BIG-IQ® Security: Administration

Version 4.5

Table of Contents

Legal Notices

Publication Date

This document was published on April 16, 2015.

Publication Number

MAN-0520-01

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-policies/patents

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, "This software" refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. "Similar operating systems" includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software developed by Oracle America, Inc. Copyright ©2012.

1. Java Technology Restrictions. Licensee shall not create, modify, change the behavior of, or authorize licensees of licensee to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Oracle in any naming convention designation. In the event that Licensee creates an additional API(s) which: (a) extends the functionality of a Java Environment; and (b) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, Licensee must promptly publish broadly an accurate specification for such API for free use by all developer.
2. Trademarks and Logos. This License does not authorize an end user licensee to use any Oracle America, Inc. name, trademark, service mark, logo or icon. The end user licensee acknowledges that Oracle owns the Java trademark and all Java-related trademarks, logos and icon including the Coffee Cup and Duke ("Java Marks") and agrees to: (a) comply with the Java Trademark Guidelines at http://www.oraclc.com/html/3party.html; (b) not do anything harmful to or inconsistent with Oracle's

rights in the Java Marks; and (c) assist Oracle in protecting those rights, including assigning to Oracle any rights acquired by Licensee in any Java Mark.

3. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of your license. Source code may not be redistributed unless expressly provided for in the terms of your license.
4. Third Party Code. Additional copyright notices and license terms applicable to portion of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file.
5. Commercial Features. Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified in Table I-I (Commercial Features In Java SE Product Editions) of tile Software documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

This product includes software developed by members of the CentOS Project under the GNU Public License, copyright ©2004-2011 by the CentOS Project.

This product includes software developed by members of the OpenJDK Project under the GNU Public License Version 2, copyright ©2012 by Oracle Corporation.

This product includes software developed by The VMWare Guest Components Team under the GNU Public License Version 2, copyright ©1999-2011 by VMWare, Inc.

This product includes software developed by The Netty Project under the Apache Public License Version 2, copyright ©2008-2012 by The Netty Project.

This product includes software developed by Stephen Colebourne under the Apache Public License Version 2, copyright ©2001-2011 Joda.org.

This product includes software developed by the GlassFish Community under the GNU Public License Version 2 with classpath exception, copyright ©2012 Oracle Corporation.

This product includes software developed by the Mort Bay Consulting under the Apache Public License Version 2, copyright ©1995-2012 Mort Bay Consulting.

This product contains software developed by members of the Jackson Project under the GNU Lesser General Public License Version 2.1, ©2007 – 2012 by the Jackson Project".

This product contains software developed by QOS.ch under the MIT License, ©2004 – 2011 by QOS.ch.

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software developed by jQuery Foundation and other contributors, distributed under the MIT License. Copyright ©2014 jQuery Foundation and other contributors (http://jquery.com/).

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,
2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This software incorporates JFreeChart, ©2000-2007 by Object Refinery Limited and Contributors, which is protected under the GNU Lesser General Public License (LGPL).

This product contains software developed by the Mojarra project. Source code for the Mojarra software may be obtained at https://javaserverfaces.dev.java.net/.

This product includes JZlib software, Copyright © 2000-2011 ymnk, JCraft,Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JCRAFT, INC. OR ANY CONTRIBUTORS TO THIS SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes Apache Lucene software, distributed by the Apache Software Foundation under the Apache License, version 2.0.

This product includes Apache MINA software, distributed by the Apache Software Foundation under the Apache License, version 2.0.

This product includes OData4J software, distributed under the Apache License version 2.0.

This product includes software developed by the Visigoth Software Society (http://www.visigoths.org/).

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

All code not authored by the Depressed Press is attributed (where possible) to its rightful owners/authors, used with permission and should be assumed to be under copyright restrictions as well.

This product includes Angular software developed by Google, Inc., http://angularjs.org, copyright © 2010-2012 Google, Inc., and distributed under the MIT license.

This product includes node.js software, copyright © Joyent, Inc. and other Node contributors. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

- The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes the epoxy.js library for backbone, copyright © 2012-2013 Greg MacWilliam. (http://epoxyjs.org)

This product includes Javamail software, copyright ©1997-2013 Oracle and/or its affiliates, all rights reserved; and copyright © 2009-2013 Jason Mehrens, all rights reserved. This software is distributed under the GPLv2 license.

This product includes underscore software, copyright © 2009-2014 Jeremy Ashkenas, DocumentCloud, and Investigative Reporters & Editors.

This product includes node-static software, copyright © 2010-2014 Alexis Sellier.

This product includes jxrlib software, copyright ©2009 Microsoft Corp. All rights reserved. Distributed under the new BSD license.

This product includes node-uuid software, copyright © 2010-2012, Robert Kieffer, and distributed under the MIT license.

This product includes opencsv software, which is distributed under the Apache 2.0 license.

This product includes owasp-jave-encoder software, copyright © 2014, Jeff Ichnowski, and distributed under the New BSD license.

This product includes cookies software, copyright © 2014, Jed Schmidt, http://jed.is/, and distributed under the MIT license.

This product includes node-fastcgi software, copyright © 2013, Fabio Massaioli, and distributed under the MIT license.

This product includes socket.io software, copyright © 2013, Guillermo Rauch, and distributed under the MIT license.

This product includes node-querystring software, copyright © 2012. Irakli Gozalishvili. All rights reserved.

Chapter 1

Overview: BIG-IQ Security

- *Understanding BIG-IQ Network Security and firewall management*
- *Understanding Shared Security in BIG-IQ Security*
- *Understanding BIG-IQ Web Application Security and application management*
- *About the BIG-IQ Security system interface*
- *About multi-user editing*

Understanding BIG-IQ Network Security and firewall management

BIG-IQ® Network Security is a platform designed for the central management of security firewalls for multiple BIG-IP® systems, where firewall administrators have installed and provisioned the Advanced Firewall Manager™ (AFM™) module.

The BIG-IQ Network Security system provides:

- Device discovery with import of firewalls referenced by discovered devices
- Management of shared objects (address lists, port lists, rule lists, policies, and schedules)
- L3/L4 firewall policy support, including staged and enforced policies
- Firewall audit log used to record every firewall policy change and event
- Role-based access control
- Deployment of configurations from snapshots, and the ability to preview differences between snapshots
- Multi-user editing through a locking mechanism
- Monitoring of rules
- Reports on security

Managing a firewall configuration includes discovering, importing, editing, and deploying changes to the firewall configuration, as well as consolidation of shared firewall objects (policies, rule lists, rules, address lists, port lists, and schedules). BIG-IQ Network Security provides a centralized management platform so you can perform all these tasks from a single location. Rather than log in to each device to manage the security policy locally, it is more expedient to use one interface to manage many devices. Not only does this simplify logistics, but you can maintain a common set of firewall configuration objects and deploy a common set of policies, rule lists, and other shared objects to multiple, similar devices from a central interface.

Bringing a device under central management means that its configuration is stored in the BIG-IQ Network Security database, which is the authoritative source for all firewall configuration entities. This database is also known as the working configuration or working-configuration set.

Once a device is under central management, do not make changes locally (on the BIG-IP device) unless there is an exceptional need. If changes are made locally for any reason, reimport the device to reconcile those changes with the BIG-IQ Network Security working configuration set. Unless local changes are reconciled, the deployment process overwrites any local changes.

In addition, BIG-IQ Network Security is aware of functionality that exists in one BIG-IP system version but not in another. This means, for example, that it prohibits using policies on BIG-IP devices that do not have the software version required to support them.

Understanding Shared Security in BIG-IQ Security

BIG-IQ® Security contains several groups of capabilities. The Shared Security group contains capabilities that can be used by objects in Network Security and by objects in Web Application Security.

You can manage each object using the Shared Security panels that BIG-IQ Security provides:

- Virtual Servers
- Self IPs
- Route Domains
- Logging Profiles
- DoS Profiles

- Device DoS

Understanding BIG-IQ Web Application Security and application management

BIG-IQ® Web Application Security enables enterprise-wide management and configuration of multiple BIG-IP® devices from a central management platform. You can centrally manage BIG-IP devices and security policies, and import policies from files on those devices.

For each device that it discovers, the system creates an additional virtual server to hold all security policies that are not related to any virtual server on the device. To deploy a policy to a device, the policy must be attached to one of the device's virtual servers. You can deploy policies to a device that already has the policy by overwriting it. If the policy does not yet exist on the device, you have the option to deploy it as a new policy attached to an available virtual server or as an inactive policy.

From this central management platform, you can perform the following actions:

- Import Application Security Manager™ (ASM) policies from files.
- Import ASM™ policies from discovered devices.
- Distribute policies to devices.
- Export policies, including an option to export policy files in XML format.
- Manage configuration snapshots.

About the BIG-IQ Security system interface

The BIG-IQ® Security system interface provides many features to assist you in completing tasks.

About filtering

Using filtering, you can rapidly narrow the search scope to more easily locate an entity within the system interface. Each frame in the system interface has its own filter text entry field.

Note: *When you begin typing in the text entry field, you may notice that your browser has cached entries from previous sessions. You can select from the list or continue typing.*

You can filter from the **Overview** frame or you can filter from the **Policy Editor** frame. You can also search for related items in the **Policy Editor** frame.

Filtering the Overview frame

You can filter the contents of panels within each frame to reduce the set of data that is visible in the system interface. Filtering techniques can be important for troubleshooting.

1. Log in to BIG-IQ® Network Security.
2. Navigate to **Network Security** > **Overview**.
3. In the filter text field, type the text you want to filter on and click **Apply**.

Filtering works by performing a wildcard search of the underlying JSON, not just the name of the object. For example, if you type a `1` (the number one) in the filter, the system will display any object with a `1` in it anywhere in its JSON.

Note that the system populates the top of each panel (under the Filter field) with the text you entered inside a gray box.

All panels are filtered on the text entered.

Clearing the filter in the Overview frame

You can easily clear the filters for all panels in BIG-IQ® Network Security Overview, using **Clear All**.

1. Log in to BIG-IQ Network Security.
2. Navigate to **Network Security** > **Overview**.
3. In the filter text field at the top of the interface, type the text you want to filter on and click **Apply**.

   Note that the system filters each panel (**Devices**, **Deployment**, and **Snapshots**). It also populates the top of each panel (under the Filter field) with the text you entered inside a gray box.
4. Clear all text in the filter by clicking **Clear All**.

   Clear the filter for each individual panel by clicking the **X** to the right of the test at the top of the panel.

This action resets all panels and returns the system interface to a display of all objects.

Filtering the Policy Editor frame

You can filter the contents of panels within the Policy Editor frame to reduce the set of data that is visible in the system interface. Filtering techniques can be important for troubleshooting.

1. To filter the contents of the Policy Editor frame, log in to BIG-IQ® Security.
2. Navigate to **Network Security** > **Policy Editor**.
3. In the filter text field, type the text you want to filter on and press **Return**.

   Filtering works by performing a wildcard search of the underlying JSON, not just the name of the object. For example, if you type a `1` (the number one) in the filter, the system will display any object with a `1` in its JSON.

   You can clear the filter field by clicking the **X** to the right of the filter field.

Objects are filtered on the text entered and a count for each appears to the right of each object type.

Filtering the Policy Editor toolbox frame

You can filter the contents of the toolbox (the bottom frame within the Policy Editor frame) to reduce the set of objects visible in the system interface. Filtering techniques can be important for troubleshooting.

1. To filter the contents of the toolbox, log in to BIG-IQ® Security.
2. Navigate to **Network Security** > **Policy Editor** > **Toolbox at the bottom of the right frame**.

   The filter appears to the right of the **Show** dropdown list.
3. In the filter text field, type the text you want to filter on and click the filter icon.

Filtering works by performing a wildcard search of the underlying JSON, not just the name of the object. For example, if you type a `1` (the number one) in the filter, the system will display any object with a `1` in its JSON.

You can clear the filter by clicking the **X** to the left of the filter field.

Filtering the Policy Editor for related objects

You can filter the contents of panels within the Policy Editor frame to show objects related to a selected object.

1. To filter for related objects within the Policy Editor frame, log in to BIG-IQ® Network Security.
2. Navigate to **Network Security** > **Policy Editor**.
3. Locate the object you want to filter on in either the left panel (under **Objects**) or in the toolbox at the bottom of the right frame.
4. Right-click the object.
5. Click **Filter 'related to'**.

   You can clear the **Related to** filter by clicking the **X** to the right of the text under the filter field.

All object types in the left frame are filtered and a count of each **related to** object found appears to the right of each object type.

About panels

BIG-IQ® Security system panels expand to display details such as settings or properties for a particular device or shared object. These expanded panels include a triangle slanted at a 45-degree angle on the right side of their headers. If the triangle is slanted up, you can click it to widen the panel. If the triangle is slanted down, you can click it to collapse the panel. You can also click **Cancel** to close the panel without saving edits or initiating actions.

Expanding panels

You can expand the BIG-IQ® system panels to display settings or properties for a particular device or shared object.

1. Hover over the panel header and click the + icon to widen the panel and create the object (device, deployment, snapshot, and so on).
2. Hover over the object name and click the **gear** icon to expand the panel and view properties for the object, to edit the object, or to initiate other actions.

Reordering panels

You can customize the BIG-IQ® system interface by arranging the panels to suit your needs.

To reorder panels, drag and drop them to the new locations of your choice.

The customized order persists until you clear the browser history/cache/cookies.

About browser resolution

F5® recommends a minimum screen resolution of 1280 x 1024 to properly display and use the panels efficiently.

It is possible to shrink the browser screen so that system interface elements (panels, scroll bars, icons) no longer appear in the visible screen. Should this occur, use the browser's zoom-out function to shrink the panels and controls.

Setting user preferences

As a firewall policy editor, you can customize the BIG-IQ® Network Security system interface to minimize the information displayed, and to simplify routine editing sessions.

Note: *Setting user preferences is not available through the BIG-IQ Web Application Security system interface.*

For example, you can customize the set of panels displayed for a particular user. If that user never performs deployments, you might decide to hide the Deployment panel.

Note: *This customization does not create an access issue. Users still have access to the resources required by their roles; they just choose not to display them.*

User preference settings persist across sessions. If users log out, they see the same settings when logging back in.

By default, BIG-IQ Network Security replicates user preferences in BIG-IQ high-availability (HA) scenarios.

1. Log in to the BIG-IQ® Network Security system.
2. At the top-right of the screen in the black banner, hover over the **admin** icon.
3. When **User settings** appears, click it to display the Settings popup screen.
4. Edit the check box options as required for your role.

Option	Description
Rule Grid Columns	Select or clear the check boxes as required. By default, the system interface displays all columns.
Show Panels	Select or clear the check boxes as required. By default, the system interface displays all panels.
Show Firewall Types	Select or clear the check boxes as required. By default, the system interface displays all firewall contexts in the Firewall Contexts panel.

5. Click **Save** to save your preferences or click **Close** to close the popup screen without saving your selections.

Selected preferences are now in effect and persist across user sessions. If you log out, you will see the same settings when you log back in.

About multi-user editing

Within the BIG-IQ® Security system, multiple firewall editors can edit shared firewall policy objects simultaneously. This is accomplished through a locking mechanism that avoids conflicts and merges. Initially, the user interface presents all firewall configuration objects as read-only. When a firewall editor initiates an editing session, she locks the object. Once an object is locked, no one can modify or delete that object except the holder of the lock or users with privileges sufficient to break the lock (admin, Firewall_Manager, or Security_Manager).

BIG-IQ Security uses a single repository to hold firewall policies. With this single-copy design, multiple editors share the editing task through a locking mechanism. The system saves each editorial change.

Each firewall editor has her own copy of a firewall policy (a point-in-time snapshot of the policy managed by BIG-IQ across all devices) and can make changes. When done, an editor can push the changes to the preferred state as one, complete set of changes. Then, a firewall administrator can review a policy change as a single entity before committing it.

For example:

1. If a firewall editor needs to edit `Portlist_1`, `AddressList_2`, and `Rulelist_5`, the editor locks those objects.
2. When the edit pass is complete, the editor saves the object, which clears the lock.

If an editor wants to edit an object that is already locked, the system informs the editor that the object is locked and provides a way to clear the lock if the editor has sufficient privileges.

When the lock is cleared, the next firewall editor receives the latest version of the object and any referenced shared objects. Thus, merges and conflicts are avoided.

Deleting an object automatically clears all locks associated with it.

BIG-IQ Security supports:

- Multiple, independent locks.
- Locking/unlocking on an object-by-object basis where the object is defined as a shared object or a firewall.

Locking configuration objects for editing

You establish a lock on a configuration object so that you alone can edit it.

Note: *If you have editing privileges, you can lock firewalls, policies, rule lists, address lists, port lists, and schedules.*

---

1. Navigate to the object that you want to edit.
2. Hover over the name of that object, and click the gear icon to expand the panel and display object details.

   If an **Edit** button is visible, you can edit the object. If the object is already locked, a lock message is visible and there is no **Edit** button available.

   The lock header provides a date and time stamp of the lock.
3. If an **Edit** button is visible, click it to lock the object for editing.
   A lock appears on the object name, and a lock message displays.
4. Edit as appropriate.

5. When finished, click **Save**.

   If you navigate away from the panel before saving your changes, the system interface displays a dialog box asking if you want to save changes before leaving the panel.

   Click **Yes** to save your edits and release the lock.

   Click **No** to discard your edits and navigate to the location you requested without releasing the lock.

   Click **Cancel** to retain your edits, retain the lock on the object, and return to the object you were editing.

Viewing locks on all configuration objects

BIG-IQ® Security provides a way to view all locked configuration objects from a single popup screen.

1. Examine all panels to locate locked configuration objects.
2. Navigate to a locked object.
3. Hover over the lock icon.

   A tooltip shows the owner of the lock and the date and time the lock was created, as well as a link labeled **View All**.
4. Click **View All**.

The Locks popup screen opens,showing type, name, user, date and time, and a description for all locked objects.

Clearing locks on configuration objects

The owner of a lock can always clear that lock to enable editing by other users. Other roles (Administrator, Network_Security_Manager, Security_Manager) also carry sufficient privileges to clear locks held by any user.

1. Examine all panels to locate locked configuration objects.
2. Search for the object whose lock you want to clear.
3. Hover over the lock icon to the left of the object's name in the panel.

   A tooltip shows the owner of the lock, and the date and time the lock was created, as well as a link labeled **View All**. If your role carries sufficient privileges, you will also see a link labeled **Unlock**.
4. In the tooltip, click **Unlock**.
5. In the confirmation dialog box, click **Unlock**.

The lock is cleared.

Clearing multiple locks or all locks

BIG-IQ® Security provides a way to clear multiple locks or all locks from a single popup screen, providing that the user carries sufficient privileges (Administrator, Network_Security_Manager, Security_Manager).

1. Examine all panels to locate locked configuration objects.
2. Hover over the lock icon to the left of any locked object in any panel.

   A tooltip shows the owner of the lock, and the date and time the lock was created, as well as a link labeled **View All**. If your role carries sufficient privileges, you will also see a link labeled **Unlock**.
3. In the tooltip, click **Unlock**.

4. In the popup screen that opens, select or clear check boxes as appropriate (or select the check box at the top to clear all locks).
5. Click **Unlock**.
6. In the confirmation dialog box, click **Unlock**.

The locks are cleared.

Chapter 2

Managing Roles and Users

About roles

Different users have different responsibilities. As a system manager, you need a way to differentiate between users and to limit user privileges based on user responsibilities.

To assist you, the BIG-IQ® system has created a default set of roles. To view the default roles, log in to BIG-IQ and navigate to the Roles panel:

BIG-IQ > **BIG-IQ System** > **Access Control** > **Roles**

Roles persist and are available after a BIG-IQ system failover.

You can associate multiple roles with a given user; for example, you can grant a user the edit (Network_Security_Edit) and the deploy (Network_Security_Deploy) roles.

Administrator
This role is responsible for overall management of the platform. Users with this role can add individual users, install updates, activate licenses, and configure HA and networks.This role is abbreviated in the table below as Admin.

Network_Security_Deploy
This role permits viewing and deploying for all firewall configuration objects for all firewall devices under management. This role also permits creation and deletion of snapshots. Users with this role cannot edit configuration objects, discover devices, or reimport devices or otherwise make changes to the working configuration of the BIG-IQ system. Also, this role does not have access to System/Overview or Networking. This role is abbreviated in the table below as Deploy.

Network_Security_Edit
With this role, the user can view and modify all configuration objects for all firewall devices under management, including the ability to create, modify, or delete all shared and firewall-specific objects under Network Security. Users with this role cannot edit objects under Shared Security. Users with only this role cannot deploy configuration changes to remote devices under management. Also, this role does not have access to System/Overview or Networking. This role is abbreviated in the table below as Edit.

Network_Security_Manager
This role encompasses the roles of Network_Security_View, Network_Security_Edit, and Network_Security_Deploy. A user logging in with this role bypasses the System panel and is logged directly into BIG-IQ Security. This role is abbreviated in the table below as NW Sec Mgr.

Network_Security_View
With this role, the user can view all configuration objects and tasks for all firewall devices under management. Users with this role cannot edit objects and cannot initiate a discovery or deployment task. This role is abbreviated in the table below as View.

Security_Manager
This role combines the privileges of Network_Security_View, Network_Security_Edit, and Network_Security_Deploy. A user logging in with this role is logged directly into BIG-IQ Security. A user logging in with this role can also access BIG-IQ Web Application Security. This role is abbreviated in the table below as Sec Mgr.

Web_App_Security_Manager
This role carries administrator-level rights for the BIG-IQ Web Application Security module only. This role does not appear in the following table.

About access control: features and the roles that can perform them

Feature	View	Edit	Deploy	Sec Mgr	NW Sec Mgr	Admin
View policy, objects, snapshots, deployments, devices, groups	X	X	X	X	X	X
Create/update/delete configuration objects		X		X	X	X
Create/delete snapshots		X	X	X	X	X
Compare (view differences between) snapshots	X	X	X	X	X	X
Restore working configuration from snapshot		X		X	X	X
Deploy from snapshot			X	X	X	X
DMA (declare management authority)		X		X	X	X
RMA (rescind management authority)		X		X	X	X
Deploy working config; create/delete deployment tasks			X	X	X	X
View audit log	X	X	X	X	X	X
Delete, configure audit log				X		X
Create/update/delete device groups		X		X	X	X
Manage users						X
Manage system						X

About user types

By default, the BIG-IQ® Network Security system provides admin as a default user type. The admin user can assign roles to users, but cannot access the command shell or system console.

User types persist and are available after a BIG-IQ system failover.

Creating user accounts

As the firewall manager, it is your responsibility to create the right set of user accounts and associate those users with the right roles (sets of privileges). By managing user roles, you place controls on specific functions (view, edit, and deploy).

User accounts and roles persist and are available after a BIG-IQ® system failover.

1. Log in to the BIG-IQ® system and click **BIG-IQ System** > **Access Control** > **Users**.
2. Hover over the Users banner, click the + icon, and select **New User**.
3. Complete the fields as required.

Option	Description
Username	Enter the user's login name.
Auth Provider	Accept the default of `local` or from the dropdown list, select the provider that supplies the credentials required for authentication.
Full Name	Enter the user's actual name. This field can contain a combination of symbols, letters (upper and lowercase), numbers, and spaces.
Password	Enter the password for this user.
Confirm Password	Retype the password.

4. Click **Add** to save your edits and create the user account (or click **Cancel** to close the panel without saving your entries).

You can now associate this user with a specific role (set of privileges).

Associating users with roles

You can control what users are able to accomplish by associating roles (sets of privileges) with particular users.

1. Log in to the BIG-IQ® system and click **BIG-IQ System** > **Access Control** > **Users**.
2. In the Users panel, click the user that you want to associate with a role and drag the user onto the role (Roles panel).

   Conversely, you can also drag the role onto the user.

The user now has the privileges commensurate with his role. To confirm, click the gear icon for the user, and select **Properties**. Or, click the gear icon for the role and view the **Active Users and Groups**.

Disassociating users from roles

You disable a user's ability to perform a given function by disassociating roles (sets of privileges) from that user.

1. Log in to the BIG-IQ® system and click **BIG-IQ System** > **Access Control** > **Roles**.
2. In the Roles panel, hover over the role that contains the user you want to disassociate, click the gear icon, and select **Properties**.
3. To the right of **Active Users and Groups**, view the list of users and groups associated with the role.
4. Click the **X** next to the user or group that you want to disassociate from the role.
5. Click **Save**.

The user is now disassociated from the role, and no longer has the privileges associated with the role.

Chapter 3

Configuring for High Availability

About active-standby, high-availability configurations

To ensure that you always have access to the BIG-IP® devices under BIG-IQ® management, install two BIG-IQ systems in an active-standby, high-availability (HA) configuration.

Note: *Currently, a BIG-IQ Security HA configuration is limited to two systems, configured as peers.*

Configuring a high-availability pair is optional. However, if you configure a high-availability BIG-IQ system and the active peer fails, the standby peer will become active, enabling you to continue to manage devices.

BIG-IQ Security performs asynchronous replication per transaction, which means that data is replicated continuously, asynchronously, on a transaction-by-transaction basis as changes are made or commands are run on the active system.

Continuous, asynchronous replication ensures you that the stored state on each BIG-IQ system is identical to the state on the other BIG-IQ system(s) in the HA configuration. You can resume managing firewalls after a failover without loss of any configuration change that might have occurred prior to failover.

In addition, all intermediate generations of a configuration object are identical on all HA peers. This is required because snapshots can refer to previous generations, and the system must be able to restore on any node a snapshot that was originally taken on a peer.

About high-availability terminology

Terminology is crucial in understanding the status of the high-availability (HA) relationship. The following list defines some important terms used in HA configurations.

Primary
The node you are logged in to when establishing the pair is deemed the *primary node*; the system added is deemed the *secondary node*. The primary node determines which node is active if both nodes are up and communicating. This is the node that wins if a conflict occurs. Initiate the pairing from the primary node.

Secondary
Any node added to the configuration is deemed the secondary node. Currently, BIG-IQ ®Security supports a 2-node pairing. When finished discovering its peer, the primary node triggers a snapshot of the current state of the storage on the primary node. When the snapshot is finished, it is copied to the secondary node. The restjavad process on the secondary node is restarted.

Active
The node that is running commands is the *active node*.If you see the status indications Active (Secondary) on the secondary device, you have failed over to the node that is not the primary. In the unlikely event of network segmentation, both systems may report that they are active.

Standby
The *standby node* is the node that instructs the user to perform all module-related activity on the active node through a yellow status bar at the top of the interface that indicates its standby status.

Cluster
A synonym for a high-availability configuration is *cluster*. A cluster comprises at least two BIG-IQ systems (fully installed and licensed, and running the same version of software), and is configured in a high-availability relationship through **BIG-IQ** > **BIG-IQ Systems** > **Properties**.

Pairing BIG-IQ Security systems for high-availability

Before you can configure BIG-IQ® systems for high-availability (HA), you must have two licensed BIG-IQ systems, installed with the required system components. For the high-availability pair to synchronize properly, each must be running the same BIG-IQ version, and the clocks on each system must be synchronized within 60 seconds, and remain synchronized. Prior to establishing the pair, examine the NTP settings at the BIG-IQ system level and the current system time value.

Note: *Perform the following procedure on the BIG-IQ system that is deemed the active node.*

You can ensure that you always have access to managed BIG-IP® devices by installing two BIG-IQ systems in a high availability (HA) cluster. Any configuration change that occurs on one BIG-IQ system is immediately synchronized with its peer device. If a BIG-IQ system in an HA cluster fails, a peer BIG-IQ system takes over device management that was previously performed by the original device. When an event occurs that prevents one of the BIG-IQ systems from processing network traffic, the peer in the redundant system immediately begins processing that traffic, and users experience no interruption in service.

1. Log in to the BIG-IQ system, using administrator credentials.
2. From the BIG-IQ dropdown list, select **System**.
3. From the BIG-IQ Systems panel header, click + and select **Add Device**.
4. In the New Device panel, complete the following fields:

Option	Description
IP Address	Type the self IP address.
User name	Type the administrative user name.
Password	Type the administrative password.
Group	From the Group dropdown list, select **Management Group**.
High Availability Mode	Select **Active-Standby**.

5. Click **Add**.

When you expand the Management Group, you will see the addition of the standby peer under localhost.

Splitting a high-availability pair

To change or reconfigure peers that are in a BIG-IQ® high-availability pair, you must first delete the HA relationship or split the pair.

1. Log in to the BIG-IQ system, using administrator credentials.
2. From the BIG-IQ dropdown list, select **System**.
3. From the BIG-IQ Systems panel, expand the Management Group.
4. Hover over the secondary-standby peer and when the gear icon appears, click it to open the panel.
5. In the expanded panel, click **Remove**.

The pair is now split. Consult the banner at the top for status. Both nodes will display a status of Standalone.

About automatic failback

BIG-IQ® Security forces an automatic failback mechanism in which the Active (Primary) node goes down and the Active (Secondary) node takes over. Subsequently, the Active (Secondary) node may be labeled Active (Secondary). When the Active (Primary) node comes back up, it takes over primary responsibilities automatically, becomes the Active (Primary) node, and synchronizes its configuration with the configuration on the Standby (Secondary) node. Thus, you are guaranteed that no data is lost.

Chapter 4

Managing BIG-IP Devices

About device discovery

About device discovery: BIG-IQ Network Security

The process of importing a firewall device's configuration or designating a firewall device for central management by BIG-IQ® Network Security is called *discovery*.

After discovery, BIG-IQ Network Security provides a way to view device properties and to perform device-specific and firewall-specific actions through a centralized management platform.

The BIG-IQ Security Devices panel displays user-defined and system-defined groups and imported BIG-IP devices.

Note: *Groups are simply a way to group devices visually and manage them more efficiently.*

Before discovering devices and importing firewalls, you must install specific components required by the BIG-IQ system on each BIG-IP® device you want to manage. Installing these components results in a framework that supports the required Java-based management services.

To view all devices under management, in BIG-IQ Network Security, navigate to the Devices panel.

To display only those items related to the specific device, hover over the device and when the **gear** icon appears, click it. Then, you can select **Properties** to display properties or **Show Only Related Items** to filter by device.

About device discovery: BIG-IQ Web Application Security

The process of designating a device for central management by BIG-IQ Web Application Security is called *discovery*. Once a BIG-IP device is discovered, all security policies and virtual servers on the device come under management by the BIG-IQ system.

For each discovered device, the system creates an extra virtual server to hold all policies not related to any virtual server in the discovered device.

After discovery, BIG-IQ Web Application Security enables a view of devices and properties, policies, and virtual servers associated with those devices, and a way to perform device-specific and policy-specific actions.

To view all devices under management, in BIG-IQ Web Application Security, navigate to the Devices panel.

About declaring management authority

The process of bringing a device under central management is known as *declaring management authority (DMA)*. The firewall administrator initiates DMA through device discovery and import (or reimport).

The DMA process is modal. Once the process starts, you are blocked from performing any other tasks or interacting with BIG-IQ® Security in any way until the process is complete or canceled. Before starting a discovery or reimport process, it is important to understand how you will resolve any conflicts that arise.

Note: *In this scenario, a conflict is defined as two configuration objects (such as policies) in the same partition having the same name, but containing different data.*

Discovering devices on BIG-IQ Network Security

Before discovering BIG-IP® devices, ensure that the required BIG-IQ® components are installed on those devices. For details, consult the BIG-IQ-Device: Device Management section on installing required BIG-IQ components on managed devices.

