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

Contents

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

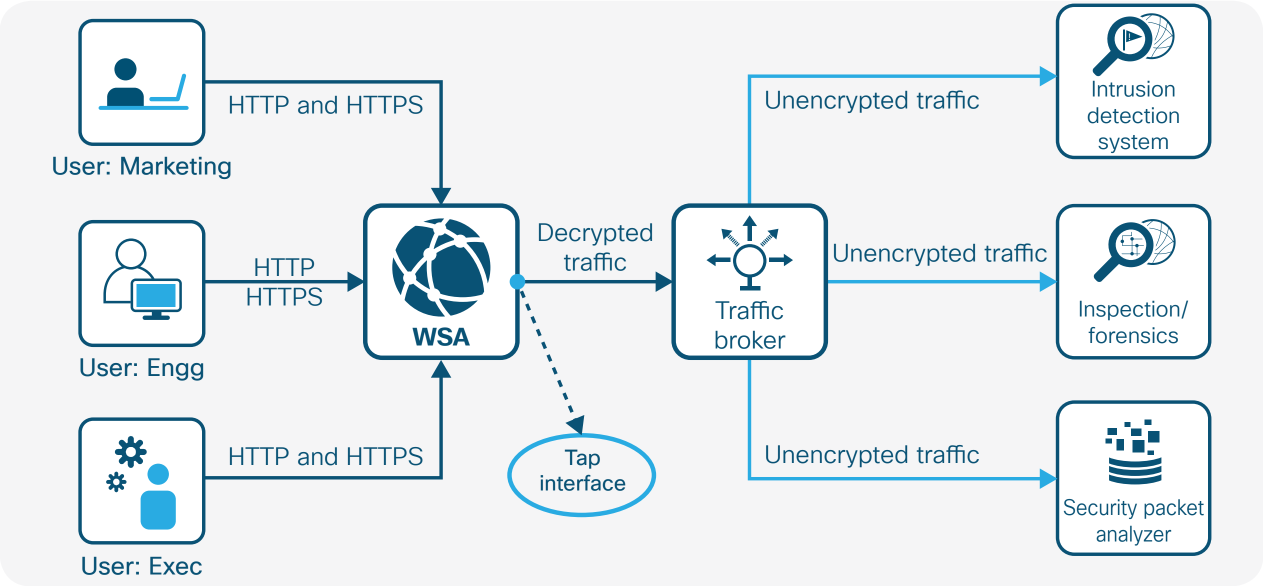
In this document, we are integrating LogRhythm NetMon with WSA Web Traffic Tap to run advanced forensics and compliance.

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



Contents

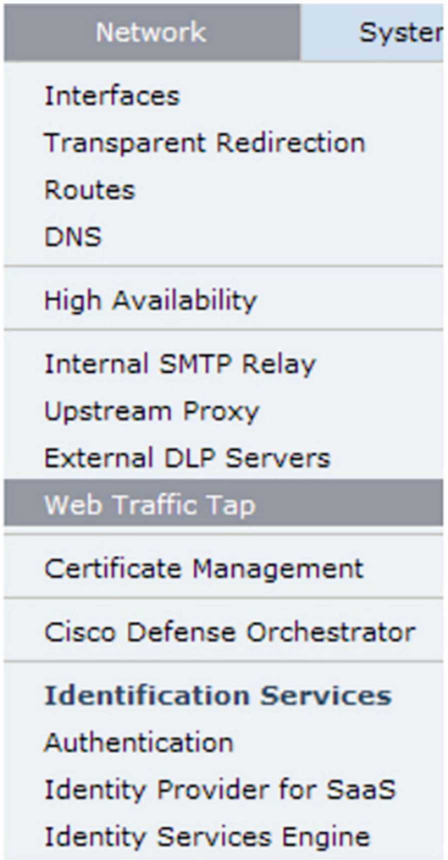
Cisco product/software and third-party product requirements

- 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

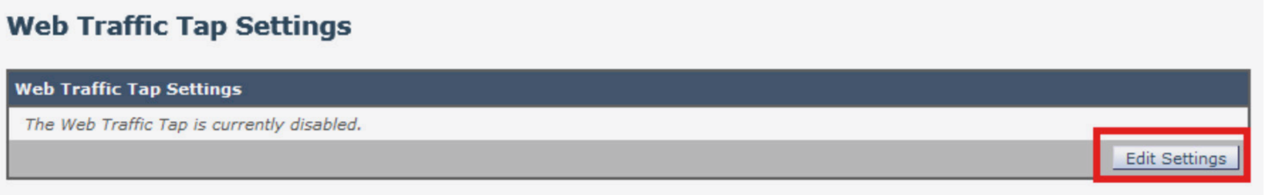
Step 1. Log in to the WSA user interface using admin credentials https://wsa_hostname:8443

Step 2. Navigate to **Network > Web Traffic Tap**.



Contents

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

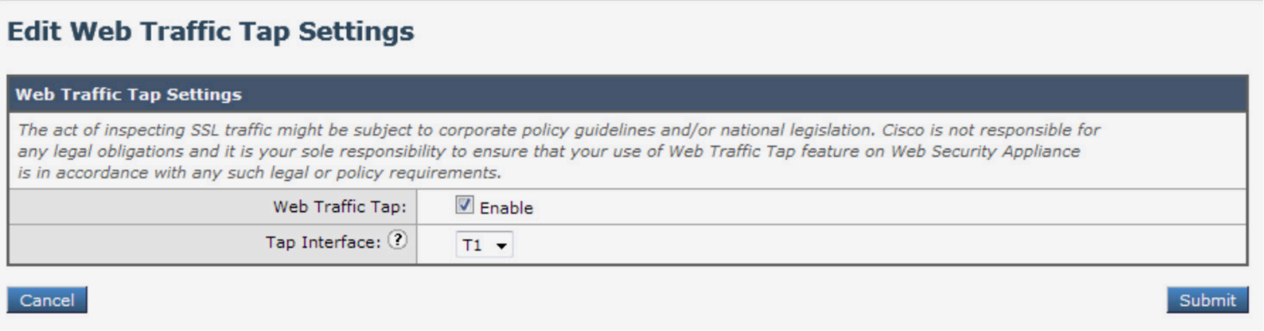


Web Traffic Tap Settings

Web Traffic Tap Settings
The Web Traffic Tap is currently disabled.

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.



