# Integration of Cisco Web Security Appliance Web Traffic Tap with Cisco IDS

## 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 log management system to provide a consolidated end point, network, and security analytics. This provides a faster detection rate, which, in turn, will prevent cyber threats. Consolidated log systems also provide 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 Intrusion Detection System (IDS). In this setup, we have used Cisco Next-Generation Intrusion Prevention System (NGIPS) to function as IDS via Cisco Firepower® Management Center (FMC). Because virtual devices do not have web interfaces, you must use the Command-Line Interface (CLI) to register a virtual device to FMC, which can be physical or virtual.

This document covers:

- Introduction to Cisco IDS (NGIPS in passive mode)
- Introduction to Web Traffic Tap
- Prerequisites
- Web Traffic Tap configuration on WSA
- Traffic collection configuration on Cisco IDS and FMC
- View and analyze web traffic in FMC
- Build a view in FMC
- Conclusion

## Introduction to Cisco IDS

Cisco Intrusion Detection System is a signature-based detection approach. In IDS mode, it generates an alert when the signature matches the malicious traffic, whereas in IPS mode, it generates an alert and blocks malicious traffic.

Cisco Next-generation Intrusion Prevention System deployed in passive mode functions as an IDS. In a passive deployment, virtual devices can perform network-based file and malware detection and security intelligence monitoring, as well as network discovery. In this document, IDS is deployed in promiscuous mode, where it can sense the network traffic but is not in the direct path within the network, which eliminates the possibility of any network impact in the event of failure.

The core capabilities of Cisco IDS are:

- Set a baseline of normal network behavior to help identify abnormal activities
- Perform deep packet capture for advanced forensics
- Detect unauthorized or suspicious application activities

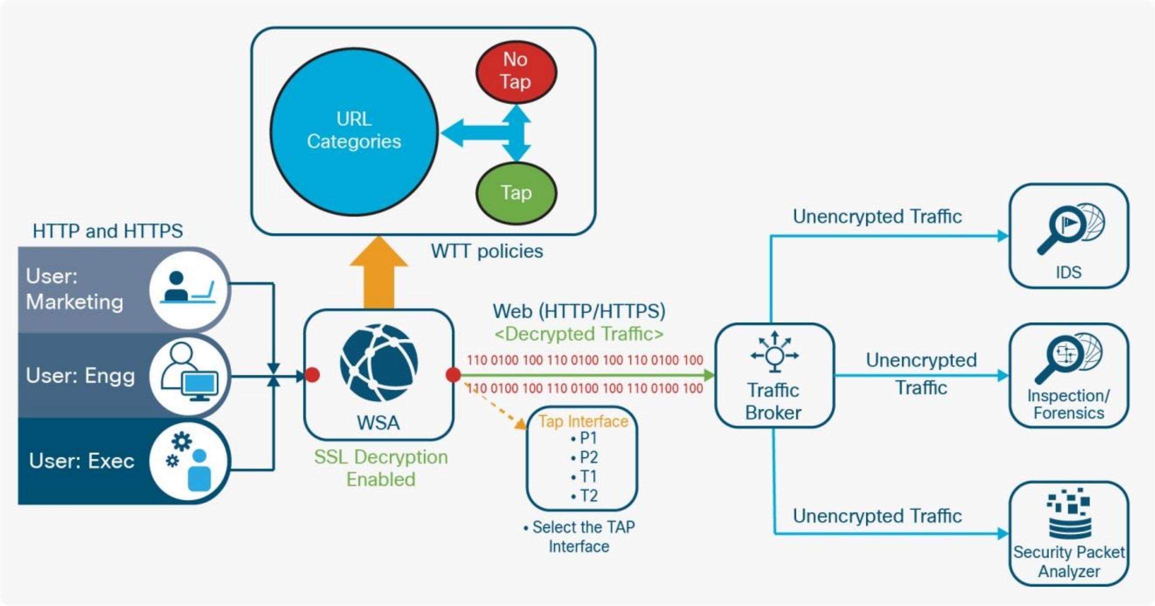
In this document, we are integrating IDS with WSA Web Traffic Tap to run advanced forensics and compliance.

## 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 (WTT) – Feature overview



## Prerequisites

Cisco recommends that you have knowledge of these topics:

- Cisco WSA
- Cisco NGIPS/IDS
- Cisco FMC

### Components Used

The information in this document is based on these software and hardware versions:

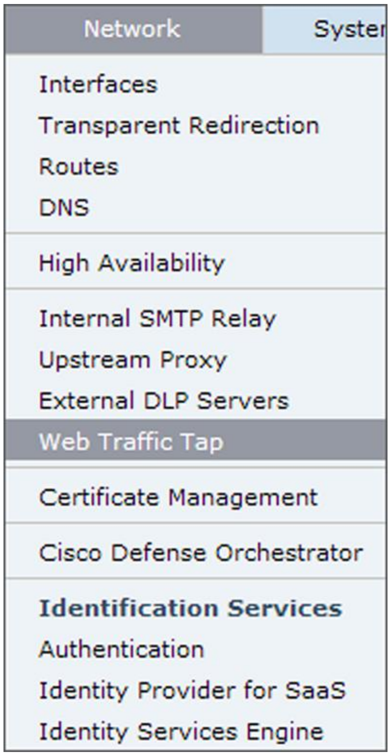
- Cisco WSA Version 11.5.1
- Cisco NGIPSv for VMware Version 6.2.2 (build 81)
- Cisco FMC for VMWare Version 6.2.2 (build 81)

**Note:** Contents of the document were created from the devices in a specific lab environment. All of the devices used in this document were started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

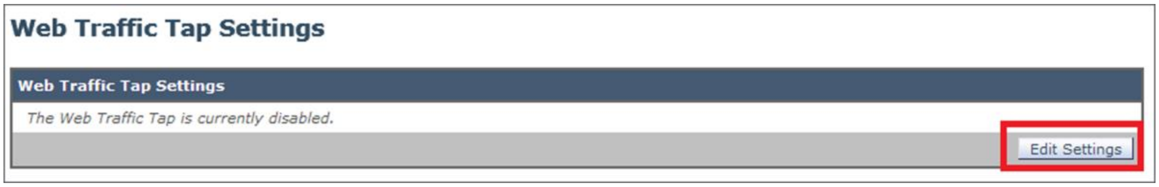
## Web Traffic Tap configuration on WSA

**Step 1** – Log in to the WSA UI using admin credential: https://wsa_hostname:8443.

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



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

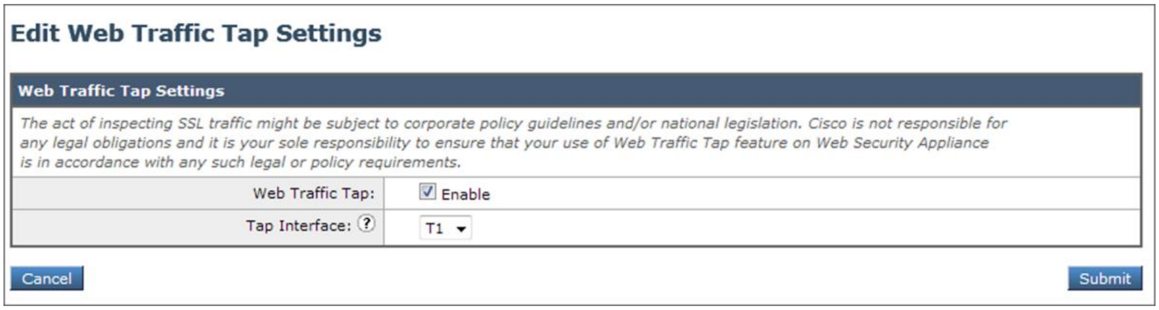

Web Traffic Tap Settings

Web Traffic Tap Settings

The Web Traffic Tap is currently disabled.