You can perform device discovery to bring a BIG-IP device under central management. Once a device is under central management, the device's configuration is stored in the BIG-IQ Security database, which is the authoritative source for all configuration objects. After that occurs, do not manage the firewall device locally unless there is an exceptional need. Otherwise, changes made locally could be overwritten on the next deployment task.

During discovery, a **Remove Device** button appears after the task has identified the device and started importing the firewall configuration. If you click **Remove Device** at this point, the import is canceled and management authority over the device is rescinded. Subsequently, the device is removed.

1. Navigate to the Devices panel.
2. Hover over the Devices header, click the + icon to display the available options (**New Device** and **New Group**), and click **New Device**.
3. Click **New Device**.
4. Complete the property fields as required.

Option	Description
IP Address	Type the BIG-IP® device self IP address or management IP address. ***Note:*** *Each managed device must be configured with a communication route from its self IP address or management IP address to a BIG-IQ system self IP addresses. Otherwise, discovery will fail. F5 recommends that you use a BIG-IP self IP address for discovery.*
Cluster Name	Type a name for the cluster. Optional, but highly recommended if the BIG-IP device is in a config sync relationship with other BIG-IP devices. The cluster name will create a new group if one does not exist, or add the device to an existing cluster group if it does exist. For more information, consult the sections on managing groups in this guide.
User Name	Type the user's login name. For example: `admin`.
Password	Type the password for this user.
Snapshot	Ensure that this check box is selected (the default) to snapshot the configuration on the BIG-IP device before importing. BIG-IQ® Security uses snapshots to protect the working-configuration set of the Security module. Thus, at any time, you can back up, restore, and deploy the BIG-IQ working configuration to a specific configuration state, or deploy a specific set of working configuration edits back to a BIG-IP® device.
Update Framework	Select the Update Framework on Discovery check box to update the REST framework installed on the BIG-IP device. Certain BIG-IQ system components must be installed and kept up-to-date on all BIG-IP devices brought under central management. These components provide a REST framework on the BIG-IP devices that support the required Java-based management services. To ensure the framework is up-to-date, select this check box.

Option	Description
Root User Name	If the framework on the target BIG-IP device must be updated, you must specify the root user name as part of the discovery process. Type the root user name, which is `root`, by default.
Root Password	If the framework on the target BIG-IP device must be updated, you must specify the root password as part of the discovery process. Type the root password.

5. Click **Add**.
   A popup screen opens prompting for confirmation.

After discovery, the BIG-IP device is listed in the Devices panel by its FQDN and internal self IP address. By default, the device is added to the Firewall group. If a cluster group is specified, it is added to the specified cluster group. Also, the system lists the snapshot of the working configuration taken during import in the Snapshots panel. The system imports any firewall policies on this device and makes them available for configuration management.

Discovering devices on BIG-IQ Web Application Security

You perform device discovery to bring a BIG-IP® device under central management. Once a device is under central management, information about the device and objects stored on the device are located in the BIG-IQ® database, which is the authoritative source for all configuration objects.

Note: *Do not manage the BIG-IP device locally. If you make changes locally, you (or another Administrator) might overwrite those changes when performing a deployment from the BIG-IQ system.*

---

1. Navigate to **Security** > **Web Application Security** > **Overview**.
2. Hover over the Devices header, click the + icon to display the available options (**New Device** and **New Group**), and click **New Device**.
3. Complete the property fields as required.

Option	Description
Device Address	Type the IP address for the BIG-IP device. ***Note:*** *Each managed device must be configured with a communication route from its self IP address or management IP address to a BIG-IQ system self IP address. Otherwise, discovery fails. F5 recommends that you use a BIG-IP system self IP address for discovery.*
User Name	Type the user's login name. For example: `admin`.
Password	Type the password for this user.
Update on Discovery	Select this check box to force an update of the REST framework on the BIG-IP device. Certain BIG-IQ system components should be installed and kept up-to-date on all BIG-IP devices brought under central management. These components provide a REST framework that supports the required Java-based management services. If this box is checked, the discovery process updates all system components automatically.

Option	Description
Root Username	If the framework on the target BIG-IP device must be updated, you must specify the root user name as part of the discovery process. Type the root user name, which is `root` by default.
Root Password	If the framework on the target BIG-IP device must be updated, you must specify the root password as part of the discovery process. Type the root password.

4. Click **Add**.
   A popup screen opens prompting for confirmation.
5. Click **Yes**.
   Another popup screen takes its place, showing you the status of the discovery as it occurs.

After discovery, the BIG-IP device is listed in the Devices panel, and any discovered virtual servers and Web Application Security policies are listed in the other panels.

About conflict resolution

A *conflict* is found when two objects of the same type have the same name but contain different data. Thus, an address list named `list1` and a port list named `list1` would not be in conflict.

Note: *An object is defined as an address list, port list, rule list, policy, or schedule.*

Conflicts prevent processes from running to completion.

Note: *It is the responsibility of the administrator to know how to resolve conflicts between shared objects, and to deploy the resolution. If you encounter conflicts during discovery, import, reimport, or deployment, you must resolve those conflicts before you can interact further with BIG-IQ® Security.*

If conflicts are found, BIG-IQ Security displays the Resolve Conflicts dialog box, which lists all conflicts found, displays detailed differences for conflicting shared objects, and provides for conflict resolution. The Resolve Conflicts dialog box may be displayed two times: once for Network Security objects, and once for Shared Security objects.

Although conflict resolution often results in changes to either the BIG-IP® configuration or the BIG-IQ configuration, no changes are applied until they are deployed. You can deploy changes when a deployment task displays a status of `READY TO DEPLOY`.

Resolving conflicts

After importing or reimporting a BIG-IP® device, you can use the Resolve Conflicts dialog box to view the differences between configurations, and to resolve conflicts.

1. Navigate to the Devices panel.
2. Hover over the name of the device you want to import/reimport and when the gear icon appears, click it to display the expanded screen. You can modify only a few of the properties displayed.

Option	Description
Host Name	Fully-qualified domain name (FQDN), identified at time of discovery.
Cluster Name	BIG-IP device cluster name, provided at time of discovery.

Option	Description
IP Address / Management Address	IP address for the communication route to the BIG-IQ system internal self IP address. Each managed device must be configured with a communication route from its self IP address or management IP address to a BIG-IQ system self IP addresses. Otherwise, discovery will fail. F5 recommends that you use a BIG-IP system self IP address for discovery.
Product	Product identity.
Version	Version and hotfix level of the device under management.
Status	(BIG-IQ Web Application Security) Active.
Snapshot	Check box used to take a snapshot of the configuration on the BIG-IP device before importing (the default).
Username	Administrative login name. For example: `admin`.
Password	Administrative password for this user.
Update Framework	Check box used to update the REST framework installed on the BIG-IP device. Certain BIG-IQ system components must be installed and kept up-to-date on all BIG-IP devices brought under central management. These components provide a REST framework on the BIG-IP devices that support the required Java-based management services. To ensure the framework is up-to-date, select this **Update On Save** check box.
Root Username	If the framework on the target BIG-IP device must be updated, you must specify the root user name as part of the reimport process. Type the root user name, which is `root`, by default.
Root Password	If the framework on the target BIG-IP device must be updated, you must specify the root password as part of the reimport process. Type the root password.

3. In the Device Properties screen, click **Add/Reimport**.
4. When the Conflict Resolution dialog box opens, the conflicting shared objects are highlighted in the upper half of the dialog box. Click the shared object to view details in the lower half of the dialog box.

   The object's configuration on the BIG-IP device is displayed on the left and the object's configuration on BIG-IQ® Security is displayed on the right.

   A gray area indicates that a line has been removed. Yellow indicates that a line has changed, and green indicates that a line has been added or modified.

   The Resolve Conflicts dialog box also provides a **Cancel Task** button. If you click **Cancel Task**, the reimport is canceled. Management authority over the device, if established, is not rescinded, and the device is not removed.
5. Examine differences. From the Action list, select one of the following for each object in conflict:

Option	Description
Keep BIG-IQ Version	Keep the object as configured on BIG-IQ Security, and overwrite the object as configured on the BIG-IP device.
Keep BIG-IP Version	Keep the object as configured on the BIG-IP device, and overwrite the object as configured in the central BIG-IQ Security database.

6. Alternately, from the **Apply this action to all conflicts:** list , select an action to resolve all existing conflicts.

After conflict resolution, the device's configuration is refreshed and synchronized with the configuration stored in BIG-IQ Security.

About BIG-IQ Security configuration sets

BIG-IQ® Security systems use the following terminology to refer to firewall configuration sets for a centrally-managed device:

Current configuration set
The configuration of the BIG-IP® device as discovered by BIG-IQ Security. The current configuration is updated during a reimport/rediscovery and before calculating differences during the deployment process. After deployment (and after the resolution of any conflicting shared objects), BIG-IQ Security overwrites the BIG-IP current configuration (if the option **Keep BIG-IQ Version** is chosen).

Working configuration set
The configuration as maintained by the BIG-IQ Security system. Initially, the working configuration is created when the firewall manager elects to manage the device from BIG-IQ Security (DMA). It is the configuration that is edited on BIG-IQ Security and deployed back to BIG-IP devices.

Configuring devices to accept traffic

When using the BIG-IP® device's self IP address during discovery, you must configure that device to accept traffic from a BIG-IQ® Security system. Specifically, if the BIG-IP device has the Virtual Server & Self IP Contexts option set to Reject or Drop, the BIG-IP device will not accept traffic from the BIG-IQ system. Use the following procedure to set this option to **Accept**.

Alternately, you can add a rule to handle traffic between the self IP addresses of the BIG-IQ Security system and the self IP addresses of the specific BIG-IP device being discovered. In this scenario, you can leave the Virtual Server & Self IP Contexts option set to Reject or Drop.

In this case, ensure the following ports remain open:

- 22 (SSH, TCP protocol)
- 443 (HTTPS, TCP protocol)
- 4353 (iQuery, TCP protocol)

Note: *Whichever scenario you choose, configure the BIG-IP device to allow traffic to/from the self IP addresses of both BIG-IQ nodes in a BIG-IQ HA pair.*

---

1. On the BIG-IP device, on the Main tab, click **Security** > **Options** > **Network Firewall**.
2. From the **Virtual Server & Self IP Contexts** list, select **Accept**.
3. Click **Update**.

Packets with BIG-IQ Security as the source are then able to pass through the BIG-IP firewall and traverse the system.

Displaying device properties

You can display properties and health and performance statistics for an individual device to assist in identifying potential trouble spots.

1. In the Devices panel, hover over the name of the device you want to examine until the gear icon appears, then display the properties in one of these ways:
   - Select **Show Properties** from the sub-menu.
   - Click the gear icon to expand the panel.
2. Review the statistics in the properties screen for that device.

Device properties

Device properties are displayed for informational purposes mostly, and are read-only, except for the check boxes.

Device Property	Description
Device Address	IP address for the BIG-IP® device entered at time of discovery and used for communication between the device and the BIG-IQ® system.
Host Name	Fully-qualified domain name (FQDN), identified at discovery time.
Cluster Name	BIG-IP device cluster name, provided at discovery time.
IP Address / Management Address	IP address for the communication route to the BIG-IQ system internal self IP address.Each managed device must be configured with a communication route from its internal self IP or management IP address to a BIG-IQ system internal self IP address on a configured BIG-IP VLAN. Otherwise, discovery fails. F5 recommends that you use a self IP address (on the BIG-IP device) to gain access to additional functionality that is not provided through the management port.
Username	User's login name. For example: `admin`.
Password	User's password.
Product	Identifies the product.
Version	Identifies the version and hotfix level of the device under management.
Status	(BIG-IQ Web Application Security) Status of the device under management (Active or Standby).
Snapshot	Check box used to invoke a snapshot prior to reimporting the BIG-IP device's working configuration.

Device Property	Description
Update Framework	Check box used to update the REST framework on the BIG-IP device on discovery or on save.
Check to overwrite the source of imported policies that already exist	Check box used to determine whether the discovery process overwrites the source of imported policies already on the BIG-IQ system.
Signature file Version	Identifies the BIG-IP version that the Attack Signature Database is packaged with.
Root Username	If the framework on the target BIG-IP device must be updated, you must specify the root user name as part of the discovery process. Enter the root user name which is `root`, by default.
Root Password	If the framework on the target BIG-IP device must be updated, you must specify the root password as part of the discovery process.

Displaying the device inventory

From the BIG-IQ® Network Security Devices panel, you can display an inventory with accompanying details for all devices under BIG-IQ Network Security central management. For further use, you can export this inventory to a CSV file.

1. Navigate to the Devices panel.
2. Hover over the name of the device for which you want to view an inventory.
3. When the right-pointing arrow appears, click it to read inventory details.

Option	Description
Name	Fully-qualified domain name (FQDN) for the BIG-IP device.
Marketing Name	BIG-IP Virtual Edition.
Product	Product identity. For example, `BIG-IP`.
Version	Version and hotfix level of the device under management.
Build	Build level of the device under management.
Mgmt IP Address	Management IP address for the BIG-IP device, used to manage the device.
License	License end date and end time, registration key, and a list of active modules.
Slots	For each slot, a listing of volume label, product occupying the slot, version, build, cluster status (active, standby).
Network Interfaces	Configured network interfaces.
Serial Number	Serial number for the BIG-IP device.
Mac Address	Mac address for the BIG-IP device.
CPU Info	Manufacturer and technical details. For example, Intel(R) Xeon(R) CPU X5660 @ 2.80GHz.

Option	Description
Memory (MB)	Memory on the BIG-IP device.
Platform	Z100
HAL ID	For example, 4208f88e-3f9e-0d7e-b75e-ca1dc2dd630c.
UUID	Universally unique identifier. For example, 6b8bf5ef-bcb0-4d1b-b61f-8c95f70475a8.

4. To exit from the inventory, click **Close**.

About device reimport/rediscovery

Once configurations are in sync between BIG-IP® devices and the BIG-IQ® Security system, there is seldom a need to reimport a BIG-IP device.

Some possible reasons to reimport include:

- Additions, deletions, or changes made to management IPs or virtual servers on the BIG-IP device.
- Changes to policies, firewall rules, shared objects, or signature files made locally on the BIG-IP device.
- Updates made to the BIG-IP device's software that need to be recognized by BIG-IQ Security.

If any of these reasons occur, you must reimport/rediscover to reconcile any changes with the configuration maintained on BIG-IQ Security. If you do not reconcile changes, a subsequent deployment process will overwrite any changes made locally.

The reimport/rediscovery process is modal. Once reimport starts, the process blocks you from performing any other tasks or interacting with BIG-IQ Security in any way until the process completes or is canceled.

During reimport/rediscovery, a **Remove Device** button appears in the dialog box after the task has identified the device and started the import process. If you click **Remove Device**, the reimport/rediscovery is canceled, management authority over the device is rescinded, and the device is removed.

Reimporting or rediscovering devices

You reimport/rediscover BIG-IP® devices to reconcile any configuration changes with the configuration maintained on BIG-IQ® Security. If you do not reconcile changes, a subsequent deployment process will overwrite any changes made locally.

1. Navigate to the Devices panel.
2. Hover over the name of the device you want to import/reimport and when the gear icon appears, click it to display the expanded screen. You can modify only a few of the properties displayed.

Option	Description
Host Name	Fully-qualified domain name (FQDN), identified at time of discovery.
Cluster Name	BIG-IP device cluster name, provided at time of discovery.
IP Address / Management Address	IP address for the communication route to the BIG-IQ system internal self IP address. Each managed device must be configured with a communication route from its self IP address or management IP address to a BIG-IQ system self IP

Option	Description
	addresses. Otherwise, discovery will fail. F5 recommends that you use a BIG-IP system self IP address for discovery.
Product	Product identity.
Version	Version and hotfix level of the device under management.
Status	(BIG-IQ Web Application Security) Active.
Snapshot	Check box used to take a snapshot of the configuration on the BIG-IP device before importing (the default).
Username	Administrative login name. For example: `admin`.
Password	Administrative password for this user.
Update Framework	Check box used to update the REST framework installed on the BIG-IP device. Certain BIG-IQ system components must be installed and kept up-to-date on all BIG-IP devices brought under central management. These components provide a REST framework on the BIG-IP devices that support the required Java-based management services. To ensure the framework is up-to-date, select this **Update On Save** check box.
Root Username	If the framework on the target BIG-IP device must be updated, you must specify the root user name as part of the reimport process. Type the root user name, which is `root`, by default.
Root Password	If the framework on the target BIG-IP device must be updated, you must specify the root password as part of the reimport process. Type the root password.

3. In the Device Properties screen, click **Add**/**Reimport**.

After reimport/rediscovery, the configuration for the selected device is refreshed and synchronized with the configuration stored in BIG-IQ Security.

Monitoring device health and performance

Before you can view device properties, health, and performance, that device must be under central management.

You can assess the health and performance of your network to provide early intervention for trouble spots.

1. Navigate to the Devices panel.
2. To display properties and health and performance statistics for an individual device, hover over the name for that device (in the Devices panel).
3. When the gear icon appears, select **Show Properties** or click the gear to expand the panel.
4. Scroll past the properties to examine the health and performance statistics for this device.

Chapter 5

Managing Groups

About groups

In BIG-IQ® Security, groups are:

- Specific to BIG-IQ. Groups do not exist on BIG-IP® devices. There is no discovery of groups on BIG-IP devices or distribution of groups to BIG-IP devices.
- Used for navigation and deployment purposes only.

When you have many BIG-IP devices to manage, you can group devices, which helps you visualize and manage large numbers of devices.

You can use the panel filtering options to show the devices you are interested in. Then, you can save this group with a name and description. Subsequently, you can select this group or any group saved earlier. You can easily delete other user-created groups.

Note: *There are some system-created groups that cannot be deleted.*

You can also filter the Devices panel (devices and groups) by typing text in the Filter field and pressing the Enter key. Clear the filter by clicking the **X** to the right of the text in the gray box under the filter.

System-defined groups (the Firewall Group and cluster groups) do not allow users to edit their memberships directly. Devices are added to these groups through the discovery process and deleted from this groups using the Remove button on the device's Properties panel.

You can arrange user-defined groups in a hierarchy of groups and subgroups.

System-defined groups always appear at the top of the hierarchy (root) and cannot contain child groups.

Adding devices to groups

After device discovery, you can create groups to organize devices into a visual hierarchy for ease of identification and management.

1. From the Create Group panel, complete the fields as appropriate.

Option	Description
Group Name	Name of the group. Must be unique across all groups. Give the group a name that will assist you in remembering the group's purpose, managing the group, or identify the group.
Description	Optional description for the group. Descriptions can contain useful information about groups.
Parent Group	>Accept the default (root) or select another group from the dropdown list to reside at the top of the group hierarchy.
Available Devices	Begin typing to see the list of available devices. Select an available device and click **Add Device** to add a device to the table.

2. Click **Save**.

The device is added to the group and appears in the Devices panel.

Managing groups

After adding a BIG-IP® device to a pre-existing group, you can manage the group through the Group Properties screen. This means you can change the group hierarchy, add or remove devices from groups, delete groups, and modify group descriptions.

Changing group hierarchy

From the Group Properties screen, you can change the hierarchy of groups and subgroups through the **Parent Group** list.

Note: *System-defined groups always appear at the top of the hierarchy (`root`) and cannot contain subgroups.*

To change group hierarchy:

1. From the **Parent Group** list, select **root** (the default) or another group to reside at the top of the hierarchy.
2. Click **Save**.

Adding or removing devices from groups

System-defined groups (the Firewall Group and cluster groups) do not allow users to edit memberships directly. Devices are added to these groups through the discovery process and deleted from these groups using the **Remove** button on the device's Properties screen.

To add a device to a group:

1. In the **Available Devices** field, begin typing and the list of available devices appears.
2. Select an available device and click **Add Device**. The device is added to the table.
3. Click **Save**. The device is added to the group.

To remove a device from a group:

1. In the table below the **Available Devices** field, click the **X** at the end of the row containing the device you want to remove. The device is removed from the table.
2. Click **Save**. The device is removed from the group.

Deleting groups

Note: *You can delete user-created groups; there are some system-created groups that cannot be deleted.*

To delete a group:

1. Click the **Delete** button.
2. When prompted, confirm the deletion by clicking **Delete**.

This action permanently removes the group from BIG-IQ Network Security.

Modifying group descriptions

To modify the group description, type a description in the **Description** field, or modify the existing description and click **Save**. The description could be written to help you remember the purpose of the group, or it could contain other useful information about the group.

Chapter 6

Managing Firewall Contexts

About managing firewall contexts in BIG-IQ Network Security

In BIG-IQ® Network Security, a firewall context is a BIG-IP® network object to which a firewall policy can be attached. In BIG-IQ Network Security, these network objects are called Global (global), Route Domain (rd), Virtual Server (vip), Self IP (sip), or Management (mgmt).

Firewall contexts provide policy-based access control to and from address and port pairs, inside and outside the network. Using a combination of contexts, a firewall can apply rules in a number of different ways, including at a global level, per virtual server, per route domain, and even for the management port or a self IP address.

Firewall properties include the firewall name, an (optional) description), its partition, its type, and its parent device on the partition in which it resides. Note that an *administrative partition* is a part of the BIG-IP configuration that is accessible only to a particular group of administrators. The default partition for all BIG-IP configurations, /Common, is accessible to all administrators. A sufficiently-privileged administrator can make additional partitions. Each partition corresponds to a folder (with the same name) to hold its configuration objects.

From the Enforced tab, you can view and configure policies or rules/rule lists whose actions (accept, accept decisively, drop, reject) are in force. You are restricted to a single, enforced policy on any specific firewall. If you have an enforced policy on a firewall, you cannot also have inline rules and rule lists on that same firewall.

You can edit inline rules from the Enforced tab. You can edit all other firewall shared objects only from within the object's panel. For example, you can edit rule lists, including the reordering of rules inside rule lists, only from the Rule Lists panel.

Note: *Policies can be enforced in one firewall context and staged in another.*

About BIG-IP system firewall contexts

A *firewall context* is the category of object to which a rule applies. In this case, category refers to Global, Route Domain, Virtual Server, Self IP, or Management. Rules can be viewed and reorganized separately within each context.

It is possible to have multiple layers of firewalls on a single BIG-IP® device. These layers constitute the firewall hierarchy. Within the firewall hierarchy, rules progress from Global, to Route Domain, and then to either Virtual Server or Self IP.

If a packet matches a firewall rule within a given context, that action is applied to the packet, and the packet then moves to the next context for further processing. If the packet is accepted, it travels on to the next context. If the packet is accepted decisively, it goes directly to its destination. If the packet is dropped or rejected, all processing stops for that packet; it travels no further.

On each firewall, you can have rules, rule lists, or policies that are enforced or staged. Rules, rule lists, or policies are processed in order within their context and within the context hierarchy.

Rules for the Management interface are processed separately and not as part of the context hierarchy.

About global firewalls

A *global firewall* is an IP packet filter that resides on a global firewall on a BIG-IP® device. Except for packets traveling to the management firewall, it is the first firewall that an IP packet encounters. Any packet reaching a BIG-IP device must pass through the global firewall first.

When you create firewall rules, rule lists, or policies, you can select one of several contexts. Global is one of the contexts you can select. Rules for each context form their own list, and are processed both in the context hierarchy and in the order within each context list.

About route domain firewalls

A *route domain firewall* is an IP packet filter that resides on a route domain firewall on a BIG-IP® device.

A *route domain* is a BIG-IP system object that represents a particular network configuration. After creating a route domain, you can associate various BIG-IP system objects with the domain: unique VLANs, routing table entries such as a default gateway and static routes, self IP addresses, virtual servers, pool members, and firewalls.

When a route domain firewall is configured to apply to one route domain, it means that any IP packet that passes through the route domain is assessed and possibly filtered out by the configured firewall.

When you create firewall rules, rule lists, or policies, you can select one of several contexts. Route domain is one of the contexts you can select. Rules for each context form their own list and are processed both in the context hierarchy and in the order within each context list.

Route domain rules apply to a specific route domain configured on the server. Route domain rules are checked after global rules. Even if you have not configured a route domain, you can apply route domain rules to `Route Domain 0`, which is effectively the same as the global rule context.

Route domain rules are collected in the Route Domain context. Route domain rules apply to a specific route domain defined on the server. Route domain rules are checked after global rules.

About virtual server firewalls

A *virtual server firewall* is an IP packet filter configured on the virtual server and, therefore, designated for client-side traffic. Any IP packet that passes through the virtual server IP address is assessed and possibly filtered out by this firewall.

When you create firewall rules, rule lists, or policies, you can select one of several contexts, including virtual server. Rules for each context form their own list and are processed both in the context hierarchy and in the order within each context list.

Virtual server rules apply to the selected virtual server only. Virtual server rules are checked after route domain rules.

About self IP firewalls

A *self IP firewall* is an IP packet filter configured on the self IP address, a firewall designated for server-side traffic. Any IP packet that passes through the self IP is assessed and possibly filtered out by this firewall.

A self IP address is an IP address on a BIG-IP® system that is associated with a VLAN and used to access hosts in that VLAN. By virtue of its netmask, a self IP address represents an address space; that is, a range of IP addresses spanning the hosts in the VLAN, rather than a single host address.

A static self IP address is an IP address that is assigned to the system and does not migrate between BIG-IP systems. By default, the self IP addresses created with the Configuration utility are static self IP addresses. One self IP address must be defined for each VLAN.

When you create firewall rules, rule lists, or policies, you can select one of several contexts, including self IP. Rules for each context form their own list and are processed both in the context hierarchy and in the order within each context list.

The self IP context collects firewall rules that apply to the self IP address on the BIG-IP device. Self IP rules are checked after route domain rules.

About management IP firewalls

A *management IP firewall* is an IP packet filter configured on the management IP address and, therefore, designated to examine management traffic. Any IP packet that passes through the management IP address is assessed and possibly filtered out by this firewall.

The network software compares IP packets to the criteria specified in management firewall rules. If a packet matches the criteria, then the system takes the action specified by the rule. If a packet does not match a rule, then the software compares the packet against the next rule. If a packet does not match any rule, the packet is accepted.

Management IP firewalls collect firewall rules that apply to the management port on the BIG-IP® device. Management port firewalls are outside the firewall context hierarchy and management port rules are checked independently of other rules.

Note: *Policies and rule lists are not permitted on management IP firewalls. In addition, the management IP firewall context does not support the use of iRules® or geolocation in rules. For management IP firewalls, only inline rules are allowed. To add inline rules, drag-and-drop them onto the management firewall.*

You can also drag-and-drop address lists, and port lists onto management IP firewalls.

About firewall policy types

In BIG-IQ® Network Security, you can add the following firewall policy types:

Enforced
An enforced firewall policy modifies network traffic based on a set of firewall rules.

Staged
A staged firewall policy allows you to evaluate the effect a policy has on traffic without actually modifying the traffic based on the firewall rules.

You can assign to a firewall either an enforced firewall policy or a set of explicitly-defined rules and rule lists. The firewall cannot have both in force at the same time. However, you can configure simultaneously on the same firewall both staged firewall policies and enforced inline rules and rule lists.

Firewall properties

The Properties tab displays the properties for the selected firewall. All fields are for information purposes only and cannot be edited, with the exception of the (optional) description.

Property	Description
Name	Name as shown in the system interface: `global` for the global firewall; `management-ip` for the management IP firewall; `0` for route domain; the IP address for self-ip; and the firewall name for a virtual server.
Description	(Optional) description for the firewall.
Partition	Usually, `Common`. An *administrative partition* is a part of the BIG-IP® configuration that is accessible only to a particular group of administrators. The default partition for all BIG-IP configurations, `Common`, is accessible to all administrators. A sufficiently-privileged administrator can make additional partitions. Each partition corresponds to a folder (with the same name, for instance, `/Common`) to hold its configuration objects.
Type	One of the following: global (global); route-domain (rd); virtual server (vip); self-ip (self-ip); or management-ip (mgmt).
Route Domain ID	Used for Route Domain firewall types only; displays a number that identifies the route domain.
IP Address	For Virtual server (VIP), self IP, and Management firewall types only; this is an informational, read-only field displaying the IP address retrieved (if available) during DMA.
Device	Name of the BIG-IP® device where the firewall resides.

Adding an enforced firewall policy

You can view and configure firewall policies or rules/rule lists to force or refine actions (accept, accept decisively, drop, reject) using the Enforced settings. You are restricted to a single, enforced firewall policy on any specific firewall context. If you have an enforced policy on a firewall, you cannot also have inline rules and rule lists on that same firewall.

Note: *Policies can be enforced in one firewall context and staged in another.*

1. Log in to BIG-IQ® Network Security.
2. Click **Policy Editor**.
3. Click **Contexts** to expand the contents.
4. Click the context you want to edit. The contents appear in the editing pane.

5. In the editing pane, click **Enforced**.
6. On the Enforced screen, click **Edit** to establish a lock.

   If necessary, review *Locking configuration objects for editing*.
7. Add a firewall policy by dragging and dropping a policy from Policies, or click **Add Policy**, select a policy from among those listed in the popup, and then click **Add**.

   If the firewall has inline rules already configured, you are notified that adding a policy will result in the removal of all existing rules and rule lists.
8. Click**Create Rule** to open a rule template in the Enforced Firewall Rules table where you can add a rule by editing the fields in the template.

   Before attempting to add an inline rule on any firewall context except the management IP context, be sure inline rules are supported on the version running on your BIG-IP® device.

   You can also add rules by right-clicking in the last rule in the table and selecting **Add rule before** or **Add rule after**. If you right-click after the bottom row in the Rules table, you can select the option **Add rule**. You can then reorder rules by dragging and dropping them until they are in the correct order for execution. You can also reorder rules by right-clicking in the row and selecting among the ordering options.
9. Add a rule list by clicking **Add Rule List**.
10. In the popup screen that opens, select the name of the rule list that you want to add and then click **Add**.
11. Click **Save** to save changes.

    To clear a lock without saving changes, click the **Unlock** link.
12. When finished, click **Save and Close** to save your edits, clear the lock, and exit.

Adding a staged firewall policy

You can stage firewall policies using the Staged settings. Actions (accept, accept decisively, drop, reject) have no effect on network traffic. Rather, they are logged. This gives you the ability to stage a firewall policy first and examine the logs to determine how the firewall policy has affected traffic. Then, you can determine the timing for turning the firewall policy from staged to enforced.

Rule and rule lists are not allowed on staged firewall policies.

Note: *A firewall policy can be staged in one context and enforced in another.*

---

1. Log in to BIG-IQ® Network Security.
2. Click **Policy Editor**.
3. Click **Contexts** to expand the contents.
4. Click the context you want to edit. The contents appear in the editing pane.
5. In the editing pane, click **Staged**.
6. On the Staged screen, click **Edit** to establish a lock.

   If necessary, review *Locking configuration objects for editing*.
7. Add a policy by dragging and dropping a policy from Policies, or click the **Add Policy** link, select a policy from among those listed in the popup screen, and then click **Add**.
8. Click **Save** to save changes.

   To clear a lock without saving changes, click the **Unlock** link.
9. When finished, click **Save and Close** to save your edits, clear the lock, and exit.

Chapter 7

Managing Rules and Rule Lists

About rules and rule lists

Rule lists are containers for rules, which are run in the order they appear in their assigned rule list. A rule list can contain thousands of ordered rules, but cannot be nested inside another rule list. You can reorder rules in a given rule list at any time.