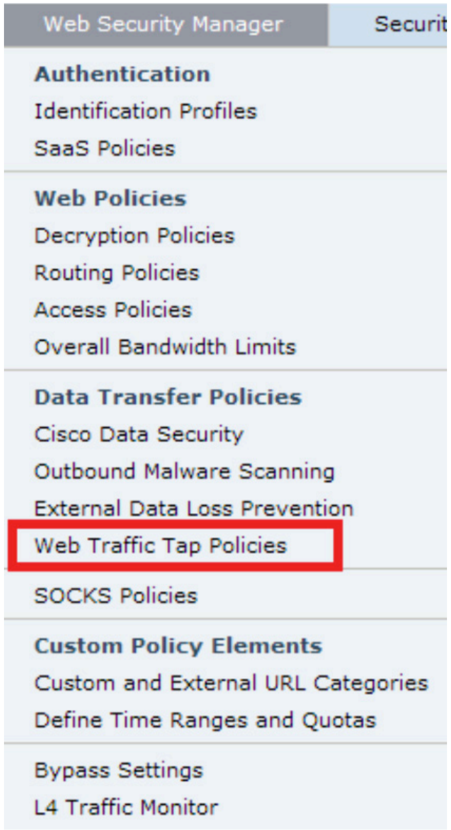
Edit Web Traffic Tap Settings

Web Traffic Tap Settings	
The act of inspecting SSL traffic might be subject to corporate policy guidelines and/or national legislation. Cisco is not responsible for any legal obligations and it is your sole responsibility to ensure that your use of Web Traffic Tap feature on Web Security Appliance is in accordance with any such legal or policy requirements.	
Web Traffic Tap:	☑ Enable
Tap Interface: ?	T1

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

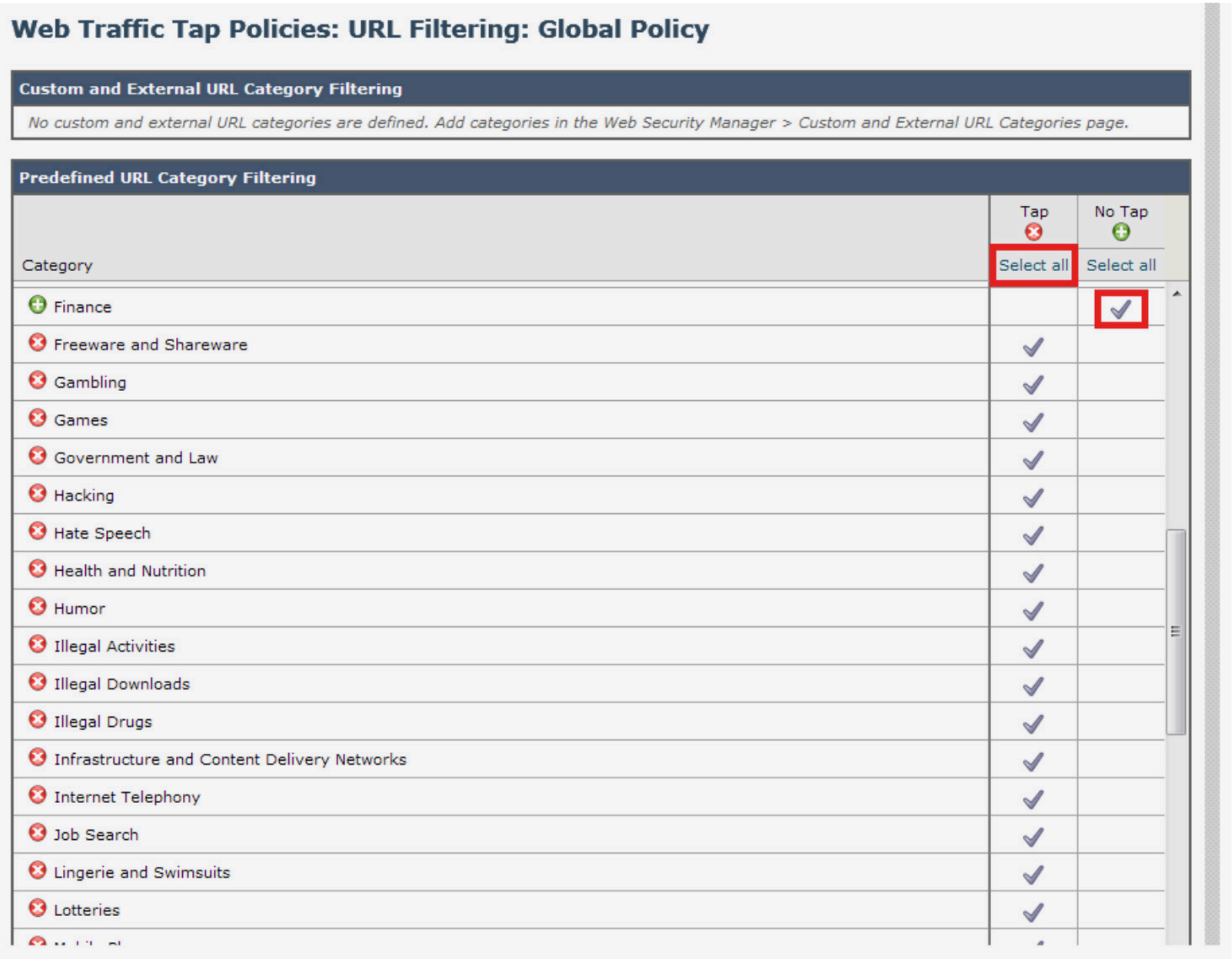
Note: A default **Global Policy** has been preconfigured with **No Tap** policy configured.

Contents



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.

Contents



Web Traffic Tap Policies: URL Filtering: Global Policy

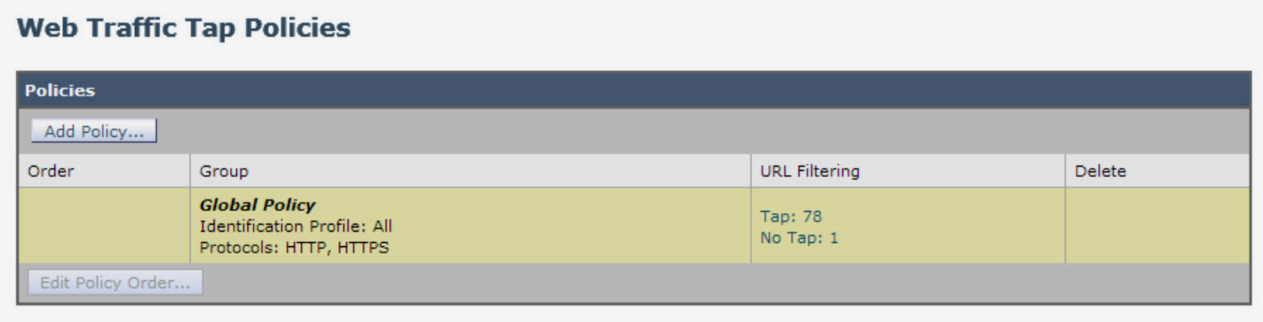
Custom and External URL Category Filtering

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

Category	Tap ⊗ Select all	No Tap ⊕ Select all
⊕ Finance		✓
⊗ Freeware and Shareware	✓	
⊗ Gambling	✓	
⊗ Games	✓	
⊗ Government and Law	✓	
⊗ Hacking	✓	
⊗ Hate Speech	✓	
⊗ Health and Nutrition	✓	
⊗ Humor	✓	
⊗ Illegal Activities	✓	
⊗ Illegal Downloads	✓	
⊗ Illegal Drugs	✓	
⊗ Infrastructure and Content Delivery Networks	✓	
⊗ Internet Telephony	✓	
⊗ Job Search	✓	
⊗ Lingerie and Swimsuits	✓	
⊗ Lotteries	✓	

Here is a summary of the Web Traffic Tap policies.



