



The NGX platform delivers a unified security architecture for Check Point perimeter, internal, and Web security.

PRODUCT DESCRIPTION

FloodGate-1® solves the network congestion problem with a policy-based QoS management solution included with VPN-1® Power and integrated with VPN-1 UTM as an optional feature.

PRODUCT FEATURES

- Integrated with VPN-1 Power, optional component of VPN-1 UTM
- QoS for both encrypted and unencrypted traffic
- Performance analysis through optional SmartView Monitor™
- Load sharing through ClusterXL™
- Integrated DiffServ support and low-latency queuing

PRODUCT BENEFITS

- Optimizes network performance for VPN and unencrypted traffic
- Enables proactive management of network costs
- Eliminates need to deploy separate VPN, firewall, and QoS or management devices
- Provides revenue opportunities for Service Providers by enabling end-to-end QoS for IP networks

NGX HIGHLIGHTS

- Integrated with Check Point's Unified Security Architecture



Check Point protects every part of your network—perimeter, internal, Web—to keep your information resources safe, accessible, and easy to manage.

FloodGate-1

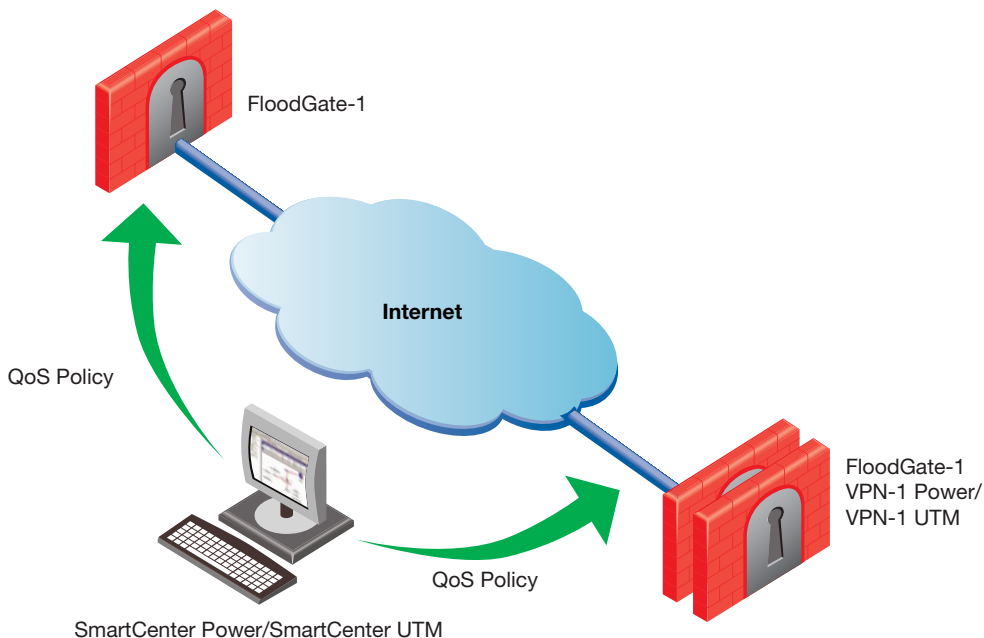
Quality of Service for VPN-1

YOUR CHALLENGE

Organizations around the world, including yours, are increasingly using IP-based technologies to support critical applications on VPN, Internet, and private WAN links. Yet increased traffic on access links can lead to congestion, with discretionary traffic overwhelming business-critical traffic. The effect on your business can be severe—slow response times can reduce employee productivity, and customers can have negative online experiences.

OUR SOLUTION

Check Point solves the network congestion problem with FloodGate-1®, a policy-based Quality of Service (QoS) management solution. FloodGate-1 lets you to prioritize business-critical traffic such as ERP, database, and Web services traffic over less time-critical traffic. It also allows you to guarantee bandwidth and control latency for streaming applications such as Voice over Internet Protocol (VoIP) and video conferencing. In addition, with highly granular controls, FloodGate-1 enables guaranteed or priority access to specific employees—even if they are remotely accessing network resources through a VPN tunnel.