With BIG-IQ® Network Security, you can manage rules and rule lists from the Rule Lists option (Policy Editor > Rule Lists). You can also create rules and add rule lists from the Contexts and the Polices options. You can import and manage rules (and/or rule lists) from BIG-IP® devices. Furthermore, you can define rules and rule lists within BIG-IQ Network Security, and then deploy back to the BIG-IP device.

You can define a list of rules for a specific firewall and/or refer to one or more shared rule lists by name from other firewalls.

Network firewalls use rules and rule lists to specify traffic-handling actions. The network software compares IP packets to the criteria specified in rules. If a packet matches the criteria, then the system takes the action specified by the rule. If a packet does not match any rule from the list, the software accepts the packet or passes it to the next rule or rule list. For example, the system compares the packet to self IP rules if the packet is destined for a network associated with a self IP address that has firewall rules defined.

A packet must pass all tests to match successfully. For example, to match against a source subnet and several destination ports, a packet must originate from the given subnet and also have one of the specified destination ports.

Rules and rule lists can be applied to all firewall types, such as:

- Global
- Route domain
- Virtual server
- Self IP
- Management IP (rules only, no iRule or geolocation support)

Filtering rule lists

To filter the system interface to display only those objects related to a selected rule list, hover over the rule list name, right-click and then click **Filter 'related to'**. The interface is filtered and a count appears to the right of each object type. The frame to the right provides its own filter field where you can enter text and click on the filter icon to constrain the display to those items that match the filter.

Creating rules

To support a context or policy, you can create specific rules, gather those rules in a rule list, and assign the rule list to the context or policy.

1. Log in to BIG-IQ® Network Security.
2. Click **Object Editor**.
3. Select the object that you want to add the rule to:

Option	Description
Rule list	In the left pane, hover over **Rule Lists** and click the + icon to display the New Rule List frame, which provides access to **Properties** and **Rules** options.

Option	Description
Context	In the left pane, expand **Contexts** and click the name of the specific firewall context to gain access to **Properties**, **Enforced**, and **Staged** options.
Policy	In the left pane, hover over **Policies**, and click the + icon to display New Policy frame, which provides access to **Properties** and **Rules & Rule Lists** options.

4. Click **Properties** and complete the properties fields as required.

Option	Description
Name	Unique name. The field is read-only field unless creating or cloning the rule list.
Description	Optional description.
Partition	Although pre-populated with `Common` (default), you can set the partition name by typing a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP device. No whitespace is allowed in the partition name.* The firewall partition itself is not editable.

5. Click **Rules** or **Enforced**, and then click **Create Rule**.
   A new row appears in the table. The row contains a rule template, including defaults, for the new rule.
6. Complete the fields as appropriate.
   You can also add rules by right-clicking in the Rules table, or by right-clicking any row in the Rules table and choosing **add rule before** or **add rule after**.
7. When you are finished, click **Add** or **Save**, as appropriate.

Reordering rules in rule lists

You can optimize your network security firewall policy by reordering rules in rule lists.

1. Log in to BIG-IQ® Network Security.
2. Click **Object Editor**.
3. Expand **Rule Lists** and click the specific rule list you want to edit.
4. Click the **Rules** tab to ensure it is selected.
5. Click **Edit** to lock for editing.
6. Drag-and-drop the rules until they are in the correct order.
   If the list of rules expands beyond the editing frame, drag-and-drop will not work. Instead, copy the rule by right-clicking and selecting **Copy rule**. Then, navigate to the new location for the rule, right-click, and select **Paste rule before** or **Paste rule after** as appropriate. After the copy, delete the rule that you copied.
7. When you are finished, click **Save and Close** to save your edits, clear the lock, and exit the panel.

Removing rules

You can remove specific rules from rule lists, firewalls, or policies, to fine tune security policies.

Note: *You can remove a rule even if it is the only rule in the rule list.*

1. You remove a rule based on the object that you remove it from:

Option	Description
From a rule list	In the left pane, expand **Rules Lists** and click the name of the rule list containing the rule that you want to delete. This opens the Rule List frame that provides access to **Properties**and **Rules** options.
From a firewall context	In the left pane, expand **Contexts**, click the name of the context containing the rule that you want to delete.This opens the Properties frame and provides access to **Properties**, **Enforced** and **Staged** options. Then, select **Enforced** or **Staged** as appropriate.
From a policy	In the left pane, expand **Policies**, click the name of the policy containing the rule that you want to delete. The Policy frame opens and provides access to **Properties** and **Rules & Rule Lists** options. Select **Rules & Rule Lists**.

2. Click **Edit** to lock for editing.
3. Hover over the row containing the rule, and right-click.
4. Select **Delete Rule** and confirm the deletion.
5. Click **Save** to save your changes.

Adding rule lists

To support a specific firewall or policy, you can create a rule list and then assign it to the firewall context or policy.

1. Click **Object Editor**.
2. Select the object that you want to add the rule list to:

Option	Description
Rule list	In the left pane, hover over **Rule Lists** and click the + icon to display the New Rule List frame, which provides access to **Properties** and **Rules** options.
Context	In the left pane, expand **Contexts** and click the name of the specific firewall context to gain access to **Properties**, **Enforced**, and **Staged** options.
Policy	In the left pane, hover over **Policies**, and click the + icon to display New Policy frame, which provides access to **Properties** and **Rules & Rule Lists** options.

3. Click **Properties** and complete the properties fields as required.

Option	Description
Name	Unique name. The field is read-only field unless creating or cloning the rule list.

Option	Description
Description	Optional description.
Partition	Although pre-populated with `Common` (default), you can set the partition name by typing a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP device. No whitespace is allowed in the partition name.* The firewall partition itself is not editable.

4. Continue with the configuration:

Option	Description
New Rule List screen	Click **Rules**, and click **Create Rule**.
Firewall context	Click **Enforced**, and click **Edit** to lock the firewall for editing. Then, click **Add Rule List** and select from the rule lists that appear in the popup dialog.
Policy	Click **Rules & Rule Lists**, then click **Add Rule List**.

5. Complete the fields as appropriate.

   You can also add rules by right-clicking in the Rules table, or by right-clicking any row in the Rules table and choosing **add rule before** or **add rule after**.
6. When you are finished, click **Add** or **Save**, as appropriate.
7. If you are editing a firewall context to add the rule list, you must, when finished, click **Save and Close** to save your edits, clear the lock, and exit the panel.

The new rule list appears at the bottom of the Rule Lists panel.

Editing rule lists

You can edit the content of rule lists from Policy Editor Rule Lists, including the order of rules in rule lists.

Note: *You must lock a rule list before editing it.*

1. Log in to BIG-IQ® Network Security.
2. Click **Policy Editor**.
3. Expand **Rule Lists** and click the specific rule list you want to edit.
4. Click **Edit** to lock for editing.
5. Click **Properties**.

Option	Description
Name	Informational, read-only field set when creating or cloning the rule list.
Description	Optional description.
Partition	Informational, read-only field set when creating or cloning the rule list.

6. Select **Rules** , and click the row of the rule you want to edit.
7. Complete the fields as appropriate.

   You can also add rules by right-clicking in the Rules table, or by right-clicking any row in the Rules table and choosing **add rule before** or **add rule after**.
8. Complete fields as appropriate.

   To reorder rules, simply drag-and-drop the rules until they are in the correct order. If the list of rules expands beyond the editing frame, drag-and-drop will not work. Instead, copy the rule by right-clicking and selecting **Copy rule**. Then, navigate to the new location for the rule, right-click, and select **Paste rule before** or **Paste rule after** as appropriate. After the copy, delete the rule that you copied.
9. Click **Save** to save your changes.

Changes made to the rule list are reflected the next time the Contexts or Policies screen is refreshed.

Clearing fields in rules

You can clear the text from fields in rules to fine tune them and, in turn, rule lists and security policies.

1. Log in to BIG-IQ® Network Security.
2. Click **Object Editor**.
3. Expand **Rule Lists** and click the name of a rule list that you want to edit.
4. Click **Edit** to lock for editing.
5. Click the **Rules** tab to ensure it is selected.
6. Locate the rule containing the fields whose contents you want to remove.
7. Not all fields can be cleared, but you can remove the contents of these fields as follows:

Option	Description
Address (source or destination)	Hover over the text in the field. Right-click and select **Remove item**.
Port (source or destination)	Hover over the text in the field. Right-click and select **Remove item**.
VLAN	Hover over the text in the field. Right-click and select **Remove item**.
iRule	Hover over the text in the field. Right-click and select **Remove item**.
Description	Hover over the text in the field. Right-click and select **Remove item**.

8. Click **Save** to save your changes.
9. When you are finished, click **Save and Close** to save your edits, clear the lock, and exit the panel.

Cloning rule lists

Cloning enables you to create and customize rule lists to address unique aspects of your network firewall environment. When you clone a rule list, you create an exact copy of the rule list, which you can then edit to address any special considerations.

Note: *Users with the roles of Network_Security_View or Network_Security_Deploy cannot clone policies.*

1. Log in to BIG-IQ® Network Security.
2. Click **Object Editor**.
3. Expand **Rule Lists** and click the specific rule list you want to clone.
4. Click **Clone**.
5. Click **Properties** and complete the properties fields as required.

Option	Description
Name	Unique name. The field is read-only field unless creating or cloning the rule list.
Description	Optional description.
Partition	Although pre-populated with `Common` (default), you can set the partition name by typing a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP device. No whitespace is allowed in the partition name.* The firewall partition itself is not editable.

6. Click **Rules**, edit the rules as required to configure the clone.
   You can also click **Create Rule** to add a new rule.
7. When you are finished, click **Add**.
   If you click **Cancel**, the rule list is not cloned.

The cloned rule list is added alphabetically under **Rule Lists**. In a high-availability configuration, the cloned rule list is replicated on the standby system as soon as it is cloned.

Removing rule lists

You can remove rule lists from firewalls or policies to fine tune security policies.

1. Log in to BIG-IQ® Network Security.
2. Click **Object Editor**.
3. In the left pane, expand **Rule Lists**, and click the list that you want to remove.
4. At the top of the screen, click **Remove**.
5. If it is safe to remove the rule list, a confirmation dialog box opens; click **Remove** to confirm.
   If the rule list is in use, you cannot complete the removal. A popup screen opens informing you that you cannot remove the rule list because it is in use. Click **Close** to acknowledge this message, and then click

Cancel in the Remove popup screen. To see where a rule list is used, click the rule list and the name appears in the search field. Then click **Apply**. The system interface displays only those objects related to the search. To clear the search, click the **x** icon to the right of the search string.

The system removes the rule list from the **Rule Lists** listing.

Rule properties

The following table lists and describes the properties required when configuring network firewall rules.

Property	Description
Name	Unique, user-provided name for the rule. If the name is a rule list name, it is preceded by: `referenceTo_` when moved to a firewall or policy. For example: `referenceTo_sys_self_allow_all`.
Address (Source)	There are many ways to construct an IPv4 or IPv6 address, address range, or address list. The following methods and examples are not meant to be exhaustive. • IPv4 format: *a.b.c.d*[/*prefix*]. For example: `60.63.10.10` • IPv6 format: *a*:*b*:*c*:*d*:*e*:*f*:*g*:*h*[/*prefix*]. For example: `2001:db7:3f4a:9dd:ca90:ff00:42:8329` • You can specify subnets using forward slash (/) notation; for example: `60.63.10.0/24`. An example of an IPv6 subnet is as follows: `2001:db8:a::/64`. • You can append a route domain to an address using the format %RouteDomainID/Mask. For example, `12.2.0.0%44/16`. From the list, select: • **Address**. Enter the address in the **Addresses** field. You can also type an address range in the **Addresses** field using the format: n.n.n.n-n.n.n.n. For example: `1.1.1.1-2.2.2.2`. • **Address range**. Type the beginning address in the first **Addresses** field and the ending address in the second **Addresses** field. • **Address list**. In the **Addresses** field, type text to display stored address lists. You can select any of the address lists displayed. • **Country/Region**. From the first **Addresses** list, select a country. Once you select a country, the second list automatically updates with all available regions for that country. Optionally, select a region from the second list. The wildcard, Unknown, is supported. Note that geolocation is not supported on the management IP context. Options are provided to add additional addresses, address ranges, address lists, or countries/regions (+) and to delete addresses, address ranges, address lists, or countries/regions (**X**). When you are finished, click **Save** or **Add**.
Port	Ports, port ranges, or port lists. From the list, select: • **Port**. Type the port in the **Ports** field. You can also enter a port range in the port field by typing a range in the format: n-n. For example: `43-44`. • **Port range**. Type the beginning port in the first **Ports** field and the ending port in the second **Ports** field. • **Port list**. In the **Ports** field, type text to display stored port lists. You can select any of the port lists displayed. Options are provided to add additional ports, port ranges, or port lists (+) and to delete ports, port ranges, or port lists (**X**). When you are finished, click **Save** or **Add**.

Property	Description
VLAN	Name of the VLAN physically present on the device (Internal, External, or Any). If you specify a VLAN in a rule without also specifying the VLAN's partition, the deployment task will fail when you attempt to deploy that rule to a firewall. Use the format `partition/VLAN` or `/partition/VLAN`. For example: `Common/external` or `/Common/external`. When finished, click **Save** or **Add**.
Address (Destination)	There are many ways to construct an IPv4 or IPv6 address, address range, or address list. The following methods and examples are not meant to be exhaustive. • IPv4 format: *a.b.c.d*[/*prefix*]. For example: `60.63.10.10` • IPv6 format: *a*:*b*:*c*:*d*:*e*:*f*:*g*:*h*[/*prefix*]. For example: `2001:db7:3f4a:9dd:ca90:ff00:42:8329` • You can specify subnets using forward slash (/) notation; for example: `60.63.10.0/24`. An example of an IPv6 subnet is as follows: `2001:db8:a::/64`. • You can append a route domain to an address using the format %RouteDomainID/Mask. For example, `12.2.0.0%44/16`. From the list, select: • **Address**. Type the address in the **Addresses** field. You can also enter an address range in the **Addresses** field using the format: n.n.n.n-n.n.n.n. For example: `1.1.1.1-2.2.2.2`. • **Address range**. Type the beginning address in the first **Addresses** field, and the ending address in the second **Addresses** field. • **Address list**. In the **Addresses** field, type text to display stored address lists. You can select any of the address lists displayed. • **Country/Region**. From the first **Addresses** list, select a country. Once you select a country, the second list automatically updates with all available regions for that country. Optionally, select a region from the second list. The wildcard, Unknown, is supported. Note that geolocation is not supported on the management IP context. Options are provided to add additional addresses, address ranges, address lists, or countries/regions (+) and to delete addresses, address ranges, address lists, or countries/regions (**X**). When you are finished, click **Save** or **Add**.
Port	Ports, port ranges, or port lists. From the list, select: • **Port**. Type the port in the **Ports** field. You can also enter a port range in the port field by typing a range in the format: n-n. For example: **43-44**. • **Port range**. Type the beginning port in the first **Ports** field and the ending port in the second **Ports** field. • **Port list**. In the **Ports** field, type text to display stored port lists. You can select any of the port lists displayed. Options are provided to add additional ports, port ranges, or port lists (+) and to delete ports, port ranges, or port lists (**X**). When you are finished, click **Save** or **Add**.
Action	Click in the column and select one of the following: • **Accept**. Allows packets with the specified source, destination, and protocol to pass through the firewall. Packets that match the rule, and are accepted, traverse the system as if the firewall is not present. • **Accept decisively**. Allows packets with the specified source, destination, and protocol to pass through the firewall, and does not require any further processing by any of the further firewalls. Packets that match the rule, and are accepted, traverse the system as if the firewall is not present. If the Rule List is applied to a virtual server, management IP, or self IP firewall rule, then Accept Decisively is equivalent to Accept.

Property	Description
	• **Drop**. Drops packets with the specified source, destination, and protocol. Dropping a packet is a silent action with no notification to the source or destination systems. Dropping the packet causes the connection to be retried until the retry threshold is reached. • **Reject**. Rejects packets with the specified source, destination, and protocol. When a packet is rejected the firewall sends a destination unreachable message to the sender. When you are finished, click **Save** or **Add**.
iRule	Click in the column and enter the iRule name, including partition. For example: `/Common/_sys_AXX_Support_OA_BasicAuth`. iRules® use syntax based on the industry-standard Tools Command Language (Tcl). For complete and detailed information on iRules syntax, see the F5 Networks DevCentral web site, `http://devcentral.f5.com`. Note that iRules must conform to standard Tcl grammar rules. For more information on Tcl syntax, see `http://tmml.sourceforge.net/doc/tcl/index.html`. Note that iRules are not supported on the management IP context.
Description	Optional description for the current rule. To add a description, click in the column, type text, and click **Save** or **Add**.
Protocol	IP protocol to compare against the packet. Select the appropriate protocol from the list and click **Save** or **Add**. If you select **ICMP**, **IPv6-ICMP**, or **Other**, a popup dialog box opens where you can specify **Type** and **Code** combinations. The default type is **Any** and the default code is **Any**. ***Note:*** *The type and code combinations are too numerous to document here. For details, consult the F5 Networks DevCentral site,* `http://devcentral.f5.com` *or the documentation for the specific BIG-IP® platform.*
State	Click in the column and select an option from the list to specify whether the rule is enabled, disabled, or scheduled. The field is updated. Click **Save** or **Add** when you are ready to save your changes. If you select **scheduled** from the list, the **Select Schedule** list is displayed in the screen. Select a schedule and click **OK**. If you have assigned a schedule, then a gear icon appears to the right of the **State** setting in the State column. To make changes to the **State** setting, click the gear icon to open the Select Schedule popup screen. If you have no pre-defined schedules, you cannot assign the scheduled state to the rule.
Log	Click in the column and select an option from the list to specify whether or not the firewall software should write a log entry for any packets that match this rule. From the list, select **true** (log an entry) or **false** (do not log an entry). When finished, click **Save** or **Add**. For you to set or edit this setting, the discovered device must be at version 11.3 HF6 or later. The setting is not editable earlier than version 11.3 HF6. When a new rule is added to a firewall through the BIG-IQ® Network Security system interface, editing is enabled for the **Log** setting even for devices with versions earlier than 11.3 HF6.

Chapter 8

Managing Notification Rules

About notification rules

Notification rules are accessed from within the Policy Editor and are used to notify users when a policy is changed or when a percentage of the maximum supported configuration objects is reached. The notifications are configured using notification rules and are delivered through email, such an email is referred to as a notification email. Notification rules can be useful for administrators who wish to be notified when policies are changed, or who wish to notify others of such changes. Notifications can also be sent based on shared resources used by policies.

Adding and scheduling notification rules

Use the Notification Rules panel of the Policy Editor to add and schedule a new notification rule.

Adding notification rules

1. Select Notification Rules from the left to display the Notification Rules panel.
2. Click **Add** and the Notification Rules - New Item panel is displayed.
3. On the Properties tab, specify the appropriate values for the following fields.

Property	Description
Name	Specify a name for the notification. This is required.
Description	Specify a description for the notification
Email Comment	Specify the content of the email for this notification
Format	Select the format of the notification to be either **Plain Text** or **CSV**.
Rule Type	Select the type of notification rule to use. • **Policy Notify** indicates that the notification is triggered when the policy has changed. You specify the policy on the Policy Notify tab. • **Limit Notify** indicates that the notification is triggered when a limit has been reached. You specify the limit on the Limit Notify tab.
Email Recipients	Specify information about one or more email recipients. • In the **Name** field, specify a name for the recipient. • In the **Email Address** field, specify the email address of the recipient. To add another recipient, click the (+) plus sign and supply the **Name** and **Email Address** fields for that recipient. To remove a recipient, click the (**X**) to the right of the email recipient.

4. If you specified the **Rule Type** as **Policy Notify**, specify the appropriate values for the following fields on the Policy Notify tab.

Field	Description
Available Policies	Select the policy the rule should monitor and notify you when it changes, then click **Add Policy**. The selected policy is added to the list of policies below the **Available Policies** field.

Field	Description
Notify on Dependent Objects	Determines whether or not dependent objects, such as shared resources, are also monitored by the rule. By default this option is selected, indicating that shared resources should also be monitored.

You can also add policies by dragging them from the Shared Resources area and dropping them on the Drop Policies here to add to the Policies list area.

To delete a policy from the list, click the **X** to the right of the **Notify on Dependent Objects** option.

5. If you specified the **Rule Type** as **Limit Notify**, specify the appropriate values for the following fields on the Limit Notify tab.

Field	Description
Device Limit Notification	Select this check box to be notified when the BIG-IQ system reaches a specified limit.
Device Limit Thresholds	Specify the device limit thresholds at which a notification email is sent. A device limit is a percentage of the number of BIG-IP devices your BIG-IQ system is managing.You can set up to three limits that are each a percentage of the limit amount by modifying the percentage amount in each of the three device limit threshold fields. For example, if your BIG-IQ system is licensed to handle 10 BIG-IP devices, you would go over the threshhold of 49% when 5 BIG-IP devices were being managed.
Object Limit Notification	Select this check box to be notified when a specified object limit is exceeded.
Object Limit Thresholds	Specify the object limit thresholds at which a notification email is sent. You can set up to three limits that are each a percentage of the limit amount by modifying the percentage amount in each of the three object limit threshold fields.As more operations occur with more BIG-IP devices, the number of objects in use by the BIG-IQ system grows. The maximum number of objects supported varies depending on the BIG-IP device configuration.

6. Click **Save** to save the information you have entered and to verify it is syntactically correct.
7. When finished, click **Save & Close** to save changes, release the lock, and exit the panel.

Scheduling notification rules

Once a notification rule has been created it can be scheduled. To schedule a notification rule, click the check box to the left of the rule to select it, and then click **Edit Schedule**. The Notification Rules Evaluation Interval dialog is displayed. In this dialog, specify the interval at which the schedule should run.

Editing notification rules

From the Notification Rules panel in the Policy Editor, you can edit notification rules.

1. Click the name of the notification rule to edit that rule and display the editing panel.
2. The rule is locked for editing.
3. Change the property and field values that you need to modify.
4. Click **Save** to save changes.
5. When finished, click **Save and Close** to save changes, release the lock, and exit the panel.

Deleting notification rules

From the Notification Rules panel in the Policy Editor, you can remove notification rules.

1. Select the rule to be removed by clicking the check box to the left of the rule.
2. Click **Remove**.

Chapter 9

Managing Locks

About locks

The Locks panel of the Policy Editor displays objects that are locked on the BIG-IQ® system, and provides details about the user who locked the object and when the lock was created. You can also use the Locks panel to remove those locks.

Viewing and deleting locks

You can display objects that are locked on the BIG-IQ® system, and see details about the user who locked the object and when the lock was created.

1. Log in to BIG-IQ Security with your administrator user name and password.
2. At the top of the screen, click **Network Security**, then **Policy Editor**, and on the left, click **Locks**.
3. Review the locked objects.
4. To unlock an object, select the check box to the left of that object and click **Unlock**.
5. Confirm the unlocking by clicking **Delete** in the Delete Lock dialog box.

If you decide not to unlock the object, click **Cancel** instead of **Delete**.

Chapter 10

Managing Security Reports

About security reporting

You can use BIG-IQ® Security Reporting to view reports for managed BIG-IP® devices that are provisioned for Application Visibility and Reporting (AVR). Reports can be for a single BIG-IP device or can contain aggregated data for multiple BIG-IP devices (that are of the same BIG-IP device version).

Network Firewall, DoS and IP Intelligence reports can be created. Analytic reports provide detailed metrics about application performance such as transactions per second, server and client latency, request and response throughput, and sessions. Metrics are provided for applications, virtual servers, pool members, URLs, specific countries, and additional detailed statistics about application traffic running through one or more managed devices. You can view the analytics reports for a single device, view aggregated reports for a group of devices, and create custom lists to view analytics for only specified devices.

Chapter 11

Managing Virtual Servers in Shared Security

About virtual servers

On BIG-IP® devices, network objects such as virtual servers, self IP addresses, the management IP, route domains, and the global firewall all have firewalls, rules, and policies attached to them. On BIG-IQ® systems, an instance of one of these network objects is called a *firewall context*.

Using a BIG-IQ Security system, you can discover all firewall contexts on a BIG-IP device, and edit the firewall rules, policies, or both, that are attached to the firewall context. Using the Virtual Servers panel, you can create and delete virtual server objects on BIG-IP devices that have L3/L4 firewalls attached to them. In scenarios where virtual servers are used primarily for security purposes, this provides a way for security administrators to quickly create additional firewalls.

BIG-IQ Security virtual servers only support BIG-IP device profiles from the LTM® module (`/ltm/profile`) and from the Security DoS module (`/security/dos`). If a BIG-IP device is discovered with virtual servers using another type of profile, an invalid profile error may be encountered during discovery and the BIG-IP device would not be discovered by the BIG-IQ Security system.

To close the New Virtual Server properties screen without making any changes, click **Cancel**.

To get help on any panel, click the **(?)** icon in the upper right corner.

Adding virtual servers

Hover over the Virtual Servers header and click the + icon when it appears, then click **New Virtual Server**. The panel expands to display the New Virtual Server properties.

Editing virtual servers

Hover over the name of the virtual server you want to edit and when the gear icon appears, click it to expand the panel.

Adding virtual servers

Use the New Virtual Server screen to configure a new virtual server.

Note: *Depending on the settings you configure, you may see only some of the screen elements described here.*

Adding virtual servers

1. Hover over the Virtual Servers header, click the + icon when it appears, and click **New Virtual Server**. The panel expands to display the New Virtual Server properties.
2. In the New Virtual Server screen, review, and add or modify the properties of the new virtual server as appropriate.

Property	Description
Device	Specifies the discovered BIG-IP® device for the virtual server.
Name	Specifies the name of the virtual server.
Description	Specifies a description for the virtual server.

Property	Description
Partition	Specifies the partition or path to which the virtual server belongs. Only users with access to a partition can view the objects (such as the self IP address) that it contains. If the virtual server resides in the `Common` partition, all users can access it. ***Note:*** *Although pre-populated with* ***Common*** *(default), you can set the partition by replacing* ***Common*** *with a unique name for the partition. The partition with that name must already exist on the BIG-IP device. If it does not exist, then, at deployment, the deployment will fail. No whitespace is allowed in the partition name.*
Type	Specifies the network service provided by this virtual server. The default type is **Standard**. The possible types are listed. ***Note:*** *Not all properties are valid for all types. When you specify the type, certain properties may become available or unavailable.* • **Standard**: Specifies a virtual server that directs client traffic to a load balancing pool and is the most basic type of virtual server. When you first create the virtual server, you assign an existing default pool to it. From then on, the virtual server automatically directs traffic to that default pool. • **Forwarding (Layer 2)**: Specifies a virtual server that shares the same IP address as a node in an associated VLAN. This type of virtual server has no pool members to load balance. • **Forwarding (IP)**: Specifies a virtual server like other virtual servers, except that the virtual server has no pool members to load balance. The virtual server simply forwards the packet directly to the destination IP address specified in the client request. • **Performance (HTTP)**: Specifies a virtual server with which you associate a Fast HTTP profile. Together, the virtual server and profile increase the speed at which the virtual server processes HTTP requests. • **Performance (Layer 4)**: Specifies a virtual server with which you associate a Fast L4 profile. Together, the virtual server and profile increase the speed at which the virtual server processes Layer 4 requests. • **Stateless**: Specifies a virtual server that accepts traffic matching the virtual server address, and load balances the packet to the pool members without attempting to match the packet to a pre-existing connection in the connection table. New connections are immediately removed from the connection table. This addresses the requirement for one-way UDP traffic that needs to be processed at very high throughput levels, for example, load balancing syslog traffic to a pool of syslog servers. Stateless virtual servers are not suitable for processing traffic that requires stateful tracking, such as TCP traffic. Stateless virtual servers do not support iRules®, persistence, connection mirroring, rateshaping, or SNAT automap. • **Reject**: Specifies that the BIG-IP system rejects any traffic destined for the virtual server IP address. • **DHCP**: Specifies a virtual server that relays Dynamic Host Control Protocol (DHCP) client requests for an IP address to one or more DHCP servers, and provides DHCP server responses with an available IP address for the client. • **Internal**: Specifies a virtual server that supports modification of HTTP requests and responses.

Property	Description
Source	Specifies an IP address or network from which the virtual server accepts traffic. The virtual server accepts clients only from one of these IP addresses. For this setting to function effectively, specify a value other than `0.0.0.0/0` or `::/0` (that is, `any/0`, or `any6/0`). In order to maximize utility of this setting, specify the most specific address prefixes covering all customer addresses and no others. Specify the IP address in Classless Inter-Domain Routing (CIDR) format: address/prefix, where the prefix length is in bits: for example, for IPv4: `10.0.0.1/32` or `10.0.0.0/24`, and for IPv6: `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`.
Destination	Specifies the destination IP address information to which the virtual server sends traffic. • If the destination type is set to **Host**, specify only the IP address in the **Address** field. Specify the IP address in CIDR format: address/prefix, where the prefix length is in bits: for example, for IPv4: `10.0.0.1/32` or `10.0.0.0/24`, and for IPv6: `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. The defaults for DHCP are `255.255.255.255` (IPv4 Default) and ff02::1:2 (IPv6 Default). You can also select `Other` to specify another destination address. • If the destination type is set to **Network**, specify both the IP address in the **Address** field, and the network mask in the **Mask** field. Specify the mask address in CIDR format as you did the IP address.
Service Port	Type a service port or select a type from the list. When you select a type from the list, the value in the **Service Port** field changes to reflect the associated default, which you can change.
State	Specifies whether the virtual server and its resources are available for load balancing. The default is **Enabled**.
Connection Mirroring	Specifies that the system mirrors connections on each member in a redundant configuration. Connection mirroring is the process of duplicating connections from the active system to the standby system. Enabling this setting ensures a higher level of connection reliability, but it may also have an impact on system performance.
Protocol	Specifies a network protocol name that you want the system to use to direct traffic on this virtual server. The default is **TCP**. If the **Type** is set to **Performance (HTTP)**, the network protocol is set to **TCP**. If the **Type** is set to **DHCP**, the **Protocol** property is not available. The following are valid network protocol keywords. • ***All Protocols**: Specifies that the virtual server supports all network protocols. This setting is not available when you select the **Type** of **Standard**. • **TCP**: Specifies that the virtual server supports the TCP protocol, defined in RFC 675. • **UDP**: Specifies that the virtual server supports the UDP protocol, defined in RFC 768. • **SCTP**: Specifies that the virtual server supports the Stream Control Transmission Protocol (SCTP) protocol, defined in RFC 4960. • **Other**: Provides the ability to specify another protocol. This setting is not available when you select the **Type** of **Standard**.

