Detecting Rogue Traffic on Non-Standard Ports

This chapter contains the following sections:

Overview of Detecting Rogue Traffic

The Web Security appliance has an integrated Layer-4 Traffic Monitor that detects rogue traffic across all network ports and stops malware attempts to bypass port 80. When internal clients are infected with malware and attempt to phone-home across non-standard ports and protocols, the L4 Traffic Monitor prevents phone-home activity from going outside the corporate network. By default, the L4 Traffic Monitor is enabled and set to monitor traffic on all ports. This includes DNS and other services.

The L4 Traffic Monitor uses and maintains its own internal database. This database is continuously updated with matched results for IP addresses and domain names.

Configuring the L4 Traffic Monitor

Step 1 Configure the L4 Traffic Monitor inside the firewall.

Step 2 Ensure the L4 Traffic Monitor is “logically” connected after the proxy ports and before any device that performs network address translation (NAT) on client IP addresses.

Step 3 Configure the Global Settings

See Configuring L4 Traffic Monitor Global Settings, on page 2.

Step 4 Create L4 TrafficMonitor Policies

See Creating a Policy to Detect Rogue Traffic, on page 3.

List of Known Sites

Address	Description
Known allowed	Any IP address or hostname listed in the Allow List property. These addresses appear in the log files as "whitelist" addresses.
Unlisted	Any IP address that is not known to be a malware site nor is a known allowed address. They are not listed on the Allow List, Additional Suspected Malware Addresses properties, or in the L4 Traffic Monitor Database. These addresses do not appear in the log files.
Ambiguous	These appear in the log files as "greylist" addresses and include: • Any *IP address* that is associated with both an unlisted *hostname* and a known malware *hostname* . • Any *IP address* that is associated with both an unlisted *hostname* and a *hostname* from the Additional Suspected Malware Addresses property
Known malware	These appear in the log files as "blacklist" addresses and include: • Any IP address or hostname that the L4 Traffic Monitor Database determines to be a known malware site and *not* listed in the Allow List. • Any *IP address* that is listed in the Additional Suspected Malware Addresses property, *not* listed in the Allow List and is *not* ambiguous

Configuring L4 Traffic Monitor Global Settings

Step 1 Choose **Security Services > L4 Traffic Monitor**.

Step 2 Click **Edit Global Settings**.

Step 3 Choose whether or not to enable the L4 Traffic Monitor.

Step 4 When you enable the L4 Traffic Monitor, choose which ports it should monitor:

- **All ports.** Monitors all 65535 TCP ports for rogue activity.
- **All ports except proxy ports.** Monitors all TCP ports except the following ports for rogue activity.
  - Ports configured in the "HTTP Ports to Proxy" property on the Security Services > Web Proxy page (usually port 80).
  - Ports configured in the "Transparent HTTPS Ports to Proxy" property on the Security Services > HTTPS Proxy page (usually port 443).

Step 5 Submit and Commit Changes.

Updating L4 Traffic Monitor Anti-Malware Rules

Step 1 Choose **Security Services > L4 Traffic Monitor**.

Step 2 Click **Update Now**.

Creating a Policy to Detect Rogue Traffic

The actions the L4 Traffic Monitor takes depends on the L4 Traffic Monitor policies you configure :

Step 1 Choose **Web Security Manager > L4 Traffic Monitor**.

Step 2 Click **Edit Settings**.

Step 3 On the **Edit L4 Traffic Monitor Policies** page, configure the L4 Traffic Monitor policies:

a) **Define** the **Allow List**

b) Add known good sites to the **Allow List**

Note Do not include the Web Security appliance IP address or hostname to the Allow List otherwise the L4 Traffic Monitor does not block any traffic.

c) Determine which action to perform for **Suspected Malware Addresses**:

Action	Description
Allow	It always allows traffic to and from known allowed and unlisted addresses
Monitor	It monitors traffic under the following circumstances: • When the Action for Suspected Malware Addresses option is set to Monitor, it always monitors all traffic that is not to or from a known allowed address. • When the Action for Suspected Malware Addresses option is set to Block, it monitors traffic to and from ambiguous addresses
Block	When the Action for Suspected Malware Addresses option is set to Block, it blocks traffic to and from known malware addresses

Note - When you choose to block suspected malware traffic, you can also choose whether or not to always block ambiguous addresses. By default, ambiguous addresses are monitored.

- If the L4 Traffic Monitor is configured to block, the L4 Traffic Monitor and the Web Proxy must be configured on the same network. Use the **Network > Routes** page to confirm that all clients are accessible on routes that are configured for data traffic.

d) Define the **Additional Suspected Malware Addresses** properties

Note Adding internal IP addresses to the Additional Suspected Malware Addresses list causes legitimate destination URLs to show up as malware in L4 Traffic Monitor reports. To avoid this do not enter internal IP addresses in the “**Additional Suspected Malware Addresses**” field on the **Web Security Manager > L4 Traffic Monitor Policies** page.

Step 4 Submit and Commit Changes.

What to do next

Related Topics

- Overview of Detecting Rogue Traffic, on page 1
- Valid Formats, on page 4.

Valid Formats

When you add addresses to the Allow List or Additional Suspected Malware Addresses properties, separate multiple entries with whitespace or commas. You can enter addresses in any of the following formats:

- **IPv4 IP address.** Example: IPv4 format: 10.1.1.0. IPv6 format: 2002:4559:1FE2::4559:1FE2
- **CIDR address.** Example: 10.1.1.0/24.
- **Domain name.** Example: example.com.
- **Hostname.** Example: crm.example.com.

Viewing L4 Traffic Monitor Activity

The S-Series appliance supports several options for generating feature specific reports and interactive displays of summary statistics.

Monitoring Activity and Viewing Summary Statistics

The **Reporting > L4 Traffic Monitor** page provides statistical summaries of monitoring activity. You can use the following displays and reporting tools to view the results of L4 Traffic Monitor activity:

To view...	See...
Client statistics	Reporting > Client Activity
Malware statistics Port statistics	Reporting > L4 Traffic Monitor
L4 Traffic Monitor log files	System Administration > Log Subscriptions • trafmon_errlogs • trafmonlogs

Note If the Web Proxy is configured as a forward proxy and L4 Traffic Monitor is set to monitor all ports, the IP address of the proxy's data port is recorded and displayed as a client IP address in the client activity report on the **Reporting > Client Activity** page. If the Web Proxy is configured as a transparent proxy, enable IP spoofing to correctly record and display the client IP addresses.

L4 Traffic Monitor Log File Entries

The L4 Traffic Monitor log file provides a detailed record of monitoring activity.