

The background features a vibrant, abstract design with a color gradient from dark blue on the left to bright yellow and white on the right. The design consists of overlapping, wavy horizontal bands and a radial pattern of lines emanating from a bright white point on the right side, creating a sense of motion and energy.

CISCO *Live!*

Let's go

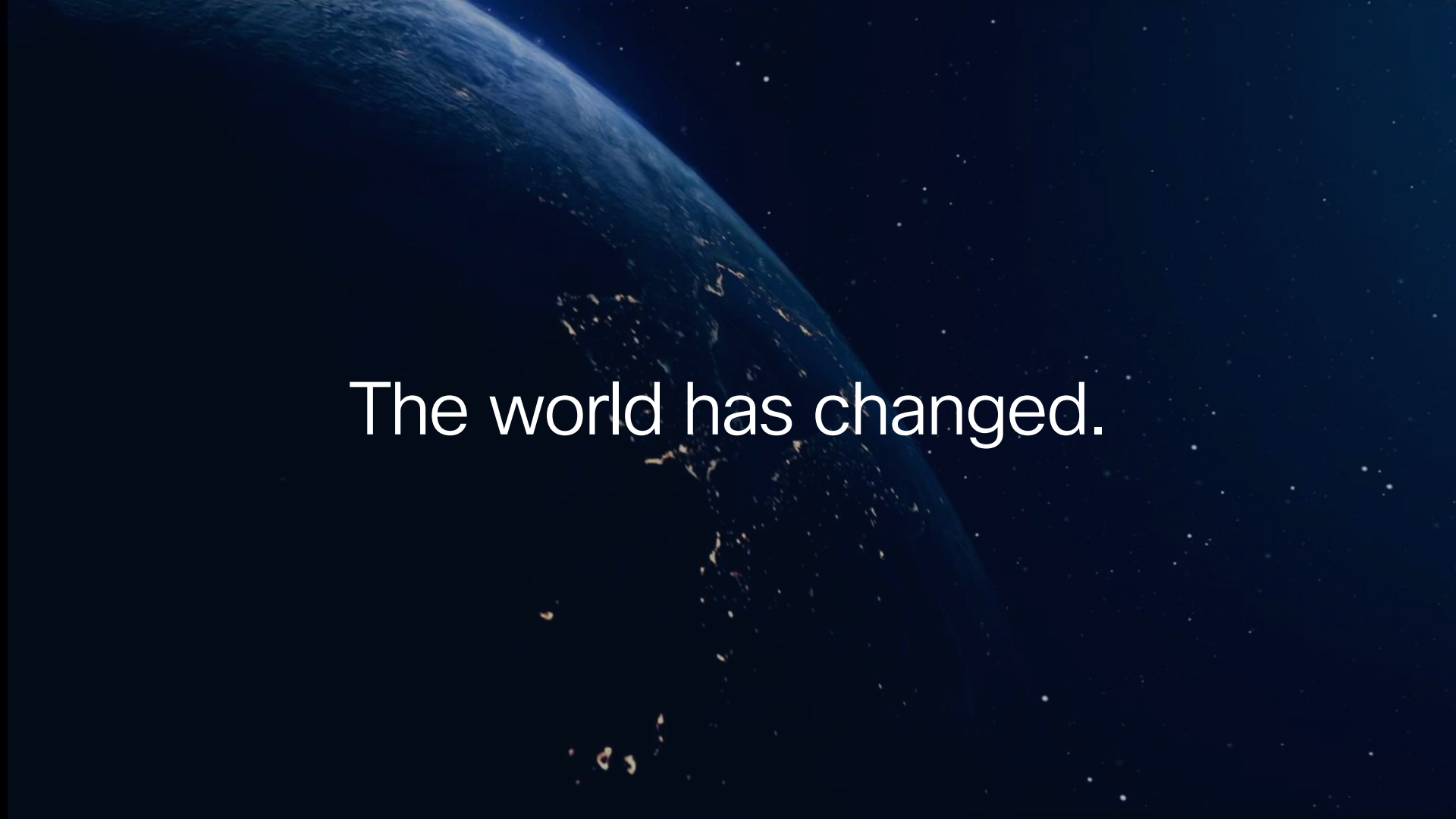


The bridge to possible

Who is Behind the Umbrella?

