cisco

You make **possible**

cisco

Advanced WSA Deployment and Troubleshooting

with a side of Advanced Threat Technologies

Christian Clasen Technical Marketing Engineer
@xianclasen

BRKSEC-3771

cisco Live!
Barcelona | January 27-31, 2020

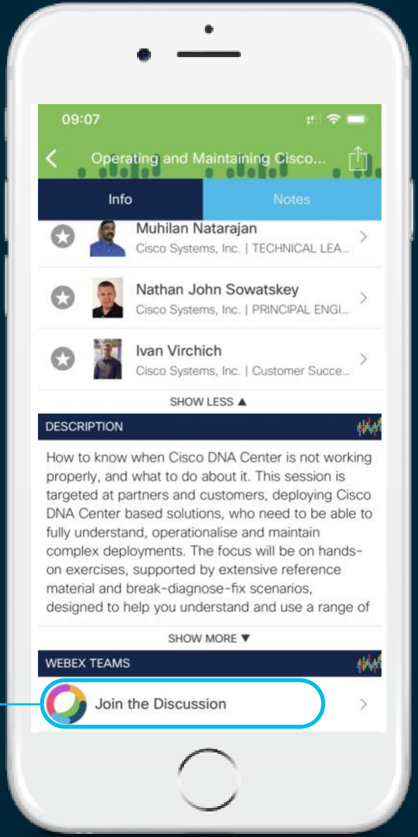
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



09:07

Operating and Maintaining Cisco...

Info | Notes

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

SHOW LESS ▲

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

SHOW MORE ▼

WEBEX TEAMS

Join the Discussion

This session is about Advanced Deployment & Configuration of the Web Security Appliance (WSA). Topics include web deployment topologies and best practices.

We will dive deep in performance troubleshooting and configurations around some of the WSA's leading Advanced Threat integrations. Advanced Malware Protection (AMP), Cognitive Threat Analytics and Threat Grid.

This Session is targeted at Security & Network Administrators that are deploying the WSA and are familiar with the basic installation of the WSA.

Abstract

About me

Literally who?

Professional

- Content Security TME
- Previously…
  - MSP Technical Lead
  - TAC engineer
  - Sysadmin / NetAdmin
- CCIE Security

Personal

- Father of three, husband of one
- Musician, fisherman, beer drinker
- Raleigh, NC USA

Agenda

- Introduction
- Network Topology and Configuration
- Services Configuration
- Policy Configuration
- Monitoring and Troubleshooting
- Q&A

Disclaimer

Best Practices are Guidelines *Not Laws*

Network Design and Configuration

Network environment and topology

ICMP

- WSA uses Path MTU Discovery
- Set MTU manually if needed with etherconfig

Firewall

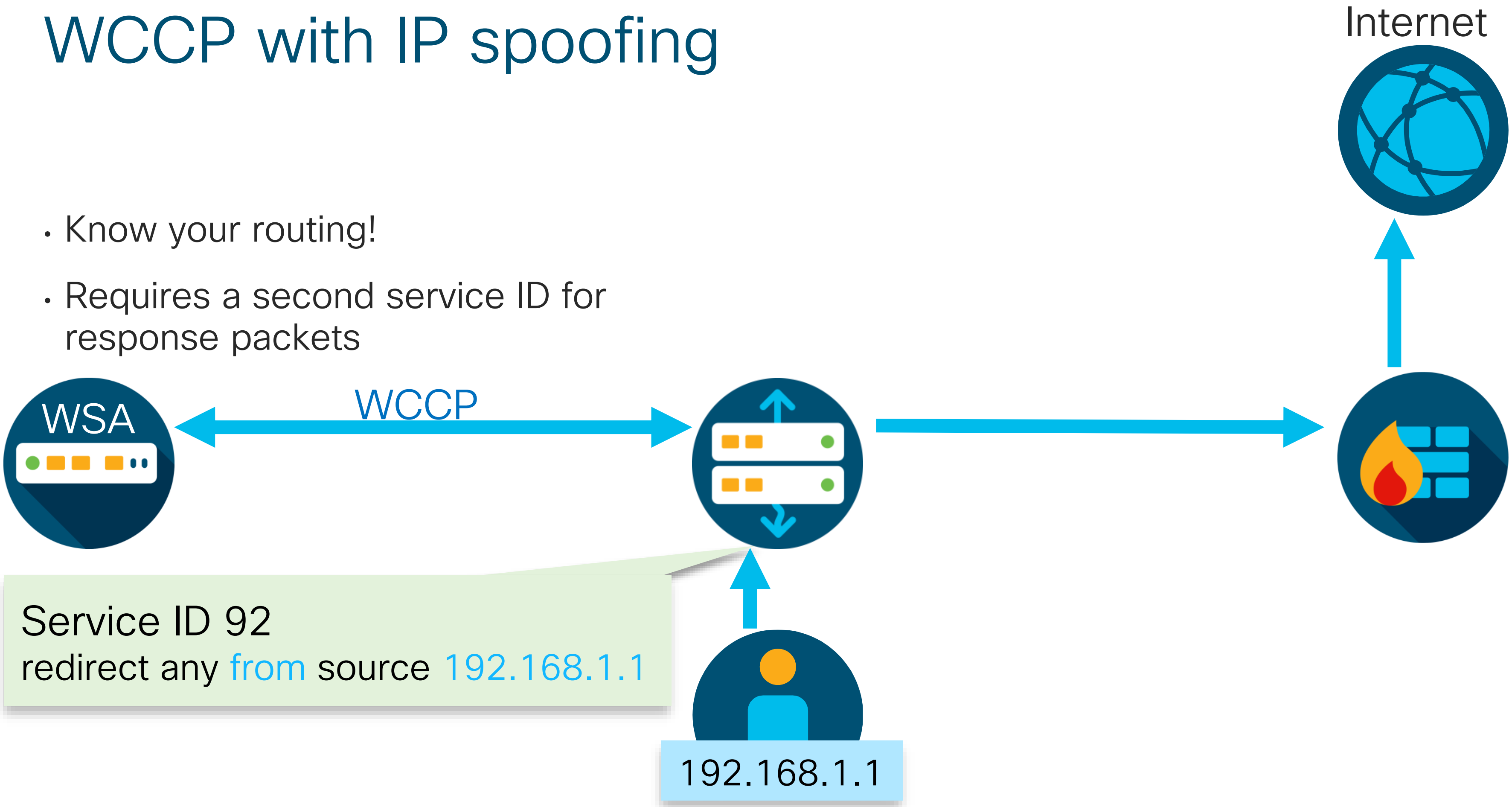
- Prevent NAT pool exhaustion
- Exempt from outbound DoS protections

Anti-Spoofing

- Beware of unicast reverse path forwarding and similar protections

WCCP with IP spoofing

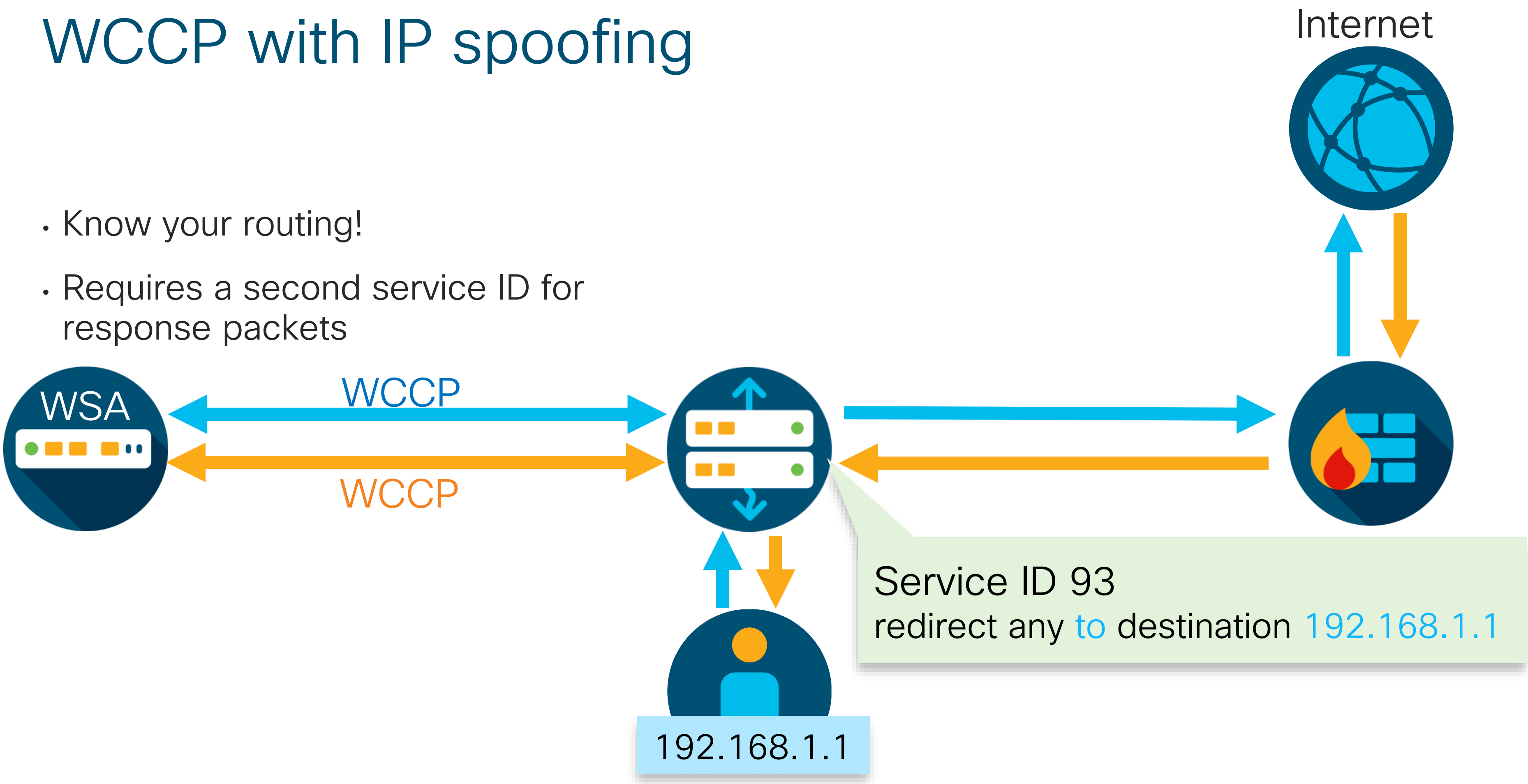
- Know your routing!
- Requires a second service ID for response packets



Service ID 92
redirect any from source 192.168.1.1

WCCP with IP spoofing

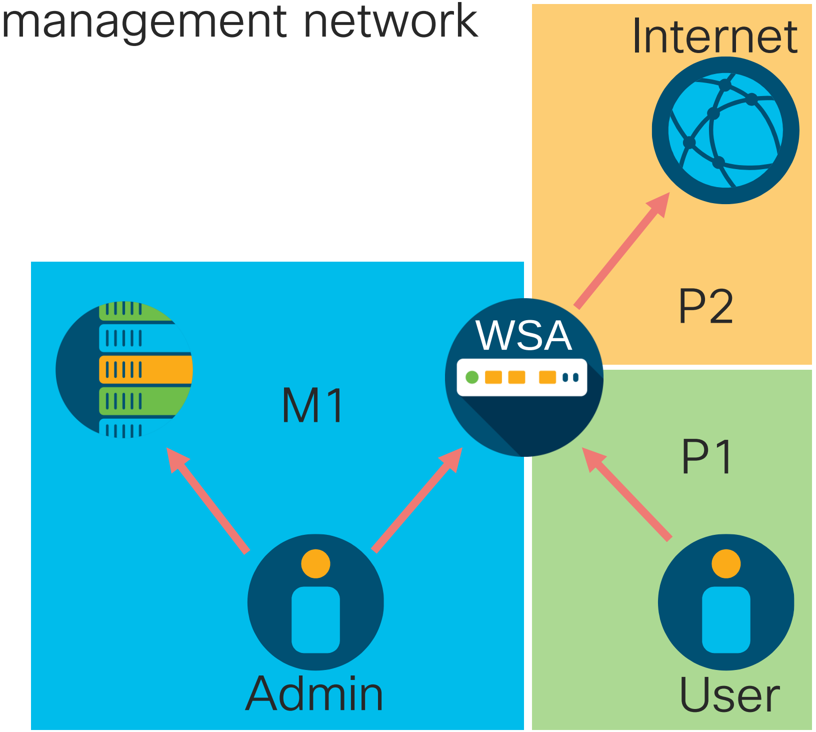
- Know your routing!
- Requires a second service ID for response packets



Service ID 93
redirect any to destination 192.168.1.1

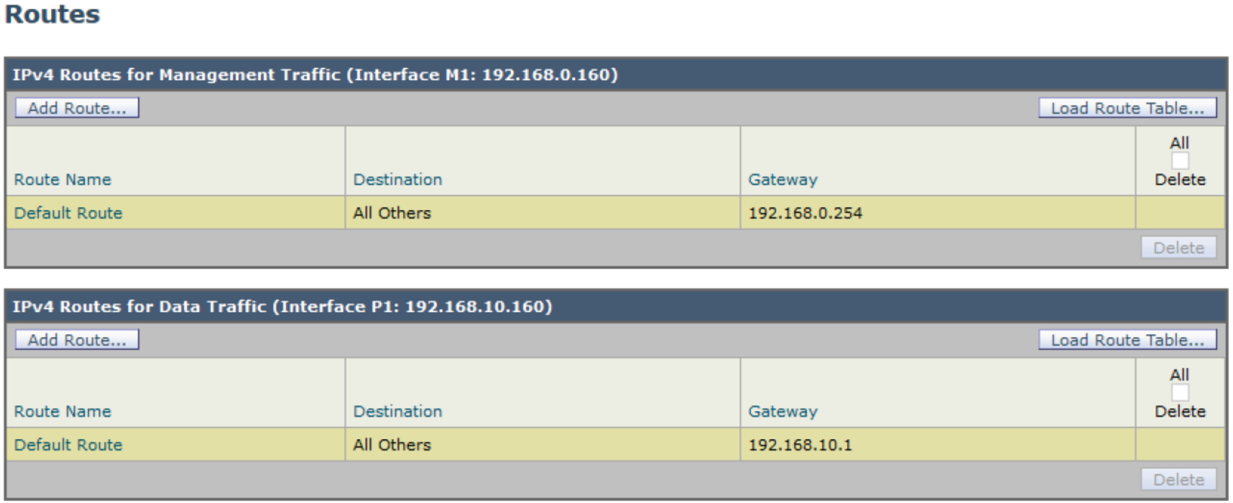
Management network

- M1 should be connected to a dedicated management network
  - Good network security hygiene
  - Reduces attack surface
  - Protects management availability
- Enable split-routing
  - Restricts management services to M1
  - Creates two routing tables



Routing by service

- Specify the routing table to use for the following services
  - External URL feeds
  - AMP services
  - Updates and upgrades
  - Authentication services
  - DNS



Routes

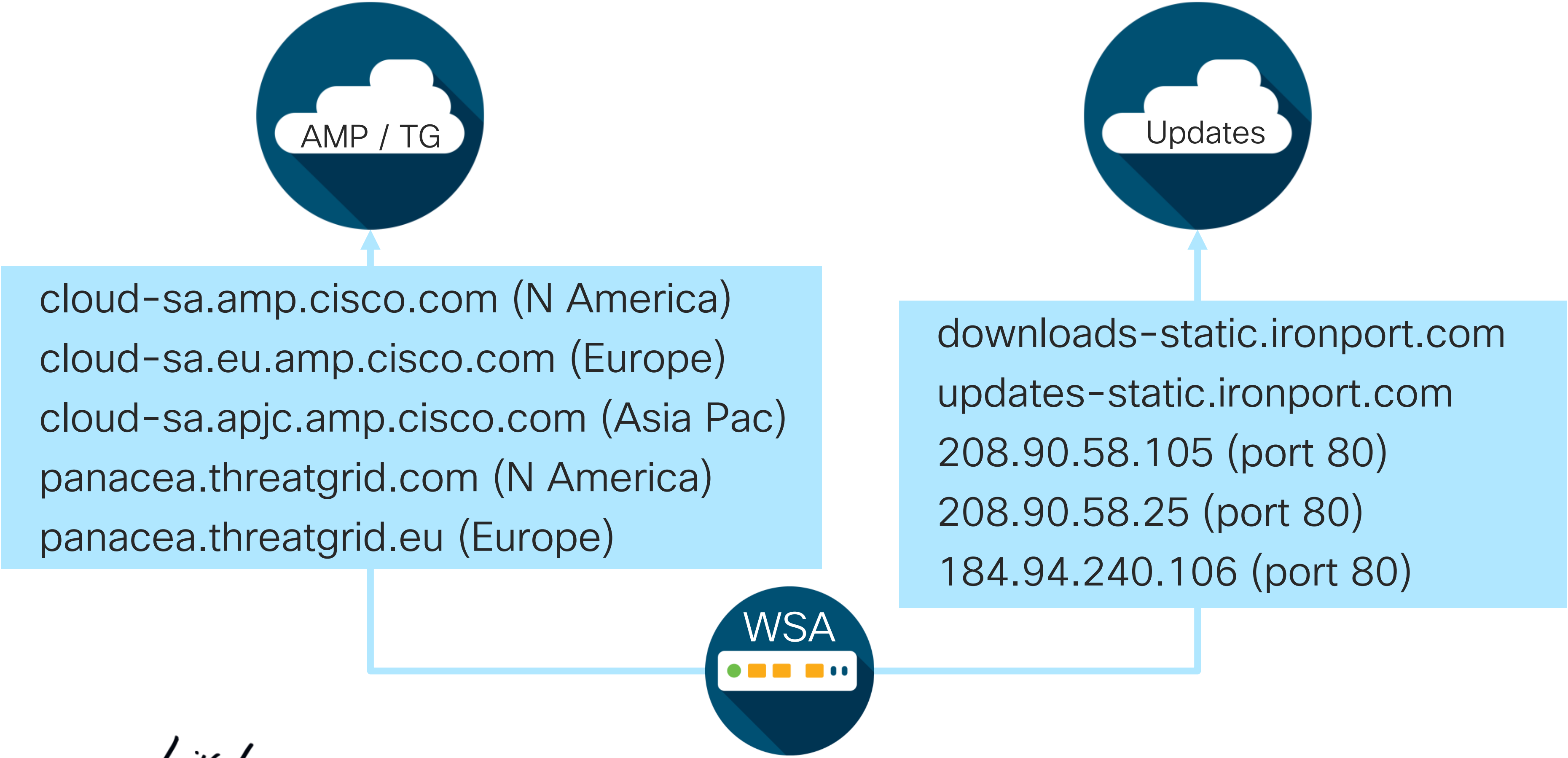
IPv4 Routes for Management Traffic (Interface M1: 192.168.0.160)

Route Name	Destination	Gateway	All □ Delete
Default Route	All Others	192.168.0.254	

IPv4 Routes for Data Traffic (Interface P1: 192.168.10.160)

Route Name	Destination	Gateway	All □ Delete
Default Route	All Others	192.168.10.1	

Whitelisting outbound services



AMP / TG

cloud-sa.amp.cisco.com (N America)
cloud-sa.eu.amp.cisco.com (Europe)
cloud-sa.apjc.amp.cisco.com (Asia Pac)
panacea.threatgrid.com (N America)
panacea.threatgrid.eu (Europe)

Updates

downloads-static.ironport.com
updates-static.ironport.com
208.90.58.105 (port 80)
208.90.58.25 (port 80)
184.94.240.106 (port 80)

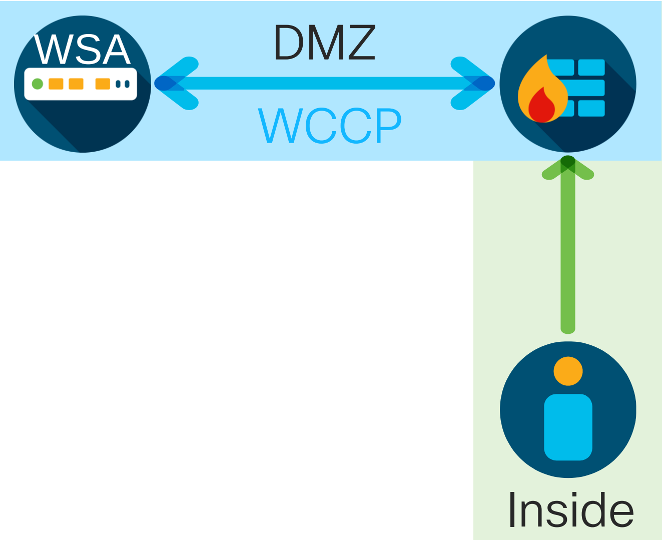
WSA

Transparent load balancing

- WCCP is the best method
  - Flexible bypass methods
  - Provides weighted load balancing
- Catalyst switches
  - Use ingress redirection
  - Use mask-based assignment
- ASA firewall
  - No IP spoofing
  - Client and WSA must be in the same zone

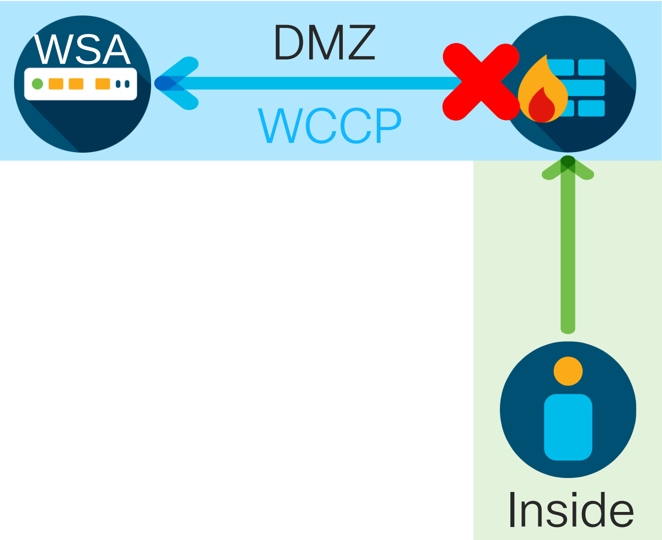
Transparent load balancing

- WCCP is the best method
  - Flexible bypass methods
  - Provides weighted load balancing
- Catalyst switches
  - Use ingress redirection
  - Use mask-based assignment
- ASA firewall
  - No IP spoofing
  - Client and WSA must be in the same zone



Transparent load balancing

- WCCP is the best method
  - Flexible bypass methods
  - Provides weighted load balancing
- Catalyst switches
  - Use ingress redirection
  - Use mask-based assignment
- ASA firewall
  - No IP spoofing
  - Client and WSA must be in the same zone



Explicit load balancing

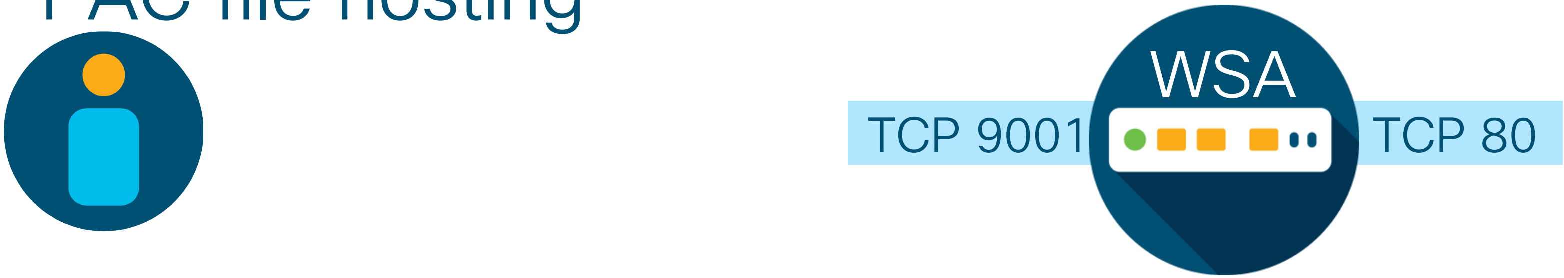
Load Balancer

- Most flexible method
- Can also work well in transparent deployments

PAC File

- Use GPO, not WPAD
- Host the file on a web server or the WSA

PAC file hosting

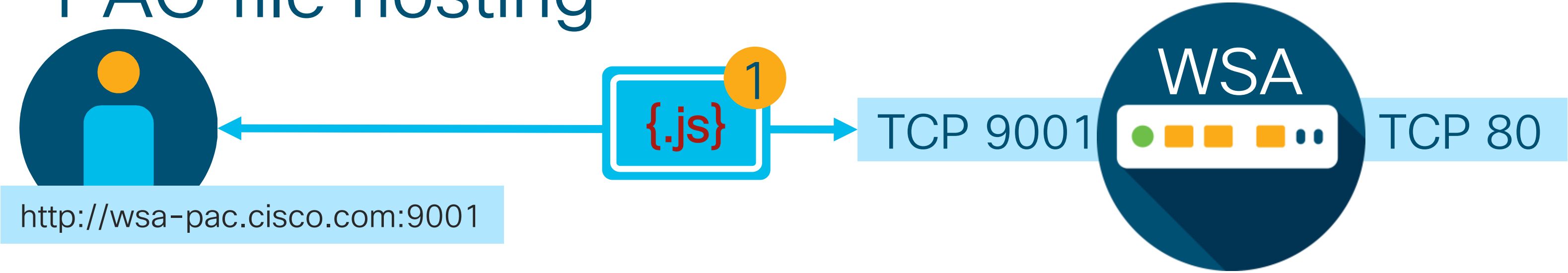


WSA

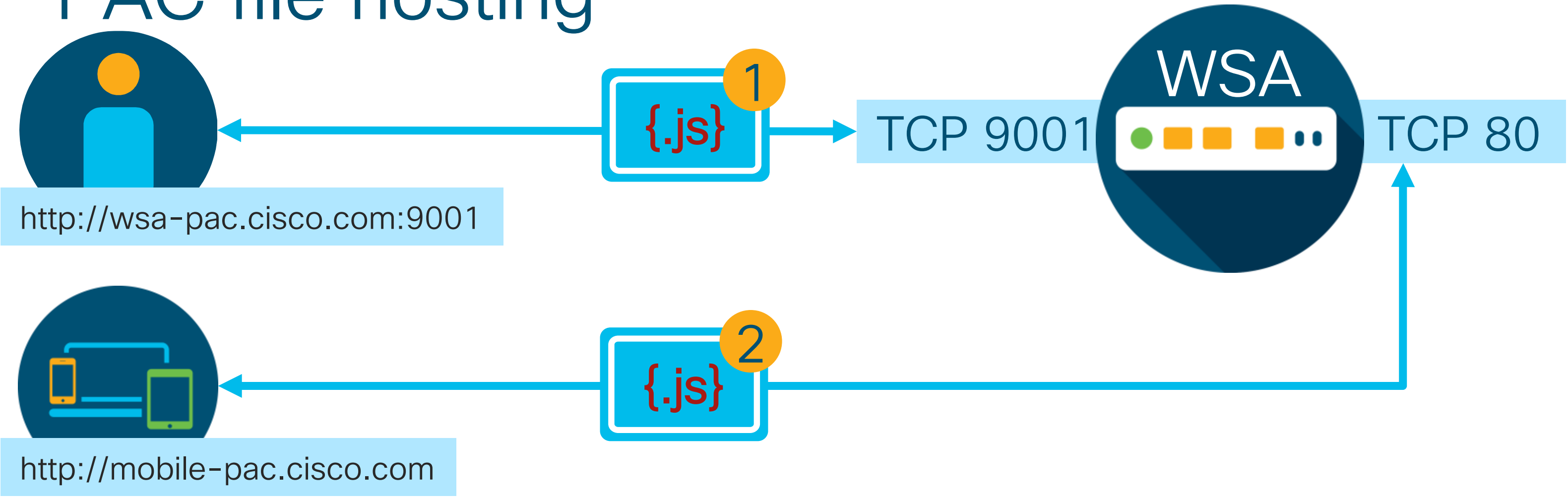
TCP 9001

TCP 80

PAC file hosting



PAC file hosting



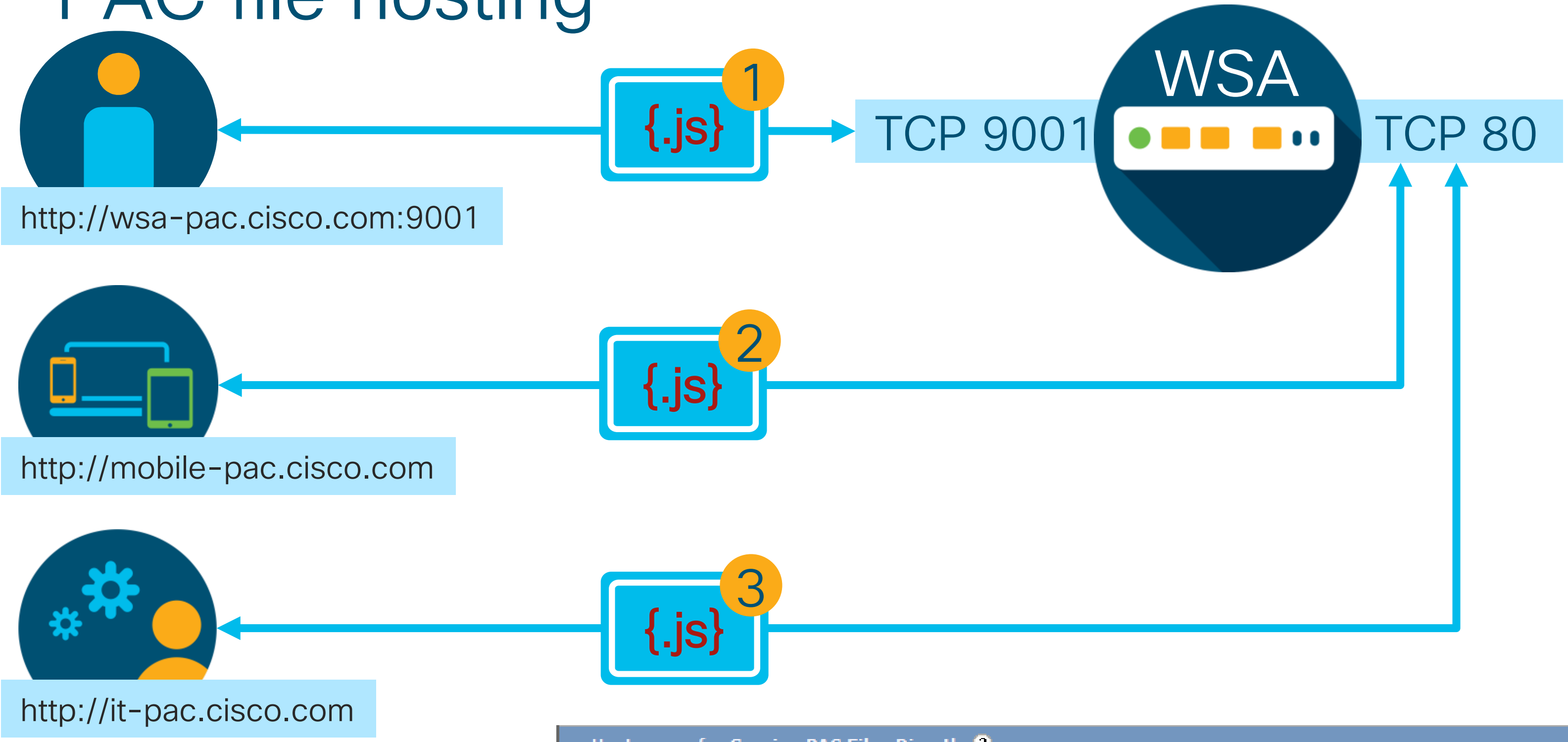
http://wsa-pac.cisco.com:9001

http://mobile-pac.cisco.com

TCP 9001

TCP 80

PAC file hosting



WSA

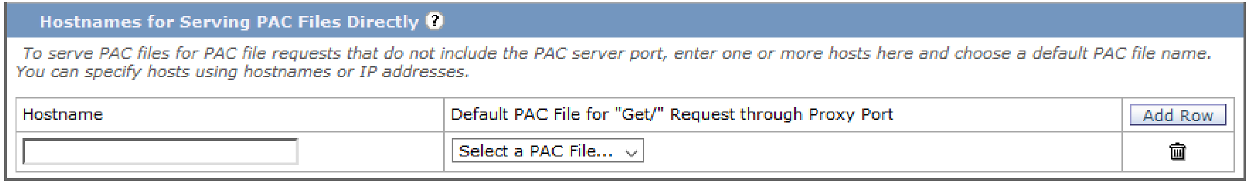
TCP 9001

TCP 80

http://wsa-pac.cisco.com:9001

http://mobile-pac.cisco.com

http://it-pac.cisco.com



Hostnames for Serving PAC Files Directly

To serve PAC files for PAC file requests that do not include the PAC server port, enter one or more hosts here and choose a default PAC file name. You can specify hosts using hostnames or IP addresses.

Hostname	Default PAC File for "Get/" Request through Proxy Port	Add Row
	Select a PAC File...	🗑

Services Configuration

DNS

Authoritative vs. Recursive

- Separate resolvers is recommended
- If only one, consider the query load
- WSA can use internet root servers for external domains only
- Individual domains can be assigned to different servers

Minimum TTL

- Default minimum TTL is 1800 seconds
- Suggested minimum is 300 seconds
- Reduces conflicts with client resolution for CDN records

Advanced DNS options

```
Select one of the following options:
0 = Always use DNS answers in order ← Default
1 = Use client-supplied address then DNS
2 = Limited DNS usage
3 = Very limited DNS usage
```

Advanced DNS options

```
Select one of the following options:
0 = Always use DNS answers in order  ← Default
1 = Use client-supplied address then DNS
2 = Limited DNS usage
3 = Very limited DNS usage
```

Advanced DNS options

```
Select one of the following options:
0 = Always use DNS answers in order ← Default
1 = Use client-supplied address then DNS
2 = Limited DNS usage
3 = Very limited DNS usage
```

Client

Dest: 30.1.1.1
Host: cisco.com

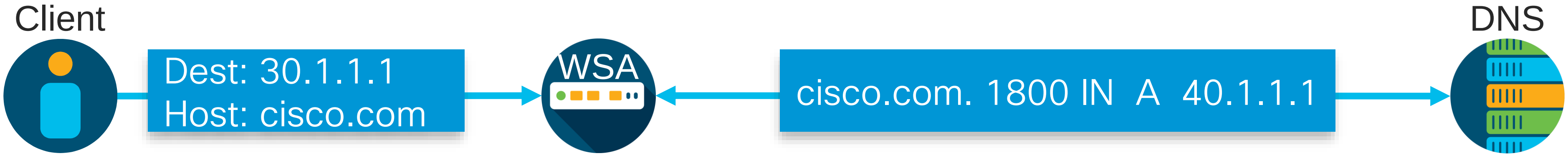
WSA

DNS

Advanced DNS options

```
Select one of the following options:
0 = Always use DNS answers in order
1 = Use client-supplied address then DNS
2 = Limited DNS usage
3 = Very limited DNS usage
```

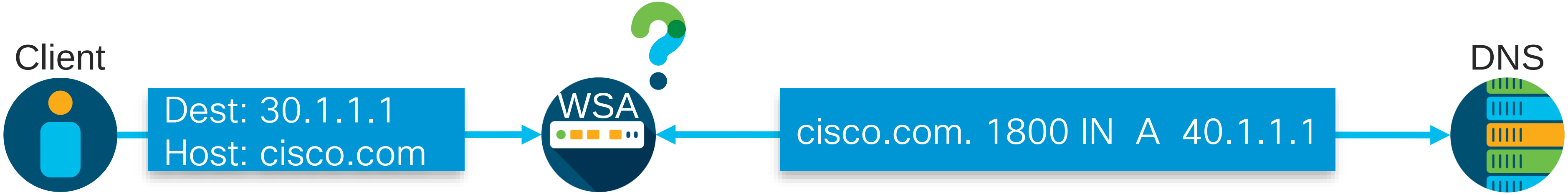
← Default



Advanced DNS options

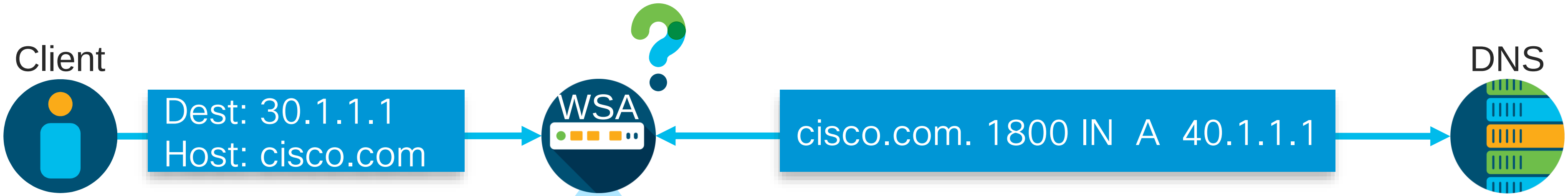
```
Select one of the following options:
0 = Always use DNS answers in order
1 = Use client-supplied address then DNS
2 = Limited DNS usage
3 = Very limited DNS usage
```

← Default



Advanced DNS options

```
Select one of the following options:
0 = Always use DNS answers in order ← Default
1 = Use client-supplied address then DNS
2 = Limited DNS usage
3 = Very limited DNS usage
```



Client

Dest: 30.1.1.1
Host: cisco.com

WSA

cisco.com. 1800 IN A 40.1.1.1

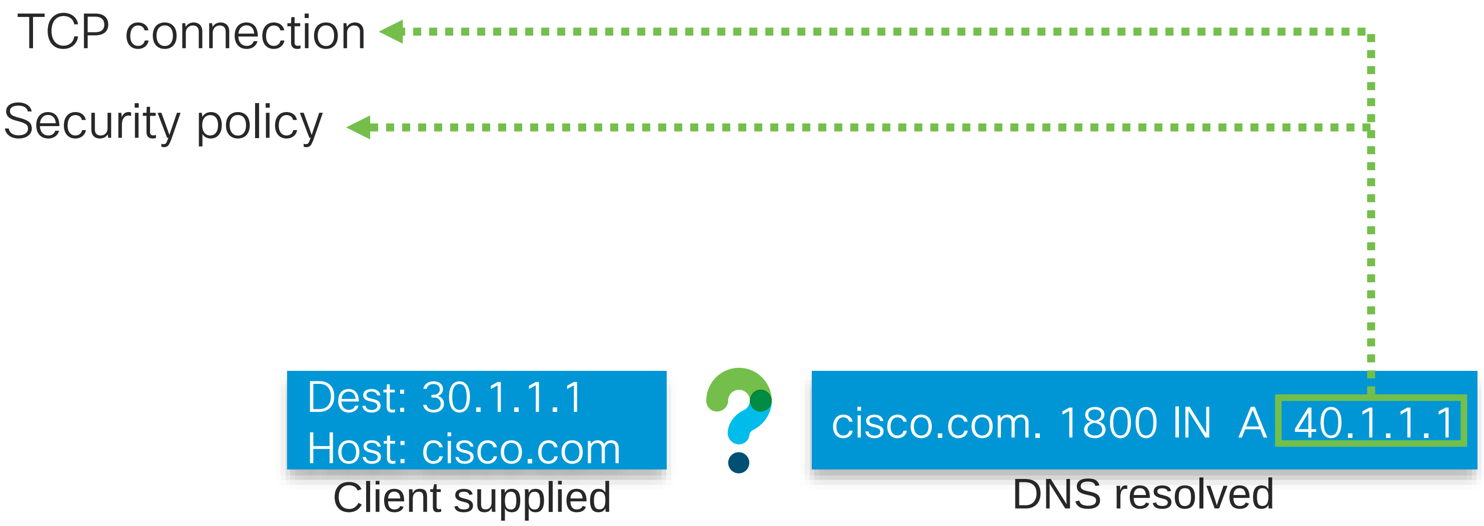
DNS

How much do you trust your client?

