BIG-IP® Network Firewall: Policies and Implementations

Version 11.4

Table of Contents

Legal Notices

Publication Date

This document was published on May 15, 2013.

Publication Number

MAN-0439-01

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

Access Policy Manager, Advanced Client Authentication, Advanced Routing, APM, Application Security Manager, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Management Pack, F5 Networks, F5 World, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iApps, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, Message Security Manager, MSM, OneConnect, OpenBloX, OpenBloX [DESIGN], Packet Velocity, Policy Enforcement Manager, PEM, Protocol Security Manager, PSM, Real Traffic Policy Builder, Rosetta Diameter Gateway, Scale^N, Signaling Delivery Controller, SDC, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, Traffix Diameter Load Balancer, Traffix Systems, Traffix Systems (DESIGN), Transparent Data Reduction, UNITY, VAULT, VIPRION, vCMP, virtual Clustered Multiprocessing, WA, WAN Optimization Manager, WebAccelerator, WOM, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

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 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 ©2012 jQuery Foundation and other contributors (http://jquery.com/).

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,

Chapter 1

About the Network Firewall

What is the BIG-IP Network Firewall?

The BIG-IP® Network Firewall provides policy-based access control to and from address and port pairs, inside and outside of your network. Using a combination of contexts, the network firewall can apply rules in a number of different ways, including: at a global level, on a per-virtual server level, and even for the management port or a self IP address. Firewall rules can be combined in a firewall policy, which can contain multiple context and address pairs, and is applied directly to a virtual server.

By default, the Network Firewall is configured in *ADC mode*, a default allow configuration, in which all traffic is allowed through the firewall, and any traffic you want to block must be explicitly specified.

The system is configured in this mode by default so all traffic on your system continues to pass after you provision the Advanced Firewall Manager. You should create appropriate firewall rules to allow necessary traffic to pass before you switch the Advanced Firewall Manager to Firewall mode. In *Firewall mode*, a default deny configuration, all traffic is blocked through the firewall, and any traffic you want to allow through the firewall must be explicitly specified.

About firewall modes

The BIG-IP® Network Firewall provides policy-based access control to and from address and port pairs, inside and outside of your network. By default, the network firewall is configured in ADC mode, which is a *default allow* configuration, in which all traffic is allowed to virtual servers and self IPs on the system, and any traffic you want to block must be explicitly specified. This applies only to the Virtual Server & Self IP level on the system.

Important: *Even though the system is in a default allow configuration, if a packet matches no rule in any context on the firewall, a Global Drop rule drops the traffic.*

Configuring the Network Firewall in ADC mode

Use this task to configure the BIG-IP®Network Firewall in ADC mode.

Note: *The firewall is configured by default in ADC mode. Use this task to set the firewall back to ADC mode if you have changed the firewall setting to Firewall mode.*

1. On the Main tab, click **Security** > **Options** > **Network Firewall**.
   The Firewall Options screen opens.
2. From the **Virtual Server & Self IP Contexts** list, select the default action **Accept** for the self IP and virtual server contexts.
3. Click **Update**.
   The virtual server and self IP contexts for the firewall are changed.

Configuring the Network Firewall to drop traffic that is not specifically allowed

Use this procedure to configure the BIG-IP® Network Firewall to deny all traffic not explicitly allowed. In the Advanced Firewall Manager this is called *Firewall mode*, and this is also referred to as a *default deny* policy. Firewall mode applies a default deny policy to all self IPs and virtual servers.

1. On the Main tab, click **Security** > **Options** > **Network Firewall**.
   The Firewall Options screen opens.
2. From the **Virtual Server & Self IP Contexts** list, select the default action **Drop** for the self IP and virtual server contexts.
3. Click **Update**.
   The default Virtual Server and Self IP firewall context is changed.

If you are using ConfigSync to synchronize two or more devices, and you set the default action to Drop or Reject, you must apply the built-in firewall rules `_sys_self_allow_defaults` or `_sys_self_allow_management` to the specific self IPs that are used to support those services. To do this, add a new rule with the **Self IP** context, select the Self IP, and select the **Rule List** rule type. Select the preconfigured rules from the list of rule lists.

Chapter 2

About Firewall Rules

About firewall rules

The BIG-IP® Network Firewall uses rules to specify traffic handling actions. A rule includes:

Context
The category of object to which the rule applies. Rules can be global and apply to all addresses on the BIG-IP that match the rule, or they can be specific, applying only to a specific virtual server, or the management port.

Rule or Rule List
Specifies whether the configuration applies to this specific rule, or to a group of rules.

Source Address
One or more addresses or address lists behind the firewall to which the rule applies.

Source Port
The ports or lists of ports on the system behind the firewall to which the rule applies.

VLAN
Specifies VLANs behind the firewall to which the rule applies.

Destination Address
One or more addresses or address lists outside of the firewall to which the rule applies.

Destination Port
The ports or lists of ports outside of the firewall to which the rule applies.

Protocol
The protocol to which the rule applies. The firewall configuration allows you to select one specific protocol from a list of more than 250 protocols. The list is separated into a set of common protocols, and a longer set of other protocols. To apply a rule to more than one protocol, select **Any**.

Schedule
Specifies a schedule for the firewall rule. You configure schedules to define days and times when the firewall rule is made active.

Action
Specifies the action (accept, accept decisively, drop, or reject) for the firewall rule.

Logging
Specifies whether logging is enabled or disabled for the firewall rule.

Firewall actions

These listed actions are available in a firewall rule.

Firewall actions are processed within a context. If traffic matches a firewall rule within a given context, that action is applied to the traffic, and the traffic is then processed again at the next context.

Firewall action	Description
Accept	Allows packets with the specified source, destination, and protocol to pass through the current firewall context. Packets that match the rule, and are `accepted`, traverse the system as if the firewall is not present.

Firewall action	Description
Accept Decisively	Allows packets with the specified source, destination, and protocol to pass through the firewall. Packets that match the rule, and are `accepted decisively`, traverse the system as if the firewall is not present, and are not processed by rules in any further context after the `accept decisively` action applies. If you want a packet to be accepted in one context, and not to be processed in any remaining context or by the default firewall rules, specify the `accept decisively` action. For example, if you want to allow all packets from Network A to reach every server behind your firewall, you can specify a rule that accepts decisively at the global context, from that Network A, to any port and address. Then, you can specify that all traffic is blocked at a specific virtual server, using the virtual server context. Because traffic from Network A is accepted decisively at the global context, that traffic still traverses the virtual server.
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. Rejecting a packet is a more graceful way to deny a packet, as it sends a destination unreachable message to the sender. For example, if the protocol is TCP, a TCP RST message is sent. One benefit of using Reject is that the sending application is notified, after only one attempt, that the connection cannot be established.

About Network Firewall contexts

With the BIG-IP® Network Firewall, you use a context to configure the level of specificity of a firewall rule or policy. For example, you might make a global context rule to block ICMP ping messages, and you might make a virtual server context rule to allow only a specific network to access an application.

Context is processed in this order:

1. Global
2. Route domain
3. Virtual server / self IP
4. Management port*
5. Global drop*

The firewall processes policies and rules in order, progressing from the global context, to the route domain context, and then to either the virtual server or self IP context. Management port rules are processed separately, and are not processed after previous rules. Rules can be viewed in one list, and viewed and reorganized separately within each context. You can enforce a firewall policy on any context except the management port. You can also stage a firewall policy in any context except management.

Important: *You cannot configure or change the Global Drop context. The Global Drop context is the final context for traffic. Note that even though it is a global context, it is not processed first, like the main global context, but last. If a packet matches no rule in any previous context, the Global Drop rule drops the traffic.*

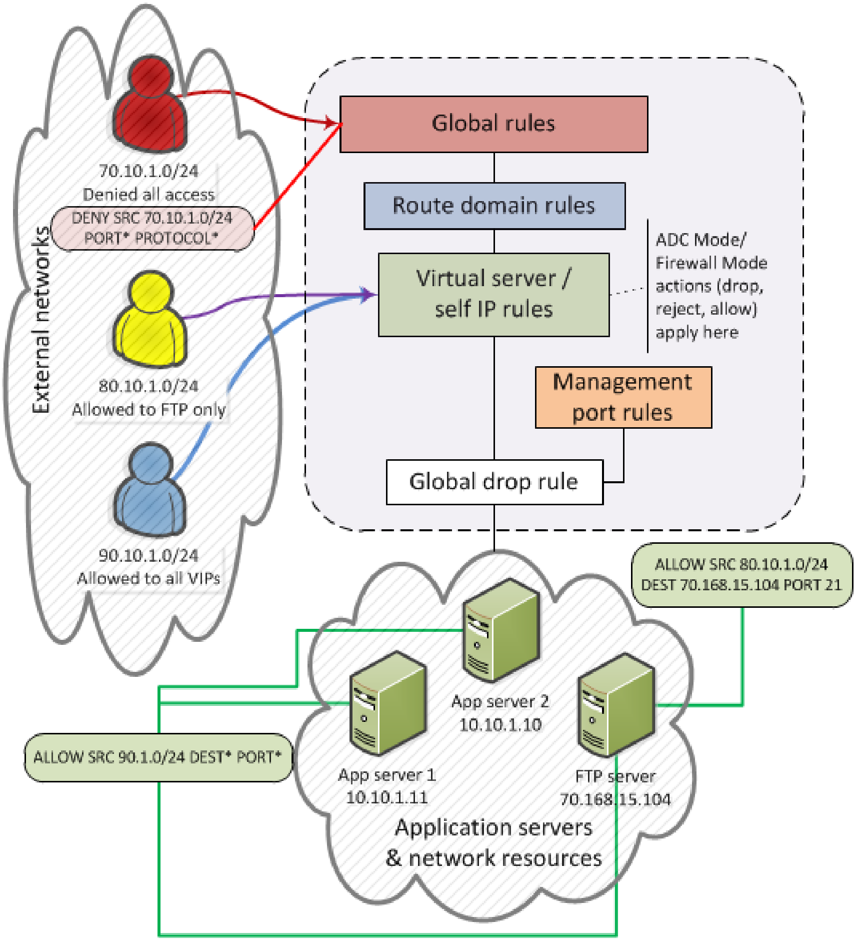

External networks
70.10.1.0/24
Denied all access
DENY SRC 70.10.1.0/24 PORT* PROTOCOL*
80.10.1.0/24
Allowed to FTP only
90.10.1.0/24
Allowed to all VIPs
Global rules
Route domain rules
Virtual server / self IP rules
ADC Mode/ Firewall Mode actions (drop, reject, allow) apply here
Management port rules
Global drop rule
ALLOW SRC 80.10.1.0/24 DEST 70.168.15.104 PORT 21
ALLOW SRC 90.1.0/24 DEST* PORT*
App server 2
10.10.1.10
App server 1
10.10.1.11
FTP server
70.168.15.104
Application servers & network resources