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

**Note:** The IDS needs to listen on the network configured for Tap Interface, which is covered in a later section.



Edit Web Traffic Tap Settings

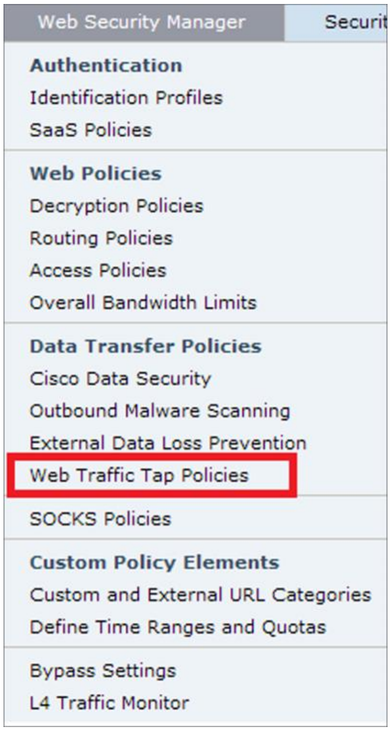
Web Traffic Tap Settings

*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.*

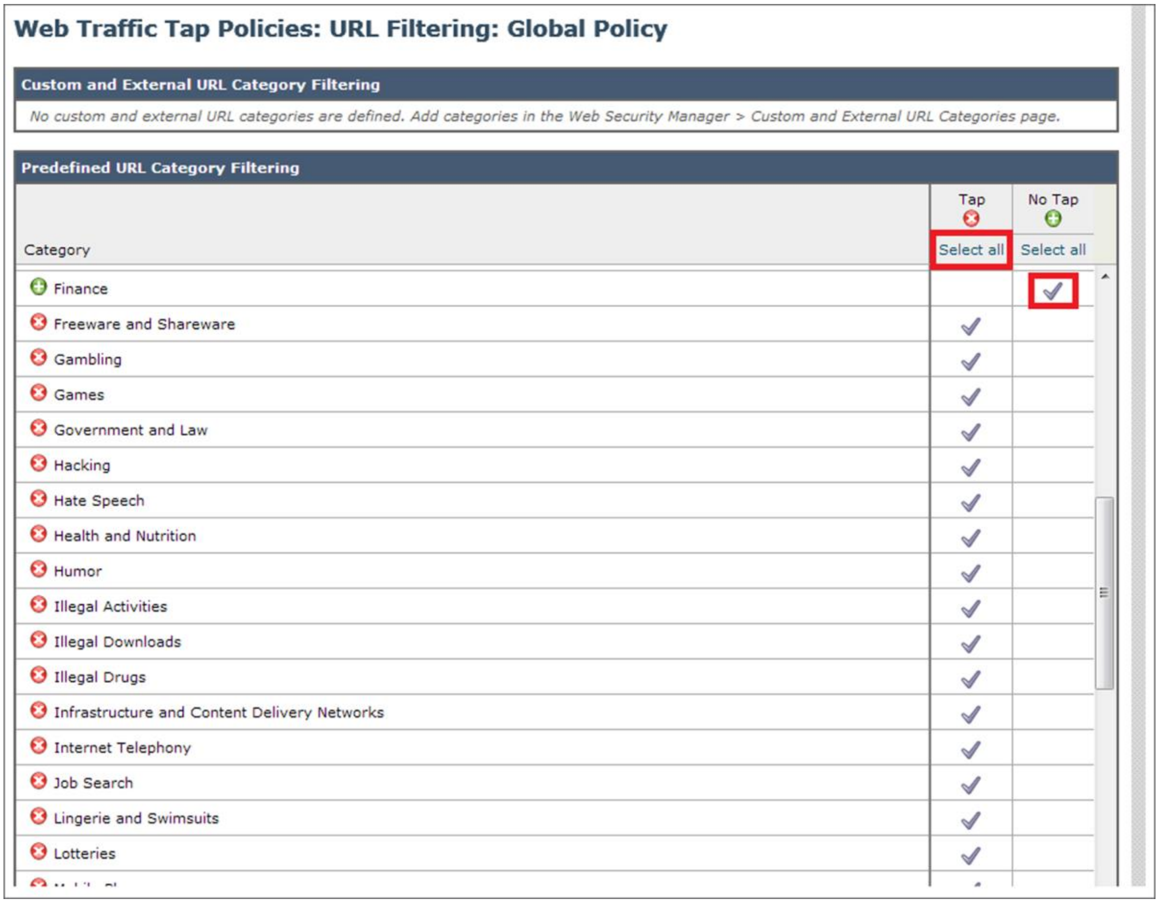
| | |
|---|---|
| Web Traffic Tap: | ☑ Enable |
| Tap Interface: ? | T1 |

**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 the **No Tap** policy configured.



**Step 6** – To enable all URL categories to be monitored by IDS except the finance category, click **Select all** on the **Tap** column and **Select Finance** on the **No Tap** column. Click **Submit** to enable it.



**Web Traffic Tap Policies: URL Filtering: Global Policy**

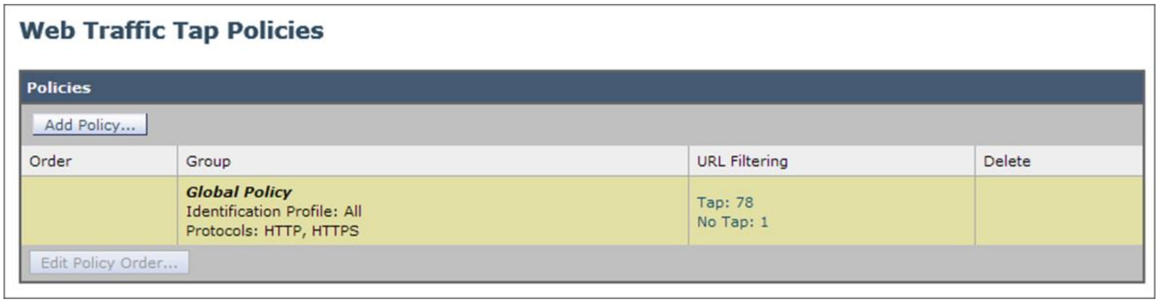
**Custom and External URL Category Filtering**

*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**

| Category | Tap ⊗<br>Select all | No Tap ⊕<br>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 policy.



