QUANTUM

20 October 2024

QOS

R82

Administration Guide

Check Point Copyright Notice

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.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R82

For more about this release, see the R82 home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
20 October 2024	First release of this document

Table of Contents

Glossary

A

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

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

C

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

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

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

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.

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

LLQ
Low Latency Queuing is a feature developed by Cisco to bring strict priority queuing (PQ) to class-based weighted fair queuing (CBWFQ). LLQ allows delay-sensitive data (such as voice) to be given preferential treatment over other traffic by letting the data to be dequeued and sent first.

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

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

R

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
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

W

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.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.

Introduction to QoS

Important - From R81, Security Gateway also refers to a VSX Virtual System.

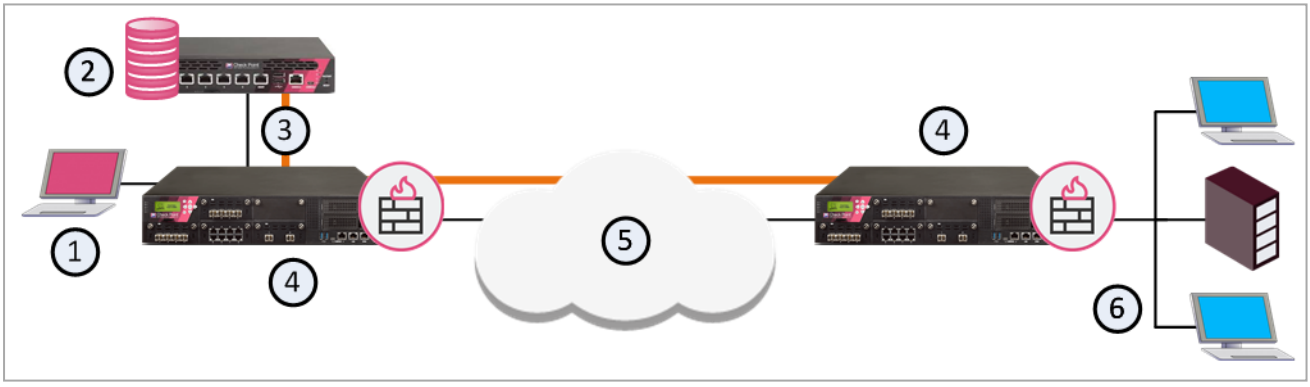
The Check Point QoS Solution

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

- Prioritize business-critical traffic, such as ERP, database and Web services traffic, over lower priority 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.

You deploy QoS with the Security Gateway.

QoS is enabled for both encrypted and unencrypted traffic.



Item	Description
1	SmartConsole
2	Security Management Server
3	QoS Policy
4	Security Gateway with QoS Software Blade
5	Internet
6	Internal network

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**

  Monitor system performance with the Logs & Events view in SmartConsole.

- **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.

- **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 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**

  Packet acceleration. IPv6 Support.

- **VSX Support**

  QoS fully supports VSX.

QoS Policy Types

This release includes two QoS Policy types:

- **Express** - Quickly create basic QoS Policies
- **Recommended** - Create advanced Policies with the full set of QoS features

This table shows the difference between the **Recommended** and **Express** policy types.

Features	Recommended	Express	To learn more
IPv6 Support	✓	✓	
Weights	✓	✓	*"Weight" on page 52*
Limits (whole rule)	✓	✓	*"Limits" on page 53*
Logging	✓	✓	*"Overview of Logging" on page 95*
Accounting	✓*	✓	
Support for hardware acceleration	✓		
High Availability and Load Sharing	✓	✓	
Guarantees (Per connection)	✓		*"Guarantees" on page 53*
Limits (Per connection)	✓		
LLQ (controlling packet delay in QoS)	✓		*"Low Latency Queuing" on page 63*
DiffServ	✓		*"Differentiated Services (DiffServ)" on page 62*
Sub-rules	✓		
Matching by URI resources	✓		
Matching by DNS string	✓		
SecureXL support	✓		
CoreXL support	✓		
SmartLSM clusters	✓		
VSX Support	✓		

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.

* You must disable SecureXL and CoreXL before you can use this feature.

To select a QoS Policy type:

1. In **SmartConsole** menu, click **Manage policies and layers**.
2. In the **Manage Policies** window, click **New** or select an existing Policy and then click **Edit**.
3. Select **QoS**, and then select **Recommended** or **Express**.

Acceleration Support for R77 Policies

After a clean install or upgrade to R82, QoS supports SecureXL and CoreXL acceleration technologies.

Important: After a clean install or upgrade, SecureXL and CoreXL are enabled by default. If you have a QoS policy created for R77 and earlier, these features *are not supported* when acceleration is enabled:

- IPSO
- Security Gateways below R77.10
- SmartView Monitor - QoS views do not correctly show traffic accelerated by SecureXL

To use these features you must disable QoS. See: *"Disabling QoS Acceleration Support" on page 124*

Workflow

This topic shows a high-level workflow for creating an effective QoS Policy.

Note: QoS must be enabled on the gateway and at least one interface for the workflow to succeed. If QoS is not enabled on at least one interface, Install Policy will fail.

Do these steps in SmartConsole:

1. Enable QoS for each applicable Security Gateway.
2. Configure QoS Global Properties.
3. Create or change a QoS Policy.
4. Configure log collection and system monitoring for QoS.
5. Publish the SmartConsole session.

Do these steps in SmartDashboard:

1. Define the gateway networks, services and other related objects.
2. Define QoS rules (basic and advanced).
3. Configure specialized QoS features.
    a. Differentiated Services (DiffServ).
    b. Low Latency Queuing.

Go back to SmartConsole to do these steps:

1. Publish the SmartConsole session.
2. Install Policy.

Note - In the SmartConsole **Install Policy** window, make sure you select **QoS**.

Limitations

These limitations apply to Scalable Platforms:

- QoS is not supported when a Security Group is configured in the Layer 4 distribution mode.
- QoS policy is applied on each Security Group Member.

Getting Started

Part 1 - Enabling QoS in the Security Gateway / Cluster Object

1. Connect with SmartConsole to the Security Management Server / Domain Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the Security Gateway / Cluster Object.
4. In the left panel, click **General Properties**.
5. On the **Network Security** tab, select **QoS**.
6. In the left panel, click **Network Management**.
7. Select and edit the applicable interface.
8. In the left panel, click **QoS**.
9. Configure the applicable QoS settings (Bandwidth, DiffServe and Low Latence classes).
10. Click **OK** to close the Interface window.
11. Click **OK** to close the Security Gateway / Cluster Object window.

Part 2 - Enabling QoS in the Policy Package

1. In the top left corner, click **Menu** > **Management policies and layers**.
2. Create a new or edit an existing policy package.
3. In the left panel, click **General**.
4. In the **Policy Types** section, select **QoS**.
5. In the **QoS** row, in the **Mode** field, select the applicable mode - **Recommended** or **Express**.
6. Click **OK** to close the **Policy** window.
7. Click **Close** to close the **Management policies and layers** window.

Part 3 - Configuring QoS Global Parameters

1. In the top left corner, click **Menu** > **Global properties**.
2. In the left panel, click **QoS**.
3. Configure the applicable settings.
4. Click **OK**.

Part 4 - Configuring QoS Policy

1. From the left navigation panel, click **Security Policies**.
2. In the **Access Control** section, click **QoS**.
3. Click **Open QoS Policy in SmartDashboard**.
4. The Legacy SmartDashboard opens in the **QoS** tab.
5. Configure the required rules.
6. In the top left corner, click **Menu** > **File** > **Update**.
7. In the top left corner, click **Menu** > **File** > **Exit**.
8. Install the Access Control policy on the Security Gateway / Cluster object.

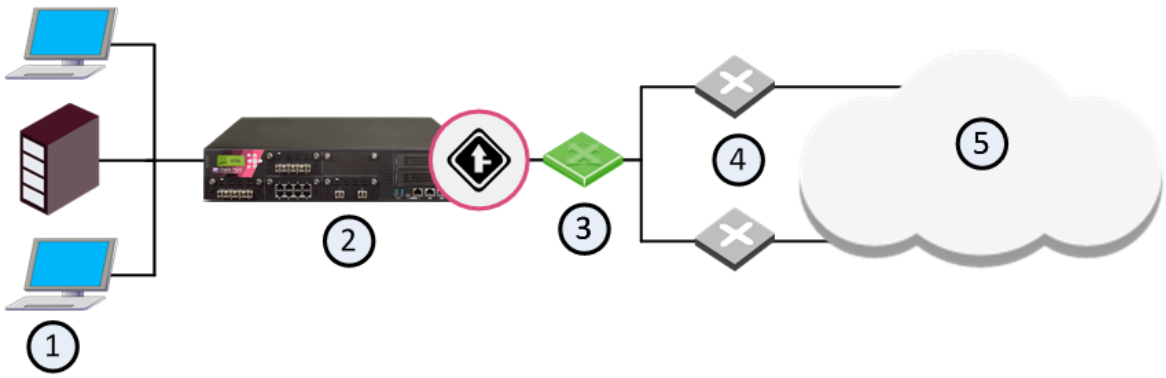
   Note - In the **Install Policy** window, make sure to select the QoS policy.