Figure 1: Firewall context processing hierarchy example

Firewall context descriptions

When you create a firewall rule, you can select one of these listed contexts. Rules for each context form their own list and are processed both in the context hierarchy, and in the order within each context list.

Firewall context	Description
Global	A global policy or global inline rules are collected in this firewall context. Global rules apply to all traffic that traverses the firewall, and global rules are checked first.
Route Domain	A route domain policy or route domain inline rules are collected in this context. Route domain rules apply to a specific route domain defined on the server. Route domain rules are checked after global rules. 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; however, if you configure another route domain after this, Route Domain 0 is no longer usable as a global context.
Virtual Server	A virtual server policy or virtual server inline rules are collected in this context. Virtual server rules apply to the selected existing virtual server only. Virtual server rules are checked after route domain rules.
Self IP	A self IP policy or self IP inline rules apply to a specified self IP address on the device. Self IP rules are checked after route domain rules.

Firewall context	Description
Management Port	The management port context collects firewall rules that apply to the management port on the BIG-IP device. Management port rules are checked independently of any other rules.
Global Drop	The Global Drop rule drops all traffic that does not match any rule in a previous context.

Creating a network firewall inline rule

If you are going to specify address lists or port lists with this rule, you must create these lists before creating the firewall rule, or add them after you save the rule.

Create a network firewall rule to manage access from an IP or web network address to a specified network location, server, or address behind a BIG-IP® system.

Note: *You cannot add rules created with this task to a rule list at a later time. You must create rules for a rule list from within the rule list.*

1. On the Main tab, click **Security** > **Network Firewall** > **Active Rules**.
   The Active Rules screen opens.
2. In the Active Network Firewall Rules area, click **Add** to add a firewall rule to the list.
3. From the **Context** list, select the context for the firewall rule.

   For a firewall rule in a rule list, the Rule List context is predefined and cannot be changed.
4. In the **Name** and **Description** fields, type the name and an optional description.
5. From the **Type** list, select whether you are creating a standalone network firewall rule or creating the rule from a predefined rule list.

   If you create a firewall rule from a predefined rule list, most options for creating a firewall rule do not apply.
6. From the **State** list, select the rule state.

   - Select **Enabled** to apply the firewall rule to the given context and addresses.
   - Select **Disabled** to set the firewall rule to not apply at all.
   - Select **Scheduled** to apply the firewall rule according to the selected schedule.
7. From the **Schedule** list, select the schedule for the firewall rule.

   This schedule is applied when the firewall rule state is set to **Scheduled**.
8. From the **Protocol** list, select the protocol to which the firewall rule applies.

   - Select **Any** to apply the firewall rule to any protocol.
   - Select the protocol name to apply the rule to a single protocol.

   Important: *ICMP is handled by BIG-IP at the global or route domain level. Because of this, ICMP messages receive a response before they reach the virtual server context. You cannot create an inline rule for ICMP or ICMPv6 on a Self IP context. You can apply a rule list to a Self IP that includes a rule for ICMP or ICMPv6; however, such a rule will be ignored. To apply firewall actions to the ICMP protocol, create a rule with the `global` or `route domain` context. ICMP rules are evaluated only for ICMP forwarding requests, and not for the IP addresses of the BIG-IP itself.*

   Note: *Note that you must select a protocol if you specify ports.*

9. From the Source **Address** list, select the type of source address to which this rule applies.
   - Select **Any** to have the rule apply to any IP address outside the firewall.
   - Select **Specify** and click **Address** to specify one or more IP addresses outside the firewall to which the rule applies. When selected, you can type single IP addresses into the **Address** field, then click **Add** to add them to the address list.
   - Select **Specify** and click **Address List** to select a predefined list of addresses outside the firewall to which the rule applies. To use an address list with this rule, select the address list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.

10. From the Source **Port** list, select the type of source ports (outside the firewalled network) to which this rule applies.
    - Select **Any** to have the rule apply to any port outside the firewall.
    - Select **Specify** and click **Port** to specify one or more ports outside the firewall to which the rule applies. When selected, you can type single port numbers into the **Port** field, then click **Add** to add them to the port list.
    - Select **Specify** and click **Port List** to specify a list of contiguous port numbers outside the firewall to which the rule applies. When selected, you can type the start and end ports into the fields, then click **Add** to add the ports to the port list.
    - Select **Specify** and click **Port List** to select a predefined list of ports outside the firewall to which the rule applies. To use a port list with this rule, select the port list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.

11. From the Source **VLAN** list, select the VLAN on which this rule applies.
    - Select **Any** to have the rule apply to traffic on any VLAN through which traffic enters the firewall.
    - Select **Specify** to specify one or more VLANs on the firewall to which the rule applies. To use a VLAN with this rule, move the VLAN from the **Available** list to the **Selected** list by clicking the << button. Similarly, to remove the VLAN from this rule, click the >> button to move the VLAN from the **Selected** list to the **Available** list.

12. From the Destination **Address** list, select the type of destination address, behind the firewall, to which this rule applies.
    - Select **Any** to have the rule apply to any IP address inside the firewall.
    - Select **Specify** and click **Address** to specify one or more IP addresses inside the firewall to which the rule applies. When selected, you can type single IP addresses into the **Address** field, then click **Add** to add them to the address list.
    - Select **Specify** and click **Address List** to select a predefined list of addresses inside the firewall to which the rule applies. To use an address list with this rule, select the address list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.

13. From the Destination **Port** list, select the type of destination ports, behind the firewall or inside the firewalled networks, to which this rule applies.
    - Select **Any** to have the rule apply to any port inside the firewall.
    - Select **Specify** and click **Port** to specify one or more ports inside the firewall to which the rule applies. When selected, you can type single port numbers into the **Port** field, then click **Add** to add them to the port list.
    - Select **Specify** and click **Port List** to specify a list of contiguous port numbers inside the firewall to which the rule applies. When selected, you can type the start and end ports into the fields, then click **Add** to add the ports to the port list.
    - Select **Specify** and click **Port List** to select a predefined list of ports inside the firewall to which the rule applies. To use a port list with this rule, select the port list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.

14. From the **Action** list, select the firewall action for traffic originating from the specified source address on the specified protocol. Choose from one of the these actions:

Option	Description
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.
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.

15. From the **Logging** list, enable or disable logging for the firewall rule.
16. Click **Finished**.
    The list screen is displayed, and the new item is displayed.

The new firewall rule is created.

Creating a network firewall rule list

Create a network firewall rule list, to which you can add firewall rules.

1. On the Main tab, click **Security** > **Network Firewall** > **Rule Lists**.
   The Rule Lists screen opens.
2. Click the **Create** button to create a new rule list.
3. In the **Name** and **Description** fields, type the name and an optional description.
4. Click **Finished**.
   The list screen is displayed, and the new item is displayed.

The firewall rule list appears in the list.

Add firewall rules to the rule list to define source, destination, and firewall actions.

Adding a network firewall rule to a rule list

Before you add a firewall rule to a rule list, you must create a rule list.

Use this procedure to add a firewall rule to a rule list.

1. On the Main tab, click **Security** > **Network Firewall** > **Rule Lists**.
   The Rule Lists screen opens.
2. In the list, click the name of a rule list you previously created.
   The Rule List properties screen opens.
3. In the Active Network Firewall Rules area, click **Add** to add a firewall rule to the list.
4. In the **Name** and **Description** fields, type the name and an optional description.

5. From the **State** list, select the rule state.
   - Select **Enabled** to apply the firewall rule to the given context and addresses.
   - Select **Disabled** to set the firewall rule to not apply at all.
   - Select **Scheduled** to apply the firewall rule according to the selected schedule.
6. From the **Schedule** list, select the schedule for the firewall rule.