Property	Description
Protocol Profile (Client)	Specifies that the selected profile is a client-side profile. The list contains entries for each defined client protocol profile for the protocol selected in the **Protocol** property.
Protocol Profile (Server)	Specifies that the selected profile is a server-side profile. Options are: **(Use Client Profile)**, and entries for each already defined server protocol profile. The default is **(Use Client Profile)**.
VLAN and Tunnel Traffic	Specifies the VLANs and tunnels for which the virtual server is enabled or disabled. The default is **All VLANs and Tunnels**. • **All VLANs and Tunnels**: Specifies that the virtual server is enabled on all VLANs and tunnels configured on the system. • **Enabled on**: Specifies that the virtual server is enabled on the VLANs and tunnels specified in the **Selected** list. • **Disabled on**: Specifies that the virtual server is disabled on the VLANs and tunnels specified in the **Selected** list.
Default Pool	Specifies the pool name that you want the virtual server to use as the default pool. A load balancing virtual server sends traffic to this pool automatically, unless an iRule directs the server to send the traffic to another pool instead. Options are: **None**, and entries for each already defined pool. The default is **None**.
DoS Profile	Specifies the DoS profile to use, if enabled. Options are: **Disabled** and **Enabled**. The default is **Disabled**. When **Enabled** is selected, choose a DoS profile from those displayed in the Profile area. DoS profiles are defined using the Shared Security DoS Profiles panel.
HTTP Profile	Specifies the HTTP profile for managing HTTP traffic. Options are: **None**, and entries for each already defined HTTP profile. The default is **None**. ***Note:*** *Adapt profiles cannot be used when the* ***http-transparent*** *profile is selected.*
SIP Profile	Specifies the Session Initiation Protocol (SIP) profile for the system to use for this virtual server. Options are: **None**, and entries for each already defined SIP profile. The default is **None**.
DNS Profile	Specifies the Domain Name System (DNS) profile for the system to use for this virtual server. Options are: **None**, and entries for each already defined DNS profile. By selecting **dns** and specifying **53** for the **Service Port**, you can create a virtual server that acts as a DNS listener. The default is **None**. If you select **None** for a currently configured listener, the object is no longer a DNS listener.
Log Profiles	Specifies the log profile to be used. To select a log profile, use the arrow keys to move the log profile to the **Selected** column. To remove a selected log profile, use the arrow keys to move the log profile to the **Available** column. Log profiles listed in the **Available** column are defined using the Shared Security Logging Profiles panel.

3. When you are finished, click **Add** to create the new virtual server.

Editing virtual servers

Expand the Virtual Servers panel and use the screen to edit a virtual server.

Note: *Depending on the settings you configure, you may see only some of the screen elements described here.*

Editing virtual servers

From the Virtual Servers panel, you can expand the screen and edit virtual server properties.

1. Hover over the virtual server that you want to edit and click the gear icon, then select **Properties** to open the screen.
2. Click **Edit** to establish the lock and make it possible to edit the values on the property page.
3. Edit the properties. Not all properties can be modified.

Property	Description
Device	Specifies the discovered BIG-IP® device for the virtual server.
Name	Specifies the name of the virtual server.
Description	Specifies a description for the virtual server.
Partition	Specifies the partition or path to which the virtual server belongs. Only users with access to a partition can view the objects (such as the self IP address) that it contains. If the virtual server resides in the `Common` partition, all users can access it. ***Note:*** *Although pre-populated with* ***Common*** *(default), you can set the partition by replacing* ***Common*** *with a unique name for the partition. The partition with that name must already exist on the BIG-IP device. If it does not exist, then, at deployment, the deployment will fail. No whitespace is allowed in the partition name.*
Type	Specifies the network service provided by this virtual server. The default type is **Standard**. The possible types are listed. ***Note:*** *Not all properties are valid for all types. When you specify the type, certain properties may become available or unavailable.* • **Standard**: Specifies a virtual server that directs client traffic to a load balancing pool and is the most basic type of virtual server. When you first create the virtual server, you assign an existing default pool to it. From then on, the virtual server automatically directs traffic to that default pool. • **Forwarding (Layer 2)**: Specifies a virtual server that shares the same IP address as a node in an associated VLAN. This type of virtual server has no pool members to load balance. • **Forwarding (IP)**: Specifies a virtual server like other virtual servers, except that the virtual server has no pool members to load balance. The virtual server simply forwards the packet directly to the destination IP address specified in the client request.

Property	Description
	• **Performance (HTTP)**: Specifies a virtual server with which you associate a Fast HTTP profile. Together, the virtual server and profile increase the speed at which the virtual server processes HTTP requests. • **Performance (Layer 4)**: Specifies a virtual server with which you associate a Fast L4 profile. Together, the virtual server and profile increase the speed at which the virtual server processes Layer 4 requests. • **Stateless**: Specifies a virtual server that accepts traffic matching the virtual server address, and load balances the packet to the pool members without attempting to match the packet to a pre-existing connection in the connection table. New connections are immediately removed from the connection table. This addresses the requirement for one-way UDP traffic that needs to be processed at very high throughput levels, for example, load balancing syslog traffic to a pool of syslog servers. Stateless virtual servers are not suitable for processing traffic that requires stateful tracking, such as TCP traffic. Stateless virtual servers do not support iRules®, persistence, connection mirroring, rateshaping, or SNAT automap. • **Reject**: Specifies that the BIG-IP system rejects any traffic destined for the virtual server IP address. • **DHCP**: Specifies a virtual server that relays Dynamic Host Control Protocol (DHCP) client requests for an IP address to one or more DHCP servers, and provides DHCP server responses with an available IP address for the client. • **Internal**: Specifies a virtual server that supports modification of HTTP requests and responses.
Source	Specifies an IP address or network from which the virtual server accepts traffic. The virtual server accepts clients only from one of these IP addresses. For this setting to function effectively, specify a value other than `0.0.0.0/0` or `::/0` (that is, `any/0`, or `any6/0`). In order to maximize utility of this setting, specify the most specific address prefixes covering all customer addresses and no others. Specify the IP address in Classless Inter-Domain Routing (CIDR) format: address/prefix, where the prefix length is in bits: for example, for IPv4: `10.0.0.1/32` or `10.0.0.0/24`, and for IPv6: `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`.
Destination	Specifies the destination IP address information to which the virtual server sends traffic. • If the destination type is set to **Host**, specify only the IP address in the **Address** field. Specify the IP address in CIDR format: address/prefix, where the prefix length is in bits: for example, for IPv4: `10.0.0.1/32` or `10.0.0.0/24`, and for IPv6: `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. The defaults for DHCP are `255.255.255.255` (IPv4 Default) and ff02::1:2 (IPv6 Default). You can also select `Other` to specify another destination address. • If the destination type is set to **Network**, specify both the IP address in the **Address** field, and the network mask in the **Mask** field. Specify the mask address in CIDR format as you did the IP address.
Service Port	Type a service port or select a type from the list. When you select a type from the list, the value in the **Service Port** field changes to reflect the associated default, which you can change.
State	Specifies whether the virtual server and its resources are available for load balancing. The default is **Enabled**.

Property	Description
Connection Mirroring	Specifies that the system mirrors connections on each member in a redundant configuration. Connection mirroring is the process of duplicating connections from the active system to the standby system. Enabling this setting ensures a higher level of connection reliability, but it may also have an impact on system performance.
Protocol	Specifies a network protocol name that you want the system to use to direct traffic on this virtual server. The default is **TCP**. If the **Type** is set to **Performance (HTTP)**, the network protocol is set to **TCP**. If the **Type** is set to **DHCP**, the **Protocol** property is not available. The following are valid network protocol keywords. • ***All Protocols**: Specifies that the virtual server supports all network protocols. This setting is not available when you select the **Type** of **Standard**. • **TCP**: Specifies that the virtual server supports the TCP protocol, defined in RFC 675. • **UDP**: Specifies that the virtual server supports the UDP protocol, defined in RFC 768. • **SCTP**: Specifies that the virtual server supports the Stream Control Transmission Protocol (SCTP) protocol, defined in RFC 4960. • **Other**: Provides the ability to specify another protocol. This setting is not available when you select the **Type** of **Standard**.
Protocol Profile (Client)	Specifies that the selected profile is a client-side profile. The list contains entries for each defined client protocol profile for the protocol selected in the **Protocol** property.
Protocol Profile (Server)	Specifies that the selected profile is a server-side profile. Options are: **(Use Client Profile)**, and entries for each already defined server protocol profile. The default is **(Use Client Profile)**.
VLAN and Tunnel Traffic	Specifies the VLANs and tunnels for which the virtual server is enabled or disabled. The default is **All VLANs and Tunnels**. • **All VLANs and Tunnels**: Specifies that the virtual server is enabled on all VLANs and tunnels configured on the system. • **Enabled on**: Specifies that the virtual server is enabled on the VLANs and tunnels specified in the **Selected** list. • **Disabled on**: Specifies that the virtual server is disabled on the VLANs and tunnels specified in the **Selected** list.
Default Pool	Specifies the pool name that you want the virtual server to use as the default pool. A load balancing virtual server sends traffic to this pool automatically, unless an iRule directs the server to send the traffic to another pool instead. Options are: **None**, and entries for each already defined pool. The default is **None**.
DoS Profile	Specifies the DoS profile to use, if enabled. Options are: **Disabled** and **Enabled**. The default is **Disabled**. When **Enabled** is selected, choose a DoS profile from those displayed in the Profile area. DoS profiles are defined using the Shared Security DoS Profiles panel.
HTTP Profile	Specifies the HTTP profile for managing HTTP traffic. Options are: **None**, and entries for each already defined HTTP profile. The default is **None**. ***Note:** Adapt profiles cannot be used when the **http-transparent** profile is selected.*

Property	Description
SIP Profile	Specifies the Session Initiation Protocol (SIP) profile for the system to use for this virtual server. Options are: **None**, and entries for each already defined SIP profile. The default is **None**.
DNS Profile	Specifies the Domain Name System (DNS) profile for the system to use for this virtual server. Options are: **None**, and entries for each already defined DNS profile. By selecting **dns** and specifying **53** for the **Service Port**, you can create a virtual server that acts as a DNS listener. The default is **None**. If you select **None** for a currently configured listener, the object is no longer a DNS listener.
Log Profiles	Specifies the log profile to be used. To select a log profile, use the arrow keys to move the log profile to the **Selected** column. To remove a selected log profile, use the arrown keys to move the log profile to the **Available** column. Log profiles listed in the **Available** column are defined using the Shared Security Logging Profiles panel.

4. Click **Save** to save your changes as you go.
5. When you are finished, click **Save and Close** to save changes, release the lock, and exit the creen.

Removing virtual servers

1. Hover over the virtual server that you want to remove, click the gear icon, and select **Properties** to expand the panel.
2. Click **Remove**.
3. In the confirmation dialog box, click **Delete**.

Chapter 12

Managing Self IPs in Shared Security

About self IPs

On BIG-IP® devices, network objects such as virtual servers, self IP addresses, the management IP, route domains, and the global firewall, all have firewalls attached to them. On BIG-IQ® systems, an instance of one of these network objects is called a *firewall context*.

Using a BIG-IQ Security system, you can discover all firewall contexts currently on a BIG-IP device, and edit the firewall rules and/or policies attached to those firewall contexts.

From the Shared Security Self IPs panel, you can also create, configure, and delete a new self IP address firewall context, and then push that configured network object to a targeted BIG-IP device. In scenarios where self IP addresses are used primarily for security purposes, this provides a centralized and remote way for security administrators to quickly create additional listeners, or, firewall contexts.

Self IP addresses have many configuration options. BIG-IQ Security provides functionality meant for very basic security-centric use cases.

To close the panel without making any changes, click **Cancel**.

To get help on any panel, click the **(?)** icon in the upper right corner.

Adding Self IP addresses

Within Shared Security, hover over the Self IPs header and click the + icon when it appears, and click **New Self IP**. The panel expands to display the New Self IP properties screen.

Editing Self IPs

Hover over the name of the self IP address to edit, and when the gear icon appears, select **Properties** to expand the panel.

Adding self IP addresses

Use the New Self IP screen to configure a new self IP address.

Adding self IP addresses

1. Hover over the Self IPs header, click the + icon when it appears, and click **New Self IP**. The panel expands to display the New Self IP properties.
2. In the New Self IP screen, modify the properties of the new self IP address as appropriate.

Device	From the list, select a discovered BIG-IP® device. If there are multiple devices discovered, the default device is the one discovered first.
Name	Type the name of the self IP address definition.
Description	Type an (optional) description for the self IP address.

Partition	Type the partition or path to which the self IP address belongs. Only users with access to a partition can view the objects (such as the self IP address) that it contains. If the self IP address resides in the `Common` partition, all users can access it. ***Note:*** *Although pre-populated with* ***Common*** *(default), you can set the partition by typing a unique name for the partition. The partition with that name must already exist on the BIG-IP device. If it does not exist, then, at deployment, the deployment will fail. No whitespace is allowed in the partition name.*
IP Address/Prefix	Type the IP address of the self IP, including the prefix.
VLAN/Tunnel	Select the VLAN associated with this self IP address. The choices are defined on the BIG-IP device, and the default is **internal**.
Port Lockdown	Specify the protocols and services from which the self IP address can accept traffic. Note that having fewer active protocols enhances the security level of the self IP address and its associated VLANs. Options are: • **Allow Default**: Activates only the default protocols and services. You can determine the supported protocols and services by running the `tmsh list net self-allow defaults` command on the command line. • **Allow All**: Activates all TCP and UDP services on this self IP address. • **Allow None**: Specifies that this self IP address accepts no traffic. If you are using this self IP address as the local endpoint for WAN optimization, select this option to avoid potential port conflicts. This is the default. • **Allow Custom**: Activates the custom protocols and services you select for this self IP address using the expanded custom list options. • **Allow Custom (include Default)**: Activates the default protocols and services as well as the custom protocols and services you select for this self IP address using the expanded custom list options.
Floating	Specifies whether the self IP is floating. This is determined by the value of the Traffic Group property.
Traffic Group	Specifies the traffic group to associate with the self IP. Whether the self IP address can inherit the traffic group is set on the BIG-IP device and is only readable on the BIG-IQ system.

3. When you are finished, click **Add** to create the new self IP address.

Editing self IP addresses

Use the Self IPs Properties screen to edit the properties of a self IP address.

Editing self IPs

From the Self IPs panel, you can edit self IP address properties.

1. Hover over the self IP address that you want to edit, click the gear icon, and select **Properties** to expand the panel.
2. Click **Edit** to establish the lock and make it possible to edit the values on the property page.
3. Edit the properties. Not all properties can be modified.

Device	From the list, select a discovered BIG-IP® device. If there are multiple devices discovered, the default device is the one discovered first.
Name	Type the name of the self IP address definition.
Description	Type an (optional) description for the self IP address.
Partition	Type the partition or path to which the self IP address belongs. Only users with access to a partition can view the objects (such as the self IP address) that it contains. If the self IP address resides in the `Common` partition, all users can access it. ***Note:*** *Although pre-populated with* ***Common*** *(default), you can set the partition by typing a unique name for the partition. The partition with that name must already exist on the BIG-IP device. If it does not exist, then, at deployment, the deployment will fail. No whitespace is allowed in the partition name.*
IP Address/Prefix	Type the IP address of the self IP, including the prefix.
VLAN/Tunnel	Select the VLAN associated with this self IP address. The choices are defined on the BIG-IP device, and the default is **internal**.
Port Lockdown	Specify the protocols and services from which the self IP address can accept traffic. Note that having fewer active protocols enhances the security level of the self IP address and its associated VLANs. Options are: • **Allow Default**: Activates only the default protocols and services. You can determine the supported protocols and services by running the `tmsh list net self-allow defaults` command on the command line. • **Allow All**: Activates all TCP and UDP services on this self IP address. • **Allow None**: Specifies that this self IP address accepts no traffic. If you are using this self IP address as the local endpoint for WAN optimization, select this option to avoid potential port conflicts. This is the default. • **Allow Custom**: Activates the custom protocols and services you select for this self IP address using the expanded custom list options. • **Allow Custom (include Default)**: Activates the default protocols and services as well as the custom protocols and services you select for this self IP address using the expanded custom list options.
Floating	Specifies whether the self IP is floating. This is determined by the value of the Traffic Group property.
Traffic Group	Specifies the traffic group to associate with the self IP. Whether the self IP address can inherit the traffic group is set on the BIG-IP device and is only readable on the BIG-IQ system.

4. Click **Save** to save your changes as you go.
5. When finished, click **Save and Close** to save changes, release the lock, and exit the screen.

Chapter 13

Managing Route Domains in Shared Security

About route domains

The Route Domains panel lists route domains configured from BIG-IQ® Shared Security.

On BIG-IP® devices, network objects such as route domains, virtual servers, self IP addresses, the management IP address, and the global firewall, all have firewalls attached to them. On BIG-IQ systems, an instance of one of these network objects is called a *firewall context*.

Using a BIG-IQ Security system, you can discover all firewall contexts on a BIG-IP device, and edit the firewall rules and/or policies attached to the firewall context.

Note: *The BIG-IQ Security system only supports a default route domain with the* `Common` *partition, and an ID of 0 (*`/Common/0`*).*

From the Route Domains panel, you can create and edit route domain configurations that have VLANs, tunnels, or both, attached to them.

To close the New Route Domain properties panel without saving, click **Cancel**.

To get help on any panel, click the **(?)** icon in the upper right corner.

Adding route domains

Hover over the Route Domains header and click the **(+)** icon when it appears, then select **New Route Domain**. The panel expands to display properties on the New Route Domain screen.

Editing route domains

Hover over the name of the route domain that you want to edit and click the gear icon, then select **Properties** to expand the panel.

Removing route domains

Removing route domains defined on the BIG-IQ system is complex, and so a **Remove** button is not available for route domains as it is for other BIG-IQ Security components. To remove a route domain defined on a BIG-IQ system, reimport the route domain data to overwrite the data of the existing route domain. The configuration data to be overwritten must not have been deployed to a BIG-IP system.

Adding route domains

Use the New Route Domain screen to add and configure a new route domain. Using route domains, you can assign the same IP address to more than one device on a network, as long as each instance of the IP address resides in a separate route domain.

Note: *Depending on the settings you configure, you might see only some of the screen elements described.*

Note: *Configure and deploy route domains one at a time, when the BIG-IQ® is not also configuring other components. Configuring and deploying route domains in this way lessens the chance that a failed route domain deployment will require you to reimport BIG-IP® device configuration data.*

Adding route domains

1. Hover over the Route Domains header, click the + icon when it appears, and click **New Route Domain**. The panel expands to display the New Route Domain properties.
2. In the General Properties area of the New Route Domain screen, review and modify the properties as needed.

Property	Description
Device	Specifies the BIG-IP device. Select the BIG-IP device from the list.
Name	Specifies the unique name of the route domain.
Description	Specifies optional descriptive text that identifies the route domain.
Partition	Although pre-populated with **Common** (default), you can set the partition when creating route domains by entering a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP device. No white space is allowed in the partition name.*
Id	Type the identifying integer representing the route domain. The integer must be unique on the BIG-IP device, and be between 1 and 65534, including those values. An **Id** value of 0 is the default and indicates that all VLANs on a system pertain to this route domain. When you create new route domains, you can assign VLANs to those route domains and then move the VLANs out of the default route domain.

3. In the Configuration area, review or modify the configuration.

Configuration	Description
Strict Isolation	Specifies whether the system enforces cross-routing restrictions. Select either **Disabled** or **Enabled**. When enabled, routes cannot cross route domain boundaries (so they are strictly isolated to the current route domain). The default is enabled. When disabled, a route can cross route domains.
VLANs	Select the VLANs, including tunnels, that you want to be members of the route domain by moving them from the **Available** area to the **Selected** area. • **Available**: Lists defined VLANs not added to the route domain. • **Selected**: Lists defined VLANs that have been added to the route domain. When adding VLANs to a route domain, be aware that deployment errors will occur if the same VLAN is assigned to two or more route domains at the same time, or if a VLAN is not assigned to any route domain. To prevent these deployment errors, add and remove VLANs from route domains as follows. To add a VLAN to a route domain: **1.** Remove the VLAN from the route domain currently assigned to it (typically the default route domain), and save that route domain. **2.** Add that VLAN to a new route domain, and save the new route domain containing the VLAN. To remove a VLAN from a route domain: **1.** Remove the VLAN from the route domain currently assigned to it, and save that route domain. **2.** Add that VLAN to another route domain (typically the default route domain), and save the route domain containing the VLAN.

4. When finished, click **Add**.

Editing route domains

Use the Route Domains Properties screen to edit route domain configurations.

Editing route domains

From the Route Domains panel, you can edit the route domain configuration.

Note: *Depending on the settings you configure, you might see only some of the screen elements described.*

1. Hover over the route domain that you want to edit, click the gear icon, and select **Properties** to expand the panel.
2. Click **Edit** to establish the lock and make it possible to edit the values.
3. Edit the properties.
4. In the General Properties area of the expanded Route Domains screen, review and modify the properties as needed.

Property	Description
Device	Specifies the BIG-IP device. Select the BIG-IP device from the list.
Name	Specifies the unique name of the route domain.
Description	Specifies optional descriptive text that identifies the route domain.
Partition	Although pre-populated with **Common** (default), you can set the partition when creating route domains by entering a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP device. No white space is allowed in the partition name.*
Id	Type the identifying integer representing the route domain. The integer must be unique on the BIG-IP device, and be between 1 and 65534, including those values. An **Id** value of 0 is the default and indicates that all VLANs on a system pertain to this route domain. When you create new route domains, you can assign VLANs to those route domains and then move the VLANs out of the default route domain.

5. In the Configuration area, review or modify the configuration.

Configuration	Description
Strict Isolation	Specifies whether the system enforces cross-routing restrictions. Select either **Disabled** or **Enabled**. When enabled, routes cannot cross route domain boundaries (so they are strictly isolated to the current route domain). The default is enabled. When disabled, a route can cross route domains.
VLANs	Select the VLANs, including tunnels, that you want to be members of the route domain by moving them from the **Available** area to the **Selected** area. • **Available**: Lists defined VLANs not added to the route domain. • **Selected**: Lists defined VLANs that have been added to the route domain. When adding VLANs to a route domain, be aware that deployment errors will occur if the same VLAN is assigned to two or more route domains at the same

Configuration	Description
	time, or if a VLAN is not assigned to any route domain. To prevent these deployment errors, add and remove VLANs from route domains as follows. To add a VLAN to a route domain: **1.** Remove the VLAN from the route domain currently assigned to it (typically the default route domain), and save that route domain. **2.** Add that VLAN to a new route domain, and save the new route domain containing the VLAN. To remove a VLAN from a route domain: **1.** Remove the VLAN from the route domain currently assigned to it, and save that route domain. **2.** Add that VLAN to another route domain (typically the default route domain), and save the route domain containing the VLAN.

6. Click **Save** to save changes as you go.
7. When you are finished, click **Save and Close** to save the changes, release the lock, and exit the screen.

Removing route domains

Removing route domains defined on the BIG-IQ® system is complex, and so a **Remove** button is not available for route domains as it is for other BIG-IQ Security components. To remove a route domain defined on a BIG-IQ system, reimport the route domain data to overwrite the data of the existing route domain. The configuration data to be overwritten must not have been deployed to a BIG-IP® system.

1. Review the configuration of the BIG-IP system from which you plan to reimport the data, to make sure that you will not overwrite other configuration information you want to retain.
2. Reimport the data from the BIG-IP system to overwrite the existing route domain data on the BIG-IQ system, using the BIG-IQ Network Security Overview Devices panel.

Note: *Use care when reimporting, since it causes existing data to be overwritten.*

Note: *Configure and deploy route domains one at a time when no other portions of the system are being configured. Configuring and deploying route domains in this way lessens the chance that a failed route domain deployment will require you to reimport BIG-IP system configuration data.*

Chapter 14

Managing DoS Profiles in Shared Security

About DoS profiles

The DoS Profiles panel in Shared Security lists configured DoS profiles.

Using BIG-IQ® Security, you can configure profiles to detect and protect against DoS (Denial of Service) attacks.

DoS attack detection and prevention serves the following functions:

- It detects and automatically drops packets that are malformed or contain errors.
- It logs unusual increases in packets of any type, including packets that are malformed, packets that contain errors, or packets of any other type that appear to rapidly increase.

You can use the DoS Protection profile to configure the percentage increase over the system baseline, which indicates that a possible attack is in process on a particular query type, or an increase in anomalous packets. Additionally, you can use reporting or logging functions to detect such packets.

You can enable Layer 7 application DoS protection of HTTP traffic, Layer 7 DoS protection for SIP traffic, and Layers 2-4 application DNS DoS security.

To cancel any operation without saving and close the panel, click **Cancel**.

To get help on any panel, click the **(?)** icon in the upper right corner.

Adding DoS profiles

Hover over the DoS Profiles header, click the **(+)** icon when it appears, and click **New DoS Profile**. The panel expands to display the new DoS Profile screen.

Editing DoS profiles

Hover over the DoS profile header you want to edit, and when the gear icon appears, select **Properties** to expand the panel.

Adding DoS profiles

Use the New DoS Profiles panel to configure a new DoS profile.

Note: *Depending on the settings you configure, you may see only some of the screen elements described here.*

Adding DoS profiles

1. Hover over the Dos Profiles header, click the + icon when it appears, and click **New DoS Profile**. The panel expands to display the New DoS Profile properties.
2. In the New DoS Profile screen, review, and add or modify the properties as appropriate.

Property	Description
Name	Specify a unique user-provided name for the DoS profile. Required.
Description	Specify an optional description for the DoS profile.
Partition	Specify the partition to which the DoS profile belongs. Only users with access to a partition can view the objects (such as the DoS profile) that it contains. If the DoS

Property	Description
	profile resides in the `Common` partition, all users can access it. Although this field is pre-populated with **Common** (default), you can set the partition when creating DoS profiles by typing a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP® device. No whitespace is allowed in the partition name.*

3. Select **Enabled** to the right of one or more protection types to enable those types. A configuration tab is added dynamically when a protection type is selected. Click the tab to configure the protection type.

Property	Description
Application Security	When enabled, protects your web application against DoS attacks. Click **Application Security** to configure the application security protection.
Protocol DNS	When enabled, protects your DNS server against DoS attacks. Note that your virtual server must include a DNS profile to work with this feature. Use the **Protocol DNS** settings to configure the DNS server protection.
Protocol SIP	When enabled, protects against SIP DoS attacks. Note that your virtual server must include a SIP profile to work with this feature. Use the **Protocol SIP** settings to configure the SIP DoS protection.
Network	hen enabled, protects your server against network DoS attacks.Use the **Network** settings to configure the network DoS protection.

4. Configure the selected protection types by clicking the matching protection type tab, and supplying or modifying any necessary property values.
5. When finished, click **Add**.

Editing DoS profiles

Expand the DoS Profiles panel to edit a DoS profile. The profile is used to fine tune both the circumstances under which the system considers traffic to be a DoS attack, and how the system handles a DoS attack.

Editing DoS profiles

From the DoS Profiles panel, you can edit DoS profile properties.

1. Hover over the DoS profile that you want to edit, click the gear icon, and select **Properties** to expand the panel.
2. Click **Edit** to lock the DoS profile for editing and make it possible to edit the property values.
3. Edit the properties.

Property	Description
Name	Specify a unique user-provided name for the DoS profile. Required.
Description	Specify an optional description for the DoS profile.
Partition	Specify the partition to which the DoS profile belongs. Only users with access to a partition can view the objects (such as the DoS profile) that it contains. If the DoS profile resides in the `Common` partition, all users can access it. Although this field is

Property	Description
	pre-populated with **Common** (default), you can set the partition when creating DoS profiles by typing a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP® device. No whitespace is allowed in the partition name.*

4. Select **Enabled** to the right of one or more protection types to enable those types. A configuration tab is added dynamically when a protection type is selected. Click the tab to configure the protection type.

Property	Description
Application Security	When enabled, protects your web application against DoS attacks. Click **Application Security** to configure the application security protection.
Protocol DNS	When enabled, protects your DNS server against DoS attacks. Note that your virtual server must include a DNS profile to work with this feature. Use the **Protocol DNS** settings to configure the DNS server protection.
Protocol SIP	When enabled, protects against SIP DoS attacks. Note that your virtual server must include a SIP profile to work with this feature. Use the **Protocol SIP** settings to configure the SIP DoS protection.
Network	hen enabled, protects your server against network DoS attacks. Use the **Network** settings to configure the network DoS protection.

5. Configure the selected protection types by clicking the matching protection type tab, and supplying or modifying any necessary property values.
6. Click **Save** to save your changes as you go.
7. When finished, click **Save and Close** to save changes, release the lock, and exit the panel.

Removing DoS profiles

1. Hover over the DoS profile that you want to remove, click the gear icon, and select **Properties** to expand the panel.
2. Click **Remove**.
3. In the confirmation dialog box, click **Delete**.

Chapter
15

Managing Device DoS in Shared Security

About device DoS

You can use the Device DoS panel to manage your devices response to DoS attacks, including having a network white list.

To get help on any panel, click the **(?)** icon in the upper right corner.

Importing devices

You do not import devices using the BIG-IQ® system; instead,you export them from BIG-IP® systems to the BIG-IQ system.

Editing devices

Hover over the header of the device you want to edit, when the gear icon appears, click it and select **Properties** to expand the panel.

Editing device DoS

Use the Device DoS panel to edit and view the device DoS properties.

1. Hover over the header of the device you want to edit and when the gear icon appears, click it and select **Properties** to expand the panel.
2. Modify the device properties as needed. Note that not all properties can be modified. Some properties are read-only.
   - Use the **Device Configuration** settings to view values within the configuration.
   - Use the **Network Whitelist** settings to add, delete or modify whitelist entries.
3. When you are finished, click **Save** to save changes and exit the panel.

Editing device configuration entries

You edit device configuration entries using the **Device Configuration** settings.

1. Locate the configuration category containing the entry to modify, click the + at the end of it. The category expands.
2. Click the value to change and then edit it.
3. To end the edit mode, click the check mark (□)at the end of the entry; to cancel the change, click the **X** at the end of the entry.
4. Click **Save** to save changes and exit the panel.

Adding network whitelist entries

You add network whitelist entries using the **Network Whitelist** settings.

1. Click **Network Whitelist** and then click**Add new**. The Edit/Add properties screen displays. Only 8 whitelist entries can exist at a time.
2. Type or modify the properties as needed. You can specify IPv4 or IPv6 addresses in CIDR notation as values to the address fields. You can specify a source address or destination address but not both in the same whitelist entry.

3. Click **Done** to complete the whitelist entry.
4. Click **Save** to save changes and exit the panel.

Editing network whitelist entries

You edit network whitelist entries using the **Network Whitelist** settings.

1. Click the edit icon at the end of the row containing the whitelist to edit. The Edit/Add properties screen displays.
2. Modify the properties as needed and click **Done**.
3. Click **Save** to save changes and close the screen.

Deleting network whitelist entries

You delete network whitelist entries using the **Network Whitelist** settings.

1. Select the check box to the left of the whitelist you want to delete.
2. Click **Delete** on the Network Whitelist tab.
3. Click **Save** to save changes and exit the screen.

Chapter
16

Managing Logging Profiles in Shared Security

About logging profiles

The Logging Profiles panel in Shared Security lists logging profiles, scaled so that a subset of profiles is visible in the panel at any given time.

A *logging profile* records requests to the virtual server. A logging profile determines where events are logged, and which items (such as which parts of requests, or which type of errors) are logged. Events can be logged either locally by the system and viewed in the Event Logs screens, or remotely by the client's server. The system forwards the log messages to the client's server using the Syslog service.

The logging profile can be associated with multiple virtual servers from multiple devices. Multiple logging profiles can be associated with a virtual server, but the multiple logging profiles cannot have an overlap subset configured. For example, two logging profiles with application security configured and enabled cannot be associated with the same virtual server.The application security and protocol security cannot be configured on the same logging profile or associated with the same virtual server. BIG-IQ Security supports importing logging profiles with spaces in the name. An imported logging profile with spaces in the name can be modified on the BIG-IQ Security system and deployed back to a BIG-IP device. However, the BIG-IQ system does not support creating logging profiles with spaces in the name.