A View on User Authentication with Cisco Umbrella

Julia Sevostianova, Technical Projects Systems Engineer

A high-contrast, low-angle view of Earth from space. The dark blue, curved horizon of the planet dominates the left and center of the frame. Below the horizon, the silhouettes of continents are visible, with numerous small, bright yellow and orange lights representing city lights at night. The background is a deep, dark blue space filled with many small, distant stars.

The world has changed.



of high-growth organizations have enabled productivity anywhere workforce models.

Accenture Future of Work Study 2021



of employees would likely look for another job if their employer didn't offer hybrid work options.

Cisco Hybrid Work Index 2022



of those who work remotely at least a few times per month show increased productivity.

ConnectSolutions study 2022

➡ the pressure on IT and facilities teams to deliver effective technologies is higher than ever.

Session abstract

Controlling access is the basis of all security.

Is it possible to have the same level of granularity of access policies for roaming users as we used to have for users in the office?

What user authentication options do we have in Umbrella?

Can a third-party identity provider be used?

This session intends to demonstrate types of user authentication methods supported by Umbrella and walk the participants through authentication use cases.

Your speaker



Julia Sevostianova

Technical Projects Systems Engineer in
dCloud

previously TAC engineer & security consultant
7 years in Cisco, 11 years in IT

CCIE (RS & Security) #53290

For Your Reference

- There are slides in your print-outs that will not be presented.
- They are there “For your Reference”



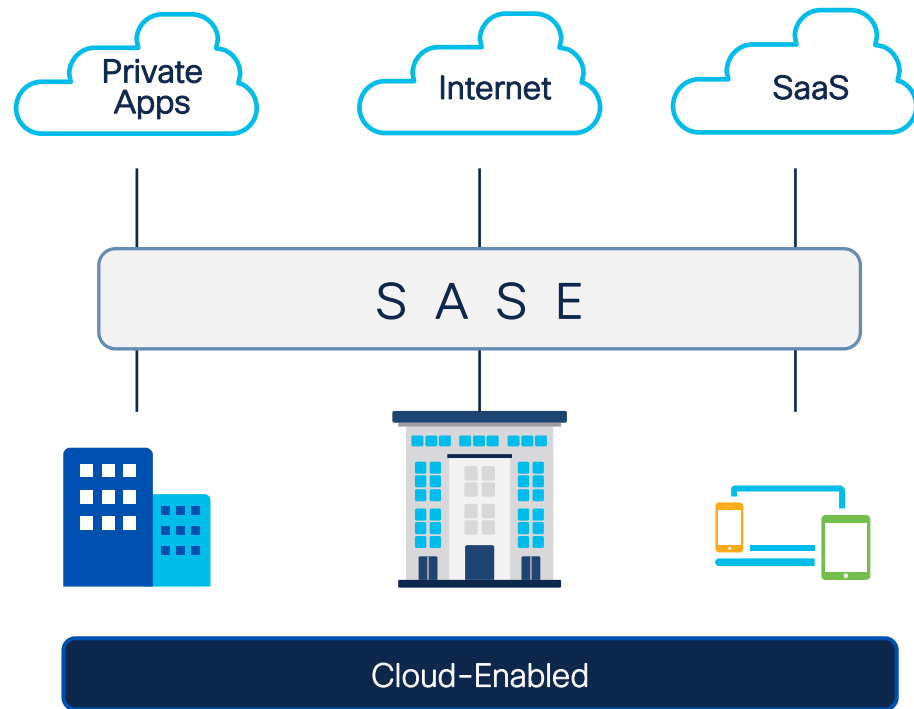
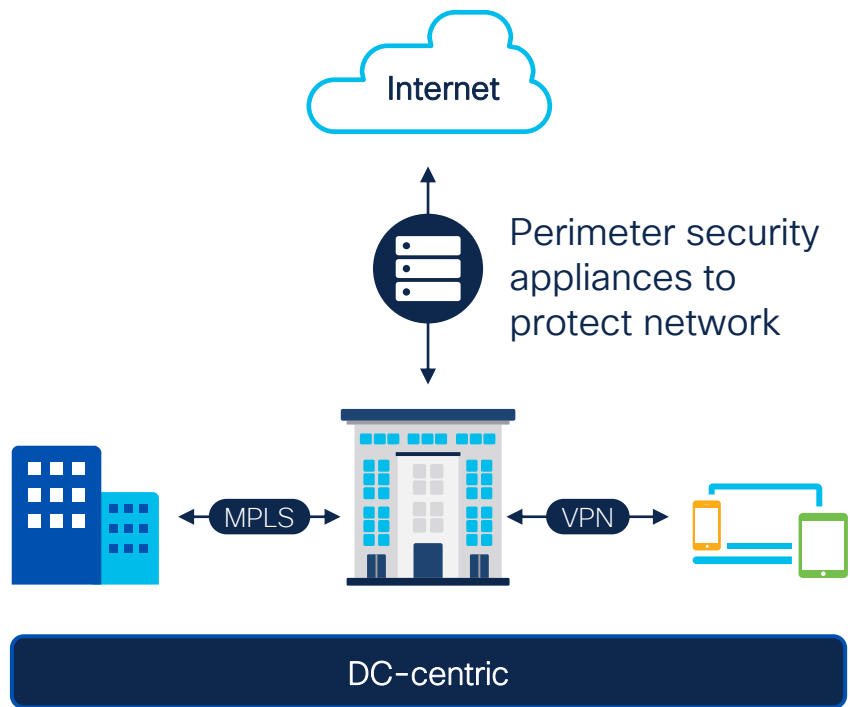
For Your
Reference

