BIG-IP® System: Implementing a Passive Monitoring Configuration

Version 13.0

Table of Contents

Configuring the BIG-IP System for Passive Monitoring.....5
Overview: Configuring the BIG-IP System for Passive Monitoring.....5
Task summary for passive monitoring.....7
Configure an interface for passive monitoring.....8
Create a BIG-IP VLAN to accept mirrored traffic.....9
Configure a TCP traffic filter for passive monitoring.....9
Configure a Fast L4 traffic filter for passive monitoring.....9
Create a listener for mirrored HTTP traffic.....10
Create a listener for non-specific mirrored traffic.....11
Create a pool of remote logging servers.....11
Create a remote high-speed log destination.....12
Create a formatted remote high-speed log destination.....12
Create a publisher 13
Create a logging filter.....13
Disable system logging 14

Legal Notices.....15
Legal notices.....15

Configuring the BIG-IP System for Passive Monitoring

Overview: Configuring the BIG-IP System for Passive Monitoring

You can configure a physical interface on a BIG-IP ®system to operate in *passive mode*. In this mode, the interface accepts mirrored traffic from another device to collect data for analysis and intrusion detection.

Passive mode behavior

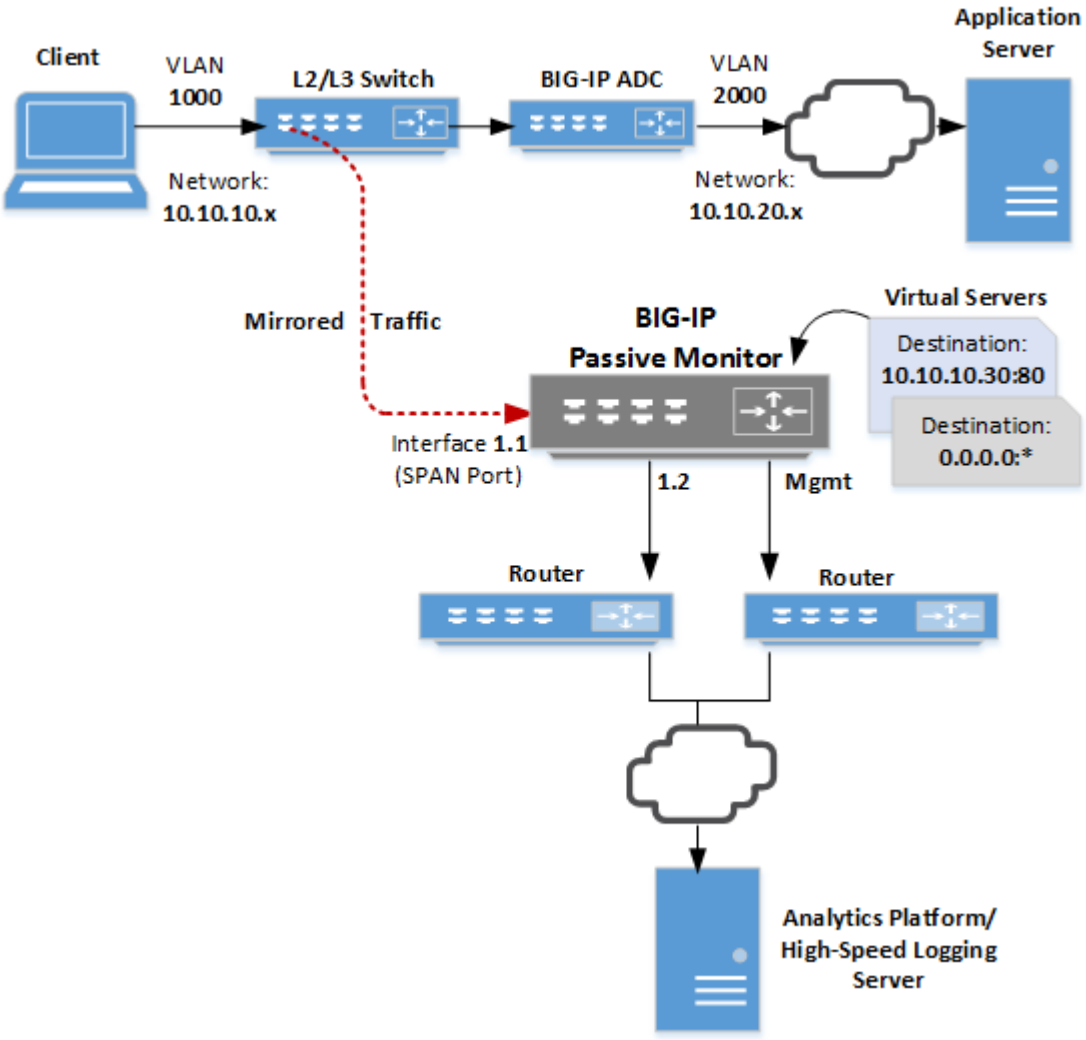
The BIG-IP system analyzes the mirrored traffic, drops it, and then sends the resulting analytics data and log messages to a remote analytics and logging server. The mirrored traffic never leaves the system, and the BIG-IP system never acts on the headers and payload.

