BIG-IP® Systems: DOS Protection and DNS Firewall Implementations
# Table of Contents

**Legal Notices** .......................................................................................................................... 5

**Chapter 1: About Detecting and Protecting Against DoS, DDoS, and DNS Service Attacks** .................................................................................................................................... 7
  - About detecting and protecting against DoS, DDoS, and DNS service attacks ............... 8
  - About profiles for DoS and DNS service attacks ............................................................. 8

**Chapter 2: About System DoS and DDoS Attacks** .................................................................. 9
  - About configuring the BIG-IP system to detect and prevent DoS and DDoS attacks ...... 10
  - Detecting and protecting against DoS and DDoS attacks ............................................. 10

**Chapter 3: About DNS DoS Attacks** ..................................................................................... 13
  - About configuring the BIG-IP system to detect DNS DoS attacks ............................... 14
  - Detecting and protecting against DNS denial of service attacks with a DoS profile .... 14
  - Creating a custom DNS profile to firewall DNS traffic ............................................... 15
  - Assigning a DNS profile to a virtual server ................................................................. 15
  - Attaching denial of service detection to a virtual server ............................................. 15

**Chapter 4: About SNMP Trap Configuration** ....................................................................... 17
  - Overview: SNMP trap configuration ............................................................................ 18
  - Task summary ................................................................................................................ 18
    - Enabling traps for specific events ............................................................................. 18
    - Setting v1 and v2c trap destinations ....................................................................... 18
    - Setting v3 trap destinations .................................................................................... 19
    - Viewing pre-configured SNMP traps ..................................................................... 20
    - Creating custom SNMP traps ................................................................................ 20

**Chapter 5: About High-Speed Remote Logging of DoS Events** ....................................... 23
  - Overview: Configuring DoS Protection event logging ................................................. 24
  - Task summary ............................................................................................................. 25
    - Creating a pool of remote logging servers .............................................................. 25
    - Creating a remote high-speed log destination ....................................................... 26
    - Creating a formatted remote high-speed log destination ........................................ 26
    - Creating a publisher ............................................................................................... 27
    - Creating a custom DoS Protection Logging profile .............................................. 27
    - Configuring an LTM virtual server for DoS Protection event logging .................... 28
    - Disabling logging .................................................................................................. 28

**Implementation result** ........................................................................................................... 28
# Table of Contents

**Chapter 6: About Filtering DNS Packets**
- About DNS protocol filtering
- Filtering DNS traffic with a DNS security profile
- Creating a custom DNS profile to firewall DNS traffic

**Chapter 7: About High-Speed Logging of Protocol Security Events**
- Overview: Configuring Remote Protocol Security Event Logging
- Task summary
  - 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 Protocol Security Logging profile
  - Configuring a virtual server for Protocol Security event logging
  - Disabling logging
- Implementation result

**Acknowledgments**
Legal Notices

Publication Date
This document was published on November 15, 2012.

Publication Number
MAN-0440-00

Copyright
Copyright © 2012-2014, F5 Networks, Inc. All rights reserved.

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

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.
Chapter 1

About Detecting and Protecting Against DoS, DDoS, and DNS Service Attacks

- About detecting and protecting against DoS, DDoS, and DNS service attacks
About detecting and protecting against DoS, DDoS, and DNS service attacks

Attackers can target the BIG-IP® system in a number of ways. The BIG-IP system addresses several possible DoS, DDoS, and DNS attack routes:

**DoS and DDoS attacks**
Denial of service (DoS) and distributed denial of service (DDoS) attacks attempt to render a machine or network resource unavailable to users. Denial of service attacks require the efforts of one or more people to disrupt the services of a host connected to the Internet. The Advanced Firewall Module allows you to configure packet limits, percentage increase thresholds, and absolute rate limits of a wide variety of packets that attackers leverage as attack vectors, to detect and prevent attacks of this type.

**DNS flood (DoS) attacks**
Denial of service (DoS) or flood attacks attempt to overwhelm a system by sending thousands of requests that are either malformed or simply attempt to overwhelm a system using a particular DNS query type or protocol extension. The BIG-IP system allows you to track such attacks.

