Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at: (http://supportcontent.checkpoint.com/documentation_download?ID=28418)
To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R77.10 home page (http://supportcontent.checkpoint.com/solutions?id=sk101208).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note: This guide is only for R77.10 and higher</td>
<td></td>
</tr>
<tr>
<td>17 November 2014</td>
<td>Updated rates calculation example (&quot;Example of Rates Calculation&quot; on page 47)</td>
</tr>
<tr>
<td>15 May 2014</td>
<td>Updated information for the asterisk character in Regular Expression Syntax (on page 91)</td>
</tr>
<tr>
<td>01 January 2014</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Quality of Service R77 Versions Administration Guide).
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>2</td>
</tr>
<tr>
<td>Terms</td>
<td>7</td>
</tr>
<tr>
<td><strong>Introduction to QoS</strong></td>
<td>8</td>
</tr>
<tr>
<td>Check Point’s QoS Solution</td>
<td>8</td>
</tr>
<tr>
<td>Features and Benefits</td>
<td>9</td>
</tr>
<tr>
<td>QoS Policy Versus QoS Express Policy</td>
<td>10</td>
</tr>
<tr>
<td>Enabling QoS Acceleration Support</td>
<td>11</td>
</tr>
<tr>
<td>Workflow</td>
<td>12</td>
</tr>
<tr>
<td>QoS Architecture</td>
<td>12</td>
</tr>
<tr>
<td>Basic Architecture</td>
<td>12</td>
</tr>
<tr>
<td>QoS Configuration</td>
<td>14</td>
</tr>
<tr>
<td>Concurrent Sessions</td>
<td>15</td>
</tr>
<tr>
<td>Interaction with VPN</td>
<td>15</td>
</tr>
<tr>
<td>Interoperability</td>
<td>15</td>
</tr>
<tr>
<td><strong>Basic Policy Management</strong></td>
<td>17</td>
</tr>
<tr>
<td>Overview</td>
<td>17</td>
</tr>
<tr>
<td>Rule Base Management</td>
<td>17</td>
</tr>
<tr>
<td>SmartDashboard Toolbar</td>
<td>17</td>
</tr>
<tr>
<td>Overview</td>
<td>18</td>
</tr>
<tr>
<td>Connection Classification</td>
<td>18</td>
</tr>
<tr>
<td>Network Objects</td>
<td>18</td>
</tr>
<tr>
<td>Services and Resources</td>
<td>19</td>
</tr>
<tr>
<td>Time Objects</td>
<td>19</td>
</tr>
<tr>
<td>Bandwidth Allocation and Rules</td>
<td>19</td>
</tr>
<tr>
<td>Default Rule</td>
<td>20</td>
</tr>
<tr>
<td>QoS Action Properties</td>
<td>20</td>
</tr>
<tr>
<td>Example of a Rule Matching VPN Traffic</td>
<td>21</td>
</tr>
<tr>
<td>Bandwidth Allocation and Sub-Rules</td>
<td>21</td>
</tr>
<tr>
<td>Implementing the Rule Base</td>
<td>22</td>
</tr>
<tr>
<td>To Verify and View the QoS Policy</td>
<td>22</td>
</tr>
<tr>
<td>To Install and Enforce the Policy</td>
<td>22</td>
</tr>
<tr>
<td>Uninstalling the QoS Policy</td>
<td>23</td>
</tr>
<tr>
<td>To Monitor the QoS Policy</td>
<td>23</td>
</tr>
<tr>
<td><strong>QoS Tutorial</strong></td>
<td>24</td>
</tr>
<tr>
<td>Introduction</td>
<td>24</td>
</tr>
<tr>
<td>Building and Installing a QoS Policy</td>
<td>25</td>
</tr>
<tr>
<td>Installing Check Point Gateways</td>
<td>25</td>
</tr>
<tr>
<td>Starting SmartDashboard</td>
<td>25</td>
</tr>
<tr>
<td>Defining the Services</td>
<td>26</td>
</tr>
<tr>
<td>Creating a Rule Base</td>
<td>29</td>
</tr>
<tr>
<td>Installing a QoS Policy</td>
<td>34</td>
</tr>
<tr>
<td><strong>Advanced QoS Policy Management</strong></td>
<td>35</td>
</tr>
<tr>
<td>Overview</td>
<td>35</td>
</tr>
<tr>
<td>Examples: Guarantees and Limits</td>
<td>35</td>
</tr>
<tr>
<td>Per Rule Guarantees</td>
<td>35</td>
</tr>
<tr>
<td>Per Connections Guarantees</td>
<td>37</td>
</tr>
<tr>
<td>Limits</td>
<td>37</td>
</tr>
<tr>
<td>Guarantee - Limit Interaction</td>
<td>37</td>
</tr>
<tr>
<td>Differentiated Services (DiffServ)</td>
<td>38</td>
</tr>
<tr>
<td>Overview</td>
<td>38</td>
</tr>
<tr>
<td>DiffServ Markings for IPSec Packets</td>
<td>38</td>
</tr>
<tr>
<td>Interaction Between DiffServ Rules and Other Rules</td>
<td>38</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring QoS Topology</td>
<td>68</td>
</tr>
<tr>
<td>Enabling Log Collection</td>
<td>68</td>
</tr>
<tr>
<td>To Turn on QoS Logging</td>
<td>68</td>
</tr>
<tr>
<td>To Confirm that the Rule is Marked for Logging</td>
<td>68</td>
</tr>
<tr>
<td>To Start SmartView Tracker</td>
<td>69</td>
</tr>
<tr>
<td>SmartView Tracker</td>
<td>70</td>
</tr>
<tr>
<td>Overview of Logging</td>
<td>70</td>
</tr>
<tr>
<td>Examples of Log Events</td>
<td>72</td>
</tr>
<tr>
<td>Connection Reject Log</td>
<td>72</td>
</tr>
<tr>
<td>LLQ Drop Log</td>
<td>72</td>
</tr>
<tr>
<td>Pool Exceeded Log</td>
<td>73</td>
</tr>
<tr>
<td>Examples of Account Statistics Logs</td>
<td>73</td>
</tr>
<tr>
<td>General Statistics Data</td>
<td>73</td>
</tr>
<tr>
<td>Drop Policy Statistics Data</td>
<td>73</td>
</tr>
<tr>
<td>LLQ Statistics Data</td>
<td>74</td>
</tr>
<tr>
<td>Command Line Interface</td>
<td>75</td>
</tr>
<tr>
<td>QoS Commands</td>
<td>75</td>
</tr>
<tr>
<td>Setup</td>
<td>75</td>
</tr>
<tr>
<td>cpstart and cpstop</td>
<td>75</td>
</tr>
<tr>
<td>fgate Menu</td>
<td>76</td>
</tr>
<tr>
<td>Control</td>
<td>76</td>
</tr>
<tr>
<td>fgate</td>
<td>76</td>
</tr>
<tr>
<td>Monitor</td>
<td>77</td>
</tr>
<tr>
<td>fgate stat</td>
<td>77</td>
</tr>
<tr>
<td>Utilities</td>
<td>78</td>
</tr>
<tr>
<td>fgate log</td>
<td>78</td>
</tr>
<tr>
<td>FAQ</td>
<td>79</td>
</tr>
<tr>
<td>QoS Basics</td>
<td>79</td>
</tr>
<tr>
<td>Other Check Point Products - Support and Management</td>
<td>81</td>
</tr>
<tr>
<td>Policy Creation</td>
<td>81</td>
</tr>
<tr>
<td>Fine-tuning QoS Performance</td>
<td>82</td>
</tr>
<tr>
<td>Protocol Support</td>
<td>82</td>
</tr>
<tr>
<td>Installation/Backward Compatibility/Licensing/Versions</td>
<td>83</td>
</tr>
<tr>
<td>How do I?</td>
<td>83</td>
</tr>
<tr>
<td>General Issues</td>
<td>84</td>
</tr>
<tr>
<td>QoS Deployment</td>
<td>85</td>
</tr>
<tr>
<td>Deploying QoS</td>
<td>85</td>
</tr>
<tr>
<td>QoS Topology Restrictions</td>
<td>85</td>
</tr>
<tr>
<td>Sample Bandwidth Allocations</td>
<td>87</td>
</tr>
<tr>
<td>Frame Relay Network</td>
<td>87</td>
</tr>
<tr>
<td>Debug Flags</td>
<td>89</td>
</tr>
<tr>
<td>Error and Debug Codes for QoS</td>
<td>89</td>
</tr>
<tr>
<td>Regular Expressions</td>
<td>91</td>
</tr>
<tr>
<td>Regular Expression Syntax</td>
<td>91</td>
</tr>
<tr>
<td>Using Non-Printable Characters</td>
<td>92</td>
</tr>
<tr>
<td>Using Character Types</td>
<td>92</td>
</tr>
<tr>
<td>Index</td>
<td>93</td>
</tr>
</tbody>
</table>
Terms

**Burstiness**
Data that is transferred or transmitted in short, uneven spurts. LAN traffic is typically bursty. Opposite of streaming data.

**CA**
Certificate Authority. Issues certificates to gateways, users, or computers, to identify itself to connecting entities with Distinguished Name, public key, and sometimes IP address. After certificate validation, entities can send encrypted data using the public keys in the certificates.

**Certificate**
An electronic document that uses a digital signature to bind a cryptographic public key to a specific identity. The identity can be an individual, organization, or software entity. The certificate is used to authenticate one identity to another.

**Citrix MetaFrame**
A client-server software application that enables a client to run a published application on a Citrix server farm from the client's desktop.

**Intelligent Queuing Engine**
A bandwidth allocation algorithm that guarantees high priority traffic takes precedence over low priority traffic.

**Interface**
A boundary across which two systems communicate independently with each other.

**Jitter**
Variation in the delay of received packets. On the sending side, packets are spaced evenly apart and sent in a continuous stream. On the receiving side, the delay between each packet can vary according to network congestion, improper queuing or configuration errors.

**Policy**
A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources through the use of packet inspection.

**QoS**
A policy-based bandwidth management solution.

**QoS Action Properties**
Properties that define bandwidth allocation, limits, and guarantees for a rule.

**RDED**
Retransmit Detect Early Drop. The bottleneck that results from the connection of a LAN to the WAN causes TCP to retransmit packets. RDED prevents inefficiencies by detecting retransmits in TCP streams and preventing the transmission of redundant packets when multiple copies of a packet are concurrently queued on the same flow.

**Rule**
A set of traffic parameters and other conditions that cause specified actions to be taken for a communication session.

**Rule Base**
The database that contains the rules in a security policy and defines the sequence in which they are enforced.

**WFQ**
Weighted Fair Queuing. An algorithm to precisely control bandwidth allocation in QoS.

**WFRED**
Weighted Flow Random Early Drop. A mechanism for managing the packet buffers of QoS. Adjusting automatically and dynamically to the network traffic situation, WFRED remains transparent to the user.
Chapter 1

Introduction to QoS

In This Section:

Check Point's QoS Solution ...................................................................................... 8
QoS Architecture ..................................................................................................... 12
Interaction with VPN ............................................................................................... 15

Important:

• This guide is only for R77.10 and higher.
• For R77, see the R77 Quality of Service Administration Guide

Check Point's QoS Solution

QoS is a policy based bandwidth management solution. QoS lets you:

• Prioritize business-critical traffic, such as ERP, database and Web services traffic, over less time-critical traffic.

• Guarantee bandwidth and control latency for streaming applications, such as Voice over IP (VoIP) and video conferencing.

• Give guaranteed or priority access to specified employees, even if they are remotely accessing network resources.

QoS is deployed with the Security Gateway. QoS is enabled for both encrypted and unencrypted traffic.
QoS leverages the industry's most advanced traffic inspection and bandwidth control technologies. Check Point patented Stateful Inspection technology captures and dynamically updates detailed state information on all network traffic. This state information is used to classify traffic by service or application. After traffic has been classified, QoS applies an innovative, hierarchical, Weighted Fair Queuing (WFQ) algorithm to accurately control bandwidth allocation.

**Features and Benefits**

QoS gives these features and benefits:

- **Flexible QoS policies with weights, limits and guarantees**
  QoS lets you create basic policies that can be modified to include the Advanced QoS features described in this section.

- **Integration with the Security Gateway**
  The integration of an organization's security and bandwidth management policies enables easier policy definition and system configuration. This lets you optimize network performance for VPN and unencrypted traffic.

- **Performance analysis through SmartView Tracker**
  Monitor the performance of your system by means of log entries recorded in SmartView Tracker.

- **Integrated DiffServ support**
  Add one or more Diffserv Classes of Service to the QoS Policy Rule Base.

- **Integrated Low Latency Queuing**
  Define special classes of service for “delay sensitive” applications like voice and video to the QoS Policy Rule Base.

- **Integrated Citrix MetaFrame support**
  Supplies a QoS solution for the Citrix ICA protocol.

- **No need to deploy separate VPN, Firewall and QoS devices**
  QoS and Firewall share a common architecture and many core technology components. User-defined network objects can be used in both solutions.

- **Proactive management of network costs**
  QoS's monitoring systems let you to be proactive in managing your network and controlling network costs.

- **Support for end-to-end QoS for IP networks**
  QoS offers full support for end-to-end QoS for IP networks by distributing enforcement throughout network hardware and software.

- **CoreXL and SecureXL support**
  For packet acceleration.
**QoS Policy Versus QoS Express Policy**

Express mode lets you define a basic policy. Included as a legacy option for backward compatibility, Express mode does not contain most of the features available in the recommended QoS policy option. To use express mode, select the QoS express policy option when creating a new package in File > New > New Policy Package.

This table compares QoS policy features with QoS Express mode policy features.

<table>
<thead>
<tr>
<th>Features</th>
<th>QoS</th>
<th>QoS Express</th>
<th>Find out more...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weights</td>
<td>✓</td>
<td>✓</td>
<td>Weight (on page 19)</td>
</tr>
<tr>
<td>Limits (whole rule)</td>
<td>✓</td>
<td>✓</td>
<td>Limits (on page 20)</td>
</tr>
<tr>
<td>Authenticated QoS</td>
<td>✓*</td>
<td></td>
<td>Authenticated QoS (on page 43)</td>
</tr>
<tr>
<td>Logging</td>
<td>✓</td>
<td>✓</td>
<td>Overview of Logging (on page 70)</td>
</tr>
<tr>
<td>Accounting</td>
<td>✓*</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Support of platforms and HW accelerator</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High Availability and Load Sharing</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Guarantee (Per connection)</td>
<td>✓</td>
<td></td>
<td>Per Connections Guarantees (on page 37)</td>
</tr>
<tr>
<td>Limit (Per connection)</td>
<td>✓</td>
<td></td>
<td>Limits (on page 20)</td>
</tr>
<tr>
<td>LLQ (controlling packet delay in QoS)</td>
<td>✓</td>
<td></td>
<td>Low Latency Queuing (on page 39)</td>
</tr>
<tr>
<td>DiffServ</td>
<td>✓</td>
<td></td>
<td>Differentiated Services (DiffServ) (on page 38)</td>
</tr>
<tr>
<td>Sub-rules</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Matching by URI resources</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Enabling QoS Acceleration Support

After a clean install or upgrade to R77.10, QoS supports SecureXL and CoreXL acceleration technologies. **Important**: After a clean install or upgrade, SecureXL and CoreXL must be manually enabled on the QoS Security Gateway. If the gateway is a member of a cluster, QoS must be manually enabled on all the cluster members.

#### To enable:

a) On the gateway, run:

   cpprod_util CPPROD_SetValue FG1 FgWithAcceleration 1 1 1

b) Use cpconfig to turn on SecureXL/CoreXL.

c) Reboot the gateway.

#### To disable:

a) On the gateway, run: cpconfig to turn off SecureXL and CoreXL.

b) Reboot the gateway.

c) After reboot, run:

   cpprod_util CPPROD_SetValue FG1 FgWithAcceleration 1 0 1

**Note**: If you have a QoS policy created using R77 and below, note that these features are not supported when acceleration is enabled:

- User Authority Server
- IPSO
- Citrix printing rules
- Security Gateways below R77.10
- SmartView Monitor - QoS views do not correctly show traffic accelerated by SecureXL

For more, see the QoS known limitations in the R77.10 Known Limitations (http://supportcontent.checkpoint.com/solutions?id=sk97619).
**Workflow**

This workflow shows the basic and advanced steps that System Administrators do for installation, configuration, and operation.

1. Open SmartDashboard. See Starting SmartDashboard (on page 26).
3. Define the gateway network objects.
4. Enable the QoS blade on the QoS gateway.
5. Configure the basic rules and sub-rules governing the allocation of QoS flows on the network. See Editing QoS Rule Bases (on page 51).
   After the basic rules have been defined, you can configure these advanced features:
   - 5.1 DiffServ Markings. See Working with Differentiated Services (DiffServ) (on page 61).
   - 5.2 Define Low Latency Queuing. See Working with Low Latency Classes (on page 63).
   - 5.3 Define Authenticated QoS. See Working with Authenticated QoS (on page 64).
   - 5.4 Define Citrix ICA Applications. See Managing QoS for Citrix ICA Applications (on page 65).
7. Enable log collection and monitor the system. See Enabling Log Collection (on page 68).

**Using QoS with SmartProvisioning**

For how to activate SmartLSM with QoS, see the R77 SmartProvisioning Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=28419).

**QoS Architecture**

### Basic Architecture

The architecture and flow control of QoS is similar to firewall.

QoS has three components:

- SmartConsole
- Security Management Server
- Gateway

The components can be installed on one machine or in a distributed configuration on a number of machines.

Bandwidth policy is configured using SmartDashboard. On the Security Management Server, the policy is verified and installed on the QoS gateways. The QoS gateway uses:

- The firewall chaining mechanism to receive, process and send packets.
- A proprietary classifying and rule-matching infrastructure to examine a packet.

Logging information is created using the firewall kernel API.
QoS Gateway
The primary role of the QoS blade is to:
- Implement a QoS policy at network access points
- Control the flow of inbound and outbound traffic.
QoS has two components:
- QoS kernel driver
- QoS daemon

QoS Kernel Driver
The kernel driver is the heart of QoS operations. It is in the kernel driver that IP packets are examined, queued, scheduled and released, enabling QoS traffic control abilities.

QoS Daemon (fgd50)
The QoS daemon is a user mode process that:
- Resolves DNS for the kernel (used for Rule Base matching).
- Resolves Authenticated Data for an IP (using UserAuthority - again for Rule Base matching).
- In a Cluster Load Sharing configuration, updates the kernel of changes in the cluster status. For example, if a cluster member goes down. The daemon recalculates the relative loads of the gateways and updates the kernel.

The primary SmartConsole application is SmartDashboard. Use SmartDashboard to create "bandwidth rules" for the QoS policy.

Other SmartConsole clients are the SmartView Tracker, a log entries browser, and SmartView Monitor. SmartView Monitor shows status information about active QoS gateways and their policies.

QoS in SmartDashboard
SmartDashboard is used to create and change the QoS Policy and define the network objects and services. If both VPN and QoS are licensed, they each have a tab in SmartDashboard.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
<th>Time</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site to Site VPN</td>
<td>GW-group</td>
<td>GW-group</td>
<td>CIFS, TFTP</td>
<td>Weight 20</td>
<td>Log</td>
<td>All</td>
<td>Any</td>
<td>Prioritize VPN</td>
</tr>
<tr>
<td>Facebook</td>
<td>Any</td>
<td>Any</td>
<td>http, Facebook</td>
<td>Weight 10</td>
<td>None</td>
<td>All</td>
<td></td>
<td>Work-Hours Prioritize over other</td>
</tr>
<tr>
<td>SSM</td>
<td>PC, LAN</td>
<td>GW-group</td>
<td>ssh, http, https</td>
<td>Weight 50</td>
<td>Log</td>
<td>All</td>
<td>Any</td>
<td>Prioritize SSM connections</td>
</tr>
<tr>
<td>Default</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
<td>None</td>
<td>All</td>
<td>Any</td>
<td></td>
</tr>
</tbody>
</table>

The QoS Policy rules are shown the QoS Rule Base.
**QoS Configuration**

The Security Management Server and the QoS gateway can be installed on the same machine or on two different machines. When they are installed on different machines, the configuration is known as distributed.

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>QoS gateway</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>QoS gateway</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>SmartConsole</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>Security Management Server</td>
<td></td>
</tr>
</tbody>
</table>

The example shows a distributed configuration, in which one Security Management Server (consisting of a Security Management Server and a SmartConsole) controls four QoS gateways. The four QoS gateways manage bandwidth allocation on three QoS enabled lines.

One Security Management Server can control and monitor multiple QoS gateways. The QoS gateway operates independently of the Security Management Server. QoS gateways can operate on more Internet gateways and interdepartmental gateways.
Client-Server Interaction

SmartConsole and the Security Management Server can be installed on the same machine or on two different machines. When they are installed on two different machines, QoS implements the Client/Server model, in which a SmartConsole controls a Security Management Server.

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>London QoS gateway</td>
<td>3</td>
<td>Bridge SmartConsole</td>
</tr>
<tr>
<td>2</td>
<td>Tower Security Management Server</td>
<td>4</td>
<td>Internet</td>
</tr>
</tbody>
</table>

In the configuration depicted in the above figure, the functionality of the Security Management Server is divided between two workstations (Tower and Bridge). The Security Management Server with the database is on Tower. The SmartConsole is on Bridge.

The user, working on Bridge, maintains the QoS Policy and database, which reside on Tower. The QoS gateway on London enforces the QoS Policy on the QoS enabled line.

The Security Management Server is started with the `cpstart` command, and must be running if you wish to use the SmartConsole on one of the client machines.

A SmartConsole can manage the Server only if both the administrator logged into SmartConsole and the computer on which the SmartConsole is running have been authorized to access the Security Management Server. Use `cpconfig` to:

- Add SmartConsole as gui client authorized to access the Security Management Server
- Define administrators for the Security Management Server.