Benefits of passive monitoring

You don't need to deploy the BIG-IP system in line with your BIG-IP application delivery controller (ADC), which means there's no need to make changes to your network infrastructure.

Sample configuration

This illustration shows a configuration that includes a BIG-IP passive monitoring system.



As we see in the illustration, a Layer 2/Layer 3 switch receives client traffic on the `10.10.10.x` network. The traffic comes into the switch, which mirrors it to a SPAN port on the BIG-IP system. A *SPAN port* is an interface that can receive traffic mirrored to it from another device.

After analyzing the traffic, the BIG-IP system forwards all analytics data and log messages through interface `1.2` to a remote analytics and logging server and then discards its copy of the application traffic.

We've also configured two virtual servers to listen on the SPAN port. One virtual server listens for any mirrored HTTP traffic destined for a particular destination address on port 80, while the other listens for any traffic not caught by the HTTP virtual server.

Common use cases

Typical reasons for deploying a BIG-IP system as a passive monitoring device are:

- To collect HTTP analytics data
- To collect application analytics data along with Subscriber-awareness made available by BIG-IP Policy Enforcement Manager™ (PEM™)
- To enable firewall services that report on possible infringements
- To detect denial-of-service attacks with signaling to some external entity for triggering actions
- To perform intrusion detection services
- To perform behavioral analysis

Prerequisite configuration

Before you set up a BIG-IP system as a passive monitoring system, make sure you have configured these things:

- A network device, such as a Layer 2/Layer 3 switch, configured to receive client application traffic and mirror it to the BIG-IP passive monitoring system.
- A user account with a user role that grants permission to perform all tasks (Administrator, Resource Administrator, or Manager).

Other considerations

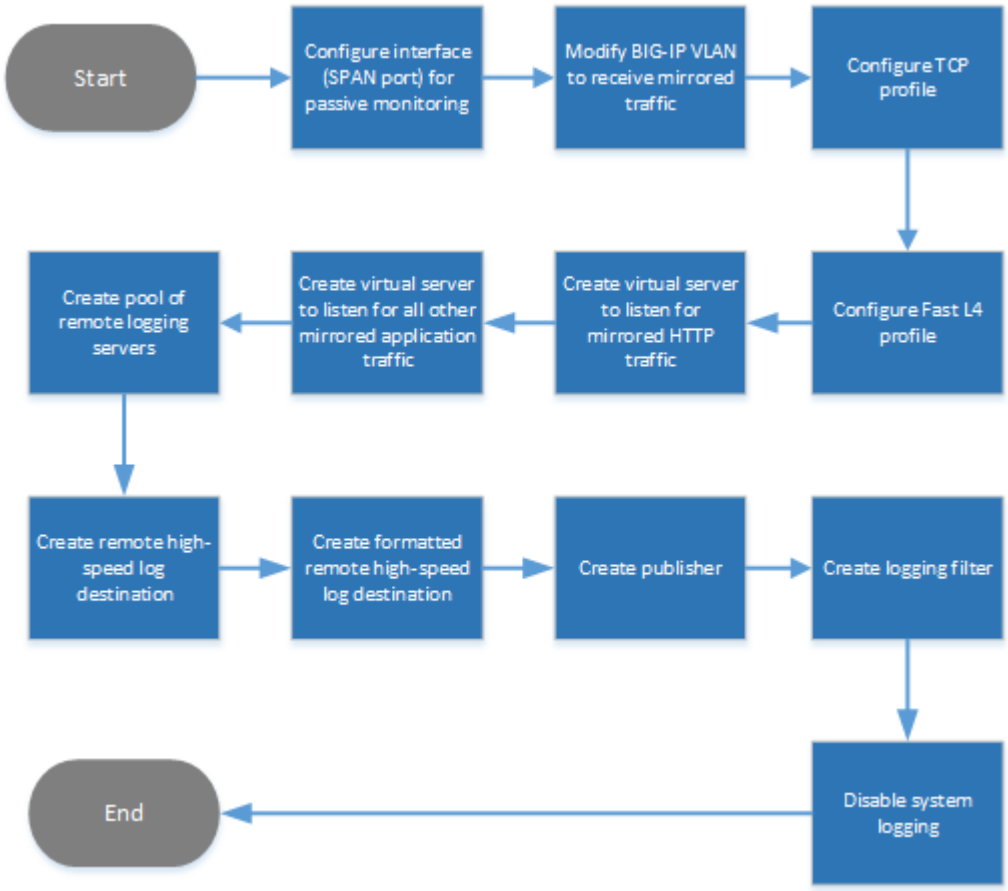
- A BIG-IP system operating in passive mode can accept mirrored traffic either raw or tunneled. In the case of tunneled traffic, the tunnel must be terminated on the BIG-IP system prior to the system analyzing the traffic.
- Global statistics do not differentiate between mirrored traffic and active traffic. However, statistics for an individual virtual server do differentiate between mirrored and active traffic because a virtual server applies to one type of traffic only.
- Passive mode is not available for interfaces on certain blade models.
- A trunk on which Link Aggregation Control Protocol (LACP) is enabled cannot operate as a passive monitoring interface.
- When you assign a passive monitoring interface to a BIG-IP VLAN, any self IP addresses associated with that VLAN will no longer respond to ARP requests.