Agenda

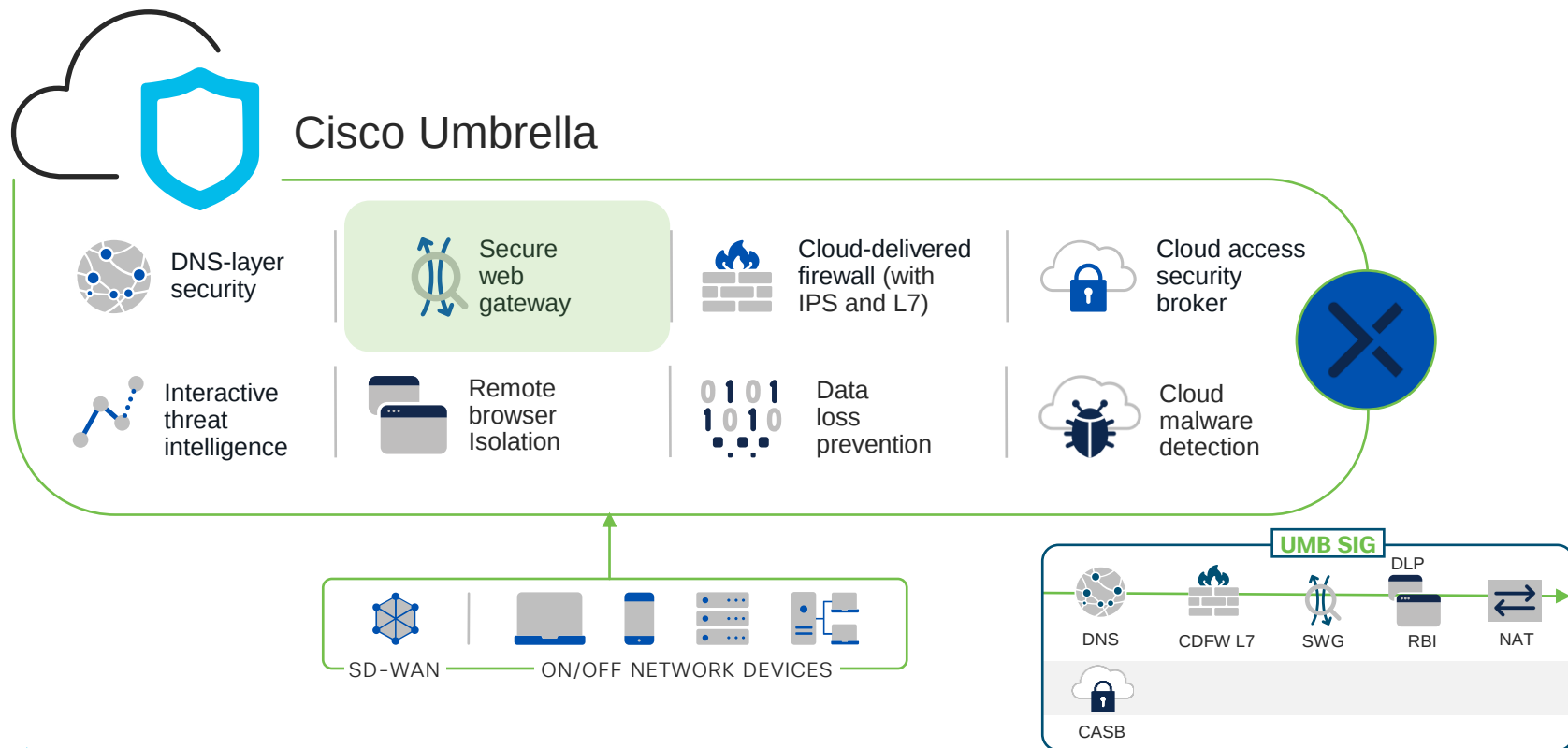
- Umbrella for Beginners
- Traffic Flow: User Authentication
- What a Proxy Needs to Know?
- Authentication Methods:
 - SAML
 - Remote User
 - Seamless Identity
- Headers in Authentication Process
- Key take aways