The logging publisher cannot be created or modified by the BIG-IQ Security system. The logging publisher specified by the BIG-IQ logging profile should be the same as that configured on the BIG-IP device.

To close the New Logging Profile properties panel without saving, click **Cancel**.

To get help on any panel, click the **(?)** icon in the upper right corner.

Adding logging profiles

Hover over the Logging Profiles header, click the + icon when it appears, and click **New Logging Profile**. The panel expands to display the New Logging Profile properties.

Editing logging profiles

Hover over the header of the logging profile you want to edit and when the gear icon appears, click it and select **Properties** to expand the panel.

Adding logging profiles

Use the New Logging Profile screen to configure a new logging profile.

Note: *Depending on the settings you configure, you may see only some of the screen elements described here.*

Adding logging profiles

1. Hover over the Logging Profiles header, click the + icon when it appears, and click **New Logging Profile**. The panel expands to display the New Logging Profile properties.
2. In the New Logging Profiles screen, review and add or modify the properties as appropriate.

Property	Description
Name	Specify a unique user-provided name for the logging profile. Required.

Property	Description
Description	Specify the optional description for the logging profile.
Partition	Specify the partition to which the logging profile belongs. Only users with access to a partition can view the objects (such as the logging profile) that it contains. If the logging profile resides in the `Common` partition, all users can access it. Although this field is pre-populated with **Common** (default), you can set the partition when creating logging profiles by typing a unique name for the partition. ***Note:*** *The partition with that name must already exist on the BIG-IP® device. No whitespace is allowed in the partition name.*

3. Select **Enabled** to the right of one or more logging types to enable those types. A configuration tab is added dynamically when a logging type is selected. Click the tab to configure the logging type.

Property	Description
Application Security	When enabled, specifies that the system logs traffic to the web application. When **Application Security** is enabled, **Protocol Security** cannot be selected at the same time. Click **Application Security** to configure the application security log.
Protocol Security	When enabled, specifies that the system logs any dropped, malformed, and/or rejected requests sent through the given protocol. When **Protocol Security** is enabled, **Application Security**cannot be selected at the same time. **Protocol Security** includes processing one or more of the following: • HTTP, FTP, and SMTP security • DNS security • SIP security
Network Firewall	When enabled, specifies that the system logs ACL rule matches, TCP events, and/or TCP/IP errors sent to the network firewall. Includes processing one or more of the following: • Network Firewall • IP Intelligence • Traffic Statistics
DoS Protection	When enabled, specifies that the system logs detected DoS attacks, and where DoS events are logged. Includes processing one or more of the following: • DoS Application Protection • DNS DoS Protection • SIP DoS Protection • Network DoS Protection

4. Configure the logging types by clicking the matching logging type tab and supplying any necessary property values. (Properties are grouped by logging type and screen area in the following tables.)

   In the **Application Security** Configuration section, you configure settings determining where to log traffic and which traffic to log.

Application Security - Configuration	Description
Local Storage	Specifies when checked (enabled), that the system stores all traffic in the system.

Application Security - Configuration	Description
Guarantee Local Logging	Specifies, when checked (enabled), that the system logs all requests, even though this may slow your web application. When cleared (disabled), specifies that the system logs requests as long as it does not slow your web application. The default is disabled. In either case, the system does not drop requests.
Response Logging	Specifies whether the system logs HTTP responses. • **Off:** Specifies that the system does not log responses. This is the default setting. • **For Illegal Requests Only:** Specifies that the system logs responses to illegal requests. • **For All Requests:** Specifies that the system logs all responses if the **Request Type** setting in the Storage Filter area of this screen is set to **All Requests**.
Remote Storage	Specifies when checked (enabled), that the system stores all traffic on a remote logging server.

In the **Application Security** Storage Filter section, you configure settings for the type of requests the system, or server logs.

Application Security - Storage Filter	Description
Logic Operation	Specifies whether requests must meet one or all criteria in the Storage Filter area for the system, or server, to log the requests. • **OR:** Specifies that requests must meet at least one of the criterion in the Storage Filter settings in order for the system, or server, to log the requests. This is the default. • **AND:** Specifies that requests must meet all of the criteria in the torage Filter settings in order for the system, or server, to log the requests.
Request Type	Specifies which kind of requests the system, or server, logs. • **Illegal requests only:** Specifies that the system, or server, logs only illegal requests. This is the default. • **Illegal requests, and requests that include staged attack signatures:** Specifies that the system, or server, logs illegal requests, and logs requests that include attack signatures in staging (even though the system considers those requests legal). • **All requests:** Specifies that the system, or server, logs all requests.
Protocols	Specifies whether request logging is dependent on the protocol. • **All:** Specifies that the system, or server, logs requests using the HTTP and HTTPS protocols. This is the default. • **Only:** Specifies that the system, or server, logs requests using only one specific protocol. Select **HTTP** or **HTTPS**.
Response Status Codes	Specifies whether request logging is dependent on the response status code. This filter setting applies only to requests that are not blocked by the system. • **All:** Specifies that the system, or server, logs all requests that generate all response status codes. This is the default.

Application Security - Storage Filter	Description
	• **Only:** Specifies that the system, or server, logs only requests that generate specific response status codes. When selected, isplaysadditional options where you specify the type of response status code to log. Unused status codes are in the **Available** list, selected status codes are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the **Available** list and the **Selected** list.
HTTP Methods	Specifies whether request logging is dependent on the HTTP method. • **All:** Specifies that the system, or server, logs requests using all HTTP methods. This is the default. • **Only:** Specifies that the system, or server, only logs requests using a specific HTTP method. When selected, displaysoptions where you specify the type of HTTP method to log. Unused HTTP methods are in the **Available** list, selected HTTP methods are in the **Selected** list.

Request Containing String	Specifies whether the request logging is dependent on a specific string.
	• **All:** Specifies that the system logs all requests, regardless of string. This is the default.
	• **Search in:** Specifies that the system logs only requests containing a specific string in a particular part of the request.
	  • Select the part of the request to search from the list (**Request**, **URI**, **Query String**, **Post Data**, or **Headers**.
	  • Type the string to search for in the request in the field to the right. The search is case-sensitive.

In the Protocol Security HTTP, FTP, and SMTP Security area, you configure where the system logs requests using the HTTP, FTP, and SMTP protocols.

Protocol Security - HTTP, FTP, and SMTP Security	Description
Publisher	Specifies where the system sends log messages. Select a publisher from the list, or accept the default of **None**.

In the Protocol Security DNS Security area, you configure where the system logs any dropped, malformed, rejected, and malicious DNS requests.

Protocol Security - DNS Security	Description
Publisher	Specifies the name of the log publisher used for logging DNS security events. Select a log publisher from the list, or accept the default of **None**.
Log Dropped Requests	Specifies, when enabled, that the system logs dropped DNS requests.
Log Filtered Dropped Requests	Specifies, when enabled, that the system logs dropped DNS requests.
Log Malformed Requests	Specifies, when enabled, that the system logs malformed DNS requests.

Protocol Security - DNS Security	Description
Log Rejected Requests	Specifies, when enabled, that the system logs rejected DNS requests.
Log Malicious Requests	Specifies, when enabled, that the system logs malicious DNS requests.

Storage Format	Specifies the format type for log messages. You can configure the following options:
	• **None** Specifies that the system uses the default format type to log the messages to a Remote Syslog server. This is the default setting.
	• **Field-List** Specifies that the system uses a set of fields, set in a specific order, to log messages. When **Field-List** is selected, specify the field list as follows.
	  • Specify the delimiter string in the **Delimiter** field. The default delimiter is the comma character (,).
	  *Note: You may not use the **$** character because it is reserved for internal usage.*
	  • Select the fields to use. Unused fields are in the **Available** list, selected fields are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.
	• **User-Defined** Specifies that the format the system uses to log messages is in the form of a user-defined string. Select the items for the server to log. Unused items are in the **Available** list, selected items are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.

In the Protocol Security SIP Security section, you configure where the system logs any dropped and malformed malicious SIP requests, global and request failures, redirected responses, and server errors.

Protocol Security - SIP Security	Description
Publisher	Specifies the name of the log publisher used for logging SIP protocol security events. Select a log publisher configured in your system.
Log Dropped Requests	Specifies, when enabled, that the system logs dropped requests.
Log Global Failures Requests	Specifies, when enabled, that the system logs global failures.
Log Malformed Requests	Specifies, when enabled, that the system logs malformed requests.
Log Redirection Responses Requests	Specifies, when enabled, that the system logs redirection responses.
Log Request Failures	Specifies, when enabled, that the system logs request failures.
Log Server Errors	Specifies, when enabled, that the system logs server errors.

Protocol Security - SIP Security	Description

Storage Format	Specifies the format type for log messages. You can configure the following options:
	• **None** Specifies that the system uses the default format type to log the messages to a Remote Syslog server. This is the default setting.
	• **Field-List** Specifies that the system uses a set of fields, set in a specific order, to log messages. When **Field-List** is selected, specify the field list as follows.
	  • Specify the delimiter string in the **Delimiter** field. The default delimiter is the comma character (,).
	  Note: *You may not use the* ***$*** *character because it reserved for internal usage.*
	  • Select the fields to use. Unused fields are in the **Available** list, selected fields are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.
	• **User-Defined** Specifies that the format the system uses to log messages is in the form of a user-defined string. Select the items for the server to log. Unused items are in the **Available** list, selected items are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.

In the Network Firewall section, you configure which network firewall events the system logs, and where they are logged.

Network Firewall Security - Network Firewall	Description
Publisher	Specifies the name of the log publisher used for logging Network events. Select a log publisher configured in your system.
Aggregate Rate Limit	Defines a rate limit for all combined network firewall log messages per second. Beyond this rate limit, log messages are not logged. You can select a **Rate Limit** value of **Indefinite**, which sets the rate limit to the maximum of 4294967295, or you can select **Specify** to specify a lower rate limit as an integer between 0 and 4294967295.
Log Rule Matches	Specifies, when enabled, that the system logs packets that match the ACL rules. When specifying the **Rate Limit** with one of the match types, a value of **Indefinite** sets the rate limit to the maximum of 4294967295, and a value of **Specify** allows you to specify a lower rate limit as an integer between 0 and 4294967295. • **Accept** Specifies, when enabled, that the system logs packets that match ACL rules configured with `action = Accept`. When enabled, you can specify a rate limit for all network firewall log messages with this action. If this rate limit is exceeded, log messages of this action type are not logged until the threshold drops below the specified rate. You can pecify a **Rate Limit** value of **Indefinite**or **Specify**. • **Drop** Specifies, when enabled, that the system logs packets that match ACL rules configured with `action = Drop`. When enabled, you can specify a rate limit for all network firewall log messages with this action. If this rate limit is exceeded, log messages of this action type are not logged until the threshold

Network Firewall Security - Network Firewall	Description
	drops below the specified rate. You can pecify a **Rate Limit** value of **Indefinite**or **Specify**. • **Reject** Specifies, when enabled, that the system logs packets that match ACL rules configured with `action = Reject`. When enabled, you can specify a rate limit for all network firewall log messages with this action. If this rate limit is exceeded, log messages of this action type are not logged until the threshold drops below the specified rate. You can pecify a **Rate Limit** value of **Indefinite**or **Specify**.
Log IP Errors	Specifies, when enabled, that the system logs IP error packets. When enabled, you can specify a rate limit for all network firewall log messages of this type. If this rate limit is exceeded, log messages of this type are not logged until the threshold drops below the specified rate. You can select a **Rate Limit** value of **Indefinite**, which means the rate limit is set to the maximum of 4294967295, or you can select **Specify** and specify an integer between 0 and 4294967295 that represents the number of messages per second.
Log TCP Errors	Specifies, when enabled, that the system logs TCP error packets. If this rate limit is exceeded, log messages of this type are not logged until the threshold drops below the specified rate. You can select a **Rate Limit** value of **Indefinite** which means the rate limit is set to the maximum of 4294967295, or you can select **Specify** and specify an integer between 0 and 4294967295 that represents the number of messages per second.
Log TCP Events	Specifies, when enabled, that the system logs TCP events (open and close of TCP sessions). If this rate limit is exceeded, log messages of this type are not logged until the threshold drops below the specified rate. You can select a **Rate Limit** value of **Indefinite** which means the rate limit is set to the maximum of 4294967295, or you can select **Specify** and specify an integer between 0 and 4294967295 that represents the number of messages per second.
Log Translation Fields	Specifies, when enabled, that translation values are logged if and when a network firewall event is logged.
Always Log Region	Specifies, when enabled, that the geographic location should be logged when a geolocation event causes a network firewall event.

Storage Format	Specifies the format type for log messages. You can configure the following options:
	• **None** Specifies that the system uses the default format type to log the messages to a Remote Syslog server. This is the default setting.
	• **Field-List** Specifies that the system uses a set of fields, set in a specific order, to log messages. When **Field-List** is selected, specify the field list as follows.
	  • Specify the delimiter string in the **Delimiter** field. The default delimiter is the comma character (,).
	  Note: *You may not use the* ***$*** *character because it reserved for internal usage.*
	  • Select the fields to use. Unused fields are in the **Available** list, selected fields are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.

Network Firewall Security - Network Firewall	Description
	• **User-Defined** Specifies that the format the system uses to log messages is in the form of a user-defined string. Select the items for the server to log. Unused items are in the **Available** list, selected items are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.

In the Network Firewall Security IP Intelligence section, you configure where IP intelligence events are logged. If the IP intelligence feature is enabled and licensed, you can configure the system to log source IP addresses that match an IP intelligence blacklist or whitelist category, as determined by the database of preconfigured categories, or as determined from an IP intelligence feed list.

Network Firewall Security - IP Intelligence	Description
Publisher	Specifies the name of the log publisher used for logging IP address intelligence events. Select a log publisher configured in your system.
Aggregate Rate Limit	Defines a rate limit for all combined IP intelligence log messages per second. Beyond this rate limit, log messages are not logged until the threshold drops below the specified rate. You can select a **Rate Limit** value of **Indefinite** which means the rate limit is set to the maximum of 4294967295, or you can select **Specify** and specify an integer between 0 and 4294967295 that represents the number of messages per second.
Log Translation Fields	Specifies, when enabled, that translation values are logged if and when a network firewall event is logged.

In the Network Firewall Security Traffic Statistics section, you configure logging of traffic statistics.

Network Firewall Security - Traffic Statistics	Description
Publisher	Specifies the name of the log publisher used for logging traffic statistics. Select a log publisher configured in your system.
Log Timer Events	• **Active Flows** - When enabled, logs the number of active flows each second. • **Reaped Flows** - When enabled, logs the number of reaped flows, or connections that are not established because of system resource usage levels. • **Missed Flows** - When enabled, logs the number of packets that were dropped because of a flow table miss. A *flow table miss* occurs when a TCP non-SYN packet does not match an existing flow. • **SYN Cookie (Per Session Challenge)** - When enabled, logs the number of SYN cookie challenges generated each second. • **SYN Cookie (White-listed Clients)** - When enabled, logs the number of whitelisted SYN cookie clients each second.

In the DoS Protection sections, you configure where DoS events are logged.

DoS Protection - DoS Application Protection	Description
Local Publisher	Specifies, when enabled, that the system logs DoS events to the local database.
Remote Publisher	Specifies the name of the log publisher used for logging DoS events. Select a log publisher configured in your system.

DoS Protection - DNS DoS Protection	Description
Publisher	Specifies the name of the log publisher used for logging DNS DoS events. Select a log publisher configured in your system.

DoS Protection - SIP DoS Protection	Description
Publisher	Specifies the name of the log publisher used for logging SIP DoS events. Select a log publisher configured in your system.

DoS Protection - Network DoS Protection	Description
Publisher	Specifies the name of the log publisher used for logging Network DoS events. Select a log publisher configured in your system.

5. When finished, click **Add**.

Editing logging profiles

Use the expanded Logging Profile panel to edit logging profiles.

Editing logging profile properties

Click **Properties** to edit the logging profile description and change which security levels are enabled.

1. Click **Properties** to ensure that it is selected.
2. Click **Edit** to establish the lock and make it possible to edit the properties.
3. In the Logging Profiles screen, review and add or modify the properties as appropriate.

Property	Description
Name	Specify a unique user-provided name for the logging profile. Required.
Description	Specify the optional description for the logging profile.
Partition	Specify the partition to which the logging profile belongs. Only users with access to a partition can view the objects (such as the logging profile) that it contains. If the logging profile resides in the `Common` partition, all users can access it. Although this field is pre-populated with **Common** (default), you can set the partition when creating logging profiles by typing a unique name for the partition.

Property	Description
	Note: *The partition with that name must already exist on the BIG-IP® device. No whitespace is allowed in the partition name.*

4. Select **Enabled** to the right of one or more logging types to enable those types. A configuration tab is added dynamically when a logging type is selected. Click the tab to configure the logging type.

Property	Description
Application Security	When enabled, specifies that the system logs traffic to the web application. When **Application Security** is enabled, **Protocol Security** cannot be selected at the same time. Click **Application Security** to configure the application security log.
Protocol Security	When enabled, specifies that the system logs any dropped, malformed, and/or rejected requests sent through the given protocol. When **Protocol Security** is enabled, **Application Security**cannot be selected at the same time. **Protocol Security** includes processing one or more of the following: • HTTP, FTP, and SMTP security • DNS security • SIP security
Network Firewall	When enabled, specifies that the system logs ACL rule matches, TCP events, and/or TCP/IP errors sent to the network firewall. Includes processing one or more of the following: • Network Firewall • IP Intelligence • Traffic Statistics
DoS Protection	When enabled, specifies that the system logs detected DoS attacks, and where DoS events are logged. Includes processing one or more of the following: • DoS Application Protection • DNS DoS Protection • SIP DoS Protection • Network DoS Protection

5. Configure the logging types by clicking the matching logging type tab and supplying any necessary property values. (Properties are grouped by logging type and screen area in the following tables.)

   In the **Application Security** Configuration section, you configure settings determining where to log traffic and which traffic to log.

Application Security - Configuration	Description
Local Storage	Specifies when checked (enabled), that the system stores all traffic in the system.
Guarantee Local Logging	Specifies, when checked (enabled), that the system logs all requests, even though this may slow your web application. When cleared (disabled), specifies that the system logs requests as long as it does not slow your web application. The default is disabled. In either case, the system does not drop requests.

Application Security - Configuration	Description
Response Logging	Specifies whether the system logs HTTP responses. • **Off:** Specifies that the system does not log responses. This is the default setting. • **For Illegal Requests Only:** Specifies that the system logs responses to illegal requests. • **For All Requests:** Specifies that the system logs all responses if the **Request Type** setting in the Storage Filter area of this screen is set to **All Requests**.
Remote Storage	Specifies when checked (enabled), that the system stores all traffic on a remote logging server.

In the **Application Security** Storage Filter section, you configure settings for the type of requests the system, or server logs.

Application Security - Storage Filter	Description
Logic Operation	Specifies whether requests must meet one or all criteria in the Storage Filter area for the system, or server, to log the requests. • **OR:** Specifies that requests must meet at least one of the criterion in the Storage Filter settings in order for the system, or server, to log the requests. This is the default. • **AND:** Specifies that requests must meet all of the criteria in the torage Filter settings in order for the system, or server, to log the requests.
Request Type	Specifies which kind of requests the system, or server, logs. • **Illegal requests only:** Specifies that the system, or server, logs only illegal requests. This is the default. • **Illegal requests, and requests that include staged attack signatures:** Specifies that the system, or server, logs illegal requests, and logs requests that include attack signatures in staging (even though the system considers those requests legal). • **All requests:** Specifies that the system, or server, logs all requests.
Protocols	Specifies whether request logging is dependent on the protocol. • **All:** Specifies that the system, or server, logs requests using the HTTP and HTTPS protocols. This is the default. • **Only:** Specifies that the system, or server, logs requests using only one specific protocol. Select **HTTP** or **HTTPS**.
Response Status Codes	Specifies whether request logging is dependent on the response status code. This filter setting applies only to requests that are not blocked by the system. • **All:** Specifies that the system, or server, logs all requests that generate all response status codes. This is the default. • **Only:** Specifies that the system, or server, logs only requests that generate specific response status codes. When selected, isplaysadditional options where you specify the type of response status code to log. Unused status codes are in the **Available** list, selected status codes are in the **Selected** list. Use the

Application Security - Storage Filter	Description
	Move arrow buttons to transfer the selected items between the **Available** list and the **Selected** list.
HTTP Methods	Specifies whether request logging is dependent on the HTTP method. • **All:** Specifies that the system, or server, logs requests using all HTTP methods. This is the default. • **Only:** Specifies that the system, or server, only logs requests using a specific HTTP method. When selected, displaysoptions where you specify the type of HTTP method to log. Unused HTTP methods are in the **Available** list, selected HTTP methods are in the **Selected** list.

Request Containing String	Specifies whether the request logging is dependent on a specific string.
	• **All:** Specifies that the system logs all requests, regardless of string. This is the default.
	• **Search in:** Specifies that the system logs only requests containing a specific string in a particular part of the request.
	  • Select the part of the request to search from the list (**Request**, **URI**, **Query String**, **Post Data**, or **Headers**.
	  • Type the string to search for in the request in the field to the right. The search is case-sensitive.

In the Protocol Security HTTP, FTP, and SMTP Security area, you configure where the system logs requests using the HTTP, FTP, and SMTP protocols.

Protocol Security - HTTP, FTP, and SMTP Security	Description
Publisher	Specifies where the system sends log messages. Select a publisher from the list, or accept the default of **None**.

In the Protocol Security DNS Security area, you configure where the system logs any dropped, malformed, rejected, and malicious DNS requests.

Protocol Security - DNS Security	Description
Publisher	Specifies the name of the log publisher used for logging DNS security events. Select a log publisher from the list, or accept the default of **None**.
Log Dropped Requests	Specifies, when enabled, that the system logs dropped DNS requests.
Log Filtered Dropped Requests	Specifies, when enabled, that the system logs dropped DNS requests.
Log Malformed Requests	Specifies, when enabled, that the system logs malformed DNS requests.
Log Rejected Requests	Specifies, when enabled, that the system logs rejected DNS requests.

Protocol Security - DNS Security	Description
Log Malicious Requests	Specifies, when enabled, that the system logs malicious DNS requests.

Storage Format	Specifies the format type for log messages. You can configure the following options:
	• **None** Specifies that the system uses the default format type to log the messages to a Remote Syslog server. This is the default setting.
	• **Field-List** Specifies that the system uses a set of fields, set in a specific order, to log messages. When **Field-List** is selected, specify the field list as follows.
	  • Specify the delimiter string in the **Delimiter** field. The default delimiter is the comma character (,).
	  Note: *You may not use the **$** character because it reserved for internal usage.*
	  • Select the fields to use. Unused fields are in the **Available** list, selected fields are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.
	• **User-Defined** Specifies that the format the system uses to log messages is in the form of a user-defined string. Select the items for the server to log. Unused items are in the **Available** list, selected items are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.

In the Protocol Security SIP Security section, you configure where the system logs any dropped and malformed malicious SIP requests, global and request failures, redirected responses, and server errors.

Protocol Security - SIP Security	Description
Publisher	Specifies the name of the log publisher used for logging SIP protocol security events. Select a log publisher configured in your system.
Log Dropped Requests	Specifies, when enabled, that the system logs dropped requests.
Log Global Failures Requests	Specifies, when enabled, that the system logs global failures.
Log Malformed Requests	Specifies, when enabled, that the system logs malformed requests.
Log Redirection Responses Requests	Specifies, when enabled, that the system logs redirection responses.
Log Request Failures	Specifies, when enabled, that the system logs request failures.
Log Server Errors	Specifies, when enabled, that the system logs server errors.
Storage Format	Specifies the format type for log messages. You can configure the following options: • **None** Specifies that the system uses the default format type to log the messages to a Remote Syslog server. This is the default setting.

Protocol Security - SIP Security	Description

	• **Field-List** Specifies that the system uses a set of fields, set in a specific order, to log messages. When **Field-List** is selected, specify the field list as follows.
	  • Specify the delimiter string in the **Delimiter** field. The default delimiter is the comma character (,).
	  Note: *You may not use the **$** character because it reserved for internal usage.*
	  • Select the fields to use. Unused fields are in the **Available** list, selected fields are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.
	• **User-Defined** Specifies that the format the system uses to log messages is in the form of a user-defined string. Select the items for the server to log. Unused items are in the **Available** list, selected items are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.

In the Network Firewall section, you configure which network firewall events the system logs, and where they are logged.

Network Firewall Security - Network Firewall	Description
Publisher	Specifies the name of the log publisher used for logging Network events. Select a log publisher configured in your system.
Aggregate Rate Limit	Defines a rate limit for all combined network firewall log messages per second. Beyond this rate limit, log messages are not logged. You can select a **Rate Limit** value of **Indefinite**, which sets the rate limit to the maximum of 4294967295, or you can select **Specify** to specify a lower rate limit as an integer between 0 and 4294967295.
Log Rule Matches	Specifies, when enabled, that the system logs packets that match the ACL rules. When specifying the **Rate Limit** with one of the match types, a value of **Indefinite** sets the rate limit to the maximum of 4294967295, and a value of **Specify** allows you to specify a lower rate limit as an integer between 0 and 4294967295. • **Accept** Specifies, when enabled, that the system logs packets that match ACL rules configured with `action = Accept`. When enabled, you can specify a rate limit for all network firewall log messages with this action. If this rate limit is exceeded, log messages of this action type are not logged until the threshold drops below the specified rate. You can pecify a **Rate Limit** value of **Indefinite**or **Specify**. • **Drop** Specifies, when enabled, that the system logs packets that match ACL rules configured with `action = Drop`. When enabled, you can specify a rate limit for all network firewall log messages with this action. If this rate limit is exceeded, log messages of this action type are not logged until the threshold drops below the specified rate. You can pecify a **Rate Limit** value of **Indefinite**or **Specify**.

Network Firewall Security - Network Firewall	Description
	• **Reject** Specifies, when enabled, that the system logs packets that match ACL rules configured with `action = Reject`. When enabled, you can specify a rate limit for all network firewall log messages with this action. If this rate limit is exceeded, log messages of this action type are not logged until the threshold drops below the specified rate. You can pecify a **Rate Limit** value of **Indefinite**or **Specify**.
Log IP Errors	Specifies, when enabled, that the system logs IP error packets. When enabled, you can specify a rate limit for all network firewall log messages of this type. If this rate limit is exceeded, log messages of this type are not logged until the threshold drops below the specified rate. You can select a **Rate Limit** value of **Indefinite**, which means the rate limit is set to the maximum of 4294967295, or you can select **Specify** and specify an integer between 0 and 4294967295 that represents the number of messages per second.
Log TCP Errors	Specifies, when enabled, that the system logs TCP error packets. If this rate limit is exceeded, log messages of this type are not logged until the threshold drops below the specified rate. You can select a **Rate Limit** value of **Indefinite** which means the rate limit is set to the maximum of 4294967295, or you can select **Specify** and specify an integer between 0 and 4294967295 that represents the number of messages per second.
Log TCP Events	Specifies, when enabled, that the system logs TCP events (open and close of TCP sessions). If this rate limit is exceeded, log messages of this type are not logged until the threshold drops below the specified rate. You can select a **Rate Limit** value of **Indefinite** which means the rate limit is set to the maximum of 4294967295, or you can select **Specify** and specify an integer between 0 and 4294967295 that represents the number of messages per second.
Log Translation Fields	Specifies, when enabled, that translation values are logged if and when a network firewall event is logged.
Always Log Region	Specifies, when enabled, that the geographic location should be logged when a geolocation event causes a network firewall event.

Storage Format	Specifies the format type for log messages. You can configure the following options:
	• **None** Specifies that the system uses the default format type to log the messages to a Remote Syslog server. This is the default setting.
	• **Field-List** Specifies that the system uses a set of fields, set in a specific order, to log messages. When **Field-List** is selected, specify the field list as follows.
	  • Specify the delimiter string in the **Delimiter** field. The default delimiter is the comma character (,).
	  Note: *You may not use the* ***$*** *character because it reserved for internal usage.*
	  • Select the fields to use. Unused fields are in the **Available** list, selected fields are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.
	• **User-Defined** Specifies that the format the system uses to log messages is in the form of a user-defined string. Select the items for the server to log. Unused

Network Firewall Security - Network Firewall	Description
	items are in the **Available** list, selected items are in the **Selected** list. Use the Move arrow buttons to transfer the selected items between the lists.

In the Network Firewall Security IP Intelligence section, you configure where IP intelligence events are logged. If the IP intelligence feature is enabled and licensed, you can configure the system to log source IP addresses that match an IP intelligence blacklist or whitelist category, as determined by the database of preconfigured categories, or as determined from an IP intelligence feed list.

Network Firewall Security - IP Intelligence	Description
Publisher	Specifies the name of the log publisher used for logging IP address intelligence events. Select a log publisher configured in your system.
Aggregate Rate Limit	Defines a rate limit for all combined IP intelligence log messages per second. Beyond this rate limit, log messages are not logged until the threshold drops below the specified rate. You can select a **Rate Limit** value of **Indefinite** which means the rate limit is set to the maximum of 4294967295, or you can select **Specify** and specify an integer between 0 and 4294967295 that represents the number of messages per second.
Log Translation Fields	Specifies, when enabled, that translation values are logged if and when a network firewall event is logged.

In the Network Firewall Security Traffic Statistics section, you configure logging of traffic statistics.

Network Firewall Security - Traffic Statistics	Description
Publisher	Specifies the name of the log publisher used for logging traffic statistics. Select a log publisher configured in your system.
Log Timer Events	• **Active Flows** - When enabled, logs the number of active flows each second. • **Reaped Flows** - When enabled, logs the number of reaped flows, or connections that are not established because of system resource usage levels. • **Missed Flows** - When enabled, logs the number of packets that were dropped because of a flow table miss. A *flow table miss* occurs when a TCP non-SYN packet does not match an existing flow. • **SYN Cookie (Per Session Challenge)** - When enabled, logs the number of SYN cookie challenges generated each second. • **SYN Cookie (White-listed Clients)** - When enabled, logs the number of whitelisted SYN cookie clients each second.

In the DoS Protection sections, you configure where DoS events are logged.

DoS Protection - DoS Application Protection	Description
Local Publisher	Specifies, when enabled, that the system logs DoS events to the local database.
Remote Publisher	Specifies the name of the log publisher used for logging DoS events. Select a log publisher configured in your system.

DoS Protection - DNS DoS Protection	Description
Publisher	Specifies the name of the log publisher used for logging DNS DoS events. Select a log publisher configured in your system.

DoS Protection - SIP DoS Protection	Description
Publisher	Specifies the name of the log publisher used for logging SIP DoS events. Select a log publisher configured in your system.

DoS Protection - Network DoS Protection	Description
Publisher	Specifies the name of the log publisher used for logging Network DoS events. Select a log publisher configured in your system.

6. Click **Save** to save your changes.
7. When you are finished, click **Save and Close** to save your changes, clear the lock, and exit the panel.

