



# Cisco Secure Web (WSA) Product Update

Thomas Jankowsky  
Technical Solutions Architect  
March, 2021



  
**SEVT Program**  
Knowledge is power

# WSA - License Model



**WSA Essentials**

- Web (URL) Filtering
- Web Reputation
- Application Visibility & Control




**WSA Advantage Bundle**


 WSA Essentials

**+**


 Sophos + Webroot




**WSA Premier**

 WSA Advantage

**+**

 AMP

**+**

 CTA

## A La Carte Options

AMP + CTA (Zero Day Threat)

Security Management Appliance  
(Centralized)

ThreatGrid (Sandboxing)

Advance Web Security Reporting  
(AWSR)

Sophos (Anti-Malware)

McAfee (Anti-Malware)

Webroot (Anti-Malware)

# WSA Priorities



## Simple and Flexible

- Enhance User Interface Flows to enable ease of use
- Provide seamless user experience



## Web Standards and Performance

- Support latest web standards



## Integrations

- Integration with other security products to offer overall security architecture
- Ease of deployment



## Virtual Strategy

- Enable usage in public, private data centers
- Provide customers with choice of VM's



## Threat Focus

- Provide excellent web security
- Continuous improvements in HTTP/HTTPS security

Provide Top-of-the-line defense for threats on the Internet for our customers

# WSA Roadmap

■ = Shipping ■ = Commit ■ = Planning ■ = Roadmap

## Q1CY20 AsyncOS 12.0

- High Performance WSA
- TLS 1.3
- CTR Integration on WSA
- UX Refresh

## Q3CY20 AsyncOS 12.5

- High Performance Proxy – Phase 2
- Proxy IP Spoofing
- YouTube Categories Support for WSA Controls
- Customer Success Initiative
- System Health Dashboard - WSA
- REST API for WSA – Network Config

## Q2CY21 AsyncOS 14.0

- HTTP/2 Support
- Secure-X Integration
- System Health Dashboard for WSA-Phase 2
- System Health Dashboard – SMA
- REST API Support – Policies
- Support TLS 1.3 Phase 2- Session Resumption
- Header Rewrite
- Header Consumption

## Q4CY21 AsyncOS 14.5

- Umbrella Integration
- Remote Browser Isolation Solution
- WSAv Support on Azure
- Large Virtual Model
- Config REST APIs(continued)
- Config Converter tool
- CASI Integration

## Forward Looking...

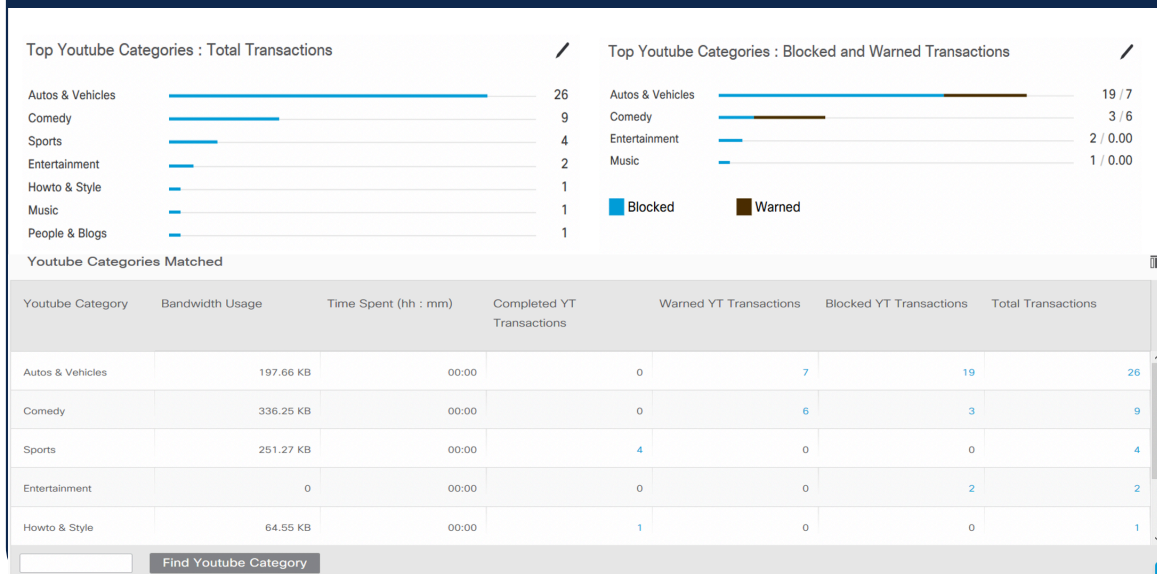
- Bluecoat Config Migrator
- AMP for FedRAMP
- Deeper Bandwidth Controls
- Simple and Scalable Policies
- Autoscaling for WSAv on Azure and AWS
- HTTP 3.0/QUIC Support

# YouTube Categories : How-To-Configure

## Step 1: Acceptable Usage Control

### Step 2: In Access Policies

### Step 3: Reporting



Enable YouTube Categorization



Enable HTTPS proxy for YouTube (if not enabled)



Define the Control for the YouTube Categories



New Reporting of YouTube Categories

Report

Positioning

Roadmap - 12.5

Field Concerns

Selling Aids

# Restful APIs Network Configuration – Phase 1



# Umbrella Integration

**WEB-UMB-SEC-SUB – ATO** is expected to be available soon for consumption

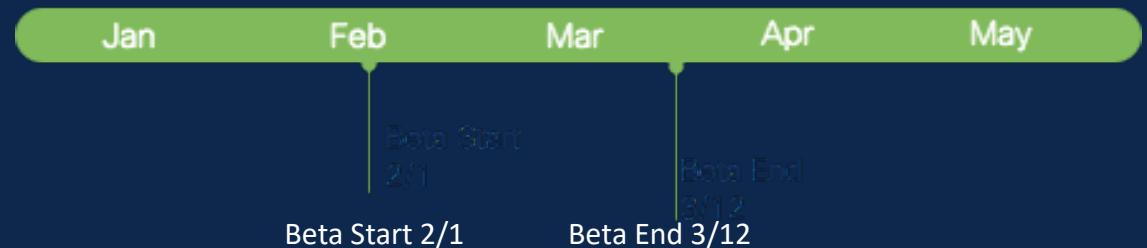
- Unified Licensing (Under work)
- Unified Identity (Roadmap)
- Unified Reporting & Policy (Roadmap)