Umbrella for Beginners

From DC-centric topology to SASE



Cisco Umbrella - SIG overview



Enforcement that works together

Layered approach

1. DNS-layer security

First check for domains associated with malware

2. Cloud-delivered firewall (CDFW)

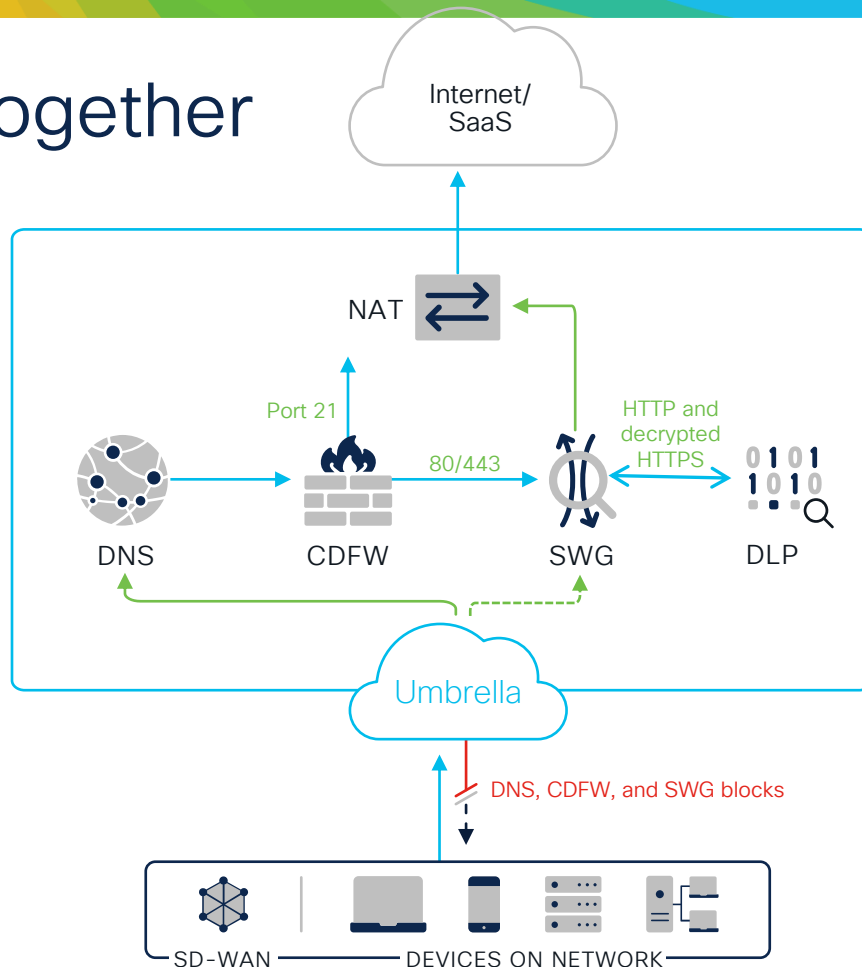
Next check for IP, port, protocol and application rules