**Web Traffic Tap Policies**

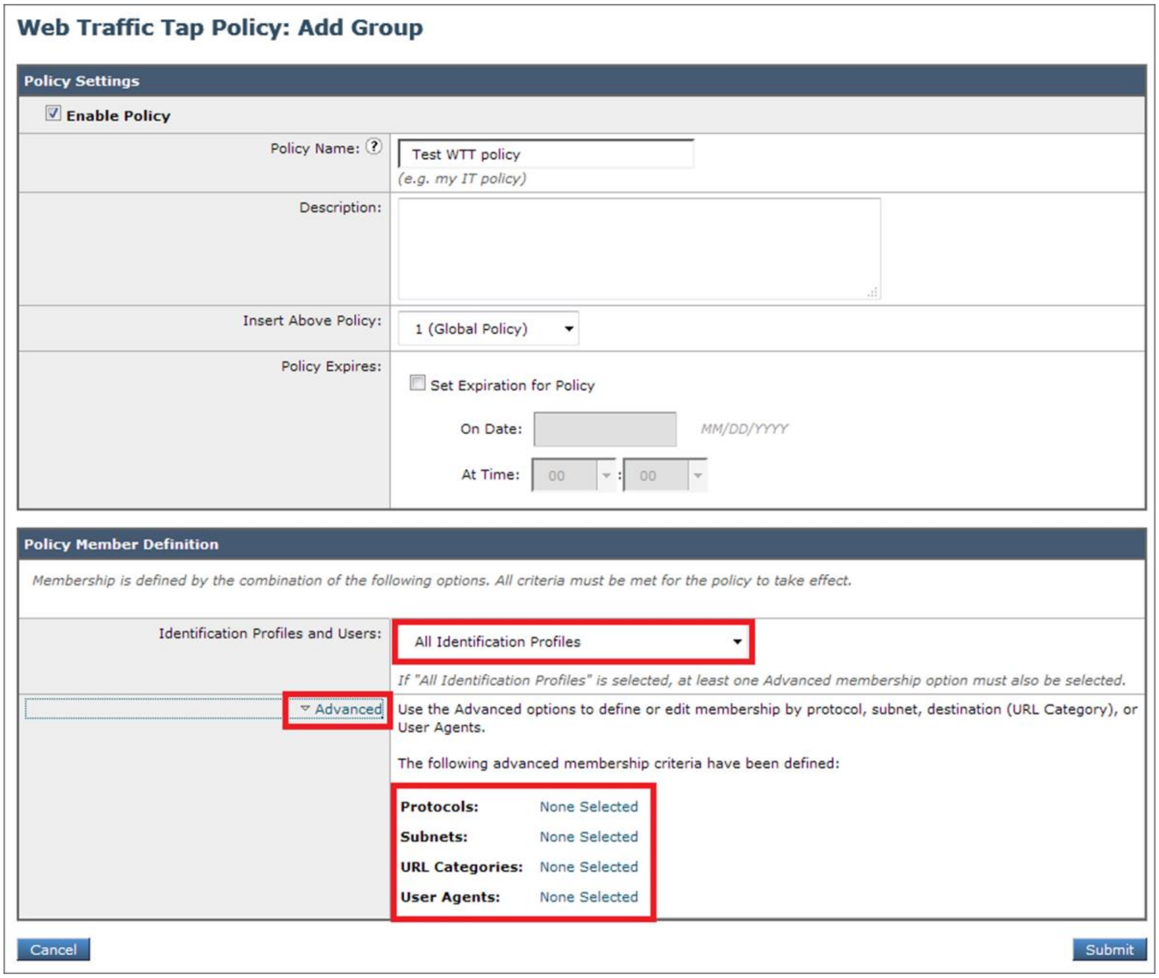
**Policies**

| Order | Group | URL Filtering | Delete |
|---|---|---|---|
| | ***Global Policy***<br>Identification Profile: All<br>Protocols: HTTP, HTTPS | Tap: 78<br>No Tap: 1 | |

**Note:** If specific policies are required, it can be added through the Add Policy… button.

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

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



**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.*

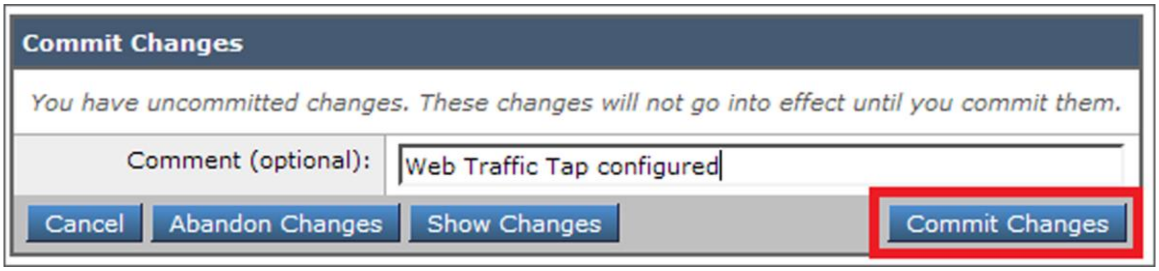
▿ Advanced

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 |

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

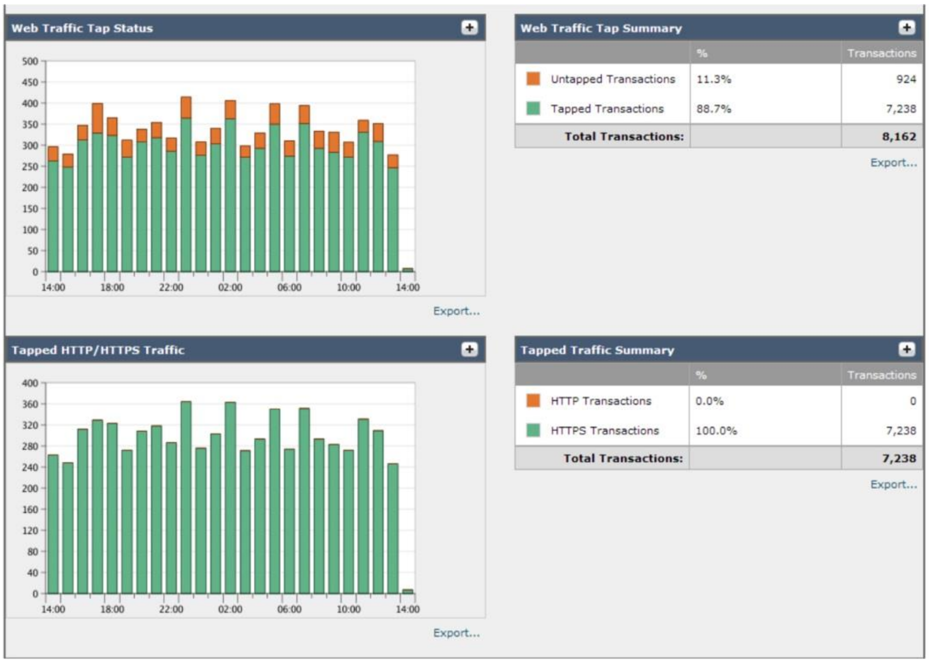


**Commit Changes**

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

Comment (optional): Web Traffic Tap configured

**Step 8** – Summary of 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...

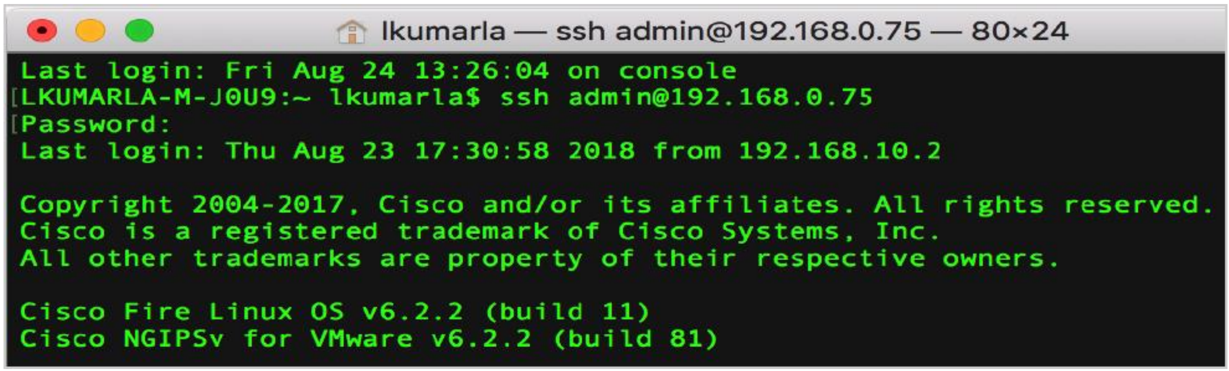
Tapped Traffic Summary

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

Export...

## Traffic collection configuration on Cisco IDS and FMC

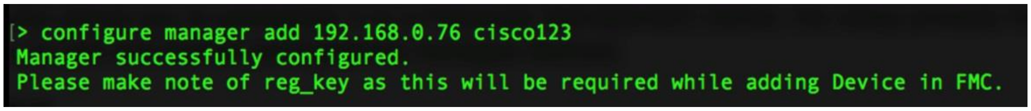
**Step 1** – Log in to Cisco IDS (NGIPS) CLI interface via Secure Shell (SSH) Protocol.



```
 Last login: Fri Aug 24 13:26:04 on console
[LKUMARLA-M-J0U9:~ lkumarla$ ssh admin@192.168.0.75
[Password:
 Last login: Thu Aug 23 17:30:58 2018 from 192.168.10.2

 Copyright 2004-2017, Cisco and/or its affiliates. All rights reserved.
 Cisco is a registered trademark of Cisco Systems, Inc.
 All other trademarks are property of their respective owners.

 Cisco Fire Linux OS v6.2.2 (build 11)
 Cisco NGIPSv for VMware v6.2.2 (build 81)
```

**Step 2** – At the prompt, register the device to an FMC using the **configure manager add** command. A unique self-generated alphanumeric registration key is always required to register a device to an FMC.