   This schedule is applied when the firewall rule state is set to **Scheduled**.
7. From the Source **Address** list, select the type of source address to which this rule applies.
   - Select **Any** to have the rule apply to any IP address outside the firewall.
   - Select **Specify** and click **Address** to specify one or more IP addresses outside the firewall to which the rule applies. When selected, you can type single IP addresses into the **Address** field, then click **Add** to add them to the address list.
   - Select **Specify** and click **Address List** to select a predefined list of addresses outside the firewall to which the rule applies. To use an address list with this rule, select the address list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.
8. From the Source **Port** list, select the type of source ports (outside the firewalled network) to which this rule applies.
   - Select **Any** to have the rule apply to any port outside the firewall.
   - Select **Specify** and click **Port** to specify one or more ports outside the firewall to which the rule applies. When selected, you can type single port numbers into the **Port** field, then click **Add** to add them to the port list.
   - Select **Specify** and click **Port List** to specify a list of contiguous port numbers outside the firewall to which the rule applies. When selected, you can type the start and end ports into the fields, then click **Add** to add the ports to the port list.
   - Select **Specify** and click **Port List** to select a predefined list of ports outside the firewall to which the rule applies. To use a port list with this rule, select the port list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.
9. From the Source **VLAN** list, select the VLAN on which this rule applies.
   - Select **Any** to have the rule apply to traffic on any VLAN through which traffic enters the firewall.
   - Select **Specify** to specify one or more VLANs on the firewall to which the rule applies. To use a VLAN with this rule, move the VLAN from the **Available** list to the **Selected** list by clicking the << button. Similarly, to remove the VLAN from this rule, click the >> button to move the VLAN from the **Selected** list to the **Available** list.
10. From the Destination **Address** list, select the type of destination address, behind the firewall, to which this rule applies.
    - Select **Any** to have the rule apply to any IP address inside the firewall.
    - Select **Specify** and click **Address** to specify one or more IP addresses inside the firewall to which the rule applies. When selected, you can type single IP addresses into the **Address** field, then click **Add** to add them to the address list.
    - Select **Specify** and click **Address List** to select a predefined list of addresses inside the firewall to which the rule applies. To use an address list with this rule, select the address list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.
11. From the Destination **Port** list, select the type of destination ports, behind the firewall or inside the firewalled networks, to which this rule applies.
    - Select **Any** to have the rule apply to any port inside the firewall.
    - Select **Specify** and click **Port** to specify one or more ports inside the firewall to which the rule applies. When selected, you can type single port numbers into the **Port** field, then click **Add** to add them to the port list.

- Select **Specify** and click **Port List** to specify a list of contiguous port numbers inside the firewall to which the rule applies. When selected, you can type the start and end ports into the fields, then click **Add** to add the ports to the port list.
- Select **Specify** and click **Port List** to select a predefined list of ports inside the firewall to which the rule applies. To use a port list with this rule, select the port list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.

12. From the **Protocol** list, select the protocol to which the firewall rule applies.
    - Select **Any** to apply the firewall rule to any protocol.
    - Select the protocol name to apply the rule to a single protocol.

    Important: *ICMP is handled by BIG-IP at the global or route domain level. Because of this, ICMP messages receive a response before they reach the virtual server context. You cannot create an inline rule for ICMP or ICMPv6 on a Self IP context. You can apply a rule list to a Self IP that includes a rule for ICMP or ICMPv6; however, such a rule will be ignored. To apply firewall actions to the ICMP protocol, create a rule with the* `global` *or* `route domain` *context. ICMP rules are evaluated only for ICMP forwarding requests, and not for the IP addresses of the BIG-IP itself.*

    Note: *Note that you must select a protocol if you specify ports.*

13. From the **Action** list, select the firewall action for traffic originating from the specified source address on the specified protocol. Choose from one of the these actions:

Option	Description
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.
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.

14. From the **Logging** list, enable or disable logging for the firewall rule.
15. Click **Finished**.
    The list screen is displayed, and the new item is displayed.

A new firewall rule is created, and appears in the Rules list.

Chapter 3

About Firewall Rule Addresses and Ports

About firewall rule addresses and ports

In a network firewall rule, you have several options for defining addresses and ports. You can use one or more of these options to configure the ports and addresses to which a firewall rule applies.

Note: *You can use any combination of inline addresses, ports, address lists, and port lists in a firewall rule.*

Any (address or port)

In both **Source** and **Destination** address and port fields, you can select **Any**. This specifies that the firewall rule applies to any address or port.

Inline addresses

An inline address is an IP address that you add directly to the network firewall rule, in either the **Source** or **Destination Address** field. Addresses can be either IPv4 or IPv6, depending on your network configuration.

Address Lists

An address list is a preconfigured list of IP addresses that you add directly to the BIG-IP® system. You can then select this list of addresses to use in either the **Source** or **Destination Address** field.

Inline ports

An inline port is a port that you add directly to the network firewall rule, in either the **Source** or **Destination Port** field. You can add a single port, or a contiguous port range.

Port lists

A port list is a preconfigured list of ports that you add directly to the BIG-IP system. You can then select this list of ports to use in either the **Source** or **Destination Port** field.

About address lists

An address list is simply a collection of IP addresses saved on the server. You can define one or more address lists, and you can select one or more address lists in a firewall rule. Firewall address lists can be used in addition to inline addresses, specified within a particular rule.

Creating an address list

Create an address list to apply to a firewall rule, in order to match IP addresses.

1. On the Main tab, click **Security** > **Network Firewall** > **Address Lists**.
   The Address Lists screen opens.
2. Click **Create** to create a new address list.
3. In the **Name** and **Description** fields, type the name and an optional description.
4. In the Addresses area, add and remove addresses.
   - To add an address, type the address and click **Add**.
   - To remove and address, select the address in the Addresses list and click **Delete**.

- To edit an address, select the address in the list and click **Edit**. The address is removed from the Addresses list and appears in the editing field. Make your changes to the address, and click **Add**.

5. Click **Finished**.
   The list screen is displayed, and the new item is displayed.

About port lists

A port list is simply a collection of port numbers saved on the server. You can define one or more port lists, and you can select one or more port lists in a firewall rule. Firewall port lists can be used in addition to inline ports, specified within a particular firewall rule.

Creating a port list

Create a port list to apply to a firewall rule, in order to match ports.

1. On the Main tab, click **Security** > **Network Firewall** > **Port Lists**.
   The Port Lists screen opens.
2. Click **Create** to create a new port list.
3. In the **Name** and **Description** fields, type the name and an optional description.
4. In the Ports area, add and remove ports.
   - To add a single port, select **Single Port**, then type the port number, and click **Add**.
   - To add a contiguous range of ports, select **Port Range**, then type the start and end port in the fields. Click **Add** to add the range of ports to the port list.
   - To remove and address, Select the address in the Addresses list and click **Delete**.
   - To edit a port entry, select the port or port range in the list and click **Edit**. The port or port range is removed from the Ports list and appears in the editing field. Make your changes to the port or range, and click **Add**.
5. Click **Finished**.
   The list screen is displayed, and the new item is displayed.

Chapter

4

About Network Firewall Schedules

About Network Firewall schedules

With a Network Firewall schedule, you can configure date ranges, days of the week, and time ranges for when a firewall rule is applied.

A schedule must be selected in a firewall rule or rule list, to apply to that firewall rule or rule list. The firewall rule or rule list must also be set to the **Scheduled** state.

When you configure a schedule for a rule list, the rules within the rule list can only be enabled when the rule list is enabled by the schedule. This means that even if the individual rules in a rule list have schedules, the rules are not enabled by their schedules unless the rule list is also enabled by the rule list schedule.

Creating a schedule

Create a schedule to define the times, dates, and days of the week for when a firewall rule is applied.

1. On the Main tab, click **Security** > **Network Firewall** > **Schedules**.
   The Schedules screen opens.
2. Click **Create** to create a new firewall schedule.
3. In the **Name** and **Description** fields, type the name and an optional description.
4. In the **Date Range** area, define the range of dates over which the schedule applies.
   - Select **Indefinite** to have the schedule apply immediately, and run indefinitely. This makes the schedule active until you change the date range, or delete the schedule.
   - Select **Until** to have the schedule apply immediately, and define an end date. This makes the schedule active now, and disables it when the end date is reached. Click in the field to choose an end date from a pop-up calendar.
   - Select **After** to have the schedule apply after the specified date, run indefinitely. This makes the schedule active starting on the selected date, until you change the start date, or delete the schedule. Click in the field to choose a start date from a pop-up calendar.
   - Select **Between** to apply the schedule starting on the specified start date, and ending on the specified end date. Click in the fields to choose the start and end dates from a pop-up calendar.
5. In the **Time Range** area, define the times over which the firewall rule applies.
   - Select **All Day** to have the schedule apply all day, for every day specified in the date range.
   - Select **Between** to apply the schedule starting at the specified time, and ending at the specified time each day. Select the start and end hours and minutes from the popup, or click **Now** to set the current time.

   Note: *Specify the hours according to a 24-hour clock. For example, you can specify 3:00 PM with the setting* `15`*.*
6. In the Days Valid area, select the days of the week when the schedule is valid. Select check boxes for days of the week when the rule applies, and clear check boxes for days of the week when the schedule does not apply.
7. Click **Finished**.
   The list screen is displayed, and the new item is displayed.

Chapter 5

About IP Address Intelligence in the Network Firewall

About IP intelligence in the network firewall

The network firewall checks traffic against an IP intelligence database to automatically handle traffic from known bad or questionable IP addresses. You can control the actions for each category of IP addresses in the network firewall.

IP address intelligence categories

Along with the IP address, the IP intelligence database stores the category that explains the reason that the IP address is considered untrustworthy.

