How does QoS in Firewall Policy work?

QoS (Quality of Service) in Firewall Policy is a new feature introduced since firmware version 3.3.5 (e.g., VigorPro 5300 series).

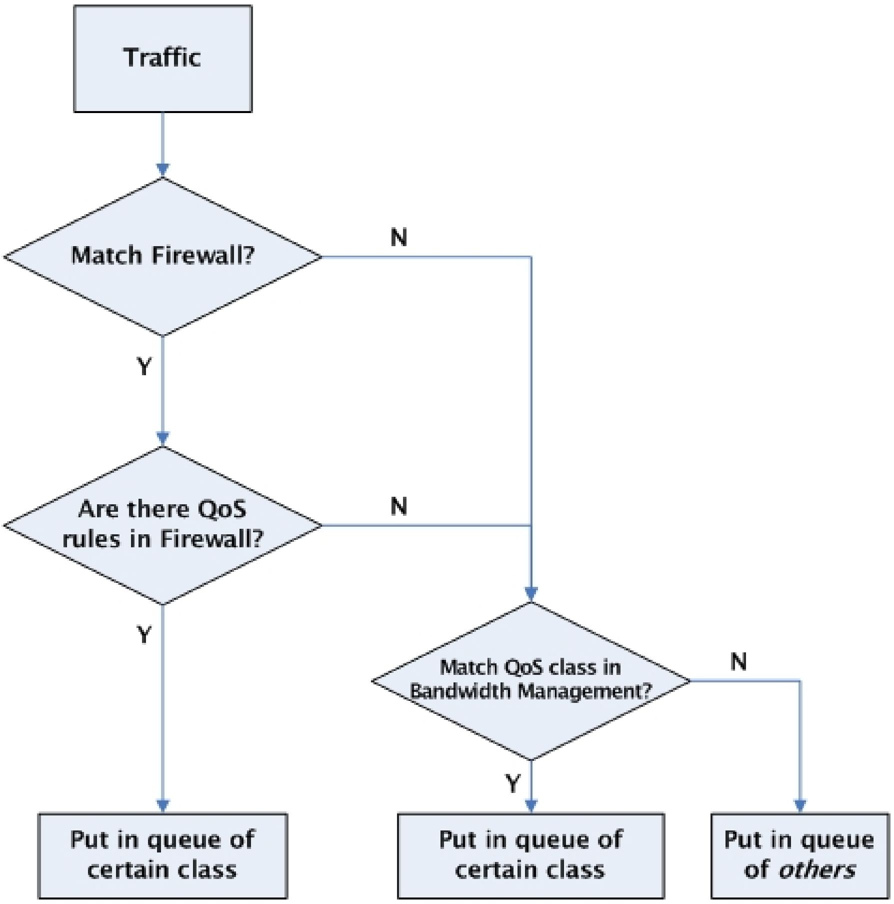
Why QoS in Firewall Policy?

In old versions, all traffic is first checked against Firewall rules. If the traffic is allowed to be passed to the Internet, QoS rules will be checked and used to determine which queue the traffic is placed in. As you can see both QoS rule and Firewall rule can use the Source IP, Destination IP and Destination Port to set a match condition. By combining Firewall rule with QoS rule, the traffic just needs to be checked against a rule once for firewall decision and QoS decision, making packet processing more efficient.

In a firewall rule Source Port can be used to set a match condition which is not supported by a QoS rule. And IP Objects/Groups can be applied to a firewall rule but not a QoS rule. So QoS in Firewall Policy makes a QoS decision more flexible.

How QoS in Firewall Policy works?