Advanced DNS options

```
Select one of the following options:
0 = Always use DNS answers in order
```

← Default



TCP connection

Security policy

Dest: 30.1.1.1
Host: cisco.com

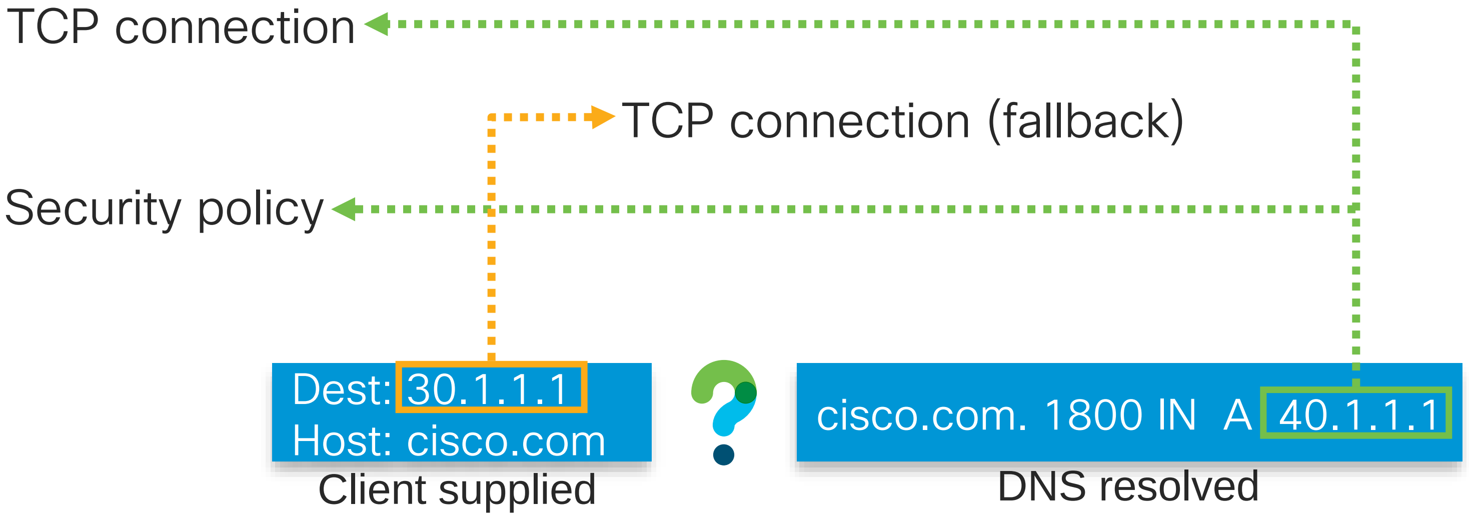
Client supplied

cisco.com. 1800 IN A 40.1.1.1

DNS resolved

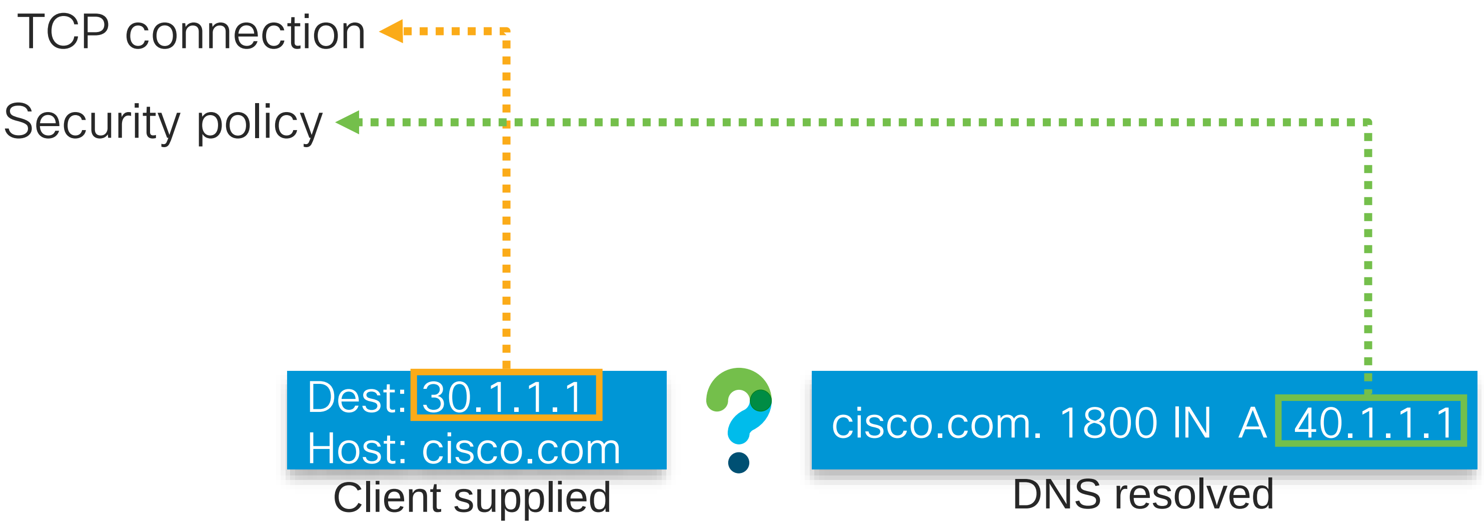
Advanced DNS options

```
Select one of the following options:
1 = Use client-supplied address then DNS
```



Advanced DNS options

```
Select one of the following options:
2 = Limited DNS usage
```



TCP connection

Security policy

Dest: 30.1.1.1
Host: cisco.com

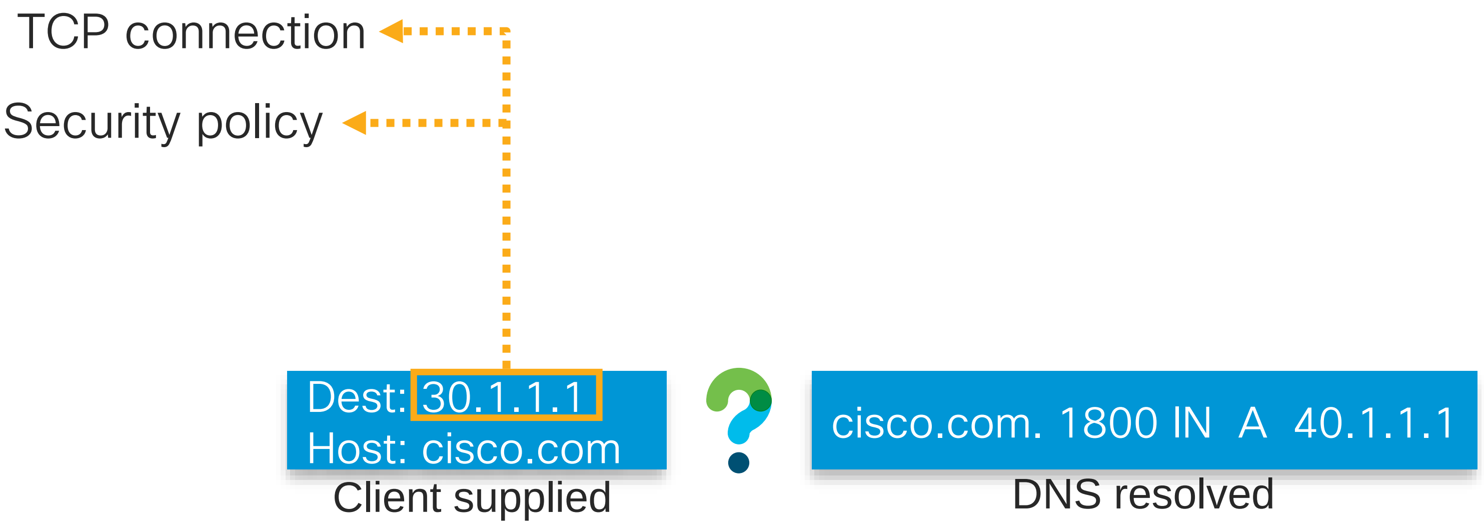
Client supplied

cisco.com. 1800 IN A 40.1.1.1

DNS resolved

Advanced DNS options

```
Select one of the following options:
3 = Very limited DNS usage
```



TCP connection

Security policy

Dest: 30.1.1.1
Host: cisco.com

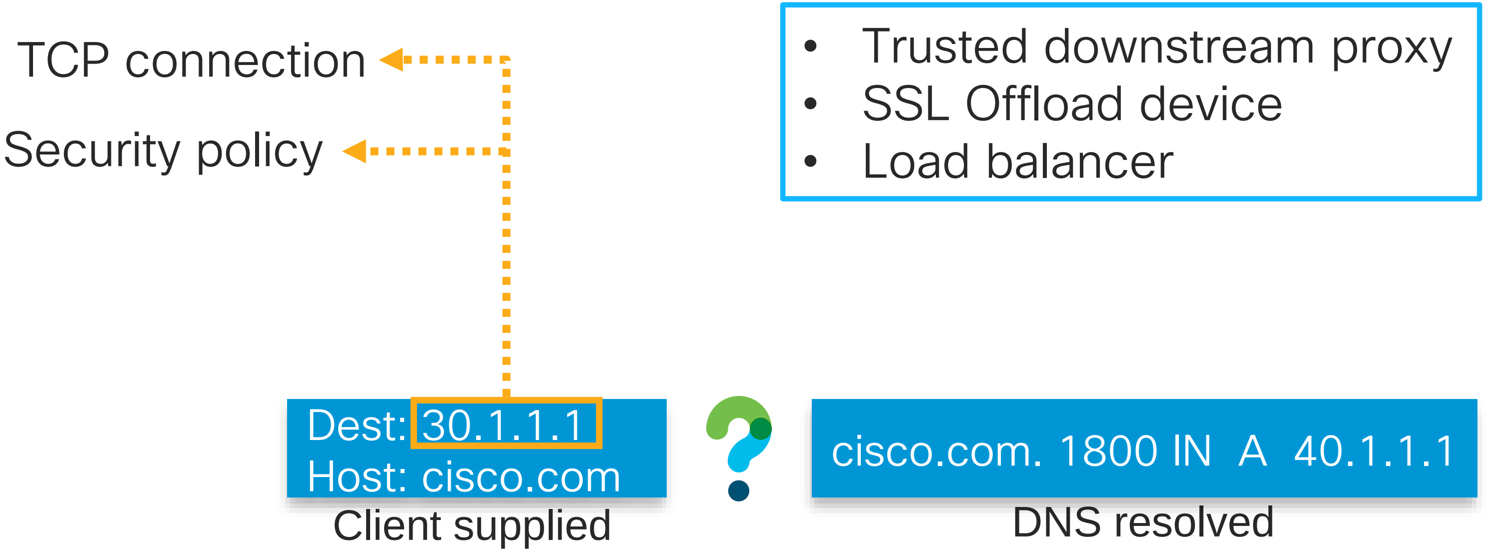
Client supplied

cisco.com. 1800 IN A 40.1.1.1

DNS resolved

Advanced DNS options

```
Select one of the following options:
3 = Very limited DNS usage
```



- Trusted downstream proxy
- SSL Offload device
- Load balancer

TCP connection

Security policy

Dest: 30.1.1.1
Host: cisco.com

Client supplied

?

cisco.com. 1800 IN A 40.1.1.1

DNS resolved

Authentication

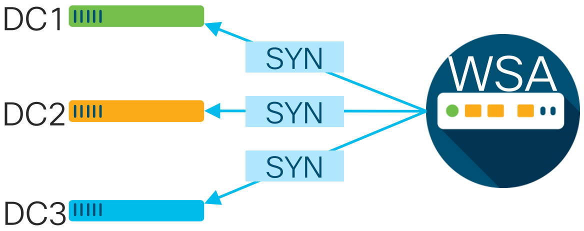
- WSA supports Kerberos, NTLM, Basic, SSO_TUI
- Always use a surrogate (IP address if possible)
- Surrogate timeout should be no lower than 15 minutes

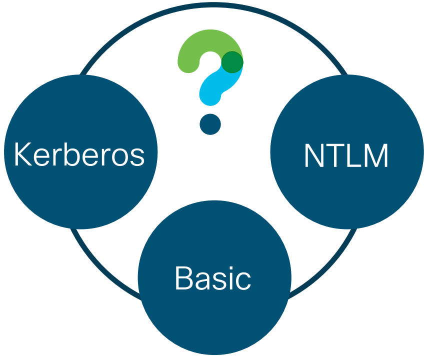
- Add custom accesslog fields to track auth mechanism and group membership

`%m` – Auth mechanism (`BASIC, NTLMSSP, NEGOTIATE,` etc.)

`%g` – Group information (“`DOMAIN\contractors`”)

Authentication





- Order doesn't matter with multiple DCs
- SYN is sent to all DCs at once
- First to respond is used, others are RST

- Kerberos is the most secure and is supported by OSX
- Do not use basic unless you have to and enable credential encryption

Kerberos integrated authentication (SSO)

Why

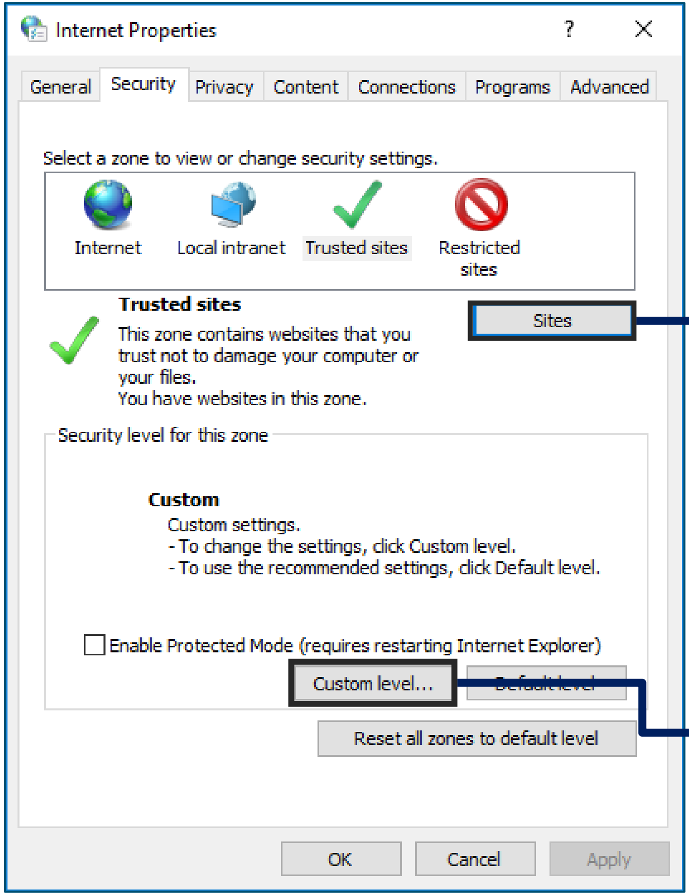
- NTLMv1/2: Hashes can be cracked offline or relayed
- Kerberos performs better
- Kerberos is supported by OSX/iOS
- Kerberos offers simpler trust management between domains

How

- Resources must use FQDNs (no short-names)
- Browsers must be configured to trust the devices
- Resources must be domain-joined

https://answers.microsoft.com/en-us/msoffice/forum/all/ntlm-vs-kerberos/d8b139bf-6b5a-4a53-9a00-bb75d4e219eb

Chrome / IE / Edge SSO on Windows



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Sites

Security level for this zone

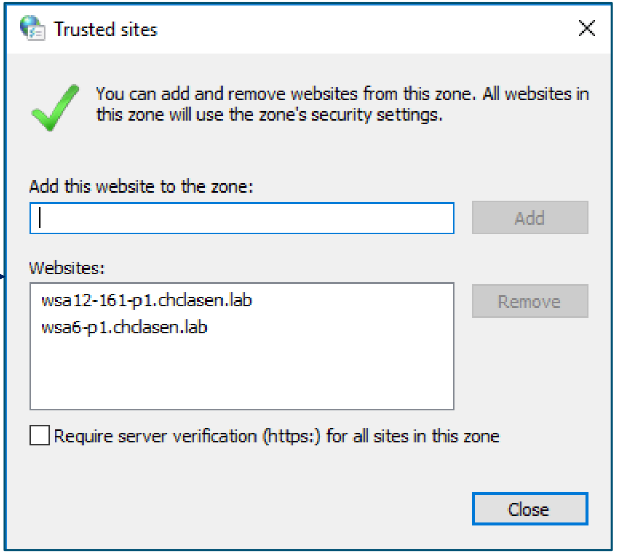
Custom
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

Reset all zones to default level

OK | Cancel | Apply



Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Add

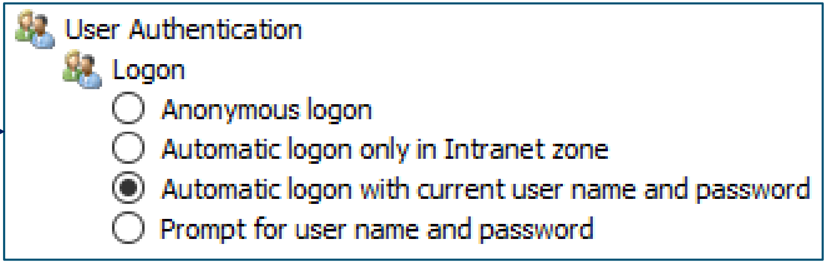
Websites:

wsa12-161-p1.chdasen.lab
wsa6-p1.chdasen.lab

Remove

□ Require server verification (https:) for all sites in this zone

Close



User Authentication

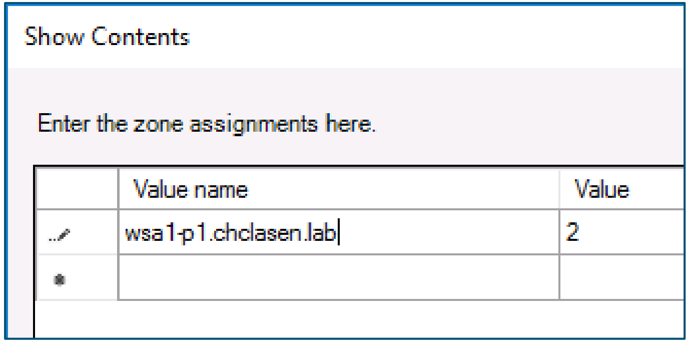
Logon

○ Anonymous logon
○ Automatic logon only in Intranet zone
● Automatic logon with current user name and password
○ Prompt for user name and password

Chrome / IE / Edge SSO in GPO

{Computer|User} Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\

Site to Zone Assignment List

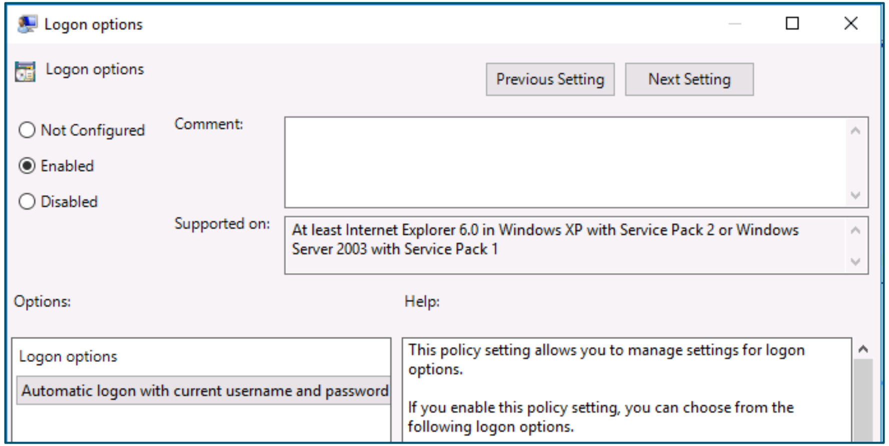


Show Contents

Enter the zone assignments here.

Value name	Value
wsa1-p1.chclasen.lab	2

Trusted Sites Zone\Logon options



Logon options

Logon options

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Internet Explorer 6.0 in Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1

Options:

Logon options

Automatic logon with current username and password

Help:

This policy setting allows you to manage settings for logon options.

If you enable this policy setting, you can choose from the following logon options.

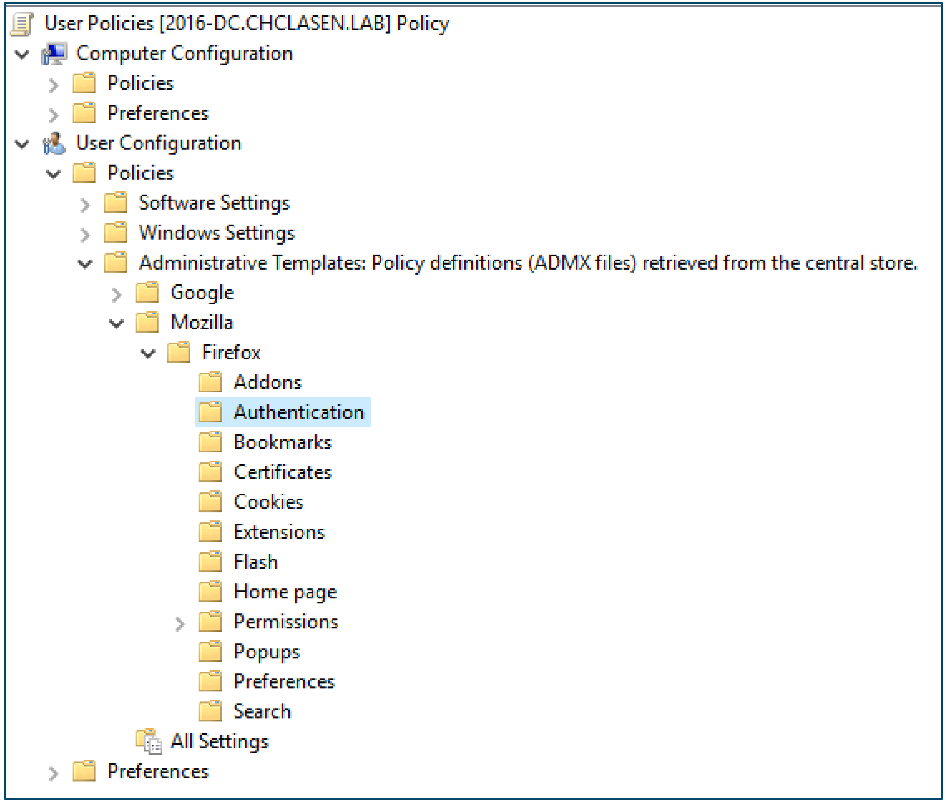
Firefox SSO

`about:config` requires the redirect hostname:

- Kerberos:
  - `network.negotiate-auth.trusted-uris`
- NTLM:
  - `network.automatic-ntlm-auth.trusted-uris`

Firefox SSO with GPO

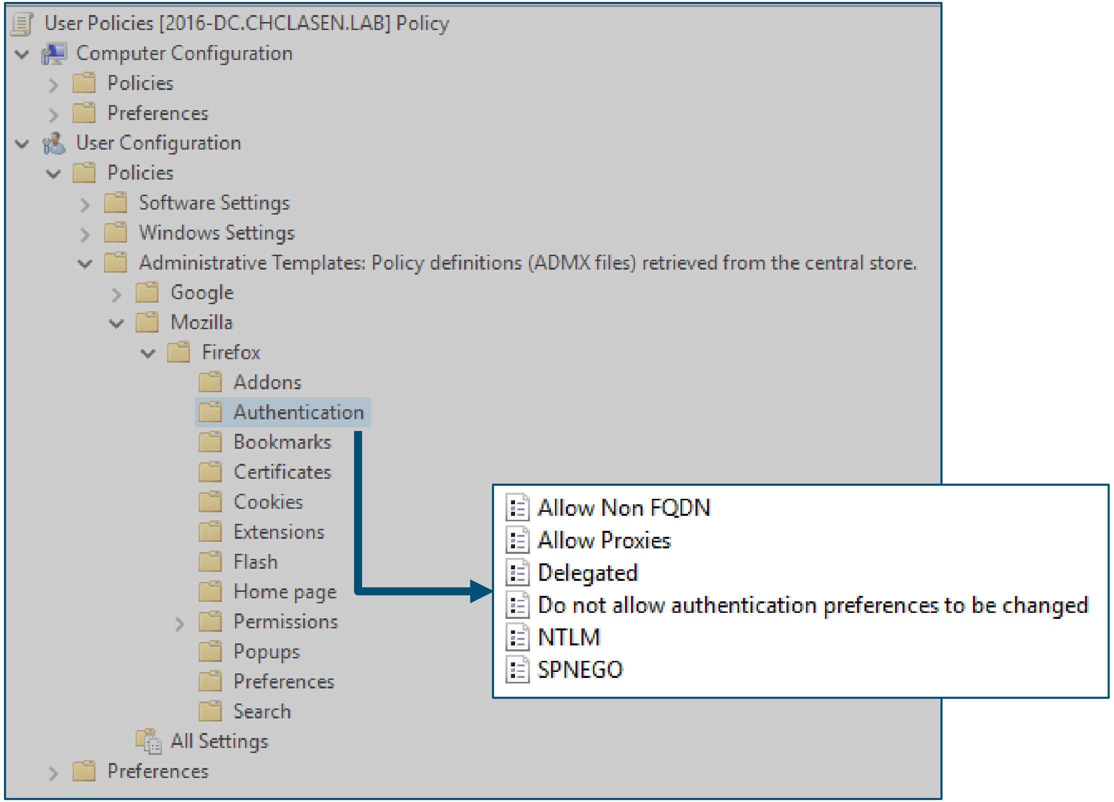
https://github.com/mozilla/policy-templates



- User Policies [2016-DC.CHCLASEN.LAB] Policy
  - Computer Configuration
    - Policies
    - Preferences
  - User Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy definitions (ADMX files) retrieved from the central store.
        - Google
        - Mozilla
          - Firefox
            - Addons
            - Authentication
            - Bookmarks
            - Certificates
            - Cookies
            - Extensions
            - Flash
            - Home page
            - Permissions
            - Popups
            - Preferences
            - Search
        - All Settings
    - Preferences

Firefox SSO with GPO

https://github.com/mozilla/policy-templates

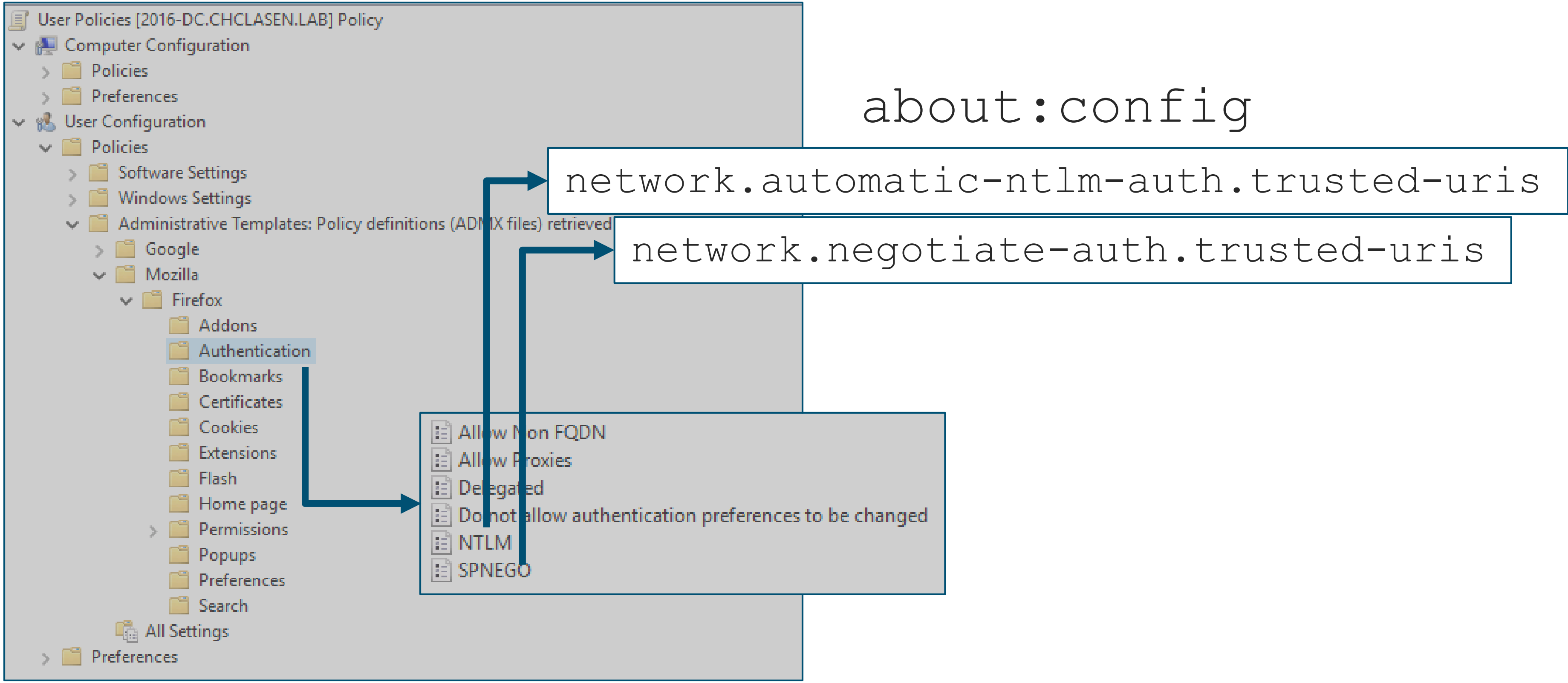


- User Policies [2016-DC.CHCLASEN.LAB] Policy
  - Computer Configuration
    - Policies
    - Preferences
  - User Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy definitions (ADMX files) retrieved from the central store.
        - Google
        - Mozilla
          - Firefox
            - Addons
            - Authentication
            - Bookmarks
            - Certificates
            - Cookies
            - Extensions
            - Flash
            - Home page
            - Permissions
            - Popups
            - Preferences
            - Search
        - All Settings
    - Preferences

Allow Non FQDN
Allow Proxies
Delegated
Do not allow authentication preferences to be changed
NTLM
SPNEGO

Firefox SSO with GPO

https://github.com/mozilla/policy-templates



- User Policies [2016-DC.CHCLASEN.LAB] Policy
  - Computer Configuration
    - Policies
    - Preferences
  - User Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy definitions (ADMX files) retrieved
        - Google
        - Mozilla
          - Firefox
            - Addons
            - Authentication
            - Bookmarks
            - Certificates
            - Cookies
            - Extensions
            - Flash
            - Home page
            - Permissions
            - Popups
            - Preferences
            - Search
          - All Settings
    - Preferences

Authentication:

- Allow Non FQDN
- Allow Proxies
- Delegated
- Do not allow authentication preferences to be changed
- NTLM
- SPNEGO

about:config

NTLM → `network.automatic-ntlm-auth.trusted-uris`

SPNEGO → `network.negotiate-auth.trusted-uris`

Chrome on Mac OSX

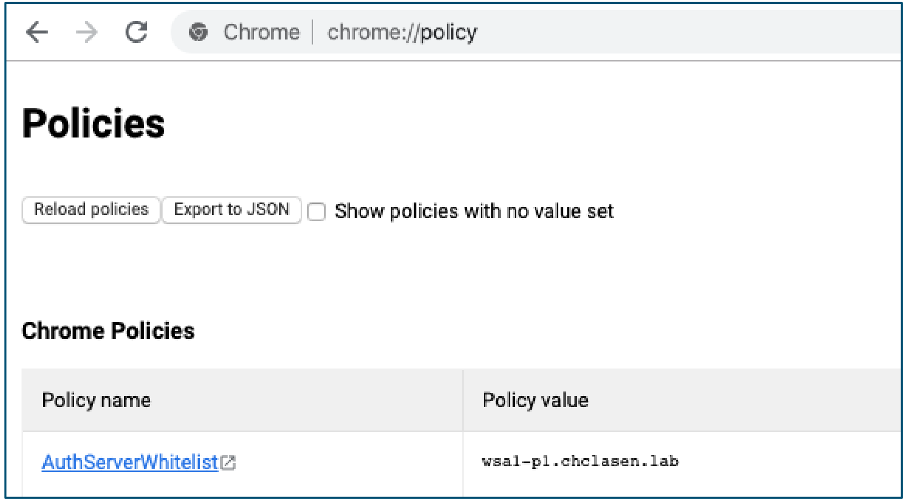
https://www.chromium.org/administrators/policy-list-3#AuthServerWhitelist

Terminal command:

```
defaults write com.google.Chrome AuthServerWhitelist ”wsa1-p1.chclasen.lab”
```

Chrome flag:

```
--args --auth-server-whitelist=”wsa1-p1.chclasen.lab"
```



Policies

Chrome Policies

Policy name	Policy value
AuthServerWhitelist	wsa1-p1.chclasen.lab

Integrated authentication (SSO)

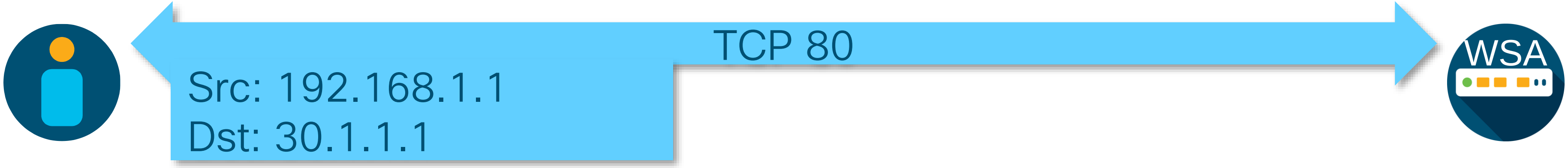
- Confirm that the SPN is set for the redirect hostname
- Manually delete old SPNs and re-join the domain if necessary
  - Use the setspn Windows utility

```
PS C:\WINDOWS\system32> setspn -L wsa6 | Select-String HTTP

        HTTP/WSA6-P1.CHCLASEN.LAB.CHCLASEN.LAB
        HTTP/WSA6-P1.CHCLASEN.LAB
        HTTP/WSA6.CHCLASEN.LAB.CHCLASEN.LAB
        HTTP/wsa6.chclasen.lab
        HTTP/WSA6
```

Transparent authentication packet flow

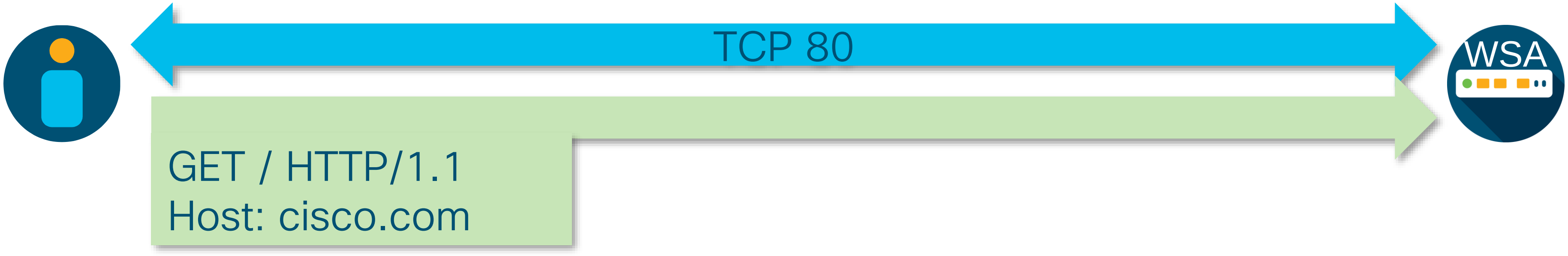
WSA

Transparent authentication packet flow



Src: 192.168.1.1
Dst: 30.1.1.1

Transparent authentication packet flow

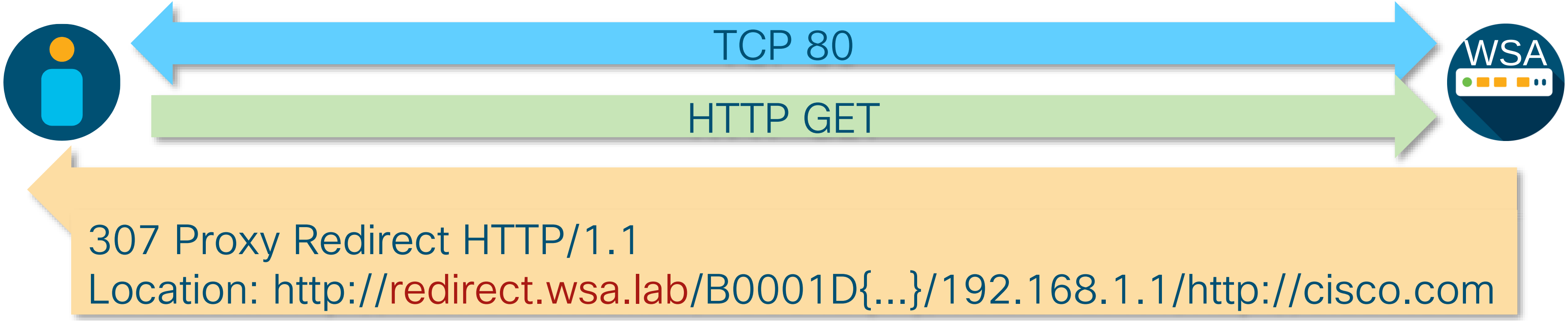


TCP 80

WSA

GET / HTTP/1.1
Host: cisco.com

Transparent authentication packet flow

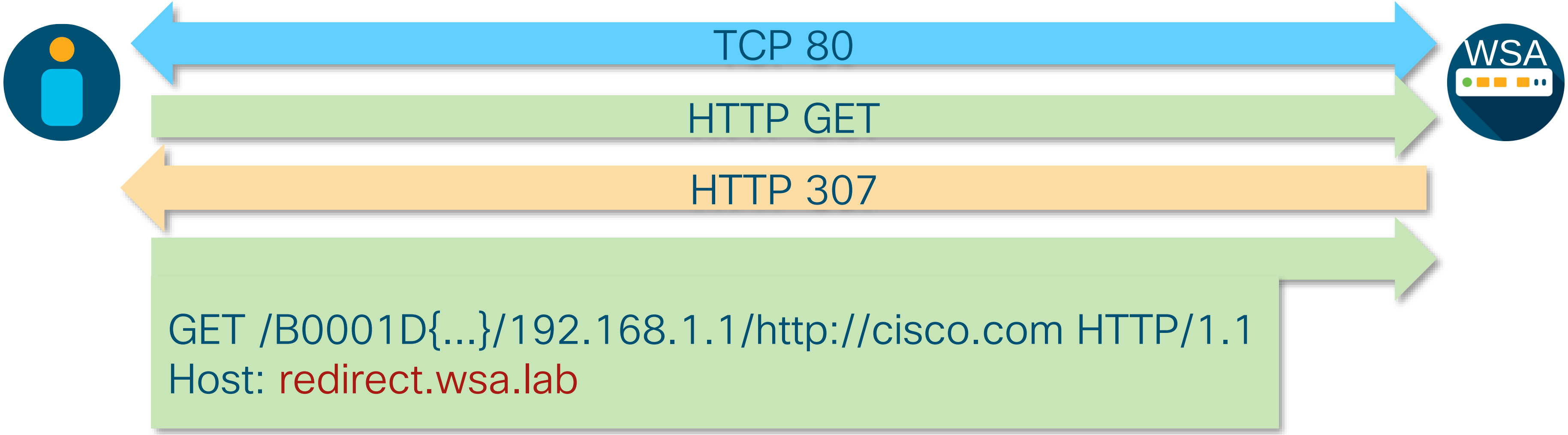


TCP 80

HTTP GET

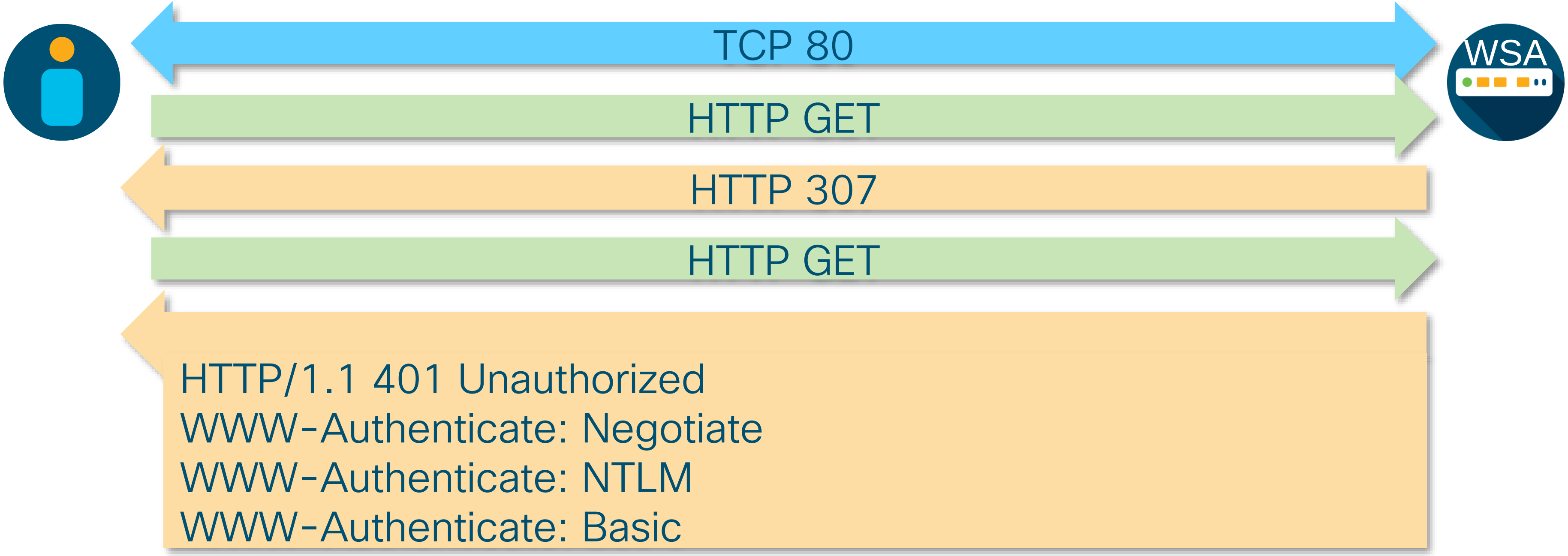
307 Proxy Redirect HTTP/1.1
Location: http://redirect.wsa.lab/B0001D{...}/192.168.1.1/http://cisco.com

Transparent authentication packet flow



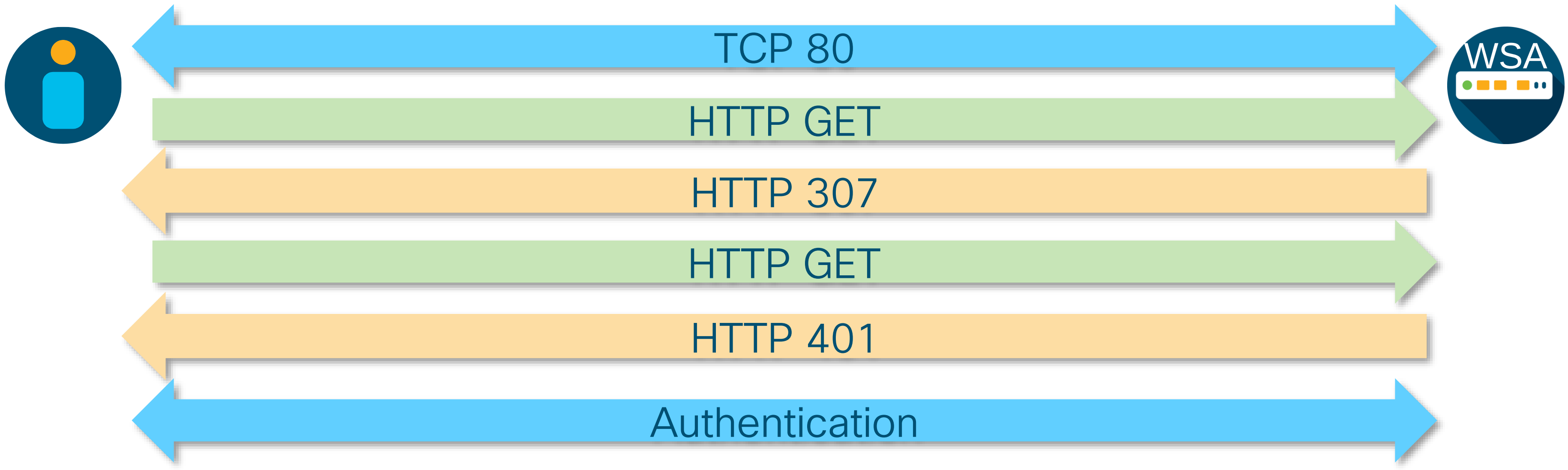
GET /B0001D{...}/192.168.1.1/http://cisco.com HTTP/1.1
Host: redirect.wsa.lab

Transparent authentication packet flow

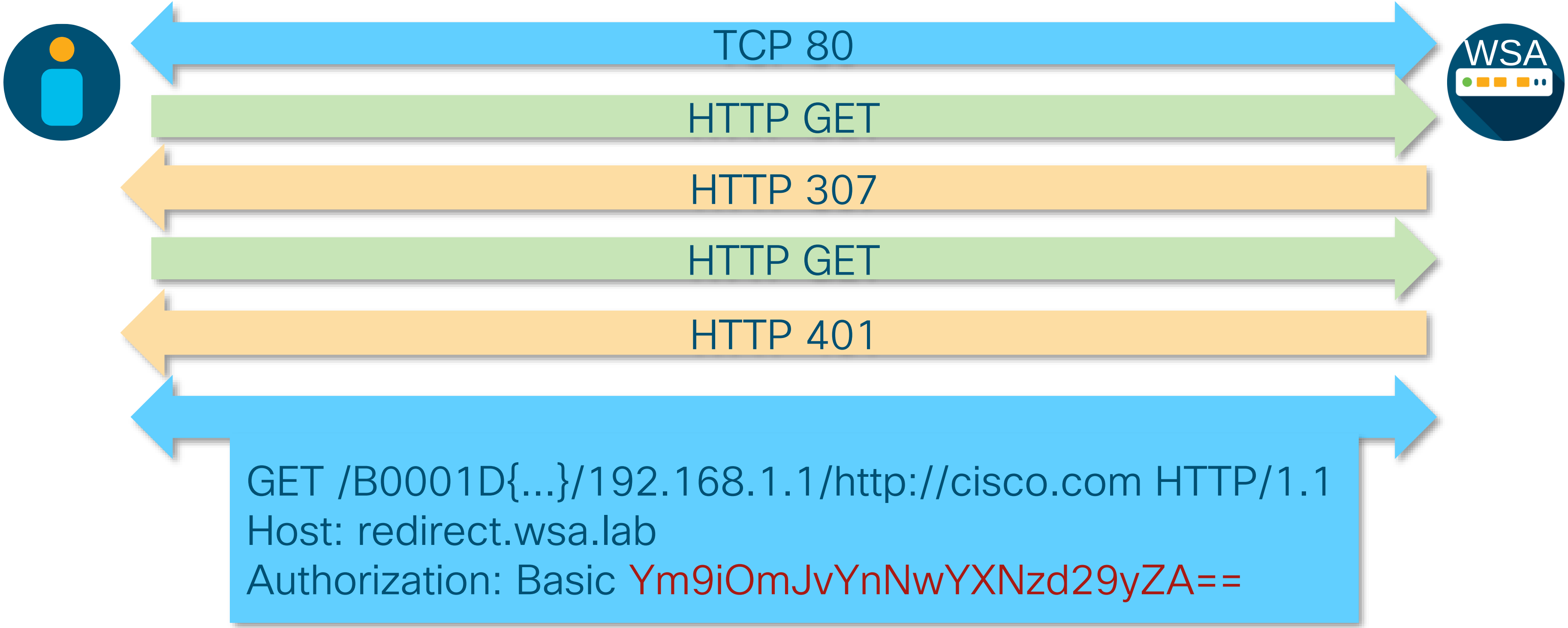


```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Negotiate
WWW-Authenticate: NTLM
WWW-Authenticate: Basic
```