**Malformed DNS packets**
Malformed DNS packets can be used to consume processing power on the BIG-IP system, ultimately causing slowdowns like a DNS flood. The BIG-IP system drops malformed DNS packets, and allows you to configure how you track such attacks.

**Protocol exploits**
Attackers can send DNS requests using unusual DNS query types or opcodes. The BIG-IP system can be configured to allow or deny certain DNS query types, and to deny specific DNS opcodes. When you configure the system to deny such protocol exploits, the system tracks these events as attacks.

About profiles for DoS and DNS service attacks

On your BIG-IP® system, you can use two profiles, both enabled by the Protocol Security Manager™ module, to detect and protect against DNS attacks.

**DoS protection profile**
Allows you to configure the response thresholds on the BIG-IP system for malformed DNS packets. Malformed packets are dropped by the system. The DoS protection profile also allows you to configure the threshold increase of packets of specific DNS query types. You can use SNMP alerts generated by these items, and information reported in realtime reports and in system logs, to mitigate a specific DNS query type attack; for example, by blocking it with the DNS security profile.

**DNS security profile**
Allows you to configure the BIG-IP system to exclude (drop) or include (allow) packets of specific DNS query types. You can also configure the profile to drop specific DNS header opcodes.
Chapter 2

About System DoS and DDoS Attacks

- About configuring the BIG-IP system to detect and prevent DoS and DDoS attacks
About configuring the BIG-IP system to detect and prevent DoS and DDoS attacks

DoS and DDoS attack detection and prevention is enabled by the BIG-IP® Advanced Firewall Module (AFM). DoS and DDoS detection and prevention serves two functions:

- To detect, and automatically mitigate, packets that present as DoS or DDoS attacks.
- To determine unusual increases in packets of specific types that are known attack vectors. Possible attack vectors are tracked over the past hour, and current possible attacks are compared to the average of that hour.

You can configure a BIG-IP device to detect all system-supported DoS attacks at levels that you specify.

Detecting and protecting against DoS and DDoS attacks


2. If you are using remote logging, from the Log Publisher list, select a destination to which the BIG-IP system sends DoS and DDoS log entries.
3. In the Attack Type column, click the name of any attack type to edit the settings. The configuration page for the particular attack appears.
4. From the Detection Threshold PPS list, select Specify or Infinite.
   - Use Specify to set a value, in packets per second, for the attack detection threshold. If packets of this type cross the threshold, an attack is logged and reported. The system continues to check every second, and marks the threshold as an attack as long as the threshold is exceeded.
   - Use Infinite to set no value for the threshold. This specifies that this type of attack is never logged or reported.
5. From the Detection Threshold Percent list, select Specify or Infinite.
   - Use Specify to set the percentage increase value, that specifies an attack is occurring. The system compares the current rate to an average rate from the last hour. For example, if the average rate for the last hour is 1000 packets per second, and you set the percentage increase threshold to 100, an attack is detected at 100 percent above the average, or 2000 packets per second. When the threshold is passed, an attack is logged and reported. The system then automatically institutes a rate limit equal to the average for the last hour, and all packets above that limit are dropped. The system continues to check every second until the incoming packet rate drops below the percentage increase threshold. Rate limiting continues until the rate drops below the specified limit again.
   - Use Infinite to set no value for the threshold. This specifies that this type of attack is never logged or reported.
6. From the Default Internal Rate Limit list, select Specify or Infinite.
   - Use Specify to set a value, in packets per second, which cannot be exceeded by packets of this type. All packets of this type over the threshold are dropped. Rate limiting continues until the rate drops below the specified limit again.
   - Use Infinite to set no value for the threshold. This specifies that this type of attack is not rate-limited.
7. Click the **Update** button.
   The selected configuration is updated, and the DoS Protection Device Configuration screen opens again.

8. Repeat the previous steps for any other attack types for which you want to change the configuration.

Now you have configured the system to provide custom responses to possible DoS and DDoS attacks, and to allow such attacks to be identified in system logs and reports.

