

CheckPoint Software Technologies LTD.ä

*How to Configure & Demo
Integrated QoS with FloodGate-1*

Event: Partner Exchange Conference

Date: October 5, 1999

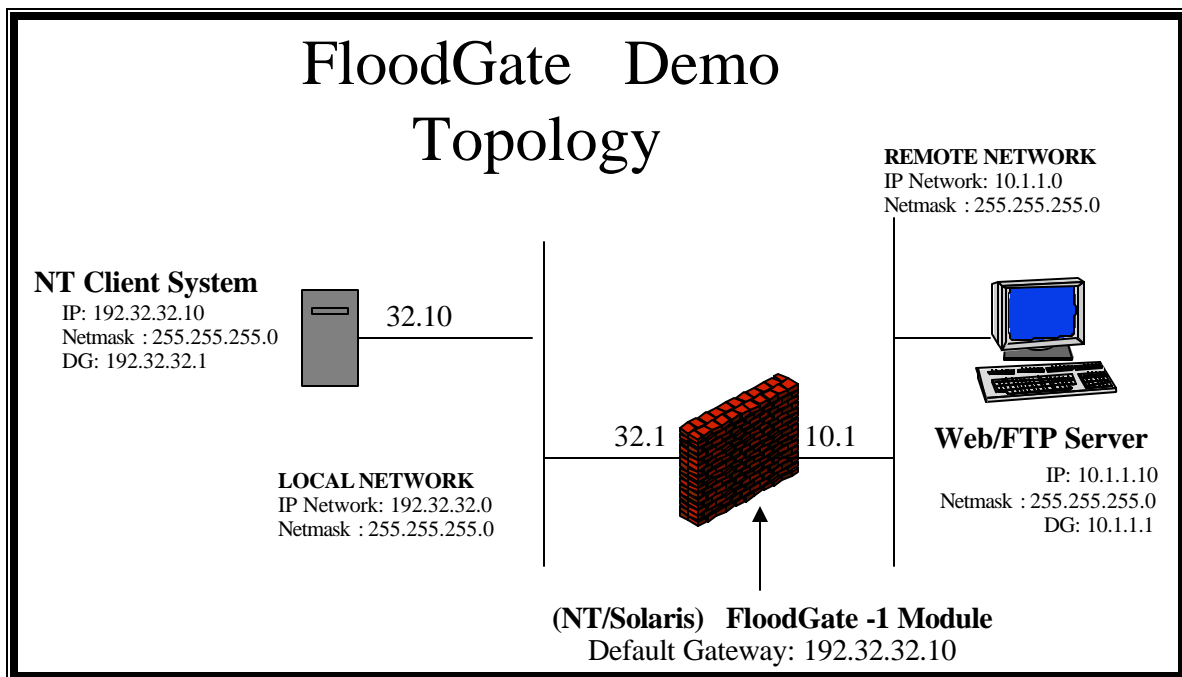
Revision 1.2

Author: Lewis Colascione Jr., Regional Technical Manager, NE.

Enterprise Traffic Management QoS with integrated Floodgate-1

Limited bandwidth is common customer issue. Two solutions to this are to purchase more bandwidth or manage the existing bandwidth. With Floodgate-1 our customers have the ability to mandate and deploy an enterprise wide policy on how data flows through their networks and VPN's. Floodgate-1 can run on a stand-alone gateway or integrated on a VPN-1 Gateway providing integrated access control, authentication, and VPN. This document outlines how to build and demonstrate the integrated QoS in Floodgate-1 v4.1.

NOTE: The goal of this document is to show how to build a topology from which to demonstrate Floodgate-1 to your customers with minimal hardware.



Goal of the Demo :

- Show how deploying a Floodgate-1 policy can dynamically manage bandwidth based on an enterprise traffic policy.