Task summary for passive monitoring

To configure the BIG-IP ® system to do passive monitoring, you designate an interface on the BIG-IP passive monitoring system as a SPAN port and assign the interface to the ingress VLAN. Then, you configure a Fast L4 profile to disable SYN cookie support and Packet Velocity® Asic (PVA) acceleration. Finally, you set up whatever virtual servers you need to listen for mirrored traffic.

The result is that the system will analyze ingress traffic and send log messages and analytics data to a remote analytics and high-speed logging server.

This illustration shows the order in which you need to perform these tasks.



Configure an interface for passive monitoring
Create a BIG-IP VLAN to accept mirrored traffic
Configure a TCP traffic filter for passive monitoring
Configure a Fast L4 traffic filter for passive monitoring
Create a listener for mirrored HTTP traffic
Create a listener for non-specific mirrored traffic
Create a pool of remote logging servers
Create a remote high-speed log destination
Create a formatted remote high-speed log destination
Create a publisher
Create a logging filter
Disable system logging

Configure an interface for passive monitoring

You can designate a physical interface on the BIG-IP ® system as a SPAN port. A *SPAN port* receives mirrored traffic for the purpose of doing passive monitoring of that traffic. Through passive monitoring, the system can collect data for the purpose of analytics or intrusion detection.

Note: *You can configure a trunk for passive monitoring. In this case, you must set the* ***Forwarding Mode*** *to* ***Passive*** *separately on each link of the trunk.*

---

1. On the Main tab, click **Network** > **Interfaces** > **Interface List**.
   The Interface List screen displays the list of interfaces on the system.

2. In the Name column, click an interface number.
   This displays the properties of the interface.
3. For the **State** setting, verify that the interface is set to **Enabled**.
4. From the **Forwarding Mode** list, select **Passive**.
5. Click the **Update** button.

After you do this task, an interface on a passive monitoring system can receive mirrored traffic from another network device.

Important: *Be sure to assign the interface to a VLAN. Otherwise, the interface remains in an uninitialized state.*

Create a BIG-IP VLAN to accept mirrored traffic

Before performing this task, make sure that you have configured a VLAN with a tagged interface on the upstream switch that will mirror ingress application traffic and send it to this BIG-IP® system.

For any BIG-IP interface that you've configured to receive mirrored application traffic, you must create a VLAN and assign the interface to the VLAN.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
3. In the **Name** field, type a name for the VLAN.
4. In the **VLAN ID** field, type the same VLAN ID that you configured on the VLAN of the upstream switch that will send mirrored traffic to this BIG-IP system.
5. For the **Interfaces** setting:
   a) From the **Interface** list, select the interface that you previously set to **Passive** forwarding mode.
   b) From the **Tagging** list, select **Tagged**.

      Important: *This is the recommended configuration.*

   c) Click **Add**.
6. Click **Finished**.