Category	Description
Windows exploits	IP addresses that have exercised various exploits against Windows resources using browsers, programs, downloaded files, scripts, or operating system vulnerabilities.
Web attacks	IP addresses that have launched web attacks of various forms.
Botnets	IP addresses of computers that are infected with malicious software and are controlled as a group, and are now part of a botnet. Hackers can exploit botnets to send spam messages, launch various attacks, or cause target systems to behave in other unpredictable ways.
Scanners	IP addresses that have been observed to perform port scans or network scans, typically to identify vulnerabilities for later exploits.
Denial of Service	IP addresses that have launched Denial of Service (DoS) attacks. These attacks are usually requests for legitimate services, but occur at such a fast rate that targeted systems cannot respond and become bogged down or unable to service legitimate clients.
Infected Sources	IP addresses that issue HTTP requests with a low reputation index score, or are known malware sites.
Phishing	IP addresses that are associated with phishing web sites that masquerade as legitimate web sites.
Proxy	IP addresses that are associated with web proxies that shield the originator's IP address (such as anonymous proxies).

Configuring the firewall to check IP address reputations

You can verify IP reputation with the network firewall, and automatically allow or deny packets based on the reputation of the originating IP address.

1. On the Main tab, click **Security** > **Network Firewall** > **IP Intelligence**.
   The IP Intelligence screen opens.
2. Click **Create** to create a new IP Intelligence rule.
3. In the **Name** field, type a name for the IP intelligence profile.
4. From the **Parent Profile** list, select the parent profile on which the IP intelligence profile is to be based.
5. To configure any custom settings for the IP intelligence profile, next to **Settings**, click the **Custom** check box.

6. For each IP address intelligence category, you can select an action.
   - Select **Accept** to allow packets from sources of the specified type, as identified by the IP address intelligence database.
   - Select **Warn** to write a warning to the log and allow packets from sources of the specified type, as identified by the IP address intelligence database.
   - Select **Reject** to drop and send a reject message for packets from sources of the specified type, as identified by the IP address intelligence database.
7. Click **Finished**.
   The list screen is displayed, and the new item is displayed.

Chapter 6

About Local Logging with the Network Firewall

Overview: Configuring local Network Firewall event logging

You can configure the BIG-IP® system to log detailed information about BIG-IP system Network Firewall events and store those logs on the BIG-IP system.

Important: *The BIG-IP system Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure Network Firewall event logging.*

Task summary

Perform these tasks to configure Network Firewall logging locally on the BIG-IP® system.

Note: *Enabling logging and storing the logs locally impacts BIG-IP system performance.*

Creating a local Network Firewall Logging profile
Configuring an LTM virtual server for Network Firewall event logging
Viewing Network Firewall event logs locally on the BIG-IP system
Disabling logging

Creating a local Network Firewall Logging profile

Create a custom Logging profile to log BIG-IP® system Network Firewall events locally on the BIG-IP system.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.
   The New Logging Profile screen opens.
3. In the **Profile Name** field, type a unique name for the profile.
4. Select the **Network Firewall** check box.
5. In the Network Firewall area, from the **Publisher** list, select **local-db-publisher**.
6. For the **Log Rule Matches** setting, select how the BIG-IP system logs packets that match ACL rules.
   You can select any or all of the options.

Option	Description
Option	Enables or disables logging of packets that match ACL rules configured with:
Accept	`action=Accept`
Drop	`action=Drop`
Reject	`action=Reject`

7. Select the **Log IP Errors** check box, to enable logging of IP error packets.
8. Select the **Log TCP Errors** check box, to enable logging of TCP error packets.
9. Select the **Log TCP Events** check box, to enable logging of open and close of TCP sessions.

10. In the IP Intelligence area, from the **Publisher** list, select **local-db-publisher**.

    Note: *The IP Address Intelligence feature must be enabled and licensed.*

11. Click **Finished**.

Assign this custom Network Firewall Logging profile to a virtual server.

Configuring an LTM virtual server for Network Firewall event logging

Ensure that at least one log publisher exists on the BIG-IP® system.

Assign a custom Network Firewall Logging profile to a virtual server when you want the BIG-IP system to log Network Firewall events on the traffic that the virtual server processes.

Note: *This task applies only to LTM®-provisioned systems.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays Policy Settings and Inline Rules settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

Viewing Network Firewall event logs locally on the BIG-IP system

Ensure that the BIG-IP® system is configured to log the types of events you want to view, and to store the log messages locally on the BIG-IP system.

When the BIG-IP system is configured to log events locally, you can view those events using the Configuration utility.

1. On the Main tab, click **Security** > **Event Logs** > **Network** > **Firewall**.
   The Network Firewall event log displays.
2. To search for specific events, click **Custom Search**. Drag the event data that you want to search for from the Event Log table into the Custom Search table, and then click **Search**.

Disabling logging

Disable Network Firewall, Protocol Security, or DoS Protection event logging when you no longer want the BIG-IP® system to log specific events on the traffic handled by specific resources.

Note: *You can disable and re-enable logging for a specific resource based on your network administration needs.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.

2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays Policy Settings and Inline Rules settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save the changes.

The BIG-IP system does not log the events specified in this profile for the resources to which this profile is assigned.

Implementation result

You now have an implementation in which the BIG-IP® system logs specific Network Firewall events and stores the logs in a local database on the BIG-IP system.

Chapter 7

About Remote High-Speed Logging with the Network Firewall

Overview: Configuring remote high-speed Network Firewall event logging

You can configure the BIG-IP® system to log information about the BIG-IP system Network Firewall events and send the log messages to remote high-speed log servers.

Important: *The BIG-IP system Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure Network Firewall event logging.*

When configuring remote high-speed logging of Network Firewall events, it is helpful to understand the objects you need to create and why, as described here:

Object to create in implementation	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging profile	Create a custom Logging profile to enable logging of user-specified data at a user-specified level, and associate a log publisher with the profile.
LTM® virtual server	Associate a custom Logging profile with a virtual server to define how the BIG-IP system logs security events on the traffic that the virtual server processes.

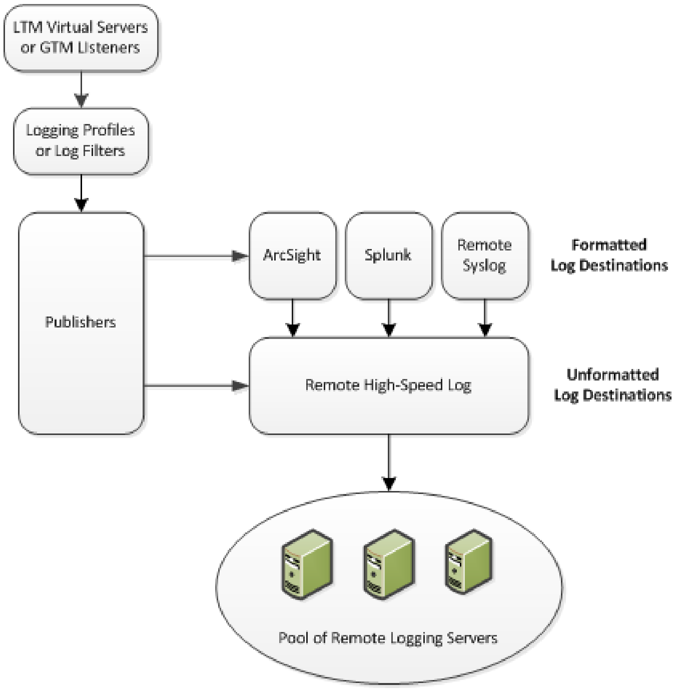

LTM Virtual Servers or GTM Listeners
Logging Profiles or Log Filters
Publishers
ArcSight
Splunk
Remote Syslog
Formatted Log Destinations
Remote High-Speed Log
Unformatted Log Destinations
Pool of Remote Logging Servers

Figure 2: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure remote high-speed network firewall logging on the BIG-IP® system.

***Note:** Enabling remote high-speed logging impacts BIG-IP system performance.*

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a custom Network Firewall Logging profile
Configuring an LTM virtual server for Network Firewall event logging
Disabling logging

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:

a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
b) Type a service number in the **Service Port** field, or select a service name from the list.

__Note:__ Typical remote logging servers require port `514`.

c) Click **Add**.

5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. This allows the BIG-IP system to send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select a formatted logging destination, such as **Remote Syslog**, **Splunk**, or **ArcSight**.

   Important: *ArcSight formatting is only available for logs coming from the network Application Firewall Manager (AFM) and the Application Security Manager (ASM™).*

The BIG-IP system is configured to send a formatted string of text to the log servers.

5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.
6. If you selected **Splunk** or **ArcSight**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating a custom Network Firewall Logging profile

Create a custom Logging profile to log messages about BIG-IP® system Network Firewall events.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.
   The New Logging Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. Select the **Network Firewall** check box.
5. In the Network Firewall area, from the **Publisher** list, select the Publisher the BIG-IP system uses to log Network Firewall events.
6. For the **Log Rule Matches** setting, select how the BIG-IP system logs packets that match ACL rules. You can select any or all of the options.

Option	Description
Option	Enables or disables logging of packets that match ACL rules configured with:
Accept	`action=Accept`
Drop	`action=Drop`
Reject	`action=Reject`

7. Select the **Log IP Errors** check box, to enable logging of IP error packets.
8. Select the **Log TCP Errors** check box, to enable logging of TCP error packets.
9. Select the **Log TCP Events** check box, to enable logging of open and close of TCP sessions.
10. From the **Storage Format** list, select how the BIG-IP system formats the log. Your choices are:

Option	Description

None	Specifies the default format type in which the BIG-IP system logs messages to a remote Syslog server, for example:
	`"management_ip_address","bigip_hostname","context_type",`
	`"context_name","src_ip","dest_ip","src_port",`
	`"dest_port","vlan","protocol","route_domain",`
	`"acl_rule_name","action","drop_reason`

Field-List	This option allows you to: • Select from a list, the fields to be included in the log. • Specify the order the fields display in the log. • Specify the delimiter that separates the content in the log. The default delimiter is the comma character
User-Defined	This option allows you to: • Select from a list, the fields to be included in the log. • Cut and paste, in a string of text, the order the fields display in the log.