Transparent authentication packet flow

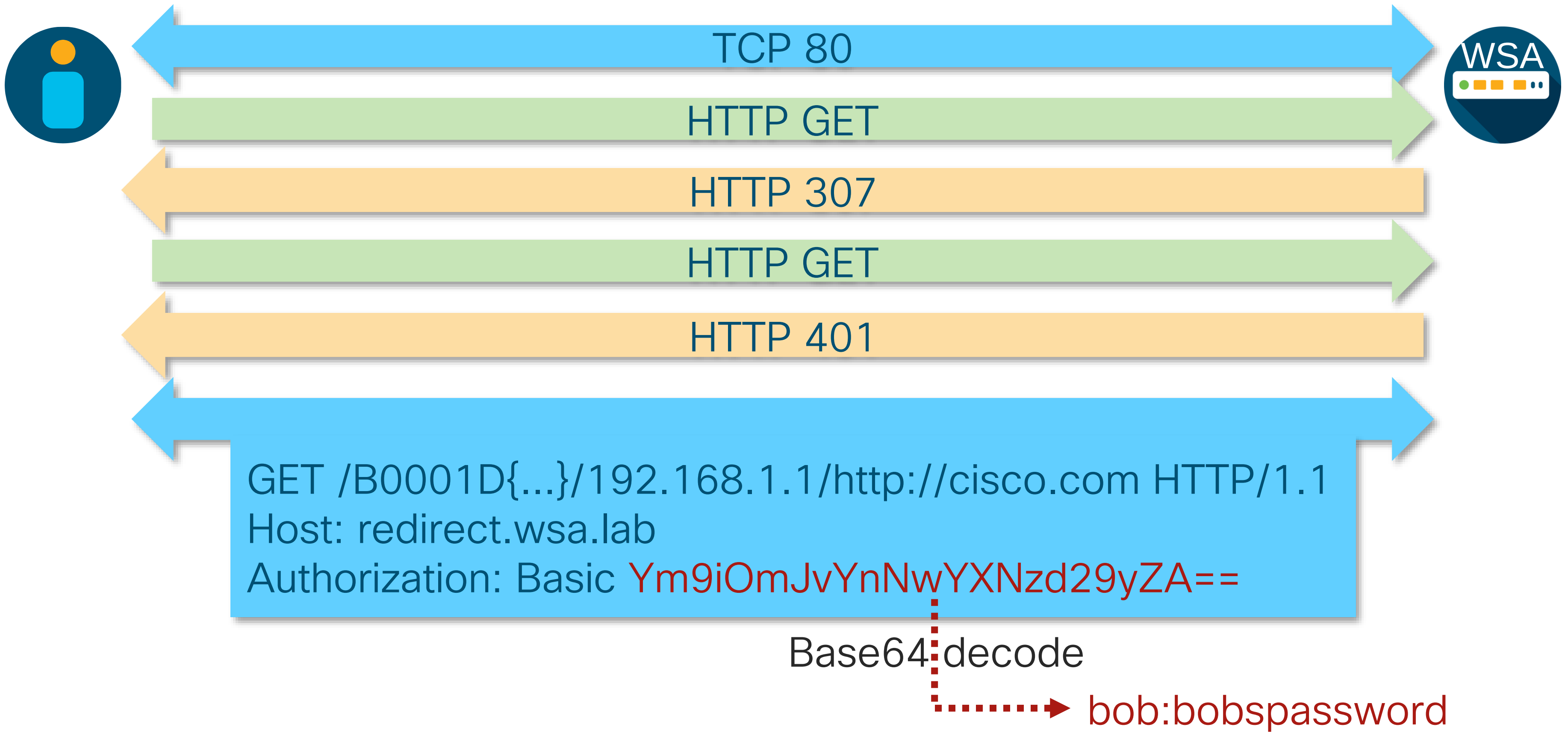


Transparent authentication packet flow



```
GET /B0001D{...}/192.168.1.1/http://cisco.com HTTP/1.1
Host: redirect.wsa.lab
Authorization: Basic Ym9iOmJvYnNwYXNzd29yZA==
```

Transparent authentication packet flow

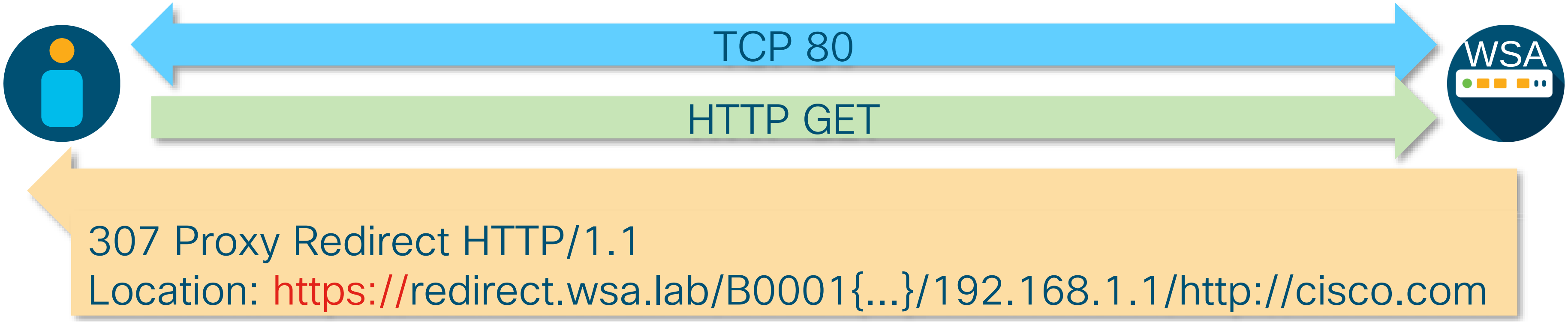


```
GET /B0001D{...}/192.168.1.1/http://cisco.com HTTP/1.1
Host: redirect.wsa.lab
Authorization: Basic Ym9iOmJvYnNwYXNzd29yZA==
```

Base64 decode

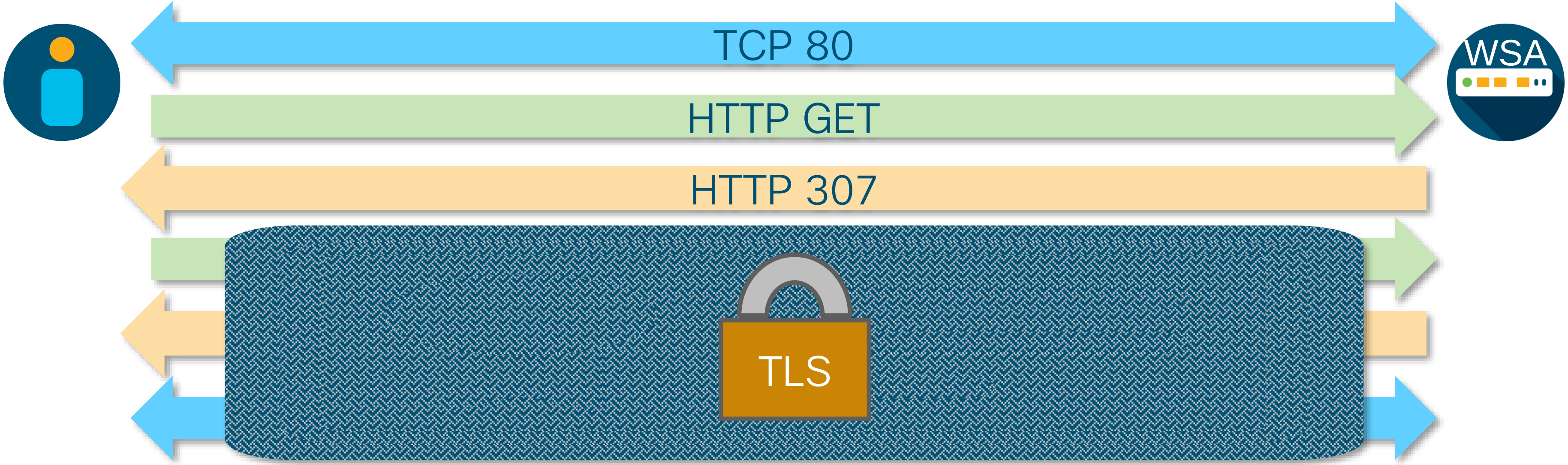
bob:bobspassword

Transparent authentication packet flow

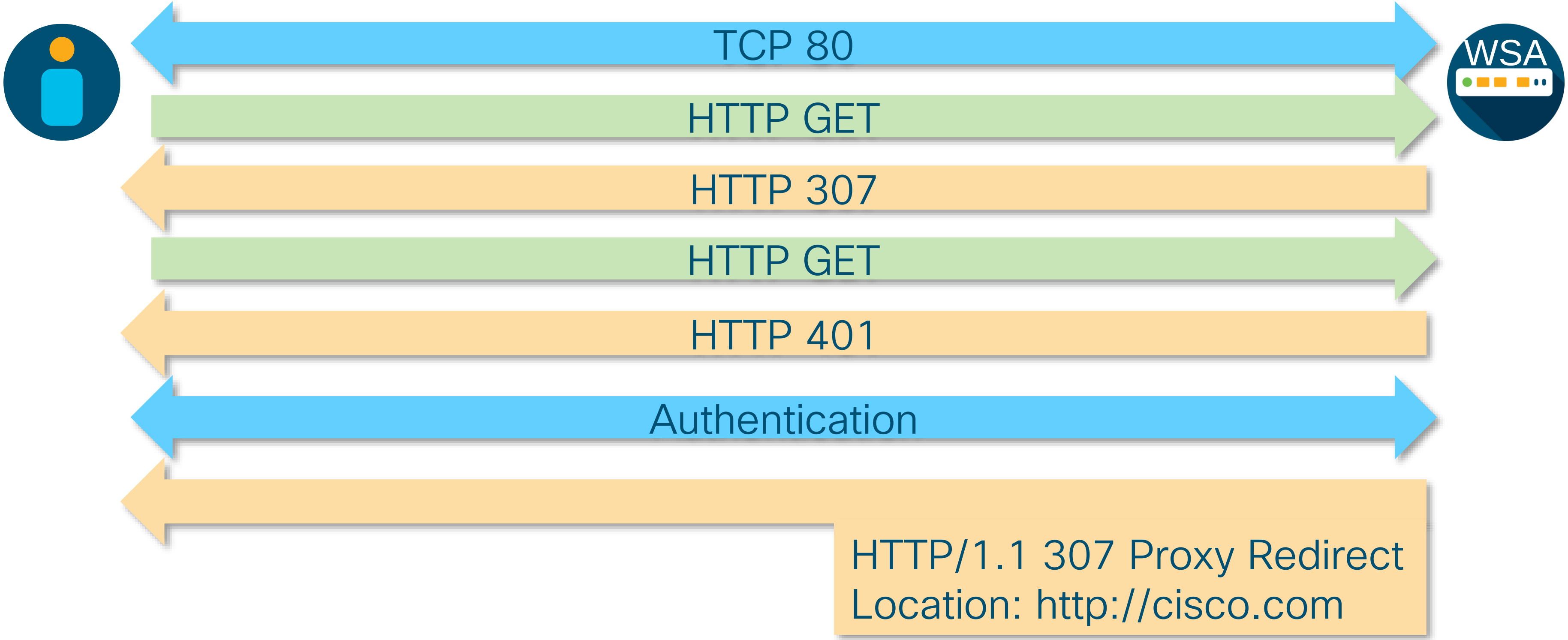


307 Proxy Redirect HTTP/1.1
Location: https://redirect.wsa.lab/B0001{...}/192.168.1.1/http://cisco.com

Transparent authentication packet flow

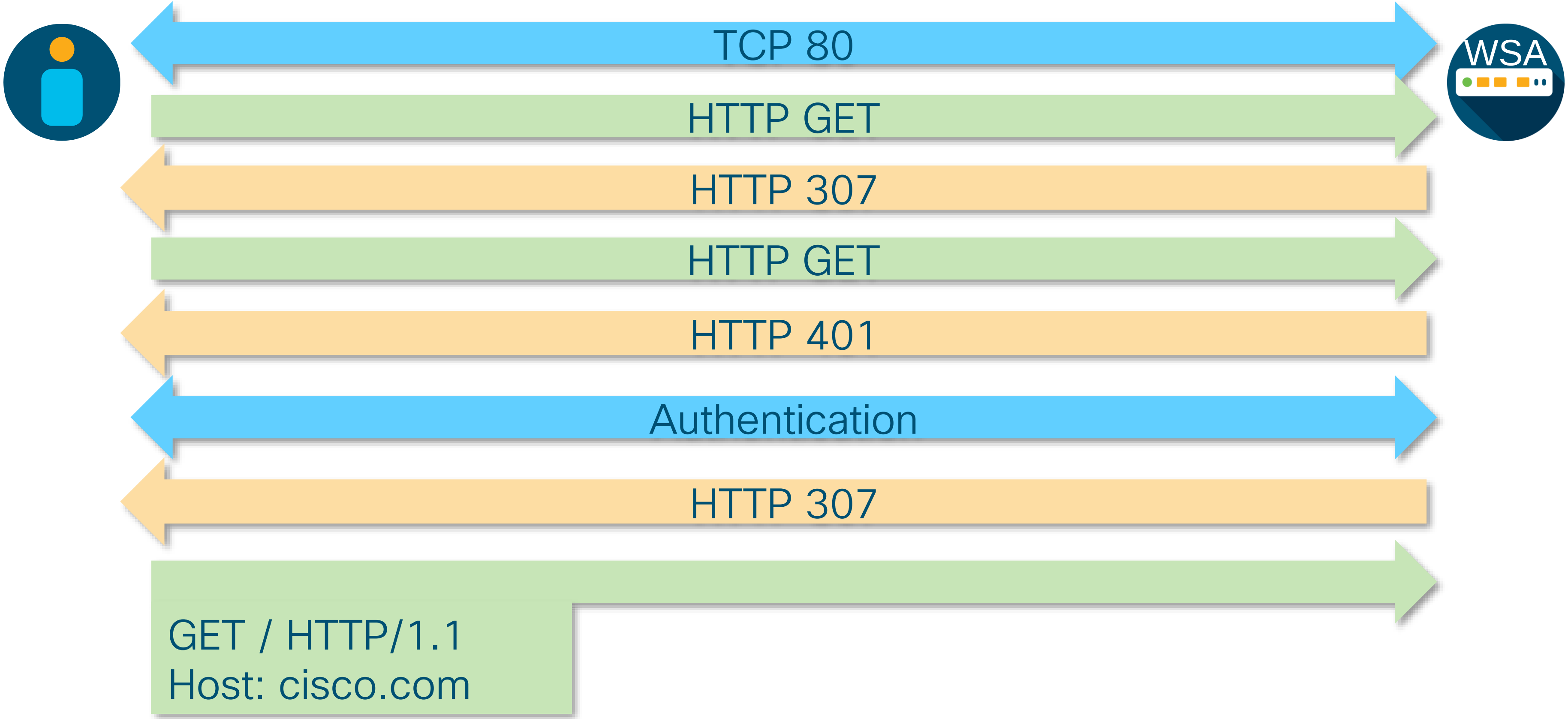


Transparent authentication packet flow



HTTP/1.1 307 Proxy Redirect
Location: http://cisco.com

Transparent authentication packet flow



TCP 80

HTTP GET

HTTP 307

HTTP GET

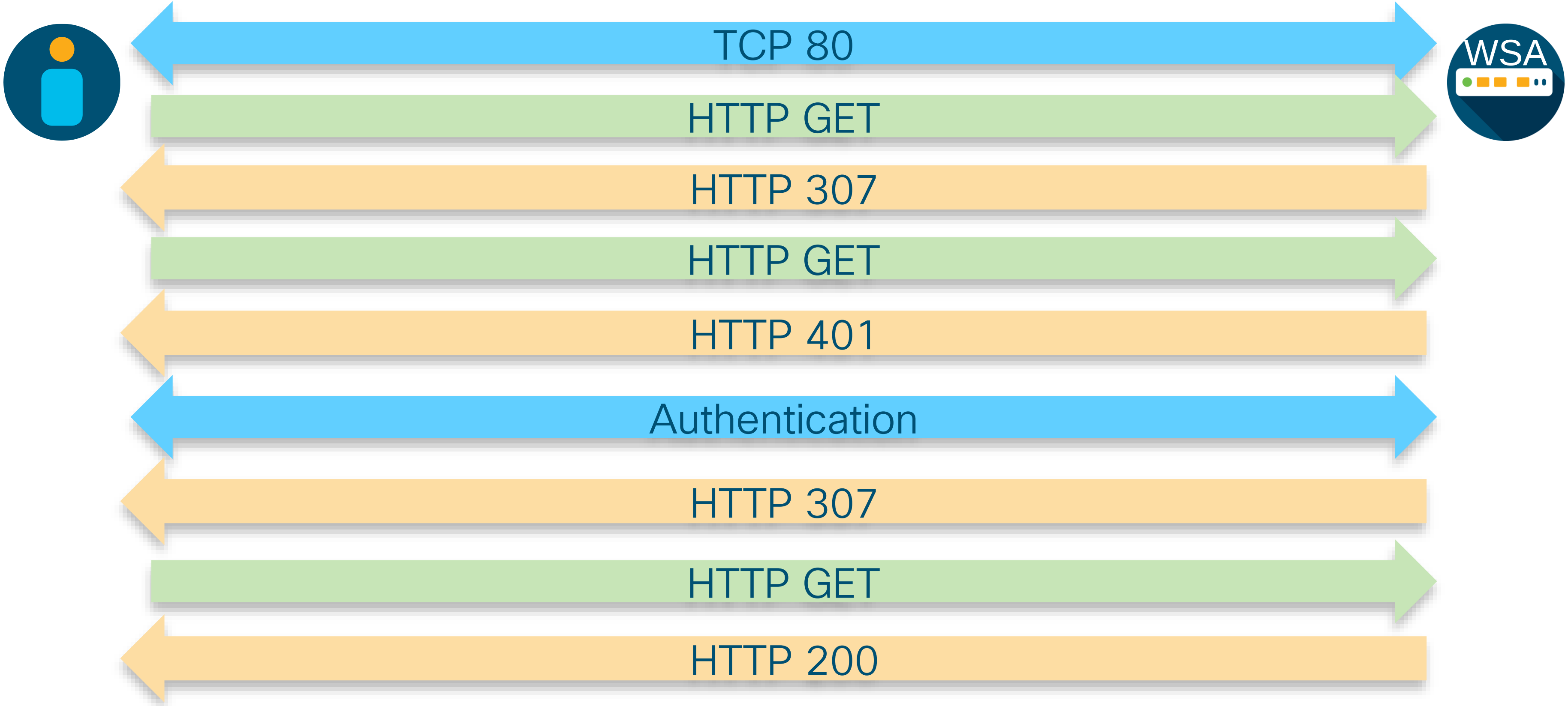
HTTP 401

Authentication

HTTP 307

GET / HTTP/1.1
Host: cisco.com

Transparent authentication packet flow



TCP 80

HTTP GET

HTTP 307

HTTP GET

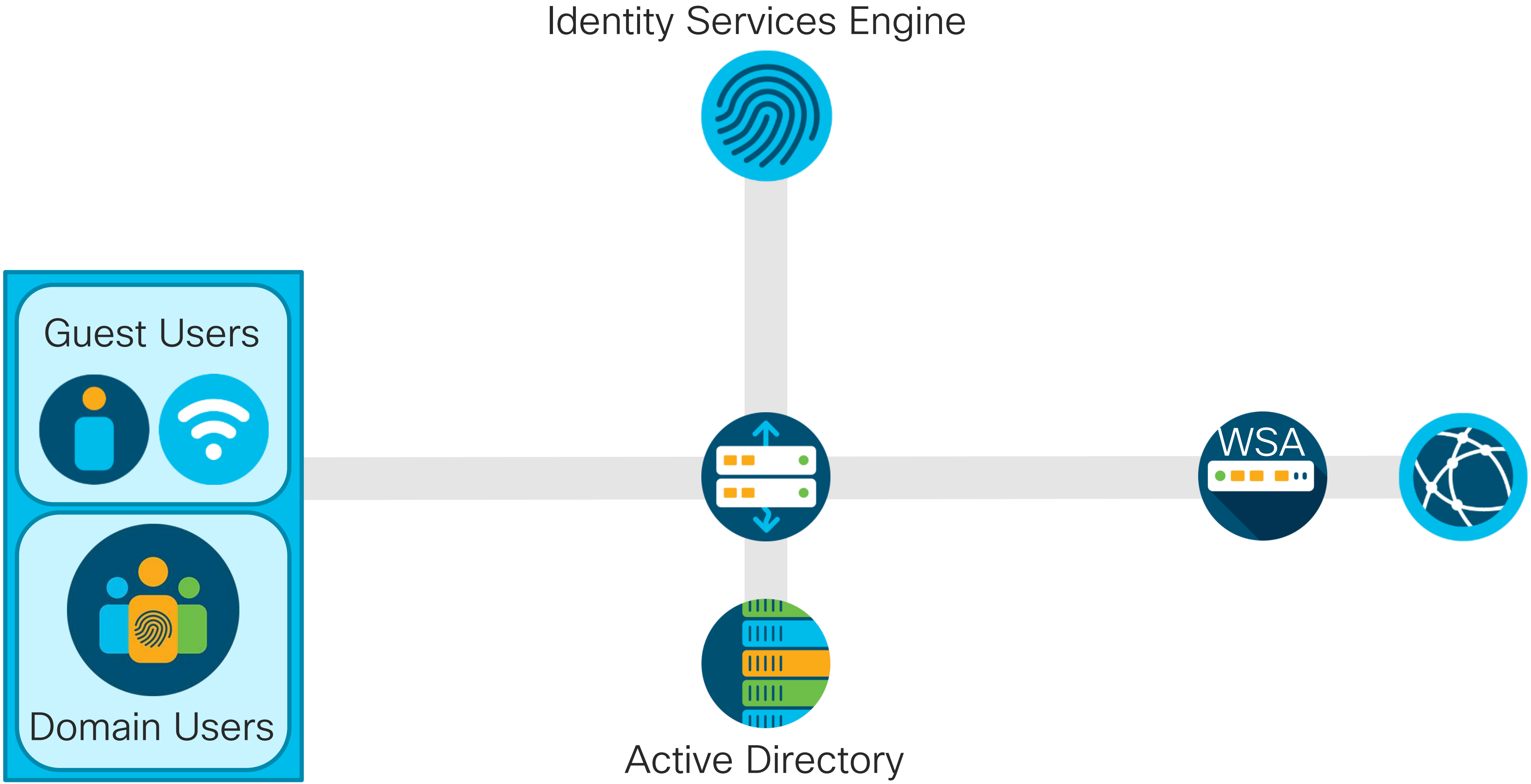
HTTP 401

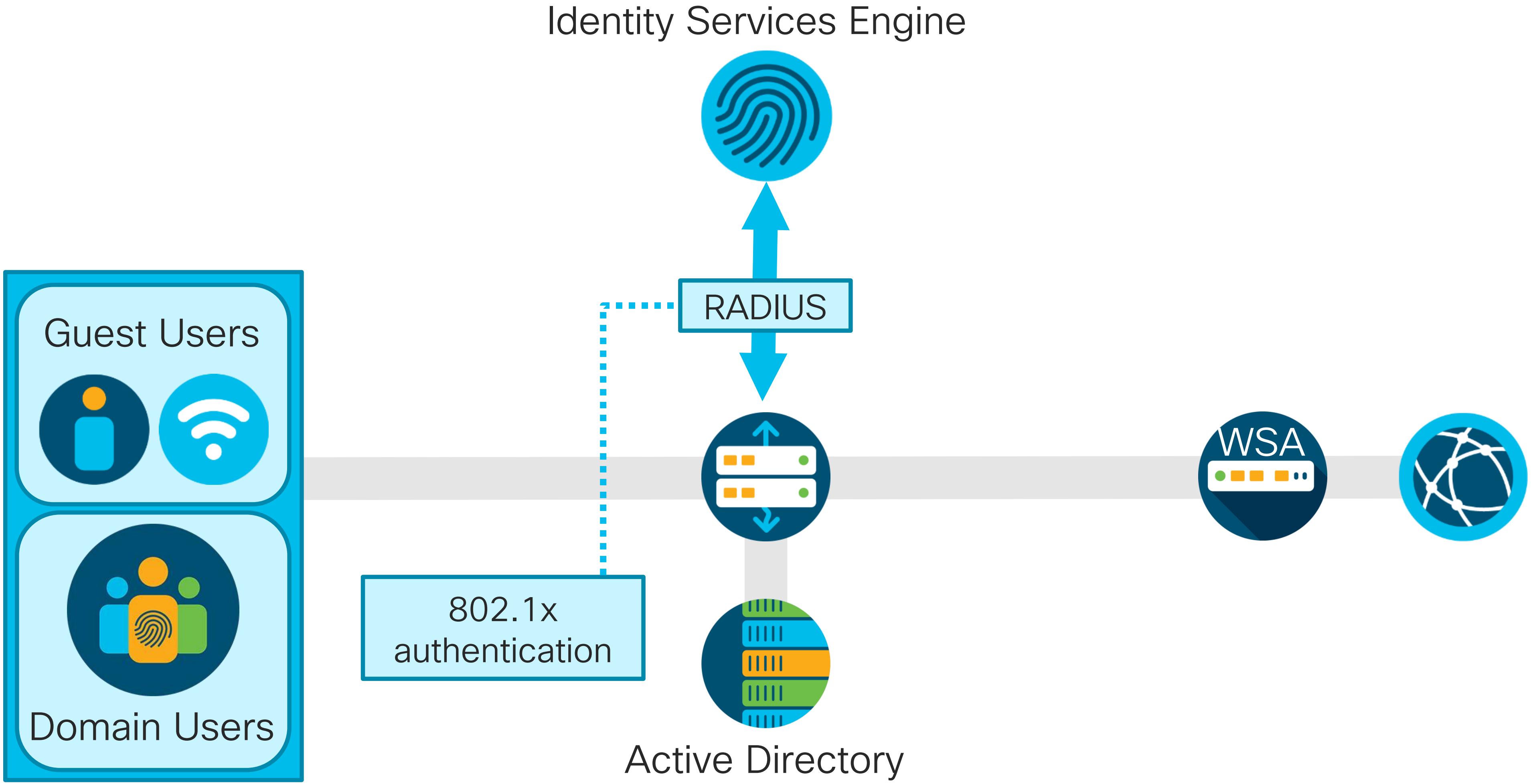
Authentication

HTTP 307

HTTP GET

HTTP 200


Identity Services Engine
Guest Users
Domain Users
WSA
Active Directory



Identity Services Engine

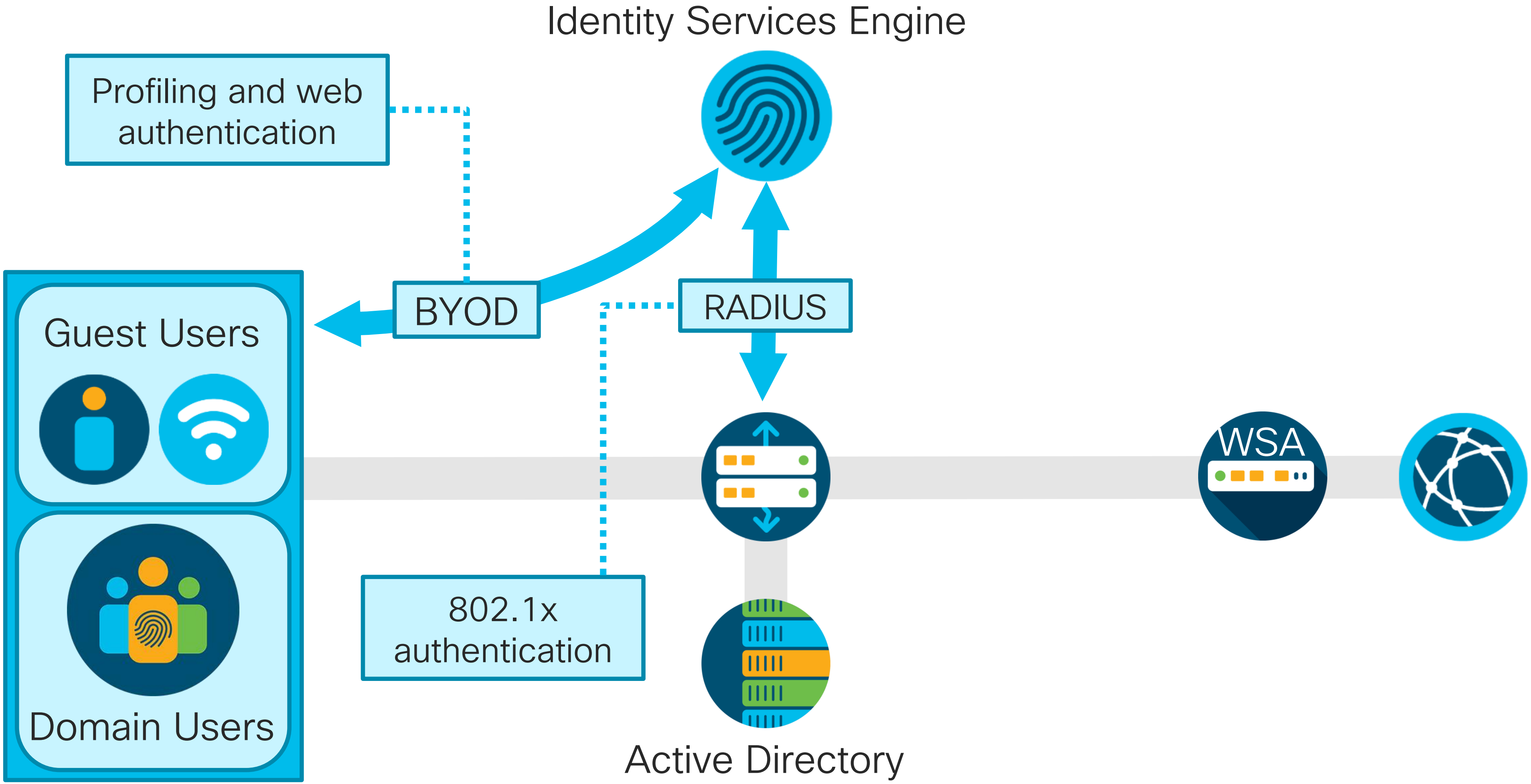
RADIUS

Guest Users

Domain Users

802.1x authentication

Active Directory



Identity Services Engine

Profiling and web authentication

BYOD

RADIUS

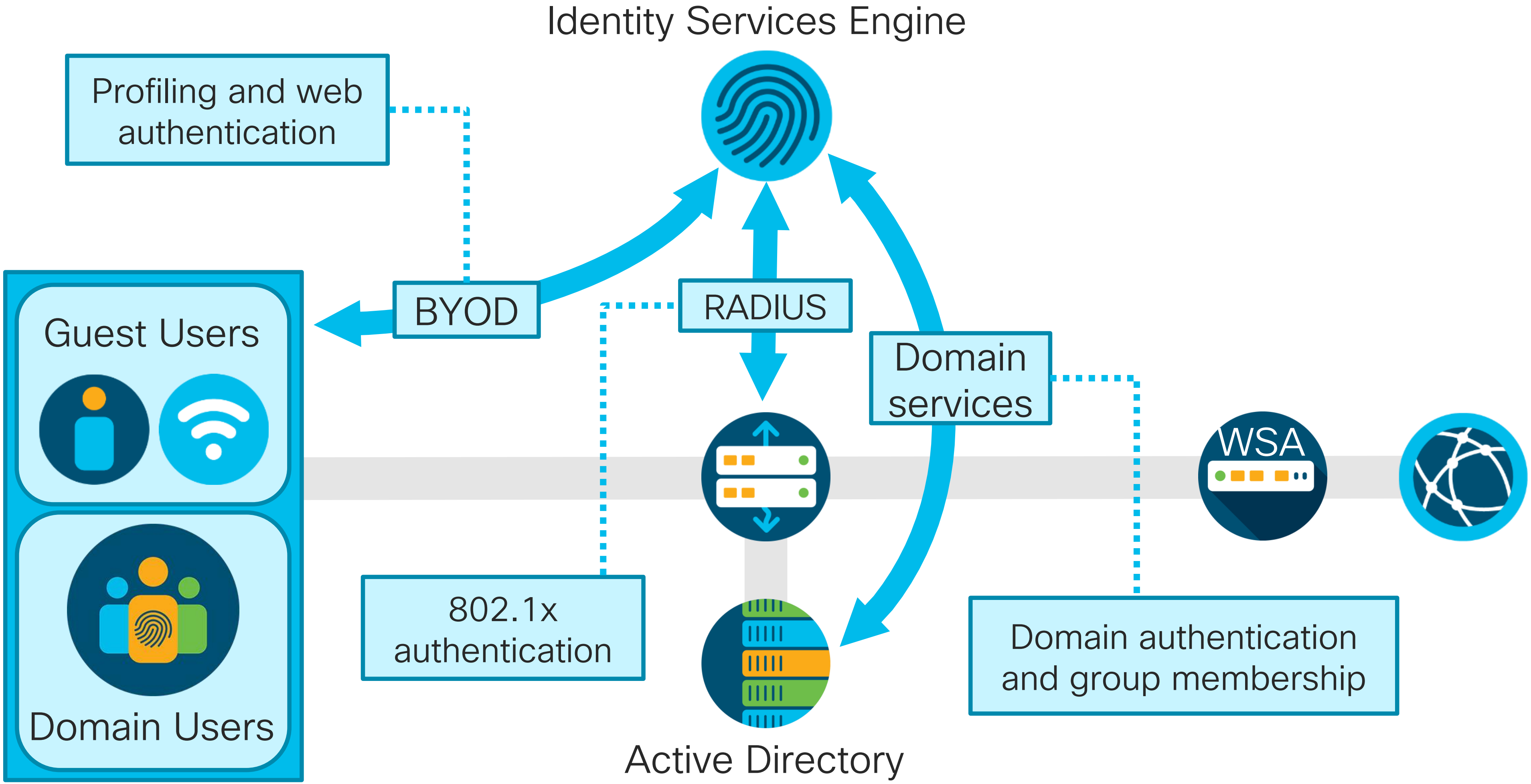
Guest Users

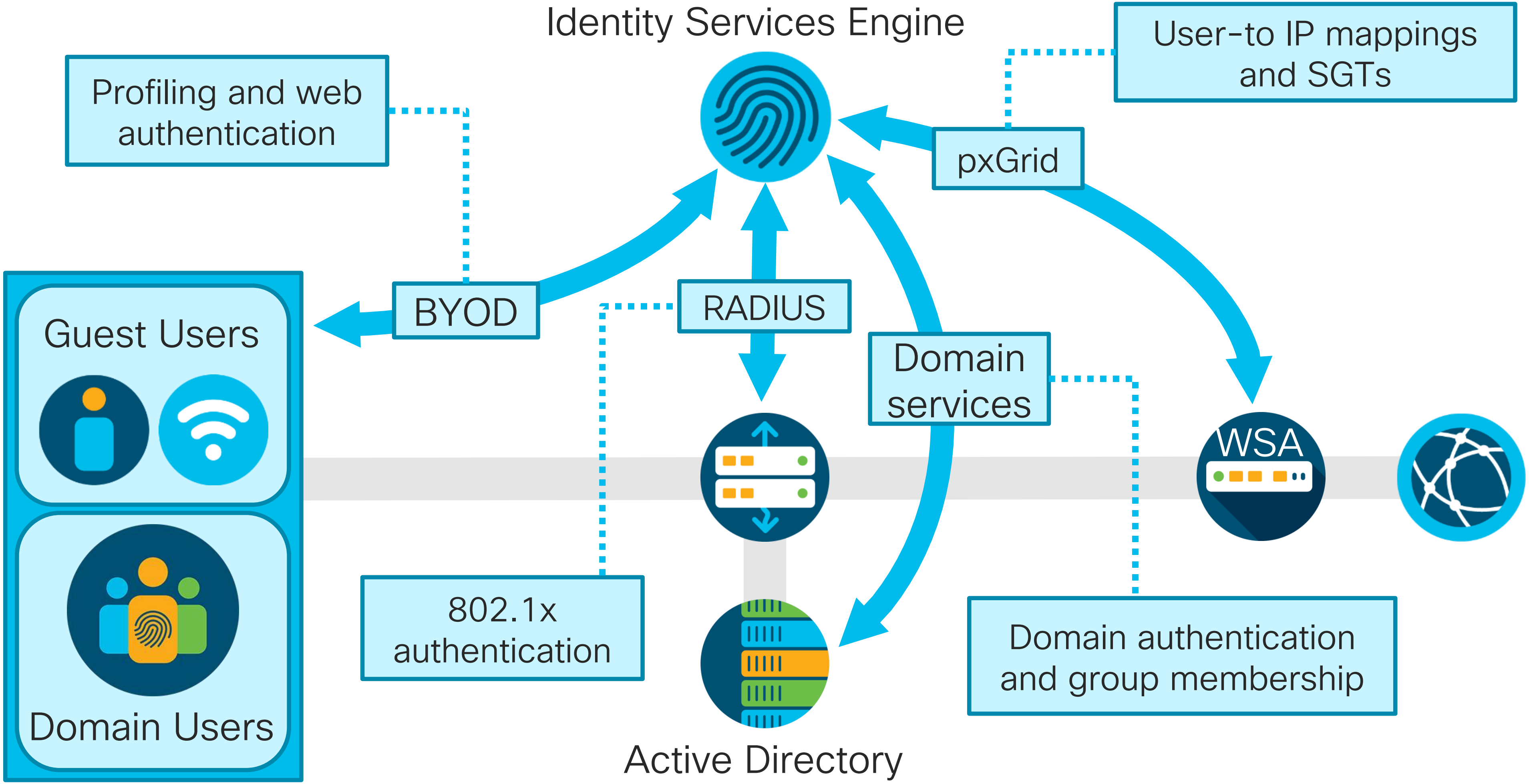
Domain Users

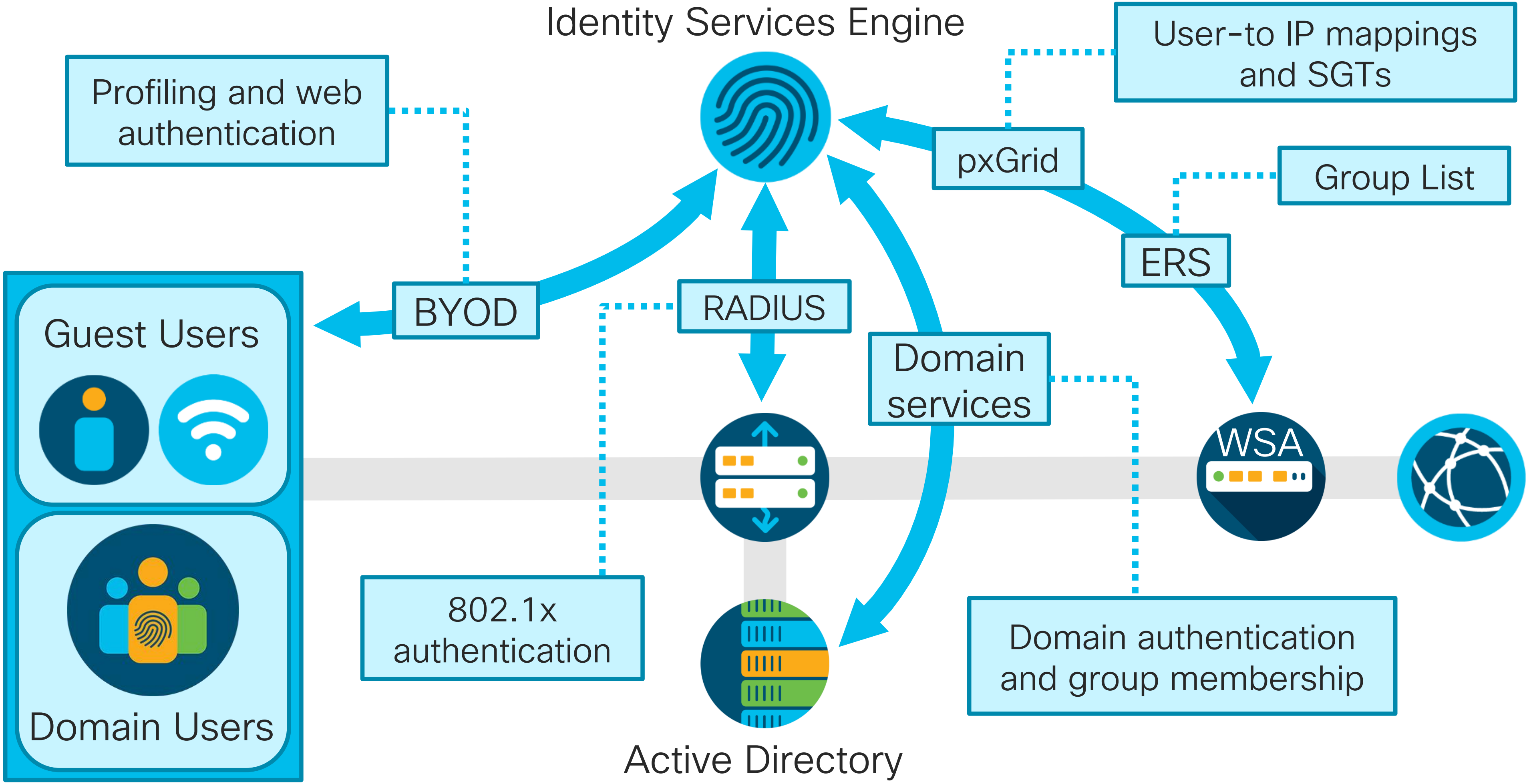
802.1x authentication

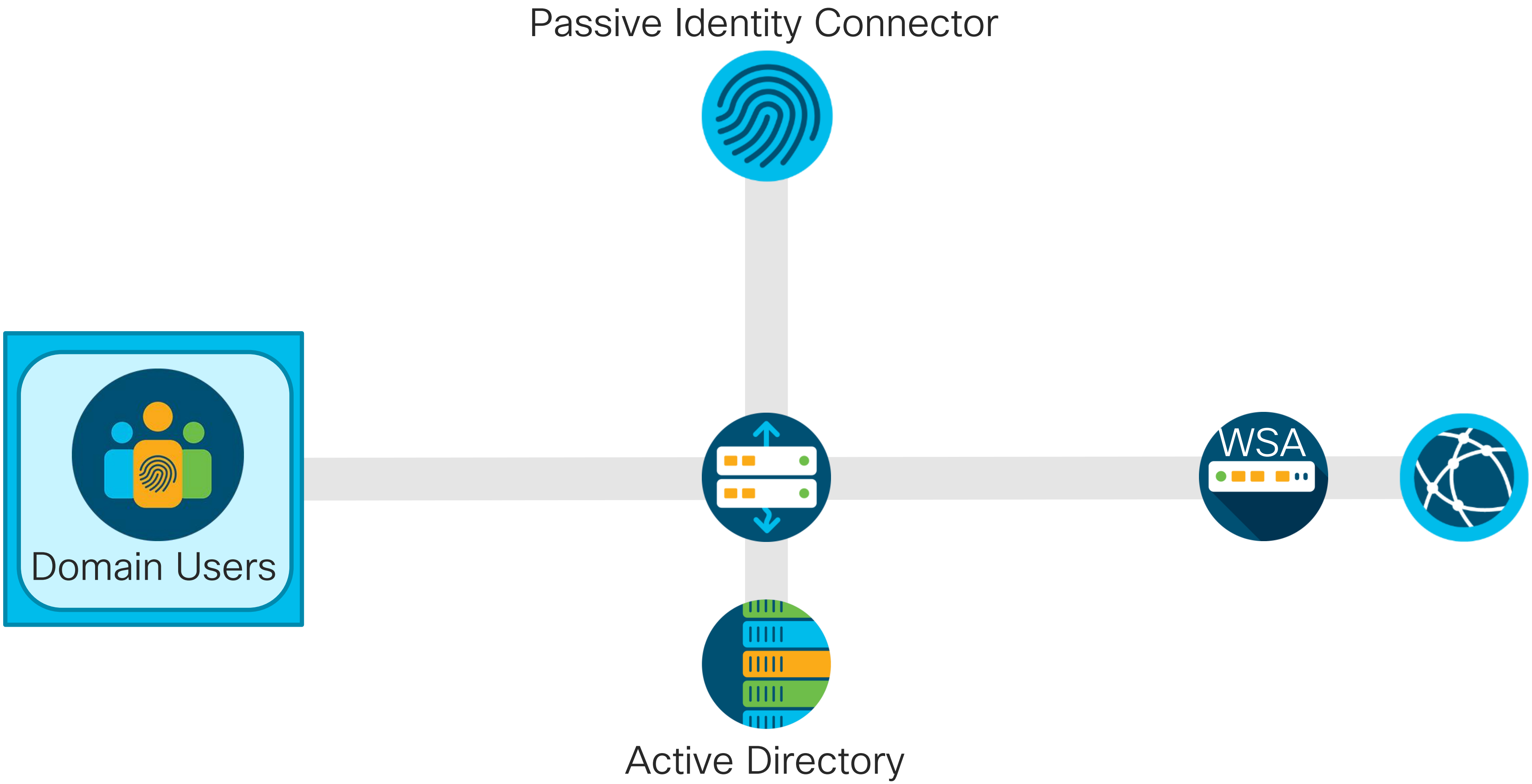
WSA

Active Directory

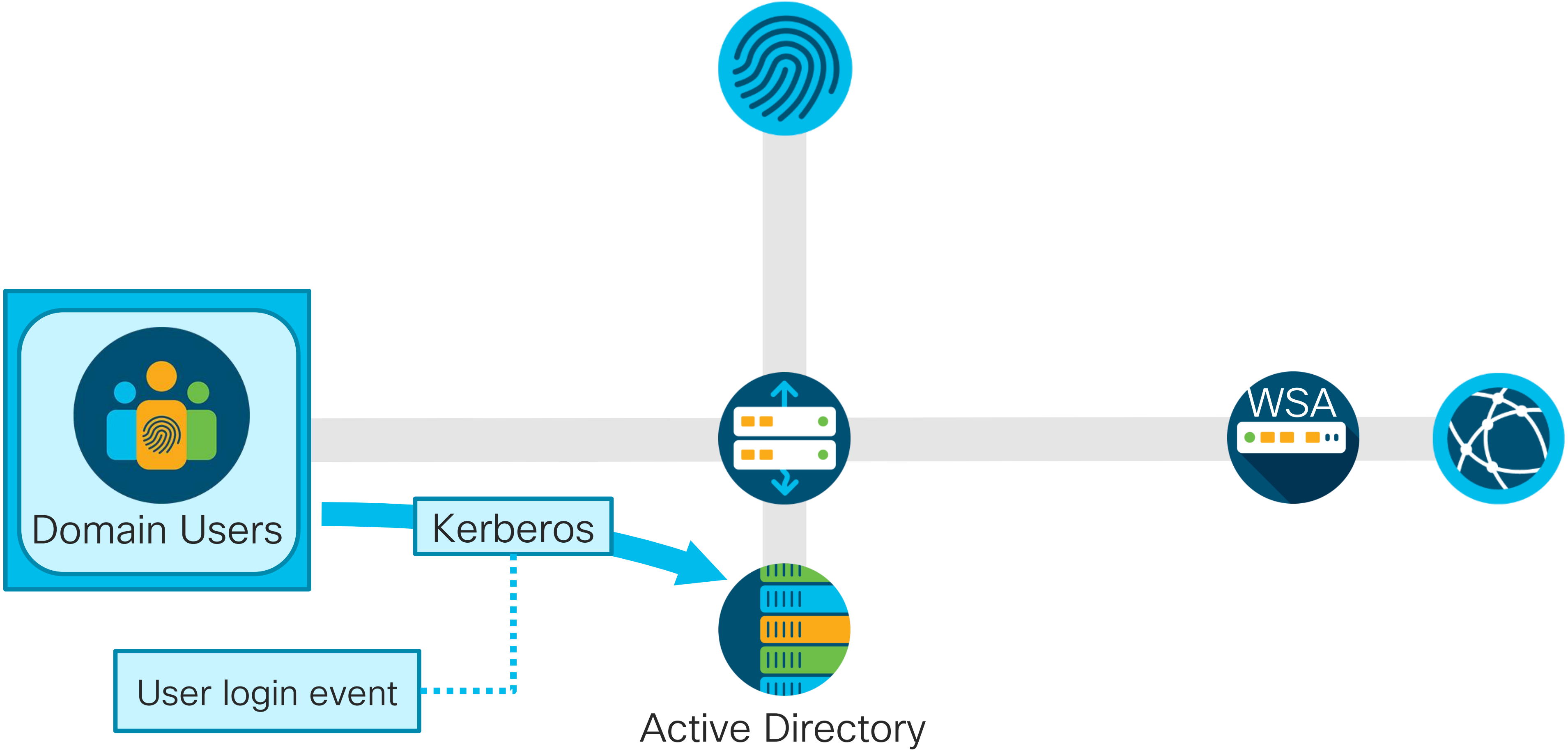

Identity Services Engine
Profiling and web authentication
BYOD
RADIUS
Domain services
Guest Users
Domain Users
802.1x authentication
WSA
Active Directory
Domain authentication and group membership