Web Traffic Tap Policies

Policies

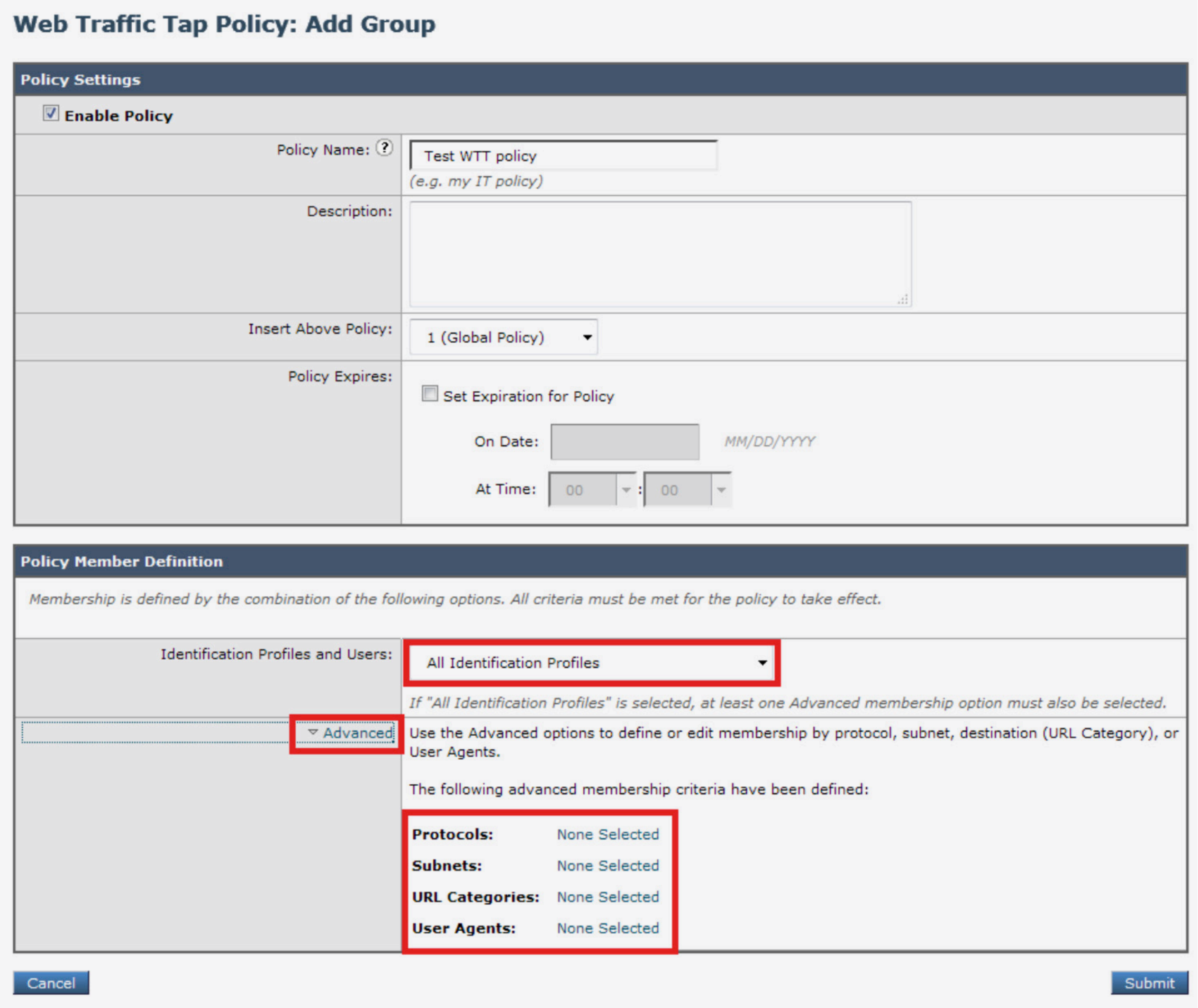
Order	Group	URL Filtering	Delete
	Global Policy Identification Profile: All Protocols: HTTP, HTTPS	Tap: 78 No Tap: 1	

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



Web Traffic Tap Policy: Add Group

Policy Settings

☑ **Enable Policy**

Policy Name: ? Test WTT policy
(e.g. my IT policy)

Description:

Insert Above Policy: 1 (Global Policy)

Policy Expires: □ Set Expiration for Policy

On Date: *MM/DD/YYYY*

At Time: 00 : 00

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: All Identification Profiles
If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.

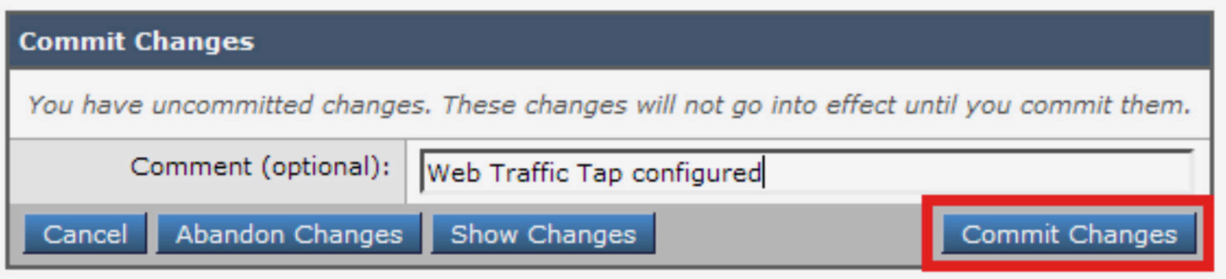
▿ Advanced: Use the Advanced options to define or edit membership by protocol, subnet, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols:	None Selected
Subnets:	None Selected
URL Categories:	None Selected
User Agents:	None Selected

Contents

Step 7. Select **Commit Changes** once the configuration has been completed.

