different kinds of outbound network traffic. When you mark traffic, you change up to six bits on packet header fields defined for this purpose. Other devices can make use of this marking and provide appropriate handling of a packet as it travels from one point to another in a network.

You can enable QoS marking for an individual interface or an individual policy. When you define QoS marking for an interface, each packet that leaves the interface is marked. When you define QoS marking for a policy, all traffic that uses that policy is also marked.

Traffic priority

You can assign different levels of priority either to policies or for traffic on a particular interface. Traffic prioritization at the firewall allows you to manage multiple type of service (ToS) queues and reserve the highest priority for real-time or streaming data. A policy with high priority can take bandwidth away from existing low priority connections when the link is congested so traffic must compete for bandwidth.