11. In the IP Intelligence area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log source IP addresses, which according to an IP Address Intelligence database have a bad reputation, and the name of the bad reputation category.

    Note: *The IP Address Intelligence feature must be enabled and licensed.*

12. Click **Finished**.

Assign this custom network firewall Logging profile to a virtual server.

Configuring an LTM virtual server for Network Firewall event logging

Ensure that at least one log publisher exists on the BIG-IP® system.

Assign a custom Network Firewall Logging profile to a virtual server when you want the BIG-IP system to log Network Firewall events on the traffic that the virtual server processes.

Note: *This task applies only to LTM®-provisioned systems.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays Policy Settings and Inline Rules settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

Disabling logging

Disable Network Firewall, Protocol Security, or DoS Protection event logging when you no longer want the BIG-IP® system to log specific events on the traffic handled by specific resources.

Note: *You can disable and re-enable logging for a specific resource based on your network administration needs.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays Policy Settings and Inline Rules settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save the changes.

The BIG-IP system does not log the events specified in this profile for the resources to which this profile is assigned.

Implementation result

You now have an implementation in which the BIG-IP® system logs specific Network Firewall events and sends the logs to a remote log server.

Chapter 8

Deploying the BIG-IP Network Firewall in ADC Mode

About deploying the network firewall in ADC mode

The BIG-IP® Network Firewall provides policy-based access control to and from address and port pairs inside and outside of your network. By default the network firewall is configured in ADC mode, which is a *default allow* configuration, in which all traffic is allowed through the firewall, and any traffic you want to block must be explicitly specified.

To understand this firewall scenario, imagine that your prerequisite system load-balances all traffic from the internet to several internal servers. The internal servers are:

Device and location	IP address	Traffic type
Externally accessible FTP server	70.168.15.104	FTP
Application virtual server	192.168.15.101	HTTP, FTP
Server on internal network	10.10.1.10	HTTP, HTTPS
Server on internal network	10.10.1.11	HTTP, HTTPS

The system does not have a separate route domain configured, however you can use Route Domain 0, which is essentially the same as a global rule.

In order for traffic from the internal application virtual server to reach the external network virtual server, you must create a VLAN and enable both internal and external virtual servers on it. In this scenario, these VLANs are specified:

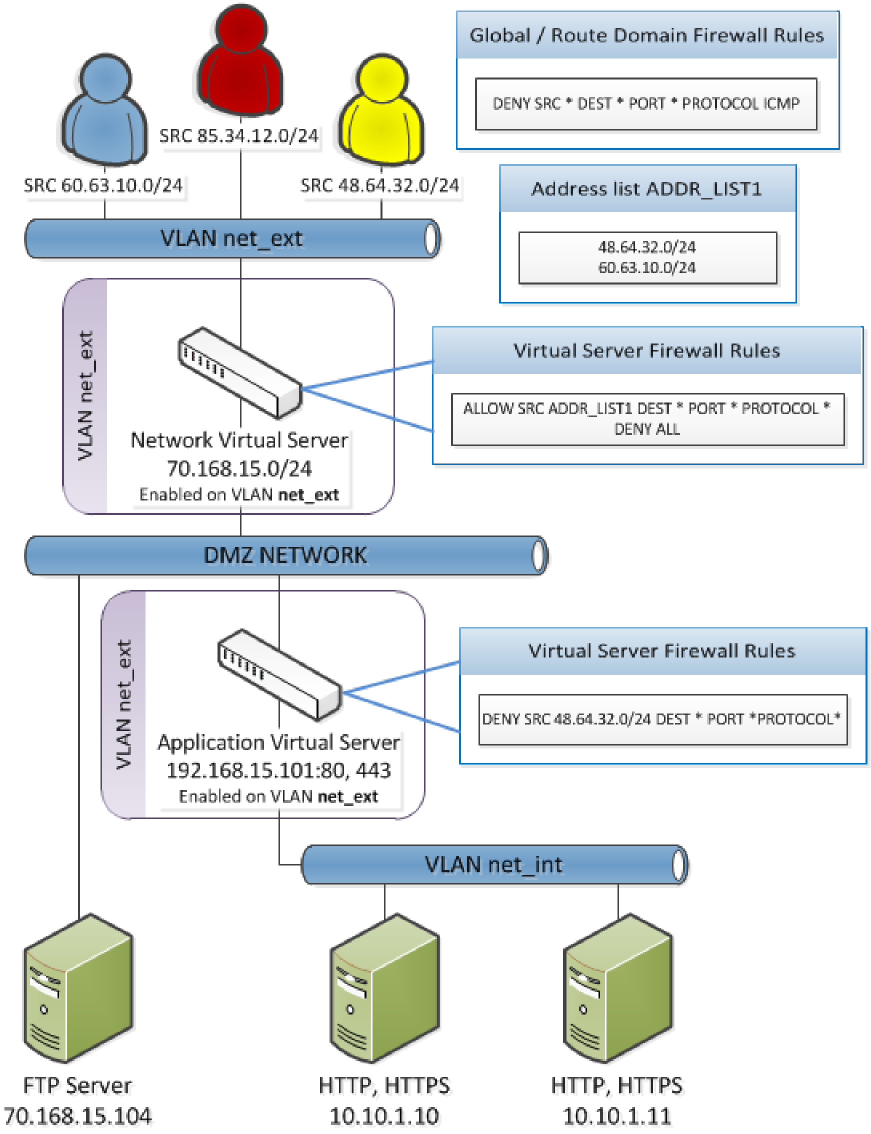
VLAN	Configuration
net_ext	Enabled on 70.168.15.0/24, 192.168.15.101
net_int	Includes pool members 10.10.1.10, 10.10.1.11

In addition, in this firewall configuration, there are three external networks that must be firewalled:

Network	Policy
60.63.10.0/24	Allow all access
85.34.12.0/24	Deny all access
48.64.32.0/24	Allow FTP, deny HTTP and HTTPS

To set up this scenario, you configure addresses, ports, and firewall rules specific to these networks, ports, and addresses. You will also configure a firewall rule that denies all ICMP traffic, to prevent pinging of network devices.

Figure 3: Firewall in ADC mode configuration scenario



Configuring the Network Firewall in ADC mode

Use this task to configure the BIG-IP®Network Firewall in ADC mode.

Note: *The firewall is configured by default in ADC mode. Use this task to set the firewall back to ADC mode if you have changed the firewall setting to Firewall mode.*

1. On the Main tab, click **Security** > **Options** > **Network Firewall**.
   The Firewall Options screen opens.
2. From the **Virtual Server & Self IP Contexts** list, select the default action **Accept** for the self IP and virtual server contexts.
3. Click **Update**.
   The virtual server and self IP contexts for the firewall are changed.

Creating a VLAN for the network firewall

Create a VLAN with tagged interfaces, so that each of the specified interfaces can process traffic destined for that VLAN.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN.

   For purposes of this implementation, name the VLAN `net_ext`.
4. For the **Interfaces** setting, click an interface number or trunk name from the **Available** list, and use the Move button to add the selected interface or trunk to the **Tagged** list. Repeat this step as necessary.

   You can use the same interface for other VLANs later, if you always assign the interface as a tagged interface.
5. Select the **Source Check** check box if you want the system to verify that the return route to an initial packet is the same VLAN from which the packet originated.
6. In the **MTU** field, retain the default number of bytes (**1500**).
7. If you want to base redundant-system failover on VLAN-related events, select the **Fail-safe** box.
8. Click **Finished**.
   The screen refreshes, and displays the new VLAN in the list.

The new VLAN appears in the VLAN list.

Enable the new VLAN on both the network virtual server and the application virtual server.

Configuring an LTM virtual server with a VLAN for Network Firewall

For this implementation, at least two virtual servers and one at least one VLAN are assumed, though your configuration might be different.

You enable two virtual servers on the same VLAN to allow traffic from hosts on one virtual server to reach or pass through the other. In the Network Firewall, if you are using multiple virtual servers to allow or deny traffic to and from specific hosts behind different virtual servers, you must enable those virtual servers on the same VLAN.

Tip: *By default, the virtual server is set to share traffic on* ***All VLANs and Tunnels****. This configuration will work for your VLANs, but in the firewall context specifying or limiting VLANs that can share traffic provides greater security.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. From the **VLAN and Tunnel Traffic** list, select **Enabled on**. Then, for the **VLANs and Tunnels** setting, move the VLAN or VLANs on which you want to allow the virtual servers to share traffic from the **Available** list to the **Selected** list.
4. Click **Update** to save the changes.
5. Repeat this task for all virtual servers that must share traffic over the VLAN.

The virtual servers on which you enabled the same VLAN can now pass traffic.

Adding a firewall rule to deny ICMP

Use this task to create a firewall rule at the Global context, that denies ICMP packets globally.

1. On the Main tab, click **Security** > **Network Firewall** > **Active Rules**.
   The Active Rules screen opens.
2. In the Active Network Firewall Rules area, click **Add** to add a firewall rule to the list.
3. From the **Context** list, select the **Global** context.
4. In the **Name** field, type **deny_icmp**.
5. From the **Type** list, select **Rule**.
6. From the **State** list, select **Enabled**.
7. From the Protocol list, select **ICMP**.
8. In the **ICMP Message** area, from the **Type** list, select `Any`, and click the **Add** button.