3. Secure web gateway (SWG)

Final check of all web traffic for malware and policy violations

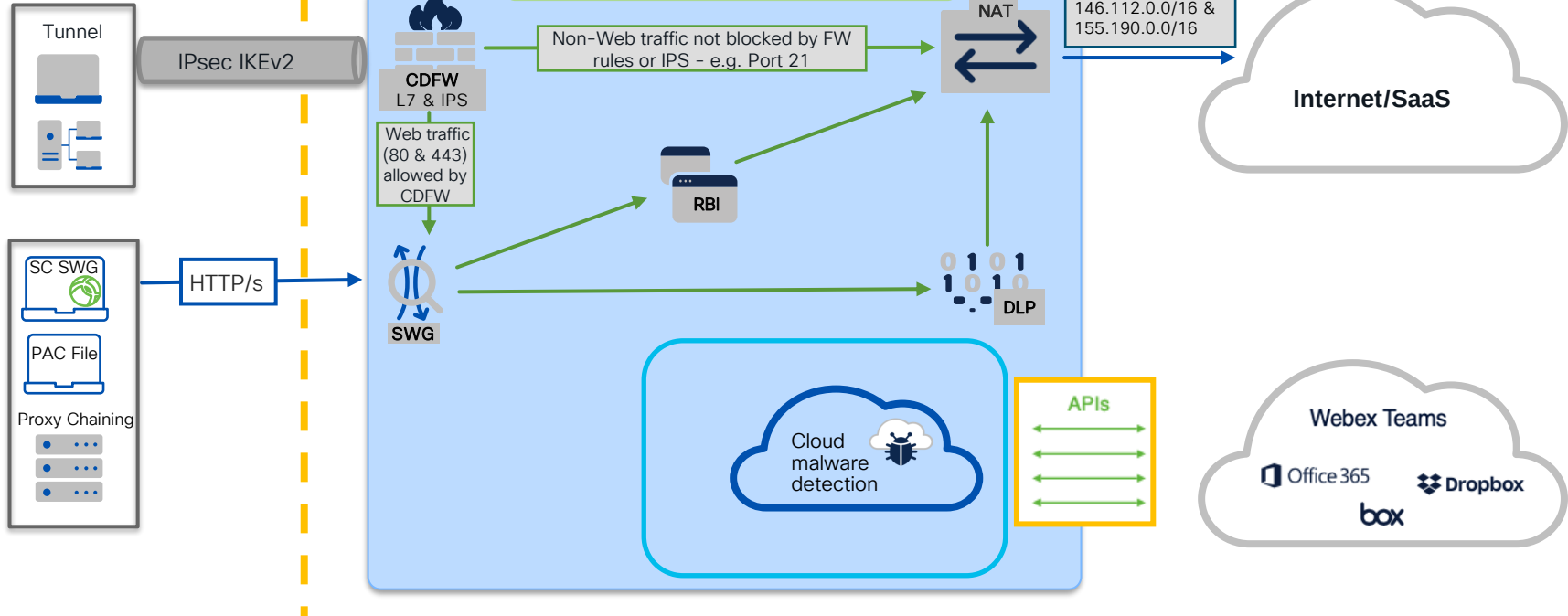
4. Data loss prevention (DLP)

Monitoring and/or blocking of sensitive data in outbound web traffic



SIG Deployment Types & Traffic Flow Diagram

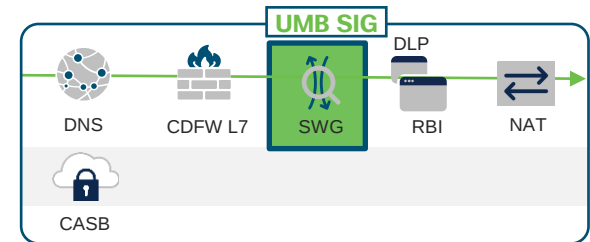
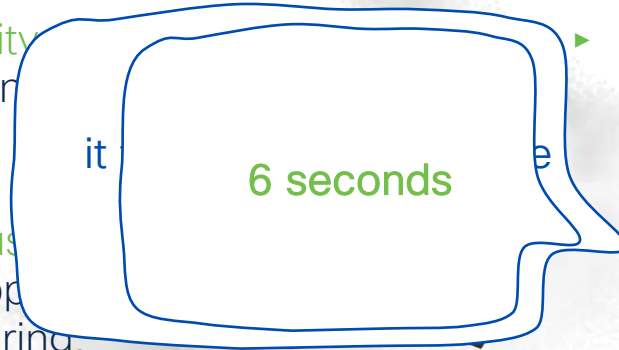
Redirection Methods