The BIG-IP system now has a VLAN capable of receiving mirrored application traffic from an an upstream switch on the network.

Configure a TCP traffic filter for passive monitoring

You create a TCP profile to disable the **SYN Challenge Handling** setting.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Protocol** > **TCP.**
2. Click **Create**.
3. In the **Name** field, type a name for the profile, such as `my_tcp_profile`.
4. Scroll down to the Security and Quality of Service area of the screen, and on the right side, select the **Custom** check box.
5. From the **SYN Challenge Handling** list, select **Disable Challenges**.
6. At the bottom of the screen, click **Finished**.

Configure a Fast L4 traffic filter for passive monitoring

You create a Fast L4 profile to disable the Packet Velocity® ASIC settings and disable the **SYN Challenge Handling** setting.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Protocol** > **Fast L4**.
   The screen displays a list of Fast L4 profiles.
2. Click **Create**.
3. In the **Name** field, type a name for the profile.
   An example of a profile name is `my_http_fastl4_profile`.
4. On the right side of the screen, select the **Custom** check box.
5. From the **PVA Acceleration** list, select **None**.
6. For the **PVA Offload Dynamic** setting, clear the check box.
7. From the **SYN Challenge Handling** list, select **Disable Challenges**.
8. Click **Finished**.

After completing these steps, the BIG-IP system has a Fast L4 profile for filtering mirrored traffic coming into the system through a SPAN port.

Create a listener for mirrored HTTP traffic

You create an HTTP virtual server (also known as a listener) on a BIG-IP passive monitoring device to intercept specific mirrored HTTP traffic. This is traffic that you want to collect analytics and intrustion detection data on and then forward the data to a remote 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. From the **Type** list, select **Performance (Layer 4)**.
5. In the **Source Address** field, type `0.0.0.0/0`.
6. In the **Destination Address** field, type the destination address found in the destination IP address header of specific HTTP traffic that gets mirrored to the BIG-IP passive monitoring system.
   For example, if client traffic is destined for the virtual server address `10.10.10.30`, the BIG-IP passive monitoring system can listen for mirrored traffic with this destination address in its header in order to receive and analyze the mirrored traffic.
7. In the **Service Port** field, type `80`, or select **HTTP** from the list.
8. From the **Configuration** list, select **Advanced**.
9. From the **Protocol** list, select the name of the TCP profile you created for filtering mirrored traffic.
10. From the **Protocol Profile (Client)** list, select the name of the Fast L4 profile you created for filtering mirrored traffic.
11. From the **HTTP Profile** list, select the default HTTP profile named **http**.

    If you'd rather assign a custom profile, create a new HTTP profile before you create this virtual server, and then select the profile from this list.
12. From the **VLAN and Tunnel Traffic** list, retain the default selection, **All VLANs and Tunnels**.
13. For the **Address Translation** setting, verify that the check box is cleared.
14. For the **Port Translation** setting, verify that the check box is cleared.
15. From the **HTTP Analytics Profile** list, select **analytics**.
16. From the **TCP Analytics Profile** list, select **tcp-analytics**.
17. Click **Finished**.

You now have a virtual server configured to accept specific HTTP traffic coming into the interface designated as a SPAN port.

Create a listener for non-specific mirrored traffic

You can create a wildcard virtual server (also known as a listener) on the BIG-IP® passive monitoring device. The purpose of a *wildcard virtual server* is to intercept any mirrored traffic that the other virtual servers on the BIG-IP passive monitoring device don't already intercept. Once the wildcard virtual server receives the traffic, it can monitor the traffic for analytics and intrusion detection.

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. From the **Type** list, select **Performance (Layer 4)**.
5. In the **Source Address** field, type `0.0.0.0/0`.
6. In the **Destination Address** field, type `0.0.0.0` to accept any IPv4 traffic.
7. In the **Service Port** field, type `*` or select *** All Ports** from the list.
8. From the **Configuration** list, select **Advanced**.
9. From the **Protocol** list, select the name of the TCP profile you created for filtering mirrored traffic.
10. From the **Protocol Profile (Client)** list, select the name of the Fast L4 profile you created for filtering mirrored traffic.
11. From the **VLAN and Tunnel Traffic** list, retain the default selection, **All VLANs and Tunnels**.
12. For the **Address Translation** setting, verify that the check box is cleared.
13. For the **Port Translation** setting, verify that the check box is cleared.
14. From the **HTTP Analytics Profile** list, select **analytics**.
15. From the **TCP Analytics Profile** list, select **tcp-analytics**.
16. Click **Finished**.