# WSA 14.0 Beta comments

*“You did a smash up job bringing [HTTP 2.0], we have been waiting for this.”—*  
**Zones Inc**

*“WSA 14.0 is working fine so far in my production environment.” –* **Opus Group**

*“REST API is massively improved over previous versions.” –* **Zones Inc**







Header Modification



Header Consumption



HTTP 2.0

# 14.0 Highlights



SecureX Integration



System Health Dashboard  
in SMA/WSA



Rest API Support

What is common here?



# HTTP2.0

A critical value proposition in HTTP/2 vs HTTP1 - Low overhead in parsing data

What makes HTTP2 better?



HTTP/2 is used by 49.4% of all the websites!

# HTTP2

1

```
wsa010.cs1> http2

HTTP/2 protocol is currently Disabled

Choose the operation you want to perform:
- RESTRICT - Manage Domains from being proxified using HTTP/2 protocol
- ENABLE - Enable HTTP/2 protocol
- DISABLE - Disable HTTP/2 protocol
[]> enable

WARNING: HTTP/2 does not supports WTT, Persistent Cookie and Session Cookie currently.
Always disable WTT, Persistent Cookie and Session Cookie before enabling HTTP/2
Are you sure you want to Enable HTTP/2? [N]> YES

Enabling HTTP/2 protocol

HTTP/2 protocol is currently Enabled

Choose the operation you want to perform:
- RESTRICT - Manage Domains from being proxified using HTTP/2 protocol
- ENABLE - Enable HTTP/2 protocol
- DISABLE - Disable HTTP/2 protocol
[]>

wsa010.cs1> commit

Please enter some comments describing your changes:
[]> Enabling HTTP2

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Thu Nov 26 08:09:33 2020 GMT
wsa010.cs1> ^D
```

2

```
wsa010.cs1> http2

HTTP/2 protocol is currently Disabled

Choose the operation you want to perform:
- RESTRICT - Manage Domains from being proxified using HTTP/2 protocol
- ENABLE - Enable HTTP/2 protocol
- DISABLE - Disable HTTP/2 protocol
[]> RESTRICT

Manage domain entries:

Choose the operation you want to perform:
- DELETE - Delete entries
- FLUSH - Delete all entries
- ADD - Add new entries
- LIST - List entries
[]> ADD

Enter a valid and unique domain name[one per line]; an empty line to finish
[]> www.cnn.com

Enter a valid and unique domain name[one per line]; an empty line to finish
[]>

Manage domain entries:

Choose the operation you want to perform:
- DELETE - Delete entries
- FLUSH - Delete all entries
- ADD - Add new entries
- LIST - List entries
[]>
```

1. Enabling HTTP2
2. Restrict any faulty Domain for HTTP2 Processing

# WSA Header Rewrite

## Use Case:

“Administrator wants to authenticate users against the WSA (client-side proxy) and would like the WSA to forward the authentication headers to the upstream proxy, so it can help recognize the user by using the information in header and apply corresponding policies”

Authentication related headers to be passed to upstream

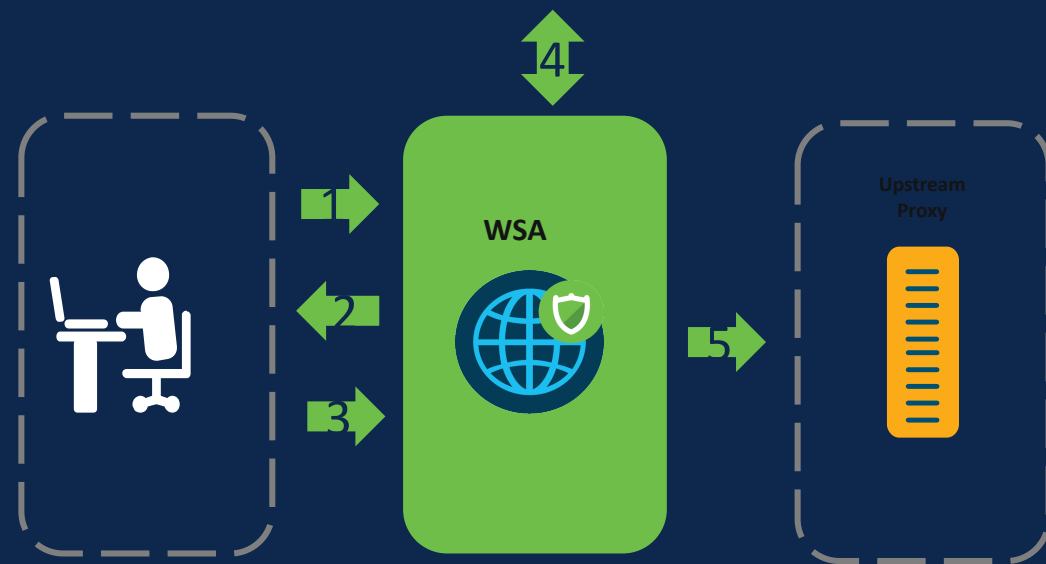
eg: X-authenticated-user , X-authenticated-groups