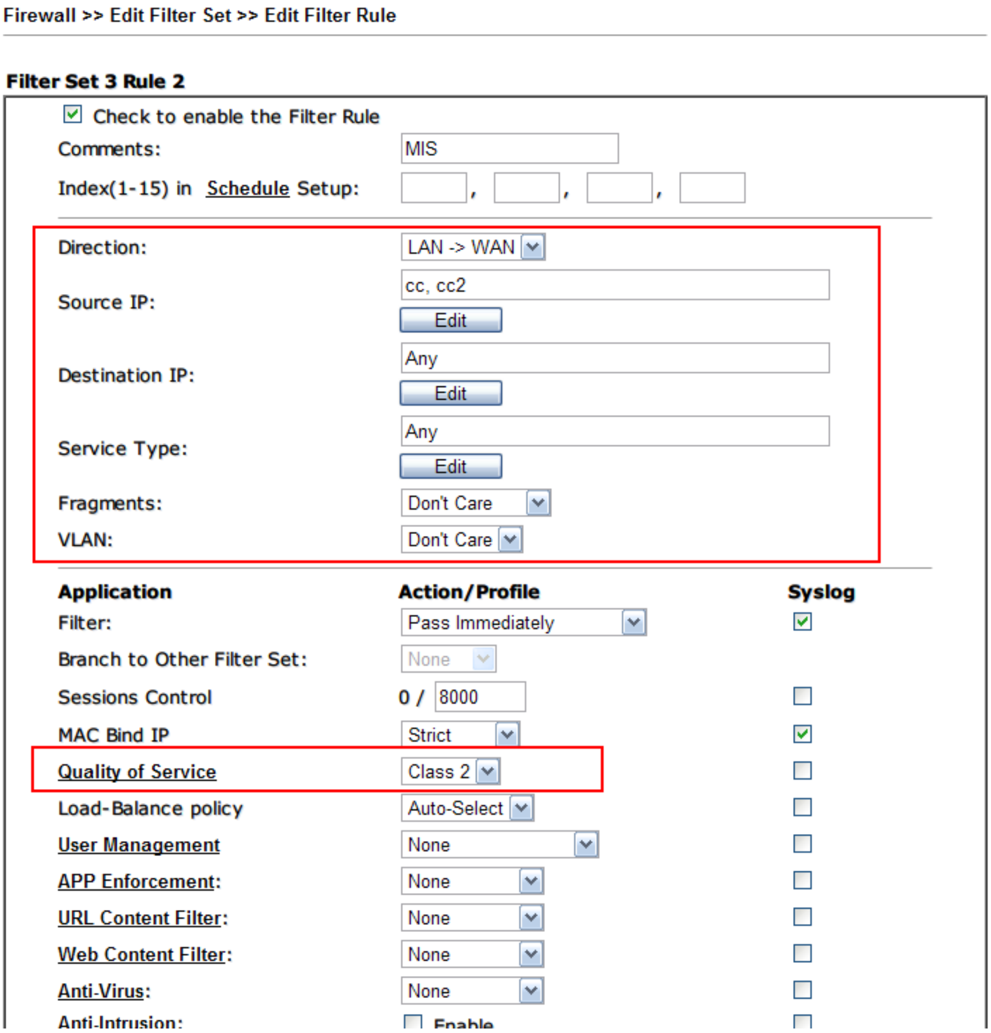
The flow chart below explains how the QoS feature works on VigorPro 5300.


Traffic
Match Firewall?
N
Y
Are there QoS rules in Firewall?
N
Y
Match QoS class in Bandwidth Management?
N
Y
Put in queue of certain class
Put in queue of certain class
Put in queue of *others*

When a packet arrives at the router, the router will check the IP filter to see if the packet matches any IP filter rules (according to Direction, Source IP, Service Type and etc).

Step 1

If the packet matches one of the IP filter rule, the router will put the packet in relevant queue, according to the class specified in Quality of Service in this rule. Like shown in the following picture, if the packet matches this rule, it will be put in to the queue of the QoS Class 2. If the Quality of Service setup is “**None**”, the packet will be further checked against the QoS rules set in the **Bandwidth Management** >> **Quality of Service** page.



Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 3 Rule 2

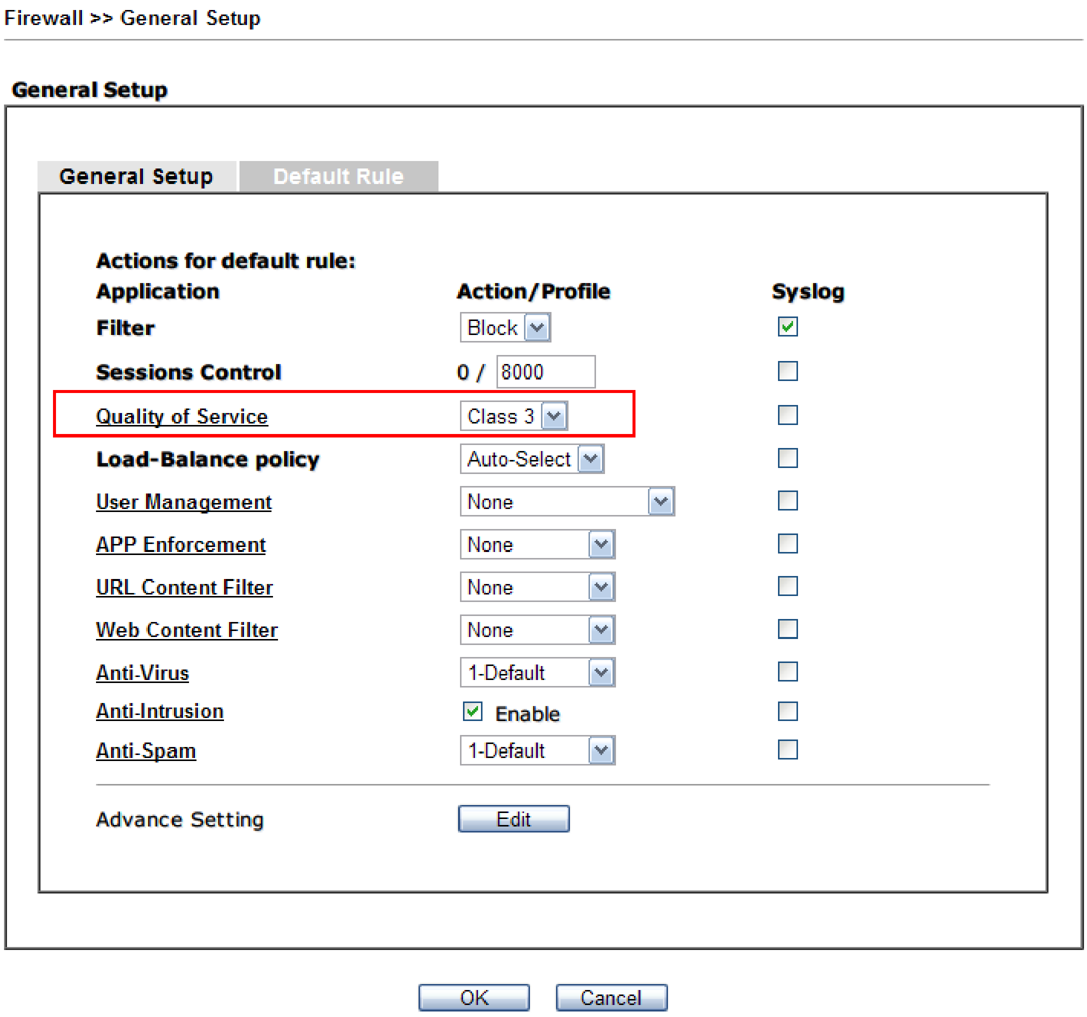
☑ Check to enable the Filter Rule

Comments:	MIS
Index(1-15) in Schedule Setup:	, , ,
Direction:	LAN -> WAN
Source IP:	cc, cc2 Edit
Destination IP:	Any Edit
Service Type:	Any Edit
Fragments:	Don't Care
VLAN:	Don't Care

Application	Action/Profile	Syslog
Filter:	Pass Immediately	☑
Branch to Other Filter Set:	None	
Sessions Control	0 / 8000	☐
MAC Bind IP	Strict	☑
Quality of Service	Class 2	☐
Load-Balance policy	Auto-Select	☐
User Management	None	☐
APP Enforcement:	None	☐
URL Content Filter:	None	☐
Web Content Filter:	None	☐
Anti-Virus:	None	☐
Anti-Intrusion:	☐ Enable	☐

Step 2

Following Step 1, if the packet does not match any of the IP filter rules but the default rule, the router will put the packet in relevant queue according to the Quality of Service setup in **Firewall >> General Setup >> Default Rule** menu. Like shown in the following picture, if the packet matches the default rule, it will be put in to the queue of the QoS Class 3. If the Quality of Service setup is **None**, the packet will be further checked against the QoS rules set in the **Bandwidth Management >> Quality of Service** page.



Firewall >> General Setup

General Setup

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Block	☑
Sessions Control	0 / 8000	□
Quality of Service	Class 3	□
Load-Balance policy	Auto-Select	□
User Management	None	□
APP Enforcement	None	□
URL Content Filter	None	□
Web Content Filter	None	□
Anti-Virus	1-Default	□
Anti-Intrusion	☑ Enable	□
Anti-Spam	1-Default	□

Advance Setting