BIG-IQ Security

DATASHEET

What's Inside

2 Centralized Policy Management

3 Policy Auditing and Security Compliance

3 Policy Monitoring and Tuning

4 BIG-IQ Security Support for BIG-IP ASM

4 BIG-IQ Security Specifications

4 More Information

Simplify Firewall Policy Management

Large organizations face a growing challenge: managing a consistent and effective security posture across an ever-expanding number of firewall devices. Too often, security administrators must independently manage each firewall device, reducing operational scalability and increasing overhead costs. In addition, configuring every firewall device in an isolated setting raises the risk of error and obscures the visibility and correlation of policies across the infrastructure.

F5® BIG-IQ™ Security centralizes policy deployment and administration for organizations managing security with F5 BIG-IP® Advanced Firewall Manager™ (AFM) and F5 BIG-IP® Application Security Manager™ (ASM). BIG-IQ Security provides administrators with a consolidated view of security policies across the entire BIG-IP AFM and ASM infrastructure. Additionally, BIG-IQ Security makes it easy to manage the entire firewall policy lifecycle for BIG-IP AFM and evaluate the effectiveness of specific policies across multiple devices, audit configuration changes to assess the results, and ensure regulatory compliance for BIG-IP AFM and ASM deployments.

Key benefits

Reduce operational costs and administrative time

Manage security policies across multiple BIG-IP AFM devices from a single pane of glass.

Increase operational scalability

Scale your firewall infrastructure without increasing management time.

Reduce errors and downtime

Eliminate redundant and error-prone manual configuration tasks.

Mitigate compliance risks

Easily audit current policies and past changes and compare configurations across multiple BIG-IP AFM devices.

Monitor the effectiveness of firewall policies

See which firewall policies are triggered the most and how they're affected by changes in network traffic.

Control administrative privileges

Limit administrative accounts to specific roles, groups, or tasks.

Centralized Policy Management

BIG-IQ Security provides a single, centralized point from which administrators can manage a consistent and effective security posture across the entire BIG-IP AFM and BIG-IP ASM deployment.

A single pane of glass

BIG-IQ Security consolidates firewall policy management across multiple BIG-IP firewall devices to a single point of control. Users can view policies and push policy changes to multiple firewall devices from a single, centralized location. Additionally, for BIG-IP AFM, administrators can modify existing firewall policies and create new policies. With BIG-IQ, administrators can easily view which policies are active and where, searching through the full set of the organization's security policies to find specific policies and identify the firewall devices on which they are running.

Shared firewall policies

BIG-IQ Security provides significant flexibility in applying centrally-managed security policies. Apply new policies or policy changes to a specific BIG-IP firewall device, to a combination of firewall devices, or across the entire BIG-IP AFM or BIG-IP ASM deployment.

Role-based access and control

BIG-IQ Security enables the delegation of administrative tasks across trusted BIG-IP AFM users based on roles. Administrative access can be defined according to job competency, title/authority, and responsibility, minimizing administrative errors that can negatively impact the overall security posture.

Intuitive and contextual management

BIG-IQ Security provides an innovative graphical user interface that simplifies administrative tasks across multiple firewall devices. The interface combines a logical layout with contextual cues to help administrators parse through large amounts of configuration data about their firewall deployment. This relationally aware approach makes it easier for administrators to understand the relationships between different policies and firewall devices, investigate specific areas or issues, and make appropriate decisions or changes.

BIG-IQ Security displays views of security policy deployment with context, simplicity, and clear organization.

Policy Auditing and Security Compliance

By centralizing firewall policy management, BIG-IQ Security makes it easy for administrators to verify existing policies, audit any policy changes, and track policy deployment to individual firewall devices.

Verification of firewall configuration

Using the relationally aware interface of BIG-IQ Security, administrators can view the full set of policies running on any BIG-IP firewall devices to compare configurations on multiple firewall devices and verify compliance with corporate policy. In addition, administrators can search for individual firewall policies to identify devices on which those policies are deployed.

Policy staging and evaluation

BIG-IQ Security enables administrators to stage and evaluate new or altered policies before deploying them to active BIG-IP AFM devices, reducing the possibility of configuration error.

Centralized auditing and control

With BIG-IQ Security, all firewall policy changes are made at a single location rather than through manual changes on individual BIG-IP firewall devices. BIG-IQ Security records every policy change or deployment to BIG-IP firewall devices in a central audit log. Administrators and auditors can examine the log to view details and identify when changes were made and by whom.

Policy Monitoring and Tuning

To help maximize the effectiveness of firewall deployments, BIG-IQ Security provides ongoing monitoring of firewall policies deployed across the BIG-IP AFM environment.

Policy monitoring

With BIG-IQ Security, an administrator can quickly determine the effect of firewall policies on the organization's security posture in real time. BIG-IQ Security continuously monitors and reports on the number of times that individual rules are triggered and reports on the most and least frequently applied, making it easy to observe the effectiveness of individual firewall policies.

Configuration snapshots and rollbacks

Using configuration snapshots, administrators can quickly review the history of policy changes, understand the depth of revisions made over time, and restore objects to a previous state. This powerful functionality provides deeper visibility into policy change, maximizes object use, and enables administrators to instantaneously restore previous configurations.

Firewall device optimization

The policy monitoring enabled by BIG-IQ Security can help administrators optimize the performance of firewall devices. By prioritizing the policies that are frequently triggered and modifying or deleting those that are infrequently triggered or unused, administrators can reduce the CPU utilization of the firewall device.

Insight for decisions

BIG-IQ Security provides integrated monitoring of BIG-IP AFM rules so administrators can easily manage security policy and quickly respond to today's changing threats and ever-evolving attack profiles. With increased information about firewall deployment, administrators can determine how the firewall is performing and assess the organization's overall security posture.

BIG-IQ Security Support for BIG-IP ASM

BIG-IQ Security provides a single view of the entire BIG-IP Application Security Manager infrastructure and enables simplified deployment of firewall policies across multiple BIG-IP ASM devices. Users are currently able to discover BIG-IP ASM instances, import, and export configurations; deploy policies to one or many BIG-IP ASM devices; and parse large amounts of configuration data. The ability to create and edit BIG-IP ASM policies and apply role-based access controls will be added in the near future.

BIG-IQ Security Specifications

BIG-IQ Security is available as a virtual edition supporting all major hypervisor technologies.

Host System Requirements	
Hypervisor	VMware vSphere Hypervisor 4.0, 4.1, or 5.0 Citrix XenServer 5.6 Microsoft Hyper-V for Windows Server 2008 R2
Processor	2-4 CPU cores. F5 highly recommends that the host system contain CPUs based on AMD-V or Intel VT technology.
Memory	2-8 GB RAM
Network Adapters	2-8 network interfaces
Disk Space	250 GB or more

More Information

To learn more about BIG-IQ Security, visit f5.com to find other resources.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

Solutions for an application world.

©2013 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. DS-15159 1213