Chapter 17

Managing Firewall Policies in BIG-IQ Network Security

About firewall policies in BIG-IQ Network Security

A *firewall policy* is a set of rules and/or rule lists. BIG-IP® network firewalls use policies to specify traffic-handling actions and to define the parameters for filtering network traffic. You can assign inline rules, rule lists, or a policy to a firewall. Policies facilitate the assigning of a common collection of rules consistently across multiple firewalls.

The network software compares IP packets to the criteria specified in policies. If a packet matches the criteria, then the system takes the action specified by the policy. If a packet does not match any rule in the policy, the software accepts the packet or passes it to the next policy, rule, or rule list.

In BIG-IQ® Network Security, the Policies list displays the policies available for assignment to firewalls.

You can configure firewall policies as enforced or staged:

- An *enforced* policy refers to a policy whose actions are executed. Actions include: accept, accept decisively, drop, and reject.

  You are restricted to assigning a single, enforced policy on any specific firewall. If you have an enforced policy on a firewall, you cannot also have inline rules and rule lists on that firewall.
- A *staged* policy refers to a policy that is evaluated but policy actions are not enforced. All activity is logged.

  You are restricted to assigning a single, staged policy on any specific firewall. You can have inline rules and rule lists assigned to a firewall (in the enforced area) and have a configured staged policy on that firewall. You cannot have inline rules/rule lists in the staged area.

Thus, you can stage a firewall policy first and then examine logs to determine how the policy has affected traffic. Then you can determine the timing for turning the policy from staged to enforced.

Firewall policies can contain any combination of rules and rule lists. Policies cannot contain other policies. You can re-order rules within a policy.

Note: *The BIG-IQ® Network Security system is aware of functionality implemented in one BIG-IP version but not in another. In terms of firewall policies, this means that you are prohibited from dropping a policy onto a firewall on a BIG-IP device that does not have the software version required to support it.*

Filtering policies

To filter the system interface to display only those objects related to a selected policy, hover over the policy name, right-click and then click **Filter 'related to'**. The interface is filtered and a count appears to the right of each object type. The frame to the right provides its own filter field where you can enter text and click on the filter icon to constrain the display to those items that match the filter.

Adding firewall policies

To fine tune your network firewalls, you can configure policies and assign them to firewalls using the Policies screen Rules & Rule Lists settings.

1. In the screen header, below Network Security, click **Object Editor**.
2. On the left, hover over **Policies** and click the + icon to open the New Policy screen.
3. Click **Properties** and complete the properties fields as required.

   All boxes outlined in gold are required fields.

Option	Description
Name	User-provided name for the policy. This field is editable when creating or cloning a policy, and read-only when editing a policy.
Description	Optional description for the policy.
Partition	Although it is pre-populated with `Common` (default), you can set the partition when creating or cloning policies by typing a unique partition name. ***Note:*** *The partition with that name must already exist on the BIG-IP device.* No whitespace is allowed in the partition name. No editing of the partition is allowed.

4. Click **Rules & Rule Lists**, and then click either:
   - **Create Rule** to createg rules.
   - **Add Rule List** to add rule lists.
5. When finished, click **Add**.

A new policy is added under Policies in the left pane, in the correct order alphabetically.

You can drag-and-drop a policy to add it to a firewall. To configure the same policy consistently across many firewalls, drag-and-drop the policy to multiple firewalls.

Managing firewall policies

To fine tune your network firewalls, you can edit policies, create/edit rules, and add rule lists. You can also reorder rules in firewall policies. You cannot edit rule lists or reorder rules within rule lists.

1. In the screen header, below Network Security, click **Object Editor**.
2. Expand **Policies**.
3. Click the policy you want to edit.
4. Click **Edit** to lock the policy while you work on it.
5. Select **Properties**.
   The only editable field is the (optional) description.
6. Click **Rules & Rule Lists**, and edit the existing rule list or click either:
   - **Create Rule** to add rules.
   - **Add Rule List** to add rule lists.
7. Click **Save** to save your changes.
8. When you are finished, click **Save and Close** to save your edits, clear the lock, and exit.

The edited firewall policy appears under **Policies** in the left pane, in the correct order alphabetically.

You can then drag-and-drop a policy to add it to a firewall. To configure the same policy consistently across many firewalls, drag-and-drop the policy to multiple firewalls.

Cloning firewall policies

Cloning creates an exact copy with a different name. It enables you to quickly and easily create policies tailored to address any unique aspects of your network firewall environment. When you clone a firewall policy, you create an exact copy of the policy which you can then edit to address any special considerations.

Users with the roles of Network_Security_View or Network_Security_Deploy cannot clone policies.

1. In the screen header, below Network Security, click **Object Editor**.
2. Expand **Policies**.
3. Click the policy you want to clone.
4. Click **Clone**.
5. Click **Properties** and complete the properties fields as required.

   All boxes outlined in gold are required fields.

Option	Description
Name	User-provided name for the policy. This field is editable when creating or cloning a policy, and read-only when editing a policy.
Description	Optional description for the policy.
Partition	Although it is pre-populated with `Common` (default), you can set the partition when creating or cloning policies by typing a unique partition name. ***Note:*** *The partition with that name must already exist on the BIG-IP device.* No whitespace is allowed in the partition name. No editing of the partition is allowed.

6. Click **Rules & Rule Lists**, and then click either:
   - **Create Rule** to createg rules.
   - **Add Rule List** to add rule lists.
7. When finished, click **Add**. If you then click **Cancel**, the policy is not cloned.

The cloned policy appears in Policies in the correct order alphabetically. In an HA configuration, the cloned policy appears on the standby BIG-IQ® system as soon as it is saved.

Reordering rules in firewall policies

Using the Policies screen, you can reorder rules in firewall policies to optimize your network firewall policies. You cannot edit rule lists or reorder rules inside rule lists.

1. In the screen header, below Network Security, click **Object Editor**.
2. Click the policy you want to edit.
3. Click **Edit** to lock the policy while you work on it.
4. Click **Rules & Rule Lists**.
5. To reorder rule lists or rules, simply drag-and-drop them until they are in the correct order.

   You can also right-click a rule name and select among the ordering options.
6. Click **Save** to save your changes.
7. When you are finished, click **Save and Close** to save your edits, clear the lock, and exit.

Removing firewall policies

You can remove firewall policies to keep network firewalls up-to-date.

If a firewall policy is in use or if any objects inside that policy are in use, you cannot remove it.

To see where a policy is used, click the policy and the name appears in the Filter field. Then, click **Apply**. The system interface filters on that policy name and displays only the instances where the policy is used.

1. In the screen header, below Network Security, click **Object Editor**.
2. Click the policy you want to remove.
3. Click **Remove** and then confirm the permanent removal in the popup dialog box.

The policy is permanently removed and the panel is closed.

About managing firewall policies using snapshots

It is possible to introduce errors during the editing of the working-configuration set. In some cases, you might not detect these errors immediately. When you discover these errors, you might want to roll back to a previous state as quickly as possible to restore service. Then, you can triage to discover the root causes of any errors.

In one scenario, you might perform multiple emergency deployments in an attempt to fix a problem. If such attempts did not fix the issue, you might want to roll back to the most stable state prior to where you first saw the problem.

In another scenario, you might want to roll back after importing a device. For example, an administrator might import a device and as part of the import process, decide to overwrite the objects stored in the BIG-IQ® database. Subsequently, the administrator decides that the import was a mistake and wants to roll back to the state of the objects before the import.

You can address all of these scenarios by restoring from a snapshot.

BIG-IQ Network Security provides the ability to create snapshots in these ways:

- During discovery, BIG-IQ Network Security takes a snapshot of the working-configuration set on the device. This is the default behavior (retain the check box selection).
- During a restore operation, you can take a snapshot of the working-configuration set on the device before the restore. This is the default behavior (retain the check box selection).
- During deployment, BIG-IQ Network Security takes a snapshot when you click **Evaluate**.
- At any time, you can create a user-defined snapshot from the Add Snapshot panel.

Chapter

18

Managing Snapshots in BIG-IQ Web Application Security

About snapshots

BIG-IQ® Web Application Security uses snapshots to protect the working-configuration set of the Web Application Security module. A best practice is to take a snapshot before every major configuration change.

The Snapshots panel displays a list of snapshots.

You can create a snapshot when you create a new deployment, or as needed. If the snapshot is created as part of a deployment, the BIG-IQ system prefixes the name of the deployment with the word `Deploy`.

To abandon an operation and close the panel without saving your changes, click **Cancel**.

To get help on any panel, click the **?** icon in the upper right corner of the interface.

Adding snapshots

It is a best practice to create a snapshot before any configuration changes, so that you can run a snapshot comparison later and verify the changes then.

Hover over the header of the Snapshots panel, and when the **(+)** icon appears, click it to open the screen, then specify a name and description for the new snapshot.

Click **Create** to create the snapshot.

Managing snapshots

Hover over a snapshot name in the panel, and when the gear icon appears, click **Show Properties**. You can now:

- View details about the snapshot.
- Click **Remove** to remove the snapshot.
- Click **Restore** to restore the snapshot.
- Compare the snapshot with the working configuration or another snapshot, and view the differences.

Displaying snapshot details

To display the details of a specific snapshot, hover over the snapshot name in the list of snapshots, and when the gear icon appears, click **Show Properties** to display the properties for that snapshot.

Comparing a snapshot with the working configuration or another snapshot

You can compare a snapshot with the working configuration or with another snapshot, and view the differences in JSON on an object-by-object basis. To compare a snapshot:

1. Hover over a snapshot name in the panel, and when the gear icon appears, click **Show Properties**.
2. Using the **Compare Against** settings, select what should be compared to the snapshot.
   - Select **Working Config** to compare the snapshot to the current working configuration.
   - Select **Snapshot** to compare the snapshot to another snapshot. Select the comparison snapshot from the list that is displayed.
3. Select how to compare the snapshot.
   - To see the ASM™ differences, click **View** for the **ASM Differences** setting.
   - To see the shared security differences, click **View** for the **Shared Differences** setting.

Chapter

19

Managing Security Policies in BIG-IQ Web Application

About security policies in BIG-IQ Web Application Security

BIG-IQ® Web Application Security imports ASM™ security policies from discovered BIG-IP® devices and lists them in the Policies panel. Each security policy is assigned a unique identifier that it carries across the enterprise. This ensures that each policy is shown only once in the Policies panel, no matter how many devices it is attached to.

In the BIG-IQ Web Application Security repository, policies are in XML format.

Displaying and modifying security policy properties

Security policies are often created on BIG-IP devices and come into the BIG-IQ® Web Application Security configuration when you discover the devices. You can view and modify the properties of individual security policies.

1. In **Web Application Security** > **Overview**, navigate to the Policies panel.
2. Hover over the name of a policy you want to edit, and click the gear icon.

   You enter the Policy Editor interface, with the select policy loaded into the editor.
3. Edit the properties of each policy object as needed. Click the object to edit in the Policy objects list, and click the **Edit** button on the right side of the panel.

   For the Signatures List object only, click the Signatures List object, then click the signature name to edit in the Name column and click **Edit**.

   Each of these policy objects can be edited individually:

   - Properties
   - Response Page
   - Data Guard
   - IP Address
   - File Types
   - Parameters
   - Character Sets
   - Attack Signatures
   - Signatures List
4. Click **Save** to save the modifications to each object.

The policy object is now edited in the working-config of the BIG-IQ system. Assuming the policy is assigned to a virtual server, the next deploy task sends the new configuration to one or more BIG-IP devices.

Adding security policies

You can use BIG-IQ® Web Application Security to add new security policies for possible later deployment.

1. Hover over the Policies panel until the **(+)** icon appears, and click it.

   The Policy Editor opens, showing required fields outlined in red.

2. Specify the following information about the new Web Application Security policy:

Option	Description
Name	Any descriptive name for the new policy.
Partition	An administrative partition for storing this policy on the BIG-IP device. In most cases, the default (`Common`) is the best choice.
Description	Any description you choose for the policy.

   Specify any remaining fields as needed on the Properties screen. Other options are not accessible until you save these initial properties.

3. Click **Save** when you are finished editing the properties.
   This makes the other policy objects available for editing.
4. In the Policy objects list on the left, click the object to edit, and then click the **Edit** button.

   For the **Signatures List** object only, click the **Signatures List** object, then in the Name column, click the signature name you want to edit, then click **Edit**.

   The policy objects that can be edited include the following:

   - Properties
   - Response Page
   - Data Guard
   - IP Address
   - File Types
   - Parameters
   - Character Sets
   - Attack Signatures
   - Signatures List

5. Click **Save** to save the modifications to each policy object before moving to another one.

The new policy object now exists in the working configuration of the BIG-IQ system. Now you can add it to any virtual server object in Web Application Security.

Importing security policies

You can use BIG-IQ® Web Application Security to import security policies.

1. Navigate to the Policies panel.
2. Hover over the Policies header and when the import icon appears, click it.
3. In the Import Policy File dialog box, select the security policy file by clicking **Choose File** and navigating to the file location, or you can drag-and-drop a file to the Drag and Drop File Here list.

   You can drag-and-drop a policy file onto the Source File area to view the content of the XML file.
4. Click **upload**.

After import, the policy is listed in the Policies panel. The uploaded policy will have the same name as the XML file.

Exporting security policies

You can use BIG-IQ® Web Application Security to export security policies (download the policy XML file) from the module.

1. Navigate to the Policies panel.
2. Hover over the name of the security policy you want to export, and hover over the gear icon to display the screen containing properties and actions.
3. Click **Export Policy** on the screen.

Displaying items related to security policies

You can use BIG-IQ® Web Application Security to display items related to a security policy.

1. Navigate to the Policies panel.
2. Hover over the name of the security policy and when the gear icon appears, hover over the gear and select **Show Related Items** from the menu.

Removing security policies

BIG-IQ® Web Application Security provides a way to remove ASM™ security policies from the BIG-IQ database.

1. Navigate to the Policies panel.
2. Hover over the name of the policy you want to remove, and when the gear icon displays, hover over it and click **Delete Policy.**
3. Click **Remove** in the Remove Policy dialog box..

The scurity policy is removed from the BIG-IQ system, and can be managed locally.

Chapter 20

Managing Objects

About objects in BIG-IQ Network Security

In BIG-IQ® Network Security, the objects that you can view and manage include:

Contexts (firewall)
Category of object to which a rule applies. In this case, category refers to Global, Route Domain, Virtual Server, Self IP, or Management. Within each context, rules can be viewed and reorganized separately. It is possible to have multiple layers of firewalls on a single BIG-IP® device. These layers constitute the firewall hierarchy. Within the firewall hierarchy, rules progress from Global, to Route Domain, and then to either Virtual Server or Self IP.

Policies (firewall)
Set of rules and/or rule lists that specify traffic-handling actions and define the parameters for filtering network traffic. You can assign inline rules, rule lists, or a policy to a firewall. Policies facilitate the assigning of a common collection of rules consistently across multiple firewalls.

Rule lists
Containers for rules; rules are run in the order they appear in their assigned rule list. A rule list can contain thousands of ordered rules, but cannot be nested inside another rule list.

Address lists
Collections of IPv4 or IPv6 addresses, address ranges, and subnets. These collections are saved on a server and used by policies, rule lists, and rules to allow or deny access to specific IP addresses in IP packets. Firewall rules compare all addresses or address ranges in a given address list to either the source or the destination IP address, depending on how the list is applied. If there is a match, the rule takes an action, such as accepting or dropping the packet.

Port lists
Collections of ports and port ranges. These collections are saved on a server and used by policies, rule lists, and rules to allow or deny access to specific IP addresses in IP packets. As with address lists, firewall rules compare all ports and port ranges in a given port list to either the source or the destination port, depending on how the list is applied. If there is a match, the rule takes an action, such as accepting or dropping the packet.

Schedules
Schedules are assigned to firewall rules, rule lists, and policies to control when rules, rule lists, and policies are active on the firewall. In the Shared Objects panel, you can hover over schedule names to see the name displayed in a tooltip. This feature is useful if the schedule name is longer than the panel.

About the policy editor in BIG-IQ Network Security

BIG-IQ® Network Security provides users with an editor that enables the ability to respond rapidly to firewall configuration change requests. The Policy Editor optimizes the use of screen real estate for firewall rule editing workflows. Information is presented on the screen so that relevant objects are more readily available for rule editing workflows.

Adding new objects

Hover over the header of the object you want to add (Policies, Rule Lists, Address Lists, Port Lists, or Schedules) and when the + icon appears, click it to open a frame for adding the object.

Viewing and editing objects

To view and/or edit objects:

1. Click the object type to expand it and display the list of individual objects.
2. Click the name of the object you want to view or edit. The object details are then displayed in the frame to the right. Help for that object type is then available by clicking the **?** in the upper right corner. The help includes instructions for cloning, editing, and removing the object.

Filtering in the Objects panel

You can filter the contents of panels within the Policy Editor frame to reduce the set of data that is visible in the system interface. Filtering techniques can be important for troubleshooting.

1. In the filter text field (under Objects), type the text you want to filter on and press **Enter**.

   Filtering works by performing a wildcard search of the underlying JSON, not just the name of the object. For example, if you type a `1` (the number one) in the filter, the system will display any object with a `1` in its JSON.

   You can clear the filter field by clicking the **X** to the right of the text under the filter field.

Objects are filtered on the text entered and a count for each appears to the right of each object type.

Adding objects

BIG-IQ® Network Security enables you to add objects. **Policy Editor** > **Contexts/Policies/Rule Lists/Address Lists/Port Lists/Schedules**

Note: *Address lists and port lists are containers and must contain at least one entry. You cannot create an empty list; you cannot remove an entry in a list if it is the only entry.*

---

1. Hover over the object type that you want to add and click the + icon.
2. In the opened screen, populate the property fields as required.
   - All fields that are outlined in gold are required.
   - The **Partition** field is outlined in gold, and although it is pre-populated with `Common`, it is an editable field.
   - You can press Tab to advance from field to field.
3. When you are finished, click **Add**.

Editing objects

BIG-IQ® Network Security enables you to select objects for deeper inspection or edit.

Note: *Address lists and port lists are containers, and must contain at least one entry. You cannot create an empty list; you cannot remove an entry in a list if it is the only entry.*

---

1. Navigate to the object you want to edit. **Object Editor** > **Contexts/Policies/Rule Lists/Address Lists/Port Lists/Schedules**
2. Click the object that you want to edit.
3. In the resulting screen, click **Edit** to lock the object.
4. Edit the properties and other areas as required.

You can use the keyboard Tab to advance from field to field.

5. When you are finished, click **Save** to save your edits, or click **Save and Close** to save and release the lock.

Filtering the Policy Editor frame

You can filter the contents of panels within the Policy Editor frame to reduce the set of data that is visible in the system interface. Filtering techniques can be important for troubleshooting.

1. To filter the contents of the Policy Editor frame, log in to BIG-IQ® Security.
2. Navigate to **Network Security** > **Policy Editor**.
3. In the filter text field, type the text you want to filter on and press **Return**.

   Filtering works by performing a wildcard search of the underlying JSON, not just the name of the object. For example, if you type a `1` (the number one) in the filter, the system will display any object with a `1` in its JSON.

   You can clear the filter field by clicking the **X** to the right of the filter field.

Objects are filtered on the text entered and a count for each appears to the right of each object type.

Adding objects to firewall contexts and rules

BIG-IQ® Network Security enables you to add objects to firewall contexts and rules (used in rule lists and policies).

1. Navigate to the context or rule to which you want to add an object. **Object Editor** > **Contexts/Rule Lists**
2. Click **Edit** to lock the object for editing.
   - If you are editing a firewall, be sure to select **Enforced** so that Enforced Firewall Rules are visible.
   - If you are editing a rule or rule list, be sure to select **Rules**.
3. Click the section name to expand the section so the name of the object is visible.
4. Select the object you want to add, and drag it onto the firewall or rule in the appropriate column.

   If you are adding a schedule, drag it onto the State column.
5. When you are finished, click **Save** to save your edits, or click **Save and Close** to save and release the lock.

About the toolbox in BIG-IQ Network Security

BIG-IQ® Network Security provides users with a toolbox that can be used to quickly add objects. The toolbox is located in the bottom half of the Policy Editor frame.

Adding new objects

To add an object quickly, select the object type from the dropdown list and click **Add**. Fill in the properties that appear in the popup box and click **Add**.

Filtering in the toolbox

You can filter the contents of panels within the Policy Editor frame to reduce the set of data that is visible in the system interface. Filtering techniques can be important for troubleshooting.

1. In the filter text field, type the text you want to filter on and click the filter icon.

   Filtering works by performing a wildcard search of the underlying JSON, not just the name of the object. For example, if you type a `1` (the number one) in the filter, the system will display any object with a `1` in its JSON.

   You can clear the filter field by clicking the red **X** to the left of the filter field.

Filtering the Policy Editor toolbox frame

You can filter the contents of the toolbox (the bottom frame within the Policy Editor frame) to reduce the set of objects visible in the system interface. Filtering techniques can be important for troubleshooting.

1. To filter the contents of the toolbox, log in to BIG-IQ® Security.
2. Navigate to **Network Security** > **Policy Editor** > **Toolbox at the bottom of the right frame**.

   The filter appears to the right of the **Show** dropdown list.
3. In the filter text field, type the text you want to filter on and click the filter icon.

   Filtering works by performing a wildcard search of the underlying JSON, not just the name of the object. For example, if you type a `1` (the number one) in the filter, the system will display any object with a `1` in its JSON.

   You can clear the filter by clicking the **X** to the left of the filter field.

Renaming objects

BIG-IQ® Network Security does not support renaming an object.

As an alternative to renaming it, you can create a new object and replace the original object where it is in use.

1. Create the new object. Consider cloning the object as the fastest and most reliable way to create a new object with the same content as the original but a new name.
2. Locate every instance of the original object by hovering over the object, right-clicking, and selecting **Filter Related To**.
   A count is added, indicating the number of times the object is used.
3. Navigate to each instance where the original object is in use, and replace it with a reference to the newly-created object.
4. Remove the original object.

   Clear the filter by clicking the **X** at the top of the panel under the filter entry box.

Note: *Note that you cannot remove an object that is still in use.*

Cloning objects

BIG-IQ® Network Security enables you to clone objects to create an object that is slightly different from the original. You may have an object that serves as a template. You can clone that object, edit it, and then use it in different contexts.

1. Navigate to the type of object you want to clone. **Object Editor** > **Contexts/Policies/Rule Lists/Address Lists/Port Lists/Schedules**
2. Click the object that you want to clone.
3. In the expanded screen, click **Clone**.
   The system displays a copy of the object with blank **Name** and **Description** fields.
4. In the opened screen, populate the property fields as required.
   - All fields that are outlined in gold are required.
   - The **Partition** field is outlined in gold, and although it is pre-populated with `Common`, it is an editable field.
   - You can press Tab to advance from field to field.
5. When you are finished, click **Add**.

The cloned object is added to the existing list in the appropriate section.

Removing objects

From the BIG-IQ® Network Security Shared Objects expanded panels, you can remove shared objects.

1. Navigate to the object you want to remove, hover over it, and then click the gear icon.
2. In the object property screen, click **Remove**.
   A popup information screen opens.
3. Respond to the popup screen prompt:
   - If the object is being used by another object, policy, rule, or rule list, you cannot remove objects that are in use; click **OK** to acknowledge this message.
   - If the object can be removed, click **OK** to confirm the removal.

About address lists

Address lists are collections of IPv4 or IPv6 addresses, address ranges, nested address lists, or subnets saved on a server and available for use in firewall rules, rule lists, and policies.

Firewall rules refer to address lists to allow or deny access to specific IP addresses in IP packets. Firewall rules compare all addresses from the list to either the source or the destination IP address (in IP packets), depending on how the list is applied. If there is a match, the rule takes an action, such as accepting or dropping the packet.

Where address lists are visible in the screens for Firewall Contexts, Policies, and Rule Lists, you can hover over nested address lists to see the first-level content displayed in a tooltip. The content (addresses, ranges, and nested address lists) is displayed whether or not the address list is locked for editing.

If a policy, rule list, or rule is locked for editing, you can right-click an address, address range, or address list in the locked object and remove that address, address range, or address list.

To view address list names that are longer than the display field, hover over the name to see the full name displayed in the tooltip.

Note: *Before nesting an address list inside an address list, check to be sure this option is supported on the BIG-IP® device.*

You can add geolocation awareness to address lists, which enables you to specify source or destination IP addresses by geographic location. Thus, you can specify firewall behavior for traffic to/from entire geographic regions by defining rules based on where the source or destination system is, rather than on its IP address (source or destination). BIG-IQ® Network Security supports specifying geolocation in rules and address lists. The geolocation is validated when the rule or address list is saved.

Note: *If you use a geolocation spec that is valid on the BIG-IQ Network Security system, but not supported on a particular BIG-IP® device because the device has a different geolocation database, it causes a deployment failure for that device. Importing a BIG-IP device with an invalid geolocation spec causes a discovery failure for that device.*

Adding address types to address lists

BIG-IQ® Network Security enables you to add addresses, address ranges, nested address lists, or geolocation to an existing address list.

1. Navigate to the Address Lists area. **Object Editor** > **Address Lists**
2. Click **Address Lists** to expand the section, and then click the address list that you want to edit.
3. In the resulting screen, click **Edit** to lock the object.
4. Click the + icon to the right of an address.
   A new row is added to the Addresses table under that row.
5. From the list under the Type column, select **Address**, **Address Range**, **Address List**, or **Country/Region**.
   - If you select **Address List**, in the **Addresses** field, type the first letter of an existing address list. A list of existing address lists appears from which you can select an address.
   - If you select **Country/Region** and then select a country from the second list, the next list automatically updates with all available regions for that country.
6. When you are finished, click **Save** to save your edits, or click **Save and Close** to save and release the lock.

Removing entries from address lists

BIG-IQ® Network Security enables you to remove entries from address lists.

1. Navigate to the Address Lists area. **Object Editor** > **Address Lists**
2. Click **Address Lists** to expand the section, and then click the address list that you want to edit.
3. In the resulting screen, click **Edit** to lock the object.
4. Click the **X** icon to the right of the address, address range, address list, or geolocation spec that you want to remove.
5. When you are finished, click **Save** to save your edits, or click **Save and Close** to save and release the lock.

Address list properties and addresses

Property	Description
Name	Unique, user-provided name for the address list. The text field accepts up to and including 255 characters, including the partition name.
Description	Optional description of the address list.
Partition	Field pre-populated with `Common` (the default). This field is editable when creating or cloning address lists.
Type	After locking the address list for editing, select one of the following: • **Address**. Then, type the address in the **Addresses** field. You can also enter an address range in this field by typing a range in the format: `n.n.n.n-n.n.n.n`. • **Address range**. The **Addresses** field becomes two fields separated by "to." Type the beginning address and ending addresses in these fields as appropriate. • **Address list**. When you type the first letter of a saved list, the **Addresses** field populates with a picker list that displays saved address lists. You then select from the list. • **Country/Region**. From the first **Addresses** list, select a country. Once you select a country, the second list automatically updates with all available regions for that country. Optionally, select a region from the second list. The wildcard, Unknown, is supported. Note that geolocation is not supported on the management IP context.
Addresses	IPv4 or IPv6 address, address range, or nested address list. There are many ways an IPv4 or IPv6 address or address range can be constructed. The following methods and examples are not meant to be exhaustive. • IPv4 format: *a.b.c.d*[/*prefix*]. For example: `60.63.10.10`. • IPv6 format: *a*:*b*:*c*:*d*:*e*:*f*:*g*:*h*[/*prefix*]. For example: `2001:db7:3f4a:9dd:ca90:ff00:42:8329`. • IPv6 abbreviated form is supported. You can shorten IPv6 addresses as defined in RFC 4291. • You can specify subnets using forward slash (/) notation; for example: `60.63.10.0/24`. Example IPv6 subnet: `2001:db8:a::/64`. • You can append a route domain to an address using the format %RouteDomainID/Mask. For example: `12.2.0.0%44/16`.
Description	Optional text field used to describe the address, address range, or nested address list.

About port lists

Port lists are collections of ports, port ranges, or port lists saved on a server and available for use in firewall rules, rule lists, and policies.

Firewall rules refer to port lists to allow or deny access to specific ports in IP packets. They compare a packet's source port and/or destination port with the ports in a port list. If there is a match, the rule takes an action, such as accepting or dropping the packet.

Port lists are containers and must contain at least one entry. You cannot create an empty port list; you cannot remove an entry in a port list if it is the only one.

Where port lists are visible in the screens for Firewall Contexts, Policies, and Rule Lists, you can hover over port lists to see the first-level content displayed in a tooltip. The content is displayed whether or not the port list is locked for editing.

If a policy, rule list, or rule is locked for editing, you can right-click a port, port range, or port list in the locked object and remove that port, port range, or port list.

To view port list names that are longer than the display field, hover over the name to see the full name displayed in the tooltip.

Note: *Before nesting a port list inside a port list, check to be sure this option is supported on your BIG-IP® device.*

Adding port types to port lists

BIG-IQ® Network Security enables you to add ports, port ranges, or nested port lists to an existing address list.

1. Navigate to the Port Lists area. **Object Editor** > **Port Lists**
2. Click **Port Lists** to expand the section, and then click the port list that you want to edit.
3. In the resulting screen, click **Edit** to lock the object.
4. Click the + icon to the right of a port.
   A new row is added to the Ports table under that row.
5. From the **Type** list, select **Port**, **Port Range**, or **Port List**.
   If you select **Port List**, and type the first letter of an existing port list in the **Ports** field, a list of existing port lists appears from which you can select a port list from the list.
6. When you are finished, click **Save** to save your edits, or click **Save and Close** to save and release the lock.

Removing entries from port lists

BIG-IQ® Network Security enables you to remove entries from port lists.

1. Navigate to the port list that you want to remove an entry from. **Object Editor** > **Port Lists**
2. Click **Port Lists** to expand the section, and then click the port list that you want to edit.
3. In the resulting screen, click **Edit** to lock the object.
4. Click the **X** icon to the right of the port, port range, or port list that you want to remove.
5. When you are finished, click **Save** to save your edits, or click **Save and Close** to save and release the lock.

Port list properties and ports

Property	Description
Name	Unique name used to identify the port list.
Description	Optional description for the port list.
Partition	Field pre-populated with `Common` (the default). This field is editable when creating or cloning port lists.

Property	Description
Type	After locking the port list for editing, select one of the following: • **Port**. Then, enter the port in the **Ports** field. You can also enter a port range in this field by entering a range in the format: n-n. Valid port numbers are 1-65535. • **Port range**. The **Ports** field becomes two fields separated by "to." Type the beginning port and ending port in these fields as appropriate. • **Port list**. When you type the first letter of a saved list, the **Ports** field is populated with a picker list that displays saved port lists. You then select from the list.
Ports	Port, port range, or port list. Valid port numbers are 1-65535.
Description	Optional text field used to describe the port, port range, or nested port list.

About schedules

Schedules are assigned to rules, rule lists, and policies to control when these shared objects are actively evaluated.

By default, all rules, rule lists, and policies are on a continuously active schedule. Schedules are *continuously active* if they are created without any scheduling specifics (such as the hour that the schedule starts). If you apply a schedule to a rule, rule list, or policy, you can reduce the time that the rule, rule list, or policy is active.