QoS Deployment

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

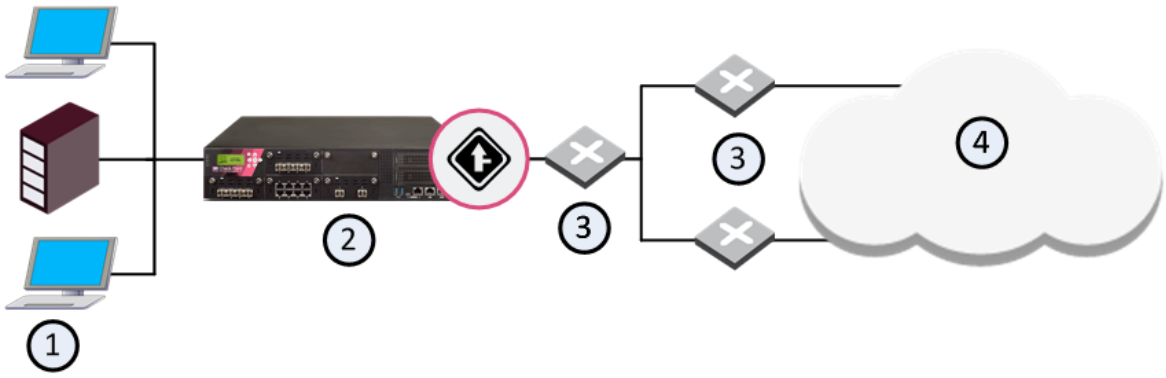
1. All of the traffic on a managed line must go through the gateway.
2. Each managed line must be connected (directly or indirectly via a router) to a separate physical interface on the QoS machine. Two managed lines cannot share a physical interface to the QoS gateway, and two network segments cannot connect to the same router.

For example, in the configuration depicted in the following diagram, the routers can pass traffic to each other through the hub without the QoS gateway being aware of the traffic.



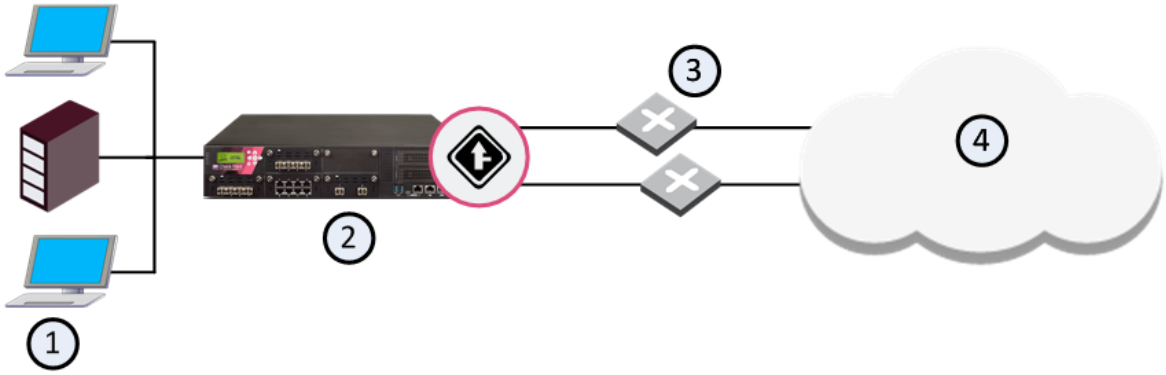
Item	Description
1	Internal network
2	Security Gateway with QoS enabled
3	Hub
4	Routers
5	Internet

You cannot manage two networks 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:



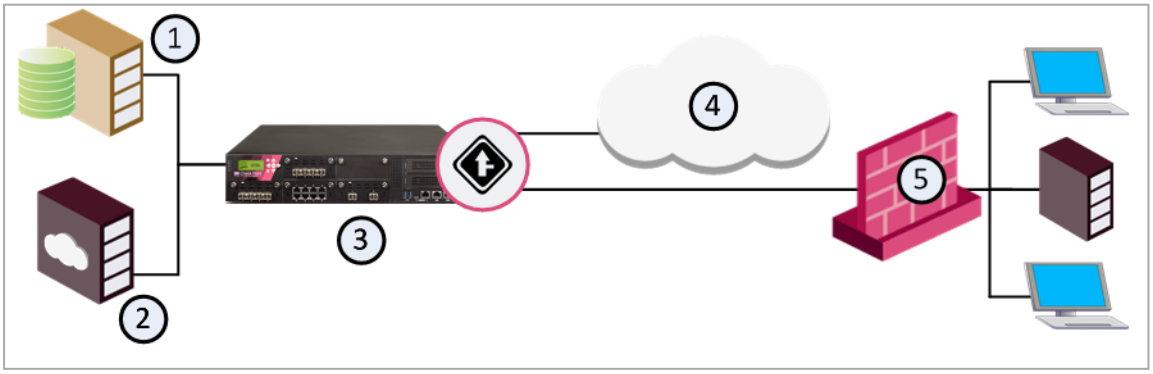
Item	Description
1	Internal network
2	Security Gateway with QoS enabled
3	Routers
4	Internet

In a correct configuration, the routers connect directly to the QoS gateway.



Sample Bandwidth Allocations

Frame Relay Network



Item	Description
1	Database server
2	Web server
3	Security Gateway with QoS enabled
4	Internet
5	Branch office

The previous diagram shows that the branch office communicates with the central site and the opposite. It only communicates directly with the Internet through the central site. The Web server makes important company documents available to the branch office, and 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

Rule Name	Source	Destination	Service	Action
Office 1	Office 1	Any	Any	Weight 10 Limit 56KBps
Office n	Office n	Any	Any	Weight 10 Limit 56KBps
Default	Any	Any	Any	Weight 10

Each office has sub-rules:

Office Sub-Rules

Rule Name	Source	Destination	Service	Action
Start of Sub-Rule				
Database Rule	Any	Database server	Database service	Weight 50
Web Rule	Any	Web Server	http	Weight 10
Branch Offices	Any	Any	Any	Weight 10
End of Sub Rule				

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 - 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.

Basic QoS 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 SmartConsole. On the Security Management Server, the policy is verified and installed on the QoS gateways. The QoS Security 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.

The QoS Blade

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 Engine

The QoS engine is the heart of QoS operations and part of Firewall-1 and SecureXL. In the QoS engine, IP packets are examined, queued, scheduled and released, a process which enables QoS traffic control.

QoS Daemon (fgd50)

The QoS daemon is a user mode process that:

- Resolves DNS for the kernel (used 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.

QoS SmartConsole

You use SmartConsole and SmartDashboard to create "bandwidth rules" for the QoS policy. Use the Logs & Events features in SmartConsole for information about the active QoS Security Gateways and their Policies.

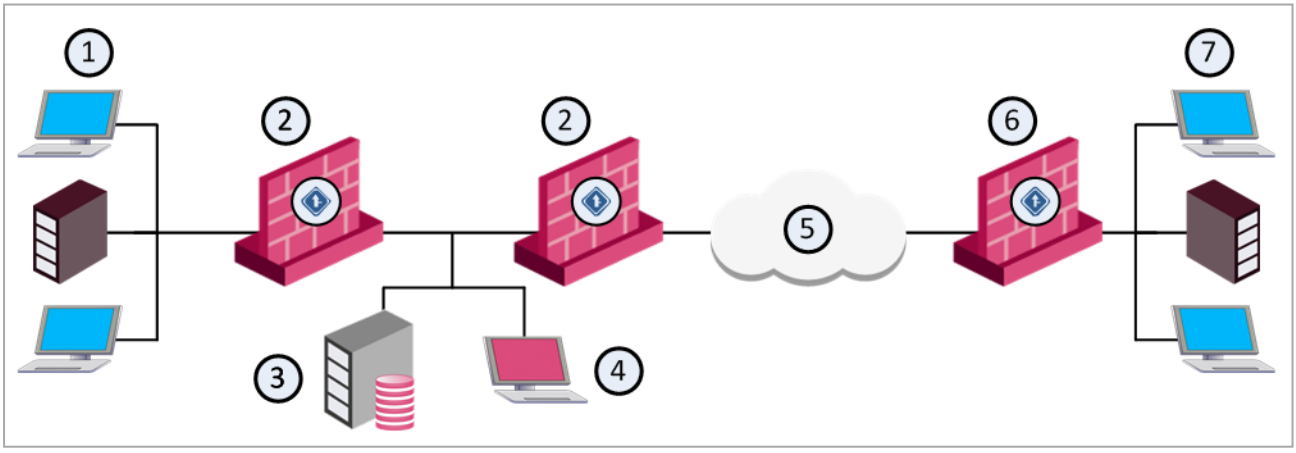
QoS SmartDashboard

Use *SmartConsole* to create and change QoS Policies. Use *SmartDashboard* to work with rules, together with their related network objects and services.

The QoS Policy rules are shown the QoS Rule Base.

QoS Configuration

The Security Management Server and the QoS Security 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.



