How To Configure Floodgate-1

26 December 2010

softwareblades™

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.
Important Information

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

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=11805
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/26/2010</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on How To Configure Floodgate-1).
Contents

Important Information.................................................................3
How To Configure FloodGate-1 ......................................................5
  Objective ........................................................................5
  Supported Versions .............................................................5
Before You Start .......................................................................5
  Related Documentation and Assumed Knowledge ..................5
  Impact on the Environment and Warnings .........................5
Background Information ............................................................6
  Technology Overview ..........................................................6
  FloodGate-1 Innovative Technologies ....................................6
  Bandwidth Allocation and Rules ..........................................7
    Weight ........................................................................7
    Guarantees ....................................................................7
    Limits ...........................................................................7
Configuring QoS ......................................................................8
  Direction and Rate ..............................................................9
  Global Settings ...................................................................11
  Configuring the Policy Type ................................................11
  Configuring QoS Rule Bases ................................................12
  Defining Sub-Rules .............................................................12
  Working with DiffServ & Low Latency .................................12
  Working with Differentiated Services (DiffServ) ...................12
  Working with Low Latency Classes .....................................13
  Working with Authenticated QoS .........................................13
  Debugging QoS-related Scenarios ........................................14
Completing the Procedure .......................................................14
Verifying QoS Works ...............................................................15
How To Configure FloodGate-1

Objective

This document explains steps for setting up Floodgate, and ways of troubleshooting QoS (quality of service) issues.

Supported Versions

- Supported on all versions up to R71
- Supported on all Platforms that appear in HCL: http://www.checkpoint.com/services/techsupport/hcl/all.html
- Supported on all operating systems that valid in TimeLine list: http://www.checkpoint.com/services/lifecycle/support_periods.html
- QoS feature supported on SmartDashboard

Before You Start

Related Documentation and Assumed Knowledge

- FloodGate-1 FAQ http://supportcontent.checkpoint.com/documentation_download?id=9037

Impact on the Environment and Warnings

- Network performance degradation and slowness can be experienced from time to time, depending on QoS configuration. It is important to perform the correct configuration in order to avoid slowness in network speed and bandwidth.
- Delay, jitter and packet loss can occur during high network performance.
- For correct operation, QoS should be activated on the external interfaces only.
- The protocols/services that are supported by Check Point QoS are listed in: http://www.checkpoint.com/products/downloads/vpn-1_fw-1_fg-1_app_support.pdf http://www.checkpoint.com/products/downloads/vpn-1_fw-1_fg-1_app_support.pdf
Background Information

Technology Overview

- Check Point QoS is a policy-based, Quality of Service (QoS) solution for VPNs, private WANs and Internet links. It optimizes network performance by assigning priority to business-critical applications and end users.

- Check Point QoS is tightly integrated with VPN-1® Pro

- A Check Point QoS policy comprises rules that specify the weights, limits and guarantees that are applied to the different classifications of traffic.

- A rule can have multiple sub-rules, enabling an administrator to define highly granular Bandwidth Policies.

FloodGate-1 Innovative Technologies

FloodGate-1 implements the following four innovative technologies:

- **Stateful Inspection**: FloodGate-1 incorporates Check Point’s patented Stateful Inspection technology to derive complete state and context information for all network traffic.

- **Intelligent Queuing Engine**: FloodGate-1’s Intelligent Queuing Engine (IQ EngineTM) uses the traffic information, derived by the Stateful Inspection technology, to accurately classify traffic and place it in the proper transmission queue. The network traffic is then scheduled for transmission based on the QoS Policy.

  The IQ Engine includes an enhanced, hierarchical Weighted Fair Queuing (WFQ) algorithm to precisely control the allocation of available bandwidth and ensure efficient line utilization.

- **WFRED (Weighted Flow Random Early Drop)**: FloodGate-1 makes use of the WFRED mechanism, which manages packet buffers transparently to users and does not require pre-configuration.

- **RDED (Retransmission Detection Early Drop)**: FloodGate-1 makes use of the RDED mechanism, which reduces the number of retransmits and retransmit storms. This Check Point mechanism drastically reduces retransmit counts, greatly improving the efficiency of the enterprise’s existing lines. The increased bandwidth that FloodGate-1 makes available to important applications comes at the expense of less important (or completely unimportant) applications. Thanks to this, the organization can make do with existing bandwidth and significantly delay purchasing more.
Bandwidth Allocation and Rules

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

- Weight
- Guarantees
- Limits

**Weight**

Weight is the relative portion of the available bandwidth that is allocated to a rule. To calculate what portion of the bandwidth the connections matched to a rule receive, use the following formula:

\[
\text{this rule’s portion} = \frac{\text{this rule’s weight}}{\text{total weight of all rules with open connections}}
\]

For example, if this rule’s weight is 12 and the total weight of all the rules under which connections are currently open is 120, then all the connections open under this rule are allocated 12/120 (or 10%) of the available bandwidth.