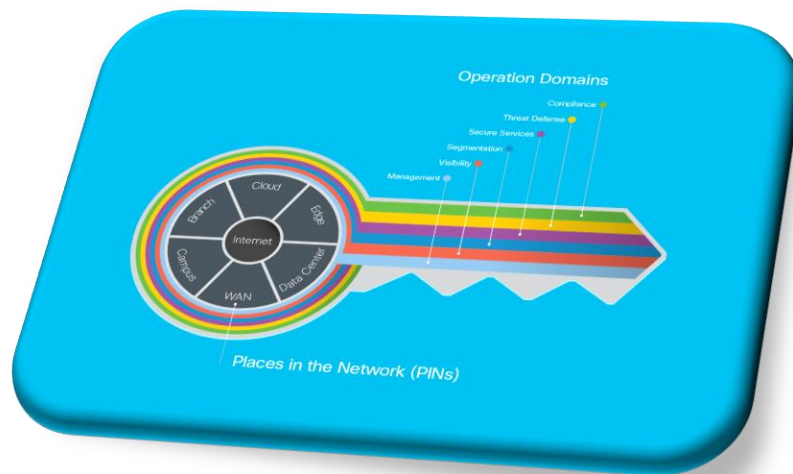
Secure web gateway: full web proxy

Deep inspection and control of web traffic

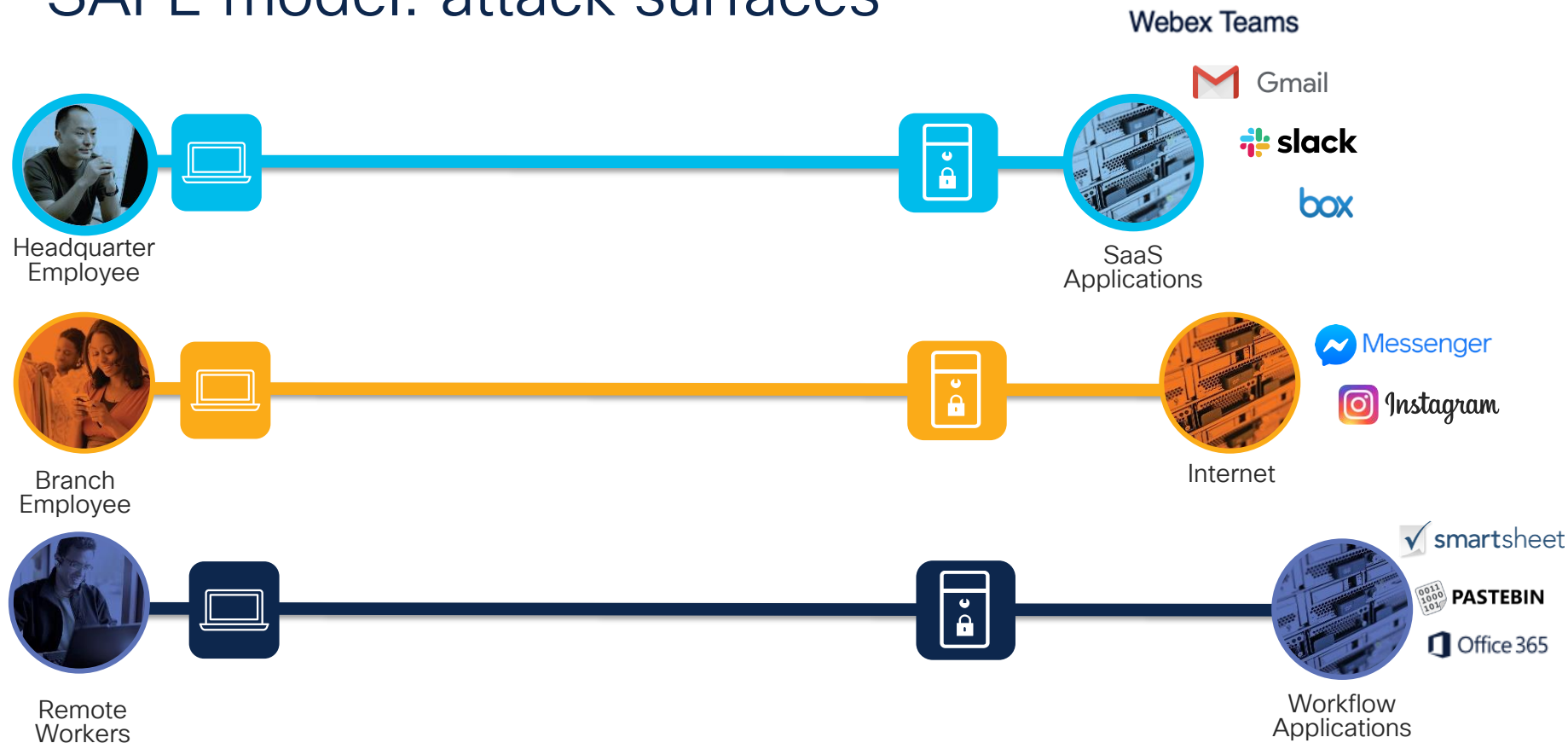
- ▶ Gain additional visibility via full URL logging and cloud app discovery
- ▶ Enforce acceptable use policy via granular app controls, content filtering, and URL block/allow lists
- ▶ Extend protection against malware via SSL decryption and file inspection
- ▶ Enrich file inspection (with retrospective alerts) via malware defense and analytics