Concurrent Sessions

To prevent more than one administrator from modifying a QoS Policy at the same time, QoS implements a locking mechanism. All but one open policy is 'Read Only'.

Interaction with VPN

Interoperability

QoS and firewall share many core technology components. The same user-defined network objects can be used in both solutions. The integration of an organization's security and bandwidth management policies gives easy policy definition and system configuration. For efficient traffic inspection and enhanced performance, the blades share state table information. The QoS blade and firewall blade let users define bandwidth allocation rules for encrypted and NATed traffic.
Security Management Server

QoS uses the Security Management Server and shares the objects database (network objects, services and resources) with the firewall. Some objects have properties that are product specific. For example, the Firewall has encryption properties which are not related to QoS. A QoS network interface has speed properties that are not related to the firewall.
Chapter 2

Basic Policy Management

In This Section:

Overview .......................................................................................................................... 17
Rule Base Management ................................................................................................. 17
Implementing the Rule Base .......................................................................................... 22

This section covers basic policy management.

Overview

This chapter describes the basic QoS Policy management that is required to enable you to define and implement a working QoS Rule Base. More advanced QoS Policy management features are discussed in Advanced QoS Policy Management (on page 35).

Rule Base Management

SmartDashboard Toolbar

You can use the SmartDashboard toolbar to do these actions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📘</td>
<td>Open the SmartDashboard menu. When instructed to select menu options, click this button to show the menu. For example, if you are instructed to select Manage &gt; Users and Administrators, click this button to open the Manage menu and then select the Users and Administrators option.</td>
</tr>
<tr>
<td>📄</td>
<td>Save current policy and all system objects.</td>
</tr>
<tr>
<td>🔗</td>
<td>Open a policy package, which is a collection of Policies saved together with the same name.</td>
</tr>
<tr>
<td>🔮</td>
<td>Refresh policy from the Security Management Server.</td>
</tr>
<tr>
<td>📁</td>
<td>Open the Database Revision Control window.</td>
</tr>
<tr>
<td>⚙️</td>
<td>Change global properties.</td>
</tr>
<tr>
<td>🐮</td>
<td>Verify Rule Base consistency.</td>
</tr>
<tr>
<td>🔅</td>
<td>Install the policy on Security Gateways or VSX Gateways.</td>
</tr>
</tbody>
</table>
Overview

QoS policy is implemented by defining a set of rules in the Rule Base. The Rule Base specifies what actions are to be taken with the data packets. The Rule Base specifies:

- Source and destination of the traffic
- Services that can be used
- Times
- Logging and logging level

The Rule Base comprises the rules you create and a default rule (see Default Rule (on page 20)). The default rule is automatically created with the Rule Base. It can be modified but cannot be deleted. Unless other rules apply, the default rule is applied to all data packets. The default rule is therefore always the last rule in the Rule Base.

An important aspect of Rule Base management is reviewing SmartView Tracker traffic logs.

QoS works by inspecting packets in a sequential manner. When QoS receives a packet belonging to a connection, it compares it against the first rule in the Rule Base. Then against the second, then the third. When QoS finds a rule that matches, it stops checking and applies that rule.

If the matching rule has sub-rules the packets are then compared against the first sub-rule. Then the second and third and other sub-rules until it finds a match.

If the packet fails to match a rule or sub-rule, the default rule or default sub-rule is applied. The first rule that matches is applied to the packet, not the rule that best matches.

After you have defined your network objects, services and resources, you can use them in building a Rule Base. For instructions on building a Rule Base, see Editing QoS Rules (see “Editing QoS Rule Bases" on page 51).


Note - It is best to organize lists of objects (network objects and services) into groups. Using groups gives you a better overview of your QoS Policy and leads to a more readable Rule Base. New objects added to groups are automatically included in the rules.

Connection Classification

A connection is classified according to four criteria:

- **Source**
  A set of network objects such as specified computers, networks, user groups or domains.

- **Destination**
  A set of network objects such as specified computers, networks, user groups or domains.

- **Service**
  A set of IP services, TCP, UDP, ICMP or URLs.

- **Time**
  Specified days or time periods.

Network Objects

The network objects that can be used in QoS rules include workstations, networks, domains, and groups.

**User Groups**

QoS lets you define Groups of predefined users. For example, all the users in the marketing department can be grouped together in a User Group called Marketing. When defining a rule, you can use this group as the **Source** instead of adding individual users to the **Source** column of the rule.

**Services and Resources**

QoS allows you to define QoS rules, not only based on the source and destination of each communication, but also according to the service requested. The services that can be used in QoS rules include TCP, Compound TCP, UDP, ICMP and Citrix TCP services, IP services.

Resources can also be used in a QoS Rule Base. They must be of type **URI for QoS**.

**Time Objects**

QoS allows you to define Time objects. Time objects are used to specify when a rule is enforced. Time objects can be defined for specified times or days. Days can be divided into days of the month or days of the week.

**Bandwidth Allocation and Rules**

A rule can specify three factors to be applied to bandwidth allocation for classified connections:

**Weight**

Weight is the percentage of the available bandwidth allocated to a rule. This is not the same as the weight in the QoS Rule Base, which is a manually assigned priority.

To calculate what percentage of the bandwidth the connections matched to a rule receives:

\[
\text{The weight} = \frac{\text{Priority in SmartDashboard}}{\text{Total priority of all the rules with open connections}}
\]

For example:

- if this rule's weight (priority in SmartDashboard) is 12
- the total weight (priority in SmartDashboard) of all the rules for which connections are currently open is 120

Then all the connections open under this rule are allocated 12/120, or 10%. The weight of this rule is 10%. The rule gets 10% of the available bandwidth if the rule is active. In practice, if other rules are not using their maximum allocated bandwidth, a rule can get more than the bandwidth allocated by this formula. Unless a per connection limit or guarantee is defined for a rule, all connections under a rule receive equal weight.

Allocating bandwidth according to weights ensures full use of the line even if a specified class is not using all of its bandwidth. In such a case, the left over bandwidth is divided between the remaining classes in accordance with their relative weights. Units are configurable, see Defining QoS Global Properties (on page 49).

**Guarantees**

A guarantee allocates a minimum bandwidth to the connections matched with a rule.

Guarantees can be defined for:

- The sum of all connections in a rule
  A total rule guarantee reserves a minimum bandwidth for all the connections below a rule. The actual bandwidth allocated to each connection depends on the number of open connections that match the
rule. The total bandwidth allocated to the rule cannot be less than the guarantee. The more connections that are open, the less bandwidth each connection receives.

- Individual connections in a rule

A per-connection guarantee means that each connection that matches the specified rule is guaranteed a minimum bandwidth.

**Note**: Although weights guarantee the bandwidth share for specified connections, only a guarantee lets you to specify an absolute bandwidth value.

**Limits**

A limit specifies the maximum bandwidth that is assigned to all the connections together. A limit defines a point after which connections below a rule are not allocated more bandwidth, even if there is surplus bandwidth available.

Limits can also be defined for the sum of all connections in a rule or for individual connections within a rule.

For more information on weights, guarantees and limits, see Action Type (on page 20).

**Note** - Bandwidth allocation is not fixed. As connections are opened and closed, QoS continuously changes the bandwidth allocation to accommodate competing connections, in accordance with the QoS Policy.

**Default Rule**

A default rule is automatically added to each QoS Policy Rule Base, and assigned the weight specified in the QoS page of the Global Properties window. You can change the weight, but you cannot delete the default rule (see Weight (on page 19)).

The default rule applies to all connections not matched by the other rules or sub-rules in the Rule Base.

A default rule is automatically added to each group of sub-rules, and applies to connections not classified by the other sub-rules in the group. For more, see: To Verify and View the QoS Policy (on page 22).

**QoS Action Properties**

In the QoS Action Properties window you can define bandwidth allocation properties, limits and guarantees for a rule.

**Action Type**

Select one of these Action Types:

<table>
<thead>
<tr>
<th>Action Type</th>
<th>QoS Policy</th>
<th>Express Mode Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Simple**

These actions are available:

- Apply rule to encrypted traffic only
- Rule weight
- Rule limit
- Rule guarantee

**Advanced**

The same actions that are available in Simple mode are available in Advanced mode. Advanced mode also has Guarantee Allocation:
Basic Policy Management

- Per rule
- Per connection
- Per rule guarantee
- Per connection guarantee
- Number of permanent connections
- Accept additional connections

**Example of a Rule Matching VPN Traffic**

VPN traffic is traffic that is encrypted in the same gateway by the Security Gateway. VPN traffic does not refer to traffic that was encrypted by a non-Check Point product prior to arriving at this gateway. This type of traffic can be matched using the IPSec service.

When *Apply rule only to encrypted traffic* is selected in the QoS Action Properties window, only VPN traffic is matched to the rule. If this field is not checked, all types of traffic (both VPN and non-VPN) are matched to the rule.

Use the *Apply rule only to encrypted traffic* option to create a Rule Base that applies only to VPN traffic. These actions are different from actions applied to non-VPN traffic. Since QoS uses the First Rule Match concept, the VPN traffic rules must be defined as the top rules in the Rule Base. Below them define rules that apply to all other types of traffic. Other types of traffic skip the top rules and match to one of the non-VPN rules. To separate VPN traffic from non-VPN traffic, define this rule at the top of the QoS Rule Base:

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>VPN Encrypt, and other configured actions</td>
</tr>
</tbody>
</table>

All the VPN traffic is matched to this rule. The rules below this VPN Traffic Rule are then checked only against non-VPN traffic. You can define sub-rules below the VPN Traffic rule that classify the VPN traffic more granularly.

**Bandwidth Allocation and Sub-Rules**

When a connection is matched to a rule with sub-rules, the sub-rules are checked for match. If none of the sub-rules apply, the default rule for the sub-rules is applied (see Default Rule (on page 20)).

Sub-rules can be nested, meaning that sub-rules themselves can have sub-rules. The same rules then apply to the nested sub-rules. If the connection matches a sub-rule that has sub-rules, the nested sub-rules are checked for a match. If none of the nested sub-rules apply, the default rule for the nested sub-rules is applied.

Bandwidth is allocated on a top/down basis. This means that:

- Sub-rules cannot give more bandwidth to a matching rule, than the rule in which the sub-rule is located.
- A nested sub-rule cannot give more bandwidth than the sub-rule in which it is located.

A Rule Guarantee must always be greater than or equal to the Rule Guarantee of a sub-rule in that rule. The same applies to Rule Guarantees in sub-rules and their nested sub-rules.

**Example:**

Bandwidth Allocation in Nested Sub-Rules:
### Basic Policy Management

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule A</td>
<td>Any</td>
<td>Any</td>
<td>ftp</td>
<td>Rule Guarantee - 100KBps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Weight 10</td>
</tr>
<tr>
<td>Start of Sub-Rule A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule A 1</td>
<td>Client-1</td>
<td>Any</td>
<td>ftp</td>
<td>Rule Guarantee - 100KBps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Weight 10</td>
</tr>
<tr>
<td>Start of Sub-Rule A1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule A1.1</td>
<td>Any</td>
<td>Any</td>
<td>ftp</td>
<td>Rule Guarantee - 80KBps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Weight 10</td>
</tr>
<tr>
<td>Rule A1.2</td>
<td>Any</td>
<td>Any</td>
<td>ftp</td>
<td>Weight 10</td>
</tr>
<tr>
<td>End of sub-rule A1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule A2</td>
<td>Client-1</td>
<td>Any</td>
<td>ftp</td>
<td>Weight 10</td>
</tr>
<tr>
<td>End of sub-rule A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule B</td>
<td>Any</td>
<td>Any</td>
<td>http</td>
<td>Weight30</td>
</tr>
</tbody>
</table>

In this example, surplus bandwidth from the application of Rule A1.1 is applied to Rule A2 before it is applied to Rule A1.2.

### Implementing the Rule Base

After defining rules, run an heuristic check (Policy > Verify) on the Rule Base to make sure the rules do not conflict.

After verifying the Rule Base, install the policy on QoS gateways that will enforce it.

- **Note** - Make sure the QoS blade is enabled on the gateway before you install the policy.

### To Verify and View the QoS Policy

1. Select Policy > Verify to run an heuristic check on the Rule Base to make sure that there are no conflicting rules.
2. Select Policy > View to see the generated rules as ASCII text.

### To Install and Enforce the Policy

To install and enforce the QoS Policy:

1. From the Policy menu, select Install.

   The Install Policy window shows.

2. Specify the QoS gateways on which to install the Policy.
   - By default, all QoS gateways are already selected.
   - For an object to be a QoS gateway, it needs to have the QoS blade enabled.
   - The objects in the list are those that have QoS Installed selected in their definition (see Specifying Interface QoS Properties (on page 50)).
   - The QoS Policy is not installed on unselected items.
3. Click OK.

**Uninstalling the QoS Policy**

2. For those gateways that have the QoS blade enabled, select the QoS option.

3. Click OK.

**Note:**
- Uninstalling the policy does not disable the QoS blade. The QoS blade remains active but does not enforce a QoS policy. The earlier policy remains on the gateway.
- The QoS Policy will be installed again if the gateway is rebooted.
- To permanently stop the gateway from enforcing QoS, disable the QoS blade.

**To Monitor the QoS Policy**

SmartView Monitor lets you to monitor traffic through a QoS interface. For more, see the *R77 SmartView Monitor Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=24848).
Chapter 3

QoS Tutorial

In This Section:

Introduction ............................................................................................................. 24
Building and Installing a QoS Policy ....................................................................... 25

Introduction

This chapter presents a step by step guide to building and installing a QoS Policy in QoS. This tutorial is based on an example network configuration.

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Private Localnet</td>
<td>7</td>
<td>HTTP Server</td>
</tr>
<tr>
<td>2</td>
<td>DMZ</td>
<td>8</td>
<td>HTTP Server</td>
</tr>
</tbody>
</table>
This example shows a typical network configuration for an organization with offices located in London, Oxford and Cambridge. The QoS gateway is located in London where the gateway to the Internet will comprise three interfaces. The Security Management Server is located at Oxford while the SmartConsole is installed at Cambridge. Within the private local network there are the Marketing and Engineering departments. In this tutorial you are shown how a QoS policy is implemented to regulate and optimize the flow in Internet traffic to these departments.

## Building and Installing a QoS Policy

Complete these steps to create and install a QoS Policy on the example network.

1. Install these gateways as needed.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Function</th>
<th>Required Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>London</td>
<td>QoS Gateway</td>
<td>QoS Gateway</td>
</tr>
<tr>
<td></td>
<td>gateway to the Internet</td>
<td>Security Gateway (required)</td>
</tr>
<tr>
<td>Cambridge</td>
<td>SmartConsole</td>
<td>Security Gateway</td>
</tr>
</tbody>
</table>

2. Open **SmartDashboard > QoS** tab.
3. Decide on the type of QoS Policy to implement:
   - QoS
   - Express mode
4. Define the network objects to be used in the Rule Base.
   Define only those objects that are explicitly used in the Rule Base. You do not have to define all of the network.
5. Define proprietary services used on the network.
   You do not have to define the commonly used services. These are already defined for you in QoS. In most cases you need only specify a name for network objects and services. QoS obtains the object's properties from the applicable databases (DNS, YP hosts file).
6. Create the QoS Rule Base that make up the Policy.

These steps are described in the sections that follow.

## Installing Check Point Gateways


Install QoS in this sequence:

1. Install QoS and Firewall on London.
2. Install SmartConsole on Cambridge.
5. On Oxford, define the administrators who will be allowed to manage the QoS Policy.

**Starting SmartDashboard**

This section describes how to start SmartDashboard and access the QoS tab.

**To Start SmartDashboard**

1. From the **Start** menu, select **Programs > Check Point SmartConsole R77.10 > SmartDashboard**. The **Welcome to Check Point SmartDashboard** window shows.

2. Log in using one of these authentication methods:
   - User Name and Password
   - Certificate

3. Enter the name of the Security Management Server as:
   - A DNS resolvable name
   - An IP address
   Select **Read Only** if you do not wish to change the policy.
   - Optionally add a session description explaining why you are changing the security policy. This text shows as a log entry in SmartView Tracker (Audit mode) in the **Session Description** column.

   **Note:** If the **Session Description** column does not show in SmartView Tracker, use the **Query Properties** pane to display it. For more on SmartView Tracker, see the **R77 SmartView Tracker Administration Guide** (http://supportcontent.checkpoint.com/documentation_download?ID=24847).

4. Click **Login**. SmartDashboard opens.

5. Click the **QoS** tab to show the QoS Rule Base.

**Determining QoS Policy**

To implement a good QoS Policy, find out how the network is used. Identify and prioritize the types of traffic. Identify users and their needs. For example:

- HTTP traffic must be allocated more bandwidth than RealAudio.
- Marketing must be allocated more bandwidth than Engineering.

You will create the rules to implement this policy in Creating a Rule Base (on page 29).

**Defining the Network Objects**

Define these Network Objects:

- London, the gateway on which the QoS gateway is running
- Sub-networks for the Marketing and Engineering departments

As an example, this step shows how to define the London gateway.

<table>
<thead>
<tr>
<th>From the...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| **Manage** menu | 1. From the **Manage** menu, choose **Network Objects**. The **Network Objects** window opens.  
2. Click **New** and choose **Check Point > Gateway** from the menu. The **Check Point Gateway - General Properties** window opens. |
| **Objects** toolbar | 1. If the **Objects** toolbar is not visible, then, from the **View** menu choose **Toolbars > Objects** to display it.  
2. Select from the toolbar. The **Network Objects** window opens.  
3. Click **New** and choose **Check Point > Gateway** from the menu. The Check Point Gateway - **General Properties** window opens. |
<table>
<thead>
<tr>
<th>From the...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Network Objects tree | 1. Right click Network Objects in the Network Objects tree and choose New > Check Point > Gateway from the menu. The Check Point Gateway - General Properties window opens.  
2. In the Check Point Gateway - General Properties window enter the information shown in the next table below to define London’s gateway. |

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>London</td>
<td>This is the name by which the object is known on the network; the response to the hostname command.</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.32.32.32</td>
<td>This is the interface associated with the host name in the DNS — get this by clicking Get Address. For gateways, this should always be the IP address of the external interface.</td>
</tr>
<tr>
<td>Comment</td>
<td>QoS gateway</td>
<td>This is the text that is displayed at the bottom of the Network Objects window when this object is selected.</td>
</tr>
<tr>
<td>Check Point Products</td>
<td>Select the Version from the drop-down list.</td>
<td>These settings specify the Check Point products installed on London, and their version number. Note that if multiple Check Point products are installed on a machine, they must all be the same version number.</td>
</tr>
<tr>
<td>SIC</td>
<td></td>
<td>Establishes a secure communication channel between Check Point gateways.</td>
</tr>
</tbody>
</table>

**London’s Check Point Gateway - General Properties Window**

**Defining Interfaces on the Gateway**

1. Click Topology in the tree on the left side of the Check Point Gateway - London window. The Topology page Check Point Gateway - London window opens.

2. Configure the interfaces according to the data in these tables:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>le0</td>
<td></td>
</tr>
<tr>
<td>Net Address</td>
<td>192.32.32.32</td>
<td></td>
</tr>
<tr>
<td>Net Mask</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Topology tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topology</td>
<td>Check External (leads out to the Internet).</td>
<td>Specifies to which network this interface leads.</td>
</tr>
<tr>
<td>Anti-Spoofing</td>
<td>Check Perform Anti-Spoofing based on network topology.</td>
<td>Specifies that each incoming packet will be examined to ensure that its source IP address is consistent with the interface through which it entered the machine.</td>
</tr>
</tbody>
</table>
### Field Values — Interface Properties Window — le1

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spoof Tracking</strong></td>
<td>Check Log.</td>
<td>Specifies that when spoofing is detected, the event will be logged.</td>
</tr>
</tbody>
</table>

### Field Values — Interface Properties Window — le2

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spoof Tracking</strong></td>
<td>Check Log.</td>
<td>Specifies that when spoofing is detected, the event will be logged.</td>
</tr>
</tbody>
</table>
### QoS Tutorial

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Spoofing</td>
<td>Check <strong>Perform Anti-Spoofing based on network topology.</strong></td>
<td>Specifies that each incoming packet will be examined to ensure that its source IP address is consistent with the interface through which it entered the machine.</td>
</tr>
<tr>
<td>Spoof Tracking</td>
<td>Check Log.</td>
<td>Specifies that when spoofing is detected, the event will be logged.</td>
</tr>
</tbody>
</table>

After the three interfaces have been defined, they are listed in the **Check Point Gateway - London - Topology** window.

1. Click **OK**.

**Define the QoS Properties for the Interfaces**

1. In the **Check Point Gateway - London - Topology** window, double-click London's external interface (le0), or select it and click **Edit**.
   
   The **Interface Properties** window opens.
2. Click the **QoS** tab.
   
   The **Interface Properties - QoS** tab opens.
3. Select **Inbound Active** and **Outbound Active**.
4. From the **Rate** list set both rates to **192000 - T1 (1.5 Mbps)**.
5. Click **OK**.
   
   To exit the **Interface Properties** window.
6. Click **OK**.
   
   To exit the **Check Point Gateway - London - Topology** window.

**Defining the Services**

The QoS Policy required for this tutorial does not require the definition of new proprietary services. The commonly used services HTTP and RealAudio are already defined in QoS.

**Creating a Rule Base**

After defining your network objects and services, create the Rule Base that makes up the QoS policy. When you start SmartDashboard, the last Policy Package is shown. The Policy Package represents the Rule Bases of all the tabs that are shown in SmartDashboard.

This tutorial is concerned with the QoS Rule Base which is opened when you select the QoS tab. In this step, you create a new QoS Policy Package. After you have created the Policy Package, you must add the rules that will enforce the QoS Policy decided in Determining QoS Policy (on page 26).

The new QoS Rule Base is created with a Default Rule (see Default Rule (on page 20)).