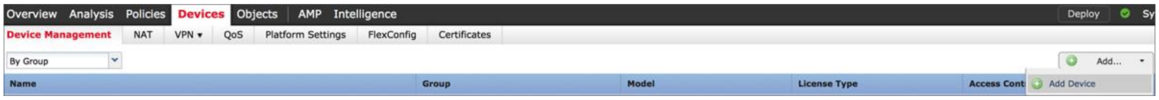
In most cases, you must provide the FMC's IP address along with the registration key. For example:



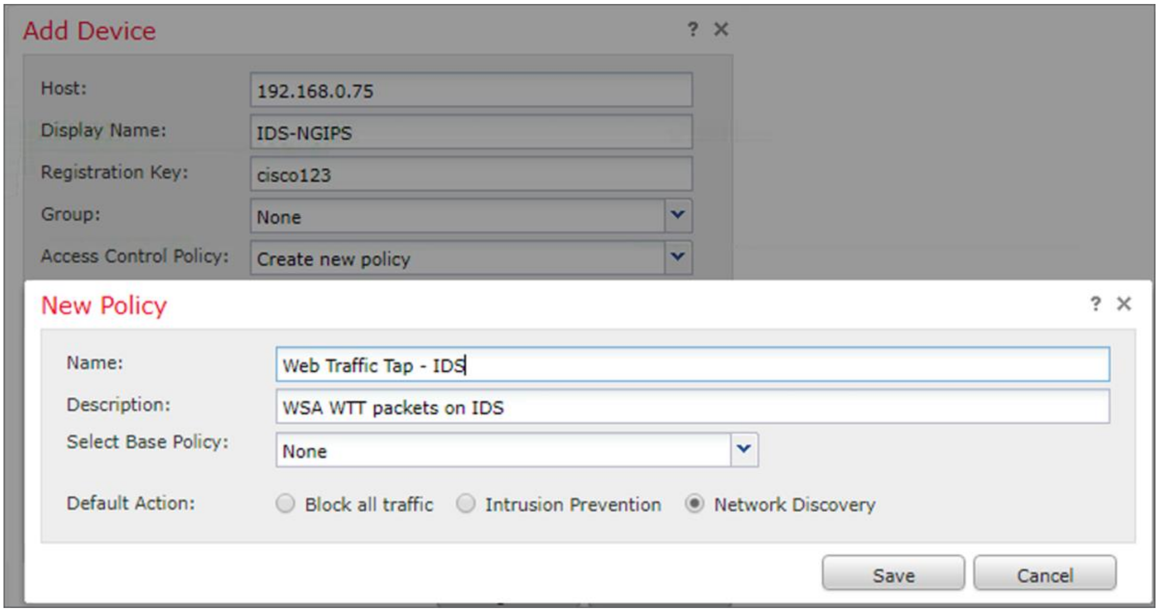
```
[> configure manager add 192.168.0.76 cisco123
 Manager successfully configured.
 Please make note of reg_key as this will be required while adding Device in FMC.
```

**Note:** When using the Esxi vSphere instance to register a virtual device to an FMC, you must use the IP address (not the hostname) of the managing FMC.

**Step 3** – Log in to the FMC web interface and use the Device Management (**Devices > Device Management**) page to add the device once you have set up the FMC. For more information, see the Managing Devices chapter in the FMC Configuration Guide.



Add IDS details with the same registration key as set on IDS CLI and create a new access policy with default action set to **Network Discovery**. Then click **Save**.



Add Device

Host: 192.168.0.75

Display Name: IDS-NGIPS

Registration Key: cisco123

Group: None

Access Control Policy: Create new policy

New Policy

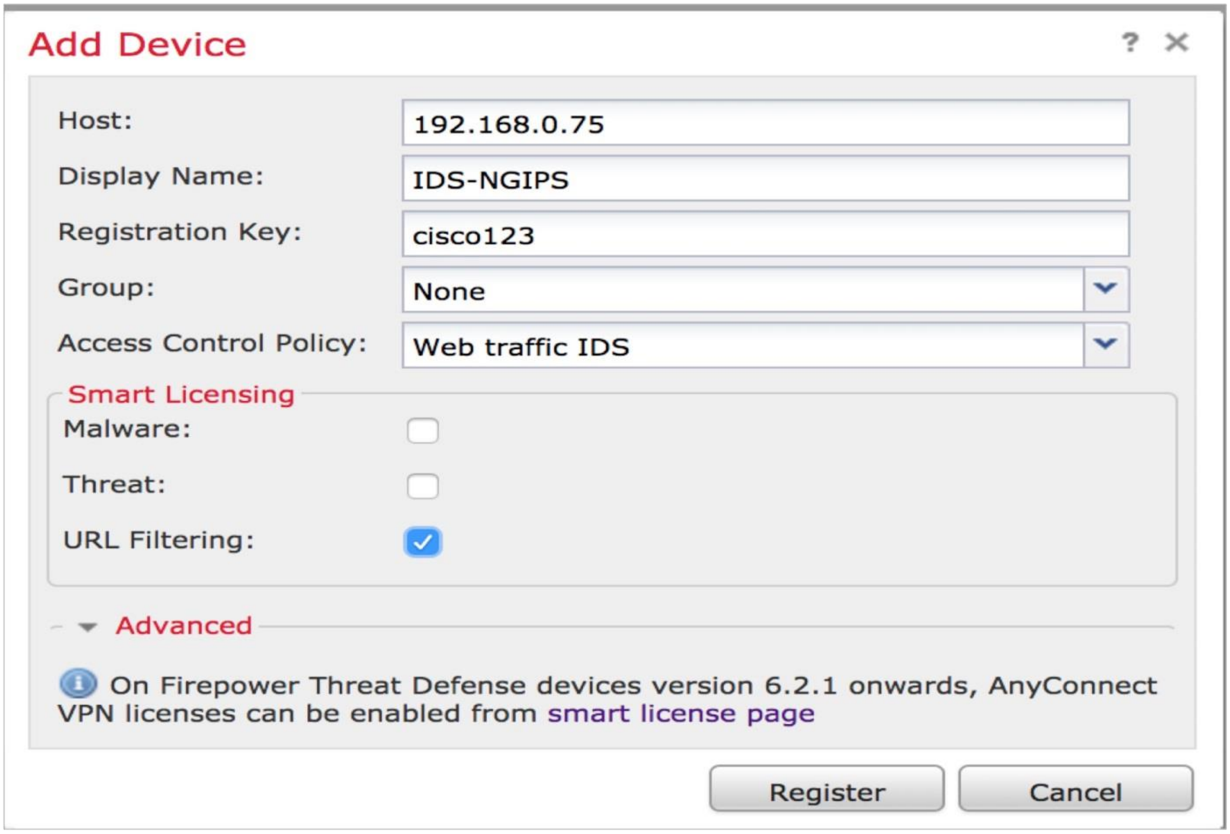
Name: Web Traffic Tap - IDS

Description: WSA WTT packets on IDS

Select Base Policy: None

Default Action: ○ Block all traffic ○ Intrusion Prevention ● Network Discovery

Next, Click on Register and add the IDS device with at least the URL filtering license enabled.



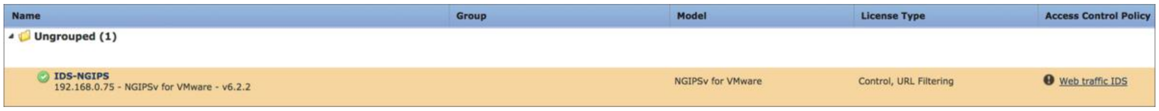
| | |
|---|---|
| Host: | 192.168.0.75 |
| Display Name: | IDS-NGIPS |
| Registration Key: | cisco123 |
| Group: | None |
| Access Control Policy: | Web traffic IDS |

Smart Licensing

| | |
|---|---|
| Malware: | □ |
| Threat: | □ |
| URL Filtering: | ☑ |

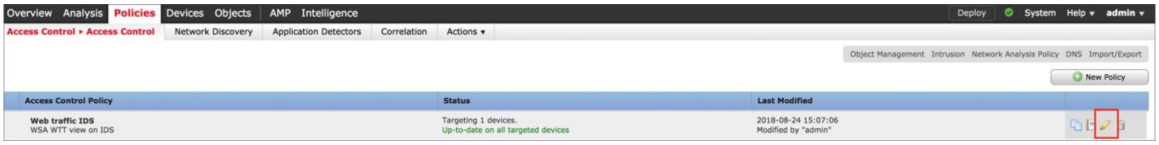
On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from smart license page