   Tip: *You can optionally deny only ICMP ping requests, by selecting* `Echo (8)` *from the* ***Type*** *list, and clicking* ***Add****.*

9. Leave the **Source** area configured to allow **Any** address, port, and VLAN.
10. Leave the **Destination** area configured to allow **Any** address or port.
11. From the **Action** list, select **Drop** or **Reject**.
    These options either drop ICMP packets from any source and port to any port and address, or send a reject message and reset the the connection.
12. From the **Logging** list, enable or disable logging for the firewall rule.
13. Click **Finished**.
    The list screen is displayed, and the new item is displayed.

A new firewall rule is created, and appears in the firewall rule list. This firewall rule denies all access to and from all sources and destinations on the ICMP protocol.

Creating an address list

Use this procedure to specify the address list to apply to allow access to specific source addresses.

1. On the Main tab, click **Security** > **Network Firewall** > **Address Lists**.
   The Address Lists screen opens.
2. Click **Create** to create a new address list.
3. In the name field, type `ADDR_LIST1`.
4. In the Addresses area, add the following addresses: `48.63.32.0/24` and `60.63.10.0/24`. Click **Add** after you type each address.
5. Click **Finished**.
   The list screen is displayed, and the new item is displayed.

Denying access with firewall rules on the network virtual server

The firewall rules in this example apply in the virtual server context. For purposes of this example, the external network-facing virtual server has an IP address of `70.168.15.0/24`. The network virtual server is configured with a pool that includes a publically accessible FTP server at `70.168.15.104`, and an application virtual server at `192.168.15.101`.

Use this task to create a firewall rule that allows all traffic from the networks on the address list ADDR_LIST1, and another firewall rule that denies all traffic. This serves the purpose of allowing all traffic from the networks that are allowed access, and denying all other traffic.

1. On the Main tab, click **Security** > **Network Firewall** > **Active Rules**.
   The Active Rules screen opens.
2. In the Active Network Firewall Rules area, click **Add** to add a firewall rule to the list.
3. Select the **Virtual Server** context, then select the external network virtual server (in this example, `70.168.15.0/24`).
4. In the **Name** field, type `allow_addr_list`.
5. From the **Type** list, select **Rule**.
6. From the **State** list, select **Enabled**.
7. From the Protocol list, select **Any**.
8. In the **Source** area, from the **Address** list, select **List**.
9. From the **Source Available** list, select `ADDR_LIST1`, then click the **<<** button to move `ADDR_LIST1` to the **Selected** list.
10. Leave the **Destination** area configured with the default **Any** / **Any** settings.
11. From the **Action** list, select **Accept**.
    This allows packets from any source on the list to the any destination and port on any protocol on the DMZ network.
12. From the **Logging** list, enable or disable logging for the firewall rule.
13. Click the **Repeat** button.
    The rule is saved, and a new rule creation page opens, with the same information, so you can create a similar rule.
14. In the **Name** field, type `deny_all`.
15. In the **Source** area, in the **Address** list, select **Any**.
16. Leave the **Destination** area configured to deny access to **Any** address or port.
17. From the **Action** list, select **Reject**.
    This creates a deny all rule for the virtual server.
18. From the **Logging** list, enable or disable logging for the firewall rule.
19. Click **Finished**.
    The list screen is displayed, and the new item is displayed.
20. From the **Context** list, select **Virtual Server**.
21. From the **Virtual Server** list, select the network virtual server.
22. Click the **Filter** button.

The list screen opens, and all firewall rules that apply to the virtual server are displayed.

Denying access with firewall rules on the application virtual server

The firewall rules in this example apply in the virtual server context. For purposes of this example, the application virtual server on the internal network has an IP address of `192.168.15.101`, and is configured to load balance traffic to servers `10.10.1.10` and `10.10.1.11` on ports `80` and `443`.

Use this task to create a firewall rule that denies all traffic from the network `48.64.32.0/24` to the internal application servers behind the virtual server **192.168.15.101**.

1. On the Main tab, click **Security** > **Network Firewall** > **Active Rules**.
   The Active Rules screen opens.
2. In the Active Network Firewall Rules area, click **Add** to add a firewall rule to the list.
3. Select the **Virtual Server** context, then select the application virtual server (in this example, `192.168.15.101`).
4. In the **Name** field, type deny_network_48
5. From the **Type** list, select **Rule**.
6. From the **State** list, select **Enabled**.
7. From the **Schedule** list, select **None**.
8. From the Protocol list, select **Any**.
9. In the **Source** area, from the **Address** list, select **Specify**.
10. In the address field, type `48.64.32.0/24`.
11. Leave the **Destination** area configured to deny access to **Any** address or port.
12. From the **Action** list, select **Drop** or **Reject**.
    This drops packets from the `48.64.32.0` network to any source.
13. From the **Logging** list, enable or disable logging for the firewall rule.
14. Click **Finished**.
    The list screen is displayed, and the new item is displayed.
15. From the **Context** list, select **Virtual Server**.
16. From the **Virtual Server** list, select the application virtual server.
17. Click the **Filter** button.

The firewall rules are created, and are displayed on the list screen for the application virtual server.

Chapter 9

Deploying the BIG-IP Network Firewall in Firewall Mode

About Firewall mode in the Network Firewall

The BIG-IP® Advanced Firewall Manager™ (AFM™) provides policy-based access control to and from address and port pairs, inside and outside of your network. In this scenario, the network firewall is configured in *Firewall mode*, a default deny configuration, in which all traffic is blocked through the firewall, and any traffic you want to allow must be explicitly specified.

To understand this firewall scenario, imagine that your prerequisite system load-balances all traffic from the Internet to several internal servers. The internal servers are:

Device and location	IP address	Traffic type
Server on DMZ network	70.168.15.104	FTP
Server on internal network	10.10.1.10	HTTP, HTTPS
Server on internal network	10.10.1.11	HTTP, HTTPS

In order for traffic from the internal application virtual server to reach the external network virtual server, you must create a VLAN and enable both internal and external virtual servers on it. In this scenario, these VLANs are specified:

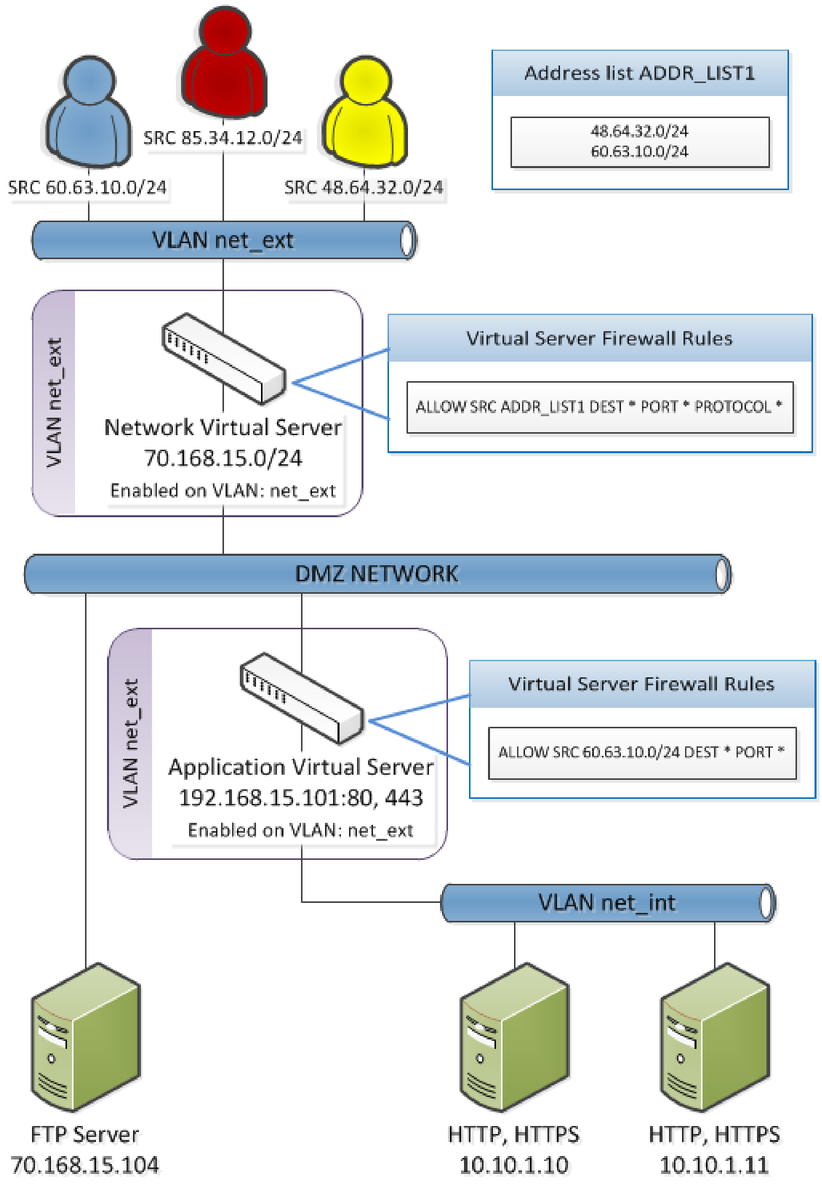
VLAN	Configuration
net_ext	Enabled on 70.168.15.0/24, 192.168.15.101
net_int	Includes pool members 10.10.1.10, 10.10.1.11

In addition, in this firewall configuration, there are three external networks that must be firewalled:

Network	Policy
60.63.10.0/24	Allow all access
85.34.12.0/24	Deny all access
48.64.32.0/24	Allow FTP, deny HTTP and HTTPS

To set up this scenario, you configure addresses, ports, and firewall rules specific to these networks, ports, and addresses.