Item	Description
1	Internal network (main office)
2	Security Gateway with QoS enabled
3	Security Management Server
4	SmartConsole

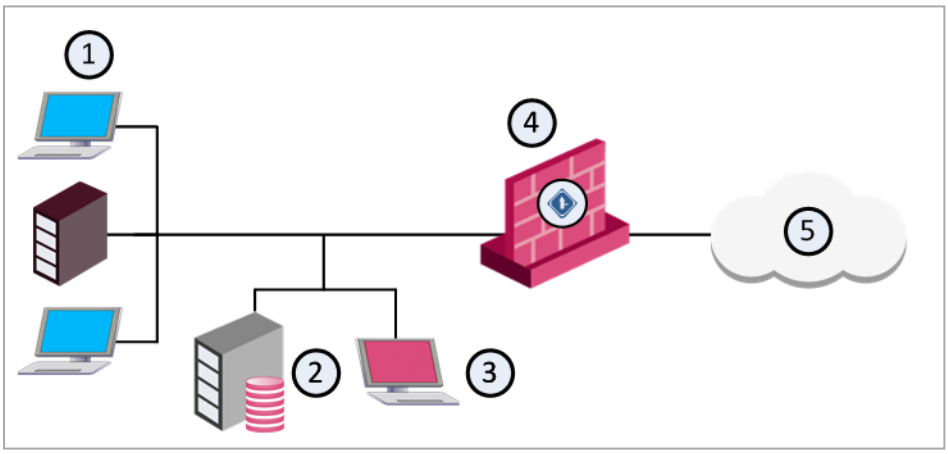
Item	Description
5	Internet
6	Security Gateway with QoS enabled (branch office)
7	Internal network (branch office)

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 Security 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.



Item	Description
1	Internal network (main office)
2	Security Management Server
3	SmartConsole
4	Security Gateway with QoS enabled
5	Internet

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 Security 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

More than one administrator can work with QoS Policies at the same time, each in a different session. A locking mechanism prevents administrators from working on the same object at one time. After you complete you work in a session, click **Publish** to make your changes available to other sessions and administrators.

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

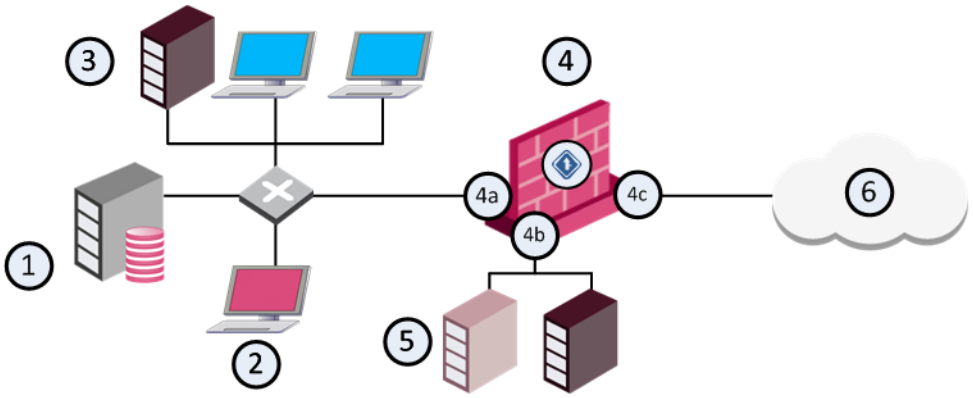
QoS uses the Security Management Server and shares the objects database (network objects, services and resources) with the firewall. Some objects have properties that are product specific. For example, the Firewall has encryption properties which are not related to QoS. A QoS network interface has speed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

QoS Tutorial

This chapter includes a step by step guide for creating a sample deployment with a QoS Policy. We recommend that you have a working knowledge of these Check Point products and concepts to use this tutorial effectively:

- Security Gateways and management servers
- Security Policies and the Rule Base
- SmartConsole and SmartDashboard
- Firewall and related Software Blades

Deployment Scenario for this Tutorial



Item	Description
1	Oxford - Security Management Server
2	Cambridge - SmartConsole client
3	Local area network - Engineering and Marketing
4	London - Security Gateway with QoS
4a	Interface eth2 - 199.199.199.32
4b	Interface eth1 - 199.32.43.32
4c	Interface eth0 - 199.32.32.32
5	DMZ with Web and FTP servers
6	Internet

This scenario is an organization with offices located in London, Oxford and Cambridge. The QoS Security Gateway is in London and has three interfaces, one of which is connected to the Internet. The Security Management Server is in Oxford and the SmartConsole is in Cambridge. The local network includes the Marketing and Engineering departments.

Tutorial Workflow

This tutorial is a simplified exercise that shows you how to do these QoS activities:

1. Install and configure the system components.
2. Create a new QoS Policy with SmartConsole.
3. Select one of these QoS Policies types:
   - **Express** - Quickly create basic QoS Policies.
   - **Recommended** - Create advanced Policies with the full set of QoS features.
4. Configure the network objects used by QoS rules.
5. Configure specialized services for use in QoS rules.
6. Create QoS Policy rules.
7. Install the Policy on the Security Gateway.

Installing the System Components

To install and configure system components for this tutorial:

1. Enable QoS, Firewall, and other Software Blades on the London Security Gateway.
2. Install a Security Management Server on the Oxford server platform.
3. Install SmartConsole on the Cambridge PC.
4. In SmartConsole, define Cambridge as a trusted client.
5. In SmartConsole, define the administrators who can manage the QoS Policy.
6. Make sure that there is the SIC trust between the Oxford Security Management Server and the London QoS Security Gateway.

Starting SmartConsole

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

To Create a New QoS Policy

1. On the gateway, make sure that the QoS blade is enabled.
2. In SmartConsole, from the **File** menu, select **Manage Policies and Layers**.
3. Click **New**.
4. In the **Policy** window, enter a Policy name.

   This name cannot:

   - Contain any reserved words or spaces
   - Start with a number
   - Contain any of these characters: `%, #, ', &, *, !, @, ?, <, >, /, \, :.`
   - End with any of the following suffixes: `.pf, .W`
5. Select **QoS** and then select a QoS Policy type:

   - **Express** - Quickly create basic QoS Policies
   - **Recommended** (default) - Create advanced Policies with the full set of QoS features

   Note: There are some limitations that can prevent you from enabling SecureXL or CoreXL with QoS Policies. For more, see: *"Acceleration Support for R77 Policies" on page 26* .
6. Click **OK**.

   The system saves the new Policy and SmartDashboard opens automatically. You can start to define your rules here.

Planning the 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.

Configuring the Security Gateway

Define these Network Objects:

- London, the Security Gateway on which the QoS is enabled
- Sub-networks for the Marketing and Engineering departments

To define the London Security Gateway:

1. In SmartConsole, click Gateways & Servers.
2. Click **New** > **Gateway** > **Classic Mode**.
3. Configure these parameters in the **General Properties** window.

Field	Value	Notes
Name	London	This is the name by which the object is known on the network; the response to the **hostname** command.
Platform	Select an appliance type or **Open Server**	The platform must be supported for R82
SIC	Click **Communication**	Establishes a secure communication channel between the Security Gateway and the management server.
Version	R82	
OS	Gaia	
IP Address	192.32.32.32	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.
Network Security Tab	**Firewall** and **QoS**	

Defining Interfaces on the Gateway

In this step you configure each interface and its QoS properties.

To configure interface properties:

1. Click **Network Management** in the navigation tree.
2. Click **Get Interfaces** on the toolbar.

   The interfaces show in the **Network Management** window.
3. Double-click each interface and configure parameters in the **Interface > General** window.

eth0

Field	Value	Notes
Net Address	192.32.32.32	
Net Mask	255.255.255.0	
Topology Settings (Click **Modify**)	**Internet External**	This interface connects to the Internet.
Anti-Spoofing	**Perform Anti-Spoofing based on interface topology**	Each incoming packet is examined to make sure that the source IP address is valid.
Spoof Tracking	**Log**	Log Anti-Spoofing events.

eth1

Field	Value	Notes
Net Address	192.32.42.32	
Net Mask	255.255.255.0	
Topology Settings (Click **Modify**)	**Internet External**	This interface connects to the Internet.
Anti-Spoofing	**Perform Anti-Spoofing based on interface topology**	Each incoming packet is examined to make sure that the source IP address is valid.
Spoof Tracking	**Log**	Log Anti-Spoofing events.

eth2

Field	Value	Notes
Net Address	192.199.199.32	
Net Mask	255.255.255.0	
Topology Settings (Click **Modify**)	**Internet External**	This interface connects to the Internet.
Anti-Spoofing	**Perform Anti-Spoofing based on interface topology**	Each incoming packet is examined to make sure that the source IP address is valid.
Spoof Tracking	**Log**	Log Anti-Spoofing events.

To Configure QoS Properties for Interfaces

1. In the **Interface** window, click the **QoS** tab.
2. Select **Inbound Active** and **Outbound Active**.
3. Set **Inbound Active** and **Outbound Active** to **192000 - T1 (1.5 Mbps)**.

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 and Configuring Rules

After you define your network objects and services, the next step is to create your QoS policy rules. This tutorial shows you how to create two simple QoS rules. A new QoS Policy always includes a Default Rule (see *"Default Rule" on page 54*).

To Create a New Policy

1. In **SmartConsole** select **New** from the **File** menu.

   The **New Policy** 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** is created together with a **Default Rule** and is displayed in the **QoS** tab.

Creating New Rules

When you create a new QoS Policy, the system automatically adds a *default rule*, which must always be the last rule in the Policy. Make sure that you add your new rules above the default rule.

Create these two rules: *Web Rule* and *RealAudio Rule*.

1. In SmartDashboard > **QoS** tab, select the default rule.
2. Click the **Before current rule** icon.
3. Enter *Web Rule* in the **Rule Name** window, and then click **OK**.

Do this procedure again for *RealAudio Rule*.

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

Rule Name	Source	Destination	Service	Action
Web Rule	Any	Any	HTTP	Weight 35
RealAudio Rule	Any	Any	RealAudio	Weight 5
Default	Any	Any	Any	Weight 10

Changing New Rule Properties

The system automatically assigns the default parameters as defined in the **Global Properties** > **QoS** to new rules. Use this procedure to change these rules to the values shown in the table below.