FloodGate-1 is a policy-based QoS solution that is integrated into VPN-1 gateways.

Deployed with Check Point's VPN-1® Power and, as an option, VPN-1 UTM security gateways, FloodGate-1 is completely integrated into these solutions. It provides QoS for both VPN and unencrypted traffic, maximizing the benefit of a secure, reliable, low-cost VPN network.

FLEXIBLE QOS POLICIES

FloodGate-1 precisely controls the flow of inbound and outbound traffic at WAN and Internet access points, based on a QoS policy. The policy comprises rules that assign bandwidth privileges to specific traffic classes. Each rule within a policy defines traffic classification criteria and corresponding QoS controls.

Traffic classification

FloodGate-1 enables you to classify traffic using a broad set of criteria by leveraging Check Point-patented Stateful Inspection technology. FloodGate-1 classifies traffic using the following criteria:

- Source, destination
- Traffic direction
- Time of day
- Internet service, application
- URL designator
- User groups with static or dynamic IP addresses

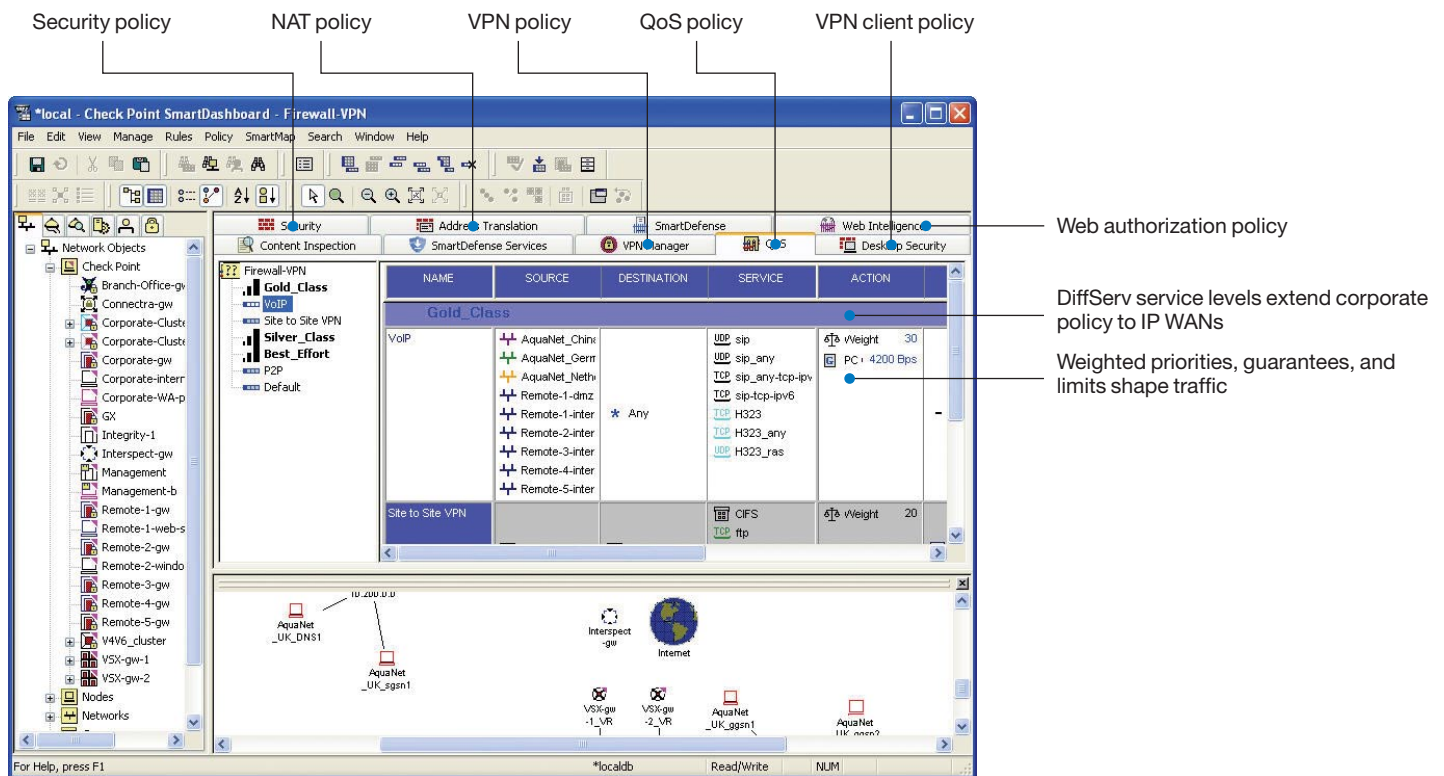
Authenticated QoS, an innovative feature found only in FloodGate-1, provides performance guarantees for users in dynamic IP environments. This enables VIP users to receive priority service even when remotely connecting to corporate resources.