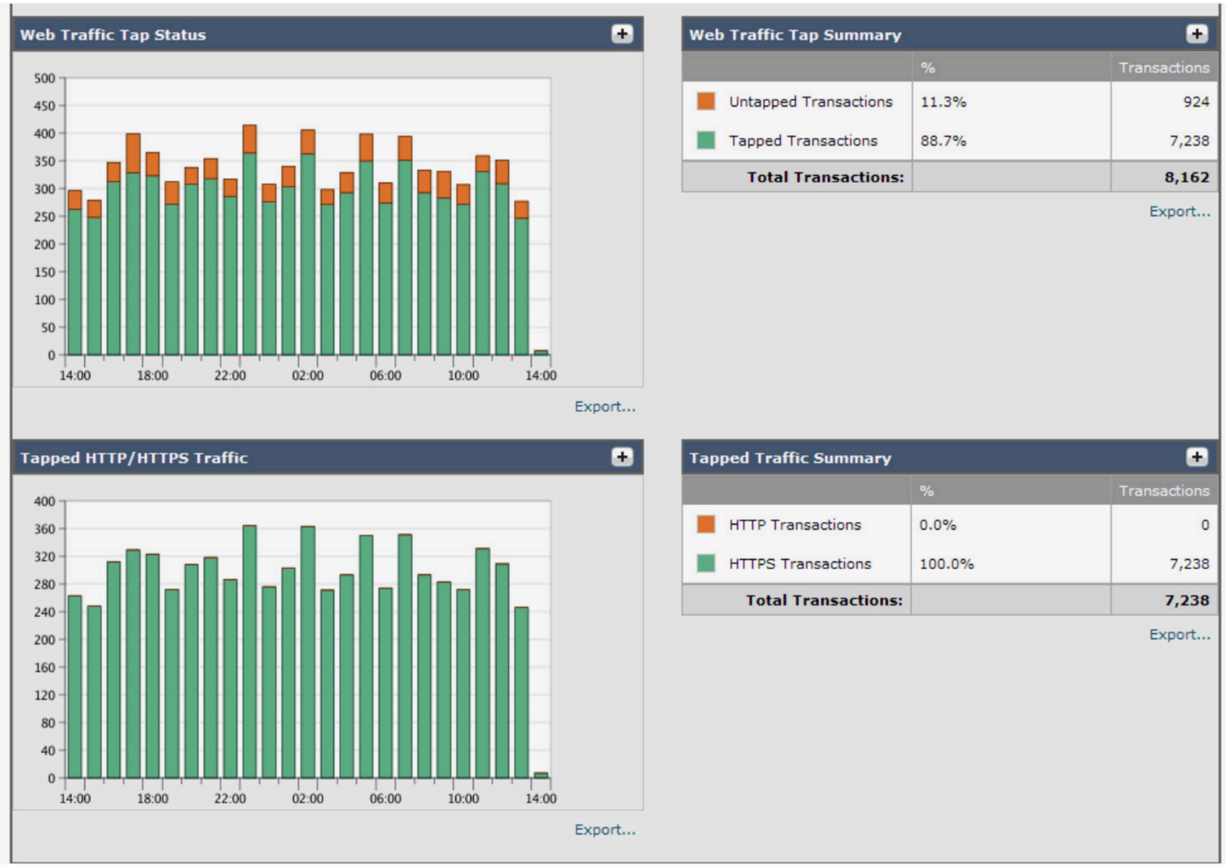


Commit Changes

You have uncommitted changes. These changes will not go into effect until you commit them.

Comment (optional): Web Traffic Tap configured

Step 8. A summary of the tapped traffic can be viewed in **Reporting > Overview**.



Web Traffic Tap Summary

	%	Transactions
🟧 Untapped Transactions	11.3%	924
🟩 Tapped Transactions	88.7%	7,238
Total Transactions:		**8,162**

Export...

Tapped Traffic Summary

	%	Transactions
🟧 HTTP Transactions	0.0%	0
🟩 HTTPS Transactions	100.0%	7,238
Total Transactions:		**7,238**

Export...

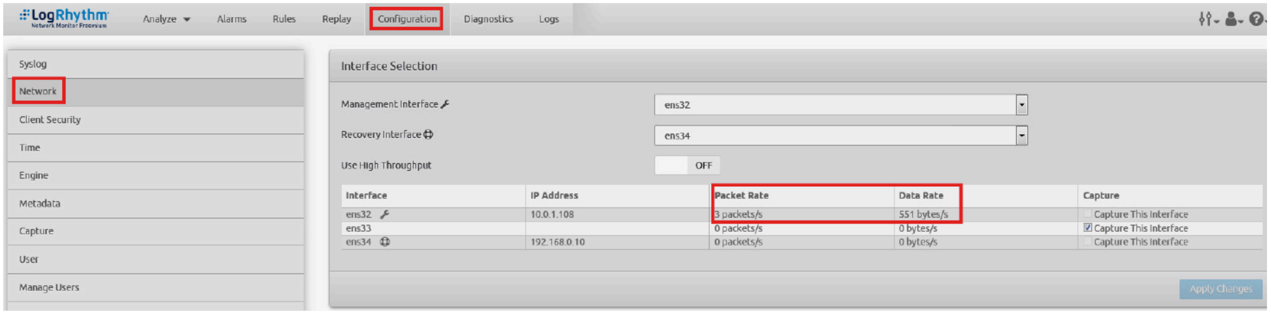
Contents

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.



Interface Selection

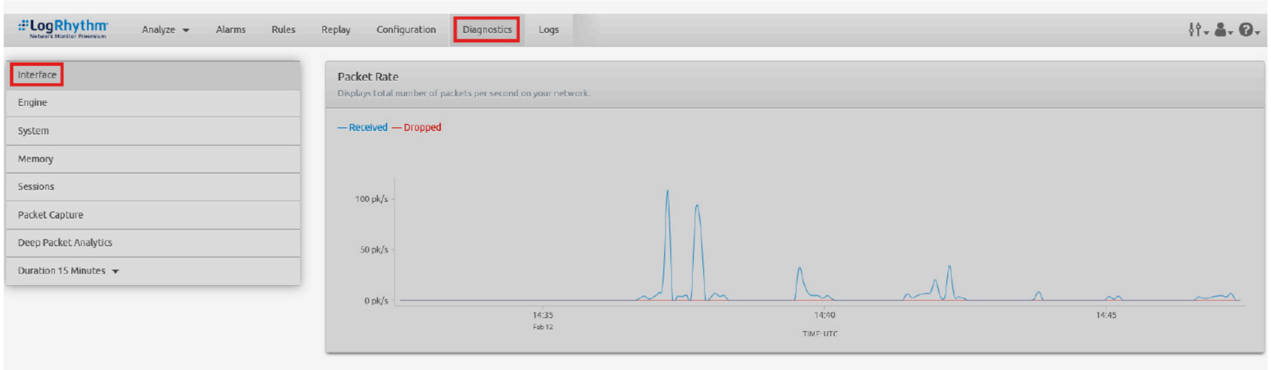
Management Interface: ens32

Recovery Interface: ens34

Use High Throughput: OFF

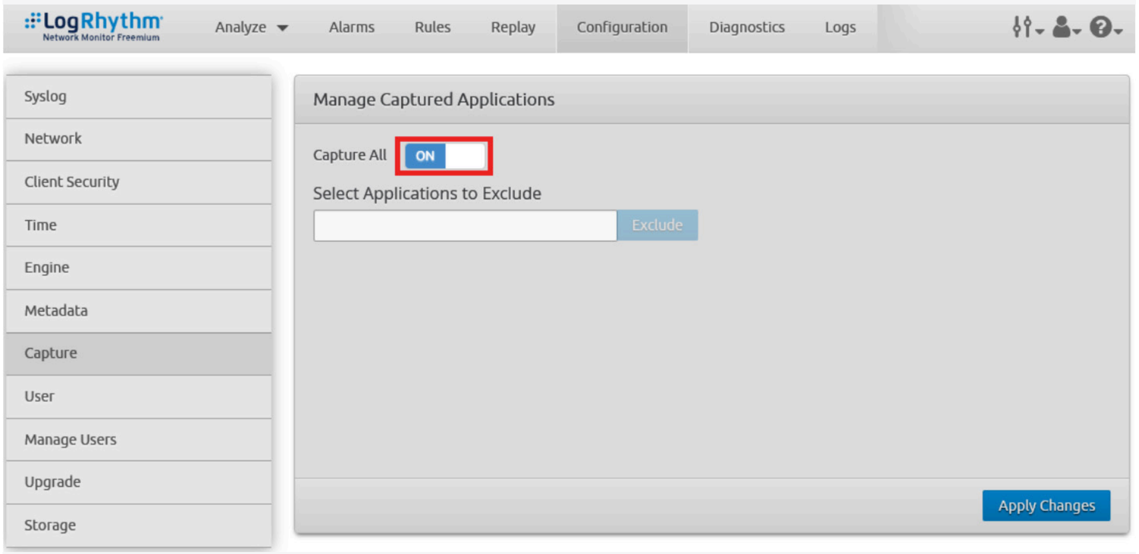
Interface	IP Address	Packet Rate	Data Rate	Capture
ens32	10.0.1.108	3 packets/s	551 bytes/s	□ Capture This Interface
ens33		0 packets/s	0 bytes/s	☑ Capture This Interface
ens34	192.168.0.10	0 packets/s	0 bytes/s	□ Capture This Interface