Rule Name	Source	Destination	Service	Action
Web Rule	Any	Any	HTTP	Weight 35
RealAudio Rule	Any	Any	RealAudio	Weight 5
Default	Any	Any	Any	Weight 10

To change the properties in a rule:

1. In the **QoS** tab, right-click in the **Service** field of the Web Rule.

   Select **Add Objects**, and then select **HTTP** from the list.

2. Double-click the **Action** field, and then change the **Rule Weight** property to 35. For more, see: *"Changing QoS Global Properties" on page 70*

Do this procedure again for the *RealAudio* and *Default* rules.

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 50*).

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

Connections	Relevant rule	Bandwidth	Comments
HTTP	**Web Rule**	70%	35 / 50 (the total weights)
RealAudio	**RealAudio Rule**	10%	5 / 50
FTP	**Default**	sharing 20%	10 /50; a rule applies to all the connections together
TELNET	**Default**	sharing 20%	10 /50; a rule applies to all the connections together

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

Connections	Relevant rule	Bandwidth	Comments
HTTP	**Web Rule**	87/5%	35 / 40 (the total weights)
RealAudio	**RealAudio Rule**	12.5%	5 / 40

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) is implemented by these rules:

Marketing is Allocated More Bandwidth Than Engineering

Rule Name	Source	Destination	Service	Action
Marketing Rule	Marketing	Any	Any	Weight 30
Engineering Rule	Engineering	Any	Any	Weight 20
Default	Any	Any	Any	Weight 10

Using the same principles described in *"Creating New Rules" on page 43* and *"Changing New Rule Properties" on page 44*, create new rules in SmartConsole and change them to match the values shown in the table above. The effect of these rules is equivalent to the rules shown here:

Connections	Relevant rule	Bandwidth	Comments
HTTP	**Web Rule**	70%	35 / 50 (the total weights)
RealAudio	**RealAudio Rule**	10%	5 / 50
FTP	**Default**	sharing 20%	10 /50 A rule applies to all the connections together
TELNET	**Default**	sharing 20%	10 /50 A rule applies to all the connections together

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

Rule Name	Source	Destination	Service	Action
Web Rule	Any	Any	HTTP	Weight 35
RealAudio Rule	Any	Any	RealAudio	Weight 5
Marketing Rule	Marketing	Any	Any	Weight 30
Engineering Rule	Engineering	Any	Any	Weight 20
Default	Any	Any	Any	Weight 10

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:

Rule Name	Source	Destination	Service	Action
Web Rule	Any	Any	HTTP	Weight 35
RealAudio Rule	Any	Any	RealAudio	Weight 5
Marketing Rule	Marketing	Any	Any	Weight 30
Engineering Rule	Engineering	Any	Any	Weight 20
Default	Any	Any	Any	Weight 10

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 the next page*.

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.

Rule Name	Source	Destination	Service	Action
Web Rule	Any	Any	HTTP	Weight 35
RealAudio Rule	Any	Any	RealAudio	Weight 5
Marketing Rule	Marketing	Any	Any	Weight 30
Engineering Rule	Engineering	Any	Any	Weight 20
Default	Any	Any	Any	Weight 10

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

Rule Name	Source	Destination	Service	Action
Web Rule	Any	Any	HTTP	Guarantee 20 KBps Weight 35
RealAudio Rule	Any	Any	RealAudio	Weight 5
Marketing Rule	Marketing	Any	Any	Weight 30
Engineering Rule	Engineering	Any	Any	Weight 20
Default	Any	Any	Any	Weight 10

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 58* and *"Bandwidth Allocation and Sub-Rules" on page 55*.

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

Rule Name	Source	Destination	Service	Action
Web Rule	Any	Any		Weight 20
Start of Sub-Rule				
Marketing HTTP	**Marketing**	Any	Any	Weight 10
Default	Any	Any	Any	Weight 1
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.

Notes:

- 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

To install a QoS Policy:

1. In SmartDashboard, make changes to Policy rules and then click **Update**.
2. In SmartConsole, click **Install Policy**.
3. From the **Policy list**, select the policy to install.
4. Click **Policy Targets** and select the Security Gateways that will get this Policy.

   Note -By default, no gateways are selected for QoS. You must select them manually.

5. Click **Install**.

If the installation is successful, the new Policy is enforced by the Security Gateways on which it is installed. If installation fails, do these steps to see the error messages:

1. Click the Task Information area, in the lower, left hand corner of SmartConsole.
2. In the **Recent Tasks** area, click **Details** on the applicable error.

In the **Install Policy Details** window, click the **^** icon in the **Status** column to see the error messages. You must resolve all errors before you can successfully install the Policy.

Basic Policy Management

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 58*.

Rule Base Management

Opening the GUI Clients

To open SmartConsole, click SmartConsole in the Windows Start menu.

SmartDashboard opens automatically when you open an existing QoS Policy, or after you create a new QoS Policy. It is generally not necessary to open SmartDashboard manually.

To open SmartDashboard manually:

1. In SmartConsole, open a QoS Policy.
2. Click **Security Policies** > **Access Control** > **QoS**.
3. In the **QoS** view, click **Open QoS Policy in SmartDashboard**.

   SmartDashboard opens and the QoS view shows.

Important - Legacy SmartDashboard does not show the QoS and Desktop policies when an administrator with read-only permissions is logged in, and the "Desktop Security" policy is enabled in the policy package.

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 54*). 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.

Best Practice - Create your QoS rules based on actual traffic patterns. Use the Logs & Events features in SmartConsole to analyze traffic logs.

QoS inspects packets in a sequential manner. When QoS receives a packet for 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, 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: *"Managing QoS" on page 70*.

The QoS Policy Rule Base concept is equivalent to the Security Policy Rule Base. For more, see the: *R82 Security Management Administration Guide*.

Best Practice - 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.

Note - In R82 an above, QoS policy supports different Service objects with the same Destination Port and different Source Ports.