- **Required Equipment Needed:**

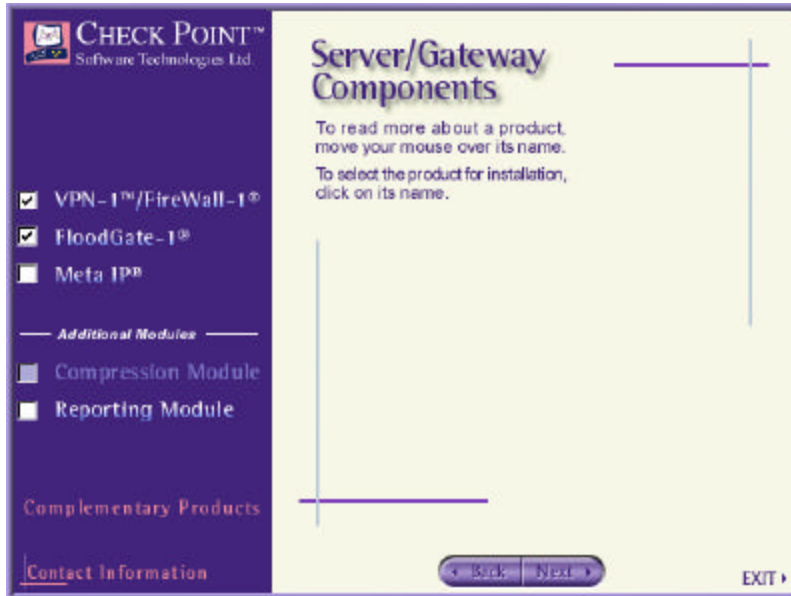
- NT or Solaris system with 2 network interface adapters, 128MB Ram for the Gateway.
- Operating Systems: NTv4.1(SP4) or Solaris v2.6 or higher.
- Check Point VPN-1/FloodGate-1 v4.1 or higher
- 2 Ethernet hubs or switches
- 2 additional systems with one running a service to be managed i.e. HTTP, FTP, etc.
- 4 Cat-5 Ethernet patch cables.

Configuration overview:

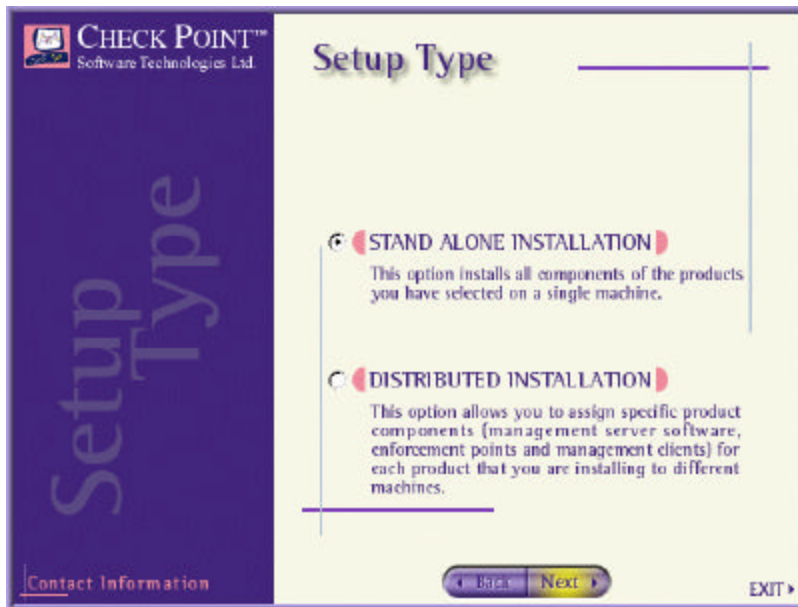
1. Interconnect systems and hubs as per topology diagram.
2. Configure Network interfaces and routing. Insure you can ping from the Client system to the application server on the Remote Net.
3. Install FloodGate-1 Module and Management Server & GUI on Gateway system.
NOTE: You can also install the VPN-1 Module as well on the same box. On Solaris use the *InstallU* installation utility to install both components simultaneously on a single gateway.
4. Install IIS or some other FTP or HTTP service on one server system to provide the service to be tested through the Floodgate gateway.
5. Create objects in the GUI to represent the FloodGate gateway and the 2 networks on either side.
6. Define and install a policy for the services to be tested.
7. Bring up the FloodGate real-time monitor.
8. Open an FTP connection between the client and server systems through the gateway and monitor the traffic with the real-time monitor.
9. Change the policy to show Floodgate-1 modifying the traffic flow.
10. View the bandwidth changes in the real-time monitor.