Once the device is added successfully, it will appear as shown below:



| Name | Group | Model | License Type | Access Control Policy |
|---|---|---|---|---|
| Ungrouped (1) | | | | |
| IDS-NGIPS<br>192.168.0.75 - NGIPSv for VMware - v6.2.2 | | NGIPSv for VMware | Control, URL Filtering | Web traffic IDS |

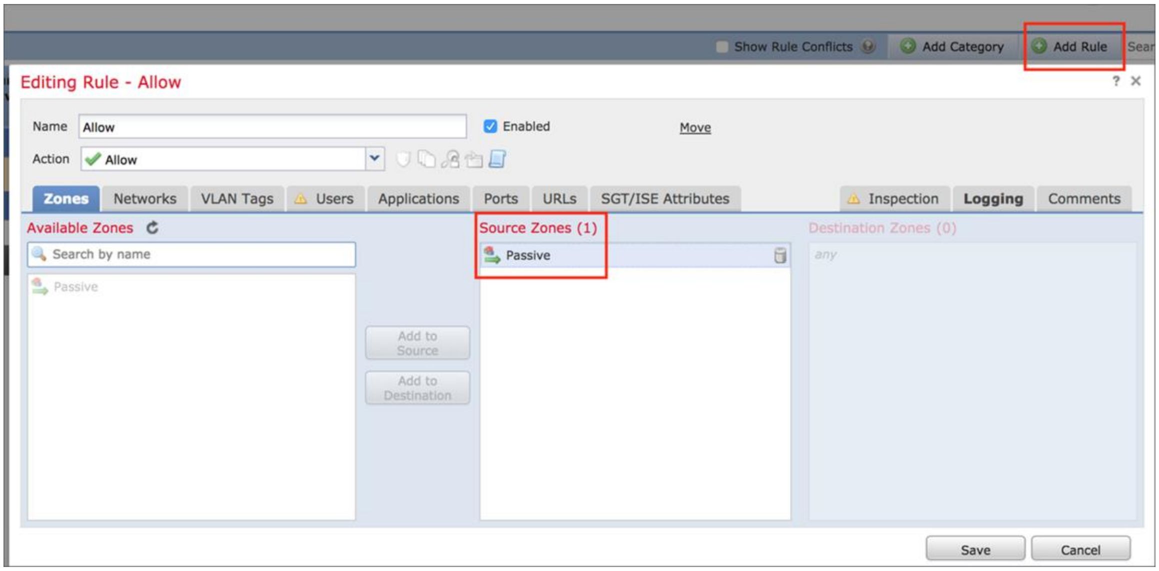
**Step 4** - Go to **Policies > Access Control** and edit the policy created at the time of device registration. Click on the pencil icon to edit a policy or rule as shown below:



Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Access Control ▸ Access Control
Network Discovery
Application Detectors
Correlation
Actions ▾
Object Management Intrusion Network Analysis Policy DNS Import/Export
New Policy

| Access Control Policy | Status | Last Modified |
|---|---|---|
| Web traffic IDS<br>WSA WTT view on IDS | Targeting 1 devices.<br>Up-to-date on all targeted devices | 2018-08-24 15:07:06<br>Modified by "admin" |

Add a new rule to allow the web traffic and set the zone and logging configuration as shown below:



Editing Rule - Allow

Name: Allow ☑ Enabled

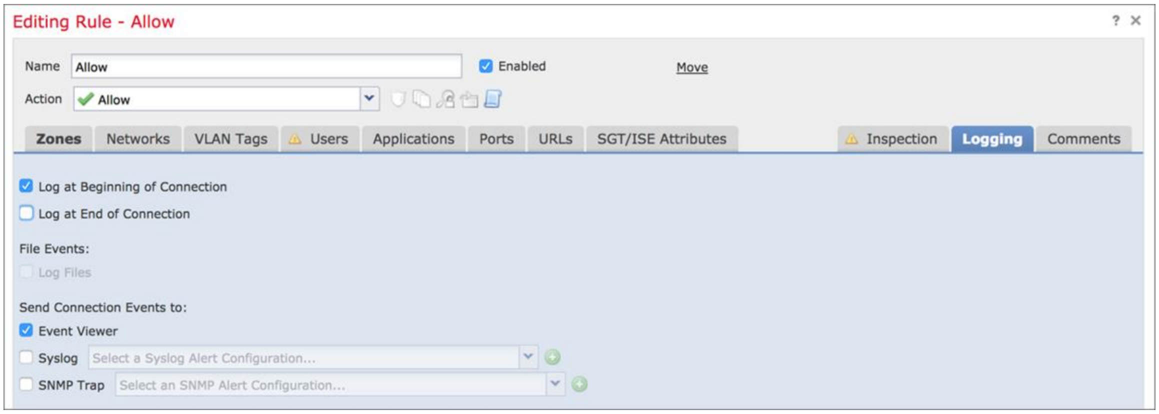
Action: ✓ Allow

Available Zones: Passive

Source Zones (1): Passive

Destination Zones (0): any

**Note:** Checking **the logging at the beginning of the connection** will display the first packet that hits the IDS.



Editing Rule - Allow

Name: Allow ☑ Enabled

Action: ✓ Allow

☑ Log at Beginning of Connection

☐ Log at End of Connection

File Events:

☐ Log Files

Send Connection Events to:

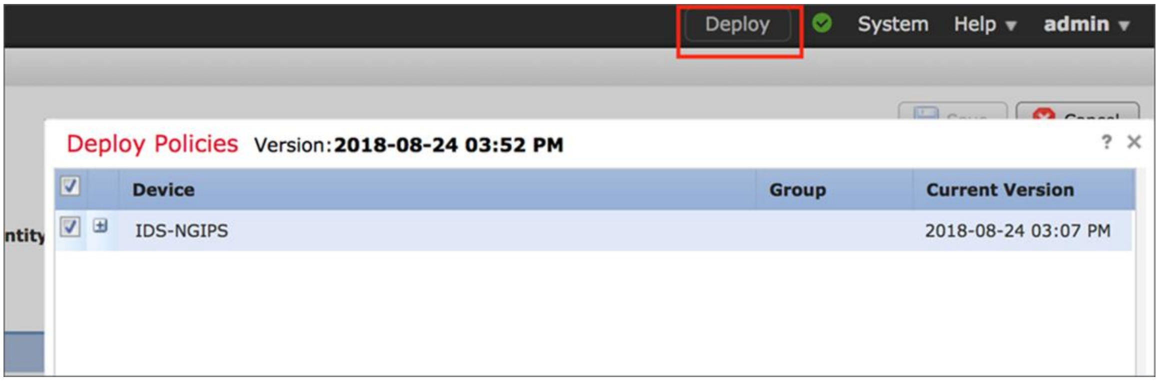
☑ Event Viewer

☐ Syslog Select a Syslog Alert Configuration...

☐ SNMP Trap Select an SNMP Alert Configuration...

Once the policy rules have been added, click **Save** and then deploy the policy to the device.

**Note:** It may take a few minutes to deploy the policy onto IDS.

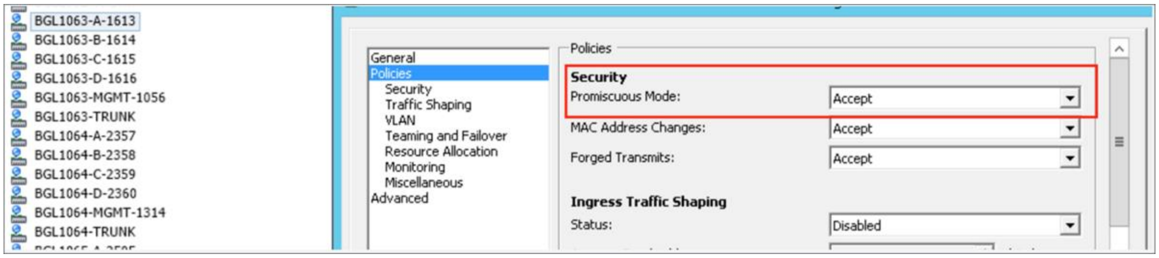


Deploy Policies Version:2018-08-24 03:52 PM

| ☑ | Device | Group | Current Version |
|---|---|---|---|
| ☑ | IDS-NGIPS | | 2018-08-24 03:07 PM |

**Step 5** – Log in to the vSphere client and ensure that the virtual machine settings are configured appropriately for IDS to be able to sense traffic.