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 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:

```
The weight = (Priority in SmartDashboard) / (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 70*

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*.

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.

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.

QoS Action Properties

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

Action Type

These are the two types of QoS actions:

Action Type	Recommended	Express
Simple	Yes	Yes
Advanced	Yes	No

Simple

The Simple action type has these action properties:

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

Advanced

The Advanced rule type has these properties:

- 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 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 Security 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:

Name	Source	Destination	Service	Action
VPN rule	Any	Any	Any	VPN Encrypt, and other configured actions

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 with more granularity.

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*).

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.

For example:

Bandwidth Allocation in Nested Sub-Rules:

Rule Name	Source	Destination	Service	Action
Rule A	Any	Any	ftp	Rule Guarantee - 100KBps Weight 10
Start of Sub-Rule A				
Rule A 1	Client-1	Any	ftp	Rule Guarantee - 100KBps Weight 10
Start of Sub-Rule A1				
Rule A1.1	Any	Any	ftp	Rule Guarantee - 80KBps Weight 10
Rule A1.2	Any	Any	ftp	Weight 10
End of sub-rule A1				
RuleA2	Client-1	Any	ftp	Weight 10
End of sub-rule A				
Rule B	Any	Any	http	Weight30

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.

Using Policies

After you define your QoS rules in the Rule Base, you must publish your SmartConsole session, and then install the policies on your Security Gateways. The policy installation procedure automatically validates the rules and objects. If there verification errors, a message shows in the in the **Install Policy Details** tab.

After policy installs successfully, the Security Gateways enforce the policy rules.

Note - Make sure the QoS blade is enabled on the Security Gateway before you install the policy.

Installing a QoS Policy

To install a QoS Policy:

1. In SmartDashboard, make changes to Policy rules and then click **Update**.
2. In SmartConsole, click **Install Policy**.
3. From the **Policy list**, select the policy to install.
4. Click **Policy Targets** and select the Security Gateways that will get this Policy.

   Note -By default, no gateways are selected for QoS. You must select them manually.

5. Click **Install**.

If the installation is successful, the new Policy is enforced by the Security Gateways on which it is installed. If installation fails, do these steps to see the error messages:

1. Click the Task Information area, in the lower, left hand corner of SmartConsole.
2. In the **Recent Tasks** area, click **Details** on the applicable error.

In the **Install Policy Details** window, click the **^** icon in the **Status** column to see the error messages. You must resolve all errors before you can successfully install the Policy.

Advanced QoS Policy Management

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 50* .

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

Rule Name	Source	Destination	Service	Action
Rule A	Any	Any	ftp	Rule Guarantee - 100KBps Weight 10
Rule B	Any	Any	http	Weight 20

  - 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.

Rule	Source	Destination	Service	Action
Rule A	Any	Any	ftp	Weight 10
Start of Sub-Rule				
Rule A1	Client-1	Any	ftp	Rule Guarantee - 100KBps Weight 10
Rule A2	Client-2	Any	ftp	Weight 10
End of Sub-Rule				
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 A1	Client-1	Any	ftp	Rule Guarantee - 80KBps Weight 10
Rule A2	Client-2	Any	ftp	Rule Guarantee - 80KBps Weight 10
Rule A3	Client-3	Any	ftp	Weight 10
End of Sub-Rule				
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 that 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 A1	Client-1	Any	ftp	Rule Guarantee - 100KBps Weight 10
Rule A2	Client-2	Any	ftp	Weight 10
End of Sub-Rule				
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) x (1/31). 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** option is selected, 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:

Rule	Source	Destination	Service	Action
Rule A	Any	Any	ftp	Rule Guarantee - 100KBps Rule Limit 100KBps Weight 10
Start of Sub-Rule				
Rule A 1	Client-1	Any	ftp	Rule Guarantee - 100KBps Weight 10
Rule A2	Client-2	Any	ftp	Rule Guarantee - 80KBps Weight 10
End of Sub-Rule				
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:*" To Configure QoS Properties for Interfaces" on page 43*

"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.

Notes.

- QoS supports adding DiffServ markings to packets that match a rule
- QoS does not support matching packets based on DiffServ tagging

Low Latency Queuing

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 maximum 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 maximum 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 maximum delay permits. If the maximum 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 maximum delay must also exceed some minimum.

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 maximum delay limitations.

Note - The maximum 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 69*. These priority levels are relative to other Low Latency classes.

Best Practice - Define more than one Low Latency class if different types of traffic require different maximum delays.

The class with the lower maximum 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 maximum 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 minimum delay that is possible for the class. This is best done by:

- Initially setting the priorities for all Low Latency classes according to maximum 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 maximum delay, see *"Calculating Maximum Delay" on the next page*.

Logging LLQ Information

The system logs data for all aspects of LLQ.

Calculating the Correct Constant Bit Rate and Maximum 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 *"Making sure that Constant Bit Rate is not Exceeded" on page 67*.

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 Maximum Delay

To calculate the maximum delay of a Low Latency class, take into account the:

- Maximum delay that streams matching the class can tolerate in QoS
- Minimum delay that QoS can guarantee this stream

It is important not to define a maximum 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 maximum 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.

Best Practice - Use the default Class Maximum 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 Maximum Delay

You can also set the Class Maximum 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 maximum 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.

     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 Security Gateway. To get an estimate of burst size, monitor the internal interface that precedes the QoS Security Gateway.

   - If no burstiness is detected, the minimum delay of the class must be no smaller than:

     [3 x (packet size)] / [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 minimum delay of the class to at least:

   ```
   [(burst size + 1) x (packet size)] / [bit rate]
   ```

The maximum delay that you select for the class must be between the smallest delay (step 2) and the greatest delay (step 1). Setting the maximum 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 maximum delay close to the value of the greatest delay.

This error message can show after you enter the maximum 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 64*). The delay value displayed in the error message depends on the Low Latency classes of higher priority, and on interface speed.

Set the maximum 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 64*.)

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 maximum 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

- 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 *"Making sure that Constant Bit Rate is not Exceeded" on the previous page* (Preventing Unwanted Drops).

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 maximum 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 maximum 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 minimum 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 Security 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 63*).

When to Use DiffServ and When to Use LLQ

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

- Supports DiffSer

  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 MPL

  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 the previous page*):

Managing QoS

This chapter shows you how to configure and manage QoS. These procedures assume that you have opened SmartConsole, as described in *"Opening the GUI Clients" on page 50* .

Defining QoS Global Properties

The QoS global properties include default values for QoS rule parameters and unit of measure.

Configure QoS global properties in SmartConsole.

Note: You must close SmartDashboard before you can work with global properties.

To configure QoS Global Properties:

1. In SmartConsole click **Application Menu** > **Global properties** > **QoS**.
2. In the Global Properties window, configure these parameters:

   Weight:

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

   Rate:

   - **Unit of measure:** The unit specified in QoS windows by default for transmission rates (for example, Bps - Bytes per second).
3. Click **Set Default** to save the default values.

Changing QoS Global Properties

To configure 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).

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

Interface QoS Properties

You must first define the network objects, that is, the Security Gateway and its interfaces on which QoS controls traffic flow.

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 Security Gateway.

Configuring Interface QoS Properties

To configure Security Gateway interfaces

1. Open SmartConsole.
2. Click **Gateways & Servers** and double-click the applicable **Security Gateway** object.
3. In the **General Properties**, click **Network Management**.

   The **Check Point Gateway - Topology** window opens.
4. If a list of interfaces does not show, click **Get Interface.**

   If you choose this method of configuring the Security Gateway, the topology fetched suggests the external interface of the Security Gateway based on the QoS Security Gateway routing table. You must make sure that this information is correct.
5. Double-click the appropriate interface.
6. In the **Interface Properties** window, click the **QoS** tab.

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 88* and *"Defining a Low Latency Class" on page 92* 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 62* and *"Low Latency Queuing" on page 63*.

8. Click **OK**.

   Changes to the interface QoS properties are saved.

Do steps 4 - 7 for each applicable interface.

Notes:

- Interfaces on the WAN side (or interfaces connected to a slower network) are typically defined as active. On a gateway with only two interfaces, enable QoS only on the interface connected to the WAN. If the gateway controls DMZ traffic, you can install QoS on the interface connected to the DMZ.
  - Select **Inbound Active** to control traffic on this interface in the inbound direction.
  - From the **Rate** list, select or enter the available bandwidth in the inbound direction.
  - Check **Outbound Active** to control traffic on this interface in the outbound direction.
  - From the **Rate** list select or enter the available bandwidth in the outbound direction.
- *Make sure that the rates correspond to the actual physical capacity of the interfaces.*

  QoS cannot not make sure the defined rates are compatible with the interface hardware.

  If the defined rate is less than the physical capacity, QoS uses only specified capacity. Excess capacity is not used. If the defined rate greater than the physical capacity, QoS cannot control traffic correctly.

Working with QoS Policies

QoS policy is an ordered set of QoS rules in the Rule Base. The Rule Base contains rules that 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 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 and defined its QoS rules you must install it on the relevant QoS gateways.

To Create New QoS Policy

1. On the gateway, make sure that the QoS blade is enabled.
2. In SmartConsole, from the **File** menu, select **Manage Policies and Layers**.
3. Click **New**.
4. In the **Policy** window, enter a Policy name.

   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: .pf, .W.
5. Select **QoS** and then select a QoS Policy type:

   - **Express** - Quickly create basic QoS Policies
   - **Recommended** (default) - Create advanced Policies with the full set of QoS features

   Note: There are some limitations that can prevent you from enabling SecureXL or CoreXL with QoS Policies. For more, see: *"Acceleration Support for R77 Policies" on page 26*.
6. Click **OK**.

   The system saves the new Policy and SmartDashboard opens automatically. You can start to define your rules here.

Opening an Existing QoS Policy

To Open an Existing Policy:

1. In SmartConsole, click **Security Policies** > **Manage Policies**.
2. In the Manage Policies window, double-click a QoS Policy.

   SmartDashboard opens.

Creating New Rules

You work with rules in SmartDashboard. When you add rules, you can put the new rule anywhere in the Rule Base except after the last rule. The Default Rule must always be at the bottom of the Rule Base.

To create a new rule:

1. In the **QoS** tab, at the position where you want to add a new rule.
2. Add a new rule from the **Rule** menu, the toolbar, or right-click a name in the **Name** column of a rule to display the **Rule** menu.

   The **Rule Name** window opens.
3. Enter the name of the rule in the **Rule Name** field.
4. Click **OK**.

   The rule is added to the Rule Base at the selected position, with the values defined in the **QoS** page of the **Global Properties** window.

To add a rule	Select from Menu
After the last rule	**Rules > Add Rule > Bottom**
Before the first rule	**Rules > Add Rule > Top**
After the current rule	**Rules > Add Rule > Below**
Before the current rule	**Rules > Add Rule > Above**
To the current rule	**Rules > Add Sub-Rule**

Right-click a rule to use these menu commands:

Menu Option	Explanation
Add Rule above	Adds a rule before the current rule.
Add Rule below	Adds a rule after the current rule.
Add Sub-Rule	Deletes the current rule.
Delete Rule	Deletes the current rule.
Copy Rule	Copies the current rule to the clipboard.
Cut Rule	Deletes the current rule and puts it in the clipboard.
Paste Rule	Pastes the rule in the clipboard (a sub-menu is displayed from which you can select whether to paste the rule above or below the current rule).
Add Class of Service	Specifies a Class of Service (see *"Differentiated Services (DiffServ)" on page 62* and *"Low Latency Queuing" on page 63*). A sub-menu is displayed from which you can select whether the Class of Service is to be added above or after the current rule.
Hide Rule	Hides the current rule. The rule is still part of the Rule Base and will be installed when the QoS Policy is installed.
Disable Rule	Disables the current rule. The rule appears in the Rule Base but is not enforced by the QoS Policy.
Rename Rule	Renames the current rule.

Best Practice - For adding new QoS rules in an environment with limited bandwidth. Open **Global Properties** and set a default weight for each new rule. Weight is the percentage of the available bandwidth allocated to a rule. Leave the default weight at 10. Changing the value to less than 10 can result in a complete loss of bandwidth for that rule.

Changing the Rule Name

To change the rule name:

1. In the **QoS** tab, double-click the **Name** column in the rule to rename.
2. In the **Rule Name** window, enter the new rule name in the **Rule Name** field.
3. Click **OK**.

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 these options:

Action	From Menu select
Cut	Edit > Cut
Copy	Edit > Copy
Paste	Edit > Paste

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 **Delete** on the toolbar.
3. Click **Yes** to delete the selected rule.

Working with Rules

You can change rule fields, as often as you like, until the rule is in the form that you require. Configure the source and destination of each communication, services that can be used (TCP, Compound TCP, UDP, and ICMP), actions to be taken with the data packets, whether to maintain a log of the entries for the selected rule, and interfaces of the QoS Security Gateway that the rule is enforced.

This section describes the procedures for modifying the various fields in a rule. Refer to *"Basic Policy Management" on page 50* 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 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.
3. Select **Where Used**.

   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.
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 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.

   - 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 supported by QoS is of form **a*b** where **a** and **b** are strings and ***** is wildcard. See *"Appendix: Regular Expressions" on page 123*.

- 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 Security Gateway by IPsec VPN. This field does not apply to traffic that was encrypted prior to arriving to this Security 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 55* .

   - 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 70*. Leave this value as is to avoid a complete loss of bandwidth. For detailed information see *"Weight" on page 52* .

  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 53* .

  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 53* .

  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 53* .

     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 53* .

- **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 70*).

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 95* . For information on how to turn logging on, see *"Enabling Log Collection" on page 94*.

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 Security Gateway the rule is enforced. You can select any number of **Install On** objects.