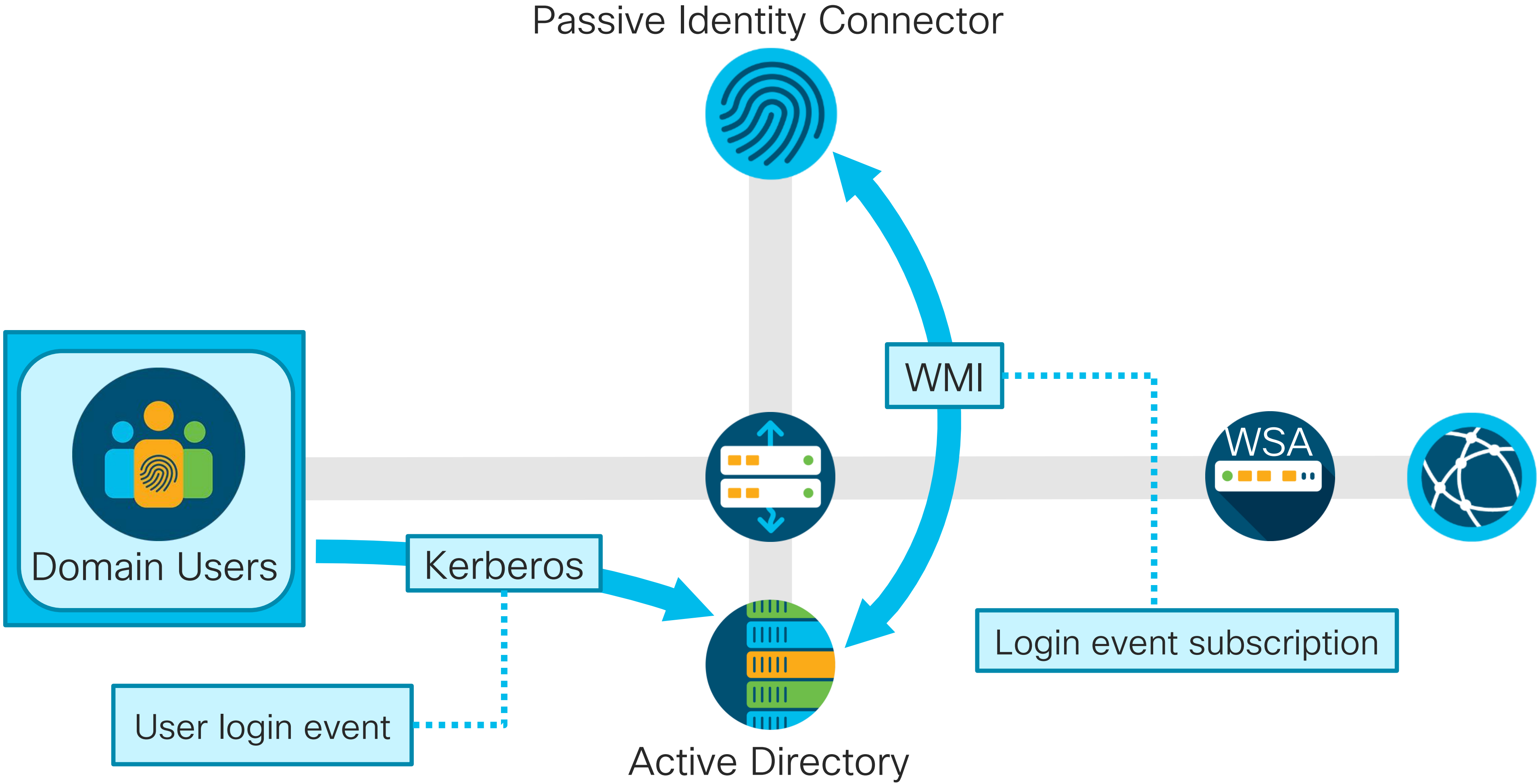

Identity Services Engine
Profiling and web authentication
User-to IP mappings and SGTs
pxGrid
BYOD
RADIUS
Guest Users
Domain services
WSA
Domain Users
802.1x authentication
Domain authentication and group membership
Active Directory

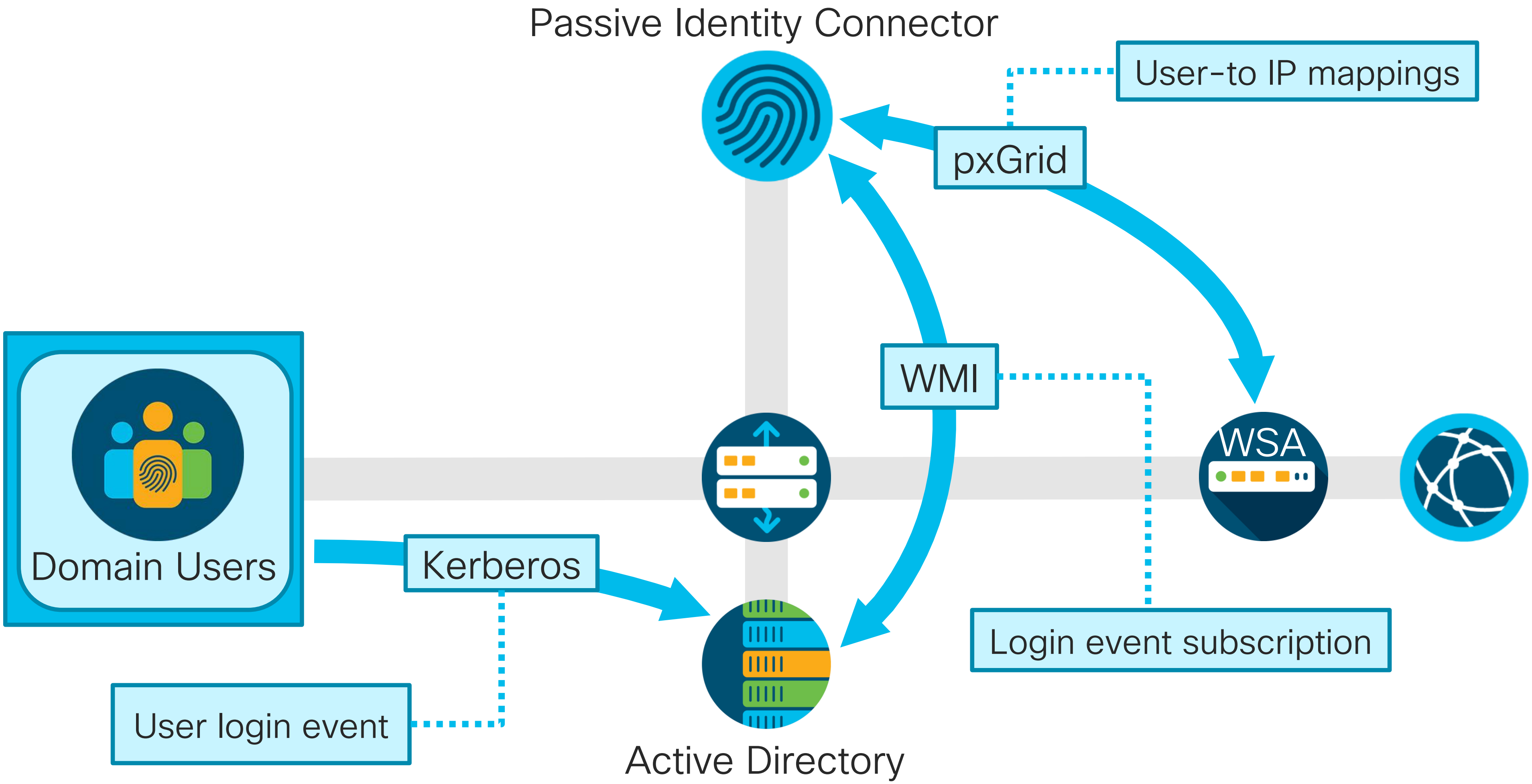

Identity Services Engine
Profiling and web authentication
User-to IP mappings and SGTs
pxGrid
Group List
ERS
BYOD
RADIUS
Domain services
Guest Users
Domain Users
WSA
802.1x authentication
Domain authentication and group membership
Active Directory

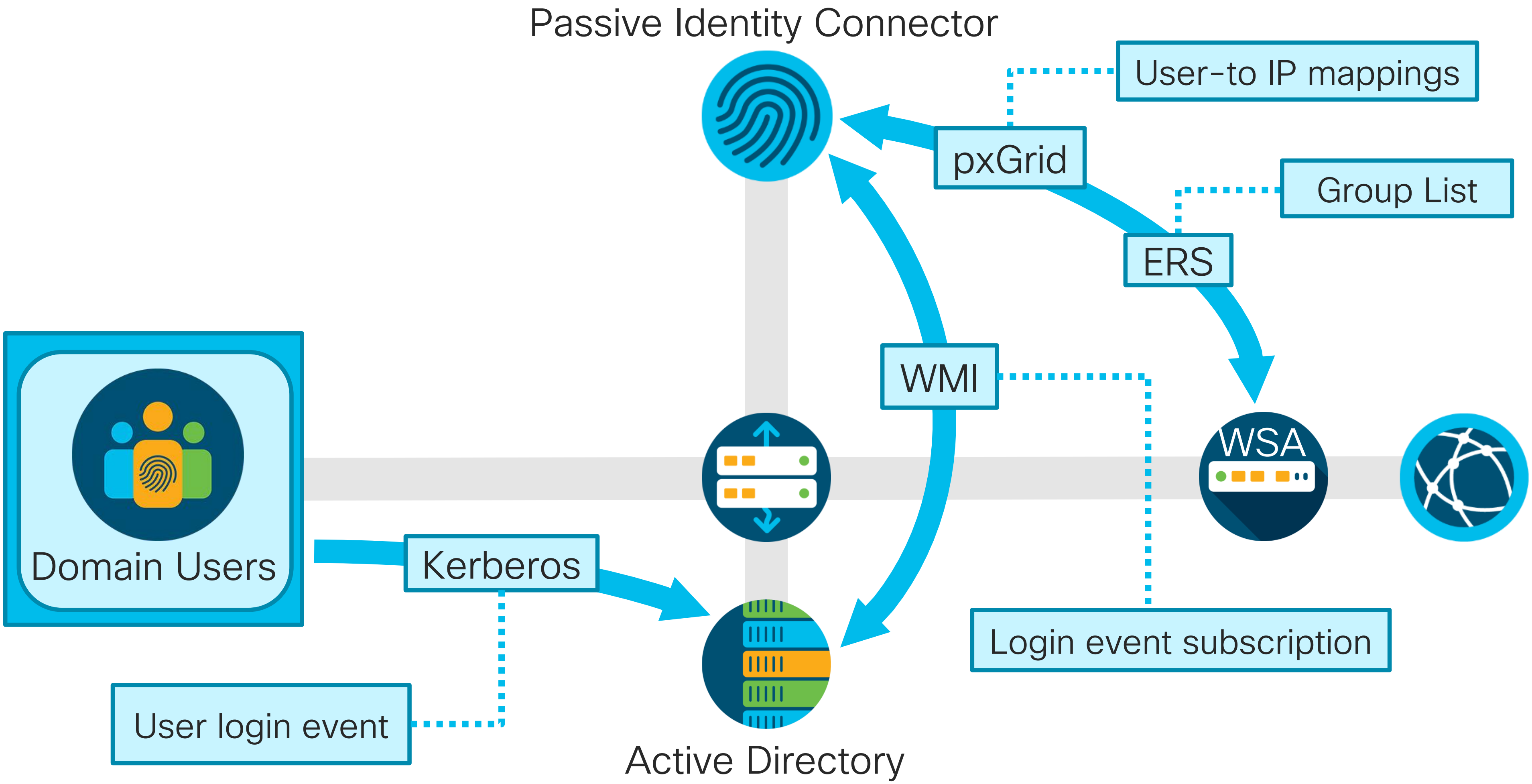

Passive Identity Connector
Domain Users
WSA
Active Directory

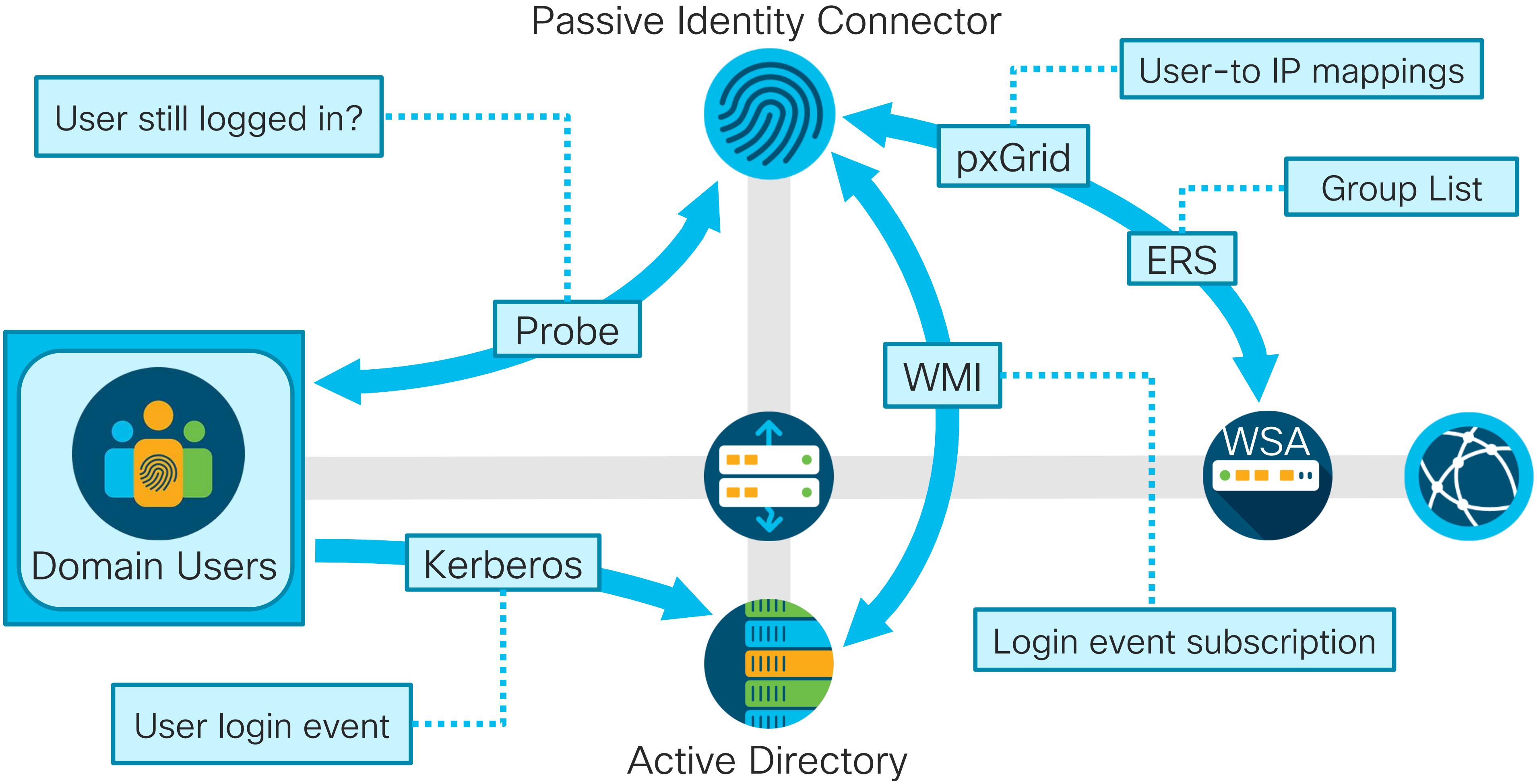
Passive Identity Connector




Passive Identity Connector
WMI
Domain Users
Kerberos
WSA
Login event subscription
User login event
Active Directory


Passive Identity Connector
User-to IP mappings
pxGrid
WMI
WSA
Domain Users
Kerberos
Login event subscription
User login event
Active Directory

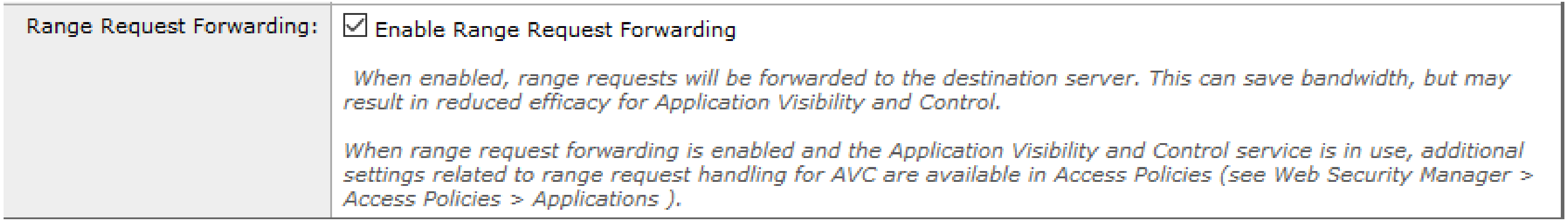

Passive Identity Connector
User-to IP mappings
pxGrid
Group List
ERS
WMI
WSA
Domain Users
Kerberos
Login event subscription
User login event
Active Directory



Passive Identity Connector
User still logged in?
User-to IP mappings
pxGrid
Group List
ERS
Probe
WMI
WSA
Domain Users
Kerberos
Login event subscription
User login event
Active Directory

Web proxy

- Specify forward mode if no transparent traffic
- Enable range request header forwarding
  - Global setting makes no changes
  - Allows for use in access policies



Range Request Forwarding:	☑ Enable Range Request Forwarding *When enabled, range requests will be forwarded to the destination server. This can save bandwidth, but may result in reduced efficacy for Application Visibility and Control.* *When range request forwarding is enabled and the Application Visibility and Control service is in use, additional settings related to range request handling for AVC are available in Access Policies (see Web Security Manager > Access Policies > Applications).*

HTTPS Proxy

Invalid Certificates / OCSP

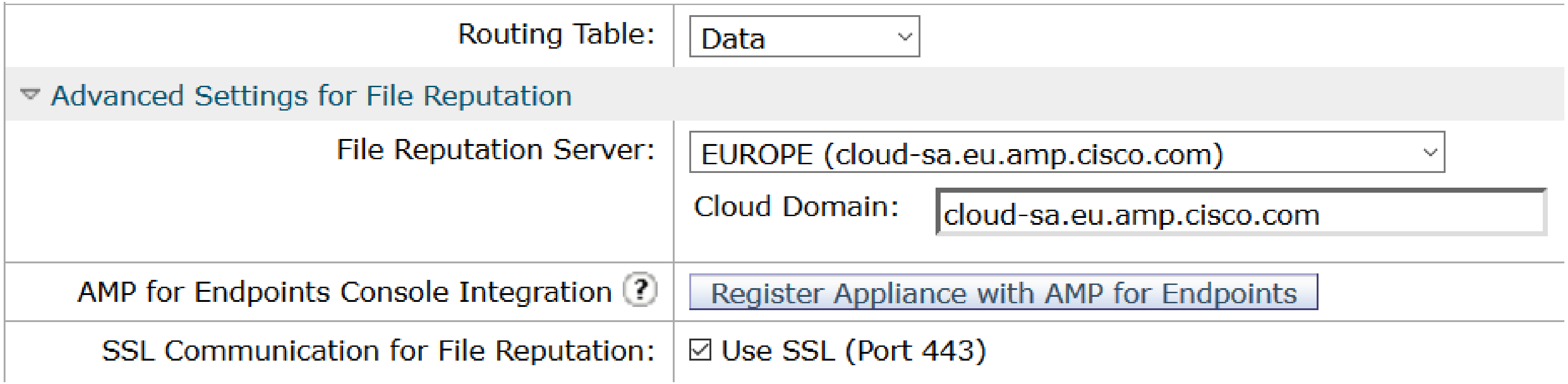
- These settings should be set to at least decrypt and never monitor
- WSA will use AIA chasing by default

Decrypt for EUN / Auth

- Enable these in order to serve an HTML block page even when set to drop
- Reduces helpdesk tickets
- DECRYPT_ADMIN_2 decision tag

AMP dashboard integration

- Additional steps are required to add the WSA to AMP Unity
- Make sure the correct region is selected
- Allows for custom whitelists/blacklists and file trajectory info

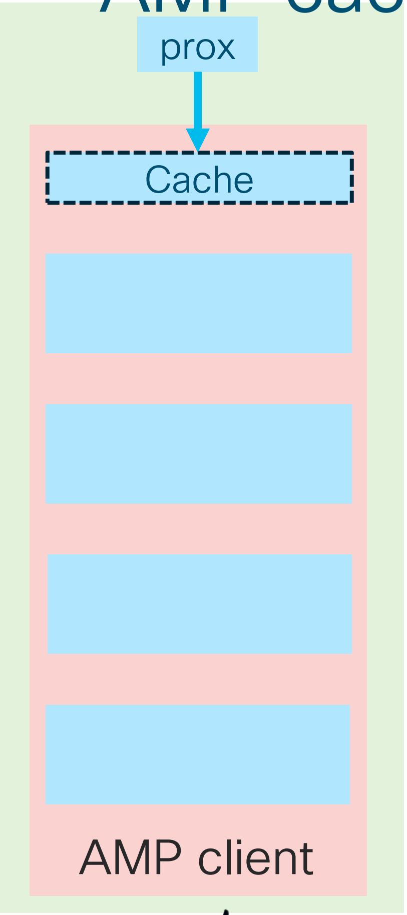


Routing Table:	Data
▿ Advanced Settings for File Reputation	
File Reputation Server:	EUROPE (cloud-sa.eu.amp.cisco.com) Cloud Domain: cloud-sa.eu.amp.cisco.com
AMP for Endpoints Console Integration ?	Register Appliance with AMP for Endpoints
SSL Communication for File Reputation:	☑ Use SSL (Port 443)

AMP client processes

prox
AMP client
Reputation
Classification
File analysis

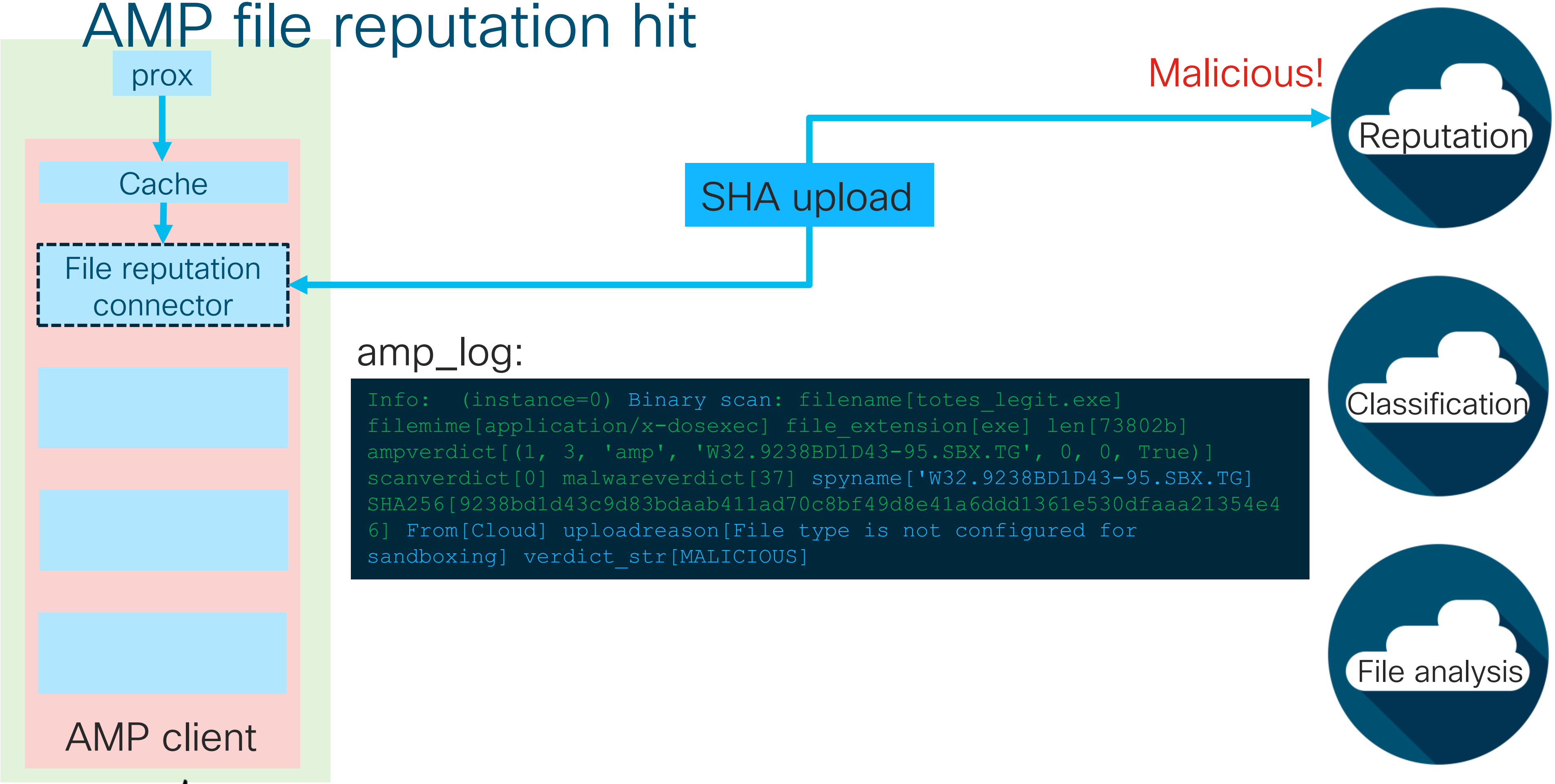
AMP cache hit



amp_log:

```
Info:  (instance=0) Binary scan: filename[totes_legit.exe]
filemime[application/x-dosexec] file_extension[exe] len[73802b]
ampverdict[(2, 3, 'amp', 'W32.9238BD1D43-95.SBX.TG', 0, 95, False)]
scanverdict[0] malwareverdict[37] spyname[W32.9238BD1D43-95.SBX.TG]
SHA256[9238bd1d43c9d83bdaab411ad70c8bf49d8e41a6ddd1361e530dfaaa21354e4
6] From[Cache] uploadreason[File reputation upload action is dont
send] verdict_str[MALICIOUS]
```

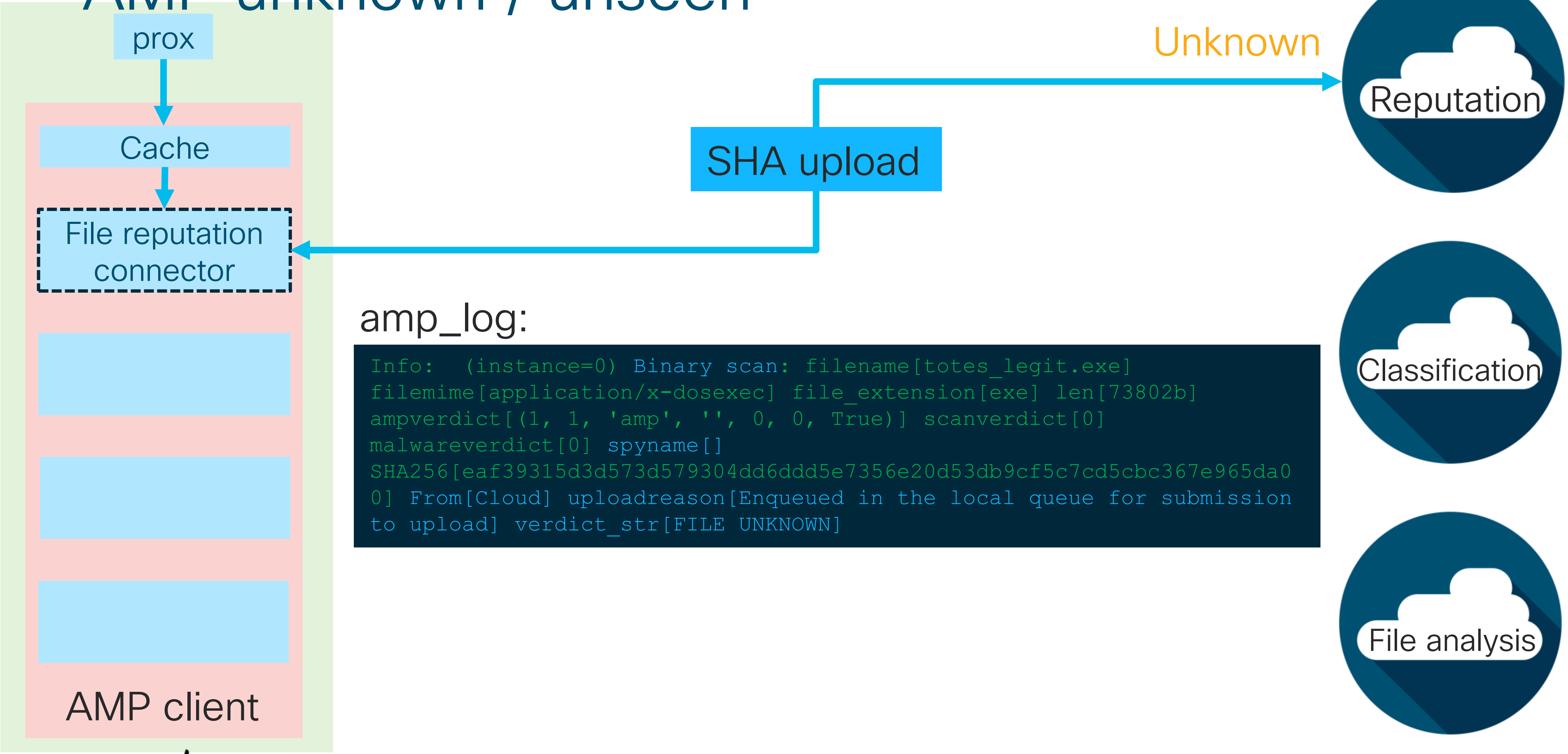
AMP file reputation hit



amp_log:

```
Info:  (instance=0) Binary scan: filename[totes_legit.exe]
filemime[application/x-dosexec] file_extension[exe] len[73802b]
ampverdict[(1, 3, 'amp', 'W32.9238BD1D43-95.SBX.TG', 0, 0, True)]
scanverdict[0] malwareverdict[37] spyname['W32.9238BD1D43-95.SBX.TG]
SHA256[9238bd1d43c9d83bdaab411ad70c8bf49d8e41a6ddd1361e530dfaaa21354e4
6] From[Cloud] uploadreason[File type is not configured for
sandboxing] verdict_str[MALICIOUS]
```

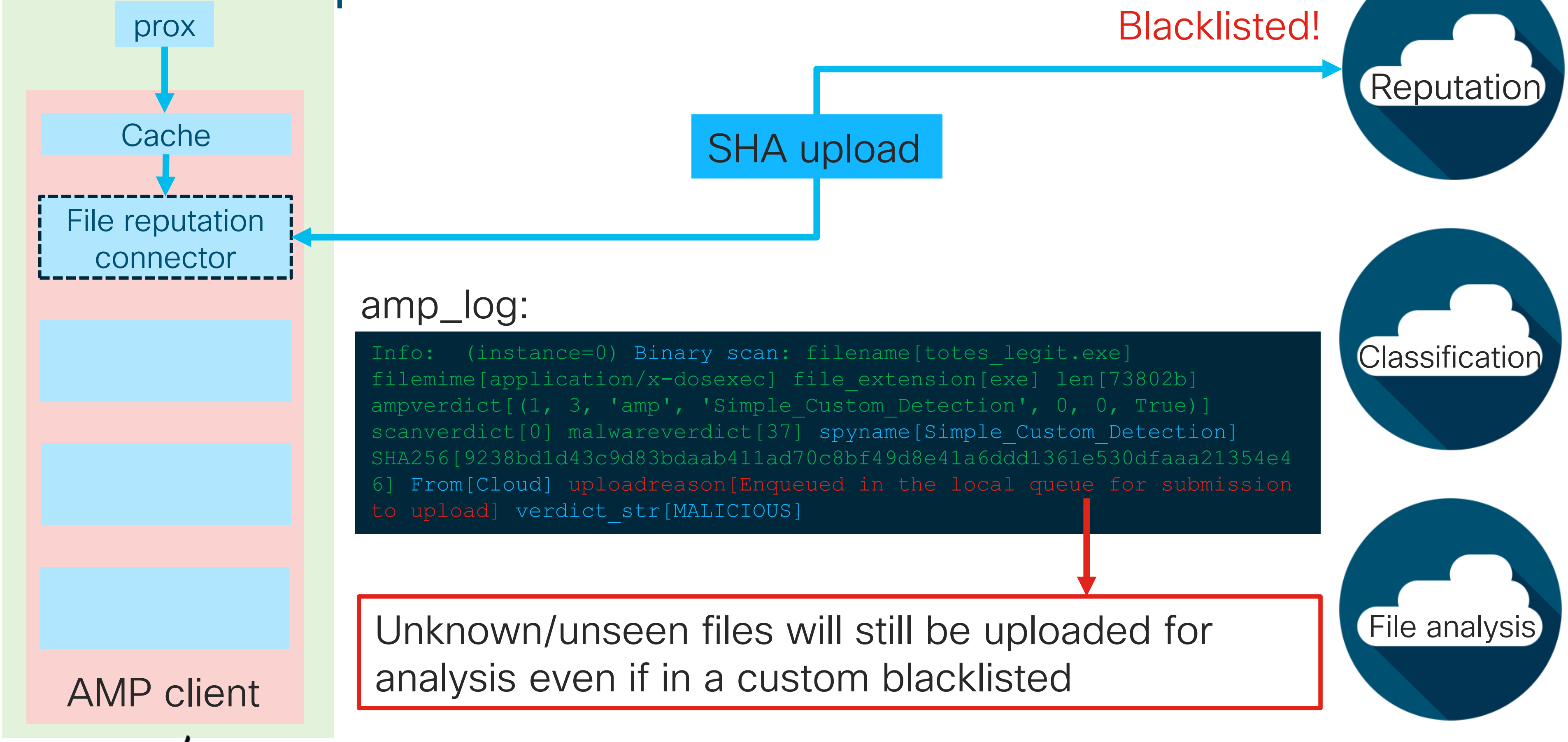
AMP unknown / unseen



amp_log:

```
Info:  (instance=0) Binary scan: filename[totes_legit.exe]
filemime[application/x-dosexec] file_extension[exe] len[73802b]
ampverdict[(1, 1, 'amp', '', 0, 0, True)] scanverdict[0]
malwareverdict[0] spyname[]
SHA256[eaf39315d3d573d579304dd6ddd5e7356e20d53db9cf5c7cd5cbc367e965da0
0] From[Cloud] uploadreason[Enqueued in the local queue for submission
to upload] verdict_str[FILE UNKNOWN]
```

AMP simple blacklist hit

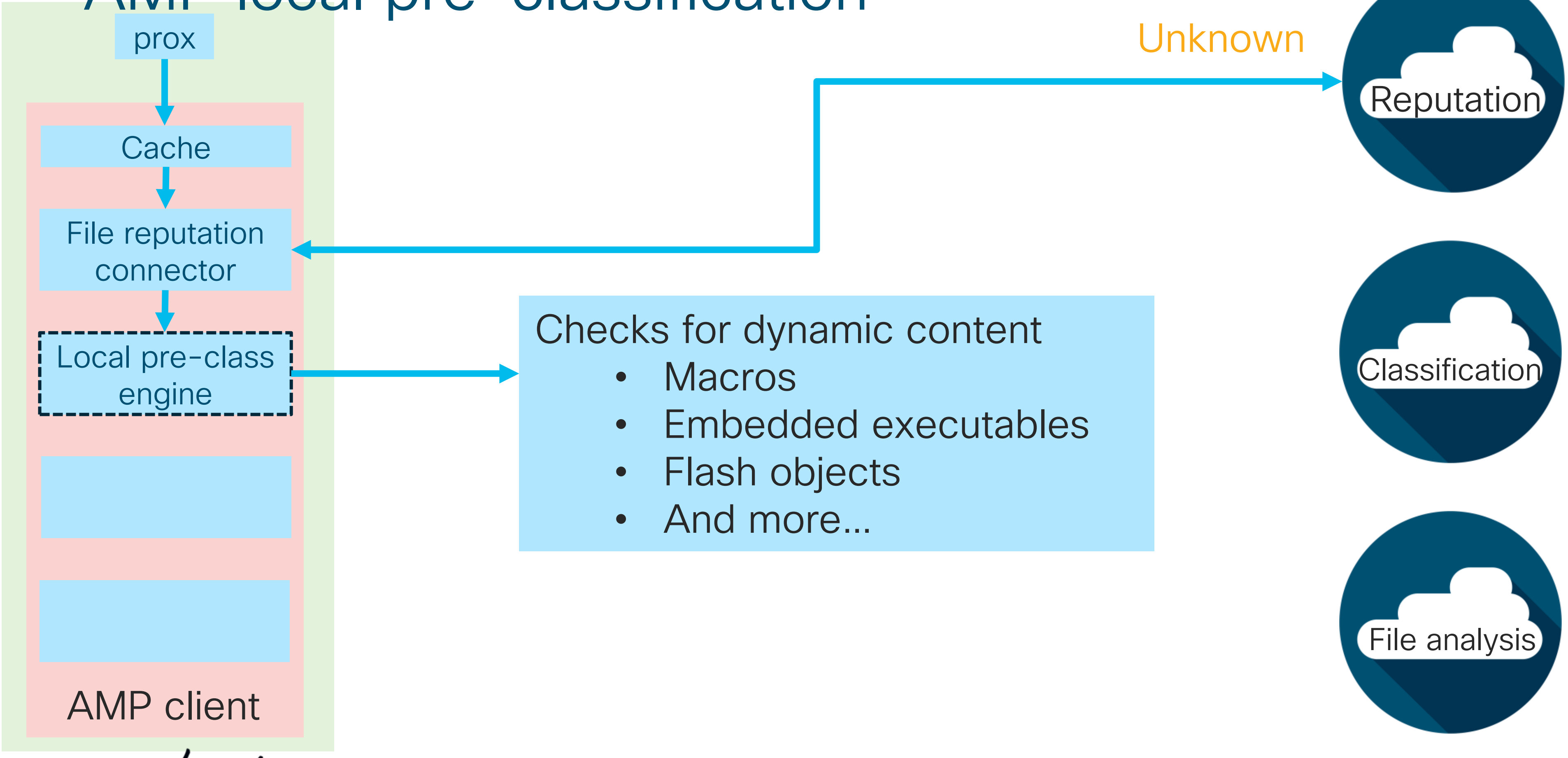


amp_log:

```
Info:  (instance=0) Binary scan: filename[totes_legit.exe]
filemime[application/x-dosexec] file_extension[exe] len[73802b]
ampverdict[(1, 3, 'amp', 'Simple_Custom_Detection', 0, 0, True)]
scanverdict[0] malwareverdict[37] spyname[Simple_Custom_Detection]
SHA256[9238bd1d43c9d83bdaab411ad70c8bf49d8e41a6ddd1361e530dfaaa21354e4
6] From[Cloud] uploadreason[Enqueued in the local queue for submission
to upload] verdict_str[MALICIOUS]
```

Unknown/unseen files will still be uploaded for analysis even if in a custom blacklisted