**To Create a New Policy Package**

1. In **SmartDashboard** select **New** from the **File** menu.
   
   The **New Policy Package** window opens.
2. Enter the name in the **New policy Package Name** field.
3. Select **QoS**.
4. Select **QoS policy (recommended)**.
5. Click **OK**.
   
   The new **Policy Package** is created together with a **Default Rule** and is displayed in the **QoS** tab.

**To Create New Rules**

This procedure describes how to create the two new rules required to enforce the Rule Base. Create two rules: **Web Rule** and **RealAudio Rule**.

1. Click the **QoS** tab to access the QoS Rule Base.
2. Right-click in the **Name** field of the **QoS** tab and select **Add Rule above** from the menu that is displayed. The **Rule Name** window is displayed.

3. Enter **Web Rule** as the **Rule Name**.

4. Click **OK**.
   
The rule is added to the Rule Base.

5. Create a new rule with the name of **RealAudio Rule**.
   
The **QoS** tab in SmartDashboard lists all the rules in the Rule Base.

**Rule Properties**

A new rule has the default values assigned by the administrator. The next procedure describes how to change these rules to the values shown in the table below.

**Changing Rules Default Values**

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Rule</td>
<td>Any</td>
<td>Any</td>
<td>HTTP</td>
<td>Weight 35</td>
</tr>
<tr>
<td>RealAudio Rule</td>
<td>Any</td>
<td>Any</td>
<td>RealAudio</td>
<td>Weight 5</td>
</tr>
<tr>
<td>Default</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
</tr>
</tbody>
</table>

**To Modify New Rules**

1. In the **QoS** tab, right-click in the **Service** field of the Web Rule.
2. Select **Add Objects** from the menu.
   
The **Add Object** window opens.
3. Select **HTTP** from the list.
4. Click **OK**.
5. Right-click in the **Action** field of the Web Rule.
6. Select **Edit Properties** from the menu.
   
The **QoS Action Properties** window opens.
7. Change the **Rule Weight** to 35.
8. Click **OK**.

**Classifying Traffic by Service**

Usually, a full Rule Base will not explicitly define rules for all the "background" services (such as DNS and ARP). Background services are handled by the **Default** rule.

The structure of the Rule Base is shown at the left of the window as a tree, with the **Default Rule** at the bottom. (For a description of the Rule Base window, see Basic Policy Management (on page 17)).

Connections receive bandwidth according to the weights (priority) assigned to the rules that apply to them. The table below describes what occurs when there are four active connections. Note that bandwidth allocation is constantly changing.

**Service Rules - Four Active Connections**

<table>
<thead>
<tr>
<th>Connections</th>
<th>Relevant rule</th>
<th>Bandwidth</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Web Rule</td>
<td>70%</td>
<td>35 / 50 (the total weights)</td>
</tr>
<tr>
<td>RealAudio</td>
<td>RealAudio Rule</td>
<td>10%</td>
<td>5 / 50</td>
</tr>
<tr>
<td>FTP</td>
<td>Default</td>
<td>sharing 20%</td>
<td>10 /50; a rule applies to all the connections together</td>
</tr>
<tr>
<td>TELNET</td>
<td>Default</td>
<td>sharing 20%</td>
<td>10 /50; a rule applies to all the connections together</td>
</tr>
</tbody>
</table>
Bandwidth is allocated between connections according to relative weight. As connections are opened and closed, QoS changes the bandwidth allocation according to the QoS Policy.

For example:

- If the HTTP, FTP and TELNET connections are all closed. The only remaining connection is the RealAudio connection. RealAudio receives 100% of the bandwidth.

- If the TELNET and FTP connections are closed, both HTTP and RealAudio benefit from the released bandwidth.

### Service Rules - Two Active Connections

<table>
<thead>
<tr>
<th>Connections</th>
<th>Relevant rule</th>
<th>Bandwidth</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Web Rule</td>
<td>87/5%</td>
<td>35 / 40 (the total weights)</td>
</tr>
<tr>
<td>RealAudio</td>
<td>RealAudio Rule</td>
<td>12.5%</td>
<td>5 / 40</td>
</tr>
</tbody>
</table>

Although RealAudio is assigned a very small weight compared to HTTP, it will not be starved of bandwidth no matter how heavy the HTTP traffic.

In practice, you will probably want to give a high relative weight to interactive services such as TELNET, which transfers small amounts of data but involves users issuing commands.

### Classifying Traffic by Source

The second part of the QoS Policy (Marketing must be allocated more bandwidth than Engineering (see "Determining QoS Policy" on page 26)) is implemented by these rules:

**Marketing is Allocated More Bandwidth Than Engineering**

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing Rule</td>
<td>Marketing</td>
<td>Any</td>
<td>Any</td>
<td>Weight 30</td>
</tr>
<tr>
<td>Engineering Rule</td>
<td>Engineering</td>
<td>Any</td>
<td>Any</td>
<td>Weight 20</td>
</tr>
<tr>
<td>Default</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
</tr>
</tbody>
</table>

Using the same principles described in To Create a New Rules (see "To Create New Rules" on page 29) and To Modify New Rules (on page 30), create new rules in SmartDashboard and change them to match the values shown in the table above. The effect of these rules is equivalent to the rules shown here:

<table>
<thead>
<tr>
<th>Connections</th>
<th>Relevant rule</th>
<th>Bandwidth</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Web Rule</td>
<td>70%</td>
<td>35 / 50 (the total weights)</td>
</tr>
<tr>
<td>RealAudio</td>
<td>RealAudio Rule</td>
<td>10%</td>
<td>5 / 50</td>
</tr>
<tr>
<td>FTP</td>
<td>Default</td>
<td>sharing 20%</td>
<td>10 /50</td>
</tr>
<tr>
<td>TELNET</td>
<td>Default</td>
<td>sharing 20%</td>
<td>10 /50</td>
</tr>
</tbody>
</table>

Except for:

- the different weights
- the fact that allocation is based on source rather than on services

### Classifying Traffic by Service and Source

The table below shows all the rules in one Rule Base.

**All the Rules Together**
In this Rule Base, bandwidth allocation is based both on sub-networks and on services.

**First Rule Match Principle**

In the Rule Base shown below:

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Rule</td>
<td>Any</td>
<td>Any</td>
<td>HTTP</td>
<td>Weight 35</td>
</tr>
<tr>
<td>RealAudio Rule</td>
<td>Any</td>
<td>Any</td>
<td>RealAudio</td>
<td>Weight 5</td>
</tr>
<tr>
<td>Marketing Rule</td>
<td>Marketing</td>
<td>Any</td>
<td>Any</td>
<td>Weight 30</td>
</tr>
<tr>
<td>Engineering Rule</td>
<td>Engineering</td>
<td>Any</td>
<td>Any</td>
<td>Weight 20</td>
</tr>
<tr>
<td>Default</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
</tr>
</tbody>
</table>

In a production environment, a connection can match more than one rule. QoS works according to a first rule match principle. Each connection is examined against the QoS Policy and receives bandwidth according to the Action defined in the first rule that is matched.

If a user in Marketing initiates an HTTP connection, the connection matches the Web Rule and the Marketing Rule. The Web Rule comes before the Marketing Rule in the Rule Base, so the connection is matched to the Web Rule and given a weight of 35.

To differentiate HTTP traffic by source, create sub-rules for the Web Rule. See Sub-Rules (on page 33).

**Guarantees and Limits**

Bandwidth allocation can also be defined using guarantees and limits. You can define guarantees and limits for rules or for individual connections in a rule.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Rule</td>
<td>Any</td>
<td>Any</td>
<td>HTTP</td>
<td>Weight 35</td>
</tr>
<tr>
<td>RealAudio Rule</td>
<td>Any</td>
<td>Any</td>
<td>RealAudio</td>
<td>Weight 5</td>
</tr>
<tr>
<td>Marketing Rule</td>
<td>Marketing</td>
<td>Any</td>
<td>Any</td>
<td>Weight 30</td>
</tr>
<tr>
<td>Engineering Rule</td>
<td>Engineering</td>
<td>Any</td>
<td>Any</td>
<td>Weight 20</td>
</tr>
<tr>
<td>Default</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
</tr>
</tbody>
</table>

The Web Rule shown in the Rule Base allocates 35% of available bandwidth to all the HTTP connections combined. The actual bandwidth allocated to connections that match this rule depends on:

- Total available bandwidth
- Open connections that match other rules
Note: 35% of available bandwidth (specified in the example above) is assured to Web Rule. Web Rule will get more bandwidth if there are fewer connections matched to other rules, but never less than 35%.

As an alternative to relative weights, a guarantee can be used to specify bandwidth as an absolute value (in Bytes per second). In this table, Web Rule is guaranteed 20 KBps:

Guarantee Example

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Rule</td>
<td>Any</td>
<td>Any</td>
<td>HTTP</td>
<td>Guarantee 20 KBps, Weight 35</td>
</tr>
<tr>
<td>RealAudio Rule</td>
<td>Any</td>
<td>Any</td>
<td>RealAudio</td>
<td>Weight 5</td>
</tr>
<tr>
<td>Marketing Rule</td>
<td>Marketing</td>
<td>Any</td>
<td>Any</td>
<td>Weight 30</td>
</tr>
<tr>
<td>Engineering Rule</td>
<td>Engineering</td>
<td>Any</td>
<td>Any</td>
<td>Weight 20</td>
</tr>
<tr>
<td>Default</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
</tr>
</tbody>
</table>

Connections matched to Web Rule will receive a total bandwidth of 20 KBps. Remaining bandwidth will be allocated to all the rules, Web Rule included, according to their weights.

For more on guarantees and limits, see Examples: Guarantees and Limits (on page 35) and Bandwidth Allocation and Rules (on page 19).

Sub-Rules

Sub-rules are rules nested in a rule. For example, you can create a sub-rule that allocates more bandwidth to HTTP connections that originate in Marketing. Connections whose Source is marketing receive more bandwidth than other HTTP traffic. In this example, the marketing sub-rule and default sub-rule is below the Web Rule:

Defining Sub-Rules

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Rule</td>
<td>Any</td>
<td>Any</td>
<td></td>
<td>Weight 20</td>
</tr>
</tbody>
</table>

Start of Sub-Rule

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing HTTP</td>
<td>Marketing</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
</tr>
<tr>
<td>Default</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Weight 1</td>
</tr>
</tbody>
</table>

End of Sub-Rule

Bandwidth is allocated to Web Rule according to its weight (20). This weight is divided between its sub-rules in a 10:1 ratio. Connections below Web Rule are allocated bandwidth according to the weights specified:

- 10 for HTTP traffic from the Marketing department
- 1 for everything else.

Note:

- There are two Default rules: one for the Rule Base and one for the Web Rule sub-rule.
- The Source, Destination and Service fields of the sub-rule must always be a "sub-set" of the parent rule.

To create a sub-rule:

1. Right-click in the Name field of the rule in which you want to create the sub-rule.
2. Select Add Sub-Rule.
Installing a QoS Policy

After you have defined the Rule Base, you can install the QoS Policy on the QoS gateways by selecting Install from the Policy menu.

The Install Policy window is displayed, showing a list of gateways defined as QoS gateways (see Defining the Network Objects (on page 26)).

Select the QoS gateways on which to install the QoS Policy. QoS will enforce the QoS Policy on the directions specified in the interface properties of each selected gateway.

For more, see Implementing the Rule Base (on page 22).
Chapter 4

Advanced QoS Policy Management

In This Section:

- Overview ................................................................................................................. 35
- Examples: Guarantees and Limits .......................................................................... 35
- Differentiated Services (DiffServ) ............................................................................ 38
- Low Latency Queuing ............................................................................................. 39
- Authenticated QoS .................................................................................................. 43
- Citrix MetaFrame Support ....................................................................................... 43
- Load Sharing ........................................................................................................... 44

Overview

This chapter covers more advanced QoS Policy management procedures that let you to refine the basic QoS Policies described in Basic Policy Management (on page 17).

Examples: Guarantees and Limits

The QoS Action properties defined in the rules and sub-rules of a QoS Policy Rule Base decide bandwidth allocation.

The guidelines and examples in the sections that follow show how to use effectively guarantees and limits.

Per Rule Guarantees

- The bandwidth allocated to the rule equals the guaranteed bandwidth plus the bandwidth allocated to the rule because of its weight. To uphold the guarantee, the guaranteed bandwidth is subtracted from the total bandwidth and set aside. The remaining bandwidth is then distributed according to the weights specified by all the rules.

The bandwidth guaranteed to a rule is the guaranteed bandwidth plus the rule's share of bandwidth according to weight.

Total Rule Guarantees

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule A</td>
<td>Any</td>
<td>Any</td>
<td>ftp</td>
<td>Rule Guarantee - 100KBps Weight 10</td>
</tr>
<tr>
<td>Rule B</td>
<td>Any</td>
<td>Any</td>
<td>http</td>
<td>Weight 20</td>
</tr>
</tbody>
</table>

- The link capacity is 190KBps.
- In this example, Rule A receives 130KBps, 100KBps from the guarantee, plus (10/30) * (190-100).
- Rule B receives 60KBps, which is (20/30) x (190-100).
- If a guarantee is defined in a sub-rule, then a guarantee must be defined for the rule above it. The guarantee of the sub-rule can also not be greater than the guarantee of the rule above it.

Guarantee is Defined in Sub-rule A1, But Not in Rule A Making the Rule Incorrect
### Advanced QoS Policy Management

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule A | Any | Any | ftp | Weight 10

### Start of Sub-Rule

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule A1 | Client-1 | Any | ftp | Rule Guarantee - 100KBps
|   |   |   | Weight 10 |   

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule A2 | Client-2 | Any | ftp | Weight 10

### End of Sub-Rule

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule B | Any | Any | http | Weight 30

---

This Rule Base is not correct. The guarantee is defined in sub-rule A1, but not in Rule A. To correct this, add a guarantee of 100KBps or more to Rule A.

- A rule guarantee must not be smaller than the sum of guarantees defined in its sub-rules.

### Example of an Incorrect Rule Base

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule A | Any | Any | ftp | Rule Guarantee - 100KBps
|   |   |   | Weight 10 |   

### Start of Sub-Rule

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule A1 | Client-1 | Any | ftp | Rule Guarantee - 80KBps
|   |   |   | Weight 10 |   

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule A2 | Client-2 | Any | ftp | Rule Guarantee - 80KBps
|   |   |   | Weight 10 |   

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule A3 | Client-3 | Any | ftp | Weight 10

### End of Sub-Rule

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule B | Any | Any | http | Weight 30

This Rule Base is incorrect. The sum of guarantees in Sub-Rules A1 and A2 is (80 + 80) = 160, which is greater than the guarantee defined in Rule A (100KBps). To correct this, define a guarantee not smaller than 160KBps in Rule A, or decrease the guarantees defined in A1 and A2.

- If a rule's weight is low, connections that match the rule might receive little bandwidth.

### If a Rule's Weight is Low, Some Connections Might Receive Little Bandwidth

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule A | Any | Any | ftp | Rule Guarantee - 100KBps
|   |   |   | Weight 1 |   

### Start of Sub-Rule

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule A1 | Client-1 | Any | ftp | Rule Guarantee - 100KBps
|   |   |   | Weight 10 |   

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule A2 | Client-2 | Any | ftp | Weight 10

### End of Sub-Rule

**Rule** | **Source** | **Destination** | **Service** | **Action**
--- | --- | --- | --- | ---
Rule B | Any | Any | http | Weight 30

The link capacity is 190KBps.
Rule A is entitled to 103KBps, which are the 100KBps guaranteed, plus \((190-100) \times \left(\frac{1}{31}\right)\). FTP traffic classified to Sub-Rule A1 receives the guaranteed 100KBps which is almost all the bandwidth to which Rule A is entitled. All connections classified to Sub-Rule A2 together receive only 1.5KBps, which is half of the remaining 3KBps.

- The sum of guarantees in rules in the top level must not be more than 90% of the capacity of the link.
- The guarantee rule reserves the bandwidth only if a connection matches the guarantee rule. If no connection matches the guarantee rule, the bandwidth is not reserved.
- When the connection speed is less than the bandwidth guarantee, the guarantee rule makes unused bandwidth available to other connections.
  For example, if the guarantee is 5MB and the connection speed is 3MB. The unused 2MB reserved by the rule is made available for other connections.

**Per Connections Guarantees**

1. If the **Accept additional connections** is checked, connections exceeding the number defined in the **Number of guaranteed connections** are opened. If the field adjacent to **Accept additional connections** is empty, additional connections receive bandwidth allocated according to the defined **Rule Weight**.

2. You can define **Per connection guarantees** for a rule and for its sub-rule. The **Per connection guarantee** of the sub-rule must not be greater than the **Per connection guarantee** of the rule.
   When such a Rule Base is defined, a connection classified to the sub-rule receives the **Per connection guarantee** that is defined in the sub-rule. If a sub-rule does not have a **Per connection guarantee**, it still receives the **Per connection guarantee** defined in the parent rule.

**Limits**

A rule can have both a **Rule limit** and a **Per connection limit**. But the **Per connection Limit** must not be greater than the **Rule Limit**.

If a limit is defined in a rule with sub-rules, and limits are defined for all the sub-rules, the rule limit has a restriction. **The rule limit must not be greater than the sum of limits defined in the sub-rules.** It is not possible to give more bandwidth to a rule than the bandwidth determined by the sum of the limits of its sub-rules.

**Guarantee - Limit Interaction**

- If a **Rule Limit** and a **Guarantee per rule** are defined in a rule, the limit must not be less than the guarantee.
- If both a Limit and a Guarantee are defined in a rule, and the Limit is equal to the Guarantee, connections might not receive bandwidth.

**Example:**

No Bandwidth Received:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule A</td>
<td>Any</td>
<td>Any</td>
<td>ftp</td>
<td>Rule Guarantee — 100KBps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Rule Limit 100KBps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Weight 10</td>
</tr>
<tr>
<td>Start of Sub-Rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule A1</td>
<td>Client-1</td>
<td>Any</td>
<td>ftp</td>
<td>Rule Guarantee - 100KBps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Weight 10</td>
</tr>
<tr>
<td>Rule A2</td>
<td>Client-2</td>
<td>Any</td>
<td>ftp</td>
<td>Rule Guarantee - 80KBps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Weight 10</td>
</tr>
</tbody>
</table>
Advanced QoS Policy Management

<table>
<thead>
<tr>
<th>Rule</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>End of Sub-Rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Rule B | Any | Any | http | Weight 30

The Guarantee in sub-rule A1 equals the Guarantee in rule A (100KBps). When there is sufficient traffic on A1 to use the full Guarantee, traffic on A2 does not receive bandwidth from A. (There is a limit on A of 100KBps).

In this example:

- A rule has both a guarantee and a limit, such that the limit equals the guarantee.
- The rule has sub-rules with Total Rule Guarantees that add up to the Total Rule Guarantee for the rule.
- The rule also has sub-rule(s) with no guarantee.

In such a case, the traffic from the sub-rule(s) with no guarantee might receive little or no bandwidth.

**Differentiated Services (DiffServ)**

**Overview**

DiffServ is an architecture for giving different types or levels of service for network traffic.

When on the enterprise network, packets are marked in the IP header TOS byte as belonging to some Class of Service (QoS Class). When outside on the public network, these packets are granted priority according to their class.

DiffServ markings have meaning on the public network, not on the enterprise network. Good implementation of DiffServ requires that packet markings be recognized on all public network segments.

**DiffServ Markings for IPSec Packets**

When DiffServ markings are used for IPSec packets, the DiffServ mark can be copied between headers by setting these properties in: `$FWDIR/conf/objects_5_0.c`.

- `:ipsec.copy_TOS_to_inner`
  The DiffServ mark is copied from the IPSec header to the IP header of the packet after decapsulation/decryption.
- `:ipsec.copy_TOS_to_outer`
  The DiffServ mark is copied from the packet's IP header to the IPSec header of the encrypted packet after encapsulation.

The default setting are:

- `:ipsec.copy_TOS_to_inner (false)`
- `:ipsec.copy_TOS_to_outer (true)`

**Interaction Between DiffServ Rules and Other Rules**

Just like QoS Policy Rules, a DiffServ rule specifies not only a QoS Class, but also a weight. These weights are enforced only on the interfaces on which the rules of this class are installed.

For example, if a DiffServ rule specifies a weight of 50 for FTP connections. That rule is installed only on the interfaces for which the QoS Class is defined. On other interfaces, the rule is not installed. FTP connections routed through the other interfaces do not get the weight specified by the rule. To specify a weight for all FTP connections, add a rule below "Best Effort."

DiffServ rules can be installed only on interfaces for which the related QoS Class has been defined. QoS class is defined on the QoS tab of the Interface Properties window. For more, see: Define the QoS Properties for the Interfaces (on page 29).
"Best Effort" rules (that is, non-DiffServ rules) can be installed on all interfaces of gateways with QoS gateways installed. Only rules installed on the same interface interact with each other.

**Note:**
- QoS supports adding diffserv markings to packets that match a rule
- QoS does not support matching packets based on diffserv tagging.

**Low Latency Queuing**

**Overview**

For most traffic on the Web (most TCP protocols), the WFQ (Weighted Fair Queuing, see Intelligent Queuing Engine) paradigm is sufficient. Packets reaching QoS are put in queues and forwarded according to the interface bandwidth and the priority of the matching rule.

Using this standard Policy, QoS avoids dropping packets. Dropped packets adversely affect TCP. Avoiding drops means holding (possibly) long queues, which can lead to non-negligible delays.

For some types of traffic, such as voice and video, bounding this delay is important. Long queues are inadequate for these types of traffic. Long queues can result in substantial delay. For most "delay sensitive" applications, it is not necessary to drop packets from queues to keep the queues short. The fact that the streams of these applications have a known, bounded bit rate can be utilized. If QoS is configured to forward as much traffic as the stream delivers, only a small number of packets are queued and delay is negligible.