Note -.To install a QoS Policy on a Security Gateway, make sure that:

- The Security 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 70* and *"Interface QoS Properties" on page 71*.)

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 Security 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.
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.

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.

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 in *"Working with QoS Policies" on page 72*.
6. Add new sub-rules by following the same procedures for creating rules described in *"Working with QoS Policies" on page 72*

Viewing 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 62*.

Defining a DiffServ Class of Service

To define a DiffServ class of service:

1. From the SmartDashboard menu, select **Manage** > **QoS** > **QoS Classes**.
2. In the **QoS Classes** window, click **New** > **DiffServ Class of Service**.
3. In the **Class of Service Properties** window, configure these settings:
   - **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**.

Defining a DiffServ Class of Service Group

To define a DiffServ class of service group:

1. In SmartDashboard, click **Manage** > **QoS** > **QoS Classes**.
2. In the **QoS Classes** window, click **New** > **DiffServ Class of Service Group**.
3. In the **Group Properties** configure these properties:
   - **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, double-click a class in the list in the **Not in Group** list.
   - To delete a class from the group, double-click a class **In Group** list.
4. Click **OK**.

Configuring an Interface for DiffServ

Use these procedures to configure interfaces and to add a DiffServ class to an interface.

To configure interface for DiffServ:

1. In SmartConsole, go to **Gateways & Servers**.
2. Double-click the applicable Security Gateway.
3. In the **Check Point Gateway** window, click **Network Management**.
4. Double-click the applicable interface.
5. In the **Interface** window, click the **QoS** tab.
6. In the **Diffserv and Low Latency classes** section, click **Add** > **DiffServ Classes** > **Others**.
7. Select **Inbound Active** and/or **Outbound Active** and set the **Rate** properties.
8. In the **Object Editor** window, select a **QoS Class** from the list.
9. Select and configure these parameters for **Inbound** and/or **Outbound** traffic:
   - **Guaranteed bandwidth** -The bandwidth guaranteed marked for priority.

     IMPORTANT: Make sure you do not exceed the guaranteed bandwidth.
   - **Bandwidth Limit** - The maximum bandwidth for this class.
     Traffic volume greater than the Bandwidth Limit is marked for QoS priority.

   Note: You must configure these properties for at least one traffic direction.
10. Click **OK**.

To add QoS Classes to the Rule Base:

1. Open SmartDashboard.
2. Do one of these actions:
   - In the **Name** column of a QoS rule, click the rule **Add Class of Service > Above**.
   - In a class header, right-click the header and then click **Add Class of Service Above** or **Add Class of Service Below**.
3. Select a class from the list. Click **OK**.

   The DiffServ class header shows in the Rule Base. If this is the first defined class, the *Best_Effort* header shows directly below the new DiffServ class header.
4. Follow the steps in the next sections to define the class properties.

Defining Expedited Forwarding Class Properties

To define Expedited Forward class properties:

1. In the SmartDashboard **Network Objects** tree, double-click the applicable Security Gateway.
2. In the **Gateway** window, click **Network Management**.
3. In the **Interface** window, click the **QoS** tab.
4. In the **DiffServ and Low Latency classes** section, click **Add** or **Edit**.
5. Click **DiffServ Classes > Expedited Forwarding**.
6. Configure these properties:
   - **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.
   - **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.

   You must configure at least one of the two directional properties (Inbound / Outbound), and you can configure both.
7. Click **OK**.

Defining DiffServ Class Properties

To define DiffServ class properties:

1. In SmartDashboard, locate the relevant Security Gateway.
2. In the **Gateway Properties** window, click **Network Management**.
3. In the **Interface** window, click the **QoS** tab.
4. In the **DiffServ and Low Latency classes** section, click **Add** or **Edit**.
5. Click **DiffServ Classes > Others**.
6. Configure these properties:

- **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.

7. Click **OK**.

Working with Low Latency Queuing

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 maximum 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 63* .

Defining a Low Latency Class

To define a Low Latency class:

1. In SmartDashboard select **Manage** > **QoS** > **QoS Classes**.
2. In the **QoS Classes** window, click **New** > **Low Latency Class of Service**.
3. In the **Class of Service Properties** window, configure these class properties:
   - **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.
4. Click **OK**.

Configuring an Interface for Low Latency

Use these procedures to configure interfaces to use a Low Latency or DiffServ Expedited Forwarding class.

To configure an interface for Low Latency:

1. Make sure that SmartDashboard is closed.
2. In SmartConsole, go to **Gateways & Servers**.
3. Double-click the applicable Security Gateway.
4. In the **Check Point Gateway** window, click **Network Management**.
5. Double-click the applicable interface.
6. In the **Interface** window, click the **QoS** tab.
7. Select **Inbound Active** and/or **Outbound Active** and set the **Rate** properties.
8. In the **Diffserv and Low Latency classes** section, click **Add** > **Low Latency Classes**.
9. In the **Low Latency QoS** window, select a class from the list.
10. Select **Inbound Active** and/or **Outbound Active**.

    Note: You must set at least one traffic direction to Active.

11. Configure these Low Latency properties:
    - **Constant Bit Rate** - The constant bit rate at which packets of this class will be transmitted.
    - **Maximal Delay** - The maximum delay allowed for packets of this class. Packets that exceed this value are dropped.

      Note: To configure an Expedited Forwarding interface to work as a DiffServ interface, set the Maximal Delay property to *99999*.

Do these steps for each applicable interface on a Security Gateway.

Defining Low Latency Class Properties

To define Low Latency class properties:

1. In SmartDashboard, click a Gateways & Servers and double click the applicable Security Gateway.
2. In the **Gateway** window, click **Network Management**.
3. In the **Interface** window, click the **QoS** tab.

4. In the **DiffServ and Low Latency classes** section, click **Add** or **Edit**.
5. Click **Low Latency**.
6. Configure these properties:
   - **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.
   - **Outbound**: Define the portion of the interface's outbound capacity to be reserved by defining a **Constant Bit Rate** and a **Maximal Delay** as described above.

   You must configure at least one of the two directional properties (Inbound / Outbound), and you can configure both.
7. Click **OK**.

Viewing QoS Security Gateway Status

To see the QoS Security Gateway status, click **Security Gateway** in the **Gateways & Servers** view in SmartConsole. The status information shows on the **Summary** tab at the bottom of the view.

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 logging features work, see *"Overview of Logging" on page 95*.

To Turn on QoS Logging

A QoS Security 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.

Confirming a Rule is logged

1. In SmartDashboard, select the rule whose connection will be logged.
2. Confirm that either **Log** or **Account** appear in the **Track** field.

Logs & Events

This chapter shows you how configure rules to create logs for specified conditions. You can use the powerful Logs & Events features in SmartConsole to see logs and to monitor the effectiveness of QoS Policies.

Overview of Logging

These events are logged. The table below describes features unique to event logs.

Non-Accounting Log Events

Log Event	Data Returned	Presentation	Policy Mode
Connection Reject			
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.	The name of the matching rule on account of which the connection was rejected.	Generated as a reject log. Unified with the initial connection log.	Recommended policy only.
Running Out of Packet Buffers			
One of the interface-direction's packet buffers is exhausted. A report is generated a maximum of once per 12 hours.	A string explaining the nature of the problem and the size of the relevant pool.	New log record created each time a global problem is reported.	Recommended policy only.
LLQ Packet Drop			
When a packet is dropped from an LLQ connection. A report is generated a maximum of once per 5 minutes.	Logged data: ■ Number of bytes dropped due to delay expiration ■ Average packet delay ■ Jitter (maximum delay difference between two consecutive packets)	Unified with the initial connection log.	Recommended policy only.

The next table describes the features unique to accounting logs.

Explaining the Accounting Log

Logged	Data Returned	Policy Mode
General Statistics		
The total bytes transmitted through QoS for each relevant interface and direction.	Inbound and outbound bytes transmitted by QoS.	Recommended and Express policies.
Drop Policy Statistics		
■ Total bytes dropped from the connection as a result of the QoS policy. ■ Count of the bytes dropped from the connection because the maximum used memory fragments for a single connection was exceeded.		Recommended policy mode only.
LLQ Statistics		
Statistics about the LLQ connection.	Logged data: ■ Number of bytes dropped due to delay expiration ■ Average packet delay ■ Jitter (maximum delay difference between two consecutive packets)	Recommended policy mode only.

These 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. (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 *"Confirming a Rule is logged" on page 94* and *"To Modify Tracking for a Rule" on page 84* .

Examples of Log Events

This section describes the log events.

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 54*). 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

Time	Product	Interface	Type	Action	Information
15:17:09	QoS	daemon	log	reject	rule_name:Best_Effort->udp2

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 minimum number of dropped bytes.

LLQ Drop Log - Example

Product	Type	Information
QoS	log	s_in_llq_drops:3000 s_in_llq_avg_xmit_delay: 900 s_in_llq_max_delay: 1351 s_in_llq_xmit_jitter: 1351 s_in_llq_recommended_delay:2000

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 interface's 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

Product	Interface	Type	Information
QoS	E100B1	control	info:Ifdir Memory Pool Exceeded Pool_size:8

Examples of Account Statistics Logs

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

Product	Type	Information
QoS	Account	segment_time 8May2002 12:24:57

Account Logs may include any or all of the above information

Note - 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

...	Information	...
	s_in_bytes:5768 s_out_bytes: 154294	

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

...	Information	...
	s_out_total_drops:3914274 s_out_exceed_drops: 3914274	

LLQ Statistics Data

Data items are the same as in LLQ Drop Log, but are generated from the beginning of the connection, **not** from the last time a log was created.

FAQ

QoS Basics

When should I use Recommended Policy type **and** when should I use **Express Policy** type **?** - Use the Recommended Policy type when you need fine-tuned functionality and advanced QoS features. Use Express if your system requires only basic QoS.

What are the benefits of using each mode? - Recommended gives you advanced QoS functionality. Express mode gives you better performance and requires less CPU and memory.

Can I change the Policy types? - You can change a policy type from Express to Recommended, but you cannot change Recommend to Express. We recommend that you start with Express if you are not certain. This way, you can change to Recommended if you require advanced QoS functionality.

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.

Example of Highest Weight Differentiation

	HTTP gets	...and equals	Comment
Policy 1			
HTTP weight = 500, FTP weight =500	500/(500+500)	= ?	Equal weight is given to each rule.
Policy 2			
HTTP weight = 2, FTP weight =2;	2/(2+2)	= ?	Equal weight is given to each
Policy 1 + third rule			
HTTP weight = 500, FTP weight =500, SMTP weight = 100	500/ (500+500+100)	= 500/1100	Due to the initial high value of the weights in Policy 1, the amount of bandwidth available to the HTTP connection is only marginally less than in Policy 1 even after the introduction of the third rule.
Policy 2 + third rule			
HTTP weight = 2, FTP weight =2; SMTP weight = 100	2/(2+2+100)	= 2/104	Due to the low value of the weights in Policy 2, the amount of bandwidth available to the HTTP connection is now significantly less as a result of the introduction of the third rule.

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.

How does QoS handle TCP retransmitted packets? - When a retransmission is detected, QoS checks to see if the retransmitted data is already contained in the QoS queue. If so, the packet is dropped. This unique QoS capability eliminates retransmissions that consume up to 40% of a WAN link, and saves memory required to store duplicated packets.

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, you can limit Web surfing to the site http://www.restrict-access-to-this-site.com. You need to add a QoS URI resource that looks for the string "www.restrict-access-to-this-site.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 the most important QoS 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
- DiffServ Support and QoS bring Better than Frame Relay QoS to the VPN world
- Log verification

Is SmartView Monitor a part of QoS? - No. 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 Security Gateway management is identical to that for any Security Gateway. Thus, the maximum number of gateways is identical to the maximum number of gateways that are managed.

Do I need to run QoS on the Security Management Server? - Yes, in order to manage a QoS Security Gateway you need to install QoS on the Security Management Server.

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 minimum guaranteed bandwidth is required for adequate performance
- low delay and jitter are required

Is QoS Rule Base "first match"? - 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

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 Security 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**.

Capacity Planning

What are the QoS memory requirements? - To run QoS, the following amount of free memory is needed (in addition to the memory needed for Multi-Domain Security Management):

QoS memory requirements

Number of connections	Management	Gateway (or Management and gateway)
5,000	0 MB	32.5 MB
10,000	0 MB	39 MB
25,000	0 MB	57 MB
50,000	0 MB	91 MB
100,000	0 MB	156 MB

- These numbers include SmartView Monitor and UserAuthority.
- Connections are counted in the Firewall connection table.
- The default size for the connection table is 25,000.
- On an average, each connection requires 1300 bytes.

How do I know what kind of hardware I need to run QoS? - Deciding on a hardware platform and vendors involves many aspects and each buyer has their own specific considerations such as support, price, appliances, knowledge, and so on.

As far as performance is concerned, CPU performance is the main factor in QoS performance. The reduced memory footprint and low memory prices, memory should not usually be the cause of a bottleneck.

How do I tune QoS performance? - Here are some tips on fine-tuning QoS performance:

1. Upgrade to the newest QoS version available.
2. In most cases you need to install QoS only on the external interfaces of the gateway.
3. Unless you are using limits for inbound traffic, installing QoS only in the outbound direction will provide you with most of the functionality and improvements.
4. Put more frequent rules at the top of your Rule Base. You can use SmartView Monitor to analyze how much a rule is used.
5. Turn "per connection limits" into "per rule limits".
6. Turn "per connection guarantees" into "per rule guarantees".

What is the maximum bandwidth supported by QoS? - 10Gbps.

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 uses 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 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 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).

Why is limiting bandwidth for an application 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. Blocking these services completely may encourage the students find a 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 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.

Command Line Reference

Syntax Legend for CLI Commands

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

Character	Description

TAB	Shows the available nested subcommands:
	`main command`
	`→ nested subcommand 1`
	`→ → nested subsubcommand 1-1`
	`→ → nested subsubcommand 1-2`
	`→ nested subcommand 2`
	Example:
	`cpwd_admin`
	`config`
	`-a <options>`
	`-d <options>`
	`-p`
	`-r`
	`del <options>`
	Meaning, you can run only **one** of these commands:
	■ This command: `cpwd_admin config -a <options>`
	■ Or this command: `cpwd_admin config -d <options>`
	■ Or this command: `cpwd_admin config -p`
	■ Or this command: `cpwd_admin config -r`
	■ Or this command: `cpwd_admin del <options>`

Character	Description
Curly brackets or braces **{ }**	Enclose a list of available commands or parameters, separated by the vertical bar **|**. User can enter only one of the available commands or parameters.
Angle brackets **< >**	Enclose a variable. User must explicitly specify a supported value.
Square brackets or brackets **[ ]**	Enclose an optional command or parameter, which user can also enter.

etmstart

Description

Starts the QoS Software Blade on the Security Gateway - starts the QoS daemon `fgd50`, and fetches the QoS policy from the Management Servers configured in the `$FWDIR/conf/masters` file on the Security Gateway.

For more information, see:

- *R82 QoS Administration Guide*
- sk41585: How to control and debug QoS (FloodGate-1)

Syntax