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



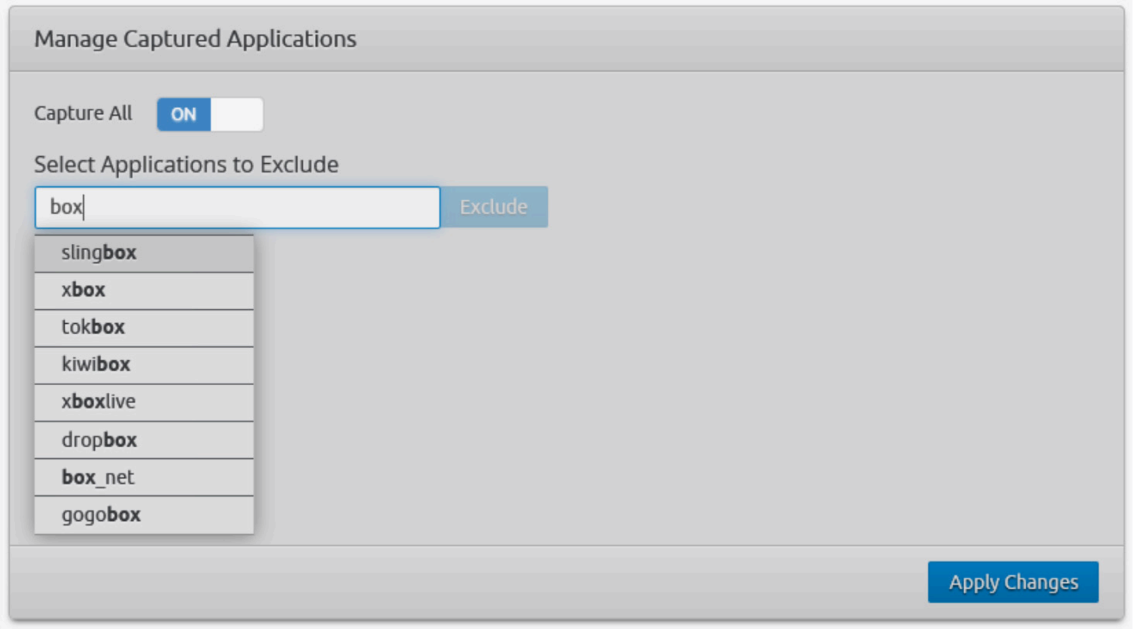
Step 3. To specify what applications are to be monitored, navigate to **Configuration > Capture**.

To capture all applications, toggle the **Capture All** field to **ON**, and click the **Apply Changes** button.



Capture All: ON

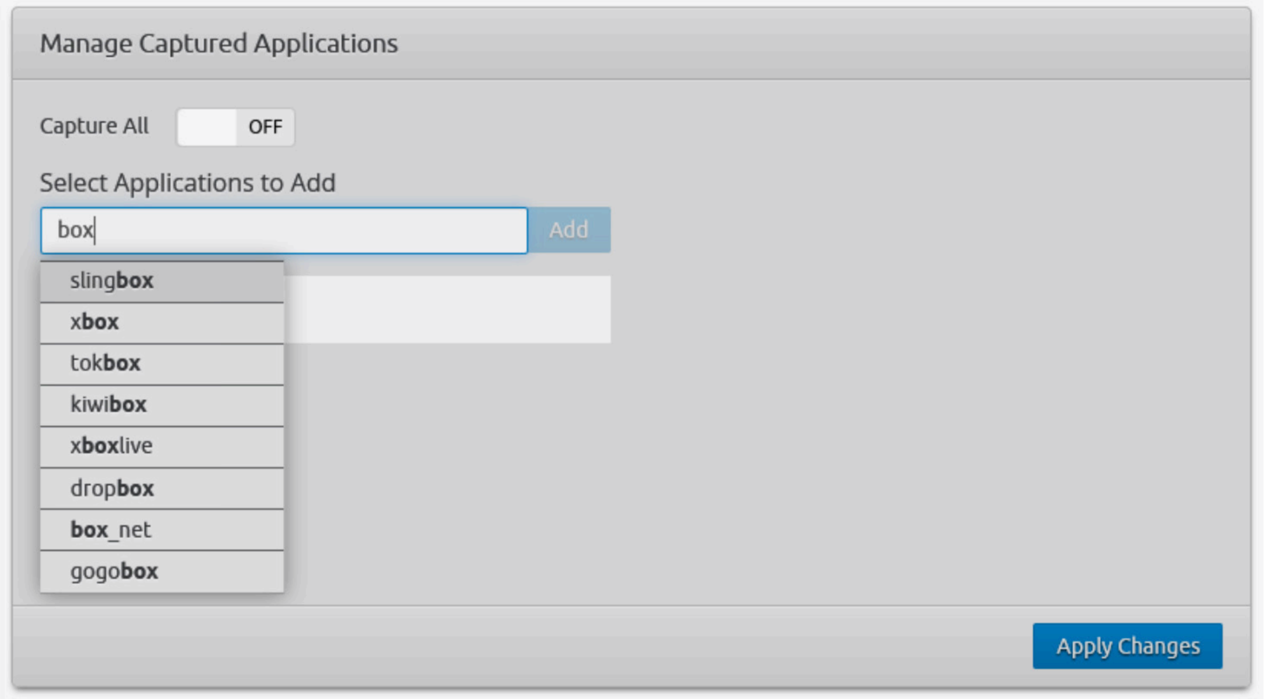
To capture all applications and exclude a subset of applications, list the applications to be excluded after the **Capture All** field is toggled **ON** by typing the application name.



Capture All: ON

Select Applications to Exclude: box

To include only a subset of applications, toggle the **Capture All** field to **OFF**, and type the application names to be included.