QoS Low Latency Queuing makes it possible to define special Classes of Service for "delay sensitive" applications like voice and video. Rules below these classes can be used together with other rules in the QoS Policy Rule Base. Low Latency classes require you to specify the maximal delay that is tolerated and a Constant Bit Rate. QoS then guarantees that traffic matching rules of this type is forwarded within the limits of the bounded delay.

**Low Latency Classes**

For each Low Latency class defined on an interface, a constant bit rate and maximal delay must be specified for active directions. QoS checks packets matched to Low Latency class rules to make sure they have not been delayed for longer than their maximal delay permits. If the maximal delay of a packet has been exceeded, it is dropped. Otherwise, it is transmitted at the defined constant bit rate for the Low Latency class to which it belongs.

If the Constant Bit Rate of the class is not smaller than the expected arrival rate of the matched traffic, packets are not dropped. The maximal delay must also exceed some minimum. For more, see Computing Maximal Delay (see "Calculating Maximal Delay" on page 40)).

When the arrival rate is higher than the specified Constant Bit Rate, packets exceeding this constant rate are dropped. This is to make sure that transmitted packets comply with the maximal delay limitations.

**Note** - The maximal delay set for a Low Latency class is an upper limit. Packets matching the class are always forwarded with a delay not greater, but often smaller, than specified.

**Low Latency Class Priorities**

In most cases, one Low Latency class is sufficient for all bounded delay traffic. In some cases, it might be necessary to define more than one Low Latency class. For this reason, Low Latency classes are assigned one out of five priority levels (not including the Expedited Forwarding class, see Low Latency versus DiffServ (on page 43)). These priority levels are relative to other Low Latency classes.

As a best practice, define more than one Low Latency class if different types of traffic require different maximal delays.

The class with the lower maximal delay must get a higher priority than the class with the higher delay. When two packets are ready to be forwarded, one for each Low Latency class, the packet from the higher priority class is forwarded first. The remaining packet (from the lower class) then encounters greater delay. The maximal delay that can be set for a Low Latency class depends on the Low Latency classes of higher priority.
Other Low Latency classes can affect the delay incurred by a class. Other Low Latency classes must be taken into consideration when determining the minimal delay that is possible for the class. This is best done by:

- Initially setting the priorities for all Low Latency classes according to maximal delay
- Defining the classes according to descending priority

When you define class two, for example, class one must already be defined.

For more on the effects of class priority on calculating maximal delay, see: Computing Maximal Delay (see "Calculating Maximal Delay" on page 40).

Logging LLQ Information
SmartView Tracker logs data for all aspects of LLQ. For more, see SmartView Tracker (on page 70).

Calculating the Correct Constant Bit Rate and Maximal Delay

Limits on Constant Bit Rate
For the inbound or outbound interface direction, the sum of the constant bit rates of all the Low Latency classes has a limit. This sum cannot exceed 20% of the total designated bandwidth rate. This 20% limit makes sure that "Best Effort" traffic does not suffer substantial jitter because of the existing Low Latency class(es).

Calculating Constant Bit Rate
To calculate the Constant Bit Rate of a Low Latency class, you must know the bit rate of one application stream in traffic that matches the:

- Class
- Number of expected streams that are simultaneously opened.

The Constant Bit Rate of the class equals the bit rate of one application multiplied by the expected number of streams opened at the same time.

If the number of streams is greater than the number you expected, the total incoming bit rate will exceed the Constant Bit Rate. Many drops will occur. To prevent drops, limit the number of concurrent streams. For more, see Ensuring that Constant Bit Rate is Not Exceeded (Preventing Unwanted Drops) (see "Making sure that Constant Bit Rate is not Exceeded" on page 42).

Note - Unlike bandwidth allocated by a Guarantee, the constant bit rate allocated to a Low Latency class on an interface in a given direction is not increased when more bandwidth is available.

Calculating Maximal Delay
To calculate the maximal delay of a Low Latency class, take into account the:

- Maximal delay that streams matching the class can tolerate in QoS
- Minimal delay that QoS can guarantee this stream

It is important not to define a maximal delay that is too small, which can result in unwanted drops. The delay value defined for a class determines the number of packets that can be queued in the Low Latency queue before drops occur. The smaller the delay, the shorter the queue. A maximal delay that is not sufficient can cause packets to be dropped before they are forwarded. Allow for some packets to be queued, as explained in the steps below.

If you are using SmartView Tracker, it is recommended to use the default Class Maximal Delay defined in the LLQ log. To obtain this default number:

- First configure the correct Constant Bit Rate for the Class
- Give an estimation for the Class Maximal Delay

For more information, see SmartView Tracker (see "To Start SmartView Tracker" on page 68).
You can also set the Class Maximal Delay by obtaining estimates for the upper and lower bounds. Set the delay to a value between the bounds.

1. Estimate the greatest delay that you can set for the class:
   a) Refer to the technical details of the streaming application and find the delay that it can tolerate.
      For voice applications, the user generally starts to experience irregularities when the overall delay exceeds 150 ms.
   b) Find or estimate the bound on the delay that your external network (commonly the WAN) imposes. Many Internet Service Providers publish Service Level Agreements (SLAs) that guarantee some bounds on delay.
   c) The maximal delay must be set at no more than:
      (i) The delay that the streaming application can tolerate minus
      (ii) The delay that the external network introduces
      This makes sure that the delay introduced by QoS plus the delay introduced by the external network is no more than the delay tolerated by the streaming application.

2. Estimate the smallest delay that you can set for the class:
   - Find the bit rate of the streaming application in the application properties, or use SmartView Monitor. (For more, see: R77.10 SmartView Monitor Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=24848).
     Note: Even if you set the Constant Bit Rate of the class to accommodate multiple simultaneous streams, do the next calculations with the rate of a single stream:
   - Estimate the typical packet size in the stream.
     - Find it in the application properties, or monitor the traffic.
     - If you do not know the packet size, use the size of the MTU of the LAN behind QoS. For Ethernet, this number is 1500 Bytes.
   - Many LAN devices, switches and NICs, introduce some burstiness to flows of constant bit rate by changing the delay between packets. For constant bit rate traffic generated in the LAN and going out to the WAN, monitor the stream packets on the QoS gateway. To get an estimate of burst size, monitor the internal interface that precedes the QoS gateway.
   - If no burstiness is detected, the minimal delay of the class must be no smaller than:
     \[
     \text{Minimal Delay} = \frac{3 \times \text{Packet Size}}{\text{Bit Rate}}
     \]
     This enables three packets to be held in the queue before drops can occur.
     The bit rate must be the bit rate of one application, even if the Constant Bit Rate of the class is for multiple streams.
   - If burstiness is detected, set the minimal delay of the class to at least:
     \[
     \text{Minimal Delay} = \frac{(\text{Burst Size} + 1) \times \text{Packet Size}}{\text{Bit Rate}}
     \]

The maximal delay that you select for the class must be between the smallest delay (step 2) and the greatest delay (step 1). Setting the maximal delay near to one of these values is not recommended. If you expect the application to burst occasionally, or if you don't know whether the application generates bursts at all, set the maximal delay close to the value of the greatest delay.

This error message can show after you enter the maximal delay: "The inbound/outbound maximal delay of class... must be greater than... milliseconds." The message shows if Class of Service that you define is not of the first priority (see Low Latency Class Priorities (on page 39)). The delay value displayed in the error message depends on the Low Latency classes of higher priority, and on interface speed.

Set the maximal delay to a value no smaller than the one printed in the error message.
Making sure that Constant Bit Rate is not Exceeded

If the total bit rate going through the Low Latency class exceeds the Constant Bit Rate of the class, then drops occur. (See: Logging LLQ Information (on page 40).)

This occurs when the number of streams opened exceeds the number you expected when you set the Constant Bit Rate.

To limit the number of streams opened through a Low Latency Class:
1. Define one rule under the class, with a per connection guarantee as its Action.
2. In the Per Connection Guarantee field of the QoS Action Properties window, define the per connection bit rate that you expect.
3. In the Number of guaranteed connections field, define the maximal number of connections that you allow in this class.
   Do not select the Accept additional non-guaranteed connections option.

The number of connections is limited to the number you used to calculate the Constant Bit Rate of the class.

Interaction between Low Latency and Other Rule Properties

To activate a Low Latency class, define at least one rule below it in the QoS Policy Rule Base. Traffic matching a Low Latency class rule receives the delay and Constant Bit Rate properties defined for the specified class. The traffic is handled according to the rule properties (weight, guarantee and limit).

You can use all types of properties in the rules below the Low Latency class:
- Weight
- Guarantee
- Limit
- Per Connection Guarantee
- Per Connection Limit.

Think of the Low Latency class with its rules as a separate network interface:
- Forwarding packets at a rate defined by the Constant Bit Rate with delay bounded by the class delay.
- With the rules defining the relative priority of the packets before they reach the interface.

If a rule has a relatively low priority, then packets matching it are entitled to a small part of the Constant Bit Rate. More packets will be dropped if the incoming rate is not sufficiently small.

Note:
- Using sub-rules under the low latency class is not recommended. Sub-rules make it difficult to calculate streams that suffer drops and the drop pattern.
- Guarantees and limits are not recommended for the same reason. Except for Per Connection Guarantees, as described in Ensuring that Constant Bit Rate is Not Exceeded (Preventing Unwanted Drops (see "Making sure that Constant Bit Rate is not Exceeded" on page 42)).

When to Use Low Latency Queuing

Use Low Latency Queuing when:
- Low delay is important, and the bit rate of the incoming stream is known. For example video and voice applications. In such cases, specify both the maximal delay and the Constant Bit Rate of the class.
- Controlling delay is important, but the bit rate is unknown. For example, Telnet requires quick responses, but the bit rate is not known. If the stream occasionally exceeds the Constant Bit Rate, you do not want to experience drops. A longer delay is recommended.
  - Set the Constant Bit Rate of the class to a high estimate of the stream rate.
  - Set a large maximal delay (such as 99999 ms).
  The large delay makes sure that packets are not dropped if a burst exceeds the Constant Bit Rate. The packets are queued and forwarded according to the Constant Bit Rate.
Note - When the incoming stream is smaller than the Constant Bit Rate, the actual delay is much smaller than 99999 ms. (As in the example above). Packets are forwarded almost as soon as they arrive. The 99999 ms bound is effective only for large bursts.

Do not use a Low Latency Class when controlling delay is not of primarily importance. For most TCP protocols (such as HTTP, FTP and SMTP) the other type of QoS rule is more applicable. Use Weights, Limits and Guarantees. The correct priority is imposed on traffic without having to adjust bit rate and delay.

QoS enforces the policy with minimal drops. Weights and guarantees dynamically fill the pipe when expected traffic is not present. Low Latency Queuing limits traffic according to the Constant Bit Rate.

Low Latency versus DiffServ

Low Latency classes are different from DiffServ classes in that they do not receive type of service (TOS) markings. Not all packets are marked as Low Latency. Preferential treatment is guaranteed only while the packets are passing through the QoS gateway.

The exception to this rule is the Expedited Forwarding DiffServ class. A DiffServ class defined as an Expedited Forwarding class automatically becomes a Low Latency class of highest priority. Such a class receives the conditions afforded it by its DiffServ marking both in QoS and on the network.

Note: To use the Expedited Forwarding class as DiffServ only, without delay being enforced, specify a Maximal Delay value of 99999 in the Interface Properties tab (see Low Latency Classes (on page 39)).

When to Use DiffServ and When to Use LLQ

Do not use Low Latency Queuing to delay traffic when your ISP:

- Supports DiffServ
  Despite the DiffServ marking that you apply, the IP packets might get a different QoS level from the ISP.

- Offers you a number of Classes of Service using MPLS
  DiffServ marking communicate to your ISP the Class of Service that you expect all packets to receive.

For these two cases, mark your traffic using a DiffServ class (see When to Use Low Latency Queuing (on page 42)):

Authenticated QoS

Check Point Authenticated QoS gives Quality of Service (QoS) for end-users in dynamic IP environments, such as remote access and DHCP environments. This lets priority users, such as corporate CEOs, to receive priority service when remotely connecting to corporate resources.

Authenticated QoS dynamically prioritizes end-users, based on information gathered during network or VPN authentication. The feature leverages Check Point UserAuthority technology to classify both inbound and outbound user connections. The User Authority Server (UAS) maintains a list of authenticated users. When you query the UAS, QoS retrieves the data and allocates bandwidth accordingly.

QoS supports Client Authentication, Encrypted Client Authentication, and SecuRemote/SecureClient Authentication. User and Session Authentication are not supported.


Note: Authenticated QoS:

- Is available for backward compatibility
- Only works in QoS policy mode but does not support CoreXL or SecureXL acceleration technologies

Citrix MetaFrame Support

This section covers support for Citrix Metaframe.
Overview

Citrix MetaFrame is a client/server software application that enables a client to run a published application on a Citrix server farm from the client's desktop. Citrix MetaFrame:

- Load balances by:
  - Automatically directing a client to the server with the lightest load
  - Allows publishing and application management from only one server in that farm.
- Supplies a secure encryption option using the ICA (Independent Computing Architecture) protocol developed by Citrix.

Note:

- Uncontrolled printing traffic on Citrix ICA networks with a slow internet connection can remove bandwidth from mission critical applications. On slow networks, it is necessary to differentiate between Citrix traffic and other types of:
  - Network traffic
  - Traffic in the same layer (layer 7)
- The Citrix Print Manager service can only be used in QoS policy mode when SecureXL or CoreXL acceleration technologies are not enabled.

QoS solves the problem of uncontrolled printing traffic on Citrix ICA networks by:

- Identifying all ICA applications running over Citrix through layer 7.
- Differentiating between the Citrix traffic based on ICA published applications, ICA printing traffic (Priority Tagging) and NFuse.

For more, see: Managing QoS for Citrix ICA Applications (on page 65).

To manage printing over Citrix, QoS uses the Citrix_ICA_printing service. The Citrix ICA printing traffic service is supported in NG with Application Intelligence (R55) and higher, but is not supported:

- In Express policy mode
- When SecureXL or CoreXL acceleration technologies are enabled.

In QoS policy mode, when SecureXL or CoreXL is enabled on the gateway, you cannot install a Policy that uses the Citrix_ICA_printing service in a rule. Policy installation will fail.

For more, see: Managing QoS for Citrix Printing (on page 67).

Limitations

- Citrix services are supported in QoS policy mode only, but not when SecureXL or CoreXL are enabled on the gateway.
- Session Sharing must be disabled.
- The inspection infrastructure detects a maximum of 2048 applications. After the 2048 limit, console errors are sent. These errors do not affect your system. To stop the errors, restart the machine.
- Versions of MetaFrame prior to 1.8 are not supported because there is no packet tagging in these versions.
- Only one Citrix TCP service can be allocated per rule.

Load Sharing

Overview

Load Sharing is a mechanism that distributes traffic in a cluster of gateways to increase the total throughput. QoS architecture guarantees that Load Sharing uses either:

- Two-way Stickiness - all packets of a connection use the same gateway in both directions.
- Conversation Stickiness - all packets of control/data connections in a conversation use the same gateway in both directions.

In Load Sharing configurations, all functioning gateways in the cluster are active, and handle network traffic (Active/Active operation). If one of the member gateways fails, its connections are redistributed to other members of the cluster.

If one gateway in the cluster becomes unreachable, transparent failover occurs to the other members. Connections are shared between the remaining gateways without interruption.

**Note** - The new Check Point High Availability is a special type of load sharing that automatically works with QoS Load Sharing. These modes can be safely switched. To enforce the change though, The QoS policy has to be reinstalled.

All cluster servers share the same set of virtual interfaces. Each virtual interface corresponds to an outgoing link. The next example shows a typical cluster.
<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>DMZ</td>
<td>16</td>
<td>Cluster Sync network</td>
</tr>
<tr>
<td>8</td>
<td>LAN</td>
<td>17</td>
<td>Virtual Interface 2</td>
</tr>
<tr>
<td>9</td>
<td>Virtual Interfaces</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

QoS gives a fault-tolerant QoS solution for cluster Load Sharing that deploys a unique, distributed WFQ bandwidth management technology. The user specifies a unified QoS policy for each virtual interface of the cluster. The resulting bandwidth allocation is the same as that obtained by installing the policy on one server.

**Note** - In a situation of heavy load, a few connections are backlogged active for short periods of time. The load is not spread evenly. In such cases the load is not spread evenly, but in this case there is no congestion and therefore no need for QoS.
QoS Cluster Infrastructure

This section describes the cluster infrastructure needed for QoS load sharing.

Cluster State

ClusterXL introduces a member's load value. A member's load, calculated in percentages, is assigned to each member by the cluster. The load is different for ClusterXL multicast and unicast modes.

Usually, the load for N members in the cluster equals \((100 / N)\)%%. If the number of cluster members changes dynamically (due to failover or recovery) the load is dynamically adjusted by the cluster to the applicable value.

Changes in Cluster State

All cluster members recalculate their rates when the load on one of the members changes. If a member fails, on the next rate calculation the members bandwidth is divided between the active cluster members.

Rates Calculation Algorithm

QoS Load Sharing uses a member's load value to get the correct rates allocation for QoS rules. QoS calculates the actual rate according to these criteria:

For a centralized policy rule:

- The rate, limit and guarantee values in the rule are proportionally divided between each cluster member according to their load value
- The rate is equally divided between each connection that matches the rule

For a physical network interface, the limit is:

- A fraction of the cluster-interface limit value
- Proportional to the cluster-member's load value

The rates, limits and guarantees are recalculated each time the cluster's state changes.

Note - If the QoS daemon cannot retrieve a load, it calculates the load statically according to the \((100 / N)\)% formula. Where N is the number of members configured in the cluster topology that are not active.

Per-connection guarantees are processed separately (per-connection limit implementation remains unchanged by the Load Sharing mechanism).

Per-Connection Guarantee Allocation

Each rule with a per connection guarantee manages its rate budget. A rule's budget is the sum of all per connection guarantee rates over the number of per-connection guarantee connections allowed by this rule.

To determine if a new connection receives its per-connection guarantee, the overall rate (already granted to the matched rule's per-connection guarantee) is checked. If this rate is below the rule's budget then the new connection is granted its per-connection guarantee.

This budget is also divided between cluster members proportionally to their load. Generally, each member will get only half the allowed per-connection guarantee matched to the rule. The cluster grants per-connection guarantee service according to the QoS policy.

Example of Rates Calculation

This example shows a cluster consisting of two members with one virtual interface configured to the rate of 125KBps. The two members of the cluster equally share the load. The centralized scheduling policy and the corresponding local scheduling policies look like this:
Conclusion

The decision function distributes traffic between all cluster members. The resultant load sharing allocates the same rates to the rules/connections as would be done by a centralized policy.
Chapter 5

Managing QoS

In This Section:

Defining QoS Global Properties .............................................................................. 49
Specifying Interface QoS Properties ....................................................................... 50
Editing QoS Rule Bases ......................................................................................... 51
Modifying Rules....................................................................................................... 53
Defining Sub-Rules ................................................................................................. 61
Working with Differentiated Services (DiffServ) ...................................................... 61
Working with Low Latency Classes ........................................................................ 63
Working with Authenticated QoS ............................................................................ 64
Managing QoS for Citrix ICA Applications .............................................................. 65
Managing QoS for Citrix Printing ............................................................................ 67
Viewing QoS Gateway Status ................................................................................. 68
Configuring QoS Topology ...................................................................................... 68
Enabling Log Collection .......................................................................................... 68

This chapter covers how to configure and manage QoS. The procedures assume that you have opened SmartDashboard as described in Starting SmartDashboard (on page 26).

Defining QoS Global Properties

You can define the QoS Global Properties, including the maximum weight of a QoS rule, the default value for the weight of a new QoS rule, the unit of measure for displaying transmission rates, and various timeout values for the implementation of the QoS rules.

To Modify the QoS Global Properties

1. From the Policy menu, choose Global Properties or click the Edit Global Properties icon in the toolbar.

   The Global Properties window opens showing these fields:

   In the Weight area:
   - **Maximum weight of rule:** The maximum weight that can be assigned to rules. The default value is 1000, but can be changed to any number.
   - **Default weight of rule:** The weight to be assigned in the Action column by default to new rules, including new Default rules.

   In the Rate area:
   - **Unit of measure:** The unit specified in QoS windows by default for transmission rates (for example, Bps - Bytes per second).

   In the Authenticated timeout for QoS area:
   - **Authenticated IP expires after:** If a user has been authenticated, all connections that are opened within the specified time receive the guaranteed bandwidth connection. Any connection opened after the specified time will be queried with the User Authority Server (UAS) again.
   - **Non authenticated IP expires after:** If a user has previously tried and failed to be authenticated by the QoS Policy, then all connections that are opened within the specified time will not receive the...
Managing QoS

guaranteed bandwidth connection. This means that they will not match that specific rule during that
time.

• **Unresponded queried IP expires after:** The User Authority Server (UAS) database is queried to
  see if a user's IP has been previously authenticated using Client Authentication or SSL. Until an
  answer is received, connections from this user will be classified to the next matching rule. If an
  answer is not received within the specified time, there will be another query.

  **Note** - Click **Set Default** to restore the default settings for the **Authentication timeout for
  QoS** parameters.

2. Click **OK** to save the changes to the QoS Global Properties.

**Specifying Interface QoS Properties**

You must first define the network objects, that is, the gateway and its interfaces on which QoS controls
traffic flow. For more, see the: *R77 Security Management Administration Guide*

After defining the interfaces you can specify the QoS properties for those interfaces. This is done in the **QoS**
tab of the **Interface Properties** window. Defining the interface QoS properties involves setting the Inbound
and Outbound active transmission rates and specifying the Differentiated Services (DiffServ) and Low
Latency classes. You can change these definitions at any time.

  **Note** - The **QoS** tab is only enabled for the interfaces of gateways that have **QoS** selected on
  the **General Properties** page of the gateway.