Configuration Details:

1. Install VPN-1/FloodGate-1 on the Gateway from the Check Point Enterprise CD.
NOTE: The equivalent utility in Solaris is InstallU in the root directory of the Enterprise CD.



You can install FloodGate-1 by itself or also install VPN-1 if you would like to show the integration of QoS, VPN, & Access control. The GUI's are integrated.



During the install choose the Stand Alone option. This will tell the installation wrapper to install all components on the gateway system.
(i.e. Floodgate-1/VPN-1 Enforcement Module + The Management Server + The GUI Interface.)

2. Once installed bring up the GUI and create the necessary network objects.
During installation you should go right into the configuration utility and configure the basic settings on the management server and module. If you did not go right into the configuration utility bring it up manually to add an administrator account to the management server.

- On NT: **Start -> Programs -> Check Point Management Clients -> Configuration**
- On Solaris: **\$FWDIR/bin/cpconfig**

NOTE: IT is assumed that you created an administrator ID for Floodgate-1/VPN-1 on the management server. For our demo we created an ID of *fwadmin* with read/write permissions to both modules.

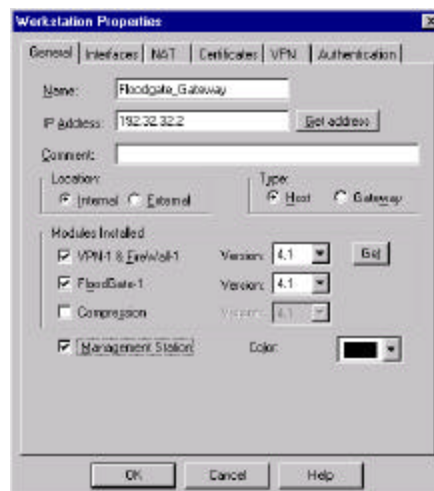
Start the integrated GUI:

- On NT: **Start -> Programs -> Check Point Management Clients -> Policy Editor 4.1**
- On Solaris: **\$FWDIR/bin/fwpolicy**
- Login to the Management Server.



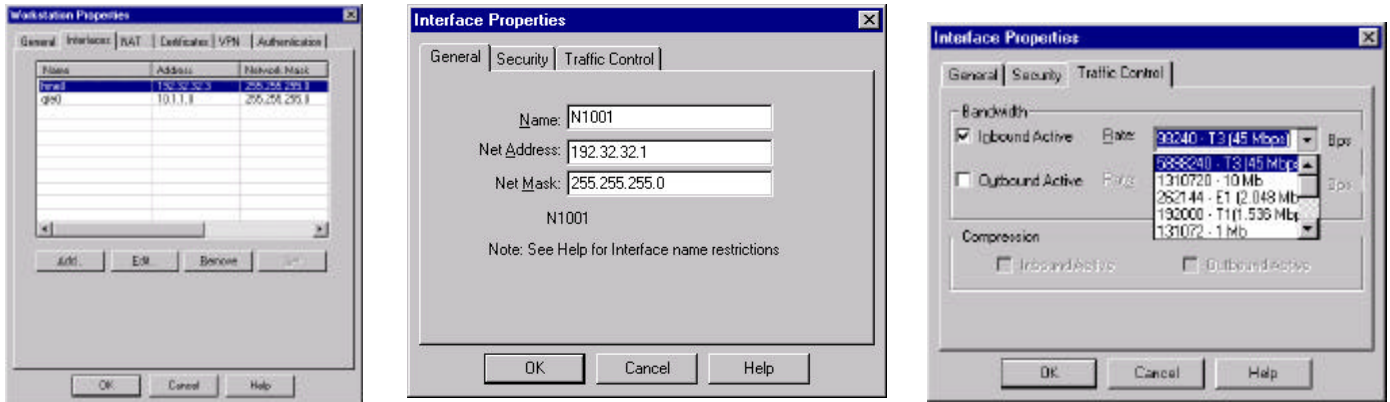
3. Create the Network Objects:

- Floodgate_Gateway – 192.32.32.1
- Local_Net - 192.32.32.0
- Remote_Net – 10.1.1.0