Schedule properties

Property	Description
Name	Unique name used to identify the schedule.
Description	Optional description for the schedule.
Partition	Informational, read-only field displaying the name of the partition associated with the schedule.
Date Range	Click the first field to display a calendar popup screen and select a start date. Click the second field to display a calendar and select an end date. You can specify: **Start date and no end date** The equivalent on the BIG-IP® system is **After**, which specifies that the schedule starts after the specified date and runs indefinitely. The schedule is activated starting on the selected date, and runs until you change the start date or delete the schedule. Click in the field to choose a start date from a popup calendar. You can specify a start time in the same popup screen. **End date and no start date** The equivalent on the BIG-IP system is **Until**, which specifies that the schedule starts immediately and runs until a specified end date. The schedule is immediately activated and not disabled until the end date is reached. Click in the field to choose an end date from a popup calendar. You can specify an end time in the same popup screen.

Property	Description
	Both a start date and an end date The equivalent on the BIG-IP system is **Between**, which specifies that the schedule starts on the specified date and runs until the specified end date. Click in the fields to choose the start and end dates from a popup calendar. You can specify start and end times in the same popup screen. **Neither a start date nor an end date** The equivalent on the BIG-IP system is **Indefinite**, which specifies that the schedule starts immediately and runs indefinitely. The schedule remains active until you change the date range or delete the schedule. ***Note:*** *Using the system interface and popup screens to specify the start and end dates and times is the preferred method. However, if you do specify dates manually, use the format: YYYY-MM-DD HH:MM:SS.*
Time Span	Time is specified in military time format: HH:MM. You can specify time manually or click in the fields and use the Choose Time popup screen. • Click the first time span field and use the sliders to specify a start time in the popup screen. • Click the second time span field and use the sliders to specify an end time in the popup screen. If you leave these fields blank, the schedule runs all day, which is the default on the BIG-IQ® Security system and on BIG-IP devices. (This option is explicitly called **All Day** on BIG-IP devices.)
Day	Select check boxes for all days that apply. You must select at least one day per week.

Chapter

21

Managing Snapshots in BIG-IQ Network Security

About snapshots

BIG-IQ® Security uses snapshots to protect the working-configuration set of the Security module. Thus, at any time, you can back up, restore, and deploy the BIG-IQ working configuration to a specific configuration state, or deploy a specific set of working configuration edits back to a BIG-IP® device. You can also compare one snapshot to another, or compare a snapshot to the BIG-IQ working configuration.

The Snapshots panel displays a list of imported snapshots. The system uses a naming convention that begins with `Import` and is followed by the self IP address or the management IP address, depending on how the device was discovered. You can also add snapshots through the **New Snapshot** panel and name the snapshot according to your own convention.

To display only those objects related to a specific snapshot, hover over the snapshot and when the **gear** icon appears, click it. Then, you can select **Properties** to display properties or **Show Only Related Objects** to filter by snapshot.

Adding snapshots

Add snapshots so that you can restore the BIG-IQ® working configuration to a specific configuration state, or deploy a specific set of working configuration edits back to a BIG-IP® device.

1. Navigate to Snapshots.
2. Hover in the Snapshots banner and click the + icon to display the New Snapshot screen.
3. Complete the property fields as required.

Option	Description
Name	Type a name for the snapshot.
Description	Type a description (optional) that will assist in remembering the reason for the snapshot.

After the process completes, the snapshot is listed in the Snapshots panel by its user-provided name, user account name, and the date and time the snapshot was taken.

Comparing snapshots

You can compare one snapshot to another, or to compare a snapshot to the BIG-IQ® Security working configuration.

1. Navigate to Snapshots.
2. Select a snapshot, and click the gear icon to expand and display the specific snapshot's screen.
3. Click **Compare**.
4. Indicate what you want to compare:
   - Select **Working Configuration** to compare the selected snapshot to the BIG-IQ Security working configuration.
   - Select **Snapshot** to compare the selected snapshot to a different snapshot.
5. To compare a snapshot with the selected snapshot:

a) Drag-and-drop that snapshot from the Snapshots panel to this area, or click the **Select Snapshot** link.
b) From the Select From Available Snapshots popup screen, select a snapshot and click **Select**.

6. Click **Evaluate** to start the comparison.
   The Differences popup screen opens.
7. To display the JSON for each difference found, click a row in the table.

   Textual JSON appears for each difference found; snapshot on the left and working configuration, or second snapshot on the right.

   Differences are listed by: name (name of the shared object), type (type of object), change (added, modified, deleted), and device (blank unless the type is **firewall**).

Restoring the working configuration from a snapshot

You can restore the working configuration using a selected snapshot as input. This process does not delete any shared objects that might have been added since the snapshot was taken.

1. Navigate to Snapshots.
2. Hover over the snapshot containing the configuration you want to restore to, click the gear icon, and then click **Properties**.
3. In the expanded screen, click **Restore**.

   You can also click the Compare tab to compare the selected snapshot against the working configuration or another snapshot before performing the restore.

   ### Working Configuration
   If you select **Working Configuration** and click **Evaluate**, a popup screen displays the differences in the JSON between the snapshot (at left in the table) and the working configuration (at right in the table). Click any row to view the JSON for the two objects. Differences are listed by: name (name of the shared object), type (type of object), change (added, modified, deleted), and device (blank unless the type is **firewall**). Click any row to view the JSON for the two objects.

   ### Snapshot
   If you select **Snapshot**, specify the snapshot selected by clicking **Select Snapshot** or by dragging-and-dropping a snapshot to the **Compare against** field. Then, click **Evaluate** to view the differences in the JSON between the two snapshots. Differences are listed by: name (name of the shared object), type (type of object), change (added, modified, deleted), and device (blank unless the type is **firewall**). Click any row to view the JSON for the two objects.
   When you are satisfied that you are restoring the correct configuration, click **Restore**.
4. In the popup screen, click **OK** to confirm that you want to continue.

   This popup screen explains that this operation will restore the BIG-IQ Security configuration with the contents of this snapshot and remove all active locks. Once the process starts, you will be blocked from performing any other tasks or interacting with the UI in any way until the process is completed or canceled. If the operation is canceled, all configuration settings are rolled back to their state before the restore started.

About snapshots in high-availability configurations

Snapshots require special consideration in high-availability (HA) configurations. For example, a scenario can occur where both peers think they are in the active state due to a disruption in communication or some other error condition.

If you take a snapshot when the system is in this condition, the snapshot Properties screen will display a message saying that the snapshot was taken when the peer device was unreachable.

When the peers are re-paired and re-synched, the snapshot will appear on both peers and both Properties screens will display the error message.

We recommend that you not attempt to restore such snapshots. The restore will likely fail and if it does not, the resulting configuration is unpredictable.

Chapter 22

Managing Signature Files

About signature files in BIG-IQ Web Application Security

The Signature files panel in BIG-IQ® Web Application Security lists the signature files for each discovered BIG-IP® device, and enables you to view the properties for these files.

Currently, administrators can manage signature files for one BIG-IP device from the BIG-IP Configuration Utility. BIG-IQ Web Application Security, however, provides central management for signature files and signature file updates for multiple devices.

Managing signatures from the BIG-IQ platform enables the administrator to spend less time on signature updates and to view the signatures update information in a single central location.

BIG-IQ Web Application Security fetches all new and relevant signature files automatically from an external server proxy configured from the system interface. It then pushes the signatures to the relevant BIG-IP device or to multiple BIG-IP devices. It displays the signature version for each device.

Note: *This feature is available to users with the Administrator role or the Security_Manager role.*

Viewing signature file properties

Use the BIG-IQ® Web Application Security Signature files panel to expand and view signature file properties.

1. Log in with administrator or Security_Manager credentials.
2. Navigate to the Signature files panel.
3. Hover over a specific signature file, and then click the gear icon to expand and display the panel containing property details.
4. When you are finished, click **Cancel**.

Signature file properties

Signature file properties are read-only and displayed for informational purposes only.

Property	Description
Name	Name of the signature file. Example: Sig_vanc_1
File version	Example: 20131103_042020
Product version	Version on the BIG-IP® device.

Updating signature files

You can use the BIG-IQ® Web Application Security Signature files panel to update signatures.

1. Log in with Administrator or Security_Manager credentials.
2. Navigate to the Signature files panel.

3. Hover over the panel header, and then click the gear icon to expand and display the Update settings.
4. Use the **Interval** list to modify settings for scheduling updates.
5. Edit the Current running task settings as needed. Click the **Update & push** button to update the signature files and push them to the server.
6. When finished, click **Save** to update all signatures (or **Cancel** to close the panel without saving your edits).

Updating and pushing signature files

You can use the BIG-IQ® Web Application Security Signature files panel to begin the process for updating and pushing the signature files.

1. Log in with Administrator or Security_Manager credentials.
2. Navigate to the Signature files panel.
3. Hover over the panel header, and then click the gear icon to expand and display the update settings.
4. Under Current running task, for the **Run now** setting, click the **Update & push** button.

The update process begins immediately.

Chapter 23

Managing Virtual Servers

About the Virtual Servers panel

Through the Virtual Servers panel, BIG-IQ® Web Application Security displays the virtual servers on each discovered BIG-IP® device, and enables you to view the properties for these virtual servers.

For each device discovered, the BIG-IQ system creates an extra virtual server to hold all security policies not related to any virtual server in the discovered device.

Displaying virtual server properties

With BIG-IQ® Web Application Security, you can easily view virtual server properties.

1. To display properties for an individual virtual server, hover over the name for that virtual server (in the Virtual Servers panel).
2. Click the gear icon to expand the panel and display the screen containing virtual server properties.

   Properties are read-only. The only actions you can take in the expanded screen concern the attached policies.

Option	Description
Name	Name of the virtual server.
Full Path	Path, including partition, to the virtual server.
IP Address	Self IP address of the BIG-IP® device.
Is Inactive Policies Holder	Yes/No.
Device	FQDN of the BIG-IP device.
Attached Policies	Remove/Change.

Virtual server properties

Virtual server properties are read-only and displayed for informational purposes only.

Property	Description
Name	Name of the virtual server.
Full Path	Full path, including partition, to the virtual server on the BIG-IP® device.
Description	Optional description of the virtual server.
IP Address	Self IP address of the BIG-IP device.
Is Inactive Policies Holder	Yes/No.
Device	FQDN of the BIG-IP device.
Attached Policies	Remove/Change/Add attached policies.

Changing security policy attachment to virtual servers

You can use the BIG-IQ® Web Application Security Virtual Server screen to add policies to a virtual server, or remove policies from the virtual server they are attached to. You can change the virtual server a given policy is attached to.

Note: *You can add to, but not remove from nor change security policies on an inactive virtual server. You can add security policies (instead of replace them) to an active virtual server only if it does not have a security policy already.*

1. Navigate to **Security** > **Web Application Security** > **Overview**.
2. In the Virtual Servers panel, hover over the name of the virtual server to change and click the gear icon to display its Properties screen.
3. On the screen, to the right of **Attached Policies**, click **Change**.

   The Select Policy popup screen opens with a list of available policies.
4. Select the policies you want to add to the current virtual server and click **Add**.

   The popup screen closes and the selected policy is listed to the right of **Attached Policies**.
5. At the top of the Virtual Server screen, click **Save**.

   A popup screen requests confirmation of the change.
6. Click **Change** to accept the virtual server change.

   The Virtual Server details screen closes.

   If an error message displays, the virtual server on the BIG-IP device may not be configured to support ASM™ policies. In this case, restart this task with another virtual server.

The selected policies are added to or changed from the current virtual server. On the next deployment operation, the policies will be deployed to the virtual server's BIG-IP® host.

Removing links between virtual servers and security policies

You can use BIG-IQ® Web Application Security to remove the link between a virtual server and a security policy.

1. To begin the process, navigate to the Virtual Servers panel.
2. In the Virtual Servers panel, hover over the name of the virtual server to change and click the gear icon to display its Properties screen.
3. In the expanded Properties screen, click **Remove**.

The link between the policy and the virtual server is deleted. This means that if the policy is attached to the virtual server on the remote BIG-IP® device, the link between them is deleted during the deployment process.

Chapter 24

Deploying Configuration Changes

About BIG-IQ Security deployments

The BIG-IQ® Security system displays individual deployments and their status (one action per row in the Deployment panel).

After you have completed edits to firewall contexts, objects, or policies you can create a deployment to distribute those changes to selected BIG-IP® devices from the Deployment panel.

Note: *You can deploy security policies to a device that already has the policy by overwriting the existing security policy. If the security policy does not yet exist on the device, you can deploy it as a new policy attached to an available virtual server or you can deploy it as an inactive policy.*

The system displays changes as follows:

- `ADDED`. New shared objects added to a rule and called by an existing rule list, policy, or firewall are counted as `ADDED`. Newly-created shared objects that are not referenced in a firewall are not counted and are not distributed.
- `MODIFIED`. Existing objects already used by an existing rule list, policy, or firewall, and subsequently edited, are counted as `MODIFIED`.
- `REMOVED`. Existing objects used by an existing rule list, policy, or firewall, and subsequently removed, are counted as `REMOVED`. If a shared object is removed from a rule and is no longer being used by any other rules, it is marked for removal from the selected devices. It is not removed from the BIG-IQ Security system unless expressly deleted.

Note: *If an individual rule in a rule list, policy, or firewall has been changed, added, or removed, the entire modified object (rule list, policy, or firewall) is marked for deployment. This also applies to adding, modifying, or removing ports in a port list, or addresses in an address list.*

During the distribution phase, configuration changes and security policies are pushed out to remote BIG-IP devices. The working-configuration set is deployed, or the selected BIG-IP device is rolled back, to the state reflected in the snapshot. Any changes made locally to the BIG-IP device are overwritten.

With BIG-IQ Security, you can deploy up to 20 devices in a single deployment.

Filtering on deployment tasks

To filter the Deployment panel, type text in the filter field and press the **Enter** key. Clear the filter by clicking the **X** to the right of the text in the gray box under the filter.

To filter on a specific deployment, hover over the deployment task and when the **gear** icon appears, click it. Then, select **Show Only Related Objects** to filter by deployment task.

Evaluation process steps

During the evaluation process, BIG-IQ Security:

1. Contacts the selected remote BIG-IP devices and synchronizes the working-configuration sets for all.
2. Takes a snapshot of the working-configuration set for each BIG-IP device.
3. Compares the remote and local configurations.
4. Calculates the set of changes to be deployed (number and type of each change).
5. Displays the number and type of each change.

Checking your Web Application Security changes before deployment

After you have changed the configuration, but before you perform a deployment, it may be useful to examine the changes you have made, to verify that they are correct.

1. Navigate to **Security** > **Web Application Security** > **Overview**.
2. Hover over a snapshot in the Snapshots panel, click the gear icon to display the expanded properties screen.
3. Select **Working Config** in the **Compare Against** field.
4. At **ASM Differences**, click the **View** link to see the differences between this snapshot and the current working configuration for Web Application Security.

   A popup appears. First it has a title of **Calculating Differences**, and the title changes to **Snapshot Differences** when the calculation is done. The popup contains a table of differences, if there are any, with one row for each difference.
5. At **Shared Differences**, click the **View** link to see the differences between this snapshot and the current working-config for Shared Security.

   The same popup and table appears.
6. To display the JSON for each difference found, click a row in the table.

   Textual JSON appears for each difference found; snapshot on the left and working configuration, or second snapshot on the right.

   Differences are listed by: name (name of the shared object), type (type of object), change (added, modified, deleted), and device (blank unless the type is **firewall**).

If you are sure the configuration changes are correct, you are ready for a configuration deployment.

Deploying your Web Application Security changes

When you have completed edits to any part of your Web Application Security configuration, you can deploy the change to one or more discovered BIG-IP® devices. To deploy your changes, create a deployment task and choose a target device.

1. Navigate to the Deployment panel.
2. Hover over the Deployment header and click the + icon, then click **Add Deployment**.
   The Deployment panel expands to show the Add Deployment screen.
3. Complete the fields as required. Your changes are saved automatically.

Option	Description
Deployment Name	Name for the deployment that indicates its purpose. It can be useful to develop a convention such as ticket numbers.
Description	Optional description, including the purpose of the deployment or other relevant information.
Select Devices to Evaluate	Available devices are listed to the right of the field. Select or clear check boxes to specify BIG-IP devices that you want to evaluate for this deployment. Devices with known changes are already checked off.

4. To evaluate differences between the working configuration (BIG-IQ® Security) and the configuration on the BIG-IP® device, click **Evaluate**.

The Deployment panel returns to its original dimensions. The new deployment task appears in the Deployments panel, showing updated status as the operation proceeds.

During the evaluation, the BIG-IQ system queries the BIG-IP devices about their current configurations, updates its current-config, compares the working-config objects to the updated current-config objects, and then shows you all of the differences that would result from an actual deployment. On successful completion, the status shows `Evaluation Completed`.

5. Hover over the header of the deployment you want to manage, and click the gear icon to expand the panel and display task properties.

Option	Description
Deployment Name	User-provided name of the deployment task.
Description	Optional description, including the purpose of the deployment or other relevant information.
Task Status	Status for deployment phases (evaluation and distribution).
Start Time	Time the deployment started in the format yyyy-mm-ddThh:mm:ss-hours-off-GMT. Example: `2013-05-31T08:16:17-07:00`
End Time	Time the deployment ended in the format yyyy-mm-ddThh:mm:ss-hours-off-GMT. Example: `2013-05-31T08:16:36-07:00`
Available Devices	List of BIG-IP® devices that can be selected for deployment.

6. Click **View Diff** if you want to check all the configuration differences that would be sent to the BIG-IP devices in the final deployment.

   A Modal window with the list of all the new, deleted, and changed objects appears. For objects with changes (as opposed to new or deleted objects), you can expand the view to see a line-by-line difference.

7. Click **Close** to close the Modal Window.
8. Click **Deploy**.

   The Deployment screen returns to its original dimensions. The new deployment task appears in the Deployments panel, showing updated status as the operation proceeds.

   On successful completion, the status shows `Deployment Completed`.

Deploying your Network Security changes

When you have completed edits to any part of your Network Security configuration, you can deploy the change to one or more discovered BIG-IP® devices. To deploy your changes, create a deployment task and choose a target device.

1. Navigate to the Deployment panel.
2. Hover over the Deployment header and click the + icon, then click **Add Deployment**.
   The Deployment panel expands to show the Add Deployment screen.
3. Complete the fields as required.

   Your changes are saved automatically.

Option	Description
Deployment Name	Name for the deployment that indicates its purpose. It can be useful to develop a convention such as ticket numbers.

Option	Description
Description	Optional description, including the purpose of the deployment or other relevant information.
Deployment Source	Choose between **Working Config** and **Snapshot**. To deploy the working configuration currently on the BIG-IQ® system, select **Working Config** and click **Evaluate**. To deploy from a snapshot, select **Snapshot**, and from the popup screen, select the snapshot you want to deploy from, and click **Evaluate**.
Select Devices to Evaluate; Available Devices	Available devices are listed. Select or clear check boxes as appropriate.

4. To evaluate differences between the working configuration (BIG-IQ® Security) and the configuration on the BIG-IP® device, click **Evaluate**.

   The Deployment panel returns to its original dimensions. The new deployment task appears in the Deployments panel, showing updated status as the operation proceeds.

   During the evaluation, the BIG-IQ system queries the BIG-IP devices about their current configurations, updates its current-config, compares the working-config objects to the updated current-config objects, and then shows you all of the differences that would result from an actual deployment. On successful completion, the status shows `Evaluation Completed`.

5. To create the deployment task, click **Deploy**.

A deployment task is created and listed in the Deployment panel along with its status. A status of `READY TO DEPLOY` indicates that you can deploy the working-configuration set. If you decide not to deploy your changes, you can roll back the selected BIG-IP® device to the state reflected in the snapshot.

Managing deployments

When a deployment displays a status of `READY TO DEPLOY`, you can distribute configuration changes to managed BIG-IP® devices. If there are no changes to deploy, a message displays to confirm this.

1. Navigate to the Deployment panel.
2. Hover over the header of the deployment you want to manage and click the gear icon to open the screen and display task properties.

Option	Description
Deployment Name	User-provided name of the deployment task.
Description	Optional description, including the purpose of the deployment or other relevant information.
User	Name of the user who initiated the deployment.
Task Status	Status for deployment phases (evaluation and distribution).
Start Time	Time the deployment started in the format yyyy-mm-ddThh:mm:ss-hours-off-GMT. Example: `2013-05-31T08:16:17-07:00`
End Time	Time the deployment ended in the format yyyy-mm-ddThh:mm:ss-hours-off-GMT. Example: `2013-05-31T08:16:36-07:00`
Select Devices to Evaluate	Available devices are listed to the right of the field. Select or clear check boxes as appropriate.

3. Click **Evaluate** to evaluate differences between the selected snapshot and the current configuration.
4. Click **View Diffs** to view differences between the configuration on BIG-IQ® Web Application Security and the BIG-IP device.

   A dialog box opens displaying the differences. The display shows four columns: Type (type of entity changed), Change (add, modify, remove), On BIG-IQ (name of the entity on BIG-IQ Web Application Security), and On BIG-IP (name of the entity on the BIG-IP® device).
5. When ready to deploy, click **Deploy** to push changes to the selected BIG-IP device.

Deployment states are displayed during the deployment process. At the end of the deployment process, the working-configuration set is deployed to selectedBIG-IP® device(s) or, if a snapshot was selected, the BIG-IP device is rolled back to the state reflected in the snapshot.

Deploying from snapshots

During deployment, use snapshots to restore a specific configuration state or to deploy a specific set of working configuration edits back to the BIG-IP® device.

1. Navigate to the Deployment panel.
2. Hover over the Deployment header and click the + icon, then click **Add Deployment**.
   The Deployment panel expands to show the Add Deployment screen.
3. Complete the fields as required.

   Your changes are saved automatically.

Option	Description
Deployment Name	Name for the deployment that indicates its purpose. It can be useful to develop a convention such as ticket numbers.
Description	Optional description, including the purpose of the deployment or other relevant information.
Deployment Source	Choose between **Working Config** and **Snapshot**. To deploy the working configuration currently on the BIG-IQ® system, select **Working Config** and click **Evaluate**. To deploy from a snapshot, select **Snapshot**, and from the popup screen, select the snapshot you want to deploy from, and click **Evaluate**.
Select Devices to Evaluate; Available Devices	Available devices are listed. Select or clear check boxes as appropriate.

4. When you see the message `READY TO DEPLOY` under the deployment name in the Deployment panel, click the gear icon to expand the panel.
   a) Under the text `Evaluate found the following changes:` you will see a device name followed by an arrow.
   b) Click the arrow to display differences. Differences are listed by: name, type, change (added, modified, deleted), and device (blank unless the type is **firewall**).
   c) Click an object name to view the JSON in the table under the list of differences.
5. When ready to deploy, click **Deploy** to push changes to the selected BIG-IP device.

The selected snapshot or the specific set of working-configuration edits is deployed to the selected BIG-IP device.

Device deployment states

This table displays states that occur during the deployment process, and a brief description of each state.

State	Description
NEW	The deployment process has started.
COMPLETED_RETRIEVE_DEVICES	Devices have been successfully retrieved. All managed devices on the BIG-IQ® Security system have been found.
FAILED_RETRIEVE_DEVICES	Failed to retrieve devices. Failed to find all managed devices on BIG-IQ Security.
COMPLETED_CHECK_DMA	Verified that the process of declaring management authority (DMA) is not currently running. The deployment process cannot run if DMA is running.
FAILED_CHECK_DMA	Verified that the process of DMA is currently running. The deployment process cannot run at the same time.
STARTED_REFRESH_CONFIG	Refresh of the current configuration for all devices included in deployment has started. This process pulls in any new configuration items from the BIG-IP® device into the current configuration.
COMPLETED_REFRESH_CONFIG	Refresh of the current configuration for all devices included in deployment that started has completed. This process pulls in any new configuration items from the BIG-IP device into the current configuration.
FAILED_REFRESH_CONFIG	Refresh of the BIG-IQ Security current configuration has failed. This refresh pulls in any new configuration items from the BIG-IP device into the current configuration.
STARTED_SNAPSHOT	Snapshot of the working configuration has started.
COMPLETED_SNAPSHOT	Snapshot of the working configuration has completed.
FAILED_SNAPSHOT	Snapshot of the working configuration has failed.
START_DIFFERENCE	Preparing to start the process of enumerating differences between the snapshot taken and the current configuration.
STARTED_DIFFERENCE	Generating the differences between the snapshot taken and the current configuration has started.
COMPLETED_DIFFERENCE	The process of enumerating differences between the snapshot taken and the current configuration has completed.
FAILED_DIFFERENCE	The process of enumerating differences between the snapshot taken and the current configuration has failed.
STARTED_PROCESSING_DIFFERENCE	Processing differences between the snapshot taken and the current configuration has started. This state transforms the difference data into a form that can be distributed.
COMPLETED_PROCESSING_DIFFERENCE	Processing differences between the snapshot taken and the current configuration has completed. This state transforms the difference data into a form that can be distributed.

State	Description
FAILED_PROCESSING_DIFFERENCE	Processing differences between the snapshot taken and the current configuration has failed. This state transforms the difference data into a form that can be distributed.
START_DISTRIBUTION	Preparing to start the distribution process.
STARTED_DISTRIBUTION	The process of distributing configuration changes to specified devices has started.
FAILED_DISTRIBUTION	The process of distributing configuration changes has failed.
COMPLETED	The deployment process has completed.

Chapter

25

Managing Audit Logs in BIG-IQ Network Security

About firewall audit logs and the viewer

In large customer environments, multiple users can make changes to security policies. These policy changes to working-configuration objects are captured in a central location (the BIG-IQ® Network Security database) not on individual BIG-IP® Advanced Firewall Manager™ (AFM™) devices.

Note: *A change is defined as: object created, object deleted, object modified.*

Users who can access the BIG-IQ Network Security console (shell) have access to this database.

BIG-IQ Network Security logs every configuration change in an audit log, which becomes an important tool for debugging and tracking changes to firewall devices. Audit log entries are visible through the system interface **Audit Logs** link. The *audit log viewer* retrieves entries from this database for display in the system interface.

Note: *All API traffic on the BIG-IQ system, every REST service command for all licensed modules, is logged in a separate, central audit log (*`restjavad-audit.n.log`*).*

About firewall audit log entry generation

Changes to these working-configuration objects generate log entries:

- Firewalls
- Policies
- Rule lists
- Address lists
- Port lists
- Schedules
- Snapshots

These actions also generate log entries:

- Add/edit BIG-IQ® Network Security system roles. Tracking role modification provides auditing for the assignment of users to roles.
- Create/cancel device discovery and reimport.
- Delete previously-discovered device.
- Create/delete deployment task.
- Create difference task.
- Create/delete snapshot.
- Edit of system information (such as host name and internal self IP).

About firewall audit logs and high-availability

In high-availability (HA) configurations, each node maintains its own audit log. Entries are synced after the HA configuration is set. If you have entries on the primary node and then configure HA, the previously-generated entries on the primary will not be replicated to the standby node; new entries will be replicated.

All deletions, whether performed manually through the Audit Log viewer or performed as part of a delete and archive operation, are not deleted on the standby node.

Also, archives are configured separately on each node.

Firewall audit log entry properties

The firewall audit log viewer displays the following properties for each entry.

Property	Description
Client IP	IP address for the BIG-IQ® system.
Time	User-friendly timeline of all changes, as well as tasks that were started and canceled. Time is preserved in UTC (Coordinated Universal Time), but the system interface displays the time in the user's local time zone.
Node	FQDN for the BIG-IQ system that recorded the event.
User	User who initiated the action.
Object Name	Object identified by a user-friendly name; for example: `newRule1`, `deploy-test`, or `Common/global`. This entry is also a link; when activated, it shows the JSON for the object.
Type	Class or group of the object modified.
Action	Type of modification (New, Delete, or Update).
Version	Number of times the system generated the object.

Locating the firewall audit log using SSH

You can review BIG-IQ® Network Security audit log contents periodically from the command line and then archive contents locally for off-device processing, troubleshooting, and future reference.

1. To examine audit logs using SSH, log in to BIG-IQ Network Security with Administrator or Security_Manager credentials.
2. Navigate to the audit log location: `/var/log/firewall`.
3. Examine files with the naming convention: `archive-audit.n.txt`.

   where *n* is the log number.
4. Once you have located the logs, you can view or save the log locally through a method of your choice.

About the firewall audit log viewer

The Audit Log viewer retrieves entries from the audit log for display in the BIG-IQ® Network Security system interface.

Note: *The Audit Log viewer is not updated dynamically. You must refresh the page to get new entries.*

All BIG-IQ system user roles have read-only access and can view entries. Only users with the role of Administrator or Security_Manager can delete entries or modify configuration settings.

Viewing differences in the viewer

You can use the built-in firewall audit log viewer provided in BIG-IQ® Network Security to examine differences between entries listed in the viewer. If the system finds no differences, it displays a message to that effect.

1. Log in to BIG-IQ Network Security with Administrator or Security_Manager credentials.
2. Below **Network Security**, click **Audit Logs** to display the viewer.
3. To display differences between object generations, click an object in the Object Name column,which open the Difference Viewer.

   Areas of differences are highlighted in gold. Additions to a generation are highlighted in green. Textual JSON appears for each difference found.

   If a generation of an object cannot be retrieved, Generation Not Available is displayed in the column. Object information may not be available if it has been automatically purged from the system to conserve disk space or if it has been deleted.

   The JSON difference displayed for a delete entry in the audit log shows the JSON difference from the previous operation because the generation identifier is not incremented when an object is deleted.
4. When you are finished, click **Close**.

Filtering entries in the viewer

The Filter field at the top of the Audit Logs page enables you to rapidly narrow the scope displayed in the viewer, and more easily locate an entry in the audit log.

- Filtering is text-based.
- Filtering is not case-sensitive.
- To clear the filter, click the **X** at the end of the search string under the Filter field.
- All BIG-IQ® system roles have read-only access to the audit log and can filter entries.

Note: *You can use wild cards in all filtering operations.*

---

1. Log in to BIG-IQ Network Security.
2. Below **Network Security**, click **Audit Logs**
3. In the Filter field, type the information specific to the object you want to filter on, and click **Apply**.

Option	Description
Client IP	Type the client IP address in the filter. Note that when a task is not initiated by a user, the entry in the Client IP column is blank.
Time (mix of letters and numbers)	Type a date/time in any of the following formats: • mmm dd yyyy hh:mm:ss. Example: `Jan 7 2014 8:30:00` • ddd mmm dd yyyy hh:mm. Example: `Thu Jan 16 2014 11:01` • ddd mmm dd yyyy hh:mm:ss. Example: `Thu Jan 16 2014 11:13:50` Formats are highly browser-dependent. Other formats might appear to filter successfully, but are not supported.