**To Define the Interface QoS Properties**

1. Open the **Properties** window for the appropriate gateway by double-clicking the gateway in the Objects
   Tree, or by choosing the gateway from the list in the **Network Objects** window.
   The **Check Point Gateway - General Properties** window opens.
2. Choose **Topology** in the tree on the left side of the **Check Point Gateway - General Properties**
   window.
   The **Check Point Gateway - Topology** window opens.
3. If a list of the gateway's interfaces are not already present, click **Get...** to automatically retrieve the
   interfaces' information.
   If you choose this method of configuring the gateway, the topology fetched suggests the external
   interface of the gateway based on the QoS gateway routing table. You must ensure that this information
   is correct.
   Alternatively, clicking **Add** displays the **Interface Properties** window. Interface information can then be
   defined in the **General** and **Topology** tabs of this window.
4. Double-click on the appropriate interface, or select it and click **Edit**.
   The **Interface Properties** window opens.
5. Click the **QoS** tab.
6. The **QoS** tab opens.

  **Note** - The interfaces on the WAN side (or the interface connected to the slower network) should usually
  be set to active. On a simple gateway with only two interfaces, QoS should be installed only on the
  interface connected to the WAN. If the gateway also controls DMZ traffic, you may want to install QoS
  on the interface connected to the DMZ.

  • Check **Inbound Active** to enable QoS to control traffic on this interface in the inbound direction.
  • From the **Rate** list select the available bandwidth in the inbound direction, or enter the interface rate
    manually.
  • Check **Outbound Active** to enable QoS to control traffic on this interface in the outbound direction.
  • From the **Rate** list select the available bandwidth in the outbound direction, or enter the interface
    rate manually.

  **Note** - Make sure that the rates correspond to the actual physical capacity of the interfaces, as QoS
does not verify these values.
If the rate is incorrectly defined as less than the line’s real capacity, QoS will not use more than the capacity defined, and the excess capacity will remain unused. If the rate is incorrectly defined as more than the line’s real capacity, QoS will not control the traffic correctly.

7. In the **DiffServ and Low Latency classes** area, you can specify the Differentiated Services (DiffServ) and Low Latency Queuing classes to be used on the interface.
   You can **Add**, **Edit** or **Remove** a class. Refer to *Working with Differentiated Services (DiffServ)* (on page 61) and *Working with Low Latency Classes* (on page 63) for more details on adding or editing DiffServ and Low Latency Classes.
   For information about DiffServ and Low Latency classes, see *Differentiated Services (DiffServ)* (on page 38) and *Low Latency Queuing* (on page 39).

8. Click **OK**
   Changes to the interface QoS properties are saved.

9. For each of the relevant interfaces, do steps 4 - 7.

### Editing QoS Rule Bases

A Policy Package comprises more than one Rule Base, depending on the policy types selected.

QoS policy is implemented by defining an ordered set of rules in the Rule Base. The Rule Base is comprised of those rules which you create, and a default rule. The default rule is automatically created with the Rule Base. It can be modified but cannot be deleted. The fundamental concept of the Rule Base is that unless other rules apply, the default rule is applied to all data packets. The default rule is therefore always the last rule in the Rule Base.

The Rule Base specifies what actions are to be taken with the data packets. It specifies the source and destination of the communication, what services can be used, at what times, whether to log the connection and the logging level.

A QoS Rule Base is applied to specific gateways and interfaces. After you have created the Policy Package and defined its QoS rules you must install it on the relevant QoS gateways.

For more, see: *Overview* (on page 17).

#### To Create a New Policy Package

1. From the **File** menu choose **New**.
   The **New Policy Package** window opens.

2. Enter the name of the Policy Package in the **New Policy Package Name** field. This name cannot:
   - Contain any reserved words or spaces.
   - Start with a number.
   - Contain any of the following characters: %, #, ', &, *, !, @, ?, <, >, /, \, :.
   - End with any of the following suffixes: .w, .pf, .W.

3. In the **QoS** area, select a mode:
   - QoS policy mode
   - QoS Express policy mode
   **Note**: A number of limitations can prevent you from enabling SecureXL or CoreXL. For more, see: QoS Policy limitations (*"Enabling QoS Acceleration Support"* on page 11).

4. Click **OK**.
   The new Policy Package is saved and a Default Rule is automatically created.

#### To Open an Existing Policy Package

1. From the **File** menu, select **Open**.
   The **Open Policy Package** window opens.

2. Double-click on the appropriate Policy Package, or select it and click **Open**.
To Add a Rule to the Rule Base

When you add rules to a Policy Package you can position the new rule at any location in the Rule Base. The automatically created Default Rule must always remain at the bottom of the Rule Base.

1. Position your mouse cursor in the Name field of the QoS tab, at the position where you want to add a new rule.

2. You can add the new rule either from the Rule menu, the toolbar, or right-click on any name in the Name column of a rule to display the Rule menu, as shown here:

Adding a Rule

<table>
<thead>
<tr>
<th>To add a rule</th>
<th>Select from Menu</th>
<th>Toolbar button</th>
</tr>
</thead>
<tbody>
<tr>
<td>After the last rule</td>
<td>Rules &gt; Add Rule &gt; Bottom</td>
<td></td>
</tr>
<tr>
<td>Before the first rule</td>
<td>Rules &gt; Add Rule &gt; Top</td>
<td></td>
</tr>
<tr>
<td>After the current rule</td>
<td>Rules &gt; Add Rule &gt; Below</td>
<td></td>
</tr>
<tr>
<td>Before the current rule</td>
<td>Rules &gt; Add Rule &gt; Above</td>
<td></td>
</tr>
<tr>
<td>To the current rule</td>
<td>Rules &gt; Add Sub-Rule</td>
<td></td>
</tr>
</tbody>
</table>

Description of Rule Menu Items

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Rule above</td>
<td>Adds a rule before the current rule.</td>
</tr>
<tr>
<td>Add Rule below</td>
<td>Adds a rule after the current rule.</td>
</tr>
<tr>
<td>Add Sub-Rule</td>
<td>Deletes the current rule.</td>
</tr>
<tr>
<td>Delete Rule</td>
<td>Deletes the current rule.</td>
</tr>
<tr>
<td>Copy Rule</td>
<td>Copies the current rule to the clipboard.</td>
</tr>
<tr>
<td>Cut Rule</td>
<td>Deletes the current rule and puts it in the clipboard.</td>
</tr>
<tr>
<td>Paste Rule</td>
<td>Pastes the rule in the clipboard (a sub-menu is displayed from which you</td>
</tr>
<tr>
<td></td>
<td>can select whether to paste the rule above or below the current rule).</td>
</tr>
<tr>
<td>Add Class of Service</td>
<td>Specifies a Class of Service (see Differentiated Services (DiffServ) (on</td>
</tr>
<tr>
<td></td>
<td>page 38) and Low Latency Queuing (on page 39)). A sub-menu is displayed</td>
</tr>
<tr>
<td></td>
<td>from which you can select whether the Class of Service is to be added</td>
</tr>
<tr>
<td></td>
<td>above or after the current rule.</td>
</tr>
<tr>
<td>Hide Rule</td>
<td>Hides the current rule. The rule is still part of the Rule Base and will</td>
</tr>
<tr>
<td></td>
<td>be installed when the QoS Policy is installed.</td>
</tr>
<tr>
<td>Disable Rule</td>
<td>Disables the current rule. The rule appears in the Rule Base but is not</td>
</tr>
<tr>
<td></td>
<td>enforced by the QoS Policy.</td>
</tr>
<tr>
<td>Rename Rule</td>
<td>Renames the current rule.</td>
</tr>
<tr>
<td>Matching Method</td>
<td>Starting from QoS NG this feature is not relevant since it is kept for</td>
</tr>
<tr>
<td></td>
<td>backward compatibility only (version 4.1).</td>
</tr>
</tbody>
</table>

3. Select one of the options for creating the new rule. The Rule Name window is displayed.
4. Enter the name of the rule in the **Rule Name** field.
5. Click **OK**. The rule is added to the Rule Base at the selected position and is comprised of the default values defined in the **QoS** page of the **Global Properties** window. Follow the procedures described in the pages that follow to modify this rule.

**To Rename a Rule**

1. In the **QoS** tab, double-click on the rule you want to rename, or right-click on the rule and select **Rename Rule**. The **Rule Name** window is displayed.
2. Enter the rule name in the **Rule Name** field.
3. Click **OK** to save the rule name.

**To Copy, Cut or Paste a Rule**

You can copy, cut or paste a rule using either the **Edit** or **Rules** menus or the right-click menu of the selected rule.

1. In the **QoS** tab, select the rule you want to copy, cut or paste.
2. From the **Edit** or **Rules** menu, select one of the options described in the table below.

<table>
<thead>
<tr>
<th>Action</th>
<th>From Menu select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cut</td>
<td><strong>Edit &gt; Cut</strong></td>
</tr>
<tr>
<td>Copy</td>
<td><strong>Edit &gt; Copy</strong></td>
</tr>
<tr>
<td>Paste</td>
<td><strong>Edit &gt; Paste</strong></td>
</tr>
</tbody>
</table>

If you select **Paste**, then the **Paste** menu will be opened. You must then select **Bottom, Top, Above**, or **Below** to specify where in the Rule Base to paste the rule.

**To Delete a Rule**

You can delete a rule using either the right-click menu of the selected rule or clicking the Delete button on the toolbar.

1. In the **QoS** tab, select the rule you want to delete.
2. Click the Delete button on the toolbar.
3. Click **Yes** to delete the selected rule.

**Modifying Rules**

You can modify any of the rule fields, as often as you like, until the rule is in the form that you require. This includes specifying the source and destination of each communication, what services can be used at what times (including TCP, Compound TCP, UDP, and ICMP services), the actions to be taken with the data packets, whether you want to maintain a log of the entries for the selected rule, and on which interfaces of the QoS gateway the rule is enforced.

This section describes the procedures for modifying the various fields in a rule. Refer to Overview (on page 17) for more details about rules.

**Modifying Sources in a Rule**

You can modify the source(s) of the communication in a rule. You can add as many sources as required. In addition, you can restrict the sources of the rule to particular user groups, or to user groups originating from specific locations.
To Add Sources to a Rule
1. From the Rule Base select the rule to modify.
2. Right-click in the Source column of the selected rule and select Add. The Add Object window shows listing the network objects defined in the Security Policy and the QoS Policy.
   Note - You can also use the Add Object window to define new objects and delete or modify objects.
3. Select one or more network objects (using the standard Windows selection keys) to add to the rule's Source.
4. Click OK.
   • The objects are added to the Source field.
   • You can add as many sources as required.

To Add User Access to the Sources of a Rule
1. From the Rule Base select the rule you want to modify.
2. Right-click in the Source column of the selected rule and select Add Users Access. The User Access window is displayed.
3. Select one of the user groups to add to the rule's Source.
4. Select whether you want to restrict the Location, as follows:
   • No restriction: There is no restriction on the source of the users. For example, if you select All Users and check No restriction, then AllUsers@Any will be inserted under Source in the rule.
   • Restrict to: The source is restricted to the network object you select in the list box. For example, the source object in the rule will be AllUsers@Local_Net.
5. Click OK to add the user access to the rule source.

To Edit, Delete, Cut, Copy or Paste a Source in a Rule
You can edit, delete, cut, copy or paste a source in a rule using the right-click menu of the selected source.
1. From the Rule Base select the rule to modify.
2. Right-click on the Source of the selected rule
3. Select one of these options:
   • Edit: The appropriate window is opened, according to the type of object selected, and you can change the object's properties. (Alternatively, you can double-click on an object in the Source column of the selected rule to edit it.)
   • Delete: The selected object is deleted. If you delete the last source object in the rule it is replaced by Any.
   • Cut: The selected object is cut and put it in the clipboard.
   • Copy: The selected object is copied to the clipboard.
   • Paste: The object is pasted from the clipboard to the rule's Source.

To View Where an Object is Used
You can view where the selected object is used (in queries, active policies, and so on).
1. From the Rule Base select the rule to modify.
2. Right-click on the Source of the selected rule
   The Object References window opens showing where the selected object is used (in queries, active policies, and so on).
4. Click Close to return to the rule.
**Modifying Destinations in a Rule**

You can modify the destination(s) of the communication in a rule. You can add as many destinations as required.

**To Add Destinations to a Rule**

1. From the Rule Base select the rule to modify.
2. Right-click in the Destination column of the selected rule.
3. Select Add.
   
   The Add Object window opens, listing the network objects defined in the Security Policy and the QoS Policy.
   
   **Note** - You can also use the Add Object window to define new objects and delete or modify objects.

4. Select one or more network objects (using the standard Windows selection keys) to add to the rule’s Destination.
5. Click OK.
   
   The objects are added to the Destination field. Add as many destinations as required.

**To Edit, Delete, Cut, Copy or Paste a Destination in a Rule**

You can edit, delete, cut, copy or paste a destination in a rule using the right-click menu of the selected source.

1. From the Rule Base select the rule you want to modify.
2. Right-click on the Destination of the selected rule and select one of the following options:
   
   - **Edit**: The appropriate window is opened, according to the type of object selected, and you can change the object's properties. (Alternatively, you can double-click on an object in the Destination column of the selected rule to edit it.)
   - **Delete**: The selected object is deleted. If you delete the last destination object in the rule it is replaced by Any.
   - **Cut**: The selected object is cut and put it in the clipboard.
   - **Copy**: The selected object is copied to the clipboard.
   - **Paste**: The object is pasted from the clipboard to the rule's Destination.

**To View Where an Object is Used**

You can view where the selected object is used (in queries, active policies, and so on).

1. From the Rule Base choose the rule you want to modify.
2. Right-click on the Source of the selected rule and choose Where Used. The Object References window is displayed showing you where the selected object is used (in queries, active policies, and so on).
3. Click Close to return to the rule.

**Modifying Services in a Rule**

You can modify the service(s) in a rule. You can add as many services as required, however, you can only add one URI for QoS resource in a single rule.

**Note** - Previous versions of QoS have not limited the number of URIs for QoS resources allowed per rule. If you are using a QoS Policy originally designed for use with a previous QoS version, be sure to redefine any rule that has more than one resource in its Service Field.

**To Add Services to a Rule**

1. From the Rule Base select the rule to modify.
Managing QoS

2. Right-click in the Service column of the selected rule.
3. Select Add.
   The Add Object window shows listing the network objects defined in the Security Policy and the QoS Policy.
4. Select one or more network objects (using the standard Windows selection keys) to add to the rule’s Service.
5. Click OK.
   The objects are added to the Service field.
   • You can add as many services as required.
   • Only one TCP Citrix or URI for QoS service is allowed.

To Add a Service with a Resource to a Rule

1. From the Rule Base choose the rule you want to modify.
2. Right-click in the Service column of the selected rule and select Add with Resources.
   The Services with Resource window opens.
   You can only add one service with a resource to a rule, so this option will only be available if you have not already added a service with a resource to this rule.
3. Select one of the services in the Location area.
4. Select the appropriate resource from the Resource list.
   Note:
   • Only resources of type URI for QoS can be added to the QoS Rule Base. URI for QoS is used for identifying HTTP traffic according to the URL (URI).
   • Do not use the protocol prefix (http://) when setting up a URI resource. HTTP services with URI for QoS resources can be defined on all ports.
   • The regular expression ("Regular Expressions" on page 91) supported by QoS is of form a*b where a and b are strings and * is wildcard.
   • Both full and relative URI are supported:
     ▪ Full URI: Use the full URI but without protocol prefix (for example, do not use"http://"). Valid full URI example: "www.my-site.com/pic/qos.gif"
     ▪ Relative URI: Use the URI that starts just after the domain name. The relative URI must start with slash. For example: "/pic/qos.gif"
5. Click OK to add the service with a URI for QoS resource to the rule.
   Note - Only one resource is allowed in a single rule.

To Edit, Delete, Cut, Copy or Paste a Service in a Rule

You can edit, delete, cut, copy or paste a service in a rule using the right-click menu of the selected service.
1. From the Rule Base the select the rule to modify.
2. Right-click on the Service of the selected rule.
3. Select one of these options:
   • Edit: The appropriate window is opened, according to the type of object selected, and you can change the object's properties. (Alternatively, you can double-click on an object in the Service column of the selected rule to edit it.)
   • Delete: The selected object is deleted. If you delete the last service object in the rule it is replaced by Any.
   • Cut: The selected object is cut and put it in the clipboard.
   • Copy: The selected object is copied to the clipboard.
   • Paste: The object is pasted from the clipboard to the rule's Service.

To View Where an Object is Used

You can view where the selected object is used (in queries, active policies, and so on).
1. From the **Rule Base** select the rule to modify.
2. Right-click on the **Service** of the selected rule.
3. Select **Where Used**.
   The **Object References** window opens showing you where the selected object is used (in queries, active policies, and so on).
4. Click **Close** to return to the rule.

**Modifying Rule Actions**

You can modify the default properties of a rule. The available options depend on whether it is a simple or advanced type of rule. The advanced rule action type enables you to specify limits and guarantee allocation on a per connection basis.

**To Edit the Rule Actions**

1. From the **Rule Base** choose the rule you want to modify.
2. Right-click in the **Action** column of the selected rule and select **Edit Properties**.
   The **QoS Action Properties** window opens.
   - If the **Action Type** of the rule is defined as **Simple**, the **QoS Action Properties** window opens:
   - If the **Action Type** of the rule is defined as **Advanced**, the **QoS Action Properties** window opens:

      **Note** - When Express QoS has been installed, **Advanced** Actions are not available.

3. The following properties are displayed for a QoS rule with a simple action type. You can change any of these fields:
   In the **Action Type** area:
   - **Simple**: The full set of actions with the exception of the **Guarantee Allocation** and the per connection limit features.
   - **Advanced**: The full set of actions with the **Guarantee Allocation** feature included.
   In the **VPN Traffic** area:
   - **Allow rule only to encrypted traffic**: Check this box if you want the rule to be matched only by VPN traffic. If you do not check this field, rules will be matched by all traffic types, both VPN and non-VPN traffic. VPN traffic means traffic that is encrypted in this same gateway by IPsec VPN. This field does not apply to traffic that was encrypted prior to arriving to this gateway. This type of traffic can be matched using the "IPSec" service. For further explanation on how to use this check box for prioritizing VPN traffic over non-VPN, see Example of a Rule Matching VPN Traffic (on page 21).
   - In the **Action Properties** area you can define the restrictions on bandwidth for connections to which the rule applies in the following fields:
     - **Rule Weight**: Enables you to define the weight of the rule. This field is checked by default and has the value defined in the **Global Properties** window in Defining QoS Global Properties (on page 49). It is recommended to leave this value as is to avoid a complete loss of bandwidth. For detailed information see Weight (on page 19).
       **Important** - 0 rate in conjunction with 0 guarantee can lead to the rule's complete loss of bandwidth. To prevent this from happening, retain some ratio in the **Rule Weight**. The default is 10.
     - **Rule Limit**: Enables you to restrict the total bandwidth consumed by the rule. For detailed information see Limits (on page 20).
       **Note** - When using weights or guarantees, the weighted fair queuing algorithm that QoS makes use of assures that no bandwidth is ever wasted. Spare bandwidth is divided among the backlogged rules. However, if you set a rule limit, it will not use spare bandwidth above this limit.
     - **Rule Guarantee**: Enables you to define the absolute bandwidth allocated to the rule. For detailed information see Guarantees (on page 19).
       **Note** - The number you enter for the **Rule Guarantee** cannot be larger than the **Rule Limit**.
4. (Optional) The following additional properties are displayed for a QoS rule with an advanced action type. You can change any of these fields:

   In the **Limit** area:
   - **Rule Limit**: Enables you to restrict the total bandwidth consumed by the rule. For detailed information see Limits (on page 20).
     
     **Note** - When using weights or guarantees, the weighted fair queuing algorithm that QoS makes use of assures that no bandwidth is ever wasted. Spare bandwidth is divided among the backlogged rules. However, if you set a rule limit, it will not use spare bandwidth above this limit.
   - **Per connection limit**: Enables you to set a rule limit per connection.
     
     **Note** - The number you enter for the Rule Guarantee cannot be larger than the Rule Limit.

   In the **Guarantee Allocation** area:
   - **Guarantee**: Enables you to allocate a minimum bandwidth to the connections matched with a rule. For detailed information see Guarantees (on page 19).
   - **Per rule**: Enables you to define the absolute bandwidth allocated to the rule.
     
     **Note** - The number you enter for the **Per rule** cannot be larger than the **Rule Limit**.
   - **Per connection**: Enables you to manage the bandwidth at the connection-level.
   - **Per connection guarantee**: Enables you to restrict the absolute bandwidth allocated per connection.
   - **Number of guaranteed connections**: Enables you to allocate a minimum number of guaranteed connections.
     
     **Note** - The **Number of guaranteed connections** multiplied by the **Per connection guarantee** cannot be greater than the rule limit.
   - **Accept additional connections**: Check this option to allow connections without per connection guarantees to pass through this rule and receive any leftover bandwidth. Enter the maximum amount of bandwidth that is allowed for this option in the text box. This only occurs if all other conditions have been met.
     
     **Note** - Select a non-zero rule weight when **Accept additional non-guaranteed connections** is checked.

5. Click **OK** to update the **QoS Action Properties** for the rule.

**To Reset the Rule Actions to Default Values**

1. From the **Rule Base** select the rule you want to modify.
2. Right-click in the **Action** column of the selected rule and select **Reset to Default**. The action properties for the selected rule are reset to their default values. The default values are defined in the QoS page of the **Global Properties** window (see Defining QoS Global Properties (on page 49)).

**Modifying Tracking for a Rule**

You can choose whether you want to maintain a log of the entries for the selected rule. If you do want to log the entries, you also have the option of logging the entries in account format. For further information on tracking and logging, see Overview of Logging (on page 70). For information on how to turn logging on, see Enabling Log Collection (on page 68).