The **promiscuous mode** setting on the distribution switch for the respective VLAN network that is used to tap the traffic and for communication between IDS and FMC is to **accept all the network traffic**. Go to **Home > Inventory > Networking > Select switch > portgroup** and edit.



BGL1063-A-1613
BGL1063-B-1614
BGL1063-C-1615
BGL1063-D-1616
BGL1063-MGMT-1056
BGL1063-TRUNK
BGL1064-A-2357
BGL1064-B-2358
BGL1064-C-2359
BGL1064-D-2360
BGL1064-MGMT-1314
BGL1064-TRUNK

Policies

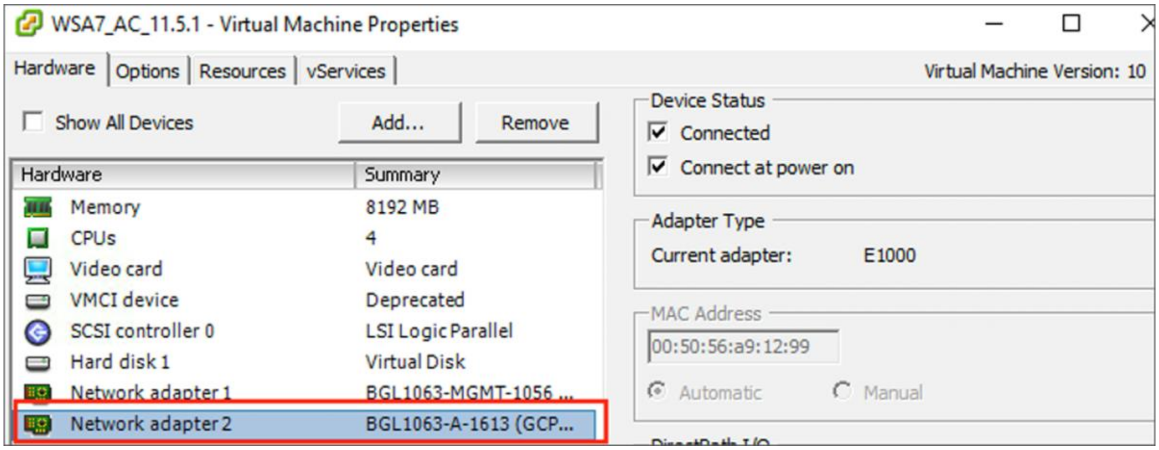
**Security**

| | |
|---|---|
| Promiscuous Mode: | Accept |
| MAC Address Changes: | Accept |
| Forged Transmits: | Accept |

**Ingress Traffic Shaping**

| | |
|---|---|
| Status: | Disabled |

Ensure that the IDS virtual machine has the WSA tap network selected and is connected in the power-on state. For example, in the image below, WSA is set to tap at the P1 interface, which corresponds to Lan A-1613:



WSA7_AC_11.5.1 - Virtual Machine Properties

Virtual Machine Version: 10

□ Show All Devices

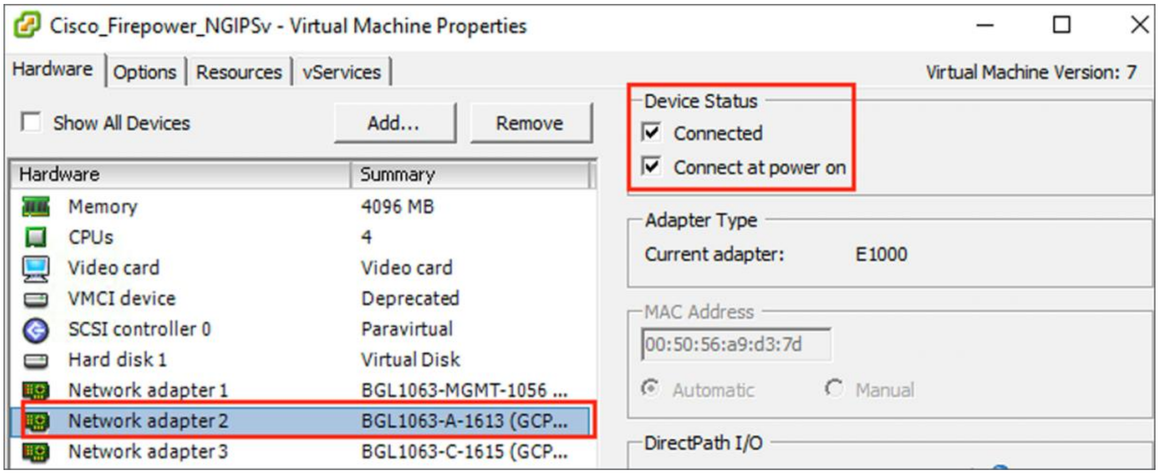
| Hardware | Summary |
|---|---|
| Memory | 8192 MB |
| CPUs | 4 |
| Video card | Video card |
| VMCI device | Deprecated |
| SCSI controller 0 | LSI Logic Parallel |
| Hard disk 1 | Virtual Disk |
| Network adapter 1 | BGL1063-MGMT-1056 ... |
| Network adapter 2 | BGL1063-A-1613 (GCP... |

Device Status
☑ Connected
☑ Connect at power on

Adapter Type
Current adapter: E1000

MAC Address
00:50:56:a9:12:99
● Automatic ○ Manual

The IDS is set to monitor **Lan A-1613** broadcast traffic, which has the WSA tap interface configuration on it.



Cisco_Firepower_NGIPSv - Virtual Machine Properties

Virtual Machine Version: 7

□ Show All Devices

| Hardware | Summary |
|---|---|
| Memory | 4096 MB |
| CPUs | 4 |
| Video card | Video card |
| VMCI device | Deprecated |
| SCSI controller 0 | Paravirtual |
| Hard disk 1 | Virtual Disk |
| Network adapter 1 | BGL1063-MGMT-1056 ... |
| Network adapter 2 | BGL1063-A-1613 (GCP... |
| Network adapter 3 | BGL1063-C-1615 (GCP... |

Device Status
☑ Connected
☑ Connect at power on

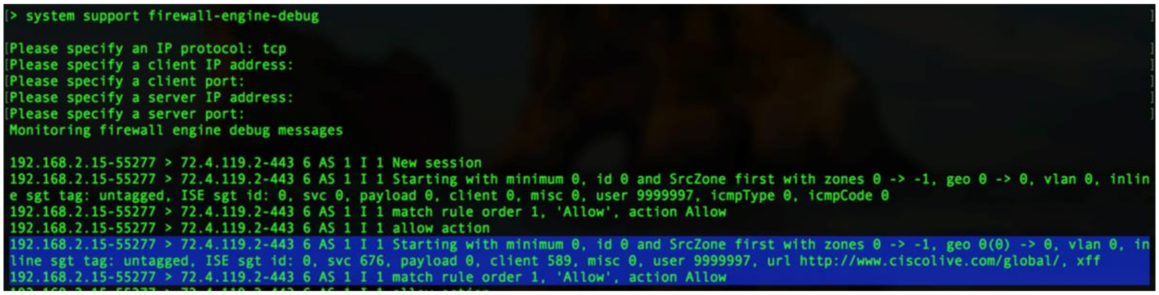
Adapter Type
Current adapter: E1000

MAC Address
00:50:56:a9:d3:7d
● Automatic ○ Manual

DirectPath I/O

With the **firewall-engine-debug** command, you can confirm whether traffic flow is evaluated against the proper access control rule and hitting the IDS device.

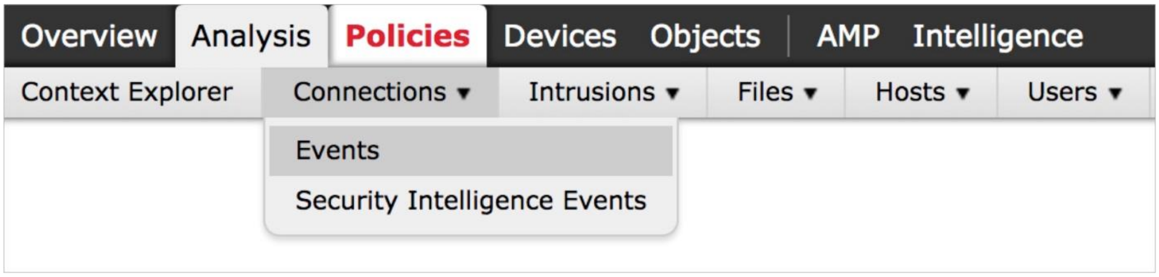
SSH into the IDS CLI interface and run the following command: **system support firewall-engine-debug**.