Tenant restriction with Microsoft Office 365

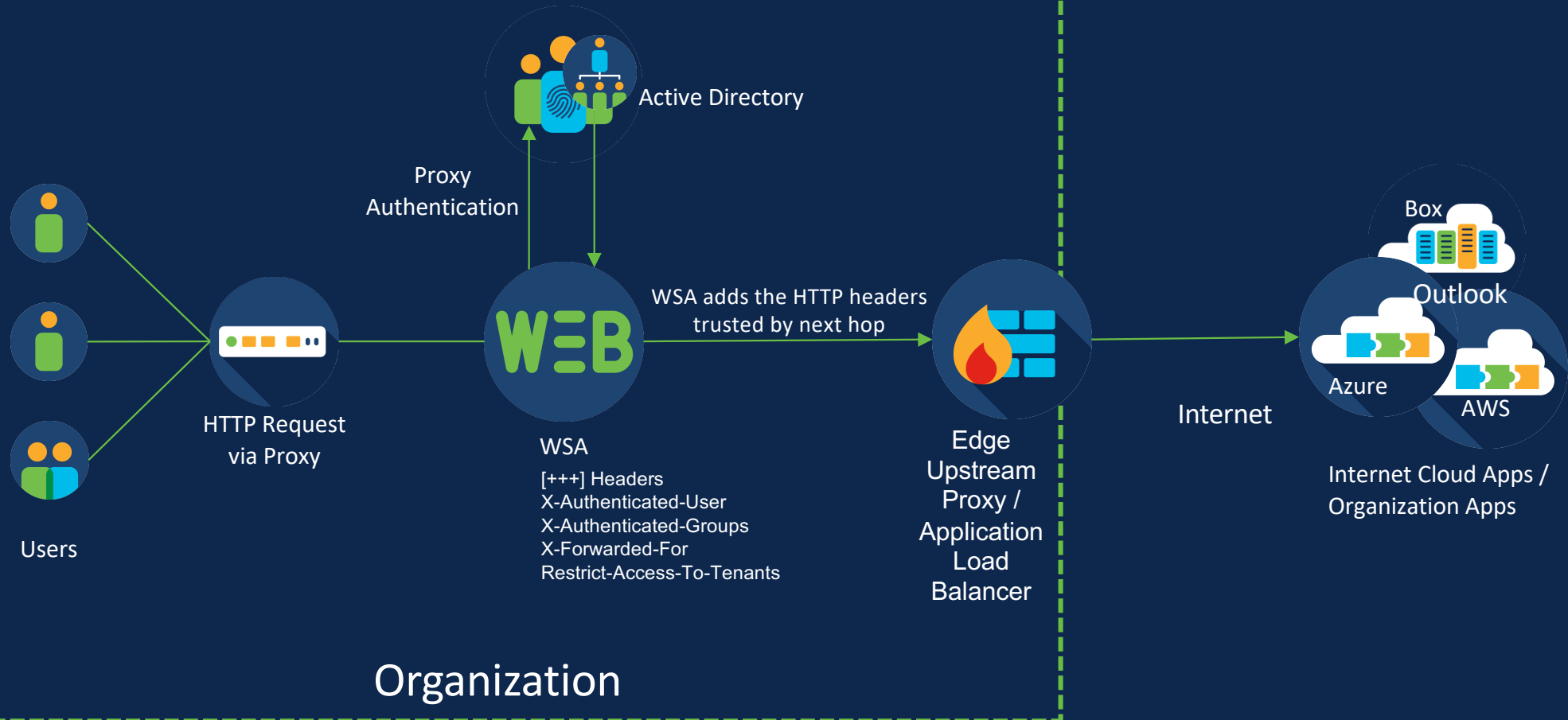
Tenant restriction solution needs capability to configure HTTP headers to have user list and Active Directory ID



- 1 Client issues an HTTP request
- 2 Collect user credentials
- 3 User submits the Directory username and password
- 4 Authentication performed by proxy
- 5 WSA inserts headers and sends it to upstream



# Header rewrite per policy



# WSA Header Rewrite

## Header ReWrite

- Request header feature enables WSA admin to configure request headers to be added, modified or deleted
- Header modification will be policy based such that finer control can be provided for adding or modifying headers
- Headers can be encoded as follows
  - Text encoding
    - UTF8
    - ASCII
  - Binary encoding
    - Base64
    - No encoding

# Header Rewrite: How-To-Configure

Reporting | Web Security Manager | Security Services | Network | System Administration

### Access Policies

Success — Settings have been saved.

**Policies**

[Add Policy...](#)

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Delete
1	<b>Client network 1 Access</b> Identification Profile: Client Network 1 6 groups (AD\W2016-02\Domain Admins...)	(global policy)	Block: 27 Warn: 24 Monitor: 34	(global policy)	(global policy)	(global policy)	my profile 1	
2	<b>Client network 2 Access</b> Identification Profile: Client Network 2 All identified users	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	(global policy)	
	<b>Global Policy</b> Identification Profile: All	No blocked items	Monitor: 85	Monitor: 356	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	<a href="#">delete_profile</a>	

[Edit Policy Order...](#)

Copyright © 2003-2020 Cisco Systems, Inc. All rights reserved. | Privacy Statement

- ✓ Create HTTP Header Profile
- ✓ Add HTTP Request Header
- ✓ Add Header Name, Value, formatting & encoding
- ✓ Add/Copy/Delete Row
- ✓ Request Header Profiles
- ✓ X-Auth Header Global Settings
- ✓ View allowed format for groups
- ✓ Associate Header ReWrite Profile to Access Policies.