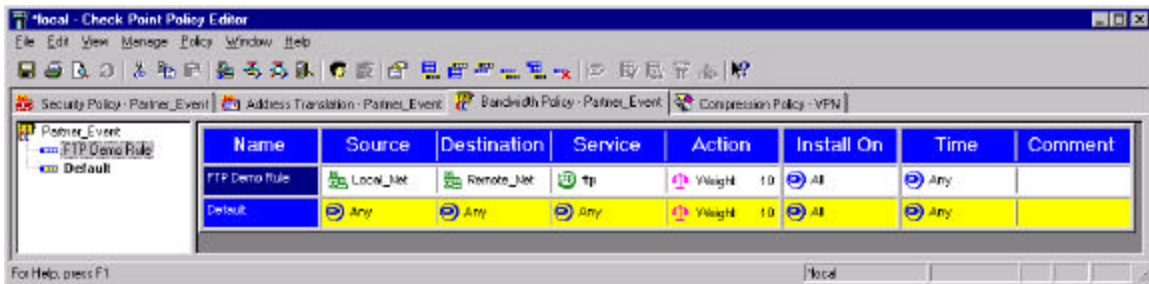


For the Gateway object fill in the name and network criteria. Check the appropriate box if the Gateway is running Floodgate alone or integrated with VPN-1/Firewall-1. Check the box indicating that this is a management server as well.

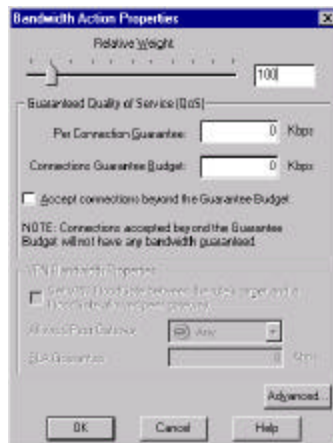
In the Interfaces tab click on “Get” to fill in the local Interface information. *Edit* each interface to configure it for Traffic Management and or Anti Spoofing if it is a Firewall as well. Select the active interfaces, direction, and bandwidth. For our demo we are providing QoS in an inbound direction only.



4. Create a Bandwidth policy and install it on the module. Under the Floodgate-1 tab of the Policy Editor add a rule called **FTP Demo Rule** to the top of the policy. Select the criteria Source: Local_Net, Destination: Remote_Net, Service: ftp.

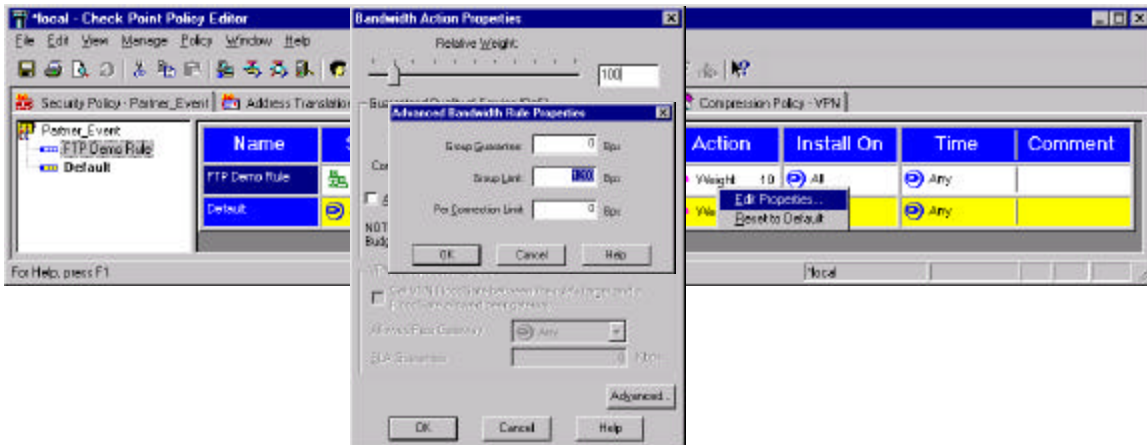


Change the Action to a Weight of **100** by clicking your right mouse button in the Action dialog box:

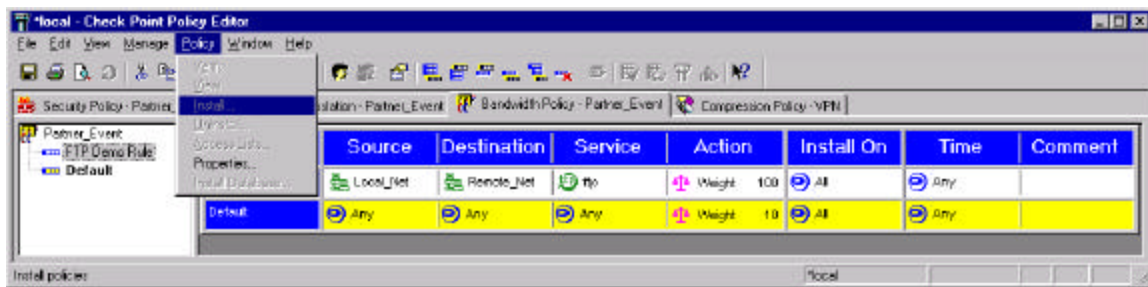


Change the relative weight to **100**.

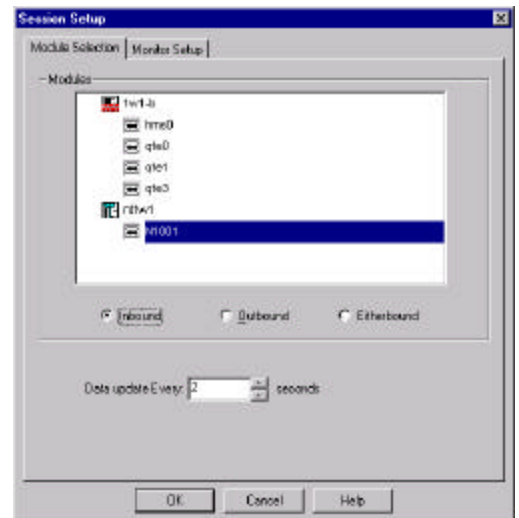
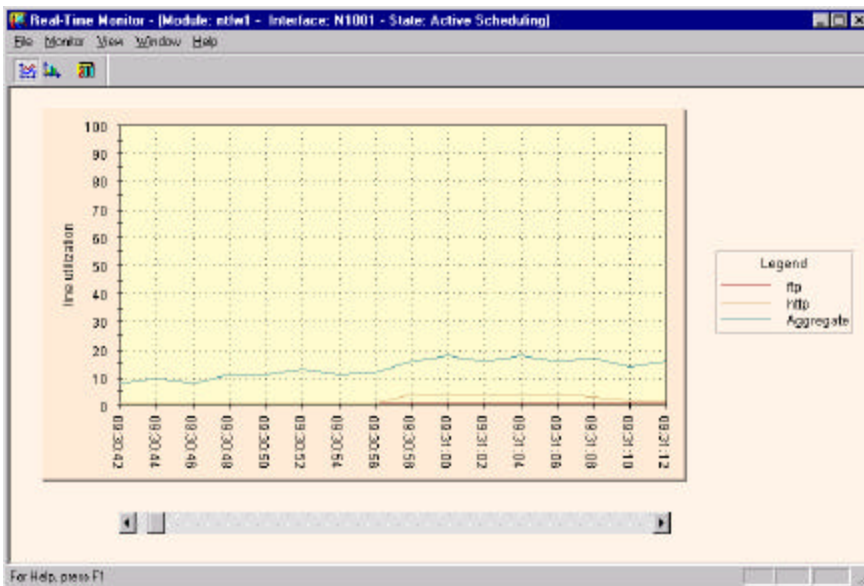
Click on *Advanced* and set a Group Limit on connections to 1200Bps. This will limit the FTP during the demo to 1200 Baud.