Figure 4: Firewall configuration scenario



Configuring the Network Firewall to drop traffic that is not specifically allowed

Use this procedure to configure the BIG-IP® Network Firewall to deny all traffic not explicitly allowed. In the Advanced Firewall Manager this is called *Firewall mode*, and this is also referred to as a *default deny* policy. Firewall mode applies a default deny policy to all self IPs and virtual servers.

1. On the Main tab, click **Security** > **Options** > **Network Firewall**.
   The Firewall Options screen opens.
2. From the **Virtual Server & Self IP Contexts** list, select the default action **Drop** for the self IP and virtual server contexts.
3. Click **Update**.
   The default Virtual Server and Self IP firewall context is changed.

If you are using ConfigSync to synchronize two or more devices, and you set the default action to Drop or Reject, you must apply the built-in firewall rules `_sys_self_allow_defaults` or `_sys_self_allow_management` to the specific self IPs that are used to support those services. To do this, add a new rule with the **Self IP** context, select the Self IP, and select the **Rule List** rule type. Select the preconfigured rules from the list of rule lists.

Creating a VLAN for the network firewall

Create a VLAN with tagged interfaces, so that each of the specified interfaces can process traffic destined for that VLAN.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type a unique name for the VLAN.

   For purposes of this implementation, name the VLAN `net_ext`.
4. For the **Interfaces** setting, click an interface number or trunk name from the **Available** list, and use the Move button to add the selected interface or trunk to the **Tagged** list. Repeat this step as necessary.

   You can use the same interface for other VLANs later, if you always assign the interface as a tagged interface.
5. Select the **Source Check** check box if you want the system to verify that the return route to an initial packet is the same VLAN from which the packet originated.
6. In the **MTU** field, retain the default number of bytes (**1500**).
7. If you want to base redundant-system failover on VLAN-related events, select the **Fail-safe** box.
8. Click **Finished**.
   The screen refreshes, and displays the new VLAN in the list.

The new VLAN appears in the VLAN list.

Enable the new VLAN on both the network virtual server and the application virtual server.

Configuring an LTM virtual server with a VLAN for Network Firewall

For this implementation, at least two virtual servers and one at least one VLAN are assumed, though your configuration might be different.

You enable two virtual servers on the same VLAN to allow traffic from hosts on one virtual server to reach or pass through the other. In the Network Firewall, if you are using multiple virtual servers to allow or deny traffic to and from specific hosts behind different virtual servers, you must enable those virtual servers on the same VLAN.

Tip: *By default, the virtual server is set to share traffic on* ***All VLANs and Tunnels****. This configuration will work for your VLANs, but in the firewall context specifying or limiting VLANs that can share traffic provides greater security.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.

3. From the **VLAN and Tunnel Traffic** list, select **Enabled on**. Then, for the **VLANs and Tunnels** setting, move the VLAN or VLANs on which you want to allow the virtual servers to share traffic from the **Available** list to the **Selected** list.
4. Click **Update** to save the changes.
5. Repeat this task for all virtual servers that must share traffic over the VLAN.

The virtual servers on which you enabled the same VLAN can now pass traffic.

Creating an address list

Use this procedure to specify the address list to apply to allow access to specific source addresses.

1. On the Main tab, click **Security** > **Network Firewall** > **Address Lists**.
   The Address Lists screen opens.
2. Click **Create** to create a new address list.
3. In the name field, type `ADDR_LIST1`.
4. In the Addresses area, add the following addresses: `48.63.32.0/24` and `60.63.10.0/24`. Click **Add** after you type each address.
5. Click **Finished**.
   The list screen is displayed, and the new item is displayed.

Allowing access from networks on an address list with a firewall rule

The firewall rules in this example apply in the virtual server context. For purposes of this example, the external network-facing virtual server is named `ex_VS` and has an IP address of `70.168.15.0/24`.

Create a firewall rule that allows traffic from the networks on `ADDR_LIST1` to the DMZ network, which includes an FTP server that is publicly addressed, and two internal servers on a second virtual server.

1. On the Main tab, click **Security** > **Network Firewall** > **Active Rules**.
   The Active Rules screen opens.
2. In the Active Network Firewall Rules area, click **Add** to add a firewall rule to the list.
3. From the **Context** list, select **Virtual Server**, and then select the external virtual server (in the example, **ex_VS**).
4. In the **Name** field, type `allow_addr_list`.
5. From the **Type** list, select **Rule**.
6. From the **State** list, select **Enabled**.
7. From the **Protocol** list, select **Any**.
8. In the Source area, from the **Address** list, select **Specify**, and click **Address List**.
9. From the list, select **/Common/ADDR_LIST1**, then click **Add** to add **ADDR_LIST1** to the list.
10. Leave the **Destination** area configured with the default **Any** / **Any** settings.
11. From the **Action** list, select **Accept**.
    This allows packets from any source on the list to the any destination and port on any protocol on the DMZ network.
12. From the **Logging** list, enable or disable logging for the firewall rule.

13. Click **Finished**.
    The list screen is displayed, and the new item is displayed.

A new firewall rule is created, and appears in the firewall rule list.

Allowing access from a network to a virtual server with a firewall rule

The firewall rules in this example apply in the virtual server context. For purposes of this example, the application virtual server is behind the network virtual server with an IP address of `192.168.15.101` and configured for traffic on ports 80 and 443.

Use this procedure to create a firewall rule that allows traffic from a specific external network to the HTTP and HTTPS servers behind an application virtual server.

1. On the Main tab, click **Security** > **Network Firewall** > **Active Rules**.
   The Active Rules screen opens.
2. In the Active Network Firewall Rules area, click **Add** to add a firewall rule to the list.
3. In the Context field, select `Virtual Server`, and select the application virtual server (in the example, `192.168.15.101`.
4. In the **Name** field, type `allow_app_vs`.
5. From the **Type** list, select **Rule**.
6. From the **State** list, select **Enabled**.
7. From the Protocol list, select **Any**.
8. In the **Source** area, from the **Address** list, select **Specify**.
9. In the address field, type `60.63.10.0/24`, then click the **Add** button.
10. Leave the **Destination** area configured with the default **Any** / **Any** settings.
11. From the **Action** list, select **Accept**.
    This allows packets from the specified source to any destination and port on any protocol on the internal virtual server. You could specify HTTP and HTTPS protocols, and the internal server addresses, but since these are the only addresses and protocols behind the virtual server, that level of granularity is not necessary.
12. From the **Logging** list, enable or disable logging for the firewall rule.
13. Click **Finished**.
    The list screen is displayed, and the new item is displayed.

A new firewall rule is created, and appears in the firewall rule list.

Chapter 10

Configuring BIG-IP Network Firewall Policies

About firewall policies

The BIG-IP® Network Firewall policies combine one or more inline rules or rule lists, and apply them as a combined policy to one or more contexts. Such policies are applied to a context directly, and cannot coexist in that context with inline rules. You can configure a context to use either a specific firewall policy or inline rules, but not both. A firewall policy and inline rules are mutually exclusive of each other. However, firewall context precedence does apply, so inline rules at the global context, for example, apply even if they contradict rules applied at a lower precedence context; for example, at a virtual server.

You can apply a network firewall policy as a staged policy, while continuing to enforce existing inline rules, or you can apply one firewall policy while staging another policy. A *staged policy* allows you to evaluate the effect a policy has on traffic by analyzing the system logs, without actually modifying traffic based on the firewall rules.

Creating a Network Firewall policy

Use this procedure to create a BIG-IP® Network Firewall policy.

1. On the Main tab, click **Security** > **Network Firewall** > **Policies**.
   The Policies screen opens.
2. Click **Create** to create a new policy.
3. Type a name and optional description for the firewall policy.
4. Click **Finished**.

The Policies screen shows the new policy in the policy list.

Define firewall rules for the policy to make it function.

Creating a Network Firewall policy rule

If you are going to specify address lists or port lists to use with this rule, you must create these lists before creating the firewall policy rule, or add them after you save the policy rule.

Create a network firewall policy rule to manage access from an IP or web network address to a specified network location, server, or address behind a BIG-IP® system.

***Note:** You cannot add rules created with this task to a rule list at a later time. You must create rules for a rule list from within the rule list. Similarly, you cannot use the rules created in a policy to apply as inline rules in another context, though you can use rule lists in a policy rule.*

1. On the Main tab, click **Security** > **Network Firewall** > **Policies**.
   The Policies screen opens.
2. Click the name of the network firewall policy to which you want to add rules.
3. In the Active Network Firewall Rules area, click **Add** to add a firewall rule to the list.
4. In the **Name** and **Description** fields, type the name and an optional description.
5. From the **Type** list, select whether you are creating a standalone network firewall policy rule or creating the rule from a predefined rule list.

   If you create a firewall policy rule from a predefined rule list, most options for creating a firewall policy rule do not apply.

6. From the **State** list, select the rule state.
   - Select **Enabled** to apply the firewall policy rule to the addresses and ports specified.
   - Select **Disabled** to set the firewall policy rule to not apply at all.
   - Select **Scheduled** to apply the firewall policy according to the selected schedule.
7. From the **Schedule** list, select the schedule for the firewall policy rule.

   This schedule is applied when the firewall policy rule state is set to **Scheduled**.
8. From the **Protocol** list, select the protocol to which the firewall rule applies.
   - Select **Any** to apply the firewall rule to any protocol.
   - Select the protocol name to apply the rule to a single protocol.

