Integration of Cisco Web Security Appliance Web Traffic Tap with LogRhythm NetMon

Overview
With the growth of sophisticated threats, information sharing has becoming an important aspect to combat threats. Many organizations are collecting web traffic from various network hops and consolidating them in a single point of a log management system to provide a consolidated end point, network, and security analytics. This provides a faster detection rate that in turn will prevent cyber threats. A consolidated log system also provides organizations with consolidated log retention and alignment with compliance.

About this document
This document describes how to configure the Web Traffic Tap feature on Cisco® Web Security Appliance (WSA) using AsyncOS® 11.5.1 to mirror web traffic across to LogRhythm as well as enabling LogRhythm to collect traffic from WSA.

This document covers:
- Introduction to NetMon
- Introduction to Web Traffic Tap
- Cisco product/software and third-party product requirements
- Web Traffic Tap configuration on WSA
- Traffic collection configuration on LogRhythm
- Conclusion
- Next Steps

© 2018 Cisco and/or its affiliates. All rights reserved.
Introduction to NetMon

Network Monitor (NetMon), as its name suggests, provides visibility into data traversing your network by performing monitoring activities. The core capabilities of NetMon are:

- Setting a baseline of normal network behavior to help identify abnormal activities
- Performing deep packet capture for advanced forensics
- Detecting unauthorized or suspicious application activities
- Monitoring bandwidth consumption of applications

In this document, we are integrating LogRhythm NetMon with WSA Web Traffic Tap to run advanced forensics and compliance.

Introduction to Web Traffic Tap

From AsyncOS 11.5.1, an admin can enable one of its network interfaces as a traffic tap interface. This interface will be used to selectively mirror both HTTP and decrypted HTTPS traffic to be forwarded to an external traffic collector. In this document, we will configure the WSA to send web traffic, both HTTP and decrypted HTTPS, to LogRhythm.

This feature provides flexible traffic selection based on policy (URL categories) and identity.

Figure 1. Web Traffic Tap traffic flow
Cisco product/software and third-party product requirements

- WSA, software version 11.5.1 or later (all hardware and virtual platforms are supported)
- LogRhythm, software version 3.8.1

Web Traffic Tap configuration on WSA

Step 1. Log in to the WSA user interface using admin credentials https://wsa_hostname:8443

Step 3. Click **Edit Settings**. The Web Traffic Tap feature is disabled by default.

![Web Traffic Tap Settings](image)

Step 4. Tick **Enable** on the Web Traffic Tap Settings and choose an unused interface for the Tap Interface. Click **Submit** to enable it.

**Note:** The Tap Interface needs to be connected directly to LogRhythm, or connected in a dedicated VLAN via a Layer 2 switch.

![Edit Web Traffic Tap Settings](image)

Step 5. To configure Web Traffic Tap policies, navigate to **Web Security Manager > Web Traffic Tap Policies**.

**Note:** A default **Global Policy** has been preconfigured with **No Tap** policy configured.
Step 6. To enable all URL categories to be mirrored to LogRhythm except the Finance category, click Select all on the Tap column and select Finance in the No Tap column. Click Submit to enable it.
Web Traffic Tap Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering

No custom and external URL categories are defined. Add categories in the Web Security Manager > Custom and External URL Categories page.

Predefined URL Category Filtering

<table>
<thead>
<tr>
<th>Category</th>
<th>Tap</th>
<th>No Tap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Freeware and Shareware</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Gambling</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Games</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Government and Law</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Hacking</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Hate Speech</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Health and Nutrition</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Humor</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Illegal Activities</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Illegal Downloads</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Illegal Drugs</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Infrastructure and Content Delivery Networks</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Internet Telephony</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Job Search</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Lingerie and Swimsuits</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Lotteries</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Music</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Here is a summary of the Web Traffic Tap policies.

![Web Traffic Tap Policies](image)

**Note:** If a specific policy is required, it can be added through the Add Policy... button.

For HTTPS traffic, please kindly ensure that matching decryption policies have been created, as mirrored HTTPS traffic will be decrypted traffic.

A comprehensive filtering policy can be created with a specific identity and/or advanced policy member definitions such as protocols (HTTP/HTTPS), subnets, URL categories, or user agents.
Contents

Overview
About this document
Introduction to NetMon
Introduction to Web Traffic Tap
Cisco product/software and third-party product requirements
Web Traffic Tap configuration on WSA
Traffic collection configuration on LogRhythm
Conclusion
Next steps
Step 7. Select **Commit Changes** once the configuration has been completed.