Configure SNMP traps, logging, and reporting for DoS attacks, to track threats to your system.
Chapter 3

About DNS DoS Attacks

• About configuring the BIG-IP system to detect DNS DoS attacks
About configuring the BIG-IP system to detect DNS DoS attacks

DNS DoS protection is enabled with the BIG-IP® Protocol Security Manager™ module. DNS attack detection and prevention serves two functions:

- To detect and automatically drop DNS packets that are malformed or contain errors.
- To log unusual increases in DNS packets of any type, including packets that are malformed, packets that contain errors, or packets of any other type that appear to rapidly increase.

You can use the DNS DoS Protection profile to configure the percentage increase over the system baseline, which indicates that a possible attack is in process on a particular DNS query type, or an increase in anomalous packets. Later, you can use reporting or logging functions to detect such packets, and you can use the DNS Security profile to drop packets with specific query types or header opcodes.

Detecting and protecting against DNS denial of service attacks with a DoS profile

In this task, you create the DoS protection profile and configure DNS settings at the same time. However, you can configure DNS attack settings in a DoS profile that already exists.

The BIG-IP® system handles DNS attacks that use malformed packets, protocol errors, and malicious attack vectors. Protocol error attack detection settings detect malformed and malicious packets, or packets that are employed to flood the system with several different types of responses. You can configure settings to identify DNS attacks with a DoS profile.

2. Click Create. The Create New DoS Profile screen opens.
3. In the Name field, type the name for the profile.
4. To configure DNS security settings, next to Protocol Security (DNS), select Enabled.
5. To enable attack detection based on the rate of DNS errors, next to Protocol Errors Attack Detection, select Enabled.
6. In the Rate Increased by % field, type the rate of change in DNS errors to detect as anomalous. The rate of detection compares the average rate over the last minute to the average rate over the last hour. For example, the 500% base rate would indicate an attack if the average rate for the previous hour was 100000 packets/second, and over the last minute the rate increased to 500000 packets/second.
7. To change the threshold or rate increase for a particular DNS query type, in the DNS Query Attack Detection area, select the Enabled check box for each query type that you want to change, then change the values for Threshold and Rate Increase in the associated fields.
   For example, to change the threshold for IPv6 address requests, select the Enabled check box next to aaaa, then set the threshold for packets per second and the rate increase percentage to be considered an attack.
   The Rate Increase compares the average rate over the last minute to the average rate over the last hour. For example, the 500% base rate would indicate an attack if the average rate for the previous hour was 100000 packets/second, and over the last minute the rate increased to 500000 packets/second.

   **Note:** DNS Query Attack Detection allows you to configure the thresholds at which the firewall registers an attack. However, no packets are dropped if an attack is detected.

8. Click Update to save your changes.
You have now configured a DoS protection profile to provide custom responses to malformed DNS attacks, and DNS flood attacks, and to allow such attacks to be identified in system logs and reports.

Associate the DoS protection profile with a virtual server to apply the settings in the profile to traffic on that virtual server. When a DNS attack on a specific query type is detected, you can configure the DNS security profile to drop packets of a query type that appears to be an attack vector.

**Creating a custom DNS profile to firewall DNS traffic**

Ensure that you have a DNS security profile created before you configure this system DNS profile.

You can create a custom DNS profile to configure the BIG-IP® system firewall traffic through the system.

1. On the Main tab, click **Local Traffic > Profiles > Services > DNS**.
   The DNS profile list screen opens.
2. Click **Create**.
   The New DNS profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. In the **Parent Profile** list, accept the default *dns* profile.
5. Select the **Custom** check box.
6. From the **DNS Security** list, select **Enabled**.
7. From the **DNS Security Profile Name** list, select the name of the DNS firewall profile.
8. Click **Finished**.

Assign the custom DNS profile to the virtual server that handles the DNS traffic that you want to firewall.

**Assigning a DNS profile to a virtual server**

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 **DNS Profile** list, select the profile you want to assign to the virtual server.
4. Click **Update**.

The virtual server now uses the DNS settings from the DNS Security profile.

**Attaching denial of service detection to a virtual server**

Create a DoS Protection Profile separately, to configure denial-of-service detection for applications and for the DNS protocol.

Add denial-of-service detection to a virtual server to provide enhanced protection for DoS attacks on a virtual server, and to more accurately track anomalous activity on a virtual server.