**To Modify Tracking for a Rule**

1. From the **Rule Base** select the rule you want to modify.
2. Right-click in the **Track** column of the selected rule. The menu that is displayed has the following options:
   - **None**. No logging is done for this connection
   - **Log**. Logging is done for this connection
• Account. Logging for this connection is done in Accounting format.

3. Select the required option.

**Modifying Install On for a Rule**

The **Install On** field specifies on which interfaces of the QoS gateway the rule is enforced. You can select any number of **Install On** objects.

**Note** - To install a QoS Policy on a gateway, make sure that:

- The gateway has the QoS option selected on the **Network Security** tab of the gateways **General Properties** page.
- The interface is defined in the **QoS** tab of the **Interface Properties** window. (See Defining QoS Global Properties (on page 49) and Specifying Interface QoS Properties (on page 50).)

**To Modify Install On for a Rule**

1. From the **Rule Base** select the rule you want to modify.
2. Right-click in the **Install On** column of the selected rule and select **Add**. The **Add Interface** window is displayed.
3. (Optional) Click **Select Targets** to select additional installable targets. The **Select Installation Targets** window is displayed.
4. To add any target(s) to the list of Installed Targets, select the target(s) in the **Not in Installation Targets** area and click **Add**.
   The selected target(s) are added to the **In Installation Targets** area.
5. To remove a target(s) from the **In Installation Targets** area, select the target(s) and click **Remove**.
   The selected targets are returned to the **Not in Installation Targets** area.
6. Click **OK**. The selected targets now appear in the **Add Interface** window.
7. Select from the list of targets in the **Add Interface** window:
   - A gateway (and all its interfaces on which QoS is defined), or
   - An interface (in both directions), or
   - One direction of an interface
8. Click **OK**. The selected interface is added to the **Install On** field.

**To Delete an Install On for a Rule**

You can remove an interface for a rule. The rule will no longer be enforced for the interface.

1. From the **Rule Base** select the rule to modify.
2. Right-click on the **Service** of the selected rule.
3. Select **Delete**.
   The selected object is deleted.

**To View Where an Object is Used**

You can view where the selected object is used.

1. From the **Rule Base** select the rule to modify.
2. Right-click on the **Install On** of the selected rule.
3. Select **Where Used**.
   The **Object References** window opens showing where the selected object is used.
4. Click **Close** to return to the rule.

**Modifying Time in a Rule**

You can specify the times that the rule is enforced. You add any number of time objects to a rule.
To Modify Time in Rules
1. From the Rule Base select the rule to modify.
2. Right-click in the Time column of the selected rule.
3. Select Add.
   The Add Object window opens.
4. (Optional) You can edit a time object:
   a) Select the required time object and click Edit to modify a time object.
      The Time Properties window opens. (Alternatively, you can double-click on an object in the Time column of the selected rule to edit it.)
   b) Edit the fields in the Time Properties window, as required.
   c) Click OK.
5. Select the required time object in the Add Object window.
The time object is added to the rule.

To Edit or Delete a Time Object for a Rule
You can edit or delete a time object in a rule using the right-click menu of the selected service.
1. From the Rule Base choose the rule to modify.
2. Right-click on the Time column of the selected rule.
3. Select one of these options:
   • Edit: The appropriate window is opened, according to the type of object selected, and you can change the object's properties. (Alternatively, you can double-click on an object in the Time column of the selected rule to edit it.)
   • Delete: The selected object is deleted. If you delete the last time object in the rule it is replaced by Any.

To View Where an Object is Used
You can view where the selected object is used (in queries, active policies, and so on).
1. From the Rule Base select the rule to modify.
2. Right-click on the Service of the selected rule.
The Object References window opens showing you where the selected object is used (in queries, active policies, and so on).
4. Click Close to return to the rule.

Adding Comments to a Rule
You can add a comment to a rule.

To Add Comments to Rules
1. From the Rule Base select the rule to modify.
2. Right-click in the Comment column of the selected rule.
3. Select Edit.
The Comment window opens. You can also open this window by double-clicking in the Comment column of the selected rule.
4. Type relevant comments in the text box.
5. Click OK.
The comment is added to the rule.
Defining Sub-Rules

Sub-rules are rules that allocate bandwidth more specifically within a rule. For example, consider the rule shown in the figure below.

![Rule Diagram]

The bandwidth allocated to the ABC_VPN rule is further allocated among the sub-rules ABC_VPN_ERP through Default under ABC_VPN.

To Define Sub-Rules

1. Select the rule under which the sub-rule is to be defined.
2. Right-click in the Rule Name column.
3. Select Add Sub-Rule from the menu. The Rule Name window is displayed.
4. Enter the sub-rule name and click OK. The new sub-rule together with a default sub-rule is automatically created, under the rule selected in 1 above, using the default values defined.
5. You may modify the sub-rules by following the same procedures for editing rules described on page in Editing QoS Rule Bases (on page 51).
6. Add new sub-rules by following the same procedures for creating rules described in Editing QoS Rule Bases (on page 51).

To View Sub-Rules

The sub-rules under a main rule can be seen by expanding the rule in the QoS Rule Tree. To view sub-rules in the Rule Base, click one of the sub-rules in the relevant main rule. The Rule Base shows all the sub-rules for that rule.

Working with Differentiated Services (DiffServ)

A DiffServ rule specifies not only a QoS Class, but also a weight, in the same way that other QoS Policy Rules do. These weights are enforced only on the interfaces on which the rule is installed.

For more on DiffServ, see: Differentiated Services (DiffServ) (on page 38).

To Implement DiffServ Marking

1. Define one or more DiffServ Classes of Service using the QoS Classes window. You can also define a Class of Service Group.
   For more, see: To Define a DiffServ Class of Service (on page 62).
2. In the QoS tab of the Interface Properties window of all interfaces on which the DiffServ class will be implemented (see Specifying Interface QoS Properties (on page 50)), click Add under DiffServ and Low Latency classes to add a new class.
   Alternatively Edit to edit the properties of an existing class. See Specifying Interface QoS Properties (on page 50).
3. In the Add QoS Class Properties window, select the QoS class and define the Inbound and Outbound parameters.
4. Click OK.
   You can now add QoS Classes to the Rule Base.
5. Right-click in the Name column of a rule and choose Add Class of Service, or select Add QoS Class from the Rules menu.
6. Specify whether the class should appear above or after the rule in the Rule Base.
7. Select the required Class of Service from the drop-down menu in the Add Class of Service window.
8. Click OK.
   A DiffServ class header appears in the Rule Base.
9. Add rules under the QoS Class you defined, by either:
   • Choosing Rules > Add Rule > Below from the menu, or
   • Right-clicking on the QoS Class and choosing Add Rule > Below from the menu

To Define a DiffServ Class of Service
1. From the Manage menu select QoS>QoS Classes.
   The QoS Classes window opens.
2. Click New to define a new DiffServ class and select DiffServ Class of Service to display the Class of Service Properties window.
3. Enter the following details in the Class of Service Properties window:
   • Name: The name of the Class of Service.
   • Comment: The text to be displayed when this class is selected in the QoS Classes window
   • Color: Select a color from the list.
   • Type: Select a type from the list. You may select a predefined or user defined class.
   • DiffServ code: This is a read-only field that displays the DiffServ marking as a bitmap.
4. Click OK to create the new DiffServ Class of Service.

To Define a DiffServ Class of Service Group
1. From the Manage menu select QoS > QoS Classes. The QoS Classes window displays.
2. Click New to define a new DiffServ class and select DiffServ Class of Service Group to display the Group Properties window.
3. Enter the following details in the Group Properties window:
   • Name: The name of the group.
   • Comment: The text to be displayed when this class is selected in the QoS Classes window.
   • Color: Select a color from the list.
   • To add a DiffServ class to the group, select the class in the list box labeled Not in Group, and click Add.
   • To delete a class from the group, select the class in the list box labeled In Group, and click Remove.
4. Click View expanded group to display all members of the selected DiffServ group.
5. Click OK to create the new DiffServ Class of Service Group.

To Add QoS Class Properties for Expedited Forwarding
1. From the QoS tab of the Interface Properties window, click Add or Edit.
2. From the menu that is displayed select either Low Latency Classes or DiffServ > Expedited Forwarding.
   The Add Low Latency QoS Class Properties window is displayed if you selected Low Latency Classes. If you selected DiffServ Expedited Forwarding, a similar window with the identical fields is displayed.
3. Enter the required information as detailed below. You should define at least one inbound or outbound direction.
   • Class: Select a Low Latency class from the list of defined classes.
   • Inbound: Define the portion of the interface's inbound capacity to be reserved.
   • Constant Bit Rate: The constant bit rate at which packets of this class will be transmitted.
   • Maximal Delay: The maximum delay that will be tolerated for packets of this class. Those packets that exceed this delay are dropped.
Managing QoS

• **Outbound:** Define the portion of the interface's outbound capacity to be reserved by defining a **Constant Bit Rate** and a **Maximum Delay** as described above.

4. Click **OK.** The new class is added.

**To Add QoS Class Properties for Non Expedited Forwarding**

1. From the **QoS** tab of the **Interface Properties** window, click **Add** or **Edit.**
2. From the menu that is displayed select **DiffServ>Others.** The **Add DiffServ QoS class Properties** window is displayed
3. Enter the required information as detailed below. You should define at least one inbound or outbound direction.  
   - **Class:** Select a DiffServ class from the list of defined classes.
   - **Inbound:** Define the portion of the interface's inbound capacity to be reserved.
   - **Guaranteed bandwidth:** The bandwidth guaranteed to be marked with the QoS Class.
   - **Bandwidth Limit:** The upper limit of the bandwidth to be marked with the QoS Class. Traffic in excess of the **Bandwidth Limit** will not be marked. For example, if the interface's capacity is 256MB and **Bandwidth Limit** to 192MB, then traffic beyond 192MB will not be marked.
   - **Outbound:** Define the portion of the interface's outbound capacity to be marked by defining a **Guaranteed Bandwidth** and a **Bandwidth Limit** as described above.
4. Click **OK.** The new class is added.

**Working with Low Latency Classes**

QoS Low Latency Queuing makes it possible to define special classes of service for "delay sensitive" applications like voice and video. Rules under these classes can be used together with other rules in the QoS Policy Rule Base. Low Latency classes require you to specify the maximal delay that is tolerated and a **Constant Bit Rate.** QoS then guarantees that traffic matching rules of this type are forwarded within the limits of the bounded delay.

For more, see: Low Latency Queuing (on page 39).

**To Implement Low Latency Queuing**

Having defined one or more Low Latency Classes of Service, you can implement Low Latency Queuing as follows:

1. In the **QoS** tab of the **Interface Properties** window of all interfaces on which Low Latency classes are implemented (see Specifying Interface QoS Properties (on page 50)), click **Add** under **DiffServ and Low Latency classes** to add a new class, or **Edit** to edit the properties of an existing class.
2. In the **Add QoS Class Properties** window, select the **Low Latency class** and define the **Inbound** and **Outbound** parameters (see To Add QoS Class Properties for Expedited Forwarding (on page 62)).
3. Click **OK.**
   You can now add Low Latency Classes to the QoS Policy Rule Base.
4. Right-click in the **Name** column of a rule and select **Add Class of Service,** or select **Add QoS Class** from the **Rules** menu.
5. Specify whether the class should appear above or below the rule in the Rule Base.
   **Note** - The order of the classes in the Rule Base must be DiffServ, followed by Low Latency, and then Best Effort. You will not be able to add a Low Latency class to the Rule Base above any DiffServ classes you may have.
6. Select the required **Class of Service** from the drop-down menu in the **Add Class of Service** window.
7. Click **OK.**
   A class header appears in the Rule Base.
8. Add rules under the QoS Class you defined, by either:
   - Choosing **Rules > Add Rule > Below** from the menu, or
   - Right-clicking on the QoS Class and choosing **Add Rule > Below** from the menu.
Managing QoS

To Define Low Latency Classes of Service

Before a Low Latency class can be implemented on an interface and used in the QoS Rule Base, it must be defined.

1. From the Manage menu select QoS > QoS Classes.
   The QoS Classes window opens.
2. Define the Low Latency Class of Service as described in To Define a DiffServ Class of Service (on page 62).
3. To define a new Low Latency class, click New.
4. Select Low Latency Class of Service.
   The Class of Service Properties window opens.

To Define Class of Service Properties for Low Latency Queuing

1. From the Manage menu select QoS > QoS Classes. The QoS Classes window is displayed.
2. Click New and select Low Latency Class of Service to display the Class of Service Properties window.
3. Enter the following details:
   • Name: The name of the Class of Service.
   • Comment: Enter the text to be displayed when this class is selected in the QoS Classes window.
   • Color: Select a color from the list.
   • Class Priority: Select one of the five priority types from the list (Class 1 being the highest priority).
4. Click OK. The new Low Latency Class of Service is saved.

Working with Authenticated QoS

Authenticated QoS provides Quality of Service (QoS) for end-users in dynamic IP environments, such as remote access and DHCP environments. This enables priority users, such as corporate CEOs, to receive priority service when remotely connecting to corporate resources.

For more detailed information, please see Authenticated QoS (on page 43).

To Use Authenticated QoS

To apply Authenticated QoS in a rule:

1. Make sure that the UAS package is installed on the gateway that does Authenticated QoS.
2. Make sure that the User Authority Server option under Check Point Products Installed is selected on the Security Gateway on which you are installing the policy.
3. Create a group in Manage > Users > New > Group.
4. In the Group Properties window, add all the priority users.
5. Create a rule.
6. In the Source column, right-click and select Add object > Add legacy user access.
   For example, if the CEO of your company is in a remote location and wants to access his email and without waiting too long, create a rule like this:

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO</td>
<td>CEO@localnet</td>
<td>Any</td>
<td>Pop-3</td>
<td>Weight 10 Guarantee 50,000 Bps</td>
</tr>
</tbody>
</table>

Note - To minimize the resources taken up by Authenticated QoS, it is recommended that Authenticated QoS rules refer to specific services, and unless absolutely necessary, you should not include Any in the Service field.

7. Install the policy.
Managing QoS

Note -

• The user must be authenticated in the UAS in order for the QoS policy to be enforced.
• Policy-wide properties for Authenticated QoS can be defined in the QoS page of the Global Properties window. For more information, see Defining QoS Global Properties (on page 49).

Managing QoS for Citrix ICA Applications

In order to deliver a QoS solution for the Citrix ICA protocol:
1. Disable session sharing in the Citrix Program Neighborhood.
2. Modify your Security Policy to allow the Citrix_ICA and Citrix_ICA_Browsing services.  
   Note - The Any service does not include the Citrix ICA service.
3. Discover the Citrix application names, as defined by the Citrix Administrator, and retrieve your Citrix ICA application names from the SmartView Tracker.
   This includes turning on the application detection check box and installing Security and QoS Policies.
4. Define new Citrix TCP services with the application names you have detected.
5. Add the appropriate Citrix TCP services to rules in your QoS Policy.
6. Install the QoS Policy.

Disabling Session Sharing

Citrix enables session sharing by default. In this mode, traffic from all the applications used by a specific client share the same TCP connection. In order for QoS to prioritize different Citrix ICA applications from the same client, you must disable session sharing. This means that every application uses a separate TCP connection (all going to the same server port, 1494, from different source ports).

You should contact the Citrix Administrator to configure the correct mode.

To Disable Session Sharing:
1. Double-click the Citrix Program Neighborhood icon placed on the desktop by the Citrix install program.
2. Click the Settings icon or, from the File menu, select Application Set Settings.
3. Select the Default Options tab.
4. From the Window Size list, select something other than Seamless Window.

Modifying your Security Policy

You must modify your Security Policy to enable the new Citrix_ICA TCP and Citrix_ICA_Browsing UDP services. The Citrix_ICA service initializes the stateful inspection of the Citrix ICA protocol. The Citrix_ICA service is not included in the Any service of the Security Policy and must therefore be enabled in one of these ways:

In the Security tab add a rule to your Security Policy with the Citrix_ICA TCP service. Similarly, add a rule for the Citrix_ICA_Browsing service. Alternatively, you can add simply add the Citrix_metaFrame group, which incorporates both the Citrix_ICA TCP and Citrix_ICA_Browsing UDP services.

Or:
1. Expand the TCP branch of the Services Tree.
2. Double-click on the Citrix_ICA service.
   The TCP Service Properties - Citrix_ICA window opens.
3. Click Advanced.
   The Advanced TCP Service Properties window opens.
4. Select Match for Any to turn on the Citrix ICA protocol inspection without having to add a specific rule for the Citrix_ICA service (if the Any service is allowed).
Discovering Citrix ICA Application Names

To discover the Citrix ICA application name, as defined by the Citrix Administrator, use QoS to snoop the wire and send logs (of type alert) to the SmartView Tracker, recording the Citrix ICA application name. The Citrix ICA application detection is turned off by default.

- **Note** - The frequency of recording an application name log (alert) is 24 hours.

**Advanced:** If you want to reset the application detection cache in order to re log a Citrix ICA application on the wire even if it was logged in the past 24 hours use this command line instruction:

```
fw tab -t fg_new_citrix_app -x
```

**To Enable Citrix ICA Application Name Logging:**

1. Double-click on the gateway in the Network Objects Tree. The General Properties window shows.
2. Select Logs and Masters > Additional Logging in the tree on the left side of the General Properties window. The Additional Logging Configuration window shows.
3. Select Detect new Citrix ICA application names to enable QoS to log the Citrix application names.
4. Click OK.
   - Citrix ICA application name detection is enabled.
5. Create a Security Policy with a valid rule that uses the Citrix_ICA service.
   - **Note** - The QoS policy content is irrelevant to the application detection feature.
7. View the QoS log entries using SmartView Tracker (the entries are of Type Alert and contain the Citrix ICA application names). Once you have the application names you can turn off the application detection, as well as define new Citrix TCP services to use in a QoS policy.
   - **Note** - It is a pre-requisite that the Citrix_ICA TCP be enabled in the Security Policy.

**To Disable Citrix ICA Application Name Logging:**

1. Double-click on the gateway in the Network Objects Tree.
   - The Gateway - General Properties window opens.
2. Select Logs and Masters > Additional Logging.
   - The Additional Logging Configuration page opens.
3. Clear the Detect new Citrix ICA application names option so that QoS will not log the Citrix application names.
4. Click OK.
   - Citrix ICA application name detection is disabled.
5. Install the QoS Policy.

**Defining a New Citrix TCP Service**

A new service type was introduced in the SmartDashboard, Citrix TCP.

**To Define a New Citrix TCP Service**

1. Right-click on the Citrix TCP branch of the Services Tree, and select New Citrix TCP. The Citrix Service Properties window is displayed.
2. Enter the following details in the Citrix Service Properties window, as shown in the example below:
   - **Name:** The name of the new service.
   - **Comment:** A comment describing the new service.
   - **Color:** Select a color from the list.
   - **Application:** The exact name (case insensitive) of the Citrix Application.
Managing QoS

Note - The application name is case insensitive.

3. Click **OK** to create the new Citrix Class of Service.

**Adding a Citrix TCP Service to a Rule**

In QoS policy mode, you can add a Citrix TCP service to a rule in the QoS Policy. For more, see: Editing QoS Rule Bases (on page 51).

**Installing the Security and QoS Policies**

Security and QoS Policies must be installed on the gateways before the policies are enforced.

**Managing QoS for Citrix Printing**

Printing generates relatively large quantities of data, causing a TCP connection to consume excessive quantities of bandwidth. This type of connection should be identified and the bandwidth made available to these connections limited.

There are three primary methods of printing in the MetaFrame environment:

- IP Network printing
- MetaFrame Auto-Creation of printers
- Local MetaFrame printing.

The QoS policy solution for printing traffic using the MetaFrame Auto-creation method is to classify each ICA connection as a printing or a non-printing connection.

A connection that is classified as printing is assigned to a Citrix printing rule. This rule can be configured to limit printing traffic and avoid excessive consumption of bandwidth. A connection that is classified as non-printing is assigned to a rule according to the regular matching method.

Classification of the connection is dynamic and is based on examining the ICA priority bits of each packet. An ICA connection is therefore matched dynamically to one of two different rules depending on the type of data passing through the connection at any point in time.

It is recommended that you limit the bandwidth per printing connection to a low value, depending on your network speed. This saves bandwidth for other traffic.

Citrix Printing rules are not supported when CoreXL or SecureXL acceleration technologies are enabled on the QoS gateway.

**Configuring a Citrix Printing Rule**

Define a printing rule to which all ICA connections that are in a printing state are assigned.

**To Configure a Citrix Printing Rule**

1. Position your cursor in the **Name** field of the **QoS** tab, at the position where you want to add a new rule.
2. Right-click and select one of the **Add Rule** options.
   - The **Rule Name** window opens.
3. Enter the rule name in the **Rule Name** field.
4. Click **OK**.
5. Right-click in the **Service** column
6. Select **Add**.
   - The **Add Object** window opens listing the network objects defined in the Security Policy and the QoS Policy.
7. Select the predefined **Citrix_ICA_printing** service.
8. Click **OK**.
9. Right-click in the **Action** column.
10. Select **Edit Properties**.
    The **QoS Action Properties** window opens.
11. Select **Advanced** in the **Action Type** area.
12. Select **Per connection limit** in the **Limit** area.
13. In the **Per connection limit** field, enter a low value.
14. Click **OK**.

**Viewing QoS Gateway Status**

This section covers viewing the QoS gateway status.

**Display QoS Gateways Configured by SmartConsole**

Use SmartView Monitor. For more, see the **R77 SmartView Monitor Administration Guide**

**Configuring QoS Topology**

When the MetaFrame Auto-Creation of printers printing method is used, the Citrix printing traffic passes
from the Citrix Server to the Citrix Client. To enforce QoS on this traffic, QoS must be installed
- On the gateway external interface on the inbound direction or
- On the gateway internal interface on the outbound direction.