In practice, a rule may get more than the bandwidth allocated by this formula, if other rules are not using their maximum allocated bandwidth. 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 utilization of the line even if a specific class is not using all of its bandwidth. In such a case, the left over bandwidth is divided among the remaining classes in accordance with their relative weights.

**Guarantees**

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

Guarantees can be defined for:

- The sum of all connections within a rule
  A total rule guarantee reserves a minimum bandwidth for all the connections under a rule combined. 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 can be no less than the guarantee, but the more connections that are open, the less bandwidth each one receives.

- Individual connections within a rule
  A per connection guarantee means that each connection that matches the particular rule is guaranteed a minimum bandwidth. Although weights do in fact guarantee the bandwidth share for specific connections, only a guarantee allows 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 beyond which connections under a rule are not allocated bandwidth, even if there is unused bandwidth available.

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

In this section:

- Direction and Rate 8
- Global Settings 10
- Configuring the Policy Type 11
- Configuring QoS Rule Bases 12
- Working with DiffServ & Low Latency 12
- Working with Authenticated QoS 13
- Debugging QoS-related Scenarios 14
Direction and Rate

This is the first thing that needs to be configured.

1. From the Gateway page, select General Properties. Select the Network Security tab and mark the module as QoS installed in the Check Point products list of the Gateway.

2. Click OK.
3. Define on which interfaces to activate the QoS, and the speed of those interfaces. From the Gateway page, select Topology. In the Interface Properties section select the QoS tab and enter the required parameters.

4. Click OK.
Global Settings

- From the Gateway page, expand Global Properties and select QoS.

On this page there are additional settings that can be tweaked, such as how to display the rate (bps, MBps, kBps...), weight settings, and various timeouts.

These settings can usually be left at the default values.

Configuring the Policy Type

FloodGate-1 can be configured by either an Express (and less Granular) policy, or by using the Traditional Policy. The selection of policy type is done when a new policy Package is created.

Both Traditional and Express modes of Check Point QoS are included in every product installation.

- **Express mode** enables you to define basic policies quickly and easily and thus “get up and running” without delay.

- **Traditional mode** incorporates the more advanced features of Check Point QoS.

You can specify whether you choose Traditional over Express or vice versa, each time you install a new policy.

You can change a policy from Express mode to Traditional mode. However, you cannot change a policy from Traditional mode to Express mode. Therefore it is recommended that if you are unsure which policy to install, you should begin with Express mode, maintaining the option to transition to Traditional mode, if you find that your policy required heightened Check Point QoS functionality.

For more information on the differences between the two policy types, refer to R71 QoS Admin Guide.

http://supportcontent.checkpoint.com/documentation_download?id=10312
Configuring QoS Rule Bases

QoS policy is implemented by defining an ordered set of rules in the Rule Base in QoS tab.

The Rule Base comprises those rules which you create, plus a default rule. The default rule is automatically created with the Rule Base. It can be modified but cannot be deleted.

The fundamental concept of the Rule Base is that unless other rules apply, the default rule is applied to all data packets. The default rule is therefore always the last rule in the Rule Base.

<table>
<thead>
<tr>
<th>NAME</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
<th>TIME</th>
<th>COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site to Site VPN</td>
<td>GW-group</td>
<td>GW-group</td>
<td>SUB</td>
<td>Log</td>
<td>All</td>
<td>Any</td>
<td></td>
<td>Prioritize VPN traffic between sites</td>
</tr>
<tr>
<td>Web</td>
<td>GW-group</td>
<td>SUB</td>
<td>HTTP</td>
<td>Log</td>
<td>All</td>
<td>Any</td>
<td></td>
<td>Prioritize HTTP traffic to and from remote</td>
</tr>
<tr>
<td>Default</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Log</td>
<td>All</td>
<td>Any</td>
<td></td>
<td>Prioritize HTTP traffic based on the source</td>
</tr>
</tbody>
</table>

Defining Sub-Rules:

Sub-rules are rules that allocate bandwidth more specifically within a rule.