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. For the **Destination** setting, select **Host** and in the **Address** field, type the IP address for the virtual server.

5. To enable custom denial-of-service protection on the virtual server, next to DoS Protection Profile, select Enabled, then select the profile from the Profile list.

6. Click Update.

DoS protection is now enabled, and the DoS protection policy is associated with the selected virtual server.
Chapter 4

About SNMP Trap Configuration

- Overview: SNMP trap configuration
- Task summary
Overview: SNMP trap configuration

SNMP traps are definitions of unsolicited notification messages that the BIG-IP® alert system and the SNMP agent send to the SNMP manager when certain events occur on the BIG-IP system. Configuring SNMP traps on a BIG-IP system means configuring how the BIG-IP system handles traps, as well as setting the destination to which the notifications are sent.

The BIG-IP system stores SNMP traps in two specific files:

/etc/alertd/alert.conf
Contains default SNMP traps.

/config/user_alert.conf
Contains user-defined SNMP traps.

Important: Do not add or remove traps from the /etc/alertd/alert.conf file.

Task summary

Perform these tasks to configure SNMP traps for certain events and set trap destinations.

Enabling traps for specific events

Setting v1 and v2c trap destinations

Setting v3 trap destinations

Viewing pre-configured SNMP traps

Creating custom SNMP traps

Enabling traps for specific events

You can configure the SNMP agent on the BIG-IP® system to send, or refrain from sending, notifications to the traps destinations.

1. On the Main tab, click System > SNMP > Traps > Configuration.
2. To send traps when an administrator starts or stops the SNMP agent, verify that the Enabled check box for the Agent Start/Stop setting is selected.
3. To send notifications when authentication warnings occur, select the Enabled check box for the Agent Authentication setting.
4. To send notifications when certain warnings occur, verify that the Enabled check box for the Device setting is selected.
5. Click Update.

The BIG-IP system automatically updates the alert.conf file.

Setting v1 and v2c trap destinations

Specify the IP address of the SNMP manager in order for the BIG-IP® system to send notifications.
1. On the Main tab, click **System > SNMP > Traps > Destination**.
2. Click **Create**.
3. For the **Version** setting, select either **v1** or **v2c**.
4. In the **Community** field, type the community name for the SNMP agent running on the BIG-IP system.
5. In the **Destination** field, type the IP address of the SNMP manager.
6. In the **Port** field, type the port number on the SNMP manager that is assigned to receive the traps.
7. Click **Finished**.

### Setting v3 trap destinations

Specify the destination SNMP manager to which the BIG-IP® system sends notifications.

1. On the Main tab, click **System > SNMP > Traps > Destination**.
2. Click **Create**.
3. For the **Version** setting, select **v3**.
4. In the **Destination** field, type the IP address of the SNMP manager.
5. In the **Port** field, type the port number on the SNMP manager that is assigned to receive the traps.
6. From the **Security Level** list, select the level of security at which you want SNMP messages processed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth, No Privacy</td>
<td>Process SNMP messages using authentication but without encryption. When you use this value, you must also provide values for the Security Name, Authentication Protocol, and Authentication Password settings.</td>
</tr>
<tr>
<td>Auth and Privacy</td>
<td>Process SNMP messages using authentication and encryption. When you use this value, you must also provide values for the Security Name, Authentication Protocol, Authentication Password, Privacy Protocol, and Privacy Password settings.</td>
</tr>
</tbody>
</table>

7. In the **Security Name** field, type the user name the system uses to handle SNMP v3 traps.
8. In the **Engine ID** field, type an administratively unique identifier for an SNMP engine. (This setting is optional.) You can find the engine ID in the /config/net-snmp/snmpd.conf file on the BIG-IP system. Please note that this ID is identified in the file as the value of the oldEngineID token.
9. From the **Authentication Protocol** list, select the algorithm the system uses to authenticate SNMP v3 traps.
   When you set this value, you must also enter a value in the **Authentication Password** field.
10. In the **Authentication Password** field, type the password the system uses to handle an SNMP v3 trap.
    When you set this value, you must also select a value from the **Authentication Protocol** list.