**Enabling Log Collection**

In order for a connection to be logged, the QoS logging flag must be turned on and the connection’s
matching rule must be marked with either **Log** or **Account** in the **Track** field of the rule. For further
information on how QoS’s logging features work, see **Overview of Logging** (on page 70).

**To Turn on QoS Logging**

A QoS gateway logs to the log if **Turn on QoS Logging** is checked in the **Additional Logging** page (under
**Logs and Masters**) of the **Properties** window. By default, QoS Logging is turned on.

**To Confirm that the Rule is Marked for Logging**

1. Select the rule whose connection will be logged.
2. Confirm that either **Log** or **Account** appear in the **Track** field.
    See **To Modify Tracking for a Rule** (on page 58).
To Start SmartView Tracker

To start SmartView Tracker, double-click on the SmartView Tracker icon, or choose SmartView Tracker from the Window menu in the SmartDashboard window.

It is now possible to view log data according to:

- Rule Name
- Rules using DiffServ
- Control type having to do with install and uninstall logs
Chapter 6

SmartView Tracker

In This Section:

- Overview of Logging .................................................................................................. 70
- Examples of Log Events .............................................................................................. 72
- Examples of Account Statistics Logs .......................................................................... 73

This section covers SmartView Tracker

Overview of Logging

SmartView Tracker enables you to view entries in the Log File. Each entry in the Log File is a record of an event or an account record. SmartView Tracker gives you control over the information displayed in the Log File. You can navigate through the Log File and select the log entries that you would like to display. You can view the log entries for all the installed Check Point products or for a selected product, such as QoS or VPN.

Two types of events are logged. The table below describes features unique to event logs:

**SmartView Tracker Non-Accounting Log Events**

<table>
<thead>
<tr>
<th>Log Event</th>
<th>Data Returned</th>
<th>Presentation</th>
<th>Policy Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Reject</strong></td>
<td>QoS rejects a connection when the number of guaranteed connections is exceeded and/or when you have configured the system not to accept additional connections.</td>
<td>The name of the matching rule on account of which the connection was rejected.</td>
<td>Generated as a reject log. Unified with the initial connection log.</td>
</tr>
<tr>
<td><strong>Running Out of Packet Buffers</strong></td>
<td>One of the interface-direction's packet buffers is exhausted. A report is generated a maximum of once per 12 hours.</td>
<td>A string explaining the nature of the problem and the size of the relevant pool.</td>
<td>New log record created each time a global problem is reported.</td>
</tr>
<tr>
<td><strong>LLQ Packet Drop</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
When a packet is dropped from an LLQ connection. A report is generated a maximum of once per 5 minutes.

The following are logged:
- Number of bytes dropped from the connection due to delay expiration
- average packet delay.
- jitter, which is computed as the maximum delay difference between two consecutive packets.

Unified with the initial connection log.

QoS policy mode only.

The next table describes the features unique to accounting logs.

**Explaining the Accounting SmartView Tracker Log**

<table>
<thead>
<tr>
<th>Logged</th>
<th>Data Returned</th>
<th>QoS policy, or Express mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Statistics</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The total bytes transmitted</td>
<td>Inbound &amp; outbound bytes transmitted by QoS.</td>
<td>Both</td>
</tr>
<tr>
<td>through QoS for each relevant</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface and direction.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Drop Policy Statistics</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total bytes dropped from the</td>
<td></td>
<td>QoS policy mode only.</td>
</tr>
<tr>
<td>connection as a result of</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QoS's drop policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Count of the bytes dropped</td>
<td></td>
<td></td>
</tr>
<tr>
<td>from the connection because</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the maximum used memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fragments for a single</td>
<td></td>
<td></td>
</tr>
<tr>
<td>connection was exceeded.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>LLQ Statistics</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statistics about the LLQ</td>
<td>The following are logged:</td>
<td>QoS policy mode only.</td>
</tr>
<tr>
<td>connection.</td>
<td>1. Number of bytes dropped from the connection due to delay expiration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Average packet delay.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Jitter which is computed as the maximum delay difference between two</td>
<td></td>
</tr>
<tr>
<td></td>
<td>consecutive packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following two conditions must be met for a connection to be logged:

- The QoS logging checkbox must be selected in the Gateway Properties - Additional Logging Configuration window (see "To Turn on QoS Logging" on page 68) must be selected. (By default this is automatically selected.)

- The connection's matching rule must be marked with either Log or Account in the Track field of the rule. See To Confirm that the Rule is Marked for Logging (on page 68) and To Modify Tracking for a Rule (on page 58).

Further information on how to start the SmartView Tracker can be found in Enabling Log Collection (on page 68).
Examples of Log Events

This section describes the log events in SmartView Tracker.

**Connection Reject Log**

The connection is rejected because the rule exceeds the number of guaranteed connections, where *Accept additional non-guaranteed connections* is unchecked in the QoS Action Properties window (see QoS Action Properties (on page 20)). The log will include the name as well as the class of the rule in the following format: `rule_name:<class>-><name>`.

In the following example, the rule belongs to the class Best_Effort. The name of the rule (rule_name) is udp2.

**Connection Reject Log — Example**

<table>
<thead>
<tr>
<th>Time</th>
<th>Product</th>
<th>Interface</th>
<th>Type</th>
<th>Action</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:17:09</td>
<td>QoS</td>
<td>daemon log</td>
<td>log</td>
<td>reject</td>
<td><code>rule_name:Best_Effort-&gt;udp2</code></td>
</tr>
</tbody>
</table>

**LLQ Drop Log**

When a packet from the LLQ connection is dropped, LLQ information is computed and logged from the last time a log was generated. This information includes significant data logged from the relevant interface-direction. In the following example, the information logged includes:

- `s_in_llq_drops`: The number of bytes dropped from the connection on the Server-In interface direction.
- `s_in_llq_avg_xmit_delay`: The average delay computed for all the connection's packets that were not dropped on the Server-In interface direction.
- `s_in_llq_max_delay`: The maximum delay of a connection packet that was not dropped on the Server-In interface direction.
- `s_in_llq_xmit_jitter`: The maximum delay difference between two consecutive successfully transmitted packets of the connection on the Server-In interface direction. Any packets which are dropped in between the two successfully transmitted packets are ignored.
- `s_in_llq_recommended_delay`: The default delay that can be entered into the Add Low Latency QoS Class Properties window in order to achieve a minimal number of dropped bytes.

**LLQ Drop Log — Example**

<table>
<thead>
<tr>
<th>Product</th>
<th>Type</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS</td>
<td>log</td>
<td><code>s_in_llq_drops:3000</code>&lt;br&gt;<code>s_in_llq_avg_xmit_delay: 900</code>&lt;br&gt;<code>s_in_llq_max_delay: 1351</code>&lt;br&gt;<code>s_in_llq_xmit_jitter: 1351</code>&lt;br&gt;<code>s_in_llq_recommended_delay:2000</code></td>
</tr>
</tbody>
</table>

In the above example relevant data was observed only on the Server-In interface direction, therefore only Server-In counters are available.

**Note** - There are several reasons why logging might not occur on a specified interface direction:

- QoS might not be installed on all the interfaces directions.
- No packets were seen on other interface directions.
- Data on other interface directions might not be significant, for instance, the values logged might be zero.
**Pool Exceeded Log**

A log for when the designated size of the ifdir pool is exceeded. In this example, the log shows:

- An interface direction (ifdir) has a pool size of 8 fragments.
- The interface name is **E100B1**, and the direction is outbound (outbound shown by the cube with an outward pointing arrow).

**Pool Exceeded Log — Example**

<table>
<thead>
<tr>
<th>Product</th>
<th>Interface</th>
<th>Type</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS</td>
<td>E100B1</td>
<td>control</td>
<td>info:Ifdir Memory Pool Exceeded Pool_size:8</td>
</tr>
</tbody>
</table>

**Examples of Account Statistics Logs**

In SmartView Tracker, the account logs always include the *segment_time* information (the time from which the information about the log was gathered) in the *Information* column.

**The Mandatory Fields in Account Logs**

<table>
<thead>
<tr>
<th>Product</th>
<th>Type</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS</td>
<td>Account</td>
<td>segment_time 8May2002 12:24:57</td>
</tr>
</tbody>
</table>

Account Logs may include any or all of the above information:

- Only significant data is logged and presented in the same log record.

**General Statistics Data**

These statistics include the number of bytes transmitted through QoS in any relevant interface direction. In the following example:

- **s_in_bytes**: 5768 bytes were transmitted through QoS on the Server-In interface direction.
- **s_out_bytes**: 154294 bytes were transmitted through QoS on the Server-Out interface direction.

**General Statistics Data — Example**

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>s_in_bytes:5768 s_out_bytes: 154294</td>
</tr>
</tbody>
</table>

**Drop Policy Statistics Data**

The number of bytes dropped from the connection in any relevant interface direction as a result of drop policy are logged. The drop policy is aimed at managing QoS packet buffers, see WFRED (Weighted Flow Random Early Drop). This includes the total number of bytes dropped from the connection since it exceeded its allocation. In the following example:

- **s_out_total_drops**: 3914274 bytes were dropped from the connection as a result of drop policy, on the Server-Out interface direction.
- **s_out_exceed_drops**: Out of total number of drops (**s_out_total_drops**) 3914274 bytes were dropped from the connection because it exceeded its allowed number of fragments, on the Server-Out interface direction.

**Drop Policy Statistics Data — Example**

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>s_out_total_drops:3914274 s_out_exceed_drops: 3914274</td>
</tr>
</tbody>
</table>
**LLQ Statistics Data**

Data items are the same as in LLQ Drop Log (on page 72), but are generated from the beginning of the connection, *not* from the last time a log was created.
Chapter 7

Command Line Interface

In This Section:

- QoS Commands ................................................................. 75
- Setup ......................................................................................... 75
- fgate Menu .............................................................................. 76
- Control ..................................................................................... 76
- Monitor ..................................................................................... 77
- Utilities ..................................................................................... 78

## QoS Commands

<table>
<thead>
<tr>
<th>QoS Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>etmstart</td>
<td>Starts QoS</td>
</tr>
<tr>
<td>etmstop</td>
<td>Stops QoS</td>
</tr>
<tr>
<td>fgd50</td>
<td>QoS daemon</td>
</tr>
</tbody>
</table>

**Note:** On Windows gateways, running `etmstop` can result in this error message: *The Check Point FloodGate-1 service could not be stopped.* This is caused by a too-short Windows service check timeout, not `etmstop` failure. To resolve, run `etmstop` again.

## Setup

**cpstart and cpstop**

Generally, to stop and start the QoS gateway you are required to stop the Firewall using the `cpstop` and `cpstart` commands. In the event that you would like to stop the QoS gateway only, you can use the QoS specific `etmstart` and `etmstop` commands.

For more on cpstop and cpstart, see the *R77 Security Management Administration Guide* ([http://supportcontent.checkpoint.com/documentation_download?ID=24830](http://supportcontent.checkpoint.com/documentation_download?ID=24830)).

**etmstart**

`etmstart` loads the QoS gateway, starts the QoS daemon (`fgd50`), and retrieves the last policy that was installed on the QoS gateway.

**etmstop**

`etmstop` kills the QoS daemon (`fgd50`) and then unloads the QoS Policy and gateway.
fgate Menu

Typing `fgate` on the command line shows this menu:

```
# fgate
Usage:
fgate load <rules-file.F> [targets]  # install targets
fgate unload [targets]               # uninstall targets
fgate fetch [-f | servers]          # fetch last policy installation
fgate stat [targets]                # display status
fgate ver [-k]                      # display version
fgate log [args]                    # control logging
fgate debug <on | off>              # control daemon debug
fgate kill [-t sig_no] procname     # send signal to FloodGate-1 daemon
fgate fetch_robo [servers]          # fetch the robo-cluster policy

[targets] and [servers] are lists of host names or IP addresses. Specifying no target performs the operation locally.
```

Control

`fgate`

The `fgate` program is used to manage QoS. Its specific action is determined by the first command line argument, as described in the following sections:

**fgate load**

`fgate load` runs a verifier on the policy file. If the policy file is valid, `fgate` compiles and installs a QoS Policy to the specified QoS gateways. It can only be run from the Security Management Server.

1. **Syntax**
   ```
   fgate load <rule-file.F> [targets]
   ```

If `targets` is not specified, the QoS Policy is installed on the local host.

**fgate unload**

`fgate unload` uninstalls a QoS Policy from the specified QoS gateways. It can only be run from both the Security Management Server and localhost.

1. **Syntax**
   ```
   fgate unload [targets]
   ```

If `targets` is not specified, the QoS Policy is uninstalled from the local host.

**fgate fetch**

`fgate fetch` retrieves the QoS Policy that was last installed on the local host. You must specify the machine where the QoS Policy is found. Use "localhost" in case there is no Security Management Server or if the Security Management Server is down. You may specify a list of Security Management Servers, which will be searched in the order listed.

`fgate fetch -f` attempts to retrieve policies from all management stations, one after the other until it succeeds. If the gateway fails to retrieve a policy from a Security Management Server, it tries to retrieve one from itself.
Syntax

fgate fetch [-f | servers]

Examples

fgate fetch localhost
fgate fetch -f
fgate fetch mgmt_server_name

Monitor

fgate stat

fgate stat displays the status of target hosts in various formats. If this command is launched from a Security Management Server, it can be run on more than one gateway. If this command is launched from a gateway, the status of the gateway is returned.

Usage

fgate stat [targets]

The default format displays the following information for each host: product, version, build number, policy name (QoS policy mode, or Express mode), install time and interfaces number.

If no target is specified, the status of localhost is shown. For example:

```
# fgate stat

Blade:          QoS
Version:        R77.10
Kernel Build:   11
Policy:    Standard
Install time:   Wed Oct 23 12:30:33 2013
Interfaces Num: 1

Interface table
---------------------
|Name| Dir| Limit (Bps)| Avg Rate (Bps)| Conns| Pend pkts| Pend bytes|
---------------------
|eth0| in | 5625000|    0|  3|     0|     0|
|eth0| out| 5625000|   58|  2|     0|     0|
```

Examples

fgate stat
fgate stat gateway1 gateway2

fgate ver

fgate ver displays the QoS version number. If the -k option is included, both the kernel version build number and QoS executable version build number are returned. Without the -k, only the QoS executable version is specified.

Syntax

fgate ver [-k]
Utilities

fgate log

fgate log turns logging on or off in the kernel. It can be used in order to save resources without reinstalling your QoS policy. The stat option returns the current state of logging.

Syntax

fgate log < on | off | stat >

By default, fgate log is turned on.

fgate debug

fgate debug turns on a debug flag which sends additional debugging information to the fgd log file: $FGDIR/log/fgd.elg. The default is off.

Syntax

fgate debug < on | off >

fgate kill

fgate kill sends a signal to a QoS daemon. The Security Management Server does not run the QoS daemon therefore this command is valid only on gateways.

Syntax

fgate kill [-t sig_no] proc-name

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>[-t sig_no] proc-name</td>
<td>If the file $FWDIR/tmp/&lt;proc-name&gt;.pid exists, send sig_no to the PID in the file. If no signal is specified, signal 15 (sigterm) is sent.</td>
</tr>
</tbody>
</table>

The QoS daemon writes the PIDs to files in the log directory upon startup. These files are named $FWDIR/tmp/<daemon_name>.pid. For example, the file containing the PID of the QoS SNMP daemon is $FWDIR/log/snmpd.pid.

Examples

<table>
<thead>
<tr>
<th>Commands</th>
<th>Example and Description</th>
</tr>
</thead>
</table>
| fgate kill | • fgate kill fgd
Sends signal 15 to the QoS fgd daemon.
• fgate kill -t 1 fgd
Sends signal 1 to the QoS fgd daemon. |
| fgate fetch_robo | • fgate fetch_robo Fetches the local robo-cluster policy
• fgate fetch_robo [server] Fetches the robo-cluster policy from the given server |
QoS Basics

When should I use QoS policy mode and when should I use Express mode?

- Use QoS policy mode to fine-tune functionality and enhanced QoS features while using acceleration
- Express mode should be selected if your system requires only basic QoS

What are the benefits of using each mode?

- QoS policy mode gives optimal QoS functionality
- Express policy mode remains available as a legacy mode

Can I change between QoS modes?

- You can change from Express mode to QoS policy mode
- You cannot change from a QoS policy mode to Express mode

What is the highest weight I can use in a rule? — Weights are relative. The only limitation is the Maximum weight of rule parameter, which is defined in the Global Properties window under QoS. The default parameter is 1000, but can be changed to any number.

Note - This parameter is only used to assist in input validation.

In the example shown here:

<table>
<thead>
<tr>
<th>Policy 1</th>
<th>HTTP gets</th>
<th>and equals</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP weight = 500, FTP weight = 500</td>
<td>500/(500+500)</td>
<td>= ½</td>
<td>Equal weight is given to each rule.</td>
</tr>
</tbody>
</table>

Policy 2

| HTTP weight = 2, FTP weight = 2 | 2/(2+2) | = ½ | Equal weight is given to each |

Policy 1 + third rule
FAQ

Policy 1

<table>
<thead>
<tr>
<th>HTTP gets</th>
<th>…and equals</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP weight = 500, FTP weight =500, SMTP weight = 100</td>
<td>500/(500+500+100)</td>
<td>= 500/1100</td>
</tr>
</tbody>
</table>

Policy 2 + third rule

<table>
<thead>
<tr>
<th>HTTP gets</th>
<th>…and equals</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP weight = 2, FTP weight =2; SMTP weight = 100</td>
<td>2/(2+2+100)</td>
<td>= 2/104</td>
</tr>
</tbody>
</table>

You can see the significance of the value of the weight allocated in two different policies. In the example both the HTTP and FTP connections initially enjoy an equal share of the available bandwidth, although they each had a weight of 500 in Policy 1 and a weight of 2 in Policy 2.

By adding a third rule to both policies you can significantly change the result. For example, an SMTP connection with a weight of 100 can be added to each policy. Due to the high initial weights used in Policy 1, there is an insignificant change to the amount of bandwidth available for the HTTP connection in Policy 1 + third rule. However, due to the low initial weights used in Policy 2, the amount of bandwidth that is available to the HTTP connection in Policy 2 + third rule is significantly reduced.

Should I install QoS on the external or the internal interface? — While QoS can run on both interfaces, it is highly recommended to position QoS on the external interface only.

What is the difference between guarantees and weights? — Guarantees and weights are similar in their behavior. Despite the difference in their dictionary meaning, they both guarantee the allocated bandwidth to the matched traffic. The differences between them are:

- Guarantees are stated in absolute numbers (for example, 20000bps) and weights are stated in relative numbers (for example, 100).
- Guarantees are allocated their share of bandwidth before weights. For example if you have a link of 1.5 MB:

Your Rule Base is:

- HTTP Guarantee 1Mb
- FTP Weight 40
- SMTP Weight 10

The result is:

- first 1 MB for HTTP is allocated, then
- 0.4 MB for FTP is allocated and 0.1MB for SMTP is allocated.

Use guarantees to define bandwidth in absolute terms or for per connection guarantees.

Which Firewall resources does QoS support in the Rule Base? — QoS can use its resources to inspect HTTP traffic. Resources are defined using the URI for QoS option and can contain specific URLs or files. For example, to restrict web surfing to http://www.example.com add a QoS URI resource that looks for the string "www.example.com" (without http://). Then use the resource in a QoS rule and add a limit.

Do guarantees waste bandwidth? — No. QoS uses a sophisticated queuing mechanism. An application only takes as much bandwidth as it needs. Any unused bandwidth is then available for use by other applications.

How do I know if loaned bandwidth is available for applications that may need it back? — There is no loaned bandwidth in QoS. Bandwidth that is not utilized by a guarantee/weighted rule is immediately (on a per-packet basis) distributed to the other connections, according to their relative priorities. The important
thing to remember is Resolution (referring to level of granularity). QoS allocates bandwidth on a per packet basis. Therefore, only one packet is allocated at a time, resulting in the most accurate scheduling policy.

Other Check Point Products - Support and Management

Where is QoS placed in the Multi-Domain Security Management Inspection chain? — QoS is composed of two components:

- QoS Policy, which is in charge of rule matching
- QoS Scheduling, which is in charge of packet scheduling

Does QoS work With Multi-Domain Security Management? — Yes. One of QoS's most important features is its unique and sophisticated integration with Multi-Domain Security Management. Its integration features include:

- accurate classification of VPN traffic (inside the VPN tunnel)
- classification of NATed traffic
- shared network objects and topology (that save you time and effort in administration)
- common SmartDashboard with an advanced GUI but a familiar look and feel
- authenticated Quality of Service allows you to assign bandwidth to VPN remote users
- DiffServ Support and QoS bring Better than Frame Relay QoS to the VPN world
- log verification

Is SmartView Monitor a part of QoS? — No. As of NG with Application Intelligence (R55), SmartView Monitor is a separate product that is bundled with QoS.

Does QoS support Load Sharing configurations? — Yes, QoS supports all ClusterXL configurations. QoS supports the SYNC mechanism and therefore can be used with CPLS/CPHA or third-party solutions. For OPSEC partner solutions, see the OPSEC Website.

Does QoS support NATed traffic? — QoS has full support for NATed traffic, including matching, scheduling, limiting and all other QoS features.

What is the maximum number of QoS gateways I can manage? — QoS gateway management is identical to that for any gateway. Thus, the maximum number of gateways is identical to the maximum number of gateways that are managed.


Policy Creation

When should I use LLQ (Low Latency Queuing)? — LLQ is best suited for VoIP applications, Video conferencing and other multimedia applications. LLQ is targeted for applications where:

- a minimal guaranteed bandwidth is required for adequate performance
- low delay and Jitter are required

Is QoS Rule Base "first match"? — From QoS NG forward, all QoS rules are matched on the "first match" principle. Meaning that only the first rule that applies to a connection is activated.

For example, if you have a rule for CEO traffic and a rule for HTTP traffic, the rule that appears first within the Rule Base will be matched to all CEO surfing.