```
etmstart
```

Important - On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

Example

```
[Expert@MyGW:0]# etmstart
QoS: Starting fgd50

QoS: Fetching QoS Policy from masters
Fetching QoS Software Blade Policy:
 Received Policy. Downloading...

eth0(inbound), eth0(outbound).
Download OK.
Done.
QoS started
[Expert@MyGW:0]#
```

etmstop

Description

Stops the QoS Software Blade on the Security Gateway - kills the QoS daemon `fgd50` and then unloads the QoS policy.

For more information, see:

- *R82 QoS Administration Guide*
- sk41585: How to control and debug FloodGate-1 (QoS)

Syntax

```
etmstop
```

Important - On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

Example

```
[Expert@CXL1_192.168.3.52:0]# etmstop
 Unloading QoS Policy:
 Target(s): CXL1_192.168.3.52
   CXL1_192.168.3.52: QoS policy unloaded successfully.
 Done.
QoS stopped
[Expert@CXL1_192.168.3.52:0]#
```

fgate

This section describes:

The 'fgate' command on Management Server

Description

Installs and uninstalls the QoS policy on the managed Security Gateways.

Shows the status of the QoS Software Blade on the managed Security Gateways.

For more information, see:

- *R82 QoS Administration Guide*
- sk41585: How to control and debug FloodGate-1 (QoS)

Syntax

```
fgate [-d]
      load <Name of QoS Policy>.F <GW1> <GW2> ... <GWN>
      stat
            -h
            <GW1> <GW2> ... <GWN>
      unload <GW1> <GW2> ... <GWN>
      ver
```

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.

Parameter	Description
`load <Name of QoS Policy>.F <GW1> <GW2> ... <GWN>`	Runs a verifier on the QoS policy <*Name_of_QoS_Policy*>. If the QoS policy is valid, the Management Server compiles and installs the QoS Policy on the specified Security Gateways `<GW1> <GW2> ... <GWN>`. **Notes:** ■ The maximum supported length of the <*Name of QoS Policy*> string is 32 characters. ■ To specify a Security Gateway, enter the main IP address of the name of its object as configured in SmartConsole. You can specify several Security Gateways or cluster members in the same command.
`stat -h`	Shows the built-in usage for the "`stat`" parameter.
`stat <GW1> <GW2> ... <GWN>`	Shows the status of the QoS Software Blade and policy on the managed Security Gateways. **Note** - To specify a Security Gateway, enter the main IP address of the name of its object as configured in SmartConsole. You can specify several Security Gateways or cluster members in the same command. **Important** - This command is outdated and exists only for backward compatibility with very old versions. Use the "cpstat" command.
`unload <GW1> <GW2> ... <GWN>`	Uninstalls the QoS Policy from the specified Security Gateways `<GW1> <GW2> ... <GWN>`. **Note** - To specify a Security Gateway, enter the main IP address of the name of its object as configured in SmartConsole. You can specify several Security Gateways or cluster members in the same command.
`ver`	Shows the QoS Software Blade version on the Management Server.

Examples

Example 1 - Installing the QoS policy on one Security Gateway specified by its IP address