**Note:** The authentication password must be at least 8 characters long.

11. If you selected **Auth and Privacy** from the **Security Level** list, from the **Privacy Protocol** list, select the algorithm the system uses to encrypt SNMP v3 traps. When you set this value, you must also enter a value in the **Privacy Password** field.
12. If you selected **Auth and Privacy** from the **Security Level** list, in the **Privacy Password** field, type the password the system uses to handle an encrypted SNMP v3 trap. When you set this value, you must also select a value from the **Privacy Protocol** list.

**Note:** The authentication password must be at least 8 characters long.
13. Click Finished.

Viewing pre-configured SNMP traps

Verify that your user account grants you access to the advanced shell.

Pre-configured traps are stored in the /etc/alertd/alert.conf file. View these SNMP traps to understand the data that the SNMP manager can use.

Use this command to view the SNMP traps that are pre-configured on the BIG-IP® system: `cat /etc/alertd/alert.conf`

Creating custom SNMP traps

Verify that your user account grants you access to tmsh.

Create custom SNMP traps that alert the SNMP manager to specific SNMP events that occur on the network when the pre-configured traps do not meet all of your needs.

1. Log in to the command line.
2. Create a backup copy of the file /config/user_alert.conf, by typing this command: `cp /config/user_alert.conf backup_file_name`
   For example, type: `cp /config/user_alert.conf /config/user_alert.conf.backup`
3. With a text editor, open the file /config/user_alert.conf.
4. Add a new SNMP trap.
   The required format is:

   ```
   alert alert_name "matched message" {
     snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.XXX"
   }
   ```

   • `alert_name` represents a descriptive name. The `alert_name` or `matched_message` value cannot match the corresponding value in any of the SNMP traps defined in the /etc/alertd/alert.conf or /config/user_alert.conf file.
   • `matched_message` represents the text that matches the Syslog message that triggers the custom trap. You can specify either a portion of the Syslog message text or use a regular expression. Do not include the Syslog prefix information, such as the date stamp and process ID, in the match string.
   • The `XXX` portion of the OID value represents a number that is unique to this OID. Specify any OID that meets all of these criteria:
     • Is in standard OID format and within the range .1.3.6.1.4.1.3375.2.4.0.300 through .1.3.6.1.4.1.3375.2.4.0.999.
     • Is in a numeric range that can be processed by your trap receiving tool.
     • Does not exist in the MIB file /usr/share/snmp/mibs/F5-BIGIP-COMMON-MIB.txt.
     • Is not used in another custom trap.
As an example, to create a custom SNMP trap that is triggered whenever the system logs switchboard failsafe status changes, add the following trap definition to `/config/user_alert.conf`:

```
alert SWITCHBOARD_FAILSAFE_STATUS "Switchboard Failsafe (*.*)" {
    snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.500"
}
```

This trap definition causes the system to log the following message to the file `/var/log/ltm`, when switchboard failsafe is enabled:

```
Sep 23 11:51:40 bigip1.askf5.com lacpd[27753]:
01160016:6: Switchboard Failsafe enabled.
```

5. Save the file.
6. Close the text editor.
7. Restart the `alertd` daemon by typing this command: `bigstart restart alertd`
   
   If the `alertd` daemon fails to start, examine the newly-added trap entry to ensure that the format is correct.
Chapter 5

About High-Speed Remote Logging of DoS Events

- Overview: Configuring DoS Protection event logging
- Task summary
- Implementation result
Overview: Configuring DoS Protection event logging

You can configure the BIG-IP® system to log information about BIG-IP system denial of service (DoS) events, and send the log messages to remote high-speed log servers.

**Important:** The BIG-IP system Protocol Security Manager™ (PSM™) module and Advanced Firewall Module (AFM) must be licensed and provisioned and DNS Services must be licensed before you can configure DoS Protection event logging. Additionally, for high volume logging requirements, such as DoS, ensure that the BIG-IP system sends the event logs to a remote log server.