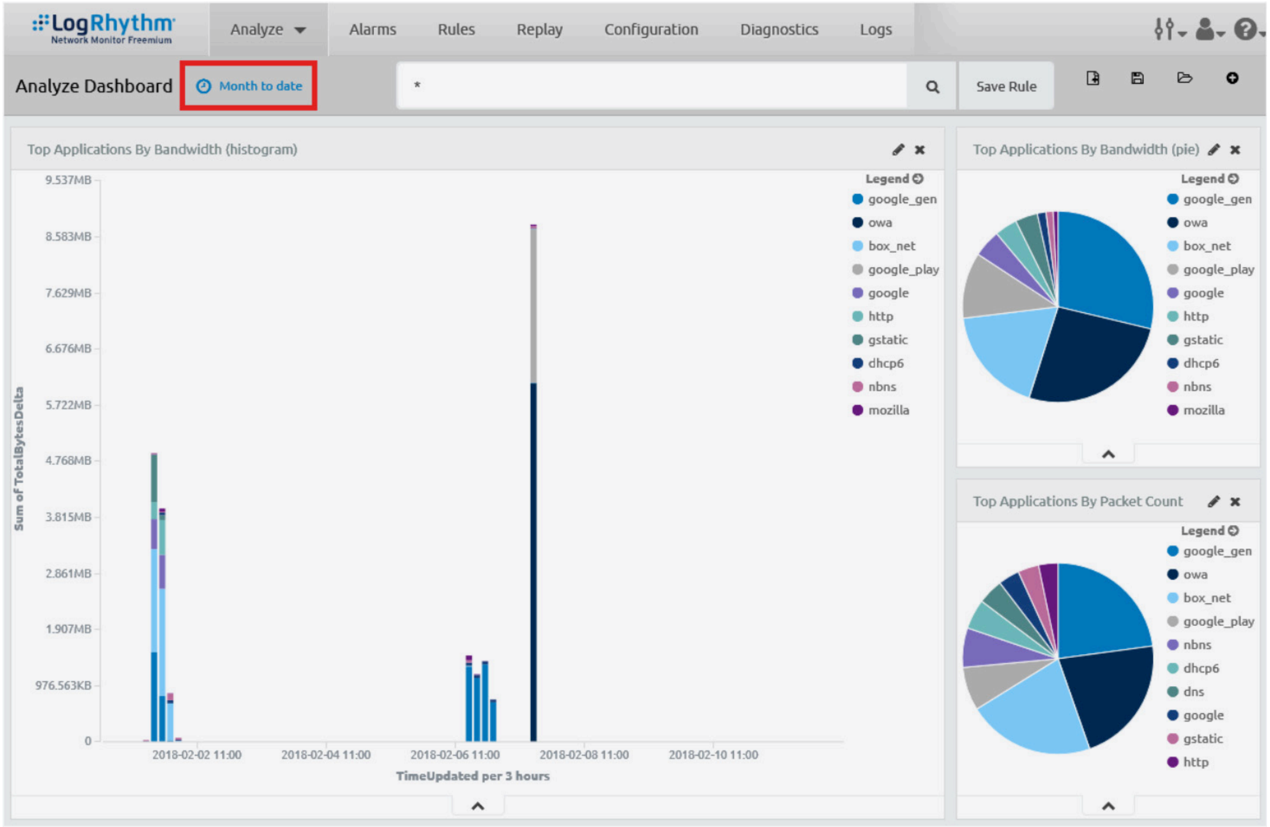
Manage Captured Applications

Capture All: OFF

Select Applications to Add: box

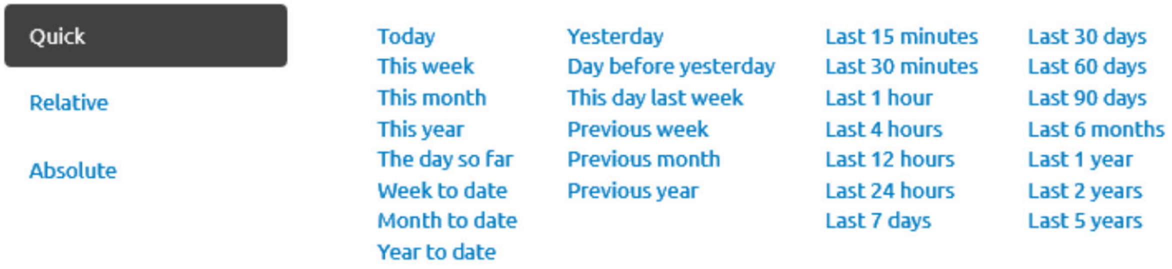
Contents

Step 4. For a quick overview of all traffic captured by LogRhythm, navigate to **Analyze > Dashboards**.

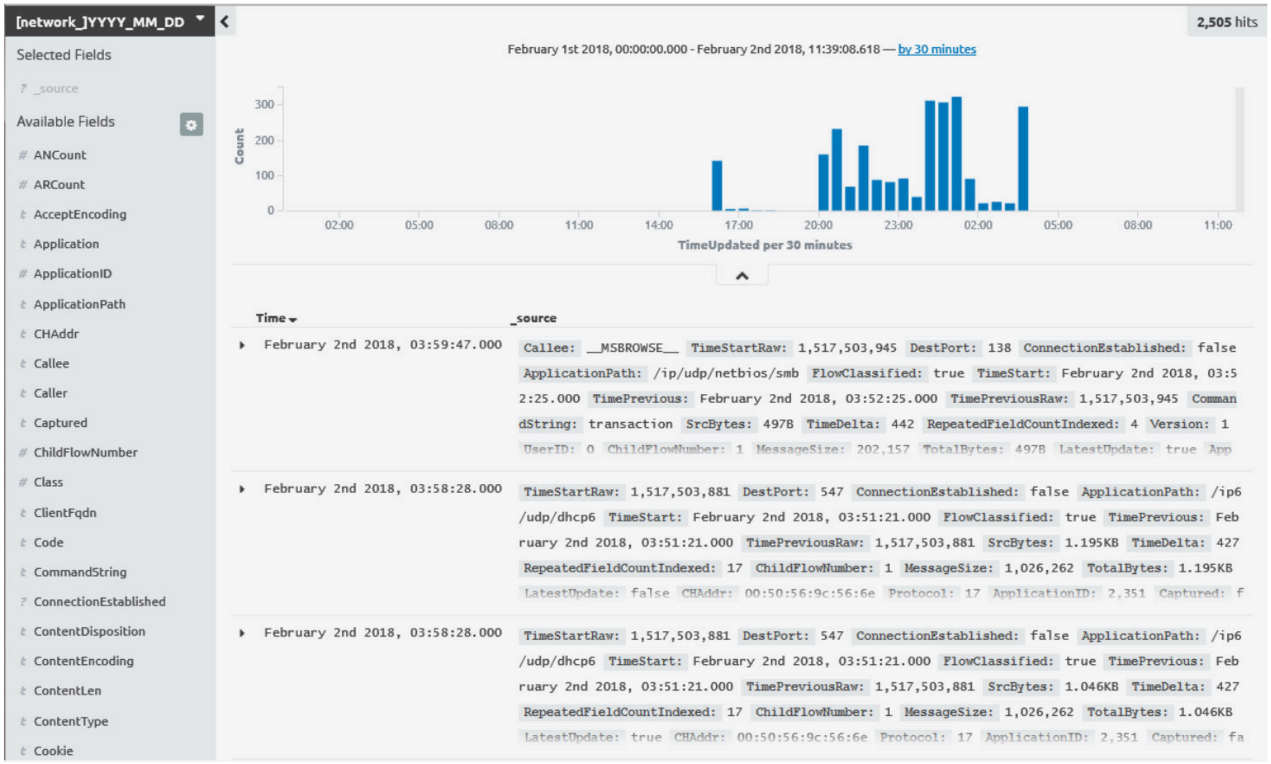


Contents

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.