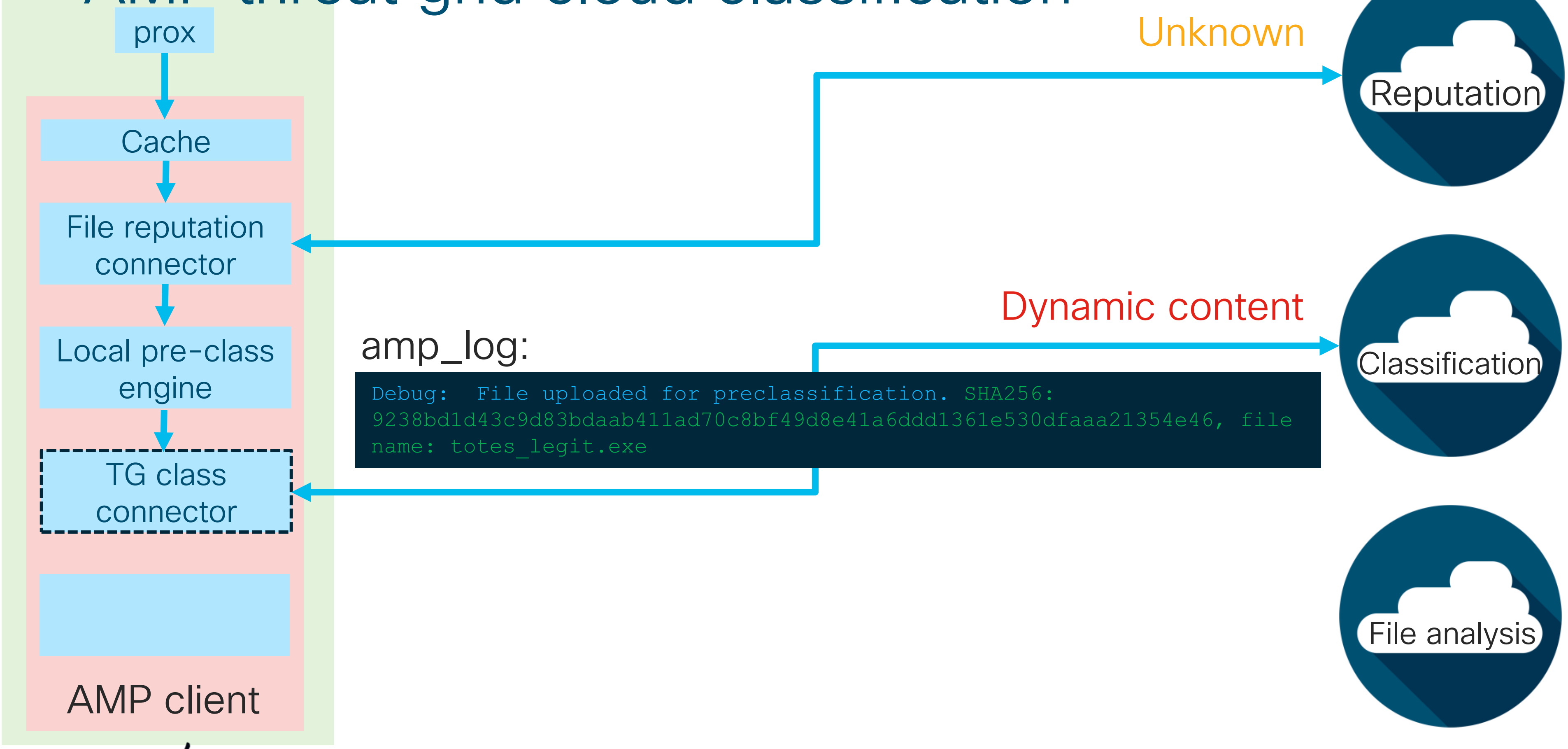
AMP local pre-classification



Checks for dynamic content

- Macros
- Embedded executables
- Flash objects
- And more…

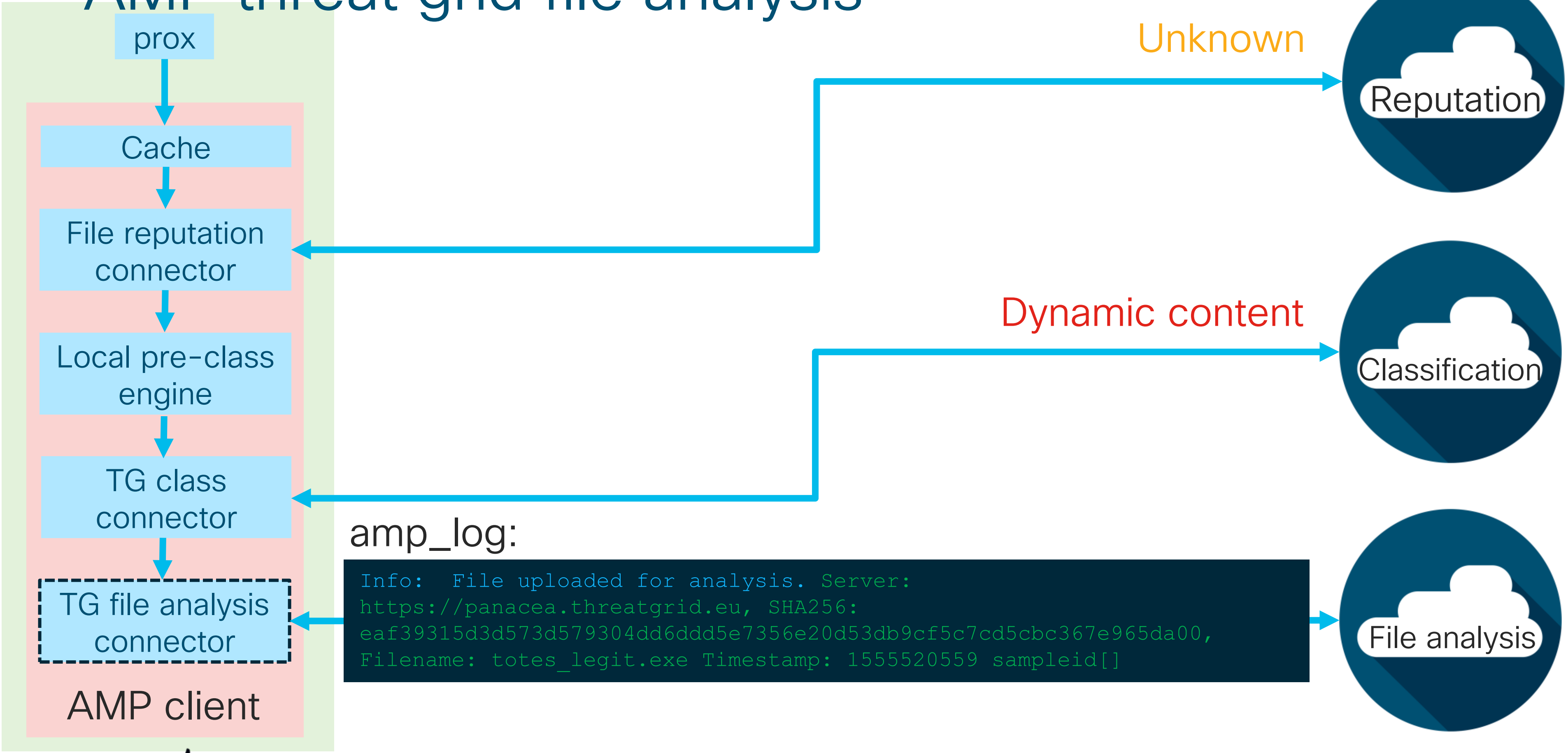
AMP threat grid cloud classification



amp_log:

```
Debug:  File uploaded for preclassification. SHA256:
9238bd1d43c9d83bdaab411ad70c8bf49d8e41a6ddd1361e530dfaaa21354e46, file
name: totes_legit.exe
```

AMP threat grid file analysis

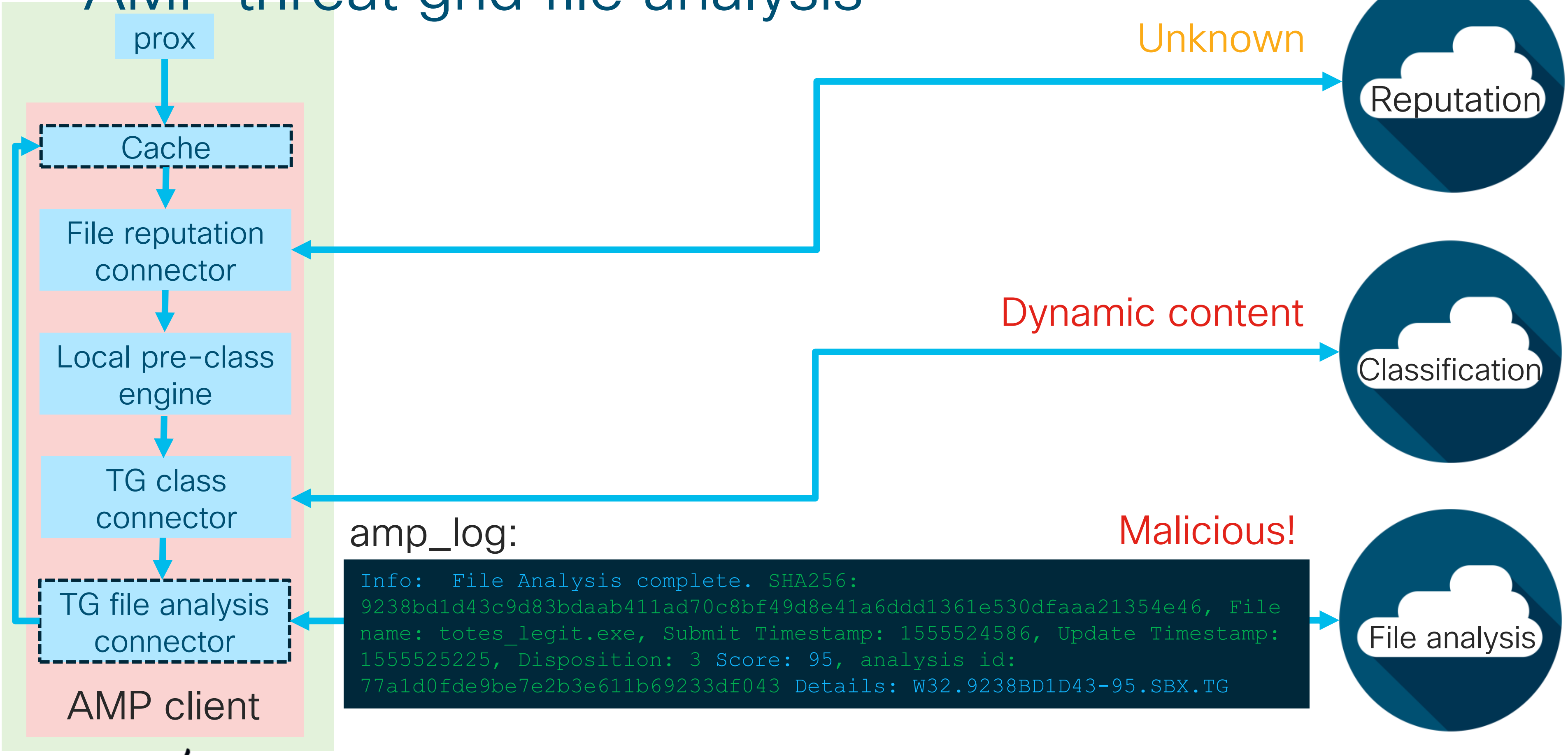


amp_log:

```
Info:  File uploaded for analysis. Server:
https://panacea.threatgrid.eu, SHA256:
eaf39315d3d573d579304dd6ddd5e7356e20d53db9cf5c7cd5cbc367e965da00,
Filename: totes_legit.exe Timestamp: 1555520559 sampleid[]
```

cisco Live!

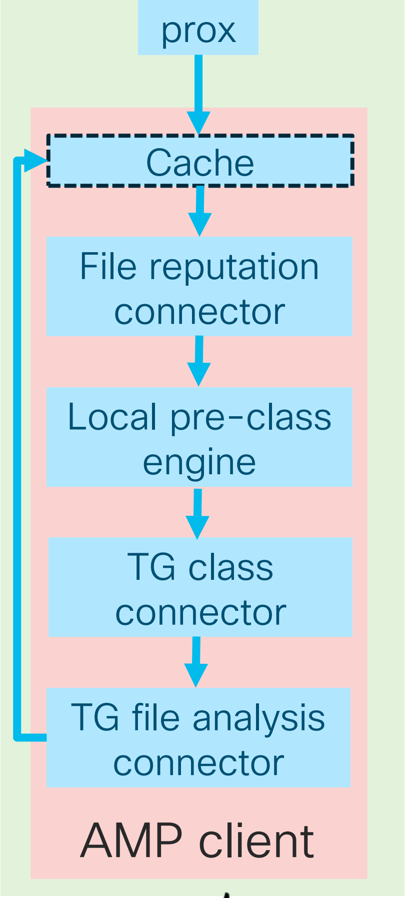
AMP threat grid file analysis



amp_log:

```
Info:  File Analysis complete. SHA256:
9238bd1d43c9d83bdaab411ad70c8bf49d8e41a6ddd1361e530dfaaa21354e46, File
name: totes_legit.exe, Submit Timestamp: 1555524586, Update Timestamp:
1555525225, Disposition: 3 Score: 95, analysis id:
77a1d0fde9be7e2b3e611b69233df043 Details: W32.9238BD1D43-95.SBX.TG
```

AMP cache hit



amp_log:

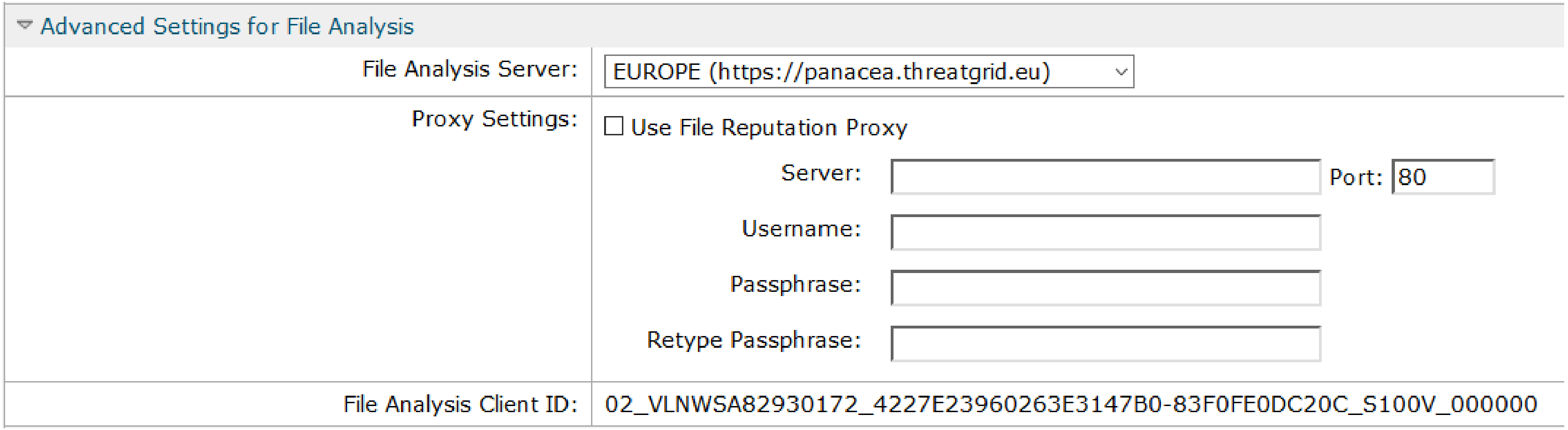
```
Info:  (instance=0) Binary scan: filename[totes_legit.exe]
filemime[application/x-dosexec] file_extension[exe] len[73802b]
ampverdict[(2, 3, 'amp', 'W32.9238BD1D43-95.SBX.TG', 0, 95, False)]
scanverdict[0] malwareverdict[37] spyname[W32.9238BD1D43-95.SBX.TG]
SHA256[9238bd1d43c9d83bdaab411ad70c8bf49d8e41a6ddd1361e530dfaaa21354e4
6] From[Cache] uploadreason[File reputation upload action is dont
send] verdict_str[MALICIOUS]
```

Threat grid information overwrites custom blacklist information in the cache

Reputation
Classification
File analysis

Threat Grid integration

- Submission is free with an AMP license (limited to 200 per day)
- Premium license is required for cloud portal access
- Add your WSA File Analysis ID to see sandbox information
  - Requires a TAC case



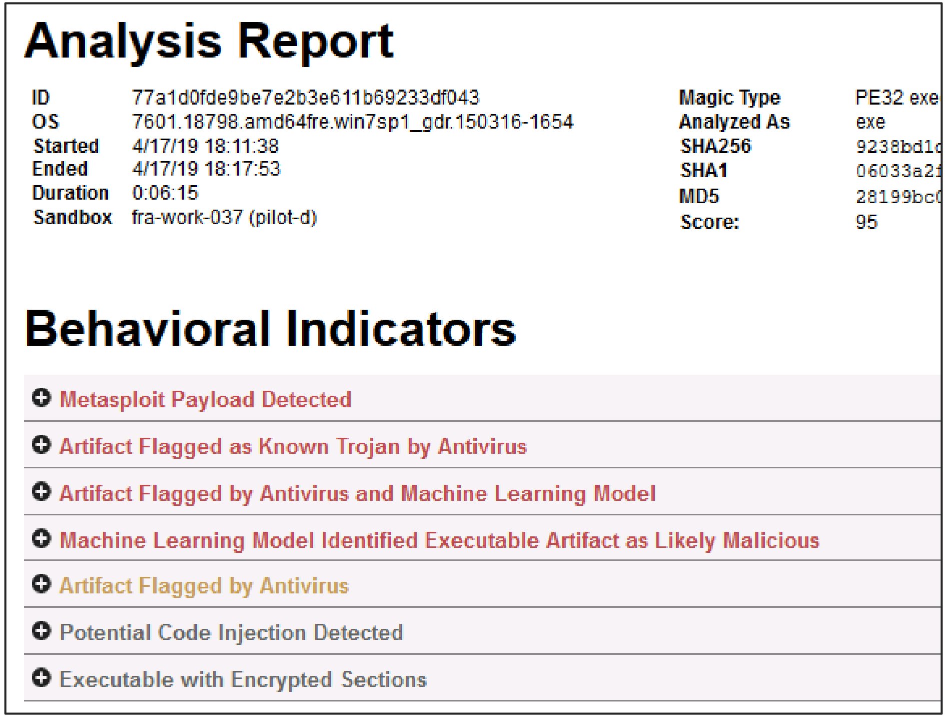
Advanced Settings for File Analysis

File Analysis Server:	EUROPE (https://panacea.threatgrid.eu)
Proxy Settings:	□ Use File Reputation Proxy Server: Port: 80 Username: Passphrase: Retype Passphrase:
File Analysis Client ID:	02_VLNWSA82930172_4227E23960263E3147B0-83F0FE0DC20C_S100V_000000

Threat Grid integration

What do I get without TG cloud access?

- General information
- Basic behavioral indicators
- Static file info (hashes)
- Link to TG information



Analysis Report

ID	77a1d0fde9be7e2b3e611b69233df043	Magic Type	PE32 exe
OS	7601.18798.amd64fre.win7sp1_gdr.150316-1654	Analyzed As	exe
Started	4/17/19 18:11:38	SHA256	9238bd1
Ended	4/17/19 18:17:53	SHA1	06033a2
Duration	0:06:15	MD5	28199bc
Sandbox	fra-work-037 (pilot-d)	Score:	95

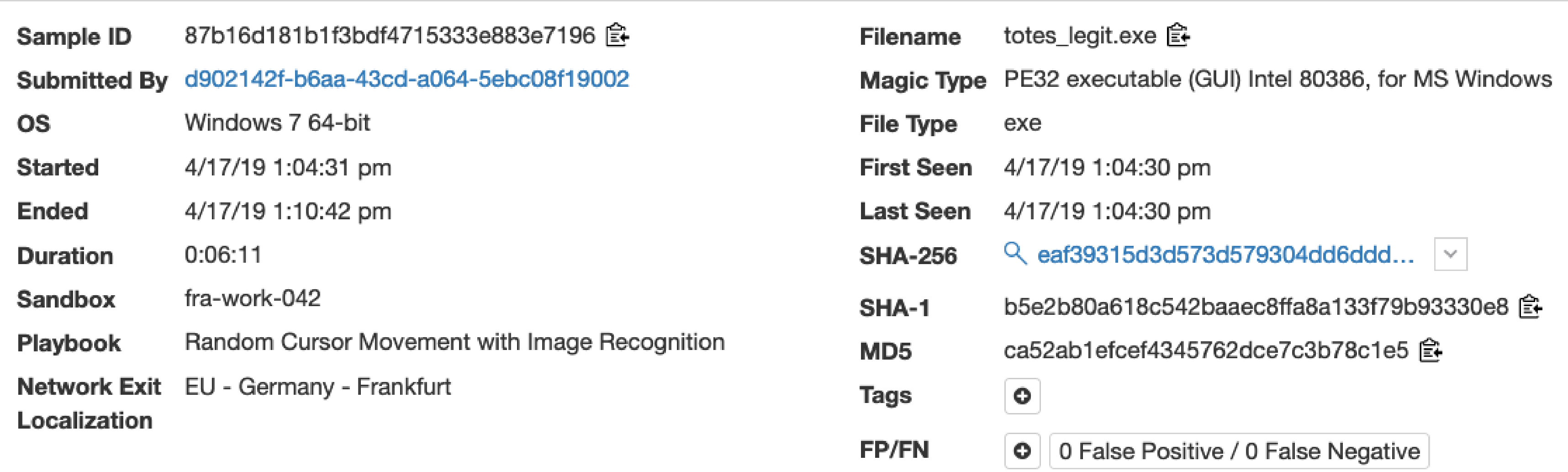
Behavioral Indicators

- Metasploit Payload Detected
- Artifact Flagged as Known Trojan by Antivirus
- Artifact Flagged by Antivirus and Machine Learning Model
- Machine Learning Model Identified Executable Artifact as Likely Malicious
- Artifact Flagged by Antivirus
- Potential Code Injection Detected
- Executable with Encrypted Sections

Threat grid integration

What do I get with TG cloud access?

- File metadata

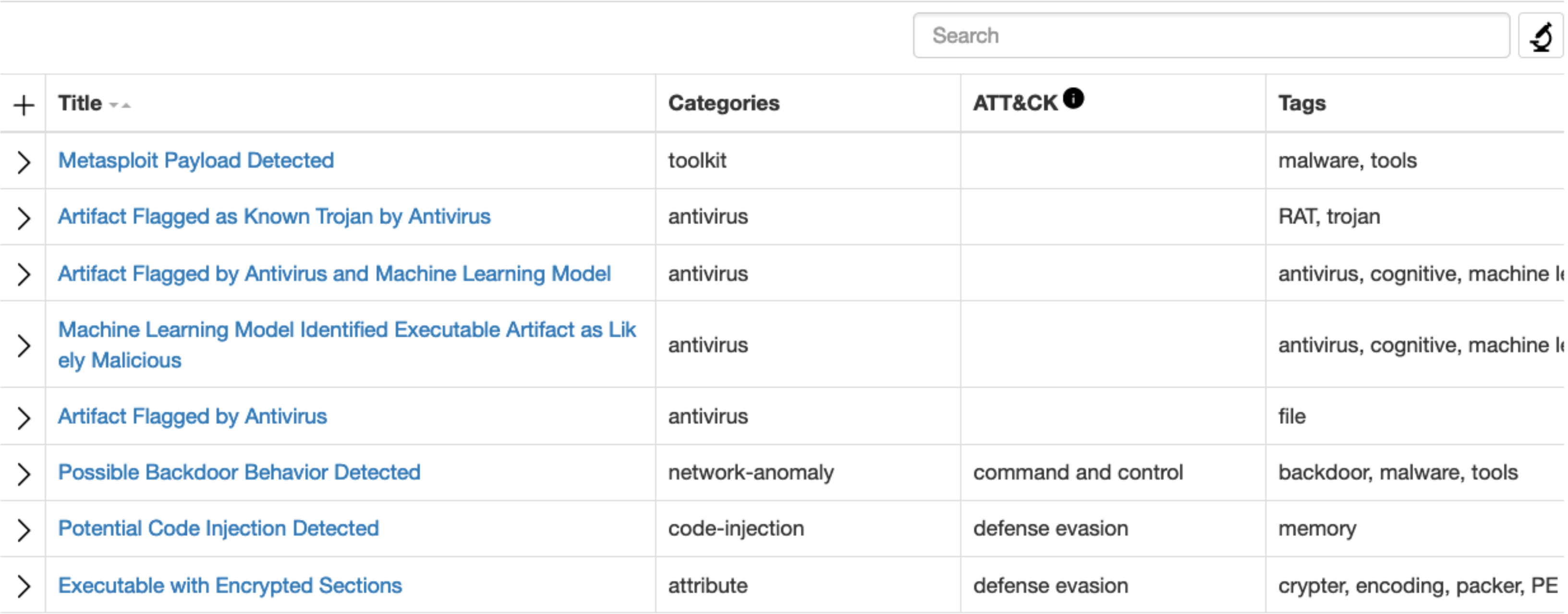


Sample ID	87b16d181b1f3bdf4715333e883e7196	**Filename**	totes_legit.exe
Submitted By	d902142f-b6aa-43cd-a064-5ebc08f19002	**Magic Type**	PE32 executable (GUI) Intel 80386, for MS Windows
OS	Windows 7 64-bit	**File Type**	exe
Started	4/17/19 1:04:31 pm	**First Seen**	4/17/19 1:04:30 pm
Ended	4/17/19 1:10:42 pm	**Last Seen**	4/17/19 1:04:30 pm
Duration	0:06:11	**SHA-256**	eaf39315d3d573d579304dd6ddd...
Sandbox	fra-work-042	**SHA-1**	b5e2b80a618c542baaec8ffa8a133f79b93330e8
Playbook	Random Cursor Movement with Image Recognition	**MD5**	ca52ab1efcef4345762dce7c3b78c1e5
Network Exit Localization	EU - Germany - Frankfurt	**Tags**	⊕
		FP/FN	⊕ 0 False Positive / 0 False Negative

Threat grid integration

What do I get with TG cloud access?

- Detailed behavioral indicators

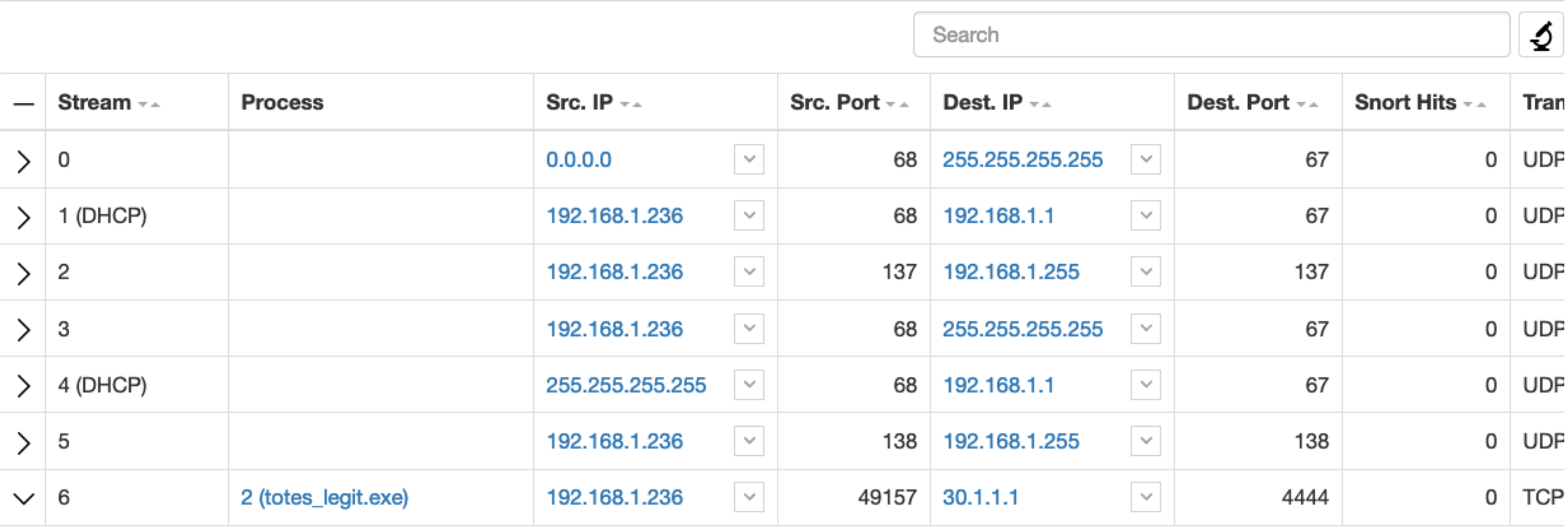


+	Title	Categories	ATT&CK	Tags
>	Metasploit Payload Detected	toolkit		malware, tools
>	Artifact Flagged as Known Trojan by Antivirus	antivirus		RAT, trojan
>	Artifact Flagged by Antivirus and Machine Learning Model	antivirus		antivirus, cognitive, machine l
>	Machine Learning Model Identified Executable Artifact as Likely Malicious	antivirus		antivirus, cognitive, machine l
>	Artifact Flagged by Antivirus	antivirus		file
>	Possible Backdoor Behavior Detected	network-anomaly	command and control	backdoor, malware, tools
>	Potential Code Injection Detected	code-injection	defense evasion	memory
>	Executable with Encrypted Sections	attribute	defense evasion	crypter, encoding, packer, PE

Threat grid integration

What do I get with TG cloud access?

- TCP/IP stream information



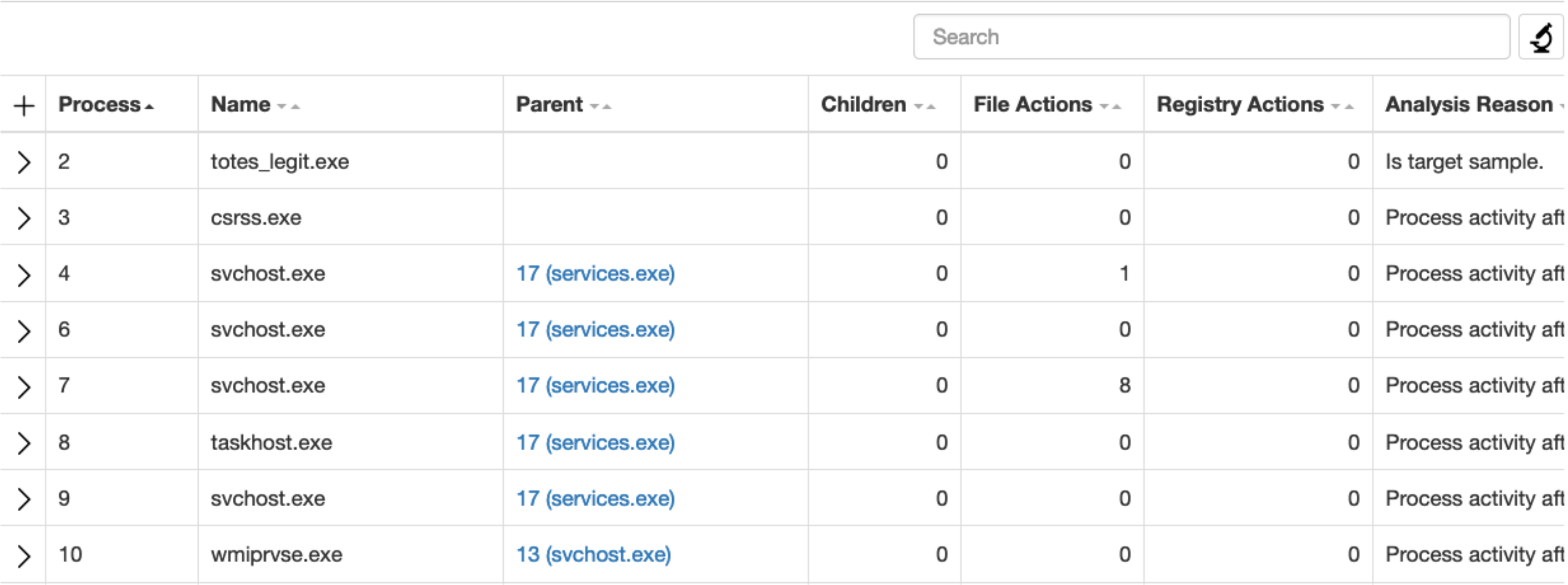
Search

—	Stream	Process	Src. IP	Src. Port	Dest. IP	Dest. Port	Snort Hits	Tran
>	0		0.0.0.0	68	255.255.255.255	67	0	UDF
>	1 (DHCP)		192.168.1.236	68	192.168.1.1	67	0	UDF
>	2		192.168.1.236	137	192.168.1.255	137	0	UDF
>	3		192.168.1.236	68	255.255.255.255	67	0	UDF
>	4 (DHCP)		255.255.255.255	68	192.168.1.1	67	0	UDF
>	5		192.168.1.236	138	192.168.1.255	138	0	UDF
∨	6	2 (totes_legit.exe)	192.168.1.236	49157	30.1.1.1	4444	0	TCP

Threat grid integration

What do I get with TG cloud access?

- Process information

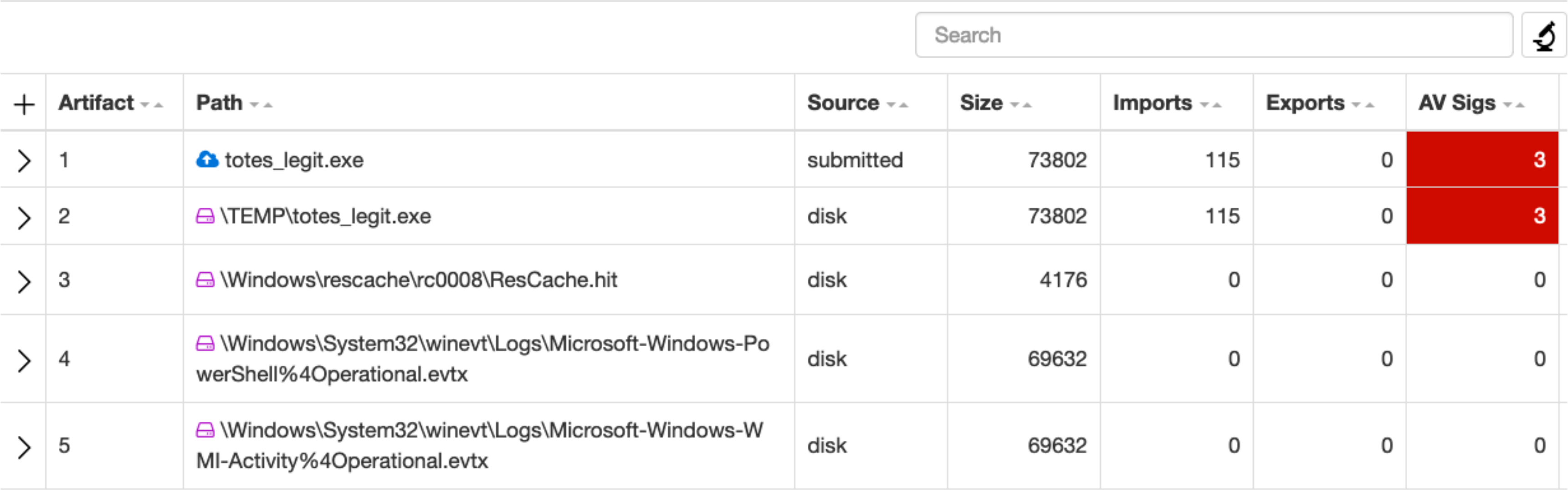


+	Process	Name	Parent	Children	File Actions	Registry Actions	Analysis Reason
>	2	totes_legit.exe		0	0	0	Is target sample.
>	3	csrss.exe		0	0	0	Process activity aft
>	4	svchost.exe	17 (services.exe)	0	1	0	Process activity aft
>	6	svchost.exe	17 (services.exe)	0	0	0	Process activity aft
>	7	svchost.exe	17 (services.exe)	0	8	0	Process activity aft
>	8	taskhost.exe	17 (services.exe)	0	0	0	Process activity aft
>	9	svchost.exe	17 (services.exe)	0	0	0	Process activity aft
>	10	wmiprvse.exe	13 (svchost.exe)	0	0	0	Process activity aft

Threat grid integration

What do I get with TG cloud access?

- Artifact information

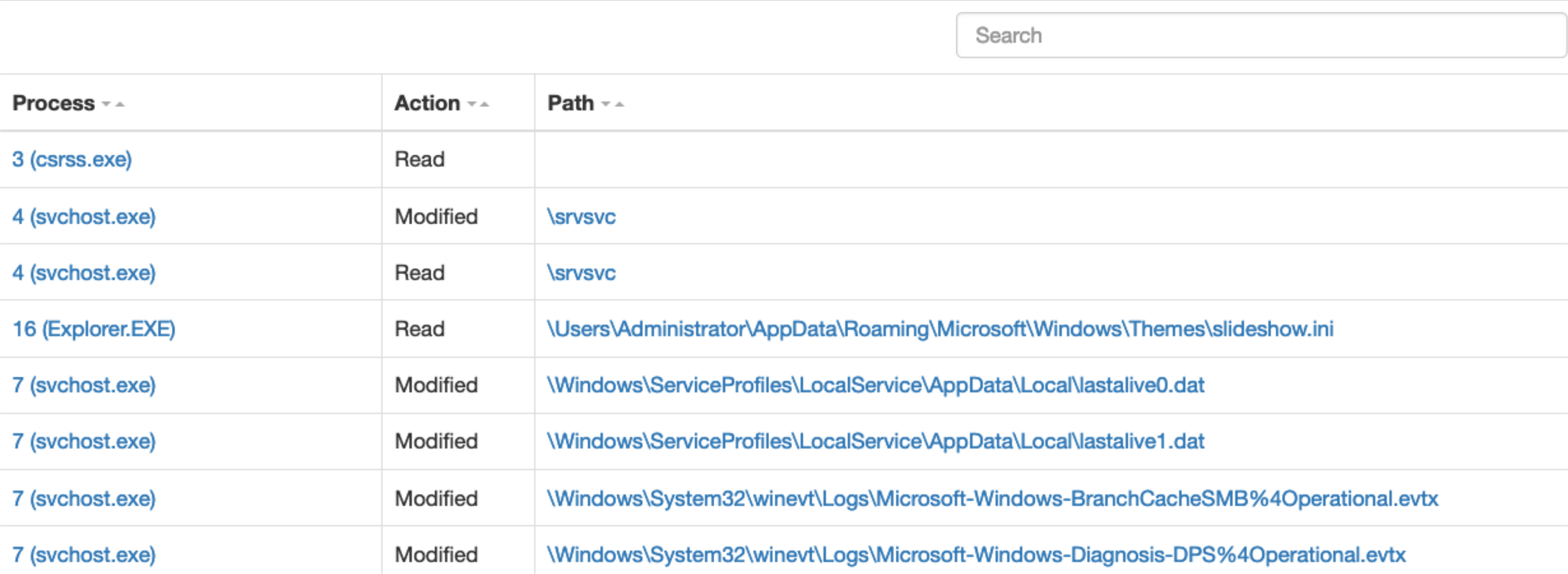


+	Artifact	Path	Source	Size	Imports	Exports	AV Sigs
>	1	totes_legit.exe	submitted	73802	115	0	3
>	2	\TEMP\totes_legit.exe	disk	73802	115	0	3
>	3	\Windows\rescache\rc0008\ResCache.hit	disk	4176	0	0	0
>	4	\Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx	disk	69632	0	0	0
>	5	\Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4Operational.evtx	disk	69632	0	0	0

Threat grid integration

What do I get with TG cloud access?