**Note:** Null / empty header values are allowed. Such headers will be ignored and won't be added in the transactions.

**Ex:** Via and Proxy Connection in this case.



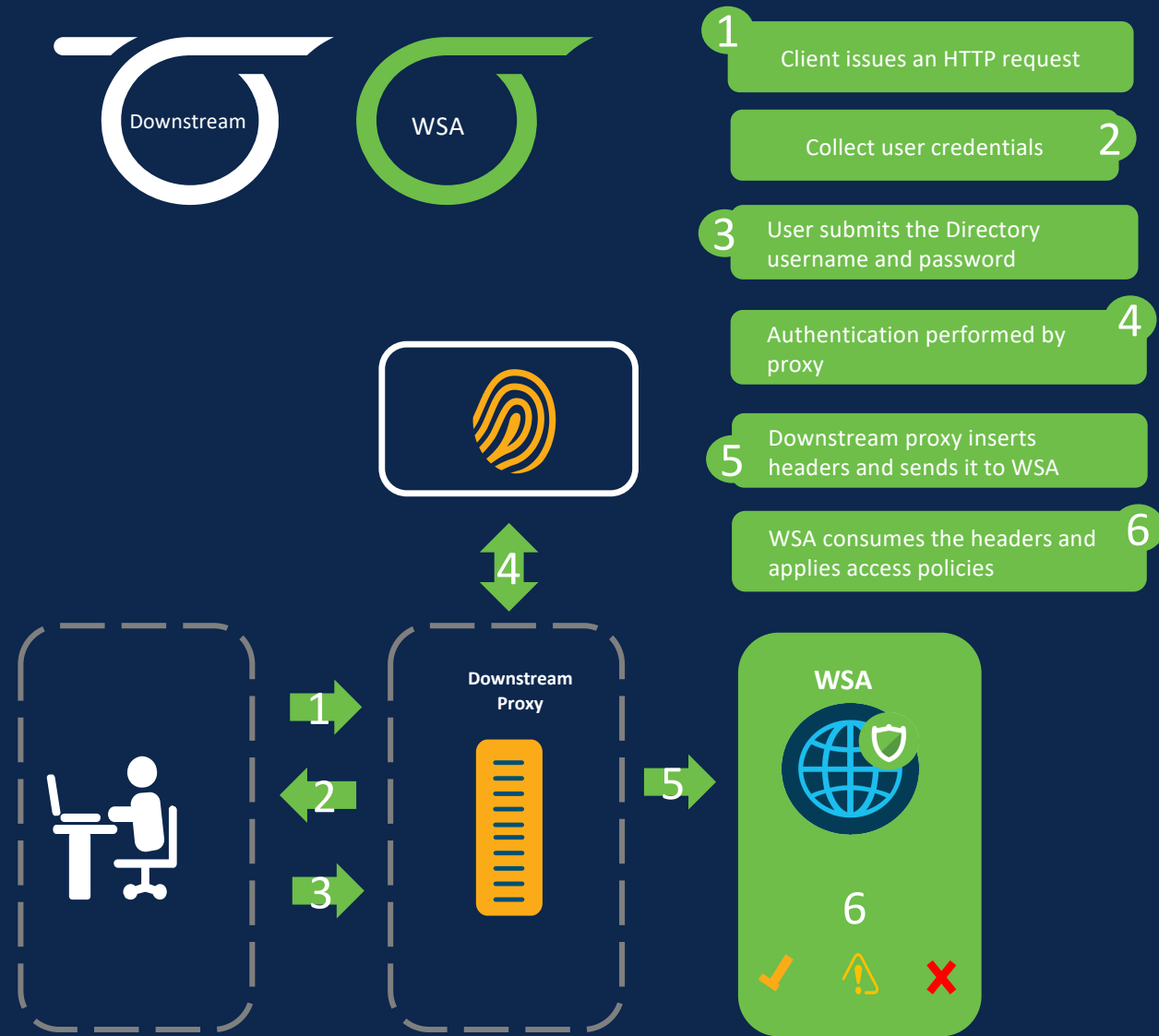
# WSA X-auth Header Consumption

## Use Case:

“Administrator wants to authenticate users against a downstream proxy and send user information to the WSA via authentication headers, so it can help WSA recognize the user by using the information in header with out requesting for authentication again and apply corresponding policies”

## Scenarios:

- A Load balancer, before sending the traffic to proxies, it authenticates the users and inserts the headers in http and sends it to the proxy
- A SSL Orchestrator performs authentication of users and sends the traffic in service chaining manner to multiple devices in the chain before sending the traffic out to internet.



# WSA X-auth Header Consumption: How-To-Configure

## Access Policy: AP1

Policy Settings	
<input checked="" type="checkbox"/> Enable Policy	
Policy Name: ?	AP1 <small>(e.g. my IT policy)</small>
Description:	
Insert Above Policy:	4 (Global Policy)
Policy Expires:	<input type="checkbox"/> Set Expiration for Policy On Date: <input type="text"/> MM/DD/YYYY At Time: <input type="text"/> : <input type="text"/>