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

<table>
<thead>
<tr>
<th>Object to create in implementation</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool of remote log servers</td>
<td>Create a pool of remote log servers to which the BIG-IP system can send log messages.</td>
</tr>
<tr>
<td>Destination (unformatted)</td>
<td>Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.</td>
</tr>
<tr>
<td>Destination (formatted)</td>
<td>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.</td>
</tr>
<tr>
<td>Publisher</td>
<td>Create a log publisher to send logs to a set of specified log destinations.</td>
</tr>
<tr>
<td>Logging profile</td>
<td>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.</td>
</tr>
<tr>
<td>LTM® virtual server</td>
<td>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.</td>
</tr>
</tbody>
</table>

This illustration shows the association of the configuration objects for remote high-speed logging of DoS Protection events.
Figure 1: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure logging of DoS Protection events on the BIG-IP® system.

**Note:** Enabling 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 DoS Protection Logging profile
- Configuring an LTM virtual server for DoS Protection 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 Module (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. From the Forward To list:
   - For ArcSight or Splunk, 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.
   - For 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. 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.


2. Click Create.

3. In the Name field, type a unique, identifiable name for this publisher.

4. For the Destinations setting, in the Available list, select a destination, 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 DoS Protection Logging profile

Create a custom Logging profile to log DoS Protection events and send the log messages to a specific location.


2. Click Create. The New Logging Profile screen opens.


4. In the DNS DoS Protection area, from the Publisher list, select the publisher that the BIG-IP system uses to log DNS DoS events.

5. Click Finished.

Assign this custom DoS Protection Logging profile to a virtual server.
Configuring an LTM virtual server for DoS Protection event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

Assign a custom DoS Protection Logging profile to a virtual server when you want the BIG-IP system to log DoS Protection events on the traffic 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. From the **Security** menu, select **Policies**. The screen displays Policy Settings and 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 your 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. From the **Security** menu, select **Policies**. The screen displays Policy Settings and Rules settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save your 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 DoS Protection events and sends the logs to a specific location.
Chapter 6

About Filtering DNS Packets

- About DNS protocol filtering
About DNS protocol filtering

With a DNS security profile, you can filter DNS to allow or deny specific DNS query types, and to deny specific DNS opcodes. The DNS security profile is attached to, and works with, a local traffic DNS profile to configure a range of DNS settings for a virtual server. Use DNS protocol filtering:

- To filter DNS query types or header opcodes that are not necessary or relevant in your configuration, or that you do not want your DNS servers to handle.
- As a remediation tool to drop packets of a specific query type, if a DoS Protection Profile identifies anomalous DNS activity with that query type.

Filtering DNS traffic with a DNS security profile

In this task, you create a DNS security profile and configure DNS security settings at the same time. However, you can also configure settings in a DNS security profile that already exists.

The BIG-IP® system can allow or drop packets of specific DNS query types, or with specific opcodes, to prevent attacks or allow legitimate DNS traffic. Use this to filter out header opcodes or query types that are not necessary on your system, or to respond to suspicious increases in packets of a certain type, as identified with the DNS security profile.

   The DNS Security Profiles list screen appears.
2. Click **Create**.
   The Create New DoS Profile screen opens.
3. In the **Name** field, type the name for the profile.
4. From the **Query Type** list, select how to handle query types you add to the **Active** list.
   - Select **Inclusion** to allow packets with the DNS query types you add to the **Active** list, and drop all others.
   - Select **Exclusion** to deny packets with the DNS query types you add to the **Active** list, and allow all others.
5. In the **Name** field, type the name for the profile.
6. In the **Name** field, type the name for the profile.
7. In the **Name** field, type the name for the profile.
8. Click **Update** to save your changes.

Now you have configured the profile to include or exclude only specified DNS query types and header opcodes.

Specify this DNS security profile in a local traffic DNS profile attached to a virtual server.

Creating a custom DNS profile to firewall DNS traffic

Ensure that you have a DNS security profile created before you configure this system DNS profile.

You can create a custom DNS profile to configure the BIG-IP® system firewall traffic through the system.

1. On the Main tab, click **Local Traffic > Profiles > Services > DNS**.
   The DNS profile list screen opens.
2. Click **Create**.
   The New DNS profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. In the **Parent Profile** list, accept the default **dns** profile.
5. Select the **Custom** check box.
6. From the **DNS Security** list, select **Enabled**.
7. From the **DNS Security Profile Name** list, select the name of the DNS firewall profile.
8. Click **Finished**.