- File system information

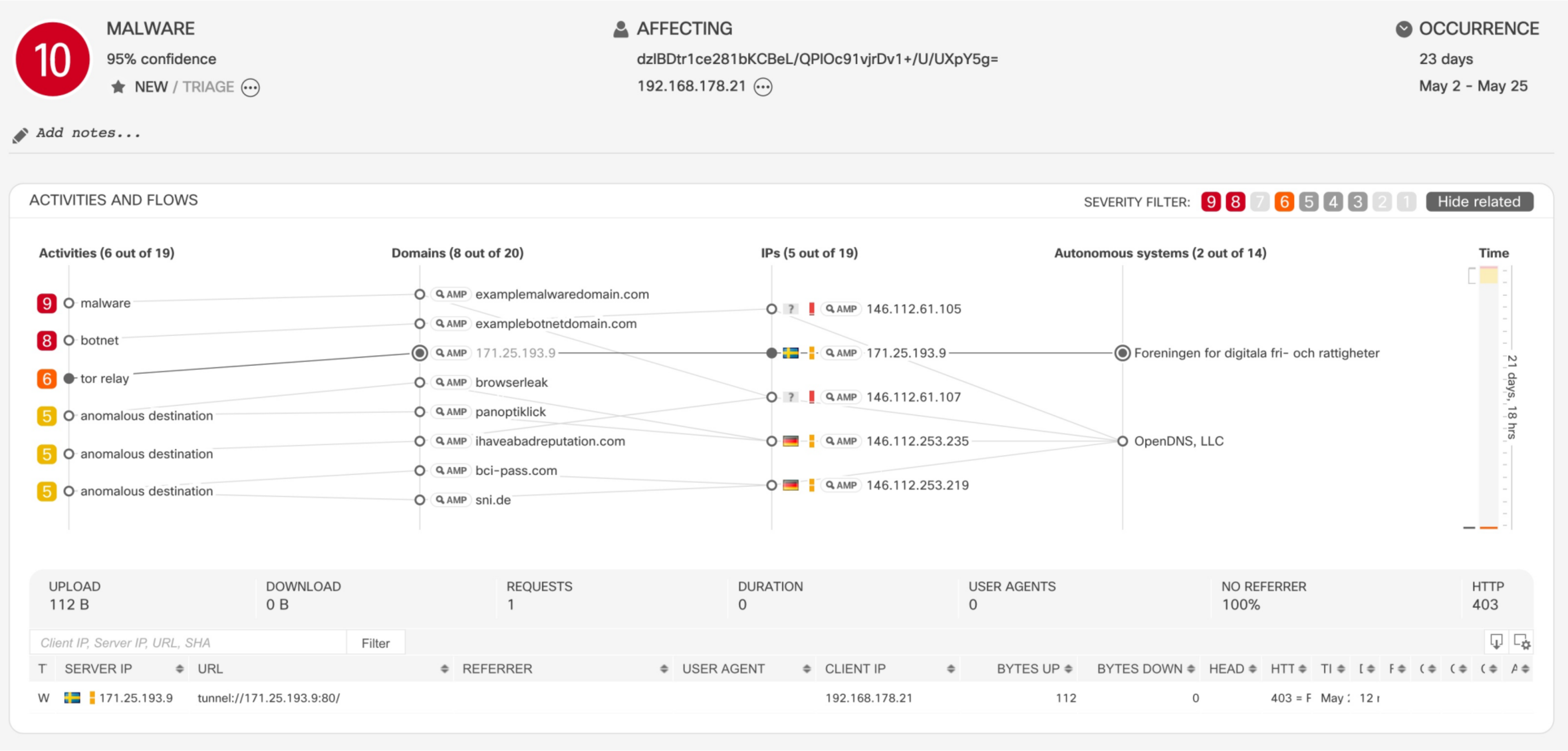


Process	Action	Path
3 (csrss.exe)	Read	
4 (svchost.exe)	Modified	\srvsvc
4 (svchost.exe)	Read	\srvsvc
16 (Explorer.EXE)	Read	\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\slideshow.ini
7 (svchost.exe)	Modified	\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat
7 (svchost.exe)	Modified	\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat
7 (svchost.exe)	Modified	\Windows\System32\winevt\Logs\Microsoft-Windows-BranchCacheSMB%4Operational.evtx
7 (svchost.exe)	Modified	\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4Operational.evtx

Cognitive Threat Analytics

- Uses the WSA as a sensor
- Establishes a baseline of traffic behavior
- Especially good at finding C&C and TOR relay traffic
- Continuously updated

- Can be connected to your AMP dashboard
- Suspicious activity is pushed from CTA to the AMP dashboard for investigation



10 MALWARE

95% confidence

★ NEW / TRIAGE

AFFECTING

dzIBDtr1ce281bKCBeL/QPlOc91vjrDv1+/U/UXpY5g=

192.168.178.21

OCCURRENCE

23 days

May 2 – May 25

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1 Hide related

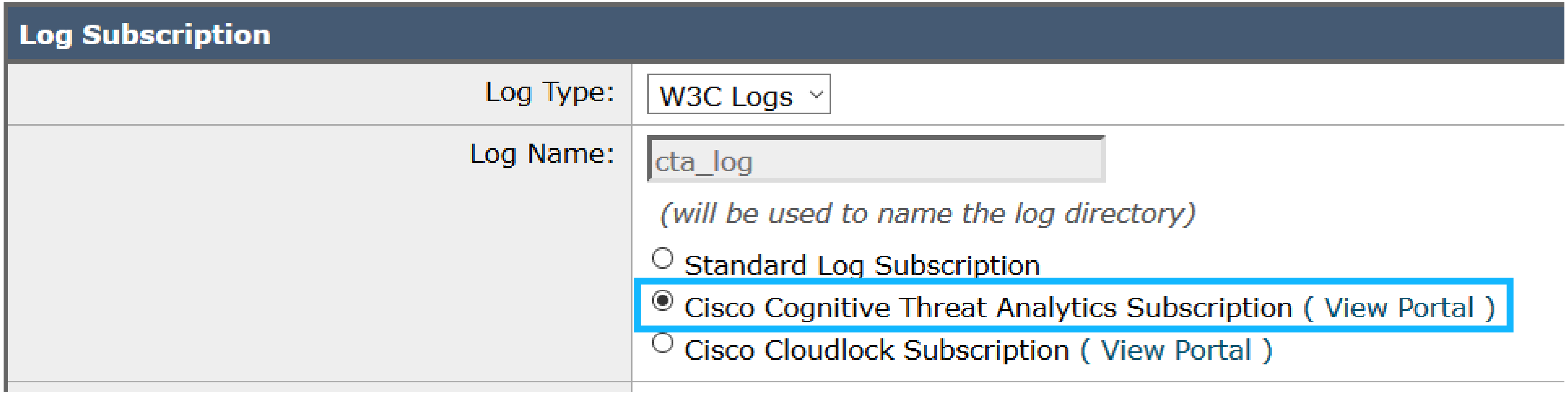
UPLOAD	DOWNLOAD	REQUESTS	DURATION	USER AGENTS	NO REFERRER	HTTP
112 B	0 B	1	0	0	100%	403

Client IP, Server IP, URL, SHA Filter

T	SERVER IP	URL	REFERRER	USER AGENT	CLIENT IP	BYTES UP	BYTES DOWN	HEAD	HTT	TI	[	F	(	(	(	A
W	171.25.193.9	tunnel://171.25.193.9:80/			192.168.178.21	112	0		403 = F	May :	12 r					

Cognitive Threat Analytics

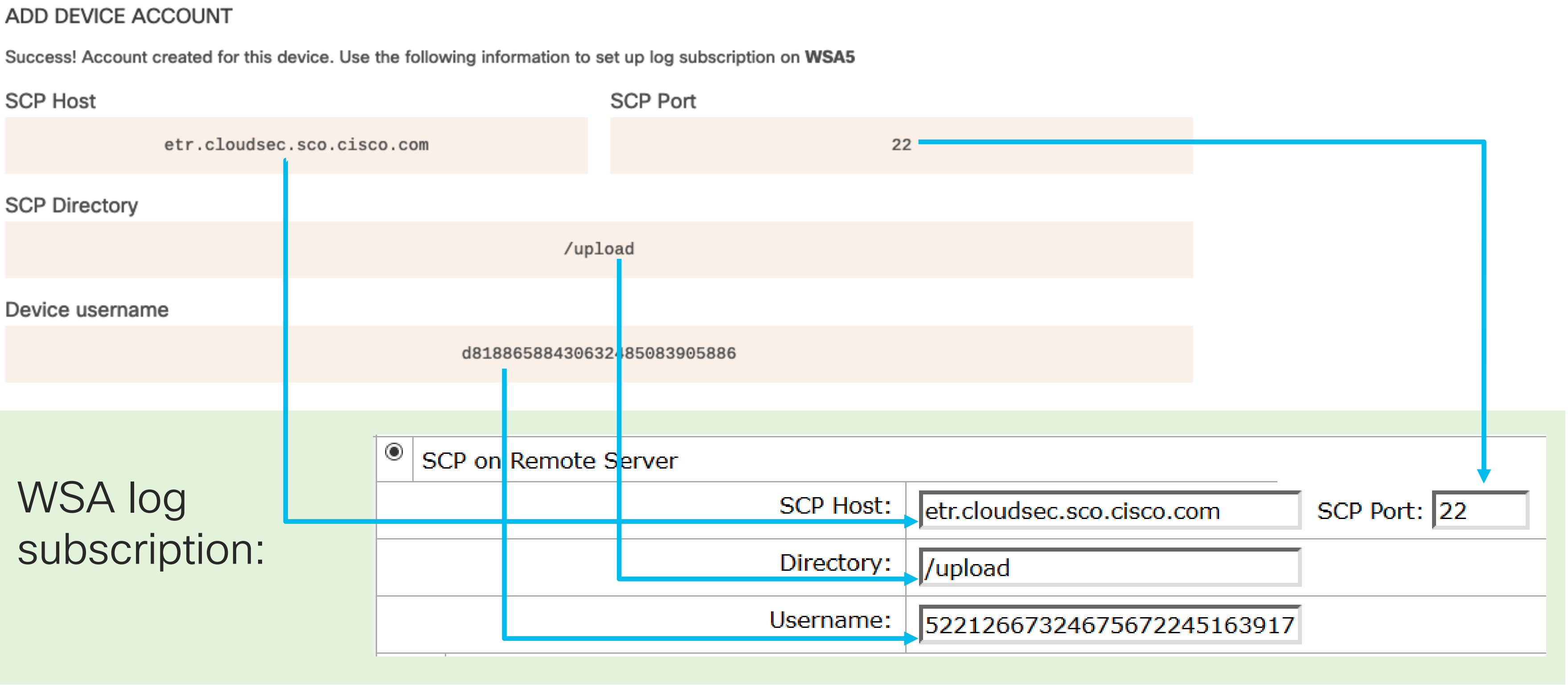
- Added as a W3C log subscription
- All appropriate fields are pre-filled



Log Subscription

Log Type:	W3C Logs
Log Name:	cta_log *(will be used to name the log directory)* ○ Standard Log Subscription ● Cisco Cognitive Threat Analytics Subscription (View Portal) ○ Cisco Cloudlock Subscription (View Portal)

Cognitive Threat Analytics



ADD DEVICE ACCOUNT

Success! Account created for this device. Use the following information to set up log subscription on **WSA5**

SCP Host: etr.cloudsec.sco.cisco.com

SCP Port: 22

SCP Directory: /upload

Device username: d81886588430632485083905886

WSA log subscription:

● SCP on Remote Server

SCP Host: etr.cloudsec.sco.cisco.com

SCP Port: 22

Directory: /upload

Username: 52212667324675672245163917

Policy Configuration

Policy configuration

- Configured in Web Security Manager
- We will focus on
  - Identification profiles
  - Decryption policies
  - Access policies
  - Custom and external categories

How you configure these policies has an effect on performance and stability!

- Slow GUI and CLI at best
- Slow request processing at worst

Identification Profiles

- Groups users together by:
  - IP/subnet
  - User-agent
  - Protocol
  - Destination URL
- All criteria must match
- Enforce authentication (or not) against those groups
- Top-down, stops at the first match (ACL logic)

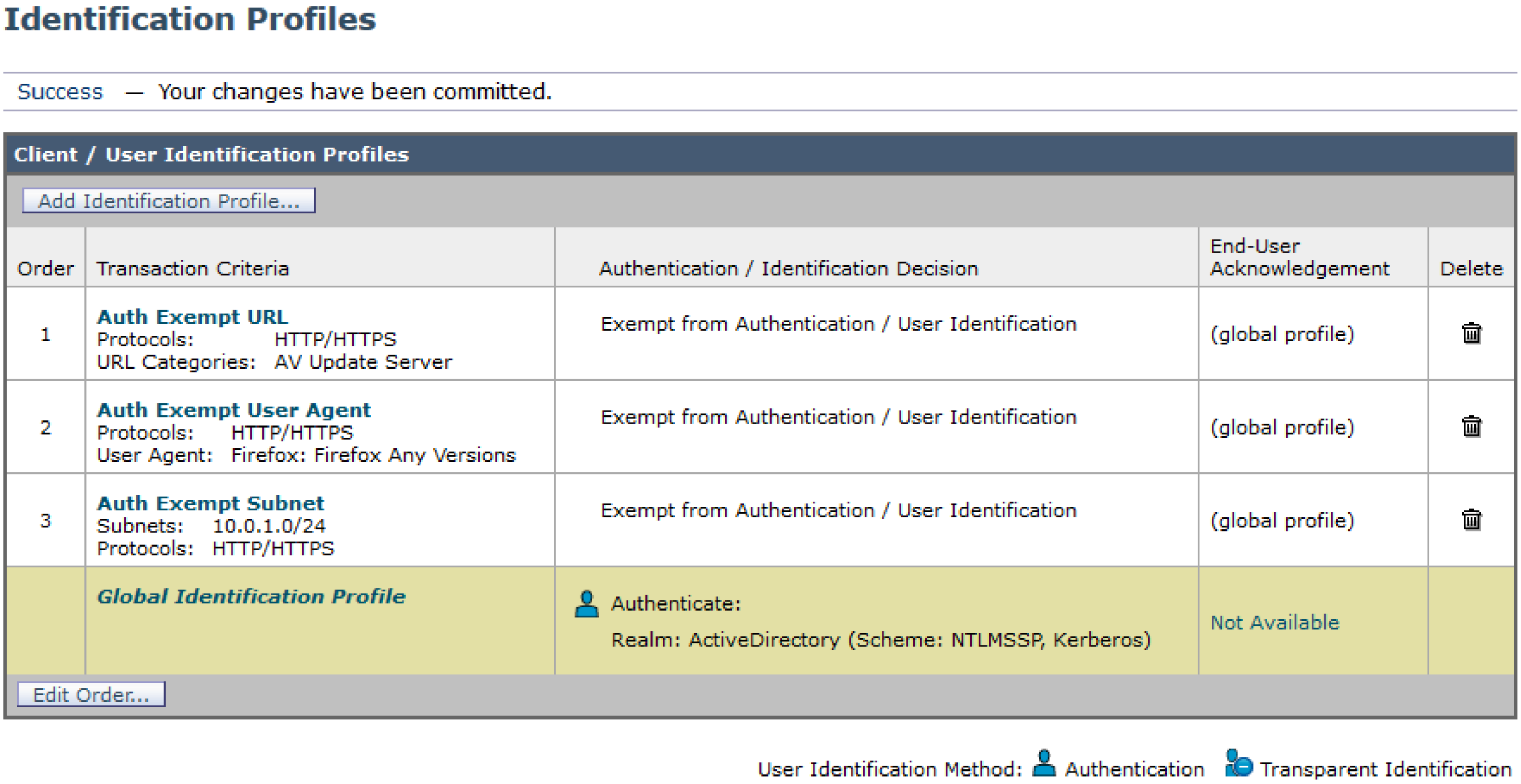
Authentication exceptions

Updater agents

AV agents

Servers

System daemons



Identification Profiles

Success — Your changes have been committed.

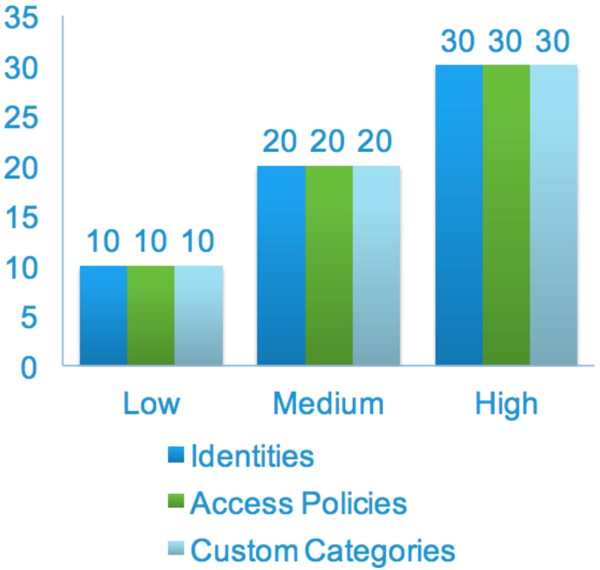
Client / User Identification Profiles

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	**Auth Exempt URL** Protocols: HTTP/HTTPS URL Categories: AV Update Server	Exempt from Authentication / User Identification	(global profile)	🗑
2	**Auth Exempt User Agent** Protocols: HTTP/HTTPS User Agent: Firefox: Firefox Any Versions	Exempt from Authentication / User Identification	(global profile)	🗑
3	**Auth Exempt Subnet** Subnets: 10.0.1.0/24 Protocols: HTTP/HTTPS	Exempt from Authentication / User Identification	(global profile)	🗑
	Global Identification Profile	👤 Authenticate: Realm: ActiveDirectory (Scheme: NTLMSSP, Kerberos)	Not Available	

User Identification Method: 👤 Authentication 👤 Transparent Identification

What is complex?

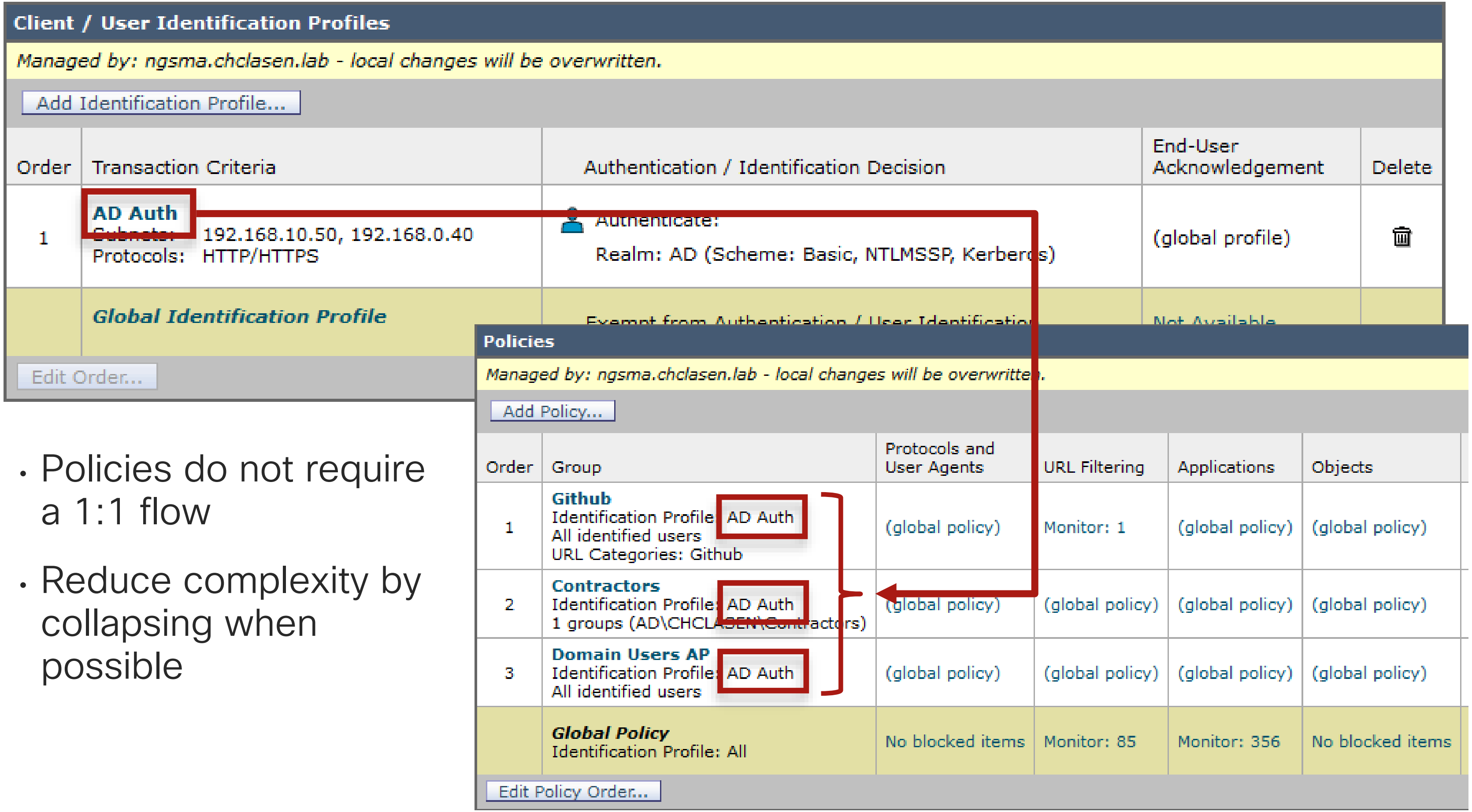
- Low complexity
  - 10 ID profiles
  - 10 Decryption policies
  - 10 Access policies
  - 10 Custom categories
    - 10 regex entries
    - 50 server IP addresses
    - 420 server names



Low Complexity Definition	
10 Access Policies	
10 Identities	
10 Custom Categories	10 Regex
	50 Server IP's
	420 Server Names

Medium Complexity = 2 x Low Complexity

High Complexity = 3 x Low Complexity



Client / User Identification Profiles

Managed by: ngsma.chclasen.lab - local changes will be overwritten.

Add Identification Profile...

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	**AD Auth** Subnets: 192.168.10.50, 192.168.0.40 Protocols: HTTP/HTTPS	Authenticate: Realm: AD (Scheme: Basic, NTLMSSP, Kerberos)	(global profile)	🗑
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

Edit Order...

Policies

Managed by: ngsma.chclasen.lab - local changes will be overwritten.

Add Policy...

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects
1	**Github** Identification Profile: AD Auth All identified users URL Categories: Github	(global policy)	Monitor: 1	(global policy)	(global policy)
2	**Contractors** Identification Profile: AD Auth 1 groups (AD\CHCLASEN\Contractors)	(global policy)	(global policy)	(global policy)	(global policy)
3	**Domain Users AP** Identification Profile: AD Auth All identified users	(global policy)	(global policy)	(global policy)	(global policy)
	Global Policy Identification Profile: All	No blocked items	Monitor: 85	Monitor: 356	No blocked items

Edit Policy Order...

- Policies do not require a 1:1 flow
- Reduce complexity by collapsing when possible

HTTPS policy operations

- Drop
  - Connection is closed
- Decrypt
  - Traffic is decrypted and evaluated by access policies
- Passthrough
  - Transaction is not decrypted
  - Client negotiates directly with server
- Monitor
  - No action is taken; move to the next column

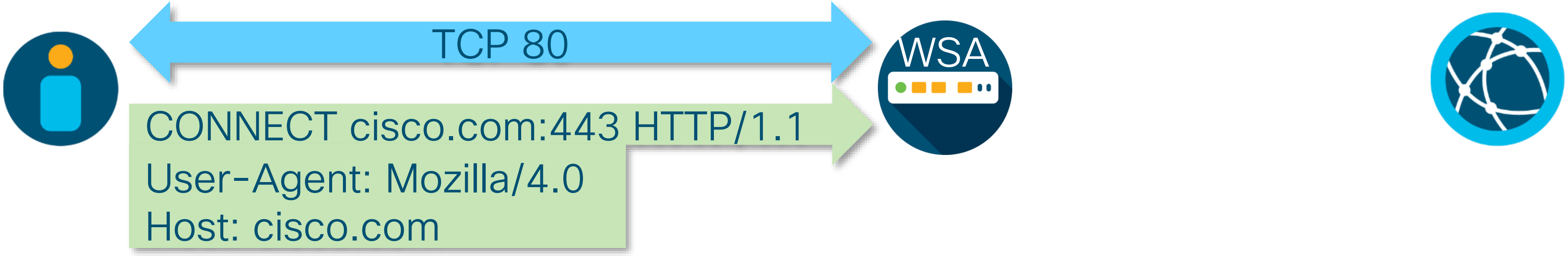
HTTPS traffic is special

- Explicit mode
  - The client asks for a tunnel using the CONNECT HTTP method
  - Host and User-agent headers are visible
- Transparent mode
  - Client expects a TLS negotiation before speaking HTTP
  - No headers are visible
  - We must decide to decrypt before decrypting (duh..)

How do we make policy decisions?

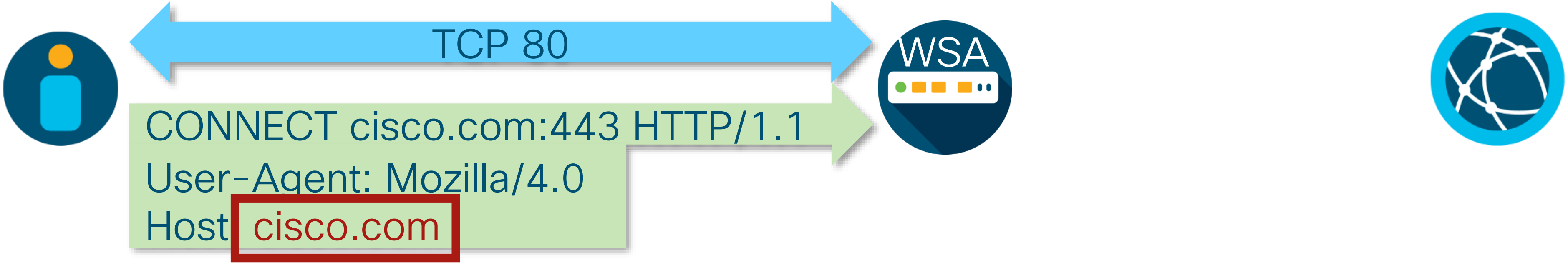
Explicit HTTPS – What do we know?

Explicit HTTPS – What do we know?



CONNECT cisco.com:443 HTTP/1.1
User-Agent: Mozilla/4.0
Host: cisco.com

Explicit HTTPS – What do we know?



TCP 80

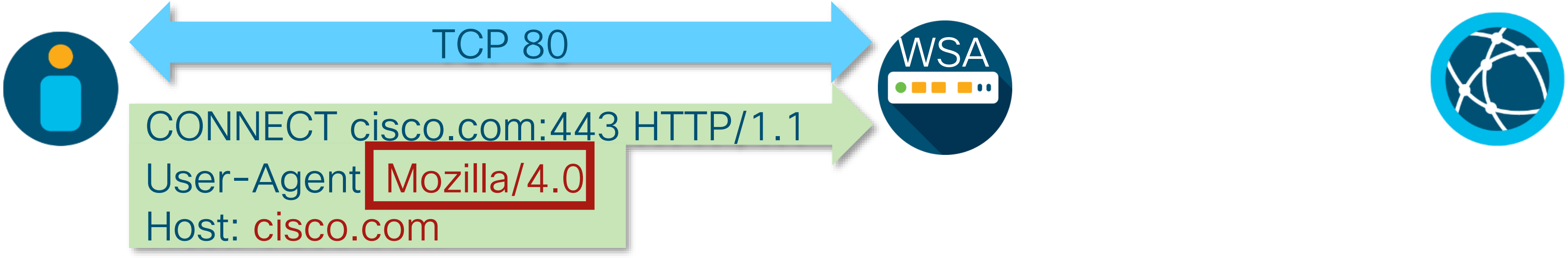
WSA

```
CONNECT cisco.com:443 HTTP/1.1
User-Agent: Mozilla/4.0
Host: cisco.com
```

We know…

1. Host header

Explicit HTTPS – What do we know?



TCP 80

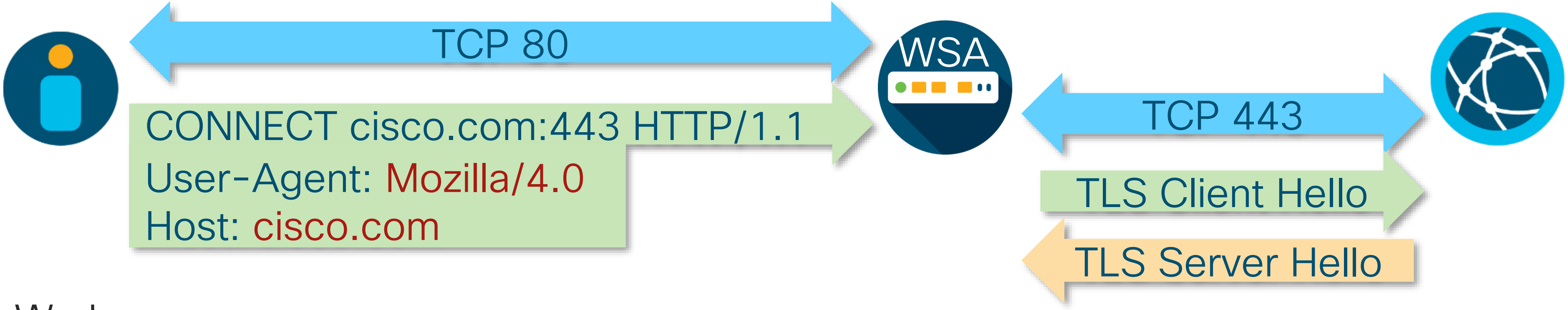
WSA

```
CONNECT cisco.com:443 HTTP/1.1
User-Agent Mozilla/4.0
Host: cisco.com
```

We know…

1. Host header
2. User-agent

Explicit HTTPS – What do we know?



CONNECT cisco.com:443 HTTP/1.1
User-Agent: Mozilla/4.0
Host: cisco.com

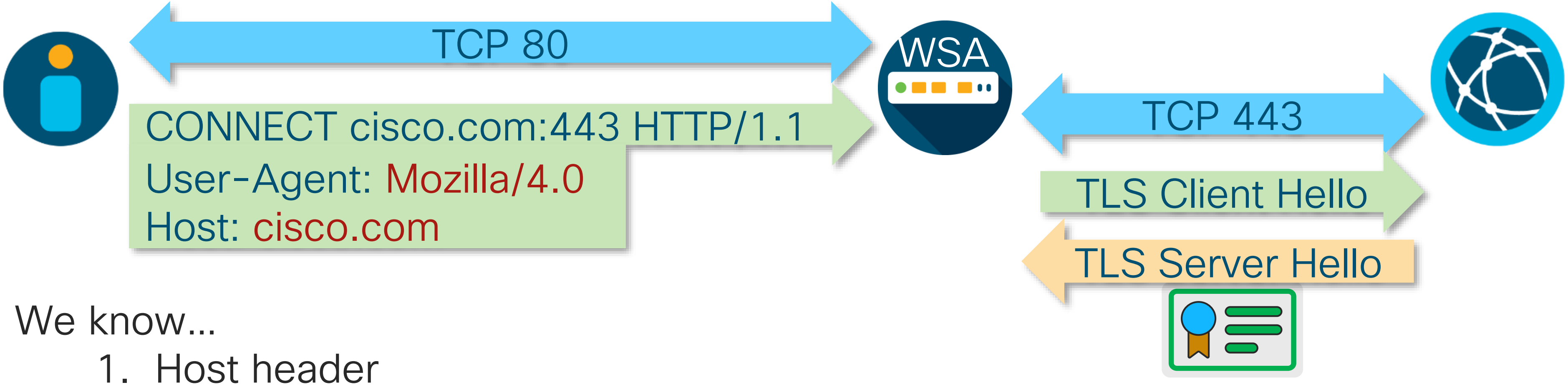
TLS Client Hello

TLS Server Hello

We know…

1. Host header
2. User-agent

Explicit HTTPS – What do we know?



TCP 80

CONNECT cisco.com:443 HTTP/1.1
User-Agent: Mozilla/4.0
Host: cisco.com

TCP 443

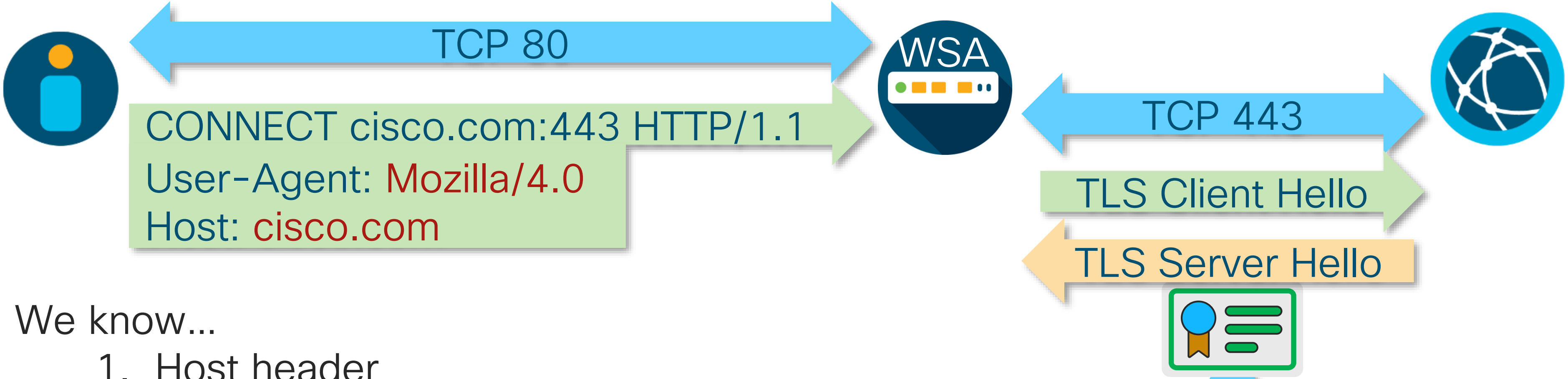
TLS Client Hello

TLS Server Hello

We know…

1. Host header
2. User-agent

Explicit HTTPS – What do we know?



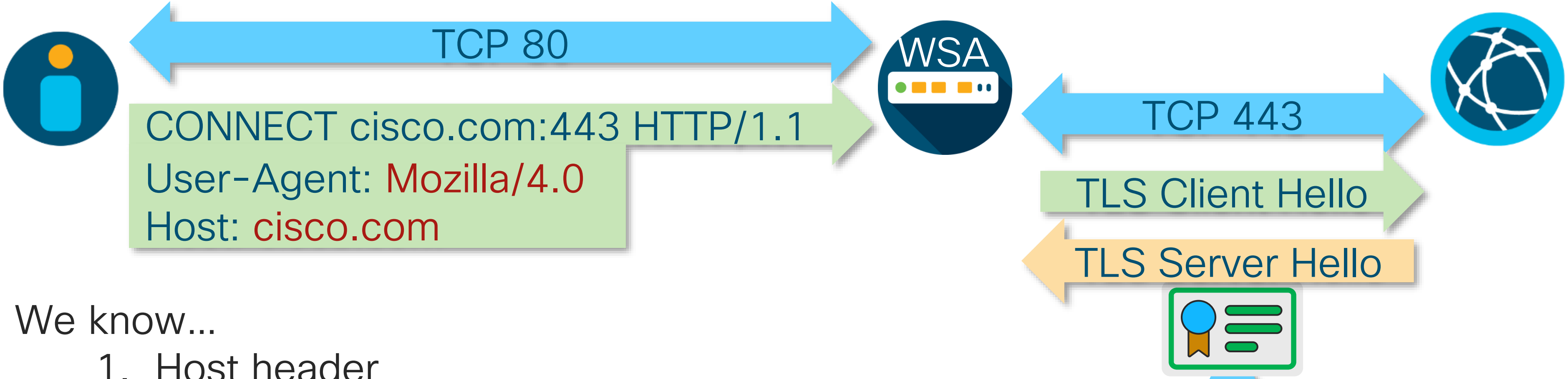
CONNECT cisco.com:443 HTTP/1.1
User-Agent: Mozilla/4.0
Host: cisco.com

We know…

1. Host header
2. User-agent
3. Certificate Issuer

```
Issuer: C=US, O=Ye Olde CA, CN=YOCA
Validity
        Not Before: Dec 19 13:45:14 2018 GMT
        Not After : Dec 19 13:45:14 2019 GMT
Subject: C=US, ST=CA, L=San Jose, O=Cisco Systems,
CN=cisco.com
        X509v3 Subject Alternative Name
            DNS:www.cisco.com, cisco.com, subdomain.cisco.com
```

Explicit HTTPS – What do we know?



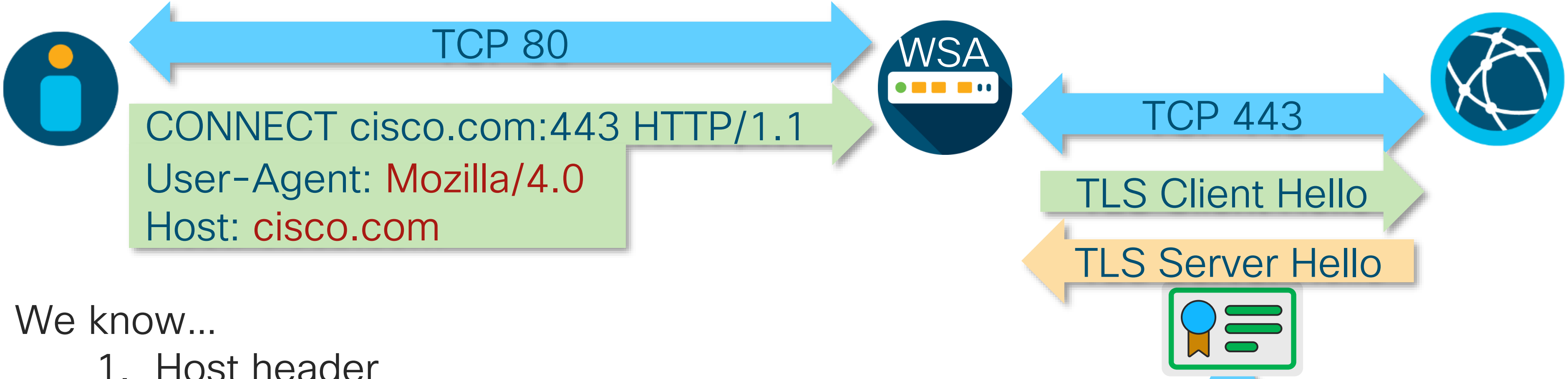
```
CONNECT cisco.com:443 HTTP/1.1
User-Agent: Mozilla/4.0
Host: cisco.com
```

We know…

1. Host header
2. User-agent
3. Certificate issuer
4. Certificate validity

```
Issuer: C=US, O=Ye Olde CA, CN=YOCA
Validity
        Not Before: Dec 19 13:45:14 2018 GMT
        Not After : Dec 19 13:45:14 2019 GMT
Subject: C=US, ST=CA, L=San Jose, O=Cisco Systems,
CN=cisco.com
        X509v3 Subject Alternative Name
            DNS:www.cisco.com, cisco.com, subdomain.cisco.com
```

Explicit HTTPS – What do we know?



TCP 80

CONNECT cisco.com:443 HTTP/1.1
User-Agent: Mozilla/4.0
Host: cisco.com

WSA

TCP 443

TLS Client Hello

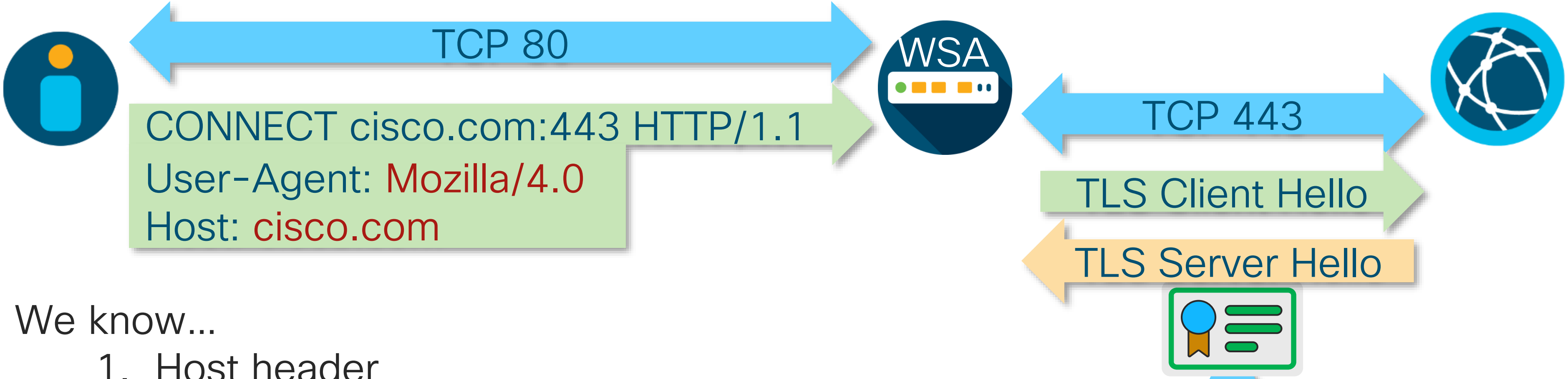
TLS Server Hello

We know...

1. Host header
2. User-agent
3. Certificate issuer
4. Certificate validity
5. SAN field

Issuer: C=US, O=Ye Olde CA, CN=YOCA
Validity
    Not Before: Dec 19 13:45:14 2018 GMT
    Not After : Dec 19 13:45:14 2019 GMT
Subject: C=US, ST=CA, L=San Jose, O=Cisco Systems, CN=cisco.com
    X509v3 Subject Alternative Name
        DNS:www.cisco.com, cisco.com, subdomain.cisco.com

Explicit HTTPS – What do we know?



CONNECT cisco.com:443 HTTP/1.1
User-Agent: Mozilla/4.0
Host: cisco.com

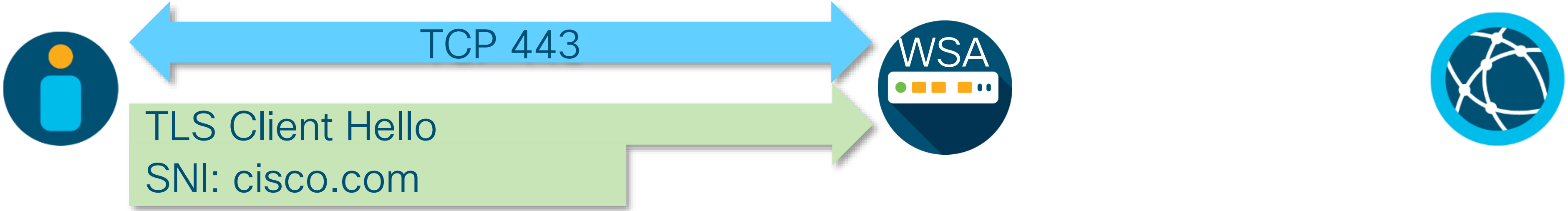
We know…

1. Host header
2. User-agent
3. Certificate issuer
4. Certificate validity
5. SAN field
6. CN field

Issuer: C=US, O=Ye Olde CA, CN=YOCA
Validity
    Not Before: Dec 19 13:45:14 2018 GMT
    Not After : Dec 19 13:45:14 2019 GMT
Subject: C=US, ST=CA, L=San Jose, O=Cisco Systems,
CN=cisco.com
    X509v3 Subject Alternative Name
        DNS:www.cisco.com, cisco.com, subdomain.cisco.com

Transparent HTTPS – What do we know?

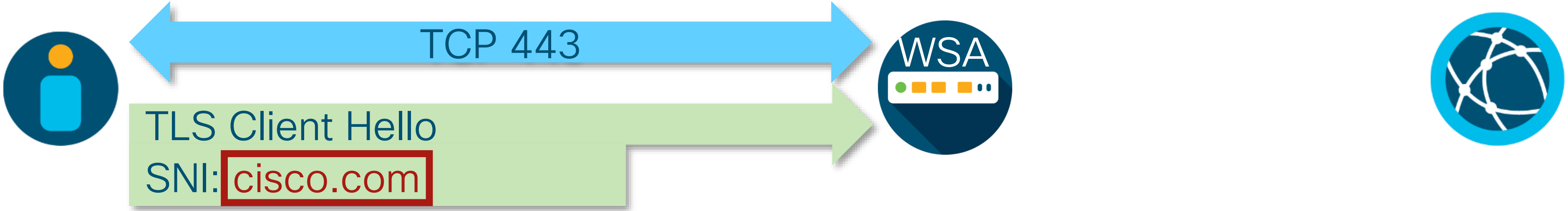
Transparent HTTPS – What do we know?



TLS Client Hello

SNI: cisco.com

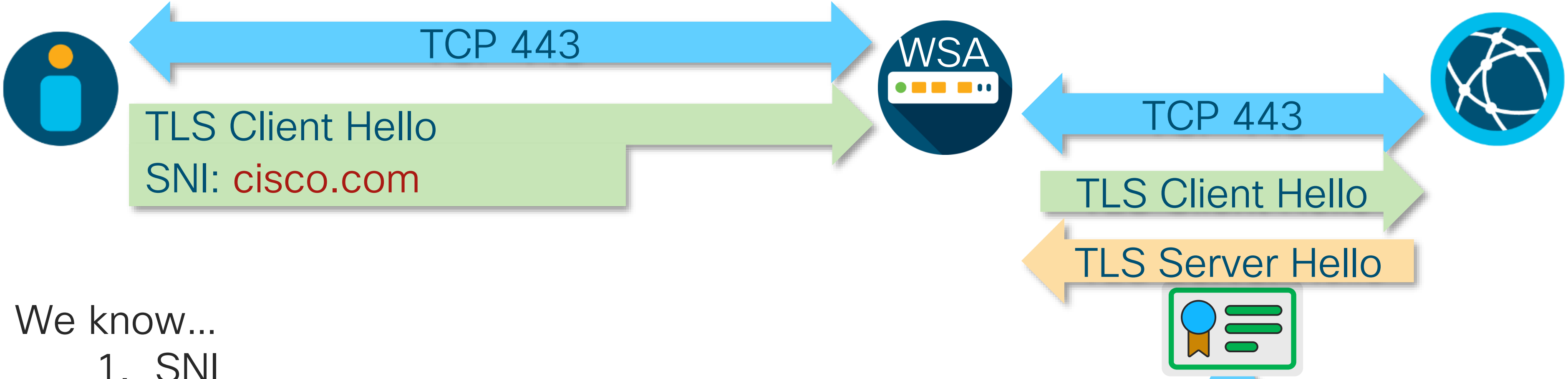
Transparent HTTPS – What do we know?



We know…

1. SNI

Transparent HTTPS – What do we know?

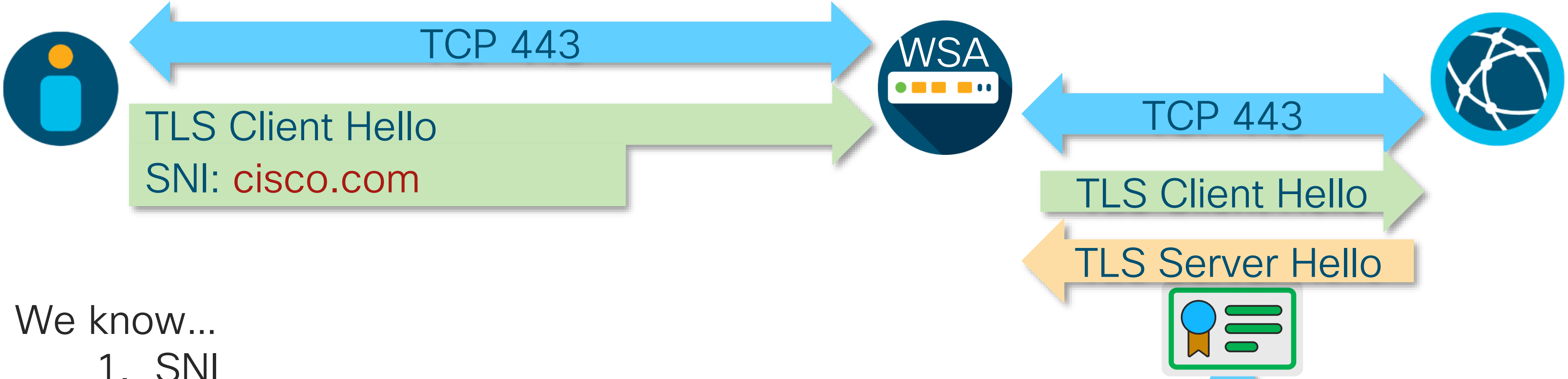


We know…

1. SNI
2. Certificate issuer

Issuer: C=US, O=Ye Olde CA, CN=YOCA
Validity
    Not Before: Dec 19 13:45:14 2018 GMT
    Not After : Dec 19 13:45:14 2019 GMT
Subject: C=US, ST=CA, L=San Jose, O=Cisco Systems,
CN=cisco.com
    X509v3 Subject Alternative Name
        DNS:www.cisco.com, cisco.com, subdomain.cisco.com

Transparent HTTPS – What do we know?