Option	Description
	You must include both a date and a time. Entering a single date/time results in a filter that displaysall entries from the specified date/time to the current date/time. To filter on a range of times, enter the dates/times in one of the supported formats, separated by a hyphen. Example: `jan 21 2014 11:04-jan 21 2014 11:05`.
Time (numbers only)	Type a date/time in any of the following formats: • m/d hh:mm:ss. Example: `1/1 12:14:15` • mm/dd hh:mm:ss. Example: `01/01 12:14:15` • m/d hh:mm. Example: `1/1 12:14` • m/d h:mm. Example: `1/1 2:14` • mm/dd hh:mm. Example: `01/01 12:14` • mm/dd/yy hh:mm:ss. Example: `01/01 12:14:15` • m/d/yy hh:mm:ss. Example: `1/1/14 12:14:15` • mm/dd/yy hh:mm. Example: `01/01/14 12:14` • m/d/yy hh:mm. Example: `1/1/14 12:14` • mm/dd/yyyy hh:mm:ss. Example: `1/1/2014 12:14:15` You must include both a date and a time. Typing a single date/time results in a filter displaying all entries from the specified date/time to the current date/time. To filter on a range of times, type the dates/times in one of the supported formats, separated by a hyphen. Example: `1/1 12:14:15-1/1 12:14:18`.
Node	Type the node name in the filter.
User	Type the user in the filter.
Object Name	Type the name of the object in the filter. If a partition name is displayed, do not include it in the filter. For example, you would specify /Common/AddressList_4 as `AddressList_4`. Note that entries in the Object Name column are links to the JSON representing the object. If the object does not have a name, the system places a dash in the column. The dash is also a link to the JSON.
Type	Type the type in the filter. Note that `WC` stands for working configuration.
Action	Type the action in the filter.
Version	Type the version number in the filter.

The result of a filter (or search) operation is a set of entries that match the filter criteria, sorted by time.

Deleting entries in the viewer

You can prune entries in the audit log viewer to constrain the list to relevant data and a manageable size. Use the scroll bar to the right to scroll through entries.

There is no set limit on the number of entries that the viewer can display, although the viewer will not display archived entries.

Users with BIG-IQ® system roles of either Administrator or Security_Manager can delete entries. All system user roles have read-only access to the audit log, and can view entries.

Note: *Exercise care when deleting entries. Once deleted, entries cannot be retrieved.*

1. Log in to BIG-IQ Network Security with Administrator or Security_Manager credentials.
2. At the top left of the screen, below **Network Security**, click **Audit Logs** to view the audit log.
3. Delete one or multiple entries as specified:

To delete:	Do this:
A single entry	Select the check box for the entry you want to delete and then click **Remove**. You will not receive a confirmation dialog box.
All entries stored on this BIG-IQ system	Select the check box in the header row and then click **Remove**. In the confirmation dialog box, click **Yes** to confirm that you want to delete all entries. ***Important:*** *This action removes all entries, not just those visible in the viewer page.*
Multiple entries	Combine selecting with the Shift key, and then click **Remove**. You will not receive a confirmation dialog box.
A filtered batch of entries	Type a text string in the Filter field at the top of the page and click **Apply**. The result after applying the filter is a batched set of entries that match the criteria. Select the check box at the top of the table in the header row and click **Remove**. The batch of entries is removed. Note that if you delete a large batch of entries, the operation may take some time if the system has a lot of entries. Also, you must keep the Audit Logs viewer open the entire time.

Setting firewall audit log archival properties in the viewer

1. Log in to BIG-IQ Network Security.
2. Below **Network Security**, click **Audit Logs**.
3. Hover over the Firewall header and click the **gear** icon to display the settable audit log properties.
4. Complete the properties and status settings, and click **Save**.

Property	Description
Days to keep entries	Default is 30 days. The field must contain an integer between 1 and 366.
Check expiration at this time	Contains the hour and minute when expirations on entries will be checked. You can type the hour and the minute manually (in the format hh:mm). Or, you can click in the field to view and edit in the Choose Time dialog box. Adjust the **Hour** and **Minute** sliders to reflect the desired hour and minute, and then click **Done**.
When entries expire	Controls whether entries are deleted from the audit log when they expire, or deleted from the audit log but archived to the audit log archive. • Select **Delete** to delete the entry. (This action is permanent; you cannot get a deleted entry back.)

Property	Description
	• Select **Delete and Archive** to delete the entry but archive it for future reference. Expired entries are saved to a predefined file at `/var/log/firewall/archive-audit.0.txt`.
Next run time	Informational, read-only setting, indicating the next time entries will be archived. Run time is expressed in the format: ddd mmm dd yyyy hh:mm:ss. Example: `Tue Jan 28 2014 02:50:00`.
Last run time	Informational, read-only setting, indicating the last time entries were archived. Run time is expressed in the format: ddd mmm yyyy hh:mm:ss. Example: `Tue Jan 28 2014 02:50:00`.
Entries expired at last run time	Number of entries that expired at the last run time.
Last Error	Informational, read-only setting. The field contains the text `No error` or the error text for any errors found.
Last Error Time	Informational, read-only setting. Time in the field is expressed in the format: ddd mmm dd yyyy hh:mm:ss Example: `Fri Jan 17 2014 23:50:00`.

The result of a filter (or search) operation is a set of entries that match the filter criteria, sorted by time.

About the REST API audit log

The REST API audit log records all API traffic on the BIG-IQ® system. It logs every REST service command for all licensed modules in a central audit log (`restjavad-audit.n.log`) located on the system.

Note: *The current iteration of the log is named `restjavad-audit.0.log`. When the log reaches a certain user-configured size, a new log is created and the number is incremented. You can configure and edit settings in `/etc/restjavad.log.conf`.*

Any user who can access the BIG-IQ Network Security console (shell) has access to this file.

Managing the REST API audit log

The REST API audit log contains an entry for every REST API command processed by the BIG-IQ® system, and is an essential source of information about the modules licensed under the BIG-IQ Network Security system. It can provide assistance in compliance, troubleshooting, and record-keeping. With it, you can review log contents periodically, and ave contents locally for off-device processing and archiving.

1. Using SSH, log in to the BIG-IQ Network Security device with administrator credentials.
2. Navigate to the `restjavad` log location: `/var/log`.
3. Examine files with the naming convention: `restjavad-audit.n.log`.

   where `n` is the log number.
4. Once you have located it, you can view or save the log locally through a method of your choice.

Chapter

26

Logging Events in BIG-IQ Web Application Security

About event logs

Viewing the event logs with BIG-IQ® Web Application Security makes browsing of system event logs easier, and provides a way to obtain useful insights regarding the activity on applications and/or servers. It also enables the viewing of logs from multiple BIG-IP® devices.

You can also view logs through the BIG-IP system interface. However, the BIG-IP system interface shows logs for one BIG-IP device only, and the current presentation has many nested views and complex filters. Thus, it is difficult to obtain a complete picture. The presentation on Web Application Security provides a single view of all the filters, log entries, and details for each entry. This provides a more intuitive navigation path through the log items.

To determine which events are logged, you must set up a logging profile on the BIG-IP system. The logging profile directs the security events to a BIG-IQ Logging Node, and the BIG-IQ system retrieves them from that node.

About installing the BIG-IQ Logging Node

A *BIG-IQ Logging Node* (also known as an ASM™ Logging Node) is a specially-provisioned BIG-IQ® system, running the same software build as the BIG-IQ device where you manage your security policies. One or more BIG-IP® systems send their logging events to a Logging Node, and the BIG-IQ system can retrieve logging events from one or more Logging Nodes.

To install a BIG-IQ Logging Node, you provision a standard BIG-IQ system as a Logging Node (by allowing a particular service on a self IP port and expanding the size of the file system that holds log files), and then upgrade the Logging Node Software to the same build that is running on its BIG-IQ partner.

Provisioning the Logging Node

You use the Config utility and `tmsh` commands to provision the Logging Node with a management IP address, a self IP address, and various network parameters.

1. The BIG-IQ VE or BIG-IQ 7000 device is shipped with a default management IP address of `192.168.1.245`. To change this, connect to the console of the device and invoke the Config utility.
   For example:

```
[root@bigiq1:Active] config # config
```

   The Config utility is a GUI-like interface on the command line. It guides you through the process of setting these parameters:

   - Management IP Address
   - Netmask for that address
   - Default Route for the Management IP Address

2. Test the management IP address by connecting to it with SSH. Use the `root` admin account and its default password, `default`.
   For example:

```
juser@bench2:~/$ ssh root@192.168.25.61
The authenticity of host '192.168.25.61 (192.168.25.61)' can't be established.
RSA key fingerprint is 8c:0a:28:e9:7a:8d:5a:1a:7a:d1:2d:c2:8a:c8:e5:83.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.25.61' (RSA) to the list of known hosts.
Password:  default
[root@bigiq1:NO LICENSE] config #
```

Currently, the system is running BIG-IQ software, and its prompt, `bigiq1`, is the default for a BIG-IQ system.

3. Invoke `tmsh`, where you can perform some initial provisioning of the Logging Node.
   For example:

```
[root@bigiq1:NO LICENSE] config # tmsh
root@(bigiq1)(NO LICENSE)(/Common)(tmos)#
```

4. Expand the `/var` directory, which holds all the event logs. Use the `modify sys disk directory` command to schedule the directory for resizing, then use the `reboot` command to reboot the Logging Node and expand the directory.
   For example, this command sequence expands the `/var` directory to 15G and reboots the Logging Node:

```
root@(lognode1)(NO LICENSE)(/Common)(tmos)# modify sys disk directory /var new-size 15000000
root@(lognode1)(NO LICENSE)(/Common)(tmos)# reboot
The system will be rebooted momentarily

Broadcast message from root (pts/0) (Thu Aug 14 09:04:44 2014):

The system is going down for reboot NOW!
root@(lognode1)(NO LICENSE)(/Common)(tmos)#  Connection to 192.168.25.61 closed by remote
host.
Connection to 192.168.25.61 closed.
juser@bench2:~/$
```

5. Wait for the Logging Node to finish the boot process, then reconnect and reopen `tmsh`.
   For example:

```
juser@bench2:~/$ ssh root@192.168.25.61
Password:  default
[root@bigiq1:NO LICENSE] config # tmsh
root@(bigiq1)(NO LICENSE)(/Common)(tmos)#
```

6. Use the `modify sys global-settings hostname` command to create an appropriate host name for the Logging Node.
   For example:

```
root@(bigiq1)(NO LICENSE)(/Common)(tmos)# modify sys global-settings hostname lognode1.myco.com
root@(lognode1)(NO LICENSE)(/Common)(tmos)#
```

7. Use the `modify sys ntp` commands to set up the Network Time Protocol (NTP) for this Logging Node. Set the timezone and add one or more NTP servers.
   For example, these commands set the time zone for New York in the U.S., and add one NTP server:

```
root@(lognode1)(NO LICENSE)(/Common)(tmos)# modify sys ntp timezone America/New_York
root@(lognode1)(NO LICENSE)(/Common)(tmos)# modify sys ntp servers add { 192.168.96.95 }
root@(lognode1)(NO LICENSE)(/Common)(tmos)#
```

8. Use the `create net vlan` command to create a VLAN named `internal`. Then use the `modify net vlan` command to assign it to the 1.1 interface.
   For example:

```
root@(lognode1)(NO LICENSE)(/Common)(tmos)# create net vlan internal
root@(lognode1)(NO LICENSE)(/Common)(tmos)# modify net vlan internal interfaces add { 1.1 }
root@(lognode1)(NO LICENSE)(/Common)(tmos)#
```

9. Use the `create net self` command to assign a self IP address to the `internal` VLAN. Also, allow service on TCP port 8514.
   For example, this assigns `10.57.140.135/16` as a self IP address:

```
root@(lognode1)(NO LICENSE)(/Common)(tmos)# create net self 10.57.140.135/16 vlan internal
address 10.57.140.135/16 allow-service add { default tcp:8514 }
root@(lognode1)(NO LICENSE)(/Common)(tmos)#
```

10. Use the `create net route` command to establish a default gateway for the VLAN.
    For example:

```
root@(lognode1)(NO LICENSE)(/Common)(tmos)# create net route internal_default_gateway gw
10.57.140.1 network default
root@(lognode1)(NO LICENSE)(/Common)(tmos)#
```

11. Use the `modify sys dns name-servers` command to add your local DNS servers and your DNS-search parameters.
    For example:

```
root@(lognode1)(NO LICENSE)(/Common)(tmos)# modify sys dns name-servers add { 10.57.1.28 }
search add { myco.com localhost }
root@(lognode1)(NO LICENSE)(/Common)(tmos)#
```

12. Use the `save sys config` command to save this configuration:
    For example:

```
root@(lognode1)(NO LICENSE)(/Common)(tmos)# save sys config
Saving running configuration...
  /config/bigip.conf
  /config/bigip_base.conf
  /config/bigip_script.conf
  /config/bigip_user.conf
Saving Ethernet mapping...done
root@(lognode1)(NO LICENSE)(/Common)(tmos)#
```

The Logging Node is ready to process network traffic, but it likely requires a software upgrade to bring it to the same build as its partner BIG-IQ system.

About upgrading the Logging Node to the BIG-IQ build

This product ships with a software build that was current at the time of the software release. Typically, a later build is available. The build on the Logging Node must be the same as the build on its partner BIG-IQ® system. If you need to upgrade the Logging Node, follow the instructions in *Upgrading BIG-IQ Systems*.

Configuring the logging profile

Each BIG-IP system sends its events to a Logging Node. You create an *event logging profile* to define the contents of these events, and to identify the Logging Node to which the events are sent.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles** > +.
   The Create New Logging Profile screen opens.

2. In the **Profile Name** field, type the name that you choose for this new profile.
3. Select the **Application Security** check box.
   Application Security settings display.
4. From the **Configuration** list, select **Advanced**.
   Some new fields appear, including the **Remote Storage** check box.
5. Select the **Remote Storage** check box.
   Several new fields appear, including the **Protocol** list.
6. From the **Protocol** list, select **TCP**.
7. In the **Server Addresses** settings, specify the address you want to use:
   a) In the **IP Address** field, type one of the Logging Node's self IP addresses.
   b) In the **Port** field, type `8514`.
   c) Click the **Add** button to add the address/port to the list of servers.
8. In the **Storage Format** setting, specify how you want to store this data:
   a) Select **User-Defined** from the list at the top.
   b) Then enter this exact format (without any line breaks) for the event logs in the **Selected Items** field:

```
unit_hostname="%unit_hostname%",management_ip_address="%management_ip_address%",
http_class_name="%http_class_name%",web_application_name="%http_class_name%",policy_name="%policy_name%",
policy_apply_date="%policy_apply_date%",violations="%violations%",support_id="%support_id%",
request_status="%request_status%",response_code="%response_code%",ip_client="%ip_client%",
route_domain="%route_domain%",method="%method%",protocol="%protocol%",query_string="%query_string%",
x_forwarded_for_header_value="%x_forwarded_for_header_value%",sig_ids="%sig_ids%",sig_names="%sig_names%",
date_time="%date_time%",severity="%severity%",attack_type="%attack_type%",geo_location="%geo_location%",
ip_address_intelligence="%ip_address_intelligence%",username="%username%",session_id="%session_id%",
src_port="%src_port%",dest_port="%dest_port%",dest_ip="%dest_ip%",sub_violations="%sub_violations%",
virus_name="%virus_name%",uri="%uri%",request="%request%",violation_details="%violation_details%",
header="%headers%",response="%response%
```

   The line breaks in the example above were necessary due to screen width; remove all of them after you paste this data. It should be a single string with no white space.
9. From the **Maximum Entry Length** list, select **64K**.
10. In the Storage Filter area, from the **Request Type** list, select **All Requests**.
11. Click the **Finished** button to save the new profile.

Adding the logging profile to a virtual server

Each BIG-IP system sends its events to a BIG-IQ Logging Node. After you create an event logging profile, you assign it to a virtual server. The virtual server (or servers) with this profile sends all of its relevant events to the Logging Node that you specified in the logging profile.

1. On the Main tab, click **Local Traffic** > **Virtual Servers** > **Virtual Server List**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server that you want to log security events.
3. From the Security menu at the top of the screen, choose Policies.
4. Use the **Log Profile** settings to specify the log profile to use:
   a) From the **Log Profile**list, select **Enabled**.
   b) From the **Available** list, select the log profile you created earlier, and move (**<<**) it to the **Selected** list.
5. Click **Update** to save your changes.

Discovering a Logging Node from BIG-IQ Security

Using the BIG-IQ Security system, you discover a Logging Node and add it to the ASM Logging Group. The BIG-IQ Security application can then access all of the security events on the Logging Node, potentially from multiple BIG-IP systems.

1. Log into BIG-IQ System GUI with your administrator user name and password.
2. From the list at the top of the screen, choose **System**.
   Several panels appear, including the BIG-IQ Systems panel.
3. In the BIG-IQ Systems panel, hover over **ASM Logging Group**, click the gear icon when it appears, and select **Add Device**.
   The panel expands to show the New Device screen.
4. In the **IP Address** field, type a self IP address on the Logging Node (for example, `10.57.140.135`).
5. In the **User name** and **Password** fields, type the credentials for an administrator on the Logging Node (for example, `admin` and `admin`).
6. Confirm that the **Group** field is set to **ASM Logging Group**.
7. Click the **Add** button at the top of the screen to add the Logging Node to the system.

All BIG-IP virtual servers that send their security events to the above Logging Node are aggregated in the event logs on the BIG-IQ system. You can repeat this task to add multiple Logging Nodes.

About the event logs interface

The Event Logs system interface consists of two filtering fields and three main panes:

- Filtering fields:
  - Selected devices list. A horizontal list below the Event Logs heading, where you select one or more devices for event viewing.
  - Filter field. A horizontal field, below the Event Logs heading to the right of the selected devices field, where you can provide text to rapidly narrow the search scope.
- Panes:
  - Devices panel. At the far left, used for selecting a group of events, policies, saved filters, or pre-configured tags. This specifies the set of items in the next pane.
  - Log items list. Using this pane, you can browse log items, or select one to view details on. Each log item displays:
    - URL
    - Source IP address
    - Response code
    - Date and time
    - Severity: Informational, Critical, Error
    - Status
  - Details pane. This pane displays details of the item selected in the Log items pane. You can view:
    - Raw HTTP[S] request
    - Geolocation details
    - Policy details (by clicking the expand triangle to the right of the policy name)
    - General request details (by clicking the triangle to the right of the URL)

- Related tags

Viewing event log details

You can view request and response details for a single log item.

1. Log in to BIG-IQ® Security.
2. Click **Web Application Security**, and then click **Event Logs**.
3. In the Log Items pane (list of events), click a single event log.
   The Details pane to the right displays a variety of information about the event.
4. In the Details pane, click **Request** to view request details.
   Details include:
   - Raw HTTP[S] request
   - General request details (by clicking the expand arrow to the right of the URL)
   - Geolocation
   - Policy details (by clicking the expand triangle to the right of the policy name)
   - List of related tags
5. Click **Response** to view response details.

Using common filters

You can use the Event Logs screen's Devices panel to update common filters for requests and security policies.

1. Log in to BIG-IQ® Security.
2. Click **Web Application Security**, and then click **Event Logs**.
3. In the Devices panel, click any sub-item under **Requests** or **Policies**.

The system updates log items according to the selected filter, and results appear in the Log Items pane.

Filtering (basic)

You can use the Event Logs screen's search filter to make viewing of events logs easier, even event logs from multiple BIG-IP® devices.

1. Log in to BIG-IQ® Security.
2. Click **Web Application Security**, and then click **Event Logs**.
3. In the Event Logs Filter field, click the expand triangle to the right of the field.
   The Search filter popup screen opens to the basic view, which is the default.
4. Complete the Search filter field or fields applicable to your search.

Setting	Description
Request type	From the list, select **All requests** or **Illegal requests** (log responses for illegal requests only).
Support ID	Type the last 4 digits of the support ID (unique ID given for a transaction).

Setting	Description
Violation	This selects the policy violation that detects attacks, such as Attack Signature Detection or Illegal Cookie Length. From the list, select nothing (indicating that any violation type matches) or a violation type.
Attack type	This selects the type of service attacks (such as Denial of Service or HTTP Parser Attack) that you want to see. From the list, select nothing (indicating that any attack type matches) or choose a particular attack type.
Time Period	In the **From** field, click the calendar icon and select a start date. Then, in the **To** field, click the calendar icon and select an end date.
Policies	Type a policy name.

5. Click the Search icon in the blue bar.

The results of the filtering process appear in the Log Items list.

Filtering (advanced)

You can use the Event Logs screen's search filter to make viewing of events logs easier, even event logs from multiple BIG-IP® devices.

1. Log in to BIG-IQ® Security.
2. Click **Web Application Security**, and then click **Event Logs**.
3. In the Event Logs Filter field, click the expand triangle to the right of the field.
   The Search filter popup screen opens to the basic view, which is the default.
4. Click **Advanced**
5. Complete the Search filter field or fields applicable to your search.

Setting	Description
Method	From the list, select **GET**, **POST**, **PATCH**, or **DELETE**.
Protocols	From the list, select **HTTP**.
Severity	From the list, select **Informational**, **Critical**, or **Error**.

6. Click the search icon in the blue bar.

The results of the filtering process appear in the Log Items list.

Filtering by entering query parameters

You can use the Filter field to enter query parameters in ODATA format. For example:

```
policy_name:/Common/policy1'
```

Note: *AND/OR constructs are supported.*

---

1. Log in to BIG-IQ® Security.
2. Click **Web Application Security**, and then click **Event Logs**.
3. In the Filter field, type a query in the format `key operator 'value'`.

4. Type a key from the following list:

Key	Description
attack_type	Name of the attack
date_time	Current date and time
dest_ip	Destination IP of this transaction (virtual server)
dest_port	Destination port of this transaction (virtual server) *
geo_location	Attacker geolocation *
header	List of request headers
http_class_name	Alias of policy name
ip_address_intelligence	IP Category such as proxy, phishing, and so on *
ip_client	Attacker IP address
management_ip_address	BIG-IP® management IP address
method	HTTP method of the request (POST/GET, and so on)
policy_apply_date	Last apply policy operation date and time
policy_name	Name of the active policy
protocol	Transport protocol (HTTP)
query_string	URI query string
request	Full request *
request_status	
response_code	HTTP response code
route_domain	
session_id	*
severity	Severity of the request (Informational/Error/Critical/Warning)
sig_ids	*
sig_names	
src_port	Source port of this transaction *
sub_violations	
support_id	Unique ID given for a transaction
unit_hostname	BIG-IP unit host name *
uri	URI of the request *
username	*
violations	List of violations
virus_name	*
web_application_name	
x_forwarded_for_header_value	

5. Type an operator from the following list:

Operator	Description
eq	Equal
ne	Not equal
lt	Less than
le	Less than or equal to
gt	Greater than
ge	Greater than or equal to

6. Type a value in any of the following formats:
   - 'value'
   - '*alue'
   - 'alu*'
   - '*ue*'

The system updates log items according to the typed query, and results appear in the Log Items list. Clearing the Filter field clears the filter as well.

Chapter

27

Upgrading BIG-IQ Systems

About the upgrade process

Upgrade involves installing the new version of the software, booting into that new version, and making any other changes that might be required.

Note: *BIG-IQ Security version 4.5 supports upgrades only from version 4.3 and higher.*

Use this process to upgrade BIG-IQ® Security using a combination of the graphic user interface and the command line interface.

If the BIG-IQ system is in a high availability (HA), the upgrade includes:

1. Ending the HA configuration.
2. Individually upgrading each BIG-IQ system.
3. Re-established the HA configuration after the systems are upgraded.

Separating an HA configuration running version 4.3 software

The upgrade process disconnects the high availability (HA) redundant system configuration during upgrade and reinstates the configuration again as the upgrade is completed. This procedure separates an HA configuration running version 4.3 software.

1. Separate the HA configuration by removing the standby device from the device group.
   a) Log in to the active BIG-IQ device and at the top-right corner of the BIG-IQ Security screen, select **System** and **Overview**.
   The Localhost screen opens.
   b) On the left, click **High Availability**.
   The screen displays the configuration for the Peer device (the standby node).
   c) Click the **Delete** button at the top-right corner of the Localhost screen.
   A pop-up screen appears to confirm that you want to remove the standby device from the device group.
   d) Click the **Remove** button to confirm.
   e) Watch the HA-status indicator at the top-left corner of the screen. When the HA configuration is separated, the indicator changes from `Active (Primary)` to `Standalone`.

   The status indicator at the top-left of the screen now reports Standalone on both BIG-IQ devices.
2. Use a secure copy method to copy the image (ISO) to the `/shared/images` directory on both devices formerly in the HA configuration.

   You can use SCP, FTP, SFTP or any other means of securely transferring ISOs between hosts.

   `scp <big-iq-iso-name> root@<big-iq-standby-node-url>:/shared/images/.`

Both devices are now standalone and have the same ISO file on them.

Separating an HA configuration running version 4.4 software

The upgrade process disconnects the HA redundant system configuration during upgrade and reinstates the configuration again as the upgrade is completed. This procedure separates an HA configuration running version 4.4 software.

1. Separate the HA configuration by removing the standby device from the management group.
   a) Log in to the active BIG-IQ device, and from the BIG-IQ option list at upper left, select **System**.
   b) In the BIG-IQ Systems panel, expand **Management Group**.
   c) Select the standby device.
   d) Hover over the gear icon, click it and select **Properties**.
   The Localhost screen opens.
   e) In the expanded screen, click **Remove**.

   The status indicator at the top-left of the screen now reports `Standalone` on both BIG-IQ devices.
2. Use a secure copy method to copy the image (ISO) to the `/shared/images` directory on both devices formerly in the HA configuration.

   You can use SCP, FTP, SFTP or any other means of securely transferring ISOs between hosts.

   `scp <big-iq-iso-name> root@<big-iq-standby-node-url>:/shared/images/.`

Both devices are now standalone and have the same ISO file on them.

Upgrading BIG-IQ Security (GUI)

Use this procedure to upgrade BIG-IQ through the user interface (GUI).

1. This step applies to BIG-IQ devices running version 4.3 software; skip to step 2 if your devices are running version 4.4 software. For version 4.3, repeat these substeps on both devices to upgrade the image on each.
   a) Log in to the active BIG-IQ device and at the top-right corner of the screen, select **System** and **Overview**.
   The Localhost screen opens.
   b) Select **Software Update** from the ptions on the left.
   Information about the current software displays in the viewing area.
   c) From **the Software Image** list, select the image to use for the update. This is the image you downloaded.
   d) From the **Install Location** list, select the location to use for the update.
   e) For the **Option** setting, select both options.
   f) Click the **Apply** button in the lower-right corner of the panel.
   A pop-up screen prompts you to confirm that you want to reboot the device.
   g) Click the **OK** button in the pop-up screen.
   The BIG-IQ system loads the new software and reboots.

2. This step applies to devices running 4.4 software; skip this step if your devices are running version 4.3 software. For version 4.4, repeat these substeps on both devices to upgrade the image on each.
   a) On the BIG-IQ Systems panel, expand **Management Group**.
   b) Hover over the gear icon, then click it and select **Properties**.

c) Click **Software Update**.
d) Click **Update**.
e) From the **Software Image** list, select the image to use for the update. This is the image you downloaded.
f) From the **Install Location** list, select the location to use for the update.
g) or the **Options** etting, click **Reboot After Live Install**.

3. For both devices, verify that the image is booted on the correct volume using the command `tmsh show sys software`.
4. From the BIG-IQ System, re-establish the HA redundant configuration.

   When re-establishing the HA configuration, the source device copies its common configuration data to the target device. The source device is the device where you start the process of re-instating the HA configuration. Select a source device whose configuration data is the most up-to-date.

   a) On the device you have selected to be the Primary/Active device, hover over the gear icon for the HA Peer Group.
   b) Click **Add Device**.
   The New Device screen opens.
   c) Enter the HA Communication Address of the peer device, and administrator credentials for the secondary BIG-IQ device.
   d) For Network Security configurations, select **Active-Standby** as the **High Availability Mode**.
   e) Click the **Add** button.
   f) Affirm the confirmation to start the re-instatement process.

5. Expand the HA Peer Group and monitor the status changes for the newly-added device.
   a) Monitor the status updates in the new device entry under the management group.
   b) Monitor the device/cluster status indicator at the top left of the screen.
   c) When the indicator changes to `Active (Primary)` the reinstatement of the redundant system configuration has completed successfully.

6. Visually examine the configuration of both devices to verify that they are synchronized.

Each device has been upgraded and reinstated into a redundant system configuration. The upgrade is complete.

After the upgrade, to prevent potential BIG-IQ system user interface issues, clear the cache in the web browser you use to access the BIG-IQ system..

Upgrading BIG-IQ Security (CLI)

Use this procedure to upgrade BIG-IQ through a combination of the user (GUI) interface and the command-line interface (`tmsh`)

1. Perform these steps on both devices.
   a) Upgrade the image (ISO) using the command:
   `tmsh install sys software image` *`big-iq-iso-image-name`* `volume` *`volume-name`*
   If installing a hotfix, in the previous example replace the keyword `image` with the keyword `hotfix` Also, when installing a hotfix, both the hotfix and the base version must be in the same directory.
   b) Monitor the progress of the upgrade using the command `tmsh show sys software`.
   c) Change the boot partition/volume using the switchboot command.

It is critical that you include the switch *-b* in the following command.

```
switchboot -b volume-name
```

d) Reboot using the command `reboot`.

2. From the BIG-IQ System, re-establish the HA redundant configuration.

When re-establishing the HA configuration, the source device copies its common configuration data to the target device. The source device is the device where you start the process of re-instating the HA configuration. Select a source device whose configuration data is the most up-to-date.

a) On the device you have selected to be the Primary/Active device, hover over the gear icon for the HA Peer Group.
b) Click **Add Device**.
The New Device screen opens.
c) Enter the HA Communication Address of the peer device, and administrator credentials for the secondary BIG-IQ device.
d) For Network Security configurations, select **Active-Standby** as the **High Availability Mode**.
e) Click the **Add** button.
f) Affirm the confirmation to start the re-instatement process.

3. Expand the HA Peer Group and monitor the status changes for the newly-added device.

a) Monitor the status updates in the new device entry under the management group.
b) Monitor the device/cluster status indicator at the top left of the screen.
c) When the indicator changes to `Active (Primary)` the reinstatement of the redundant system configuration has completed successfully.

4. Visually examine the configuration of both devices to verify that they are synchronized.

Each device has been upgraded and reinstated into a redundant system configuration. The upgrade is complete.

After the upgrade, to prevent potential BIG-IQ system user interface issues, clear the cache in the web browser you use to access the BIG-IQ system..

Chapter 28

Required BIG-IQ System Components

Installing required BIG-IQ system components

Installing BIG-IQ® system components on a BIG-IP® device requires a licensed BIG-IP device running version 11.3 or later.

You must install and keep up-to-date certain BIG-IQ system components on all BIG-IP devices that are to be brought under central management. Otherwise, device discovery will fail. These required components provide a REST framework required for the BIG-IQ platform. To install these components manually, run the commands from the command line.

Important: *When running this installation script, the traffic management interface (TMM) on each BIG-IP device restarts. Therefore, before running this script, verify that no critical network traffic is targeted to the BIG-IP devices.*

---

1. Log in to the BIG-IQ system command line as the root user.
2. Establish SSH trust between the BIG-IQ system and the managed BIG-IP device:
   `ssh-copy-id root@<BIG-IP Management IP Address>`

   This step is optional. However, if you do not establish trust, you will be required to provide the BIG-IP system's root password multiple times.
3. Navigate to the folder in which the required files reside:
   `cd /usr/lib/dco/packages/upd-adc`
4. Run the installation script:

   `./update_bigip.sh –a admin –p <password> <BIG-IP Management IP Address>`

   Where *<password>* is the administrator password for the BIG-IP device.
5. Revoke SSH trust between the BIG-IQ system and the managed BIG-IP device:
   `ssh-keygen –R <BIG-IP Management IP address>`

   This step is not required if you did not establish trust in step 2.

Installing these BIG-IQ components results in a REST framework that supports the required Java-based management services.

Index

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W