For example, you may wish to allocate bandwidth for HTTP connections by source, so that HTTP connections from a specific source will receive more bandwidth than other HTTP traffic.

In this case, you would define sub-rules under Web Rule which will specify the specific source.

Working with DiffServ & Low Latency

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.
Working with Low Latency Classes

FloodGate-1 Low Latency Queuing makes it possible to define special classes of service for “delay sensitive” applications like voice and video. Rules under these classes can be used together with other rules in the QoS Policy Rule Base. Low Latency classes require you to specify the maximal delay that is tolerated, and a Constant Bit Rate. FloodGate-1 then guarantees that traffic matching rules of this type are forwarded within the limits of the bounded delay.

To modify DiffServ and Low Latency classes:

- From the Gateway page, select Topology. In the Interface Properties section select the QoS tab. Under the section: DiffServ and Low Latency classes, Click Add to add a new class, or Edit to edit the properties of an existing class.

Example of configuration of LLC and DiffServ:

![Configuration of LLC and DiffServ](image)

Working with Authenticated QoS

Check Point Authenticated QoS provides Quality of Service (QoS) for end-users in dynamic IP environments, such as remote access and DHCP environments.

This enables priority users, such as corporate CEOs, to receive priority service when remotely connecting to corporate resources.
Debugging QoS-related Scenarios

Please run all the following debugs in parallel, at the same time, and stop them as shown below.

1. Enable FloodGate-1 process debug:
   From the CLI, run:
   
   ```bash
   # fw debug fgd50 on TDERROR_ALL_ALL=5
   # fw debug fgd50 on OPSEC_DEBUG_LEVEL=9
   ```

   To stop the debug:
   run:
   
   ```bash
   # fw debug fgd50 off TDERROR_ALL_ALL=0
   # fw debug fgd50 off OPSEC_DEBUG_LEVEL=0
   ```

   The output file should be located on $FGDIR/log

2. FireWall-1 Kernel primary debug for packet filter analysis.
   
   ```bash
   # fw ctl debug 0
   # fw ctl debug –buf 32000
   # fw ctl debug –m FG-1 all
   # fw ctl kdebug –f > output_file
   ```

   To stop the debug:
   run:
   
   ```bash
   # fw ctl debug 0
   ```

   Find more about Kernel debug options in sk41585
   http://supportcontent.checkpoint.com/solutions?id=sk41585

3. Perform firewall monitor to verify that packets tagged with QoS pass inspection points of the Firewall.
   
   For more information regarding firewall monitor, refer to sk30583

Completing the Procedure.

Make sure you have installed a QoS license. The License should look like the following with QOS inside its name, : CPTC-QOS-1-NGX

**To start FloodGate-1:**

- Perform a Policy installation, in the CLI run:
  
  ```bash
  # etmstart
  ```
Verifying QoS Works

- Check that the fgd50 daemon is running using the following command:
  
  ```sh
  # ps -aux | grep fgd50
  ```

- Verify that you can perform a Policy Installation with QoS enabled.

- Perform a download test from the required source with relevant configured service.

- Check the status of FloodGate-1 on CLI and that QoS Policy is installed:

  ```sh
  # fgate stat
  ```
  The output should look like this:

  ```
  F.E
  ```

  ```
  fgate stat
  FW [admin]# fgate stat
  ```

  ```
  Product: FloodGate-1
  Version: NGX (R65) HFA_30, Hotfix 603
  Kernel Build: 2
  Policy Name: QOS_policy (Traditional Mode)
  Install time: Mon Aug 30 14:30:30 2010
  Interfaces Num: 1
  ```

  ```
  Interface table
  "Name "^Dir"^Limit ^Avg Rate^Conns^Pend pkts^Pend bytes^Rxmt pkts^  
  --------^-------------------------
  ^ae3c0^in ^1280000^ 187675^ 832^ 0^ 0^ 0^  
  ^ae3c0^out^1280000^ 75384^ 872^ 0^ 0^ 0^  
  ```

- Manually fetch a QoS policy, using the following command:

  ```
  fgate fetch fwmanager
  ```
  For more information, use sk38926.

- Load a Policy manually in debug mode on the Management module to the Firewall, using the following command:

  ```
  # fgate -d load $FWDIR/conf/QOS_policyname>.F
  ```
  ```
  [module resolvable name or IP address] &> fgiinstall.txt
  ```