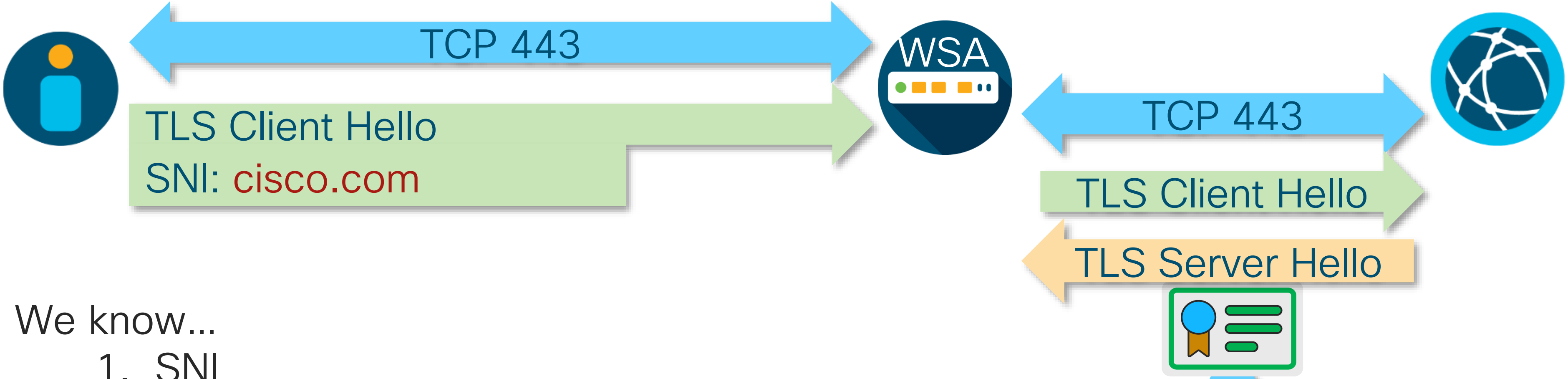


We know…

1. SNI
2. Certificate issuer
3. Certificate validity

```
Issuer: C=US, O=Ye Olde CA, CN=YOCA
Validity
        Not Before: Dec 19 13:45:14 2018 GMT
        Not After : Dec 19 13:45:14 2019 GMT
Subject: C=US, ST=CA, L=San Jose, O=Cisco Systems,
CN=cisco.com
        X509v3 Subject Alternative Name
            DNS:www.cisco.com, cisco.com, subdomain.cisco.com
```

Transparent HTTPS – What do we know?



TCP 443

TLS Client Hello

SNI: cisco.com

WSA

TCP 443

TLS Client Hello

TLS Server Hello

We know…

1. SNI
2. Certificate issuer
3. Certificate validity
4. SAN field

Issuer: C=US, O=Ye Olde CA, CN=YOCA

Validity

Not Before: Dec 19 13:45:14 2018 GMT

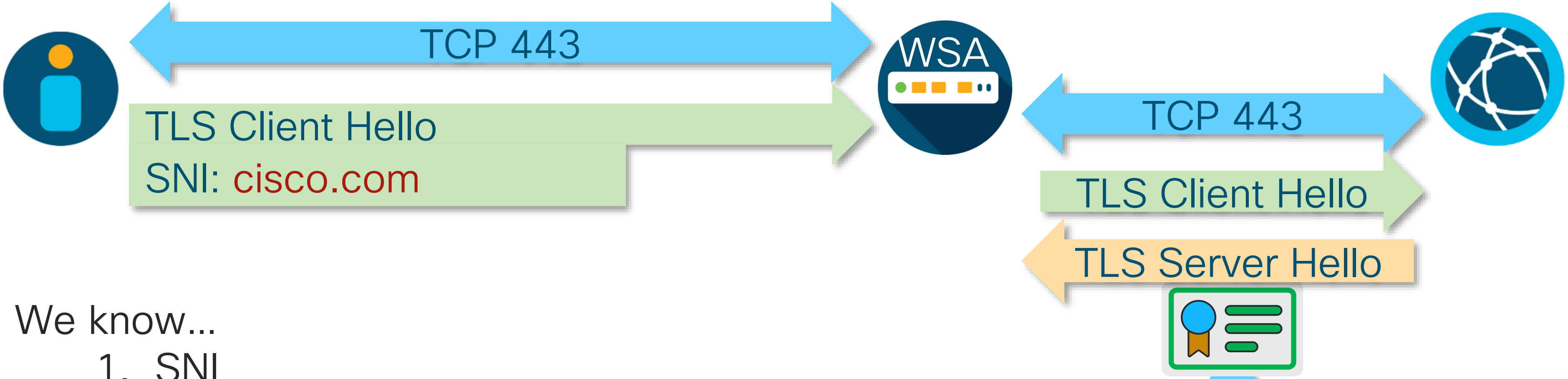
Not After : Dec 19 13:45:14 2019 GMT

Subject: C=US, ST=CA, L=San Jose, O=Cisco Systems, CN=cisco.com

X509v3 Subject Alternative Name

DNS:www.cisco.com, cisco.com, subdomain.cisco.com

Transparent HTTPS – What do we know?



We know…

1. SNI
2. Certificate issuer
3. Certificate validity
4. SAN field
5. CN field

Issuer: C=US, O=Ye Olde CA, CN=YOCA
Validity
    Not Before: Dec 19 13:45:14 2018 GMT
    Not After : Dec 19 13:45:14 2019 GMT
Subject: C=US, ST=CA, L=San Jose, O=Cisco Systems,
CN=cisco.com
    X509v3 Subject Alternative Name
        DNS:www.cisco.com, cisco.com, subdomain.cisco.com

Decryption policy baselines

- Decrypt categories that require HTTP controls
- Decrypt traffic that must be scanned for malware
- Passthrough user sensitive traffic (finance, health)
- Drop traffic that will end up being blocked by access policies
- Drop traffic that can be identified by category only

Access policies

- Decrypted connections are evaluated here
- HTTP request are evaluated immediately after ID profile match
- Two access_log entries for each decrypted connection
    - tunnel:// or tcp_connect
    - HTTP method (GET, POST, etc.)
- Do not block uncategorized requests
    - Still scanned by AV and AMP
    - Enable DCA to reduce the number of uncategorized sites

Access policies

- Enable range request headers for update services
  - If you cannot bypass OS or application updates
  - Use well-known user-agent strings to identify the traffic
- Object scanning / blocking / AV
  - Be careful inspecting all archives
  - Do not block unscannable

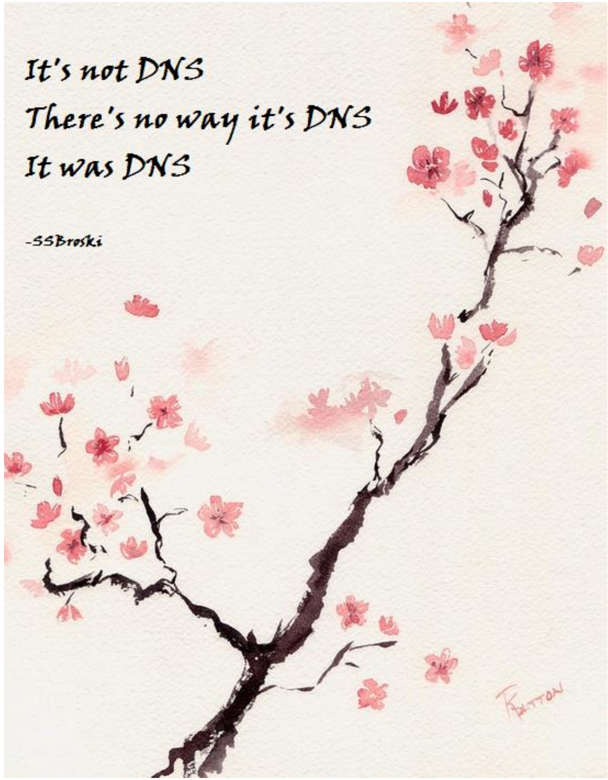
Custom URL categories

- Use regex sparingly
- Keep the total number of custom categories to less than 20
  - A larger number of category lists is more impactful on performance than a small number with many entries
- Use external custom categories for dynamic lists
  - Can be used with internal servers
  - Office365 API is available

Monitoring and Troubleshooting

The Internet is slow…must be the WSA!

- Enhance your MTTI
  - Mean time to innocence
- Things to check
  - Hardware (RAID, interfaces, etc.)
  - Sizing; are we overloaded?
  - Configuration complexity
  - DNS (The Sysadmin’s Haiku)
  - Authentication
  - Disk latency

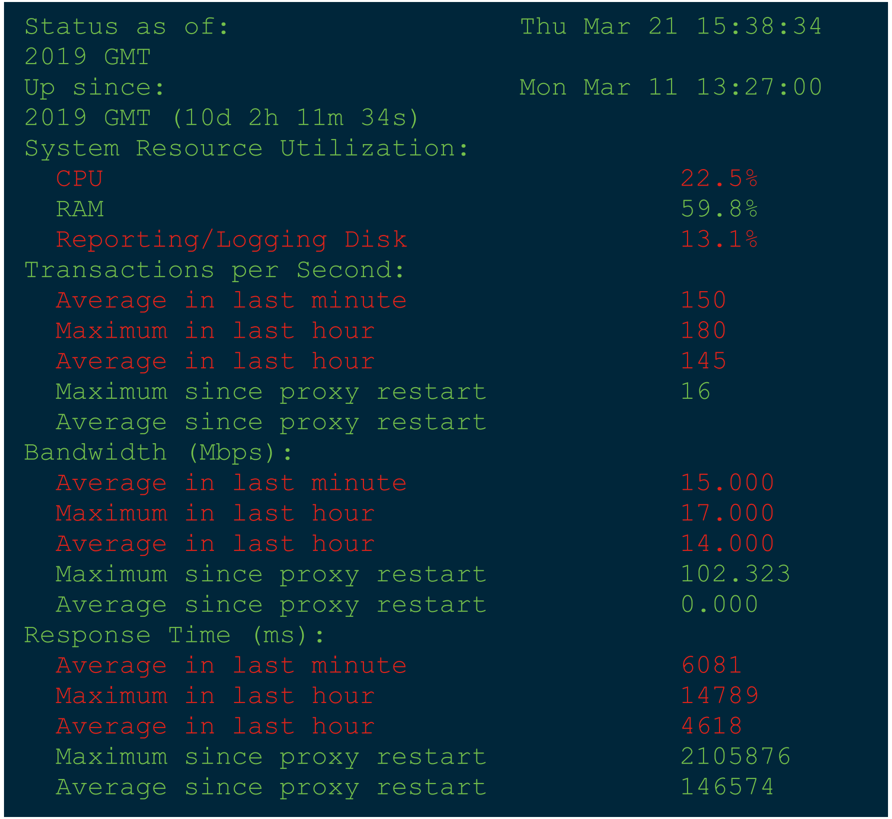


It's not DNS
There's no way it's DNS
It was DNS

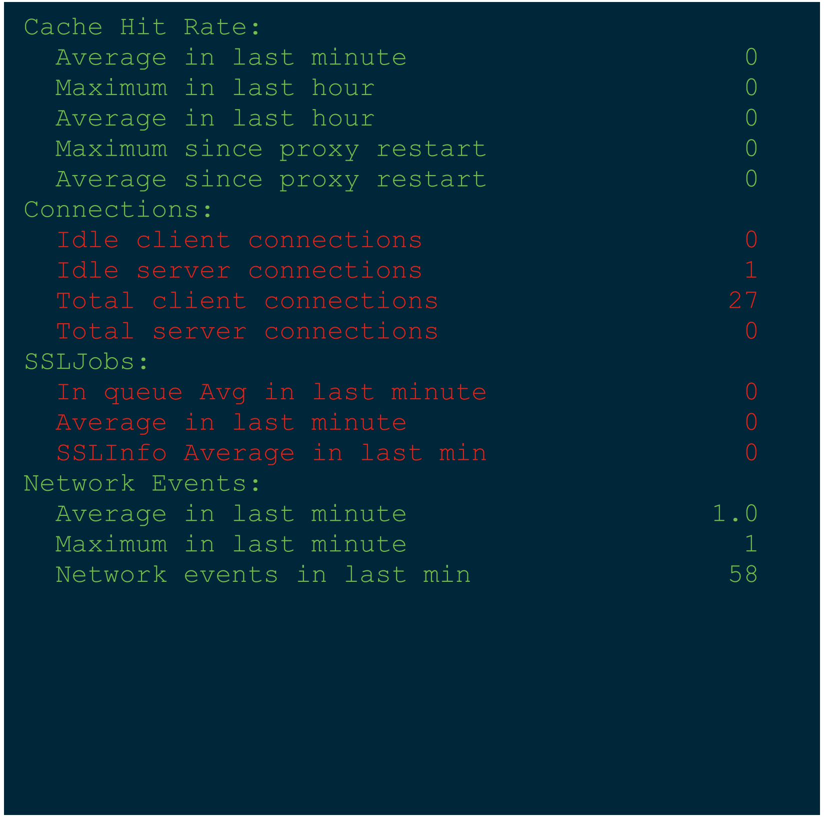
-SSBroski

Overloaded?

status detail CLI command



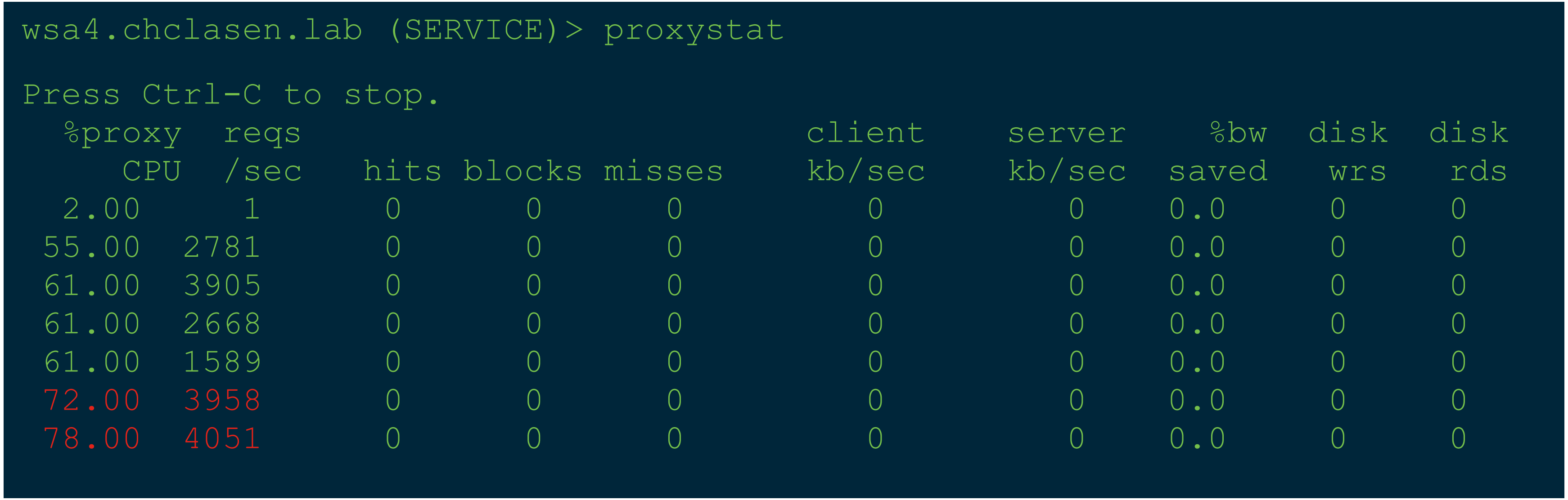
```
Status as of:                  Thu Mar 21 15:38:34
2019 GMT
Up since:                      Mon Mar 11 13:27:00
2019 GMT (10d 2h 11m 34s)
System Resource Utilization:
  CPU                                    22.5%
  RAM                                    59.8%
  Reporting/Logging Disk                 13.1%
Transactions per Second:
  Average in last minute                 150
  Maximum in last hour                   180
  Average in last hour                   145
  Maximum since proxy restart            16
  Average since proxy restart
Bandwidth (Mbps):
  Average in last minute                 15.000
  Maximum in last hour                   17.000
  Average in last hour                   14.000
  Maximum since proxy restart            102.323
  Average since proxy restart            0.000
Response Time (ms):
  Average in last minute                 6081
  Maximum in last hour                   14789
  Average in last hour                   4618
  Maximum since proxy restart            2105876
  Average since proxy restart            146574
```



```
Cache Hit Rate:
  Average in last minute                     0
  Maximum in last hour                       0
  Average in last hour                       0
  Maximum since proxy restart                0
  Average since proxy restart                0
Connections:
  Idle client connections                    0
  Idle server connections                    1
  Total client connections                  27
  Total server connections                   0
SSLJobs:
  In queue Avg in last minute                0
  Average in last minute                     0
  SSLInfo Average in last min                0
Network Events:
  Average in last minute                   1.0
  Maximum in last minute                     1
  Network events in last min                58
```

Overloaded?

proxystat CLI command



```
wsa4.chclasen.lab (SERVICE)> proxystat

Press Ctrl-C to stop.
  %proxy  reqs                         client    server    %bw  disk  disk
     CPU  /sec   hits blocks misses    kb/sec    kb/sec  saved   wrs   rds
  2.00     1      0      0      0         0         0    0.0     0     0
 55.00  2781      0      0      0         0         0    0.0     0     0
 61.00  3905      0      0      0         0         0    0.0     0     0
 61.00  2668      0      0      0         0         0    0.0     0     0
 61.00  1589      0      0      0         0         0    0.0     0     0
 72.00  3958      0      0      0         0         0    0.0     0     0
 78.00  4051      0      0      0         0         0    0.0     0     0
```

Overloaded?

shd_log subscription

- System health daemon
- Log written every one minute
- One line contains many useful fields including:
  - CPU
  - Memory
  - RPS
  - Connection count (client/server)
  - Latency
  - AV scanning time

shd_log

shd log field	Description
CPULd	Percentage of CPU in use as reported by the OS, 0-100%
DskUtil	Percentage of log partition disk usage, 0-100%
RAMUtil	Percentage of free memory as reported by the OS, 0-100%
Reqs	Average number of requests in the past minute
Band	Average bandwidth saved in the past minute
Latency	Average latency in the last minute
CacheHit	Average number of cache hits in the past minute
CliConn	Total number of client-side TCP connections
SrvConn	Total number of server-side TCP connections
Membuf	Total amount of memory buffer space that is available
SwpPgOut	Number of pages that were swapped out as reported by the OS
xLD entries	CPU utilization by individual services (AV scanners, WBRS, WTT, etc.)

track_stats log

Single most important log for performance troubleshooting

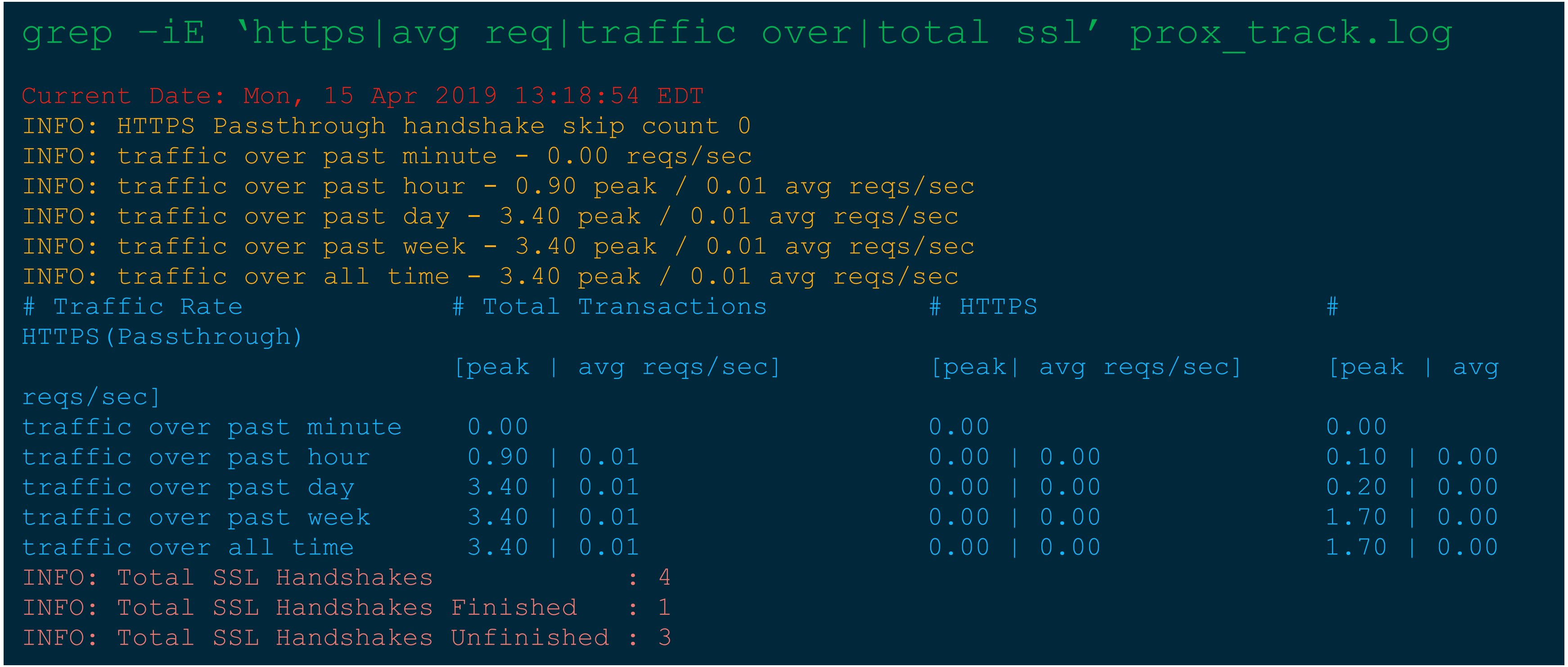
- Written every five minutes
- No log subscription
- Accessed using SCP or FTP
- Most entries have a corresponding access_log custom field

Includes:

- Request information
- Traffic statistics
- Memory allocation
- Client/Server transaction time
- Individual service latency

How to read the track_stats log

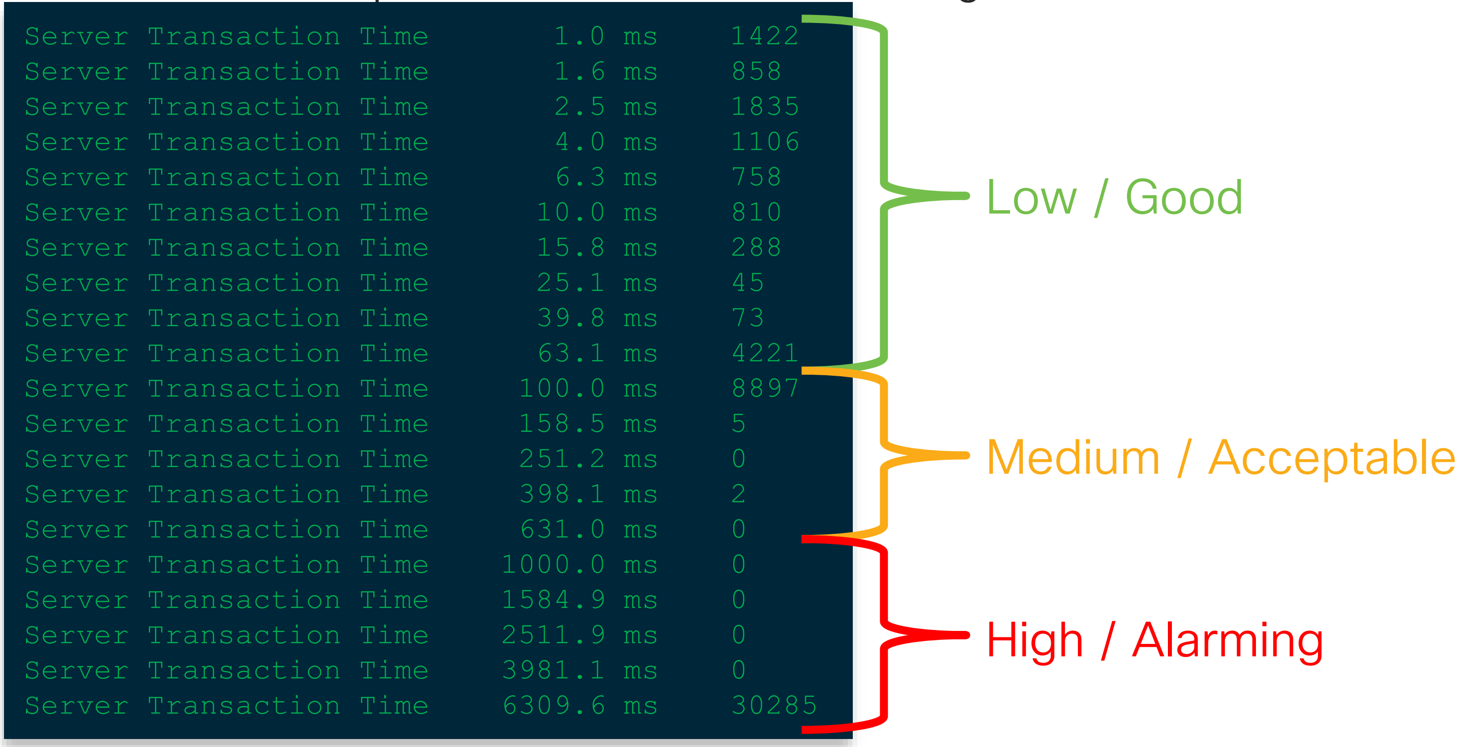
Traffic and HTTPS transaction statistics



```
grep -iE 'https|avg req|traffic over|total ssl' prox_track.log

Current Date: Mon, 15 Apr 2019 13:18:54 EDT
INFO: HTTPS Passthrough handshake skip count 0
INFO: traffic over past minute - 0.00 reqs/sec
INFO: traffic over past hour - 0.90 peak / 0.01 avg reqs/sec
INFO: traffic over past day - 3.40 peak / 0.01 avg reqs/sec
INFO: traffic over past week - 3.40 peak / 0.01 avg reqs/sec
INFO: traffic over all time - 3.40 peak / 0.01 avg reqs/sec
# Traffic Rate              # Total Transactions          # HTTPS                  #
HTTPS(Passthrough)
                            [peak | avg reqs/sec]          [peak| avg reqs/sec]     [peak | avg
reqs/sec]
traffic over past minute     0.00                          0.00                     0.00
traffic over past hour       0.90 | 0.01                   0.00 | 0.00              0.10 | 0.00
traffic over past day        3.40 | 0.01                   0.00 | 0.00              0.20 | 0.00
traffic over past week       3.40 | 0.01                   0.00 | 0.00              1.70 | 0.00
traffic over all time        3.40 | 0.01                   0.00 | 0.00              1.70 | 0.00
INFO: Total SSL Handshakes            : 4
INFO: Total SSL Handshakes Finished   : 1
INFO: Total SSL Handshakes Unfinished : 3
```

How to read the track_stats log

Statistics are reset after a restart of the prox process
Total number of requests are shown across a range of time values



```
Server Transaction Time      1.0 ms    1422
Server Transaction Time      1.6 ms    858
Server Transaction Time      2.5 ms    1835
Server Transaction Time      4.0 ms    1106
Server Transaction Time      6.3 ms    758
Server Transaction Time     10.0 ms    810
Server Transaction Time     15.8 ms    288
Server Transaction Time     25.1 ms    45
Server Transaction Time     39.8 ms    73
Server Transaction Time     63.1 ms    4221
Server Transaction Time    100.0 ms    8897
Server Transaction Time    158.5 ms    5
Server Transaction Time    251.2 ms    0
Server Transaction Time    398.1 ms    2
Server Transaction Time    631.0 ms    0
Server Transaction Time   1000.0 ms    0
Server Transaction Time   1584.9 ms    0
Server Transaction Time   2511.9 ms    0
Server Transaction Time   3981.1 ms    0
Server Transaction Time   6309.6 ms    30285
```

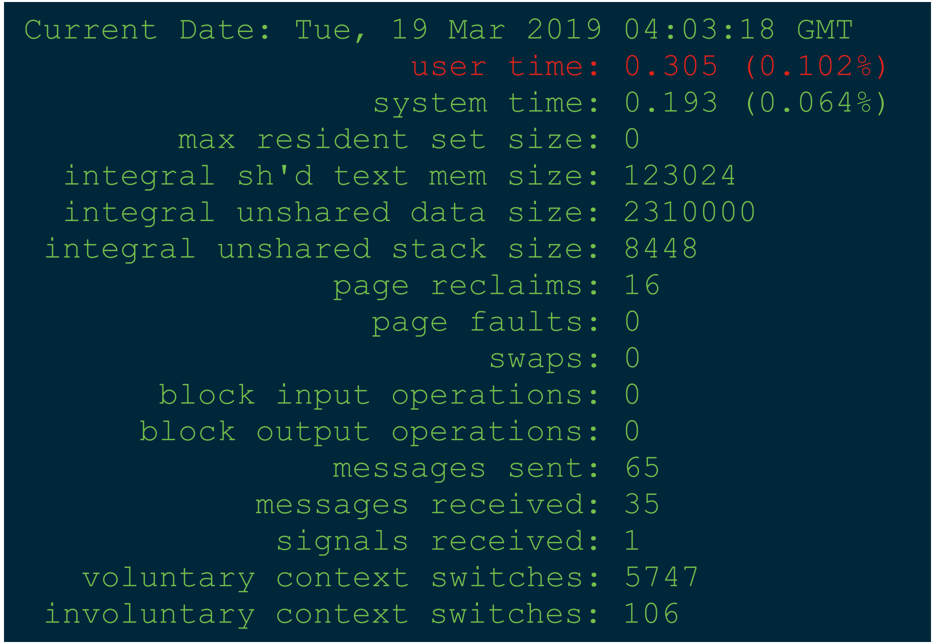
Low / Good

Medium / Acceptable

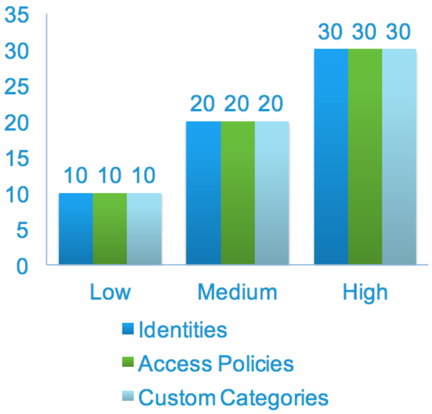
High / Alarming

Configuration too complex?

Check the user time value in the track_stats log



```
Current Date: Tue, 19 Mar 2019 04:03:18 GMT
                        user time: 0.305 (0.102%)
                      system time: 0.193 (0.064%)
             max resident set size: 0
       integral sh'd text mem size: 123024
       integral unshared data size: 2310000
      integral unshared stack size: 8448
                     page reclaims: 16
                       page faults: 0
                             swaps: 0
             block input operations: 0
            block output operations: 0
                     messages sent: 65
                 messages received: 35
                  signals received: 1
         voluntary context switches: 5747
       involuntary context switches: 106
```



Low Complexity Definition	
10 Access Policies	
10 Identities	
10 Custom Categories	10 Regex
	50 Server IP's
	420 Server Names

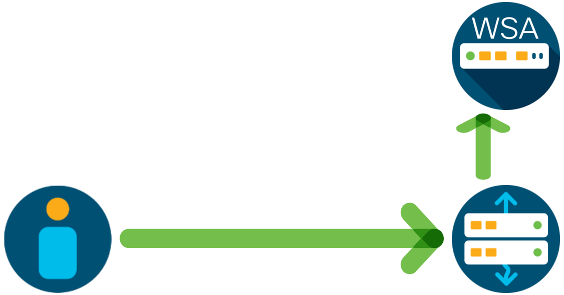
Medium Complexity = 2 x Low Complexity

High Complexity = 3 x Low Complexity

Where can latency be introduced?

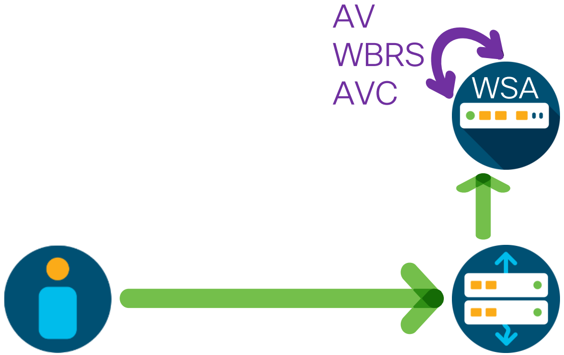
Where can latency be introduced?

- Client side



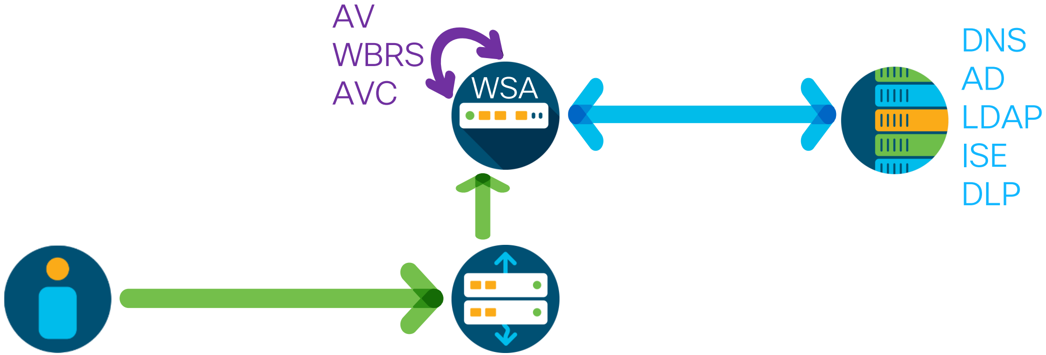
Where can latency be introduced?

- Client side
- Internal services



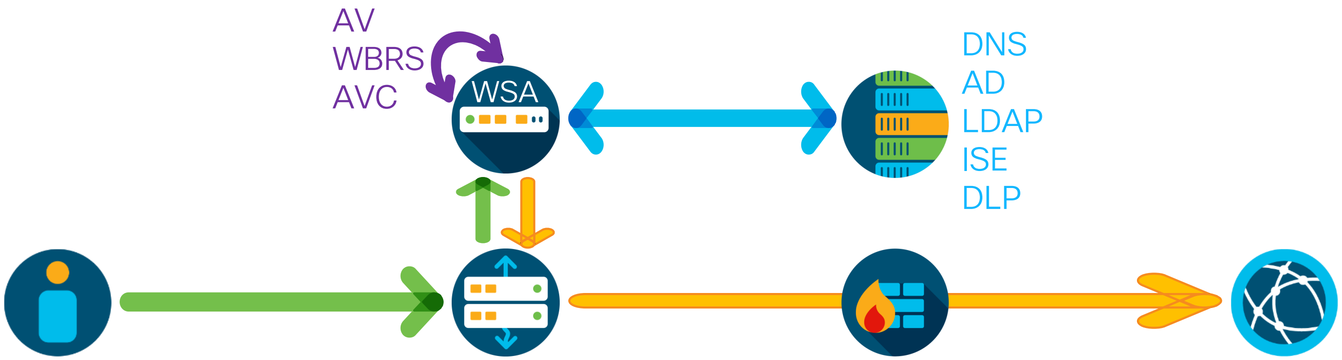
Where can latency be introduced?

- Client side
- Internal services
- External services

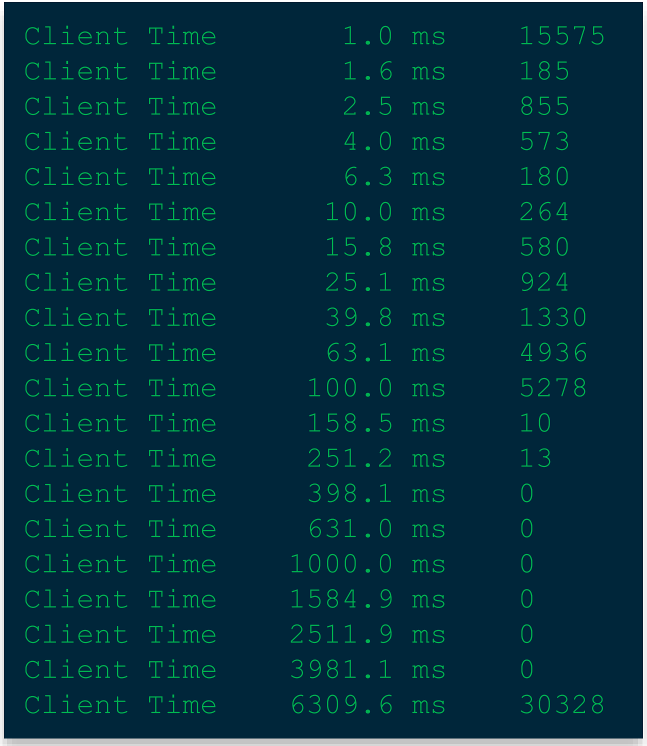


Where can latency be introduced?

- Client side
- Internal services
- External services
- Server side

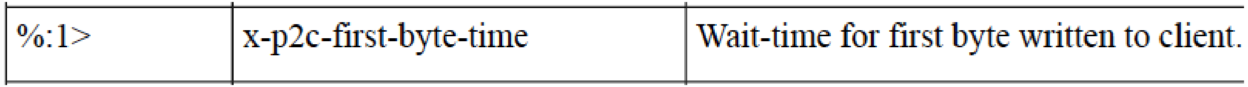


Client side latency

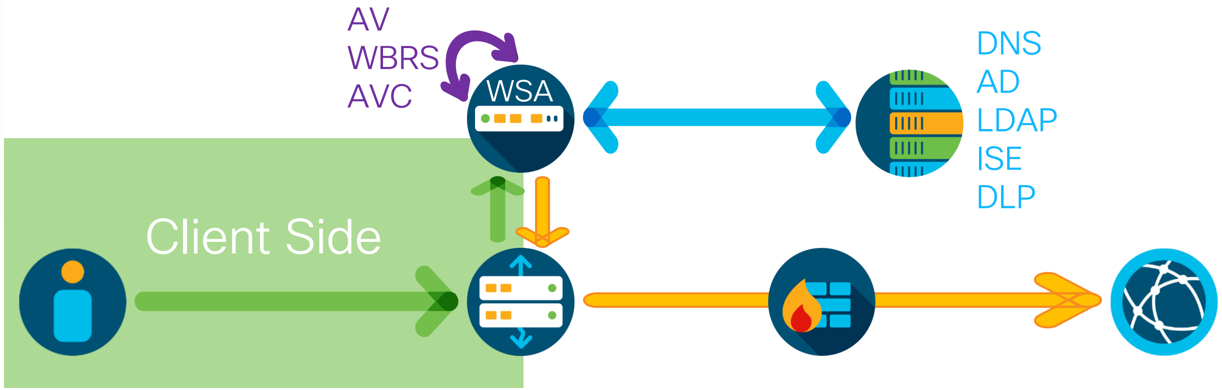


```
Client Time          1.0 ms     15575
Client Time          1.6 ms     185
Client Time          2.5 ms     855
Client Time          4.0 ms     573
Client Time          6.3 ms     180
Client Time         10.0 ms     264
Client Time         15.8 ms     580
Client Time         25.1 ms     924
Client Time         39.8 ms     1330
Client Time         63.1 ms     4936
Client Time        100.0 ms     5278
Client Time        158.5 ms     10
Client Time        251.2 ms     13
Client Time        398.1 ms     0
Client Time        631.0 ms     0
Client Time       1000.0 ms     0
Client Time       1584.9 ms     0
Client Time       2511.9 ms     0
Client Time       3981.1 ms     0
Client Time       6309.6 ms     30328
```

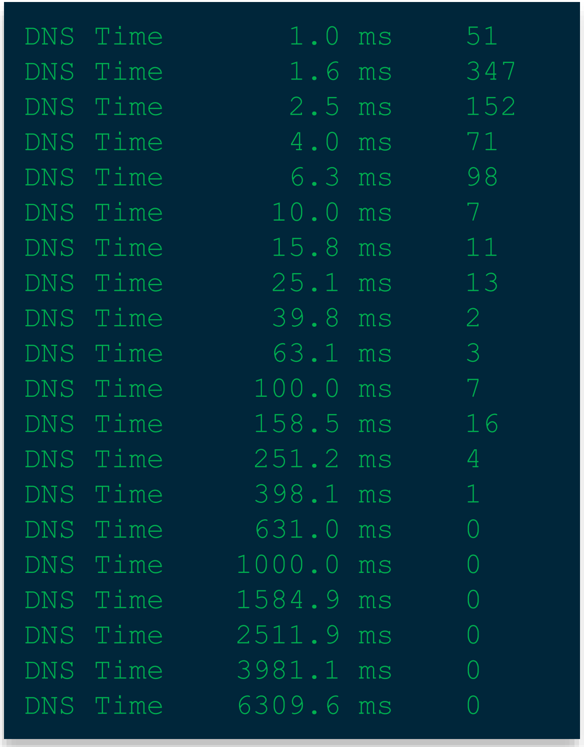
- Client time in track_stats log
- The amount of time in ms that the client was waiting for a response
- May indicate upstream issues as well



%:1>	x-p2c-first-byte-time	Wait-time for first byte written to client.

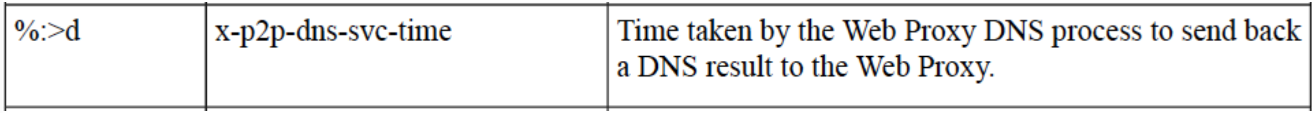


DNS latency

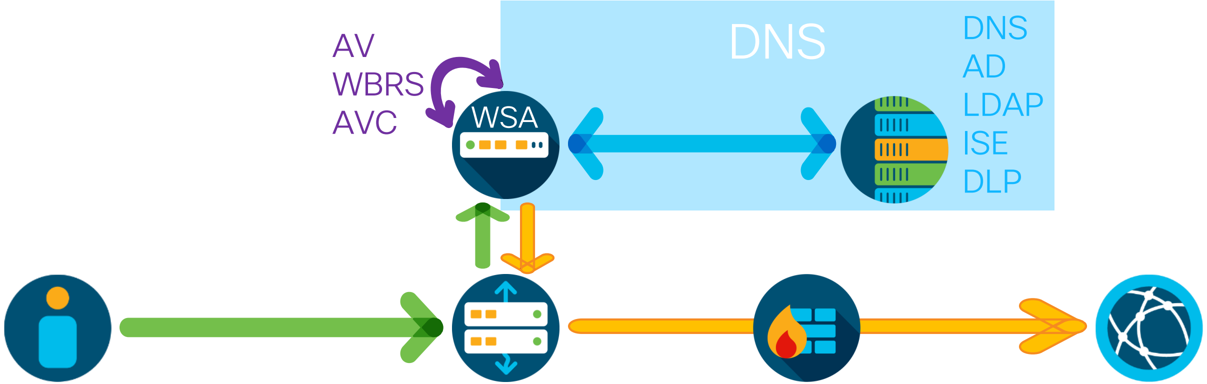


```
DNS Time          1.0 ms     51
DNS Time          1.6 ms     347
DNS Time          2.5 ms     152
DNS Time          4.0 ms     71
DNS Time          6.3 ms     98
DNS Time         10.0 ms     7
DNS Time         15.8 ms     11
DNS Time         25.1 ms     13
DNS Time         39.8 ms     2
DNS Time         63.1 ms     3
DNS Time        100.0 ms     7
DNS Time        158.5 ms     16
DNS Time        251.2 ms     4
DNS Time        398.1 ms     1
DNS Time        631.0 ms     0
DNS Time       1000.0 ms     0
DNS Time       1584.9 ms     0
DNS Time       2511.9 ms     0
DNS Time       3981.1 ms     0
DNS Time       6309.6 ms     0
```

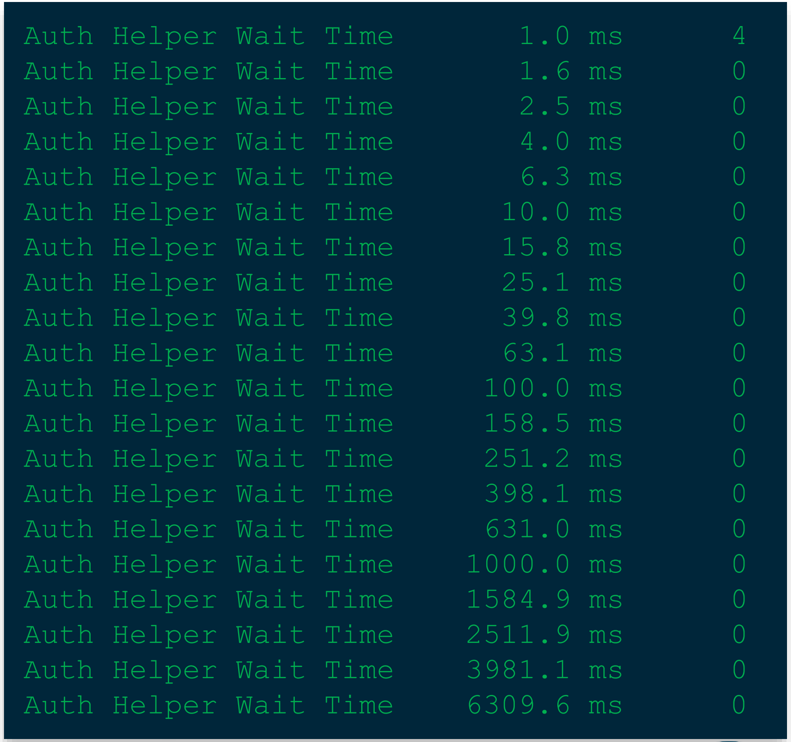
- The amount of time in ms that the WSA waited for a DNS resolution
- Calls for investigation of the DNS resolvers



%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy DNS process to send back a DNS result to the Web Proxy.