Assign the custom DNS profile to the virtual server that handles the DNS traffic that you want to firewall.

**Assigning a DNS profile to a virtual server**

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 **DNS Profile** list, select the profile you want to assign to the virtual server.
4. Click **Update**.

The virtual server now uses the DNS settings from the DNS Security profile.
Chapter 7

About High-Speed Logging of Protocol Security Events

- Overview: Configuring Remote Protocol Security Event Logging
- Task summary
- Implementation result
Overview: Configuring Remote Protocol Security Event Logging

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

**Important:** The BIG-IP system Protocol Security Manager™ (PSM™) must be licensed and provisioned and DNS Services must be licensed before you can configure Protocol Security event logging.

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

<table>
<thead>
<tr>
<th>Object to create in implementation</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool of remote log servers</td>
<td>Create a pool of remote log servers to which the BIG-IP system can send log messages.</td>
</tr>
<tr>
<td>Destination (unformatted)</td>
<td>Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.</td>
</tr>
<tr>
<td>Destination (formatted)</td>
<td>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.</td>
</tr>
<tr>
<td>Publisher</td>
<td>Create a log publisher to send logs to a set of specified log destinations.</td>
</tr>
<tr>
<td>Logging profile</td>
<td>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.</td>
</tr>
<tr>
<td>LTM® virtual server</td>
<td>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.</td>
</tr>
</tbody>
</table>
Perform these tasks to configure Protocol Security event 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 Protocol Security Logging profile
- Configuring a virtual server for Protocol Security 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**.

---

36 About High-Speed Logging of Protocol Security Events
The BIG-IP system is configured to send a formatted string of text to the log servers.

5. From the **Forward To** list:
   - For ArcSight or Splunk, 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.
   - For 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. 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, in the Available list, select a destination, 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 Protocol Security Logging profile

Create a custom Protocol Security Logging profile to log Protocol Security events on the traffic handled by the virtual server to which the profile is assigned.

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. Select the **Protocol Security** check box, to enable the BIG-IP system to log HTTP, FTP, DNS, and SMTP protocol request events.
4. In the HTTP, FTP, and SMTP Security area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log HTTP, FTP, and SMTP Security events.
5. In the DNS Security area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log DNS Security events.
6. Select the **Log Dropped DNS Requests** check box, to enable the BIG-IP system to log dropped DNS requests.
7. Select the **Log Filtered Dropped DNS Requests** check box, to enable the BIG-IP system to log DNS requests dropped due to DNS query/header-opcode filtering.

   **Note:** The system does not log DNS requests that are dropped due to errors in the way the system processes DNS packets.

8. Select the **Log Malformed DNS Requests** check box, to enable the BIG-IP system to log malformed DNS requests.

9. Select the **Log Rejected DNS Requests** check box, to enable the BIG-IP system to log rejected DNS requests.

10. Select the **Log Malicious DNS Requests** check box, to enable the BIG-IP system to log malicious DNS requests.

11. From the **Storage Format** list, select how the BIG-IP system formats the log. Your choices are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Specifies the default format type in which the BIG-IP system logs messages to a remote Syslog server, for example:</td>
</tr>
<tr>
<td></td>
<td>&quot;management_ip_address&quot;, &quot;bigip_hostname&quot;, &quot;context_type&quot;, &quot;context_name&quot;, &quot;src_ip&quot;, &quot;dest_ip&quot;, &quot;src_port&quot;, &quot;dest_port&quot;, &quot;vlan&quot;, &quot;protocol&quot;, &quot;route_domain&quot;, &quot;acl_rule_name&quot;, &quot;action&quot;, &quot;drop_reason&quot;</td>
</tr>
<tr>
<td>Field-List</td>
<td>This option allows you to:</td>
</tr>
<tr>
<td></td>
<td>• Select from a list, the fields to be included in the log.</td>
</tr>
<tr>
<td></td>
<td>• Specify the order the fields display in the log.</td>
</tr>
<tr>
<td></td>
<td>• Specify the delimiter that separates the content in the log. The default delimiter is the comma character.</td>
</tr>
<tr>
<td>User-Defined</td>
<td>This option allows you to:</td>
</tr>
<tr>
<td></td>
<td>• Select from a list, the fields to be included in the log.</td>
</tr>
<tr>
<td></td>
<td>• Cut and paste, in a string of text, the order the fields display in the log.</td>
</tr>
</tbody>
</table>

12. Click **Finished**.

Assign this custom Protocol Security event Logging profile to a virtual server.