Local access link controls

Once a packet has been classified, QoS control criteria are used to assign privileges to critical traffic and to limit less important traffic. Primary QoS control criteria include weighted priorities, guarantees, and limits. FloodGate-1 also provides low latency queuing (LLQ) controls for latency-sensitive traffic.

Weighted priorities—allocates bandwidth according to relative merit as defined by business goals. For example, you may deem secure electronic commerce transactions (HTTPS) to be twice as important as catalog browsing (HTTP). When congestion occurs, FloodGate-1 ensures the data ratio is maintained at 2:1.

An unlimited number of priorities can be defined. By allocating bandwidth according to weights, FloodGate-1 ensures that no class of traffic is completely starved.



The QoS policy (shown) as well as firewall, VPN, and NAT policies are defined through SmartDashboard.

Guarantees—allocates minimum bandwidth levels to traffic that requires certain service levels at all times. For example, streaming applications, such as video conferencing, require a minimum amount of bandwidth in order to function properly. Guarantees can be set for a group of connections in aggregate, or on a per-connection basis. FloodGate-1 guarantees permit unused bandwidth to be loaned to other traffic classes.

Limits—sets bandwidth restrictions for non-critical network applications. For example, a typical implementation might limit MP3 downloads, Instant Messaging, and non-business-critical Peer-to-Peer traffic.

Low latency queuing (LLQ)—controls, comprising maximum delay and constant bit rate (CBR) settings, reduce delay for latency-sensitive traffic. LLQ controls are typically implemented to help ensure high-quality VoIP and videoconferencing traffic.

End-to-end controls

Integrated Differentiated Services (DiffServ) enables Service Providers to offer end-to-end QoS for VPN and unencrypted traffic on IP WANs. By prioritizing traffic according to DiffServ, FloodGate-1 enables corporate QoS requirements to be extended to the WAN.

SMART management

Check Point's Security Management Architecture (SMART™) solutions enable you to centrally manage and deploy a single QoS policy to an unlimited number of FloodGate-1 gateways. Once a policy is created or modified, it is automatically distributed to all locations.

VPN-1 customers benefit from an integrated VPN, firewall, intrusion prevention, and QoS management console that leverages shared network objects and user groups. Administrative rights can be defined flexibly to allow different people to manage QoS and VPN/firewall security policies.