Correct Rule Base (CEO is the first match)
1. SRC=CEO => Guarantee = 128Kbps
2. Service=HTTP => Limit = 64Kbps

Incorrect Rule Base (CEO traffic will be limited)
1. Service=HTTP => Limit = 64Kbps
2. SRC=CEO => Guarantee = 128Kbps
FAQ

I am using QoS on multiple gateways. What is the best way to organize my Rule Base?

- If you are managing gateways with identical bandwidth and you want an identical policy for all gateways, define as All in the Install On field.
- If you are managing gateways with varied bandwidths and want an identical policy for all gateways, you can have one policy installed on all gateways. It is best to use weights since they assign relative bandwidth and not a fixed one. Remember that weights also guarantee bandwidth allocation.
- If you are managing gateways with varied bandwidths and want a different policy for all gateways, you can use different sub-rules for each gateway. You can also use common rules that are matched for gateways.

When should I use Sub-rules? — Sub-rules should be used when there is hierarchy between objects. For example, when you want to manage bandwidth according to organizational structure, such as within an organization that has R&D, Marketing and operation divisions.

How can I see the top bandwidth-hogging applications? — From the command line run the command rtmtopsvc.

Fine-tuning QoS Performance

To fine-tune QoS performance:
1. Upgrade to the latest R77.10 Security Gateway.
2. Enable acceleration ("Enabling QoS Acceleration Support" on page 11).
3. In most cases you need to install QoS only on the external interfaces of the gateway.
4. Unless you are using limits for outbound traffic, install QoS only for the inbound direction.
5. Put more frequent rules at the top of your Rule Base.
6. Turn per connection limits into per rule limits.
7. Turn per connection guarantees into per rule guarantees.

Protocol Support

What protocols/services are supported by QoS? — See: http://www.checkpoint.com/products/downloads/vpn-1_fw-1_fg-1_app_support.pdf

Note - New services and applications are added on a permanent basis.

Can I prioritize system administration traffic? — Yes. This can be done in any of the following ways:

- Guarantees for administrators based on authentication
- Guarantees for administrators based on IPs, networks
- Guarantees for applications only administrators use (for example, Multi-Domain Security Management control protocols, PC-Anywhere)
- Combinations of all the above

Does QoS support Citrix applications? — Yes. In addition:

- Citrix applications can be differentiated from one another.
- QoS identifies Citrix ICA printing traffic and reclassifies it to a proper rule.

Does QoS support SIP? — Yes. Starting from QoS FP2, the SIP protocol is supported.

Does QoS support H323? — Yes. Starting from QoS FP1, the H323 protocol is supported.

Does QoS support GRE? — Yes. This protocol is supported.
Installation/Backward Compatibility/Licensing/Versions

**When will QoS next feature pack be available?** — QoS feature packs/releases are usually shipped at the same time Multi-Domain Security Management feature packs are released.

**How do I?**

**How do I guarantee performance for my mail server?** — You need to add a rule matching your email traffic. You can do this by either matching the source/destination of your mail server, or matching mail protocols (SMTP, POP3, Exchange). For this rule, define a weight or guarantee that meets the needs of the priorities you want to set.

**How do I ensure Quality of Service for Voice Over IP?** — QoS FP1 introduced the VoIP-tuned mechanism Low Latency Queuing (LLQ). This mechanism is tuned to achieve best latency for constant bit rate applications, like VoIP.

To limit the number of connections admitted, use LLQ with a per connection guarantee. For voice, you want to give each conversation a guaranteed bandwidth. Usually you would want an admission policy that does not accept additional calls if bandwidth is not adequate.

**Note** - This is equivalent to the busy tone in old voice system.

**How can I prioritize traffic for remote users?** — Using the Authenticated QoS feature of QoS, you can prioritize bandwidth allocation for remote VPN users and Windows domain user groups.

**How do I guarantee performance for my ERP applications?** — You need to add a rule matching your ERP traffic. You can do this by either matching the source/destination of your ERP server, or matching application protocols (SAP, BAAN, ORACLE). For this rule, define a weight or guarantee that meets the needs of the priorities you want to set. If your ERP application is not a predefined service, you can either add it manually or use the first method.

If you are using ERP over HTTP, check “How can I provide bandwidth for my intranet applications”?

**Can I use QoS to prevent Denial of Service Attacks?** — QoS's main goal is not an Anti-Denial of Service tool. However, there are many situations in which QoS can be used to detect, monitor and prevent such attacks. Using SmartView Monitor and QoS you can perform detection and monitoring.

Prevention can be achieved in the following ways:

- by limiting applications that are known to be a part of DOS attacks (for example, ICMP, suspicious URLs).
- by providing guarantees for important traffic (for example, ERP, MAIL, VoIP).
- by providing guaranteed bandwidth for authenticated users using Authenticated QoS. Authenticated users can be identified with digital signatures and can rely on VPN authentication and encryption. QoS guarantees that these users will get their bandwidth. The attacker cannot authenticate to the VPN and will not get bandwidth for the attack.

**Why is limiting bandwidth for Napster better than blocking it?** — Blocking “non-work related” applications might cause users to find a way to bypass blocking. Prioritizing bandwidth lets users continue with their activities without damaging critical business processes. Consider a university where the Internet connection is being used for peer-to-peer file downloads like Napster and Kazaa. Blocking these services completely may encourage the students find a smart way to bypass the block, which in turn might cause legal problems. QoS offers smarter solutions:

- Limiting the allocated bandwidth for such applications – this can be done with or without the students' knowledge.
- Limiting the allocated bandwidth during daytime, and providing more bandwidth at night.
- Providing guarantees to important users (Professors, MIS) while allowing students to use the reminder of the bandwidth.
**General Issues**

**My machine is experiencing certain technical failures. What should I do?** — Check the Web for updated release notes on known issues and limitations. Contact your vendor for further support.

**I set up a guarantee/limit but in SmartView Monitor it seems to be broken?** — If you are looking at very low traffic limit (for example, 1000 Bytes per second) at a high frequency (update every 2 seconds) it might look, as if the limit is broken since QoS does not fragment packets. If you lower the sampling frequency of SmartView Monitor (update every 8 seconds) you will see that limits are kept.

**Can QoS prompt a user for authentication in order to use the Authenticated QoS feature?** — No. In order to use Authenticated QoS, Multi-Domain Security Management must perform an authentication session prior to the classification of the connection by QoS.

**Can I deploy QoS on LAN environments?** — Yes. You will need to position the hardware to support the network traffic you want to prioritize. QoS is best deployed in congestion points for network traffic.

**What happens if a line’s bandwidth (as defined in the QoS tab of the Interface Properties window) is less than its physical (“real”) bandwidth?** — QoS will only allocate as much bandwidth as is defined in the Interface Properties window. Additional bandwidth will not be allocated regardless of the physical bandwidth of the interface.

**What happens if a link bandwidth (of the link defined in QoS) is more than its physical (“real”) bandwidth?** — QoS will attempt to transmit more than the physical bandwidth allows. This can cause random traffic drops in the next hop that result in the loss of critical packets.
Chapter 9

QoS Deployment

In This Section:

Deploying QoS ........................................................................................................ 85
Sample Bandwidth Allocations ................................................................................ 87

Deploying QoS

This section covers topology restrictions.

QoS Topology Restrictions

QoS can manage up to the maximum number of external interfaces supported by the firewall, subject to these restrictions:

1. All of the traffic on a managed line must go through the gateway.
2. Each managed line must be connected (directly or indirectly via a router) to a separate physical interface on the QoS gateway. Two managed lines cannot:
   - Share a physical interface to the QoS gateway.
   - Be connected to the same router.

In this example configuration, the routers can pass traffic to each other through the hub without the QoS gateway being aware of the traffic.

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Private localnet</td>
<td>4</td>
<td>Router</td>
</tr>
<tr>
<td>2</td>
<td>QoS enabled gateway</td>
<td>5</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Hub</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number Description

1 Private localnet
2 QoS enabled gateway
3 Hub
4 Router
5 Internet
In addition, you cannot manage two lines connected to a single router since traffic may pass from one line to the other directly through the router, without the QoS gateway being aware of the traffic:

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Private localnet</td>
<td>4</td>
<td>Router</td>
</tr>
<tr>
<td>2</td>
<td>QoS enabled gateway</td>
<td>5</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Router</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

An example of a correct configuration is:

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Private localnet</td>
<td>4</td>
<td>Router</td>
</tr>
<tr>
<td>2</td>
<td>QoS enabled gateway</td>
<td>5</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Router</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sample Bandwidth Allocations

*Frame Relay Network*

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Database Server</td>
<td>4</td>
<td>T1</td>
</tr>
<tr>
<td>2</td>
<td>Web Server</td>
<td>5</td>
<td>Branch Offices</td>
</tr>
<tr>
<td>3</td>
<td>T1</td>
<td>6</td>
<td>Internet</td>
</tr>
</tbody>
</table>

The example shows that the branch offices communicate with the central site and the opposite. They do not communicate directly with each other or with the Internet except through the central site. The Web server makes important company documents available to the branch offices, but the database server supports the company's mission-critical applications.

The problem is that most of the branch office traffic is internal and external Web traffic, and the mission-critical database traffic suffers as a result. The network administrator has considered upgrading the 56K lines, but is reluctant to do so, not only because of the cost but also because upgrading would probably not solve the problem. The upgraded lines would still be filled mostly with Web traffic.

The goals are as follows:
1. Allocate the existing bandwidth so that access to the database server gets the largest share.
2. Take into account that the branch offices are connected to the network by 56K lines.

These goals are accomplished with the following Rule Base:

**Main Rules**

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 1</td>
<td>Office 1</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Limit 56KBps</td>
</tr>
<tr>
<td>Office n</td>
<td>Office n</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Limit 56KBps</td>
</tr>
<tr>
<td>Default</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
</tr>
</tbody>
</table>

Each office has sub-rules, as follows:

**Office Sub-Rules**
<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start of Sub-Rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Rule</td>
<td>Any</td>
<td>Database server</td>
<td>Database service</td>
<td>Weight 50</td>
</tr>
<tr>
<td>Web Rule</td>
<td>Any</td>
<td>Web Server</td>
<td>http</td>
<td>Weight 10</td>
</tr>
<tr>
<td>Branch Offices</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Weight 10</td>
</tr>
<tr>
<td>End of Sub Rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The sub-rules give database traffic priority over Web traffic and other traffic.

**Assumptions**

The following assumptions are made in this example:

- The problem (and its solution) apply to traffic outbound from the central site. Note that QoS shapes the branch office lines in the outbound direction only. QoS shapes inbound traffic only on directly controlled interfaces (that is, interfaces of the QoS machine).
- The central site has the capacity to handle the network's peak traffic load.
- There is no traffic between the offices.
Chapter 10

Debug Flags

In This Section:

Error and Debug Codes for QoS

Note:
- Error is turned on by default
- All commands begin with: `fw ctl debug -m fg +`

<table>
<thead>
<tr>
<th>Command Line</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>driver</td>
<td>Driver Attachment</td>
</tr>
<tr>
<td>error</td>
<td>General Error Flag</td>
</tr>
<tr>
<td>chain</td>
<td>Main Steps Of QoS Packet Processing</td>
</tr>
<tr>
<td>install</td>
<td>For Future Use</td>
</tr>
<tr>
<td>pkt</td>
<td>Packet recording mechanism</td>
</tr>
<tr>
<td>citrix</td>
<td>Citrix processing</td>
</tr>
<tr>
<td>ls</td>
<td>Load sharing</td>
</tr>
<tr>
<td>tcp</td>
<td>TCP Retransmission Detection</td>
</tr>
<tr>
<td>sched</td>
<td>Packet Scheduling</td>
</tr>
<tr>
<td>policy</td>
<td>QOS Policy Rules Matching</td>
</tr>
<tr>
<td>url</td>
<td>QOS URL Matching</td>
</tr>
<tr>
<td>dns</td>
<td>DNS Related Messages</td>
</tr>
<tr>
<td>rtm</td>
<td>SmartView Monitor Interaction</td>
</tr>
<tr>
<td>auth</td>
<td>Authenticated QOS</td>
</tr>
<tr>
<td>log</td>
<td>Logging</td>
</tr>
<tr>
<td>conn</td>
<td>Connections Processing</td>
</tr>
<tr>
<td>drops</td>
<td>Drop Policy</td>
</tr>
<tr>
<td>rates</td>
<td>Reporting Rule/Connection Rates</td>
</tr>
<tr>
<td>dropsv</td>
<td>Verbose Version Of Drop Policy</td>
</tr>
<tr>
<td>Command Line</td>
<td>Usage</td>
</tr>
<tr>
<td>--------------</td>
<td>-------</td>
</tr>
<tr>
<td>timers</td>
<td>Timer Events</td>
</tr>
<tr>
<td>chainq</td>
<td>Internal Chain Q Mechanism</td>
</tr>
<tr>
<td>llq</td>
<td>Low Latency Queuing</td>
</tr>
<tr>
<td>verbose</td>
<td>Used With Other Flags - Adds More Information</td>
</tr>
<tr>
<td>automatch</td>
<td>Report Matching Process (Debug Version Only)</td>
</tr>
<tr>
<td>autosched</td>
<td>Report Scheduling Process (Debug Version Only), a good way of reporting of rates on rules</td>
</tr>
<tr>
<td>qosaccel</td>
<td>Report SecureXL related data to QoS</td>
</tr>
<tr>
<td>multik</td>
<td>Report CoreXL related data to QoS</td>
</tr>
</tbody>
</table>
Appendix A

Regular Expressions

In This Appendix

Regular Expression Syntax ................................................................. 91
Using Non-Printable Characters ......................................................... 92
Using Character Types ................................................................. 92

Regular Expression Syntax

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Backslash</td>
<td>escape metacharacters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>non-printable characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>character types</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square Brackets</td>
<td>character class definition</td>
</tr>
<tr>
<td>( )</td>
<td>Parenthesis</td>
<td>subpattern, to use metacharacters on the enclosed string</td>
</tr>
<tr>
<td>{min[,max]}</td>
<td>Curly Brackets</td>
<td>min/max quantifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n} - exactly n occurrences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n,m} - from n to m occurrences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n,} - at least n occurrences</td>
</tr>
<tr>
<td>-</td>
<td>Dot</td>
<td>match any character</td>
</tr>
<tr>
<td>?</td>
<td>Question Mark</td>
<td>zero or one occurrences (equals {0,1})</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>zero or more occurrences (equals {0,})</td>
</tr>
<tr>
<td>+</td>
<td>Plus Sign</td>
<td>one or more occurrences (equals {1,})</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vertical Bar</td>
</tr>
<tr>
<td>^</td>
<td>Circumflex</td>
<td>anchor pattern to beginning of buffer (usually a word)</td>
</tr>
<tr>
<td>$</td>
<td>Dollar</td>
<td>anchor pattern to end of buffer (usually a word)</td>
</tr>
<tr>
<td>-</td>
<td>hyphen</td>
<td>range in character class</td>
</tr>
</tbody>
</table>

Note for the asterisk:

- When using regular expressions, the asterisk is a metacharacter that means zero or more instances of the preceding character.
- When not using regular expressions, the asterisk is a wildcard, for any character, zero or more number of instances.

For example, to block any domain that ends with "example.com" (such as www.example.com)
Regular Expressions

For a regular expression enter: \*.example\.com
For a wildcard enter: *.example.com

Using Non-Printable Characters
To use non-printable characters in patterns, escape the reserved character set.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\a</td>
<td>alarm; the BEL character (hex 07)</td>
</tr>
<tr>
<td>\cx</td>
<td>&quot;control-x&quot;, where x is any character</td>
</tr>
<tr>
<td>\e</td>
<td>escape (hex 1B)</td>
</tr>
<tr>
<td>\f</td>
<td>formfeed (hex 0C)</td>
</tr>
<tr>
<td>\n</td>
<td>newline (hex 0A)</td>
</tr>
<tr>
<td>\r</td>
<td>carriage return (hex 0D)</td>
</tr>
<tr>
<td>\t</td>
<td>tab (hex 09)</td>
</tr>
<tr>
<td>\ddd</td>
<td>character with octal code ddd</td>
</tr>
<tr>
<td>\xhh</td>
<td>character with hex code hh</td>
</tr>
</tbody>
</table>

Using Character Types
To specify types of characters in patterns, escape the reserved character.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\d</td>
<td>any decimal digit [0-9]</td>
</tr>
<tr>
<td>\D</td>
<td>any character that is not a decimal digit</td>
</tr>
<tr>
<td>\s</td>
<td>any whitespace character</td>
</tr>
<tr>
<td>\S</td>
<td>any character that is not whitespace</td>
</tr>
<tr>
<td>\w</td>
<td>any word character (underscore or alphanumeric character)</td>
</tr>
<tr>
<td>\W</td>
<td>any non-word character (not underscore or alphanumeric)</td>
</tr>
</tbody>
</table>
Index

A
Action Type • 20
Adding a Citrix TCP Service to a Rule • 67
Adding Comments to a Rule • 60
Advanced • 20
Advanced QoS Policy Management • 35
Assumptions • 88
Authenticated QoS • 43

B
Bandwidth Allocation and Rules • 19
Bandwidth Allocation and Sub-Rules • 21
Basic Architecture • 12
Basic Policy Management • 17
Building and Installing a QoS Policy • 25
Burstiness • 7

C
CA • 7
Calculating Maximal Delay • 40
Calculating Constant Bit Rate • 40
Calculating the Correct Constant Bit Rate and Maximal Delay • 40
Certificate • 7
Changes in Cluster State • 46
Check Point's QoS Solution • 8
Citrix MetaFrame • 7
Citrix MetaFrame Support • 43
Classifying Traffic by Service • 30
Classifying Traffic by Service and Source • 32
Classifying Traffic by Source • 31
Client-Server Interaction • 15
Cluster State • 46
Command Line Interface • 75
Conclusion • 48
Concurrent Sessions • 15
Configuring a Citrix Printing Rule • 68
Configuring QoS Topology • 68
Connection Classification • 18
Connection Reject Log • 72
Control • 76
cpstart and cpstop • 75
Creating a Rule Base • 29

D
Debug Flags • 89
Default Rule • 20
Define the QoS Properties for the Interfaces • 29
Defining a New Citrix TCP Service • 67
Defining Interfaces on the Gateway • 27
Defining QoS Global Properties • 49
Defining Sub-Rules • 61
Defining the Network Objects • 26
Defining the Services • 29
Deploying QoS • 85
Determining QoS Policy • 26
Differentiated Services (DiffServ) • 38
DiffServ Markings for IPSec Packets • 38
Disabling Session Sharing • 65
Discovering Citrix ICA Application Names • 66
Display QoS Gateways Configured by SmartConsole • 68
Drop Policy Statistics Data • 73

E
Editing QoS Rule Bases • 51
Enabling Log Collection • 68
Enabling QoS Acceleration Support • 11
Error and Debug Codes for QoS • 89
etmstart • 75
etmstop • 75
Example of a Rule Matching VPN Traffic • 21
Example of Rates Calculation • 47
Example: • 21, 37
Examples • 77, 78
Guarantees and Limits • 35
Examples of Account Statistics Logs • 73
Examples of Log Events • 72

F
FAQ • 79
Features and Benefits • 9
fgate • 76
fgate debug • 78
fgate fetch • 76
fgate kill • 78
fgate load • 76
fgate log • 78
fgate Menu • 76
fgate stat • 77
fgate unload • 76
fgate ver • 77
Fine-tuning QoS Performance • 82
First Rule Match Principle • 32
Frame Relay Network • 87

G
General Issues • 84
General Statistics Data • 73
Guarantee - Limit Interaction • 37
Guarantees • 19
Guarantees and Limits • 32

H
How do I? • 83

I
Implementing the Rule Base • 22
Important Information • 2
Installation/Backward Compatibility/Licensing/Versions • 83
Installing a QoS Policy • 34
Installing Check Point Gateways • 25
Installing the Security and QoS Policies • 67
Intelligent Queuing Engine • 7
Interaction Between DiffServ Rules and Other Rules • 38
Interaction between Low Latency and Other Rule Properties • 42
Interaction with VPN • 15
Interface • 7
To Disable Citrix ICA Application Name Logging: • 66
To Disable Session Sharing: • 65
To Edit or Delete a Time Object for a Rule • 60
To Edit the Rule Actions • 57
To Edit, Delete, Cut, Copy or Paste a Destination in a Rule • 55
To Edit, Delete, Cut, Copy or Paste a Service in a Rule • 56
To Edit, Delete, Cut, Copy or Paste a Source in a Rule • 54
To Enable Citrix ICA Application Name Logging: • 66
To Implement DiffServ Marking • 61
To Implement Low Latency Queuing • 63
To Install and Enforce the Policy • 22
To Modify Install On for a Rule • 59
To Modify New Rules • 30
To Modify the QoS Global Properties • 49
To Modify Time in Rules • 60
To Modify Tracking for a Rule • 59
To Monitor the QoS Policy • 23
To Open an Existing Policy Package • 51
To Rename a Rule • 53
To Reset the Rule Actions to Default Values • 58
To Start SmartDashboard • 26
To Start SmartView Tracker • 69
To Turn on QoS Logging • 68
To Use Authenticated QoS • 64
To Verify and View the QoS Policy • 22
To View Sub-Rules • 61
To View Where an Object is Used • 54, 55, 57, 60

U
Uninstalling the QoS Policy • 22
Usage • 77
User Groups • 19
Using Character Types • 92
Using Non-Printable Characters • 92
Utilities • 78

V
Viewing QoS Gateway Status • 68

W
Weight • 19
WFQ • 7
WFRED • 7
When to Use DiffServ and When to Use LLQ • 43
When to Use Low Latency Queuing • 42
Workflow • 12
Working with Authenticated QoS • 64
Working with Differentiated Services (DiffServ) • 61
Working with Low Latency Classes • 63