Step 5. To view the tapped traffic from WSA, navigate to **Analyze > Discover** for an overview of all captured traffic.



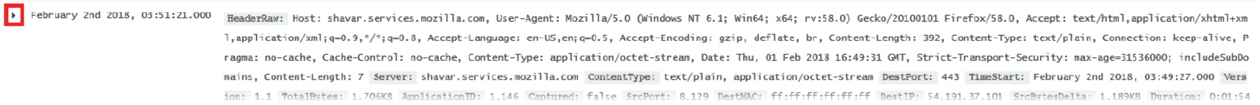
```
February 2nd 2018, 03:59:47.000   Callee: __MSBROWSE__ TimeStartRaw: 1,517,503,945 DestPort: 138 ConnectionEstablished: false
                                  ApplicationPath: /ip/udp/netbios/smb FlowClassified: true TimeStart: February 2nd 2018, 03:5
                                  2:25.000 TimePrevious: February 2nd 2018, 03:52:25.000 TimePreviousRaw: 1,517,503,945 Comman
                                  dString: transaction SrcBytes: 497B TimeDelta: 442 RepeatedFieldCountIndexed: 4 Version: 1
                                  UserID: 0 ChildFlowNumber: 1 MessageSize: 202,157 TotalBytes: 497B LatestUpdate: true App

February 2nd 2018, 03:58:28.000   TimeStartRaw: 1,517,503,881 DestPort: 547 ConnectionEstablished: false ApplicationPath: /ip6
                                  /udp/dhcp6 TimeStart: February 2nd 2018, 03:51:21.000 FlowClassified: true TimePrevious: Feb
                                  ruary 2nd 2018, 03:51:21.000 TimePreviousRaw: 1,517,503,881 SrcBytes: 1.195KB TimeDelta: 427
                                  RepeatedFieldCountIndexed: 17 ChildFlowNumber: 1 MessageSize: 1,026,262 TotalBytes: 1.195KB
                                  LatestUpdate: false CHAddr: 00:50:56:9c:56:6e Protocol: 17 ApplicationID: 2,351 Captured: f

February 2nd 2018, 03:58:28.000   TimeStartRaw: 1,517,503,881 DestPort: 547 ConnectionEstablished: false ApplicationPath: /ip6
                                  /udp/dhcp6 TimeStart: February 2nd 2018, 03:51:21.000 FlowClassified: true TimePrevious: Feb
                                  ruary 2nd 2018, 03:51:21.000 TimePreviousRaw: 1,517,503,881 SrcBytes: 1.046KB TimeDelta: 427
                                  RepeatedFieldCountIndexed: 17 ChildFlowNumber: 1 MessageSize: 1,026,262 TotalBytes: 1.046KB
                                  LatestUpdate: true CHAddr: 00:50:56:9c:56:6e Protocol: 17 ApplicationID: 2,351 Captured: fa
```

Contents

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.



```
▸ February 2nd 2018, 03:51:21.000   HeaderRaw: Host: shavar.services.mozilla.com, User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0, Accept: text/html,application/xhtml+xm
                                    l,application/xml;q=0.9,*/*;q=0.8, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, br, Content-Length: 392, Content-Type: text/plain, Connection: keep-alive, P
                                    ragma: no-cache, Cache-Control: no-cache, Content-Type: application/octet-stream, Date: Thu, 01 Feb 2018 16:49:31 GMT, Strict-Transport-Security: max-age=31536000; includeSubDo
                                    mains, Content-Length: 7 Server: shavar.services.mozilla.com ContentType: text/plain, application/octet-stream DestPort: 443 TimeStart: February 2nd 2018, 03:49:27.000 Vers
                                    ion: 1.1 TotalBytes: 1.706KB ApplicationID: 1,146 Captured: false SrcPort: 8,129 DestMAC: ff:ff:ff:ff:ff:ff DestIP: 54.191.37.101 SrcBytesDelta: 1.189KB Duration: 0:01:54
```

Step 6. Expanding on any HTTPS traffic will list header information of the plaintext HTTP.