You now have a virtual server configured to accept all traffic coming in through the interface designated as a SPAN port, except for traffic that specifically matches another virtual server on the system.

Create 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.

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

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **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**.

Create 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.

You 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. With this configuration, the BIG-IP system can 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**.

Create a formatted remote high-speed log destination

Before you start this task, ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

You 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 **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.

Important: *ArcSight formatting is only available for logs coming from Advanced Firewall Manager™ (AFM™), Application Security Manager™ (ASM™), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway. Remote Syslog formatting is the only type supported for logs coming from APM. The Splunk format is a predefined format of key value pairs.*

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

5. If you selected **Remote Syslog**, then 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.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, then 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**.

Create a publisher

Before you start this task, ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

You can 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**.

Create a logging filter

Before you start this task, ensure that at least one log publisher is configured on the BIG-IP® system.

You create a custom log filter to specify the system log messages that you want to publish to a particular log.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Filters**.
   The Log Filters screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this filter.
4. From the **Severity** list, select the level of alerts that you want the system to use for this filter.

   Note: *The severity level that you select includes all of the severity levels that display above your selection in the list. For example, if you select* ***Emergency****, the system publishes only emergency messages to the log. If you select* ***Critical****, the system publishes critical, alert, and emergency-level messages in the log.*

5. From the **Source** list, select the system processes from which messages will be sent to the log.
6. In the **Message ID** field, type the first eight hex-digits of the specific message ID that you want the system to include in the log. Use this field when you want a log to contain only each instance of one specific log message.

   Note: *BIG-IP system log messages contain message ID strings in the format:* `xxxxxxxx:x:`*. For example, in this log message:* `Oct 31 11:06:27 olgavmmgmt notice mcpd[5641]:`

`01070410:5: Removed subscription with subscriber id lind` , the message ID string is: `01070410:5:`. You enter only the first eight hex-digits: `01070410`.

7. From the **Log Publisher** list, select the publisher that includes the destinations to which you want to send log messages.
8. Click **Finished**.

Disable system logging

When you no longer want the BIG-IP® system to log information about its internal systems, you can delete the log filter that you created. For example, when mitigating a DoS attack, if you created a log filter that includes only one specific message in the log, you can delete that log filter once you handle the attack.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Filters**.
   The Log Filters screen opens.
2. Select the check box next to the name of the log filter that you want to delete. Click **Delete**, and then click **Delete** again.

Legal Notices

Legal notices

Publication Date

This document was published on June 29, 2017.

Publication Number

MAN-0658-00

Copyright

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

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

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

Export Regulation Notice

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

Index

C

configuration sequence
    illustrated *7*
content
    of LLDPDUs *8*
custom log filters
    and disabling logging *14*
    creating *13*

D

destinations
    for logging *12*
    for remote high-speed logging *12*

F

Fast L4 profile
    creating *9*

H

high-speed logging
    and server pools *11*

I

interfaces
    assigning to VLAN *9*
intrusion detection *5*

L

LLDP messages
    sending and receiving *8*
log filters
    and disabling system logging *14*
    creating *13*
logging
    and destinations *12*
    and pools *11*
    and publishers *13*
    system alerts *13*

M

message content
    for LLDPDUs *8*
messages
    transmitting and receiving *8*
mirroring
    to a BIG-IP system *9*

P

passive monitoring
    for data analysis and logging *5*
passive monitoring interfaces
    assigning to VLAN *9*
pools
    for high-speed logging *11*
publishers
    creating for logging *13*

R

remote servers
    and destinations for log messages *12*
    for high-speed logging *11*

S

servers
    and destinations for log messages *12*
    and publishers for log messages *13*
    for high-speed logging *11*
SPAN ports
    assigning to VLAN *9*
    for mirroring traffic *5*
system log filters, customizing *13*
system logging
    disabling *14*

T

tagged interfaces
    assigning to VLAN *9*
task sequence
    illustrated *7*
TCP traffic
    filtering *9*
traffic filters
    for passive monitoring *9*
transmission
    of LLDPDUs *8*
transparent forward proxy
    forwarding virtual server, use for *10*, *11*

V

virtual servers
    forwarding virtual servers *10*, *11*
VLANs
    for passive monitoring *9*

W

workflow
    illustrated *7*