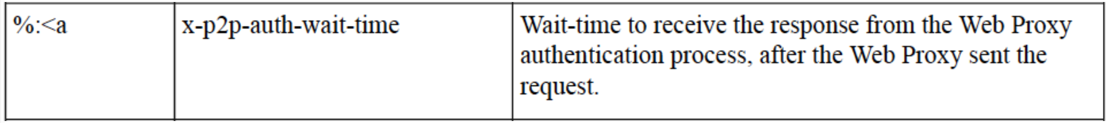


Authentication latency

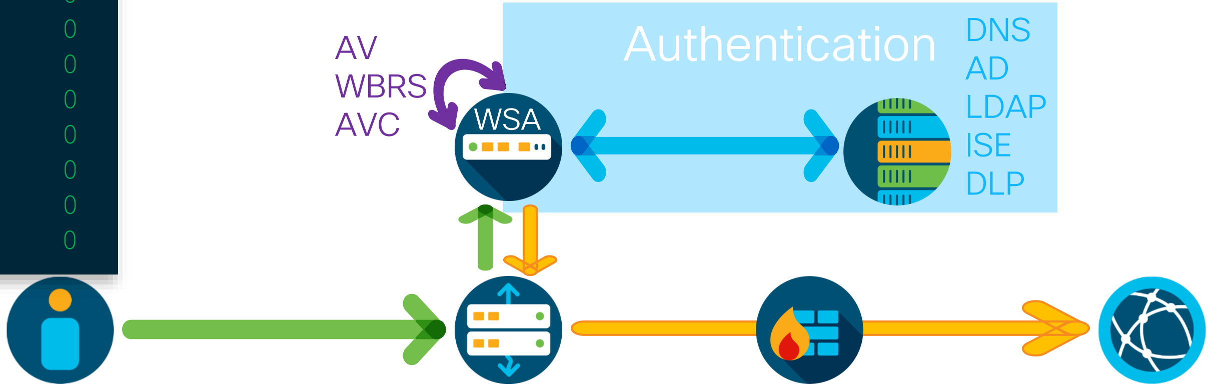


```
Auth Helper Wait Time          1.0 ms       4
Auth Helper Wait Time          1.6 ms       0
Auth Helper Wait Time          2.5 ms       0
Auth Helper Wait Time          4.0 ms       0
Auth Helper Wait Time          6.3 ms       0
Auth Helper Wait Time         10.0 ms       0
Auth Helper Wait Time         15.8 ms       0
Auth Helper Wait Time         25.1 ms       0
Auth Helper Wait Time         39.8 ms       0
Auth Helper Wait Time         63.1 ms       0
Auth Helper Wait Time        100.0 ms       0
Auth Helper Wait Time        158.5 ms       0
Auth Helper Wait Time        251.2 ms       0
Auth Helper Wait Time        398.1 ms       0
Auth Helper Wait Time        631.0 ms       0
Auth Helper Wait Time       1000.0 ms       0
Auth Helper Wait Time       1584.9 ms       0
Auth Helper Wait Time       2511.9 ms       0
Auth Helper Wait Time       3981.1 ms       0
Auth Helper Wait Time       6309.6 ms       0
```

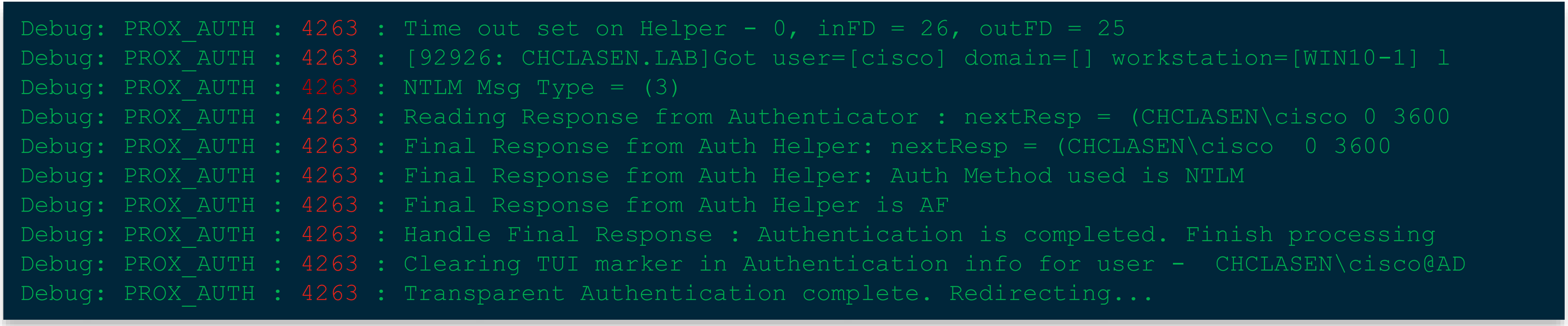
- Two metrics: auth helper wait time and auth helper service wait time
- Use the first for the pure auth time without the request time added



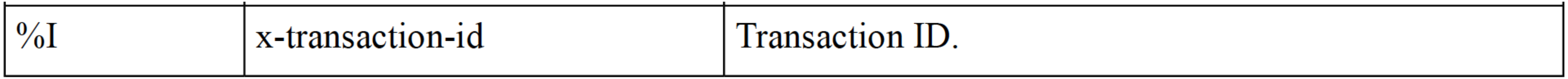
%:<a	x-p2p-auth-wait-time	Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.



Authentication latency

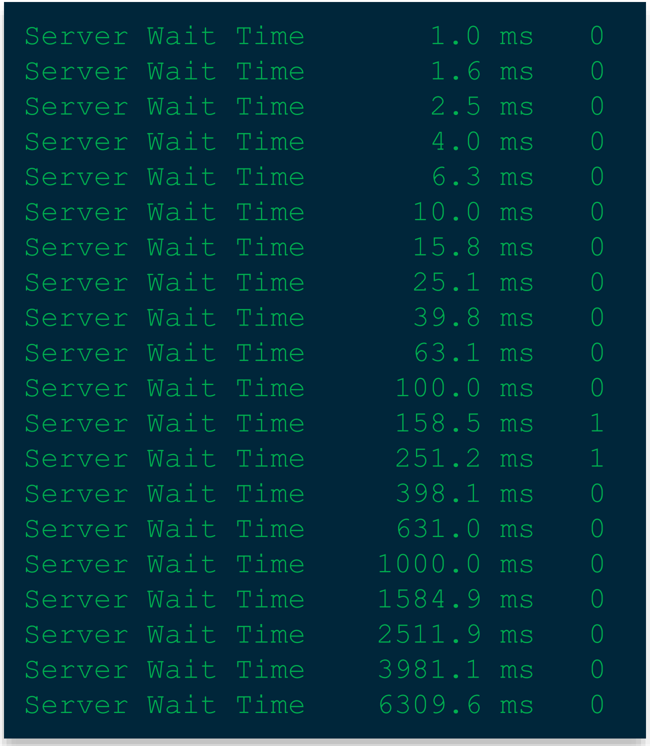


```
Debug: PROX_AUTH : 4263 : Time out set on Helper - 0, inFD = 26, outFD = 25
Debug: PROX_AUTH : 4263 : [92926: CHCLASEN.LAB]Got user=[cisco] domain=[] workstation=[WIN10-1] 1
Debug: PROX_AUTH : 4263 : NTLM Msg Type = (3)
Debug: PROX_AUTH : 4263 : Reading Response from Authenticator : nextResp = (CHCLASEN\cisco 0 3600
Debug: PROX_AUTH : 4263 : Final Response from Auth Helper: nextResp = (CHCLASEN\cisco  0 3600
Debug: PROX_AUTH : 4263 : Final Response from Auth Helper: Auth Method used is NTLM
Debug: PROX_AUTH : 4263 : Final Response from Auth Helper is AF
Debug: PROX_AUTH : 4263 : Handle Final Response : Authentication is completed. Finish processing
Debug: PROX_AUTH : 4263 : Clearing TUI marker in Authentication info for user -  CHCLASEN\cisco@AD
Debug: PROX_AUTH : 4263 : Transparent Authentication complete. Redirecting...
```



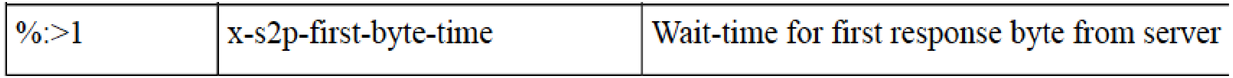
%I	x-transaction-id	Transaction ID.

Server latency – wait time

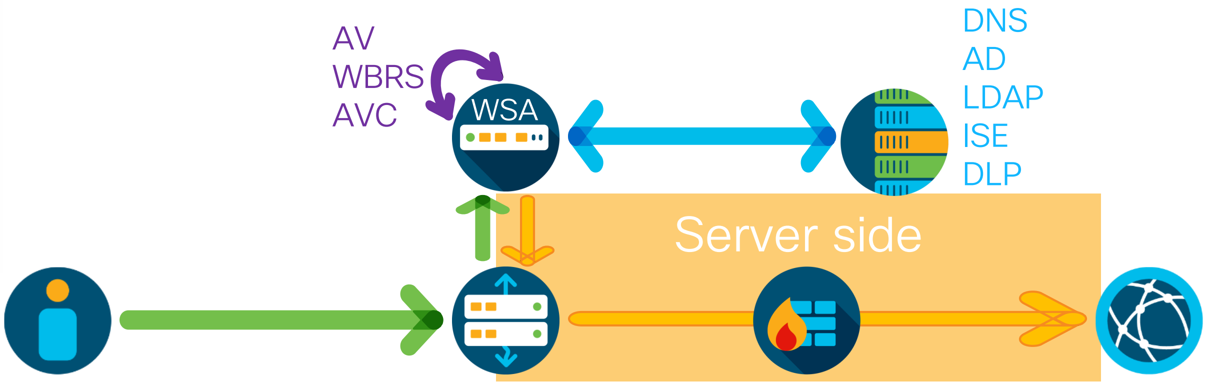


```
Server Wait Time          1.0 ms    0
Server Wait Time          1.6 ms    0
Server Wait Time          2.5 ms    0
Server Wait Time          4.0 ms    0
Server Wait Time          6.3 ms    0
Server Wait Time         10.0 ms    0
Server Wait Time         15.8 ms    0
Server Wait Time         25.1 ms    0
Server Wait Time         39.8 ms    0
Server Wait Time         63.1 ms    0
Server Wait Time        100.0 ms    0
Server Wait Time        158.5 ms    1
Server Wait Time        251.2 ms    1
Server Wait Time        398.1 ms    0
Server Wait Time        631.0 ms    0
Server Wait Time       1000.0 ms    0
Server Wait Time       1584.9 ms    0
Server Wait Time       2511.9 ms    0
Server Wait Time       3981.1 ms    0
Server Wait Time       6309.6 ms    0
```

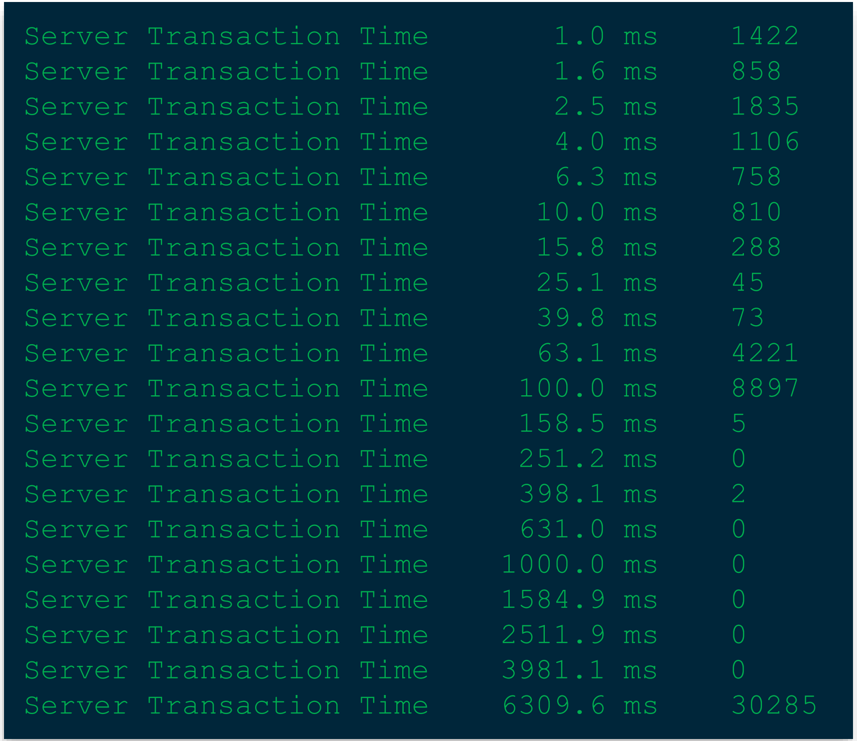
- The amount of time in ms that the WSA waited for the first byte of the server response
- Investigate upstream devices and WAN connection



%:>1	x-s2p-first-byte-time	Wait-time for first response byte from server

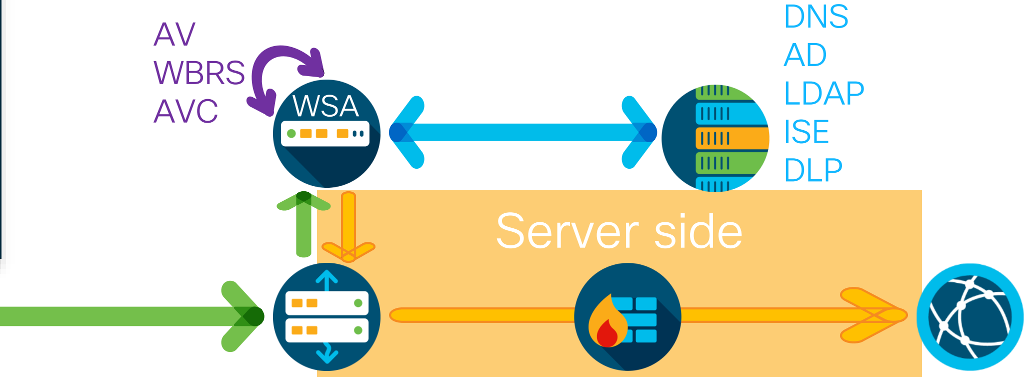


Server latency – transaction time

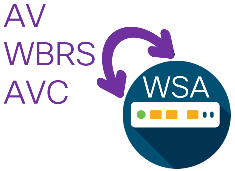


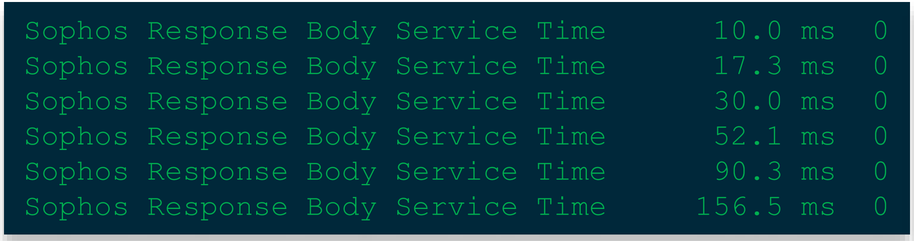
```
Server Transaction Time       1.0 ms     1422
Server Transaction Time       1.6 ms     858
Server Transaction Time       2.5 ms     1835
Server Transaction Time       4.0 ms     1106
Server Transaction Time       6.3 ms     758
Server Transaction Time      10.0 ms     810
Server Transaction Time      15.8 ms     288
Server Transaction Time      25.1 ms     45
Server Transaction Time      39.8 ms     73
Server Transaction Time      63.1 ms     4221
Server Transaction Time     100.0 ms     8897
Server Transaction Time     158.5 ms     5
Server Transaction Time     251.2 ms     0
Server Transaction Time     398.1 ms     2
Server Transaction Time     631.0 ms     0
Server Transaction Time    1000.0 ms     0
Server Transaction Time    1584.9 ms     0
Server Transaction Time    2511.9 ms     0
Server Transaction Time    3981.1 ms     0
Server Transaction Time    6309.6 ms     30285
```

- The amount of time in ms for the entire server-side transaction to complete
- Investigate upstream devices and WAN connection
- No access_log custom field but can be determined by a combination of others

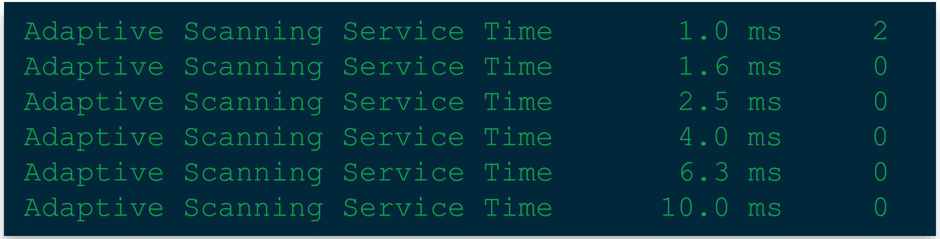


Internal services latency

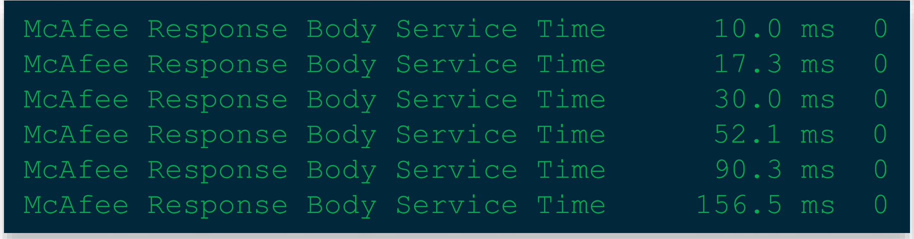




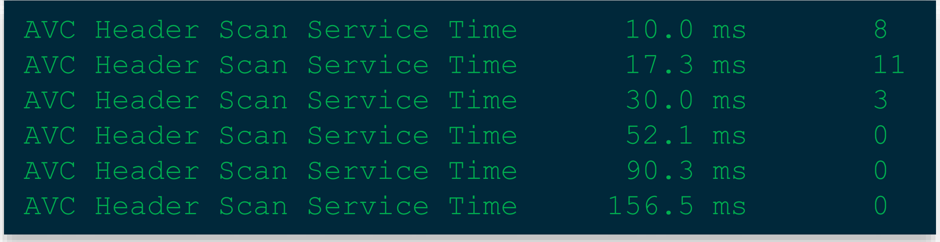
```
Sophos Response Body Service Time        10.0 ms  0
Sophos Response Body Service Time        17.3 ms  0
Sophos Response Body Service Time        30.0 ms  0
Sophos Response Body Service Time        52.1 ms  0
Sophos Response Body Service Time        90.3 ms  0
Sophos Response Body Service Time       156.5 ms  0
```



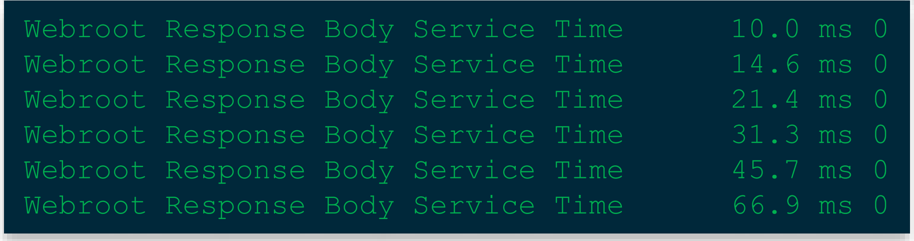
```
Adaptive Scanning Service Time          1.0 ms     2
Adaptive Scanning Service Time          1.6 ms     0
Adaptive Scanning Service Time          2.5 ms     0
Adaptive Scanning Service Time          4.0 ms     0
Adaptive Scanning Service Time          6.3 ms     0
Adaptive Scanning Service Time         10.0 ms     0
```



```
McAfee Response Body Service Time        10.0 ms  0
McAfee Response Body Service Time        17.3 ms  0
McAfee Response Body Service Time        30.0 ms  0
McAfee Response Body Service Time        52.1 ms  0
McAfee Response Body Service Time        90.3 ms  0
McAfee Response Body Service Time       156.5 ms  0
```



```
AVC Header Scan Service Time          10.0 ms      8
AVC Header Scan Service Time          17.3 ms      11
AVC Header Scan Service Time          30.0 ms      3
AVC Header Scan Service Time          52.1 ms      0
AVC Header Scan Service Time          90.3 ms      0
AVC Header Scan Service Time         156.5 ms      0
```

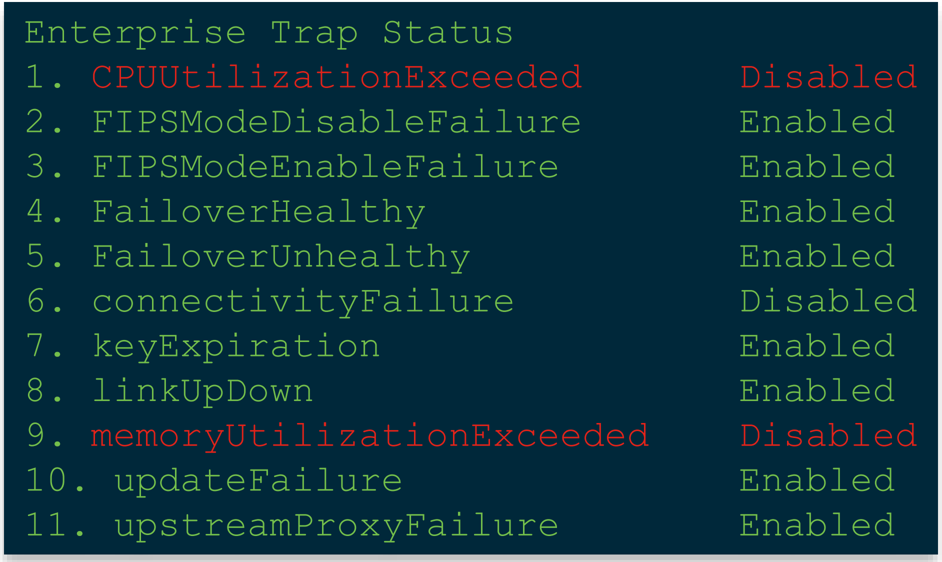


```
Webroot Response Body Service Time       10.0 ms 0
Webroot Response Body Service Time       14.6 ms 0
Webroot Response Body Service Time       21.4 ms 0
Webroot Response Body Service Time       31.3 ms 0
Webroot Response Body Service Time       45.7 ms 0
Webroot Response Body Service Time       66.9 ms 0
```

See the user guide for all of the available custom fields associated with these values

SNMP performance monitoring

- Traditional method for monitoring the WSA
- Performance MIB
  - OID 1.3.6.1.4.1.15497.1.2
- Traps are mostly hardware related



```
Enterprise Trap Status
1. CPUUtilizationExceeded        Disabled
2. FIPSModeDisableFailure        Enabled
3. FIPSModeEnableFailure         Enabled
4. FailoverHealthy               Enabled
5. FailoverUnhealthy             Enabled
6. connectivityFailure           Disabled
7. keyExpiration                 Enabled
8. linkUpDown                    Enabled
9. memoryUtilizationExceeded     Disabled
10. updateFailure                Enabled
11. upstreamProxyFailure         Enabled
```

Disk performance

- Lower end hardware and WBRS
  - S160/S170/S190 pre-11.7 required extending the update interval
  - 11.7 provides better performance for WBRS updates
- ipcheck CLI command shows free disk space
- Reporting engines could be backed up
  - Offloading to an SMA helps
  - Disable reporting via diagnostic CLI command for diagnostic purposed

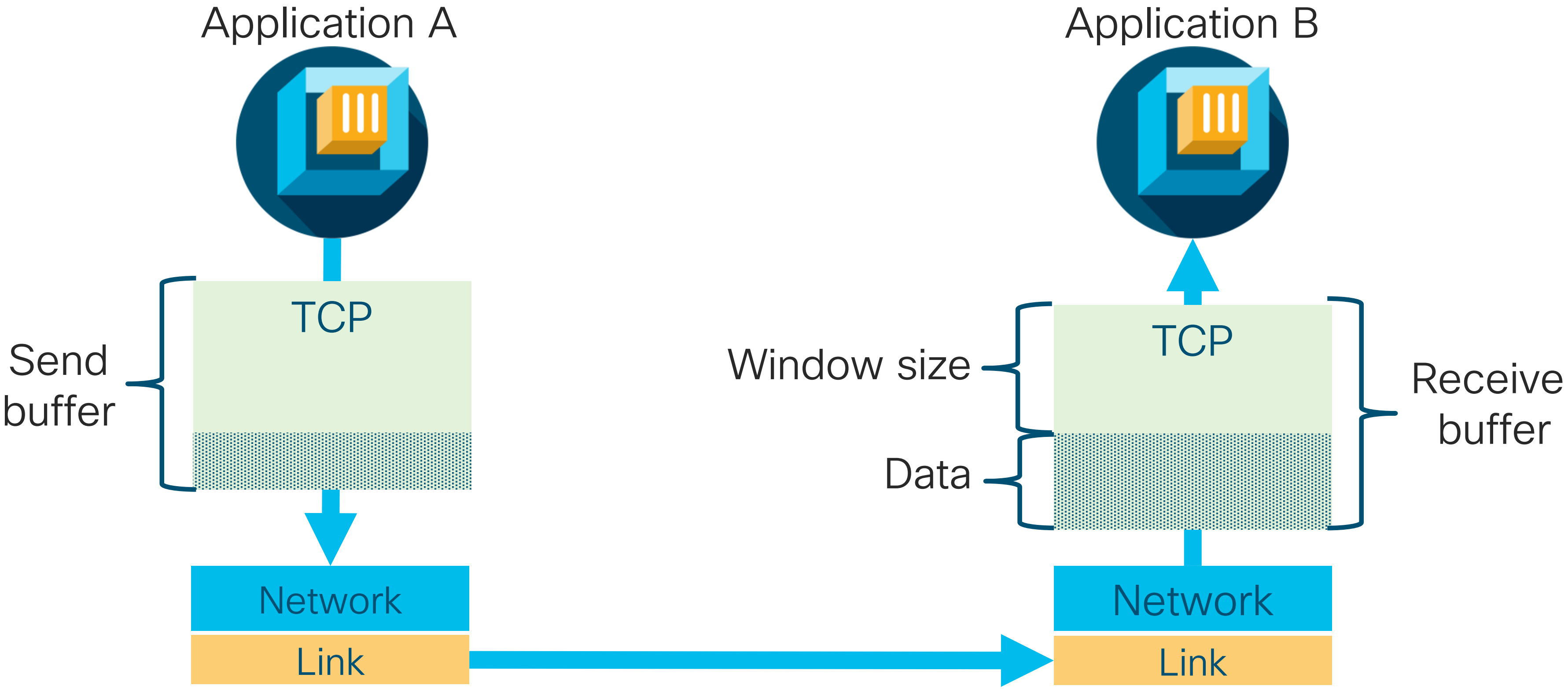
    diagnostic > reporting > DISABLE

Network tuning

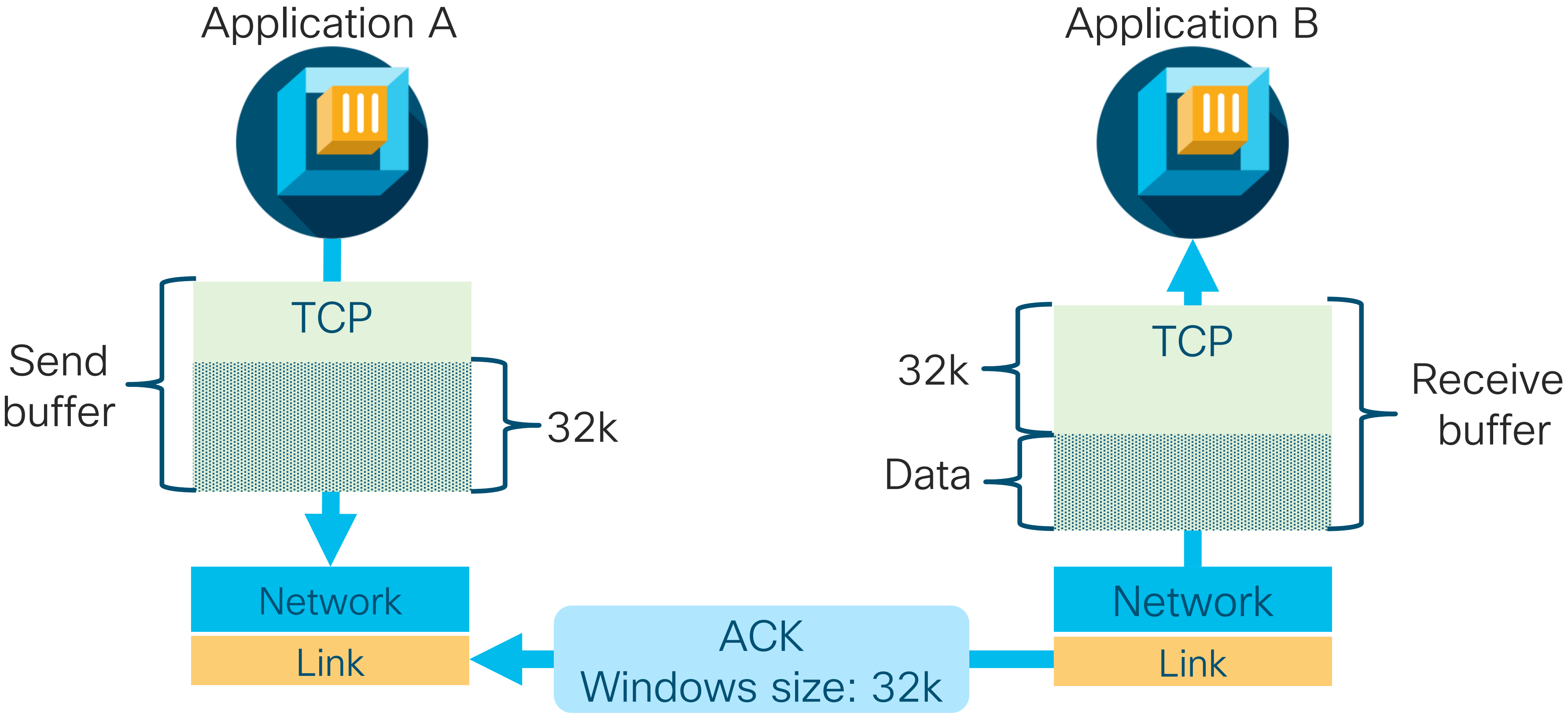
Be careful!

```
>networktuning

Choose the operation you want to perform:

- SENDSPACE - TCP sendspace (8192-262144) default 32768
- RECVSPACE - TCP recvspace (8192-262144) default 65536
- SEND_AUTO - TCP send autotuning (ON=1/OFF=0) default OFF
- RECV_AUTO - TCP receive autotuning (ON=1/OFF=0) default OFF
- MBUF_CLUSTER_COUNT - number of mbuf clusters (98304,147132) Default 98304
- SENDBUF_MAX - Maximum send buf, size(131072 - 262144) default, 256K=262144
- RECVBUF_MAX - Maximum recv buf,  size(131072 - 262144) default, 256K=262144
- CLEAN_FIB_1 - Remove all M1/M2 entries from Data routing table
```

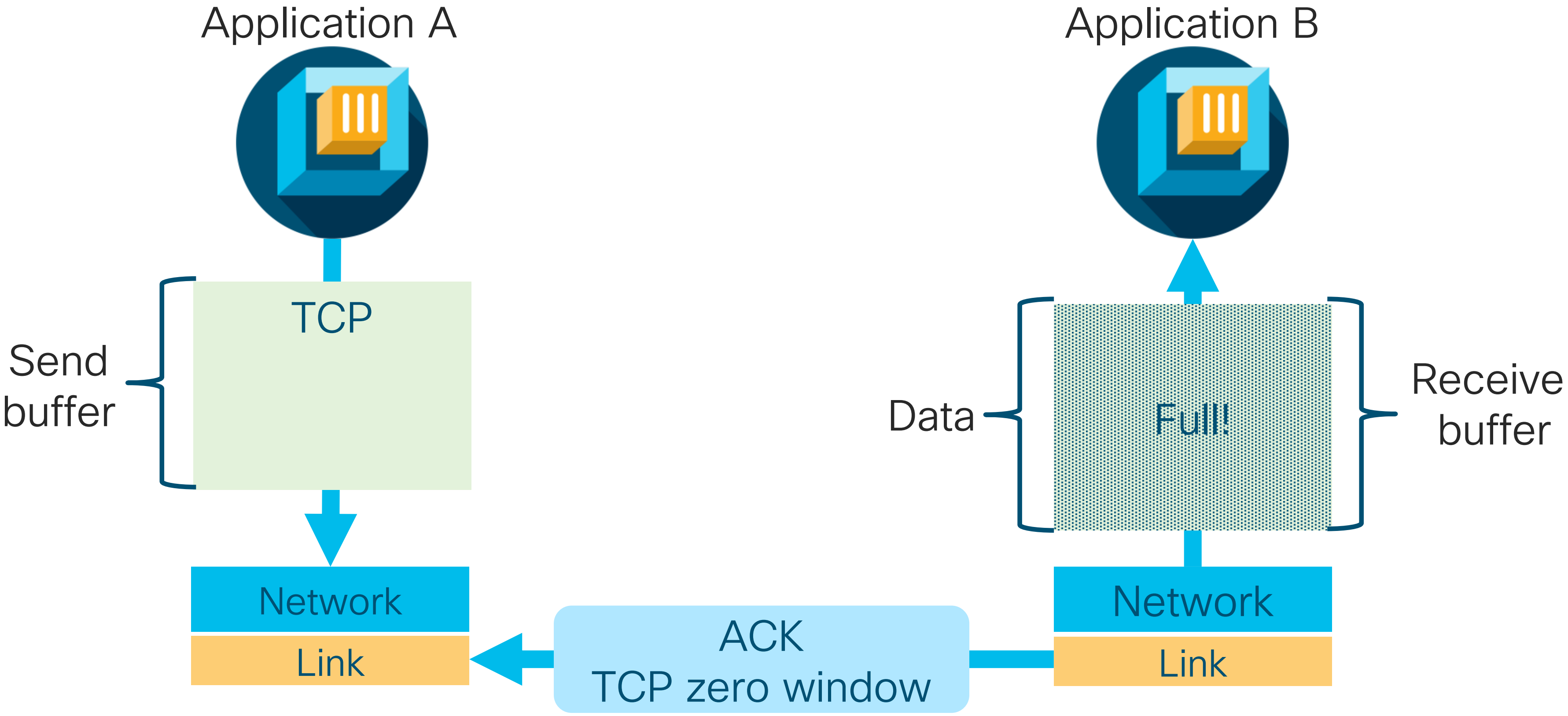
TCP flow control



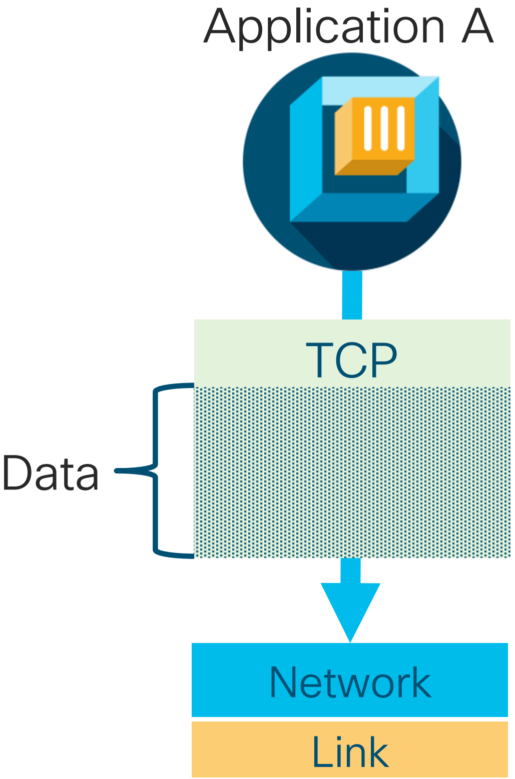
TCP flow control



TCP flow control



Buffer tuning



- Data remains in the send buffer until ACK’d in case retransmission is required
- Limits how many packets can be in flight at once time
- Too small: performance is limited
- Too large: memory usage is high
- Should be set as closely as possible to the bandwidth delay product
    - Link capacity (bits) x round-trip time (seconds)

Network tuning recommendations

Aggressive settings – your mileage may vary

Model	Memory	SEND-AUTO & RECV-AUTO	Dynamic window control	SENDSPACE	RECVSPACE	MBUF CLUSTER COUNT
S000v, S100v, S170, S370	4GB	ON	NO	32768-65536	32768-65536	98304
S370, S190, S300v	8GB	ON	NO	65536	65536	196608
S680, S390	16GB	ON	NO	131072	131072	393216
S690	32GB	ON	NO	131072	131072	786432/1572864
S690/695	64GB	ON	NO	131072	131072	1572864

```
advancedproxyconfig > MISCELLANEOUS
Would you like proxy to perform dynamic adjustment of TCP receive window size?
[Y]>N
Would you like proxy to perform dynamic adjustment of TCP send window size?
[Y]>N
```

Conclusion

- Start your move to Kerberos
- Check your DNS settings
  - TTL = 300 seconds
- Integrate!
  - ISE / ISE-PIC
  - AMP / Threat Grid
  - Cognitive Threat Analytics
  - Cisco Threat Response

- Add some custom fields to your accesslogs
  - `%m` : Auth mechanism
  - `%g` : User groups
- Start capturing your track_stats logs
- Reach out!
  - Catch me in the hall
  - chclasen@cisco.com

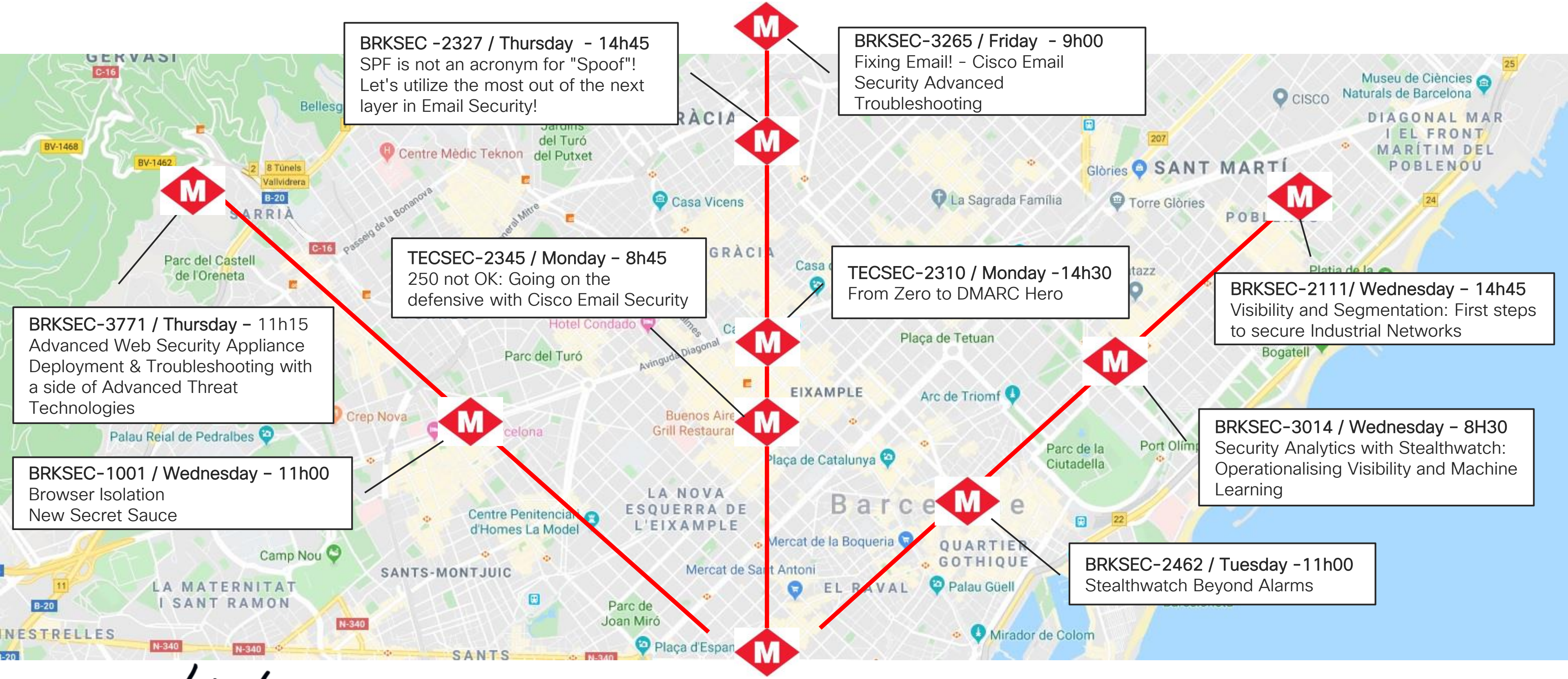
Security Beta Programs

What's in it for you?

- Direct link to product development!
- Private weekly calls with the product team
- New feature training; TAC support
- Free beta loaners for customer test labs
- Ensure your bugs are fixed by GA
- Send an email to wsa-beta@cisco.com to reserve your spot

> *"I feel a personal attachment to your company through the Beta testing we do…. You guys are listening to us…, and you don't realize how rare that is."*
>
> – Government Insurance Company

EMAIL, Web Security and Visibility Learning maps



BRKSEC -2327 / Thursday - 14h45
SPF is not an acronym for "Spoof"!
Let's utilize the most out of the next layer in Email Security!

BRKSEC-3265 / Friday - 9h00
Fixing Email! - Cisco Email Security Advanced Troubleshooting

TECSEC-2345 / Monday – 8h45
250 not OK: Going on the defensive with Cisco Email Security

TECSEC-2310 / Monday -14h30
From Zero to DMARC Hero

BRKSEC-3771 / Thursday – 11h15
Advanced Web Security Appliance Deployment & Troubleshooting with a side of Advanced Threat Technologies

BRKSEC-2111/ Wednesday – 14h45
Visibility and Segmentation: First steps to secure Industrial Networks

BRKSEC-1001 / Wednesday – 11h00
Browser Isolation
New Secret Sauce

BRKSEC-3014 / Wednesday – 8H30
Security Analytics with Stealthwatch: Operationalising Visibility and Machine Learning

BRKSEC-2462 / Tuesday -11h00
Stealthwatch Beyond Alarms

Questions?

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco campus
- Walk-in labs
- Meet the engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**