### Configuring a virtual server for Protocol Security event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

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

**Note:** This task applies only to systems provisioned at a minimum level (or higher) for Local Traffic (LTM). You can check the provisioning level on the **System > Resource Provisioning** screen.

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 **Security** menu, select **Policies**.
   
   The screen displays Policy Settings and 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 your 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.

2. Click the name of the virtual server you want to modify.
4. From the Log Profile list, select Disabled.
5. Click Update to save your 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 Protocol Security events and sends the logs to a specific location.
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,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.


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

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

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

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

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

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

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

C

custom profiles
  and DoS Protection Logging 27
  and Protocol Security Logging 37

D

DDoS attacks
  detecting 10
  detecting and preventing 8
denial of service
  detecting DNS attacks 14
  DNS attacks 8
  profiles 8
denial of service attacks
  preventing 10
denial-of-service protection
  adding to a virtual server 15
destination SNMP managers, specifying 18–19
destinations
  for logging 26, 36
  for remote high-speed logging 26, 36
distributed denial of service attacks
  preventing 10
DNS
  denial of service attacks 14
  detecting DoS attacks 14
  DoS attacks 8
  DoS profiles 8
  filtering 30
  preventing attacks 8, 30
  security 30
DNS flood attacks
  detecting with DoS profile 14
DNS profiles
  customizing for DNS firewall 15, 30
DNS protocol attacks
  preventing with DNS security profile 30
DNS security profile
  creating 30
DoS attacks
  detecting 10
  detecting and preventing 8
  detecting with device configuration 10
  profiles 8
DoS device configuration
  detecting DoS and DDoS attacks 10
DoS profile
  detecting DNS flood attacks 14
  preventing protocol error attacks 14
DoS Protection logging
  customizing profiles 27
  overview 24

E

events
  setting SNMP traps 18

F

filtering
  DNS protocol 30
  firewallsing DNS traffic 15, 30

H

high-speed logging
  and server pools 25, 35

L

logging
  and destinations 26, 36
  and DoS Protection 24
  and DoS Protection profiles 27
  and pools 25, 35
  and Protocol Security 34
  and Protocol Security profiles 37
  and publishers 27, 37
Logging profile
  and network firewalls 28
  and Protocol Security events 38
Logging profiles, disabling 28, 39

N

Network Firewall Logging
  disabling 28, 39
Network Firewall Logging profile, assigning to virtual server 28
notifications, sending 18–19

P

pools
  for high-speed logging 25, 35
profiles
  and disabling Network Firewall Logging 28, 39
  creating custom DNS 15, 30
  creating for DoS Protection Logging 27
  creating for Protocol Security Logging 37
Protocol Security logging
  customizing profiles 37
  overview 34
Protocol Security Logging profile, assigning to virtual server 38
publishers, and logging 27, 37

R

remote servers
  and destinations for log messages 26, 36
remote servers *(continued)*
  and publishers for log messages 27, 37
  for high-speed logging 25, 35

S

security profile
  DNS 8
servers
  and destinations for log messages 26, 36
  and publishers for log messages 27, 37
  for high-speed logging 25, 35
SNMP alerts, sending 18
SNMP events, setting traps 18
SNMP notifications, sending 18–19
SNMP traps
  creating 20
  defined 18
  enabling 18

SNMP traps *(continued)*
  viewing 20
SNMP v1 and v2c traps, setting destination 18
SNMP v3 traps, setting destination 19

T

traps
  defined 18

V

virtual server
  adding denial-of-service protection 15
  assigning Network Firewall Logging profile 28
  assigning Protocol Security Logging profile 38
  associating with DoS protection 15
virtual servers
  assigning a DNS profile 15, 31