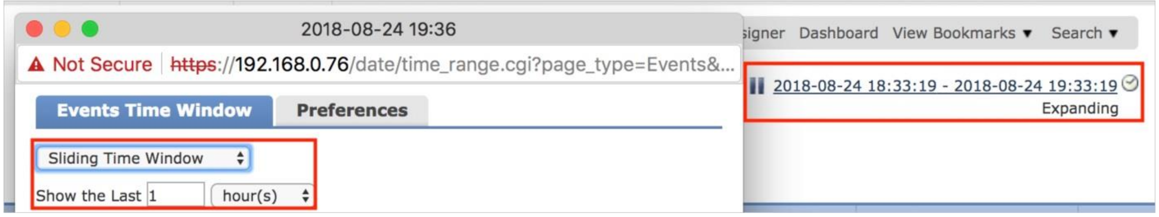
```
> system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

192.168.2.15-55277 > 72.4.119.2-443 6 AS 1 I 1 New session
192.168.2.15-55277 > 72.4.119.2-443 6 AS 1 I 1 Starting with minimum 0, id 0 and SrcZone first with zones 0 -> -1, geo 0 -> 0, vlan 0, inlin
e sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.2.15-55277 > 72.4.119.2-443 6 AS 1 I 1 match rule order 1, 'Allow', action Allow
192.168.2.15-55277 > 72.4.119.2-443 6 AS 1 I 1 allow action
192.168.2.15-55277 > 72.4.119.2-443 6 AS 1 I 1 Starting with minimum 0, id 0 and SrcZone first with zones 0 -> -1, geo 0(0) -> 0, vlan 0, in
line sgt tag: untagged, ISE sgt id: 0, svc 676, payload 0, client 589, misc 0, user 9999997, url http://www.ciscolive.com/global/, xff
192.168.2.15-55277 > 72.4.119.2-443 6 AS 1 I 1 match rule order 1, 'Allow', action Allow
```

## View and analyze web traffic in FMC

**Step 1** - Go to **Analysis > Connections > Events** to view the events. More details about the traffic view are covered in the following section.



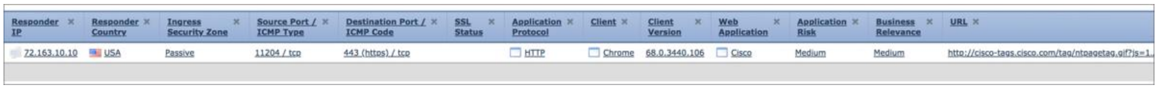
**Step 2** - Click on the time range on the right-hand top corner and select **Sliding Time Window** to show events for the previous hour. This allows you to get optimum output for testing and validation.



Sliding Time Window

Show the Last 1 hour(s)

**Step 3** - Browse the Internet traffic from any of the clients configured to route traffic via WSA and view the results.

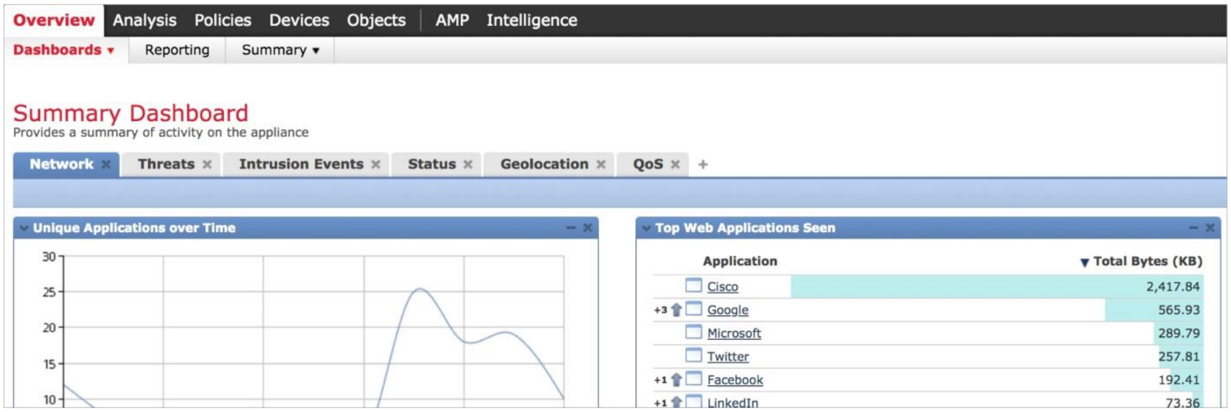


| Responder IP | Responder Country | Ingress Security Zone | Source Port / ICMP Type | Destination Port / ICMP Code | SSL Status | Application Protocol | Client | Client Version | Web Application | Application Risk | Business Relevance | URL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 72.163.10.10 | USA | Passive | 11204 / tcp | 443 (https) / tcp | | HTTP | Chrome | 68.0.3440.106 | Cisco | Medium | Medium | http://cisco-tags.cisco.com/tag/ntpagetag.gif?js=1... |

**Note:** You may pause and resume the events to reload the window.

**Step 4** - You may also browse the most-viewed applications using the **Overview > Dashboards** page.

**Note:** You can may click on any website to view the corresponding events.

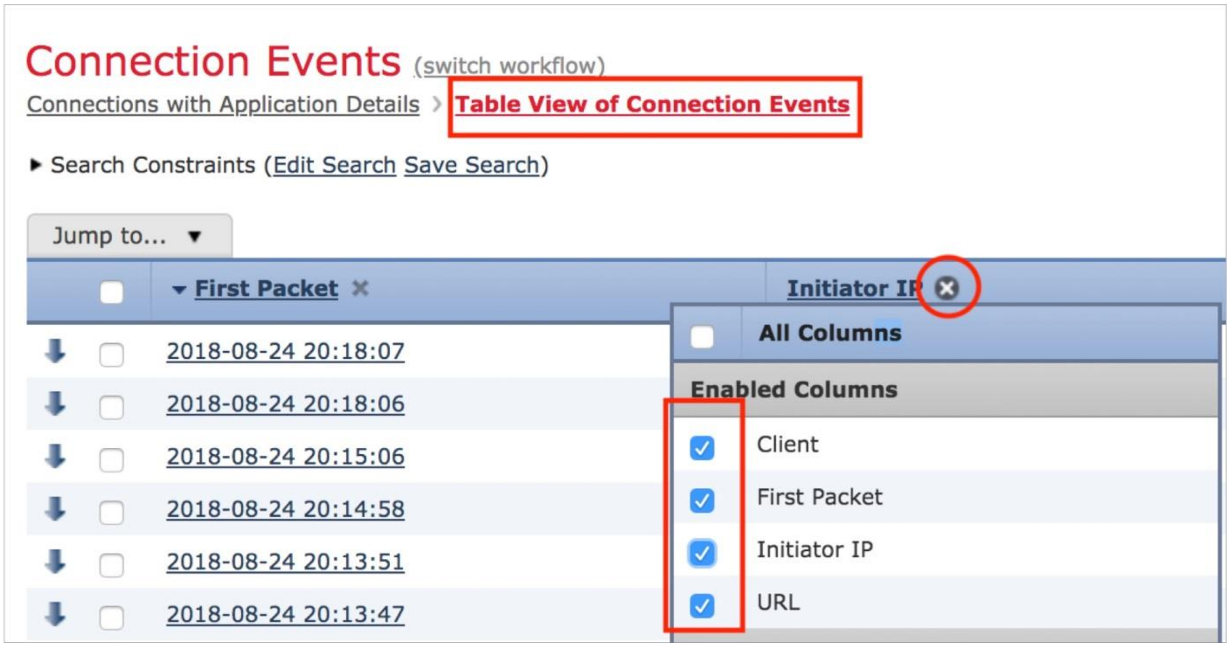


| | Application | ▼ Total Bytes (KB) |
|---|---|---|
| | Cisco | 2,417.84 |
| +3 | Google | 565.93 |
| | Microsoft | 289.79 |
| | Twitter | 257.81 |
| +1 | Facebook | 192.41 |
| +1 | LinkedIn | 73.36 |

## Build a view in FMC

You can customize what columns are shown in the displayed web traffic events and filter the events. The same can also be saved as bookmarks for future use. Shown below is an example to display limited information for a particular client IP address.