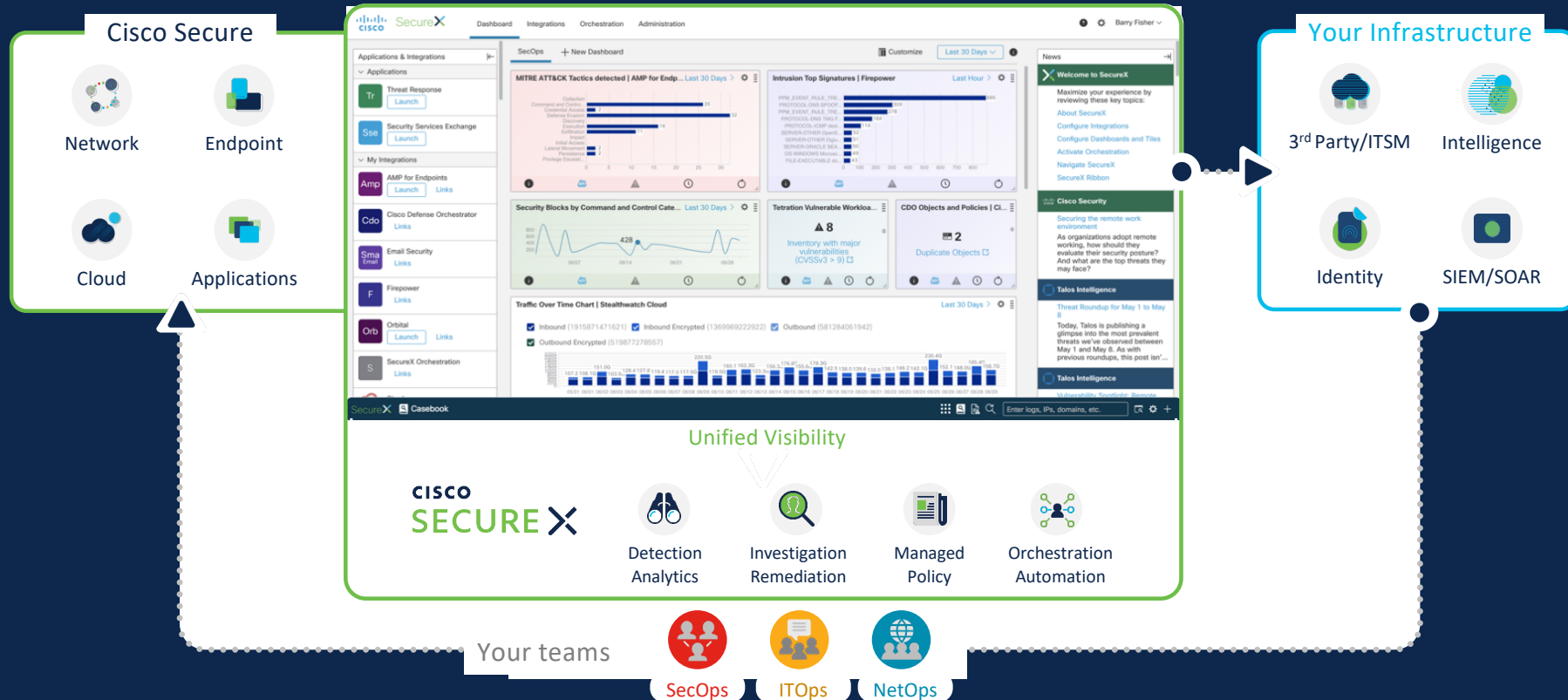
  

Policy Member Definition	
<small>Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.</small>	
Identification Profiles and Users:	Select One or More Identification Profiles
Identification Profile	Authorized Users and Groups
ID1	<input checked="" type="radio"/> All Authenticated Users <input type="radio"/> Selected Groups and Users ? Groups: No groups entered Users: No users entered
	<input type="button" value="Add Identification Profile"/>

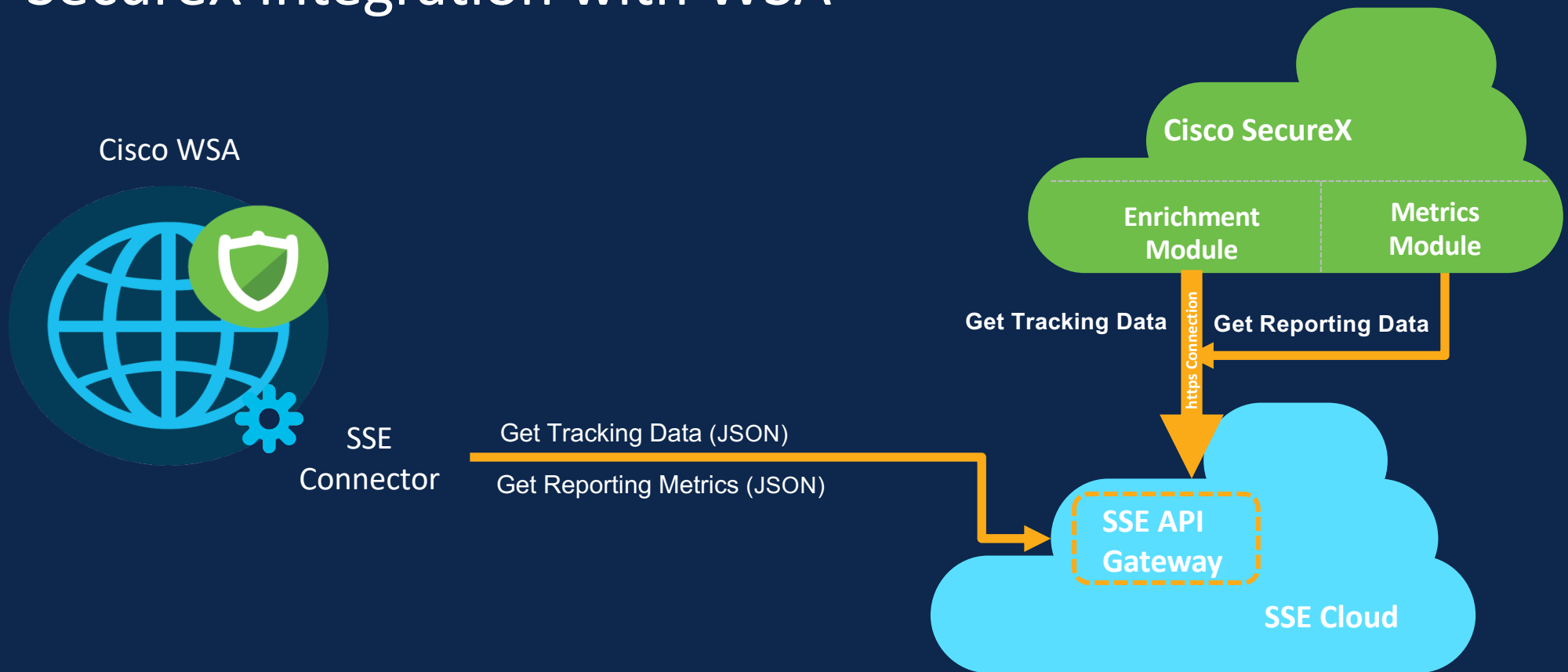
All the configurations could be done from GUI only, there are no new CLI commands added for this feature