```
[Expert@MGMT:0]# fgate load MyPolicy.F 192.168.3.52
 QoS rules verified OK!
 Downloading QoS Policy: MyPolicy.F...
 Target(s): MyGW
   MyGW: QoS policy transferred to module: MyGW.
   MyGW: QoS policy installed succesfully.
 Done.
[Expert@MGMT:0]#
```

Example 2 - Installing the QoS policy on two cluster members specified by their object names

```
[Expert@MGMT:0]# fgate load MyPolicy.F MyClusterMember1 MyClusterMember2
 QoS rules verified OK!
 Downloading QoS Policy: MyPolicy.F...
   MyClusterMember1: QoS policy transferred to module: MyClusterMember1.
   MyClusterMember1: QoS policy installed succesfully.
   MyClusterMember2: QoS policy transferred to module: MyClusterMember2.
   MyClusterMember2: QoS policy installed succesfully.
 Done.
[Expert@MGMT:0]#
```

Example 3 - Viewing the QoS status on one Security Gateway specified by its object name

```
[Expert@MGMT:0]# fgate stat MyGW

Module name: MyGW
=======================

Product: QoS Software Blade
Version: R82
Kernel Build: 456
Policy Name: MyPolicy
Install time: Wed Dec 4 19:53:48 2019
Interfaces Num: 1


Interface table
------------------------------------------------------------------
|Name|Dir|Limit (Bps)|Avg Rate (Bps)|Conns|Pend pkts|Pend bytes|
------------------------------------------------------------------
|eth0|in | 1250000000|             0|    0|        0|         0|
|eth0|out| 1250000000|             0|    0|        0|         0|
------------------------------------------------------------------

[Expert@MGMT:0]#
```

Example 4 - Viewing the QoS Software Blade version

```
[Expert@MGMT:0]# fgate ver
This is Check Point QoS Software Blade R82 - Build 123
[Expert@MGMT:0]#
```

The 'fgate' command on Security Gateway

Description

Installs and uninstalls the QoS policy on the managed Security Gateways.

Shows the status of the QoS Software Blade on the managed Security Gateways.

Controls the QoS debug.

For more information, see:

- *R82 QoS Administration Guide*
- sk41585: How to control and debug FloodGate-1 (QoS)

Syntax

```
fgate [-d]
      ctl
            -h
            <QoS Module> {on | off}
      debug
            on
            off
      fetch
            -f
            <Management Server>
      kill [-t <Signal Number>] <Name of QoS Process>
      load
      log
            on
            off
            stat
      stat [-h]
      ver [-k]
      unload
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-d`	Runs the command in debug mode. Use only if you troubleshoot the command itself. **Best Practice** - If you use this parameter, then redirect the output to a file, or use the `script` command to save the entire CLI session.
`ctl -h`	Shows the expected syntax and the list of the available QoS modules.
`ctl <QoS Module> {on | off}`	Controls the specified QoS module: ■ `on` - Enables the module (default) ■ `off` - Disables the module **Note** - In R82, the only available QoS module is `etmreg`.
`debug {on | off}`	Controls the debug mode of the QoS user space daemon `fgd50` (see sk41585): ■ `on` - Enables the debug ■ `off` - Disables the debug (default) This sends additional debugging information to the `fgd50` daemon's log file `$FGDIR/log/fgd.elg`.
`fetch -f`	Fetches and installs the QoS Policy from all the Management Servers configured in the `$FWDIR/conf/masters` file.
`fetch <Management Server>`	Fetches and installs the QoS Policy from the specified Management Server. Enter the main IP address or the name of the Management Server object as configured in SmartConsole.

Parameter	Description
`kill [-t <Signal Number>] <Name of QoS Process>`	Sends the specified signal to the specified QoS user space process. **Notes:** ■ In R82, the only available QoS user space process is `fgd50`. ■ The QoS `fgd50` daemon, upon its startup, writes the PIDs of the applicable QoS user spaces processes to the `$FWDIR/tmp/<Name of QoS Process>.pid` files. For example: `$FWDIR/tmp/fgd50.pid` ■ If the file `$FWDIR/tmp/<Name of QoS Process>.pid` exists, then this command sends the specified Signal Number to the PID in that file. ■ If you do not specify the signal explicitly, the command sends Signal 15 (`SIGTERM`). ■ For the list of available signals and their numbers, run the `kill -l` command. For information about the signals, see the manual pages for the `kill` and `signal`. ■ To restart the QoS `fgd50` daemon manually, run the *"etmstop" on page 112* and then *"etmstart" on page 111* commands.
`load`	Installs the local QoS Policy on the Security Gateway. If this command fails, run the *"etmstop" on page 112* and then *"etmstart" on page 111* commands.
`log {on | off | stat}`	Controls the state of QoS logging in the Security Gateway kernel: ■ `on` - Enables the QoS logging (default) ■ `off` - Disables the QoS logging ■ `stat` - Shows the current QoS logging status You can disable the QoS logging to save resources without reinstalling the QoS policy.

Parameter	Description
`stat [-h]`	Shows the status of the QoS Software Blade and policy on the Security Gateway. The `-h` parameter shows the built-in usage for the "`stat`" parameter. **Important** - This command is outdated and exists only for backward compatibility with very old versions. Use the "cpstat" command.
`unload`	Uninstalls the QoS Policy from the Security Gateway.
`ver [-k]`	Shows the QoS Software Blade version. If you specify the "`-k`" parameter, the output also shows the kernel version.

Examples

Example 1 - Fetching the QoS policy based on the $FWDIR/conf/masters file

```
[Expert@MyGW]# fgate fetch -f
Fetching QoS Software Blade Policy:
 Received Policy. Downloading...

eth0(inbound), eth0(outbound).
Download OK.
Done.
[Expert@MyGW]#
```

Example 2 - Fetching the QoS policy from the Management Server specified by its IP address

```
[Expert@MyGW]# fgate fetch 192.168.3.240
Fetching QoS Software Blade Policy:
 Received Policy. Downloading...

eth0(inbound), eth0(outbound).
Download OK.
Done.
[Expert@MyGW]#
```

Example 3 - Viewing the QoS status

```
[Expert@MyGW]# fgate stat

Product:        QoS Software Blade
Version:        R82
Kernel Build:   456
Policy Name:    MyPolicy
Install time:   Wed Dec 4 19:53:48 2019
Interfaces Num: 1


Interface table
-------------------------------------------------------------------
|Name|Dir|Limit (Bps)|Avg Rate (Bps)|Conns|Pend pkts|Pend bytes|
-------------------------------------------------------------------
|eth0|in | 1250000000|             0|    0|        0|         0|
|eth0|out| 1250000000|             0|    0|        0|         0|
-------------------------------------------------------------------

[Expert@MyGW]#
```

Example 4 - Viewing the QoS Software Blade version

```
[Expert@MyGW:0]# fgate ver
This is Check Point QoS Software Blade R82 - Build 123
[Expert@MyGW:0]#
[Expert@MyGW:0]# fgate ver -k
This is Check Point QoS Software Blade R82 - Build 123
kernel: R82 - Build 456
[Expert@MyGW:0]#
```

Working with Kernel Parameters

See the *R82 Quantum Security Gateway Guide* > Chapter "Working with Kernel Parameters".

Kernel Debug

See the *R82 Quantum Security Gateway Guide* > Chapter "Kernel Debug on Security Gateway".

Appendix: Regular Expressions

Regular Expression Syntax

This table shows the Check Point implementation of standard regular expression metacharacters.

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

Using Non-Printable Characters

To use non-printable characters in patterns, escape the reserved character set.

Character	Description
\a	alarm; the BEL character (hex code `07`)
\cX	"control-X", where X is any character
\e	escape (hex code `1B`)
\f	formfeed (hex code `0C`)
\n	newline (hex code `0A`)

Character	Description
\r	carriage return (hex code `0D`)
\t	tab (hex code `09`)
\ddd	character with octal code `ddd`
\xhh	character with hex code `hh`

Using Character Types

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

Character	Description
\d	any decimal digit [0-9]
\D	any character that is not a decimal digit
\s	any whitespace character
\S	any character that is not whitespace
\w	any word character (underscore or alphanumeric character)
\W	any non-word character (not underscore or alphanumeric)

Disabling QoS Acceleration Support

If you have a QoS policy created for R77 and earlier, you will have to disable QoS acceleration to use other features. See: *"Acceleration Support for R77 Policies" on page 26*

To manually disable QoS acceleration:

1. On the Security Gateway, run: `cpconfig` to turn off SecureXL and CoreXL.
2. Reboot the Security Gateway.
3. After reboot, run:

```
cpprod_util CPPROD_SetValue FG1 FgWithAcceleration 1 0 1
```

To manually enable QoS acceleration:

1. On the Security Gateway, run:

```
cpprod_util CPPROD_SetValue FG1 FgWithAcceleration 1 1 1
```

2. Use `cpconfig` to turn on SecureXL/CoreXL.

3. Reboot the Security Gateway.