**Step 1** - Go to **Analysis > Connections > Events** and click on **Table View of Connection Events**.


Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

| | □ | ▾ First Packet ✕ | Initiator IP ✕ |
|---|---|---|---|
| ⬇ | □ | 2018-08-24 20:18:07 | |
| ⬇ | □ | 2018-08-24 20:18:06 | |
| ⬇ | □ | 2018-08-24 20:15:06 | |
| ⬇ | □ | 2018-08-24 20:14:58 | |
| ⬇ | □ | 2018-08-24 20:13:51 | |
| ⬇ | □ | 2018-08-24 20:13:47 | |

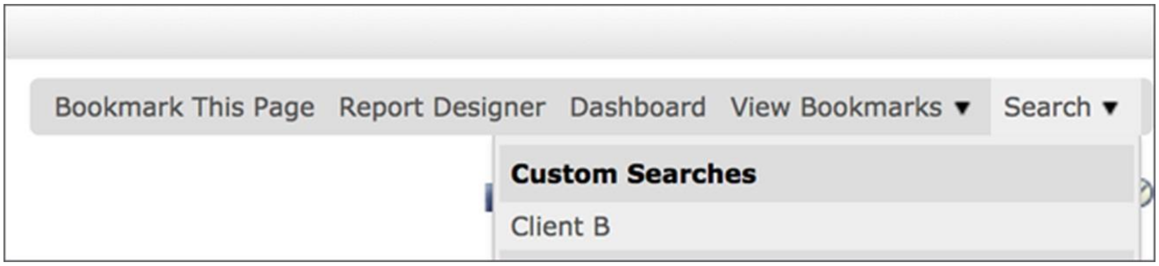
□ All Columns

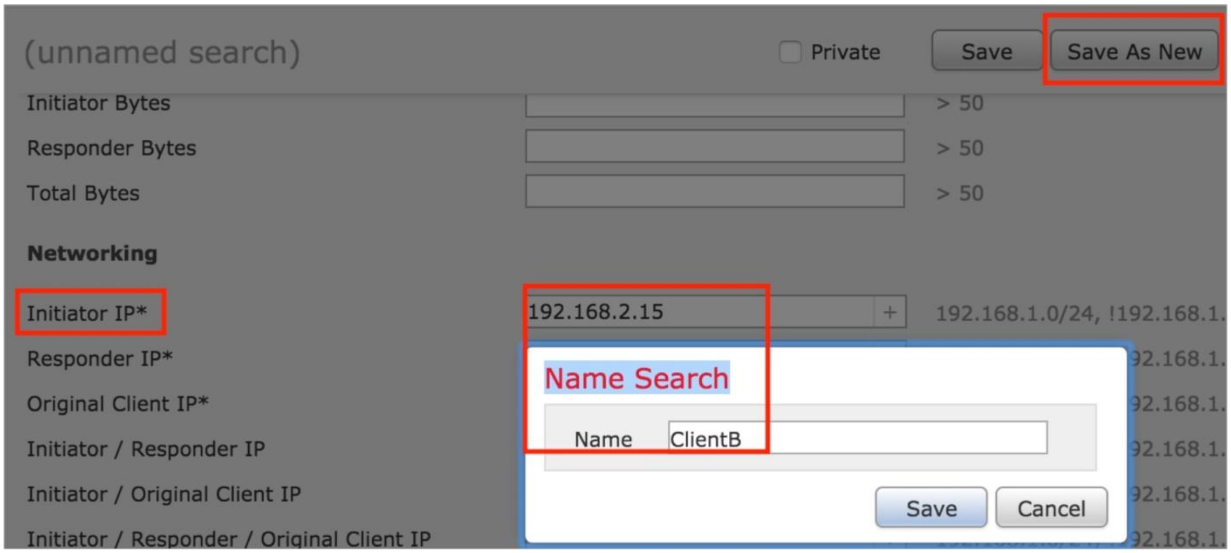
Enabled Columns

- ☑ Client
- ☑ First Packet
- ☑ Initiator IP
- ☑ URL

**Step 2** - As displayed above, click on the cross next to any column and select the options you want to be displayed. Then click **Save.**

**Step 3** - Click on the **Search** icon on the right-hand top corner and enter an initiator IP. Then save the search.

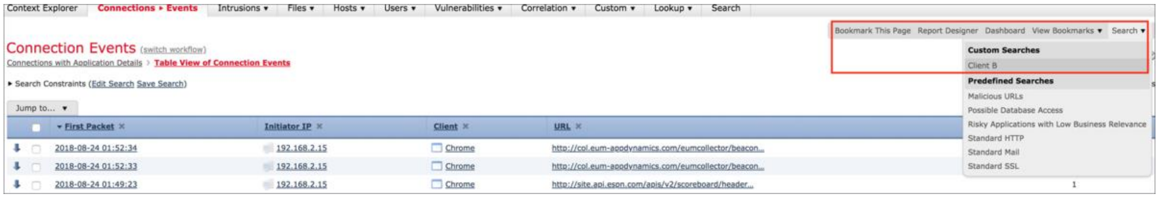




| | | |
|---|---|---|
| Initiator Bytes | | > 50 |
| Responder Bytes | | > 50 |
| Total Bytes | | > 50 |
| **Networking** | | |
| Initiator IP* | 192.168.2.15 | 192.168.1.0/24, !192.168.1. |
| Responder IP* | | 92.168.1. |
| Original Client IP* | | 92.168.1. |
| Initiator / Responder IP | | 92.168.1. |
| Initiator / Original Client IP | | 92.168.1. |
| Initiator / Responder / Original Client IP | | 92.168.1. |

Name: ClientB

**Step 4** - Select the custom search saved in the previous step and edit the columns as per step 1. Then click **Bookmark This Page**. The saved search can be later viewed by clicking on the **View Bookmarks Page**.



Connection Events (switch workflow)

Connections with Application Details › Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

| First Packet | Initiator IP | Client | URL |
|---|---|---|---|
| 2018-08-24 01:52:34 | 192.168.2.15 | Chrome | http://col.eum-appdynamics.com/eumcollector/beacon... |
| 2018-08-24 01:52:33 | 192.168.2.15 | Chrome | http://col.eum-appdynamics.com/eumcollector/beacon... |
| 2018-08-24 01:49:23 | 192.168.2.15 | Chrome | http://site.api.espn.com/apis/v2/scoreboard/header... |

**Note:** You will have to edit the time window after you select any saved search or bookmarks.

## Conclusion

In conclusion, why do we think it is important to integrate WSA with the Cisco IDS appliance?

Here is a list of the benefits:

- WSA will act as a single point of decryption for HTTPS traffic without requiring an external SSL decryption appliance.
- It allows you to use custom views and searches to monitor the desired traffic and associated threats.
- Cisco IDS helps refine policy applications with the option of creating rules that can match a number of conditions such as networks, VLAN IDs, application filters, ports, and more.
- It helps analyze network vulnerabilities at a deeper level to identify needed security policies.
- Integration with IDS provides a flexible reporting system that allows you to quickly and easily generate multisection reports with the event views or dashboards that appear on your FMC. You can also design your own custom reports from scratch and generate reports in various flows and formats.

It makes it easier to troubleshoot granular issues with the availability of a wide range of connection events such as Security Sockets Layer flow error, Quality of Service(QOS) polices, port information, and more.

## Next steps

For more detailed information on Cisco WSA, visit https://www.cisco.com/go/wsa.

For more about Cisco NGIPS, visit https://www.cisco.com/c/en/us/td/docs/security/firepower/60/quick_start/ngips_virtual/NGIPSv-quick/setup-ngipsv.html#62776.

For more about Cisco FMC, visit https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/introduction_to_the_cisco_firepower_system.html.

A Cisco sales representative, channel partner, or systems engineer can help you evaluate how Cisco web security will work for you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C07-741280-00 09/18