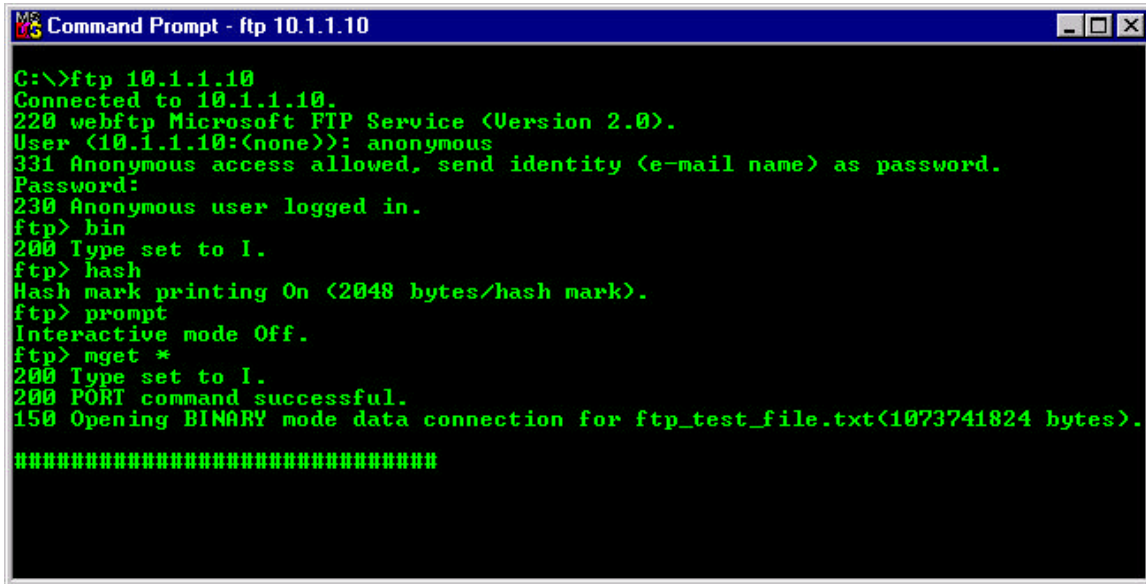
Install the Policy: *Policy -> Install*



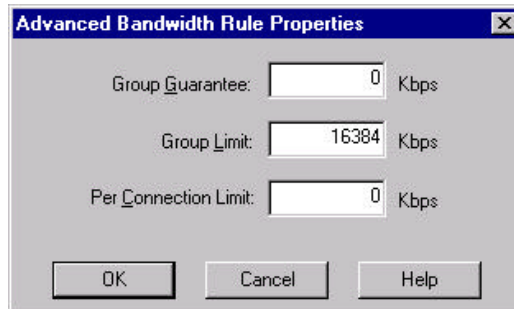
5. Bring up the FloodGate real time GUI and select the external 192.32.32.1 interface to monitor;



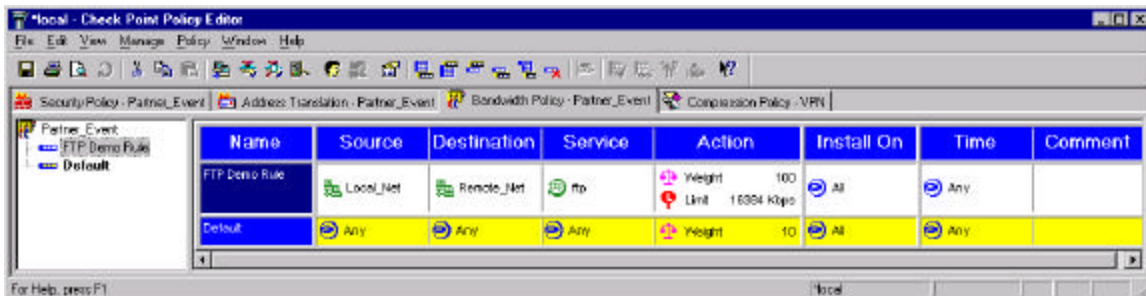
- Now Initiate an FTP from the system on the Local_Net to the system on the Remote_Net. Be sure to FTP something large and turn on the HASH marks.



- With this bandwidth policy the FTP will be getting the equivalent of 1200Bps. Now we will speed things up using the Floodgate engine. Go into the Action properties and click on *Advanced* Again:



We will set a limit on this rule to 16KBps.
Install the new policy:



- Within a few seconds the HASH marks will speed up to reflect the change in the bandwidth policy. The FTP application now thinks it is going through a 16K pipe. Check the Real-time GUI to see the increase in FTP traffic flow. Note the change in the real time GUI.