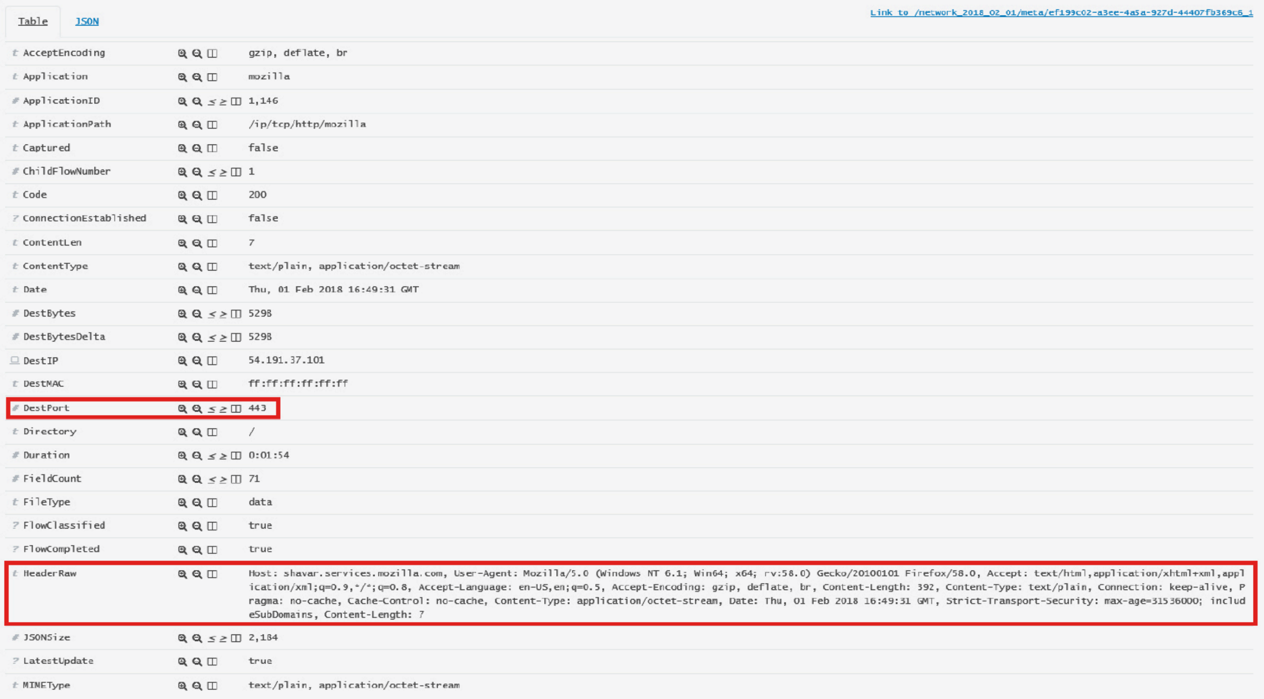


Table JSON

Link to /network_2018_02_01/meta/ef199c02-a3ee-4a5a-927d-44407fb369c6_1

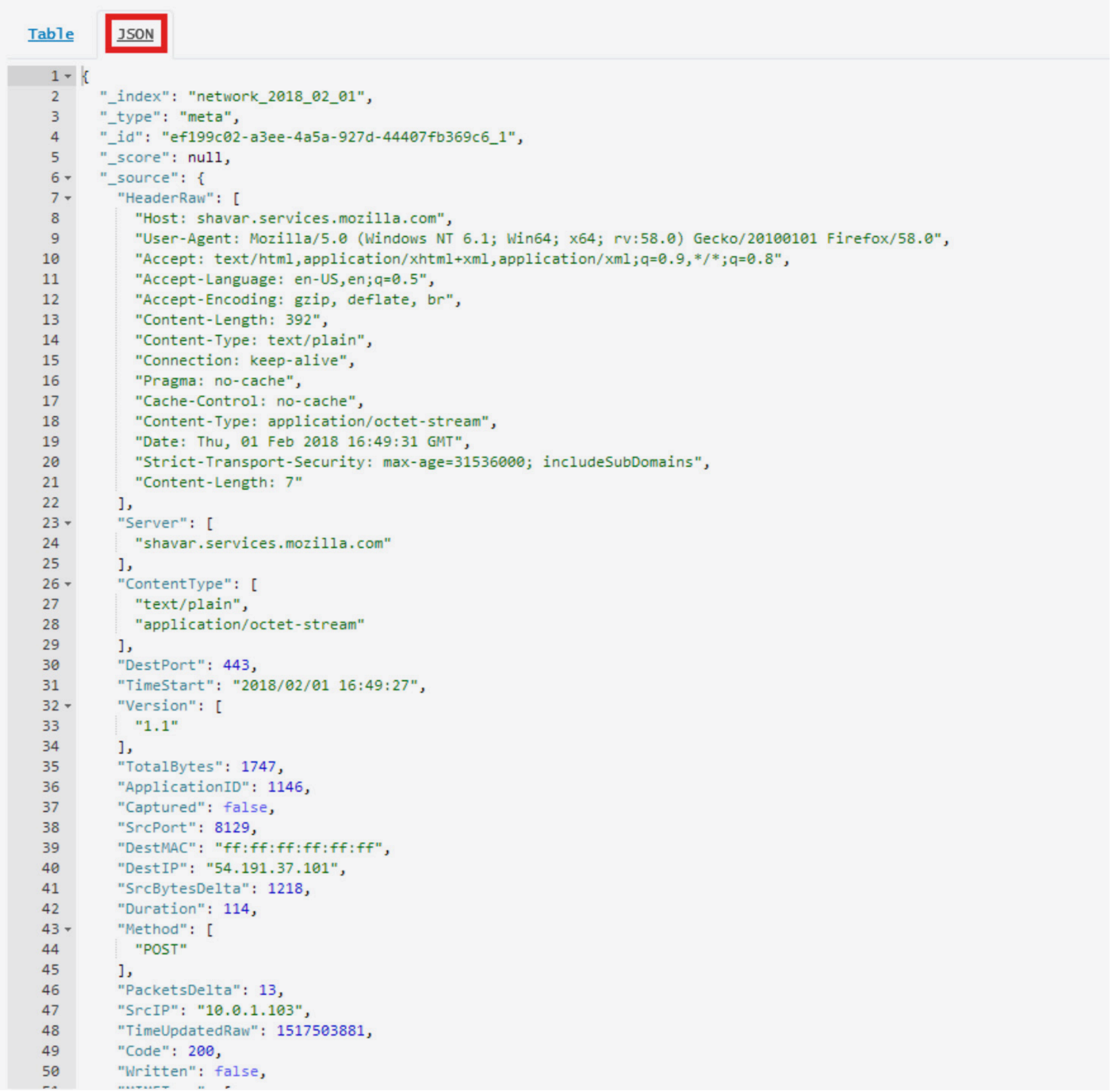
AcceptEncoding	gzip, deflate, br
Application	mozilla
ApplicationID	1,146
ApplicationPath	/ip/tcp/http/mozilla
Captured	false
ChildFlowNumber	1
Code	200
ConnectionEstablished	false
ContentLen	7
ContentType	text/plain, application/octet-stream
Date	Thu, 01 Feb 2018 16:49:31 GMT
DestBytes	529B
DestBytesDelta	529B
DestIP	54.191.37.101
DestMAC	ff:ff:ff:ff:ff:ff
DestPort	443
Directory	/
Duration	0:01:54
FieldCount	71
FileType	data
FlowClassified	true
FlowCompleted	true
HeaderRaw	Host: shavar.services.mozilla.com, User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, br, Content-Length: 392, Content-Type: text/plain, Connection: keep-alive, Pragma: no-cache, Cache-Control: no-cache, Content-Type: application/octet-stream, Date: Thu, 01 Feb 2018 16:49:31 GMT, Strict-Transport-Security: max-age=31536000; includeSubDomains, Content-Length: 7
JSONSize	2,184
LatestUpdate	true
MIMEType	text/plain, application/octet-stream

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.



```
{
  "_index": "network_2018_02_01",
  "_type": "meta",
  "_id": "ef199c02-a3ee-4a5a-927d-44407fb369c6_1",
  "_score": null,
  "_source": {
    "HeaderRaw": [
      "Host: shavar.services.mozilla.com",
      "User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0",
      "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
      "Accept-Language: en-US,en;q=0.5",
      "Accept-Encoding: gzip, deflate, br",
      "Content-Length: 392",
      "Content-Type: text/plain",
      "Connection: keep-alive",
      "Pragma: no-cache",
      "Cache-Control: no-cache",
      "Content-Type: application/octet-stream",
      "Date: Thu, 01 Feb 2018 16:49:31 GMT",
      "Strict-Transport-Security: max-age=31536000; includeSubDomains",
      "Content-Length: 7"
    ],
    "Server": [
      "shavar.services.mozilla.com"
    ],
    "ContentType": [
      "text/plain",
      "application/octet-stream"
    ],
    "DestPort": 443,
    "TimeStart": "2018/02/01 16:49:27",
    "Version": [
      "1.1"
    ],
    "TotalBytes": 1747,
    "ApplicationID": 1146,
    "Captured": false,
    "SrcPort": 8129,
    "DestMAC": "ff:ff:ff:ff:ff:ff",
    "DestIP": "54.191.37.101",
    "SrcBytesDelta": 1218,
    "Duration": 114,
    "Method": [
      "POST"
    ],
    "PacketsDelta": 13,
    "SrcIP": "10.0.1.103",
    "TimeUpdatedRaw": 1517503881,
    "Code": 200,
    "Written": false,
```

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.