SMART performance analysis

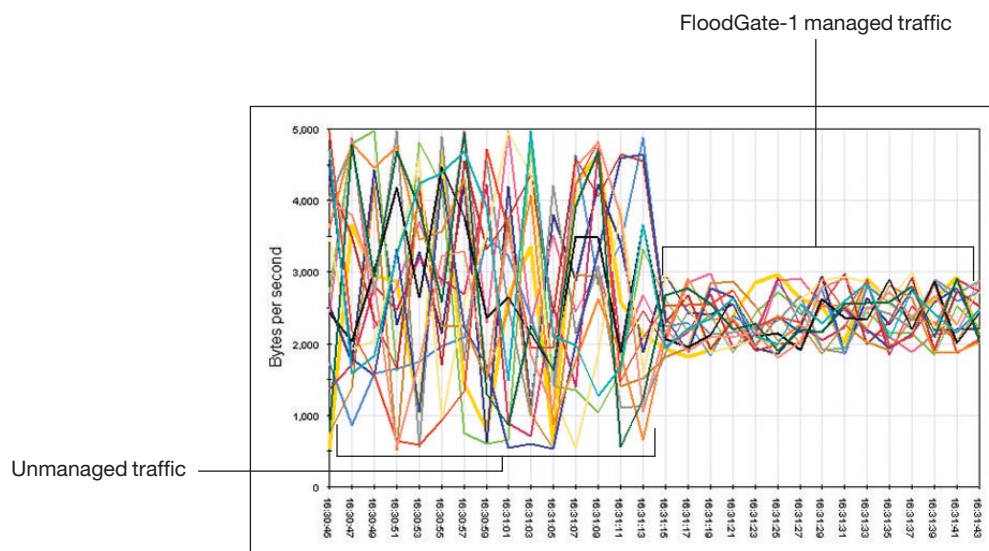
SmartView Monitor™, an optional add-on, enables you to control application performance to maximize return on investment for WAN bandwidth. SmartView Monitor collects performance data at the gateway and continuously streams it to a central SmartCenter™ server. This enables you to centrally monitor traffic through a specific gateway by QoS rule, service, or network object, and to easily create bandwidth utilization reports. Customers also implementing VPN-1 Power or VPN-1 UTM can monitor end-to-end performance of site-to-site VPN tunnels.

SMART status monitoring and auditing

SmartView Status™ and SmartView Tracker™, included with centralized management solutions, simplify tracking and responding to network events.

SmartView Status—provides real-time data on the health of Check Point gateways. FloodGate-1 data includes status, pending packets, and pending bytes.

SmartView Tracker—integrates FloodGate-1 and VPN-1 log files and provides real-time graphical tracking, monitoring and accounting information for all logged connections.



SmartView Monitor can be used to view the impact of a FloodGate-1 QoS policy.

Innovative technology

FloodGate-1 leverages INSPECT, the industry's most adaptive and intelligent inspection technology, to classify traffic by service or application. After a packet has been classified, FloodGate-1 applies QoS controls and then employs an innovative, hierarchical, weighted fair queuing (WFQ) algorithm to precisely control bandwidth allocation. This state information is used to classify traffic by service or application.

Secure choice

FloodGate-1 is supported on a broad range of deployment platforms—meeting the price/performance requirements of any size organization.

Additional capabilities

FloodGate-1 supports a number of other Check Point modules, including:

- SmartCenter UTM/SmartCenter Power, which delivers centralized management for all Check Point security, VPN, and QoS offerings
- Provider-1®/SiteManager-1™, which offers centralized management for all Check Point security, VPN and QoS offerings, as well as consolidates multiple security policies in an architecture that scales to support thousands of policies

- SmartUpdate™, providing centralized software and license management for Check Point products to ensure that a consistent security policy is enforced throughout the enterprise network
- Eventia Reporter™, a complete reporting system that delivers in-depth network security activity and event information from Check Point log data
- ClusterXL™, a software-based load sharing and High Availability solution for Check Point gateways

| System requirements | |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supported platforms | SecurePlatform, SecurePlatform Pro, Solaris UltraSPARC 8, 9, 10, Windows Server 2003 (Windows 2000 Server (SP1-4), Windows 2000 Advanced Server (SP1-4), RedHat Enterprise Linux 3.0 Kernel 2.4.21, Nokia IPSO 3.9, 4.0, 4.0.1, 4.1 |
| Disk Space | 20 MB |
| Memory | 256 MB (assumes FloodGate-1 is running on the same machine as VPN-1 Power/VPN-1 UTM) |

©2003-2006 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, ConnectControl, Connectra, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpec, IQ Engine, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Office, SecureClient, SecureKnowledge, SecuRemote, SecurePlatform, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, SiteManager-1, SmartCenter, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartL.SM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988, and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

August 14, 2006 P/N 502246

Worldwide Headquarters
3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753-4555
Fax: 972-3-575-9256
Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391; 650-628-2000
Fax: 650-654-4233
www.checkpoint.com