# SecureX

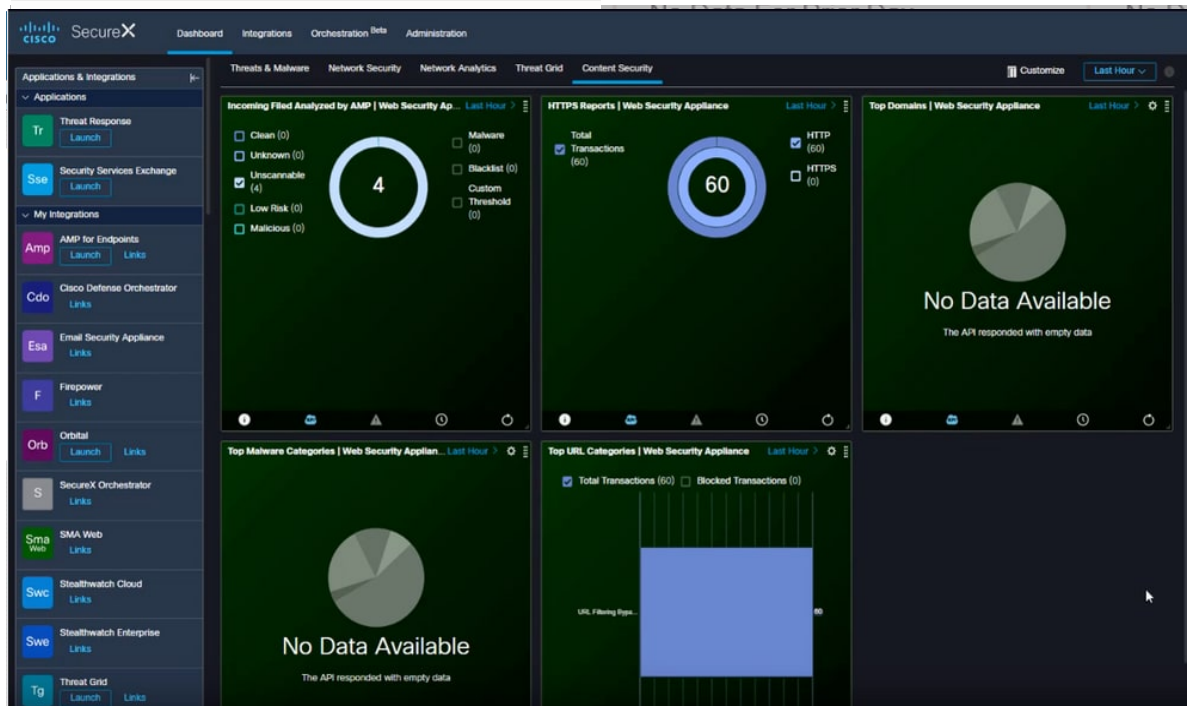
A cloud-native, built-in platform experience within our portfolio



# SecureX Integration with WSA



# SecureX Integration : How-To



- ✓ New SecureX ribbon
- ✓ SecureX WSA Tile
- ✓ Register WSA on SSE Portal
- ✓ Generate client ID and Client Secret.
- ✓ Copy client ID and Password
- ✓ Enter details back on WSA
- ✓ SecureX Pivot menus
- ✓ Reports on SecureX Portal

# Rest APIs supported in 12.5

## Rest API support for configuration

“Automate WSA configuration through scripts and integrate with third party solutions”



## 64 APIs available for configuration

- System Time
- Certificate Management
- Routes
- SMTP
- Feature Keys
- Custom and external URL Category
- Appliance Certificate
- DNS
- Proxy Bypass
- Interface

Helpful for automation of WSA configurations

Easy integration with 3<sup>rd</sup> party solutions

# Rest APIs supported in 14.0

## Rest API support for configuration

“Automate WSA configuration through scripts and integrate with third party solutions”



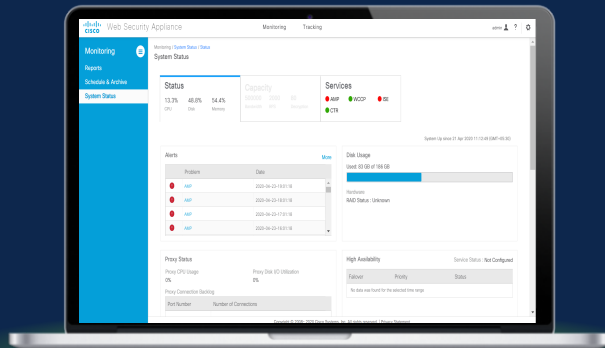
## New APIs available for configuration

- Access policies
- Identification profile
- PAC file hosting
- Domain Map
- HTTPS Proxy
- Alerts
- Upstream proxy
- Overall bandwidth limitation

# Why SHD? Visibility to System Health of WSA in a single pane of glass



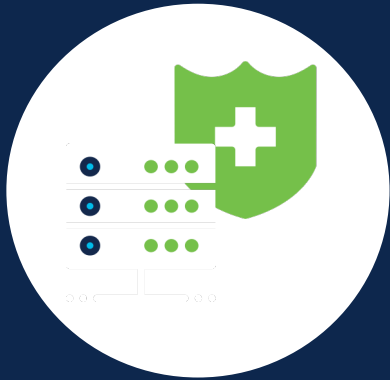
System Health Dashboard



“Admin is logged in to WSA. He goes for coffee and come back to see if anything is wrong with any of his WSA or he is occupied with some other work and wants to check if the health of his WSA device looks good”

“Admin gets a complaint saying there are some issues with his WSA in his network. He can drill down deeper in to the issues using SHD”





# System Health Dashboard

What is available in 14.0?