Step 8. A summary of the tapped traffic can be viewed in **Reporting > Overview**.
Traffic collection configuration on LogRhythm

**Step 1.** Log in to the LogRhythm user interface using admin credentials: https://logrhythm_hostname.

**Step 2.** Navigate to **Configuration > Network** and ensure that the interface is receiving traffic.

**Note:** Please ensure that the LogRhythm interface has been connected directly to the WSA Tap Interface, or in the same VLAN as the WSA Tap Interface.

Alternatively, navigate to **Diagnostics > Network** and ensure that the **Packet Rate** graph is receiving traffic (blue line).

**Step 3.** To specify what applications are to be monitored, navigate to **Configuration > Capture**.

To capture all applications, toggle the **Capture All** field to **ON**, and click the **Apply Changes** button.
To capture all applications and exclude a subset of applications, list the applications to be excluded after the **Capture All** field is toggled **ON** by typing the application name.
To include only a subset of applications, toggle the **Capture All** field to **OFF**, and type the application names to be included.

![Manage Captured Applications](image)
Step 4. For a quick overview of all traffic captured by LogRhythm, navigate to Analyze > Dashboards.
Clicking on the time period field (highlighted in the red box above) provides the flexibility of multiple selections (Quick, Relative, or Absolute) for the time period in the dashboard report.

<table>
<thead>
<tr>
<th>Quick</th>
<th>Today</th>
<th>Yesterday</th>
<th>Last 15 minutes</th>
<th>Last 30 days</th>
</tr>
</thead>
<tbody>
<tr>
<td>This week</td>
<td>Day before yesterday</td>
<td>Last 30 minutes</td>
<td>Last 60 days</td>
<td></td>
</tr>
<tr>
<td>This month</td>
<td>This last week</td>
<td>Last 1 hour</td>
<td>Last 90 days</td>
<td></td>
</tr>
<tr>
<td>This year</td>
<td>Previous week</td>
<td>Last 4 hours</td>
<td>Last 6 months</td>
<td></td>
</tr>
<tr>
<td>The day so far</td>
<td>Previous month</td>
<td>Last 12 hours</td>
<td>Last 1 year</td>
<td></td>
</tr>
<tr>
<td>Week to date</td>
<td>Previous year</td>
<td>Last 24 hours</td>
<td>Last 2 years</td>
<td></td>
</tr>
<tr>
<td>Month to date</td>
<td></td>
<td>Last 7 days</td>
<td>Last 5 years</td>
<td></td>
</tr>
<tr>
<td>Year to date</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 5.** To view the tapped traffic from WSA, navigate to Analyze > Discover for an overview of all captured traffic.
Looking closely at one of the sessions, you can see detailed information about host name, user agent, content type, date, source, destination IPs, and ports.

From the above example, we can see that the destination port is 443, which is HTTPS traffic. Expanding on the session, we can see the plaintext HTTP header information (which, in a normal HTTPS session, will be encrypted).

**Hostname:** shaver.services.mozilla.com

**User agent:** Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0

For convenience, the data can also be viewed in JSON format by clicking on the JSON tab.
Conclusion

In conclusion, why do we think it is important to integrate WSA with the LogRhythm NetMon appliance? Here is a list of the benefits:

- WSA will act as a single point of decryption device for HTTPS traffic without requiring an external SSL decryption appliance.
- WSA provides flexible policy creation to mirror ALL or a subset of web traffic that will allow an admin to only monitor interested traffic on LogRhythm.
- LogRhythm also provides further policy flexibility by creating rules that can match a number of conditions such as matching an email address with a different domain, saving PCAP files to a few IP addresses, or monitoring the usage of protocols at a specific time (for example, after hours).
- The integration will amplify any operational anomalies. For example, an admin believes that a policy has been configured to block a certain type of traffic; however, this traffic is later found within LogRhythm. This provides an opportunity for the admin to rectify the policy configuration.
- WSA has both Bandwidth and Time Quota features; however, if LogRhythm is deployed as a centralized collector from various network devices, it can be used to discover bandwidth hogs and identify time-based activity trends.
- With this integration, troubleshooting latency will become an easier task. Because LogRhythm collects data from various network devices, it is easier to pinpoint where the issue occurs.

Next steps

For detailed information on Cisco WSA, go to www.cisco.com/go/wsa.

Find out more about LogRhythm NetMon at www.logrhythm.com/products/logrhythm-netmon/.

A Cisco sales representative, consulting system engineer, or channel partner can help to evaluate how Cisco WSA will enhance your security.