   Important: *ICMP is handled by BIG-IP at the global or route domain level. Because of this, ICMP messages receive a response before they reach the virtual server context. You cannot create an inline rule for ICMP or ICMPv6 on a Self IP context. You can apply a rule list to a Self IP that includes a rule for ICMP or ICMPv6; however, such a rule will be ignored. To apply firewall actions to the ICMP protocol, create a rule with the* `global` *or* `route domain` *context. ICMP rules are evaluated only for ICMP forwarding requests, and not for the IP addresses of the BIG-IP itself.*

   Note: *Note that you must select a protocol if you specify ports.*
9. From the Source **Address** list, select the type of source address to which this rule applies.
   - Select **Any** to have the rule apply to any IP address outside the firewall.
   - Select **Specify** and click **Address** to specify one or more IP addresses outside the firewall to which the rule applies. When selected, you can type single IP addresses into the **Address** field, then click **Add** to add them to the address list.
   - Select **Specify** and click **Address List** to select a predefined list of addresses outside the firewall to which the rule applies. To use an address list with this rule, select the address list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.
10. From the Source **Port** list, select the type of source ports (outside the firewalled network) to which this rule applies.
    - Select **Any** to have the rule apply to any port outside the firewall.
    - Select **Specify** and click **Port** to specify one or more ports outside the firewall to which the rule applies. When selected, you can type single port numbers into the **Port** field, then click **Add** to add them to the port list.
    - Select **Specify** and click **Port List** to specify a list of contiguous port numbers outside the firewall to which the rule applies. When selected, you can type the start and end ports into the fields, then click **Add** to add the ports to the port list.
    - Select **Specify** and click **Port List** to select a predefined list of ports outside the firewall to which the rule applies. To use a port list with this rule, select the port list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.
11. From the Source **VLAN** list, select the VLAN on which this rule applies.
    - Select **Any** to have the rule apply to traffic on any VLAN through which traffic enters the firewall.
    - Select **Specify** to specify one or more VLANs on the firewall to which the rule applies. To use a VLAN with this rule, move the VLAN from the **Available** list to the **Selected** list by clicking the << button. Similarly, to remove the VLAN from this rule, click the >> button to move the VLAN from the **Selected** list to the **Available** list.
12. From the Destination **Address** list, select the type of destination address, behind the firewall, to which this rule applies.

- Select **Any** to have the rule apply to any IP address inside the firewall.
- Select **Specify** and click **Address** to specify one or more IP addresses inside the firewall to which the rule applies. When selected, you can type single IP addresses into the **Address** field, then click **Add** to add them to the address list.
- Select **Specify** and click **Address List** to select a predefined list of addresses inside the firewall to which the rule applies. To use an address list with this rule, select the address list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.

13. From the Destination **Port** list, select the type of destination ports, behind the firewall or inside the firewalled networks, to which this rule applies.
    - Select **Any** to have the rule apply to any port inside the firewall.
    - Select **Specify** and click **Port** to specify one or more ports inside the firewall to which the rule applies. When selected, you can type single port numbers into the **Port** field, then click **Add** to add them to the port list.
    - Select **Specify** and click **Port List** to specify a list of contiguous port numbers inside the firewall to which the rule applies. When selected, you can type the start and end ports into the fields, then click **Add** to add the ports to the port list.
    - Select **Specify** and click **Port List** to select a predefined list of ports inside the firewall to which the rule applies. To use a port list with this rule, select the port list and click the **Add** button. Similarly, to remove the list from this rule, select the list and click the **Delete** button.
14. From the **Action** list, select the firewall action for traffic originating from the specified source address on the specified protocol. Choose from one of the these actions:

Option	Description
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.
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.

15. From the **Logging** list, enable or disable logging for the firewall rule.
16. Click **Finished**.
    The list screen is displayed, and the new item is displayed.

The new firewall policy rule is created.

Setting a global firewall policy

You can create a virtual server with a firewall policy, to provide policy-based network firewall actions at the virtual server.

1. On the Main tab, click **Security** > **Network Firewall** > **Active Rules**.
   The Active Rules screen opens.

2. Under **Active Network Firewall Rules**, click the **Global** link.
   The **Global Firewall Rules** screen opens.
3. To enforce rules from a firewall policy in the selected context, in the Network Firewall area, from the **Enforcement** list, select **Policy Rules**, then select the firewall policy to enforce from the **Policy** list.
4. To stage rules from a firewall policy in the selected context, in the Network Firewall area, from the **Staging** list, select **Enabled**, then select the firewall policy to stage from the **Policy** list.

The policy rules you selected are enforced at the global level. If you chose to stage policy rules, the results of those rules are logged, but not enforced.

Configuring a route domain with a firewall policy

This task requires a pre-existing route domain.

On a route domain, you can set firewall policies for enforcement and staging. Use this task to set firewall policies on an existing route domain. You create a route domain on BIG-IP® system to segment (isolate) traffic on your network. Route domains are useful for multi-tenant configurations.

1. On the Main tab, click **Network** > **Route Domains**.
   The Route Domain List screen opens.
2. Click the name of the route domain to show the route domain configuration.
3. Click on the **Security** tab.
4. To enforce rules from a firewall policy on the route domain, in the Network Firewall area, from the **Enforcement** list, select **Policy Rules**, then select the firewall policy to enforce from the **Policy** list.
5. To stage rules from a firewall policy on the route domain, in the Network Firewall area, from the **Staging** list, select **Enabled**, then select the firewall policy to stage from the **Policy** list.
6. To enforce any inline rules that apply to the route domain, and not apply a firewall policy, in the Network Firewall area, from the **Enforcement** list, select **Inline Rules**.
7. Click **Update** to save the changes to the route domain.

You now have configured a route domain on the BIG-IP system, with either firewall policies or inline rules enforced at the route domain context.

Setting network firewall policies for a self IP address

Ensure that you have created a self IP address.

You can configure network firewall rules at a self IP address by inline rule, or you can enforce a firewall policy. You can also stage a firewall policy to check the effect without affecting traffic.

1. On the Main tab, click **Network** > **Self IPs**.
   The Self IPs screen opens.
2. Click on the self IP address to which you want to add a network firewall policy.
3. Click the **Security** tab.
4. To enforce rules from a firewall policy on the self IP, in the Network Firewall area, from the **Enforcement** list, select **Policy Rules**, then select the firewall policy to enforce from the **Policy** list.
5. To stage rules from a firewall policy on the self IP, in the Network Firewall area, from the **Staging** list, select **Enabled**, then select the firewall policy to stage from the **Policy** list.
6. To enforce any inline rules that apply to the self IP, and not apply a firewall policy, in the Network Firewall area, from the **Enforcement** list, select **Inline Rules**.

7. Click **Update** to save the changes to the self IP.

The selected self IP now enforces or stages rules according to your selections.

Creating a virtual server with a firewall policy

You can create a virtual server with a firewall policy, to provide policy-based network firewall actions at the virtual server.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, in the **Address** field, type the IP address you want to use for the virtual server.

   The IP address you type must be available and not in the loopback network.
5. In the **Service Port** field, type `*` or select *** All Ports** from the list.
6. Click **Finished**.
7. Click the name of the virtual server you want to modify.
8. On the menu bar, click **Security** > **Policies**.
   The screen displays Policy Settings and Inline Rules settings.
9. To enforce rules from a firewall policy on the virtual server, in the Network Firewall area, from the **Enforcement** list, select **Policy Rules**, then select the firewall policy to enforce from the **Policy** list.
10. To stage rules from a firewall policy on the virtual server, in the Network Firewall area, from the **Staging** list, select **Enabled**, then select the firewall policy to stage from the **Policy** list.
11. Click **Update** to save the changes.

The policy rules you selected are enforced on the virtual server. If you chose to stage policy rules, the results of those rules are logged, but not enforced.

Viewing enforced and staged policy rule logs

With BIG-IP® Advanced Firewall Manager™, you can choose to enforce either inline firewall rules or a firewall policy for a specific context. You can also choose to stage policies for a specific context. *Staged policies* apply all of the specified firewall rules to the policy context, but do not enforce the firewall action. Therefore, the result of a staged policy is informational only, and the result can be analyzed in the firewall logs. This topic describes how to view and search for enforced and staged policy rules in the local network firewall logs.

Viewing Network Firewall enforced policy events on the local BIG-IP system

Ensure that the BIG-IP® system is configured to log the types of events you want to view, and to store the log messages locally on the BIG-IP system.

When the BIG-IP system is configured to log events locally, you can view those events using the Configuration utility.

1. On the Main tab, click **Security** > **Event Logs** > **Network** > **Firewall**.
   The Network Firewall event log displays.
2. To search for enforced policy events, in the search field, type `Enforced`, then click **Search**.
3. To narrow your search for enforced events, click **Custom Search**. Drag the `Enforced` text from the **Policy Type** column to the custom search table. Narrow your search further by dragging other items from the log display, for example, from the **action**, **policy**, or **rule** columns. the event data that you want to search for from the Event Log table into the Custom Search table, and then click **Search**.

Viewing Network Firewall staged policy events on the local BIG-IP system

Ensure that the BIG-IP® system is configured to log the types of events you want to view, and to store the log messages locally on the BIG-IP system.

When the BIG-IP system is configured to log events locally, you can view those events using the Configuration utility.

1. On the Main tab, click **Security** > **Event Logs** > **Network** > **Firewall**.
   The Network Firewall event log displays.
2. To search for staged policy events, in the search field, type `Staged`, then click **Search**.
3. To narrow your search for staged policy events, click **Custom Search**. Drag the `Staged` text from the **Policy Type** column to the custom search table. Narrow your search further by dragging other items from the log display, for example, from the **action**, **policy**, or **rule** columns. the event data that you want to search for from the Event Log table into the Custom Search table, and then click **Search**.

Index