## 14.0 (New)

### Capacity Tab

- System CPU Usage
- System Memory Usage
- Bandwidth
- RPS
- CPU usage by Fn
- Client Connections
- Server Connections



### Services

- AMP
- WCCP
- CTR
- Service Response Time

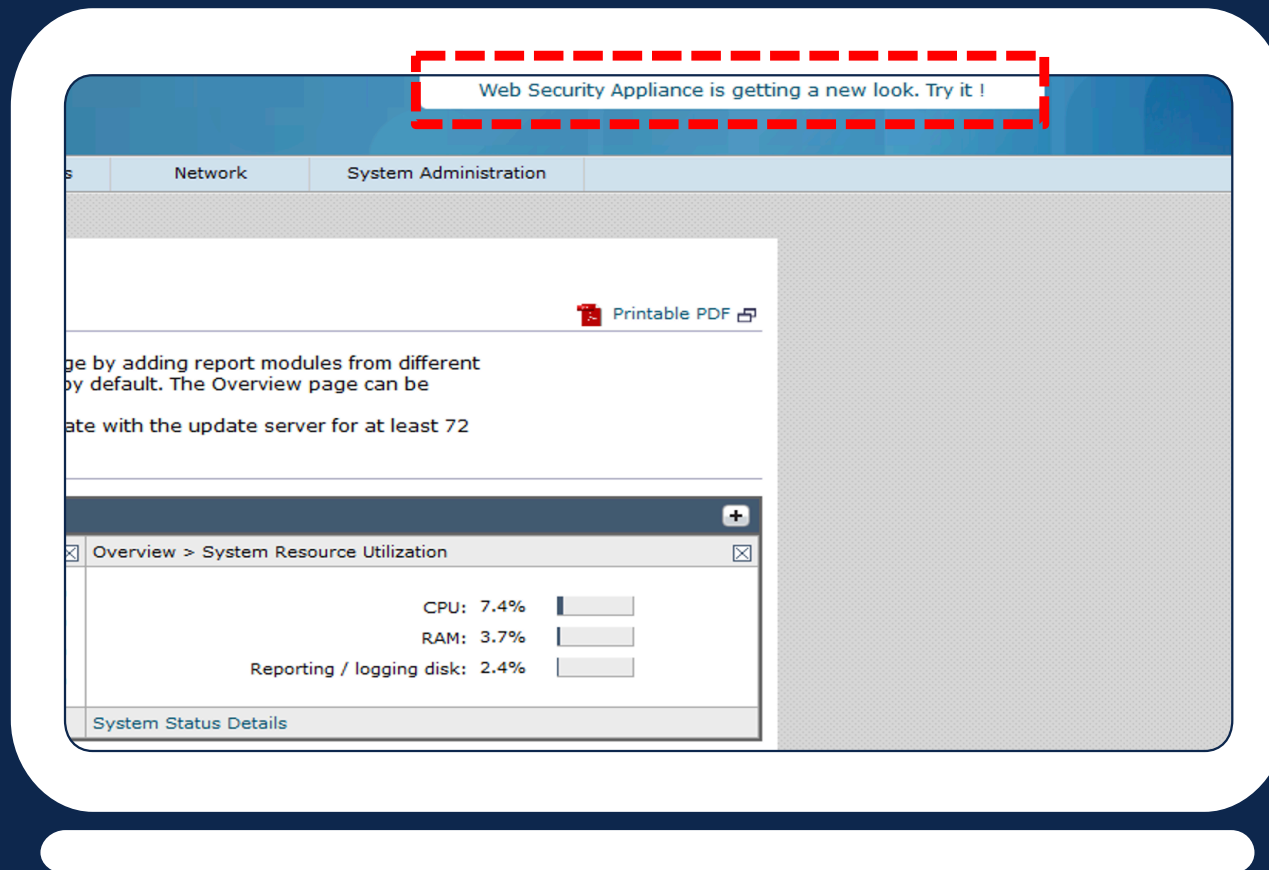
## 12.5



### Status

- Alerts
- CPU, Disk Usage
- Proxy Stats
- High Availability
- Proxy Traffic Characteristics

# System Health Dashboard - What New Added?



# System Health - Capacity Tab (Phase 2)

14.0

## Capacity

CPU Usage

Memory Usage

Disk

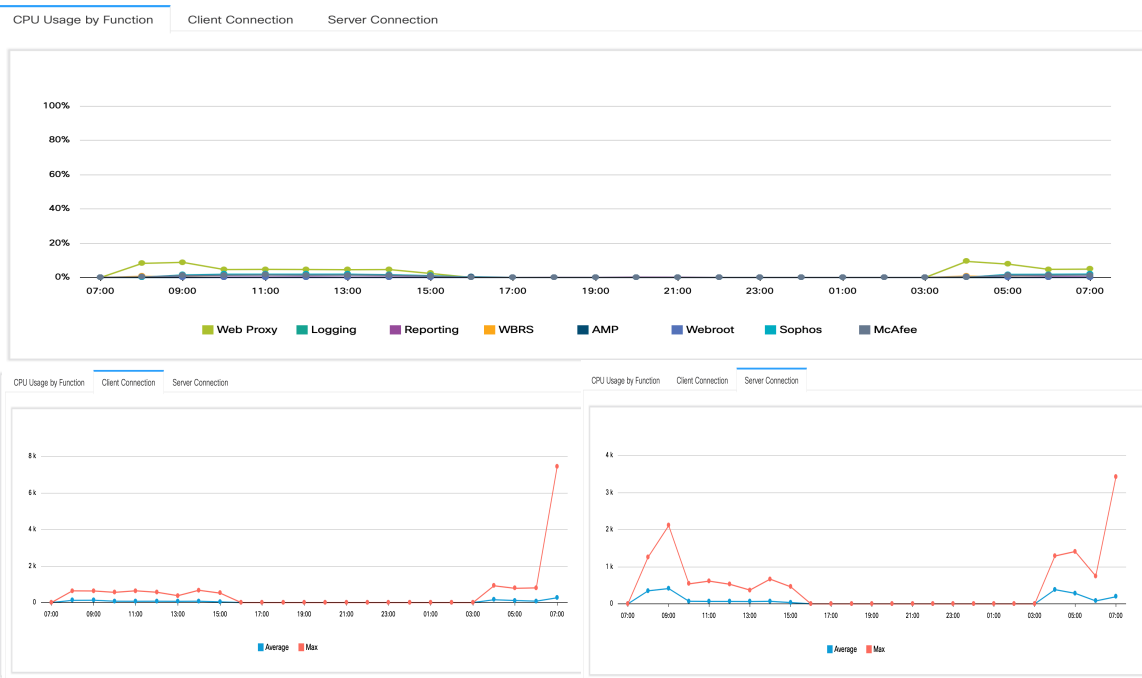
RPS

Bandwidth

CPU Usage

Client Connections

Server Connections



# System Health– in SMA

The screenshot shows the Cisco Security Management Appliance (SMA) interface. The main page is titled 'System Health' and displays a table of proxy servers. A modal window titled '4 Warning Alerts' is open, showing a warning for 'wsa119' related to vSphere HA failure. A red box highlights a 'Go To wsa119' link in the modal.

Proxy Name	Critical	Warning	Info	OK	Peak RPS	Peak Decrypted RPS	Peak Client Connections	Peak Server Connections
wsa117	0	0	0	0	-	-	-	-
dut122	0	0	0	0	-	-	-	-
wsa119	8	4	4	8	-	-	-	-
wsa114	0	0	0	0	-	-	-	-

# Advance Web Security Reporting (AWSR)



## Latest Release 7.5

- Splunk Engine update 7.3.3
- AD Group Details

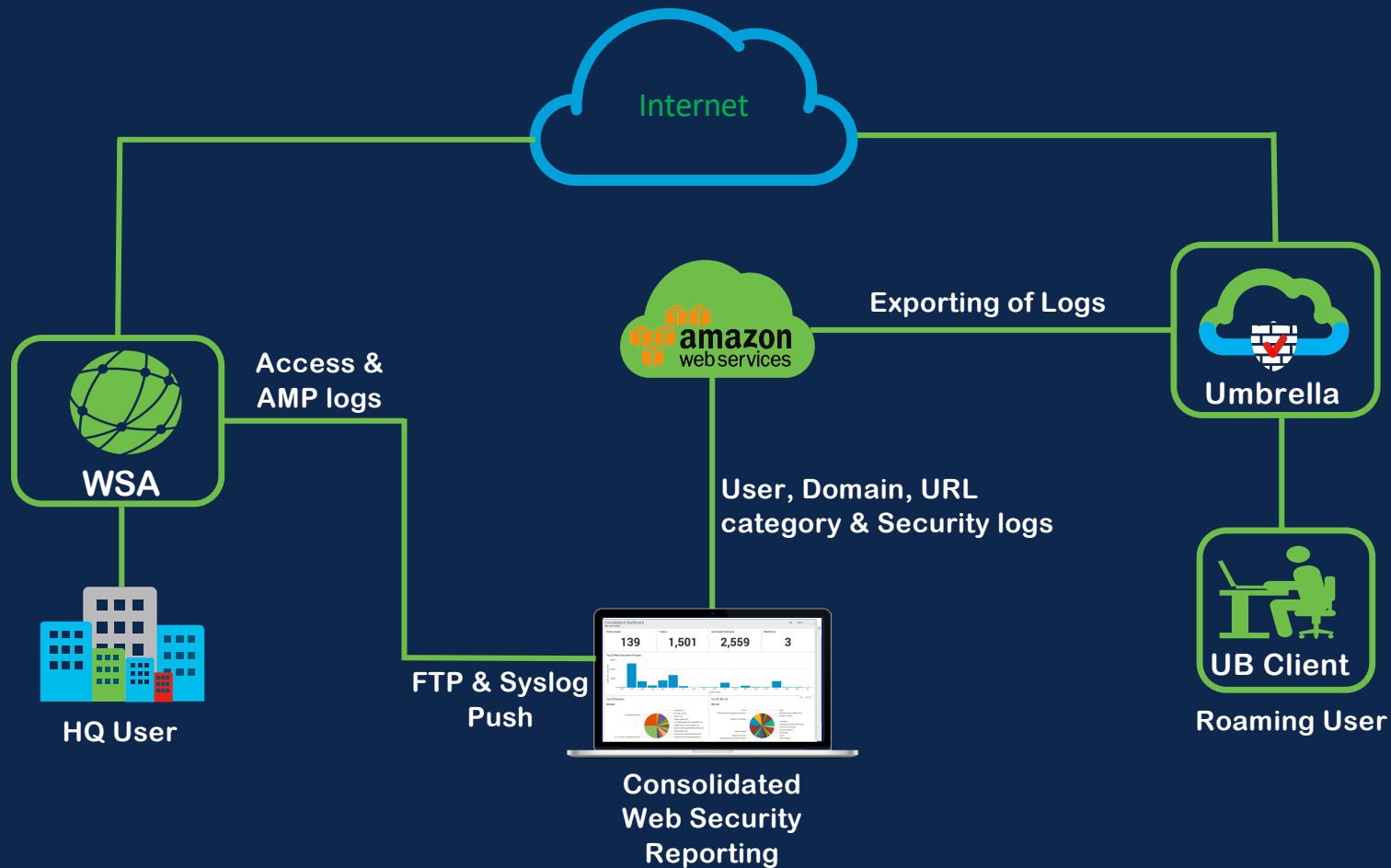


## Distributed Deployment

**Need Reporting for more users**

Link: [WSA Wiki](#)

# Advance Web Security Reporting v7.5 (WSA + Umbrella)





  
CISCO

SECURE