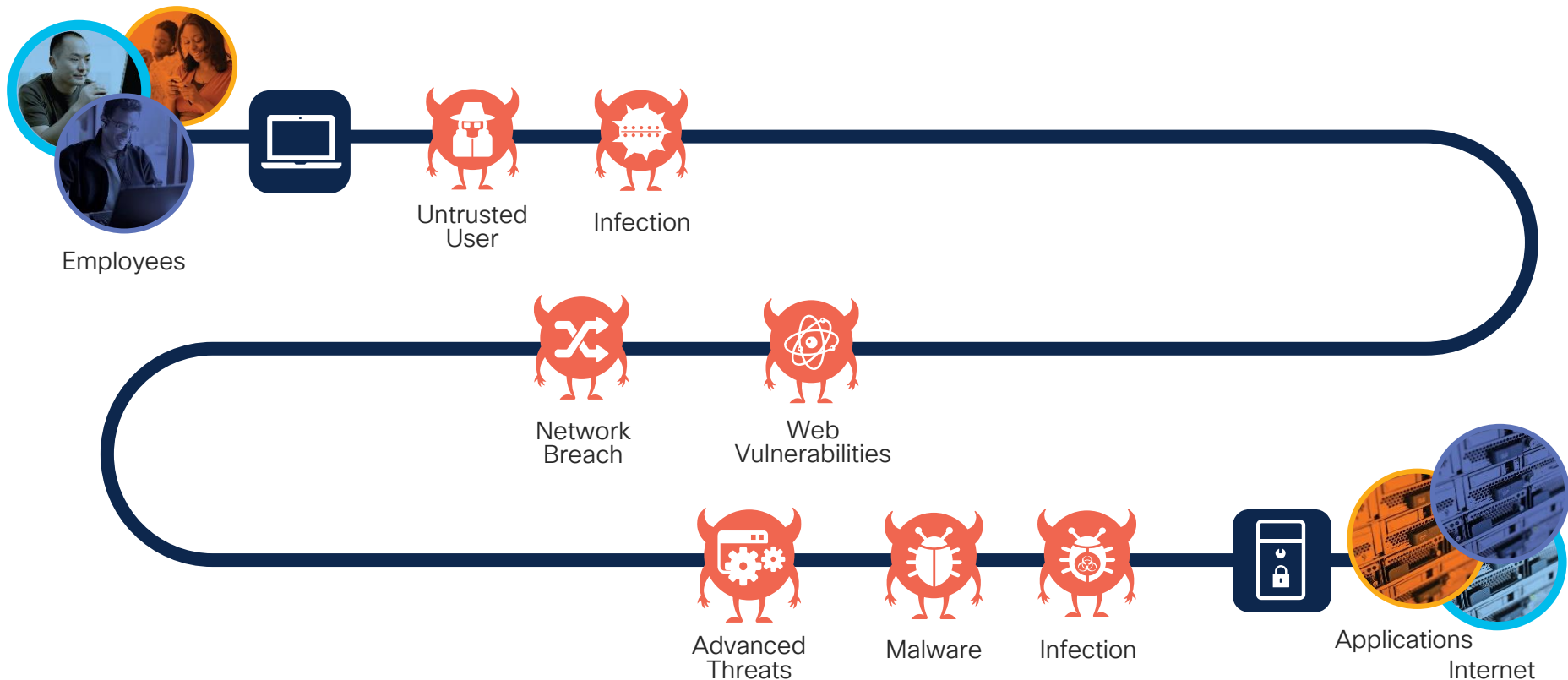
SAFE Framework



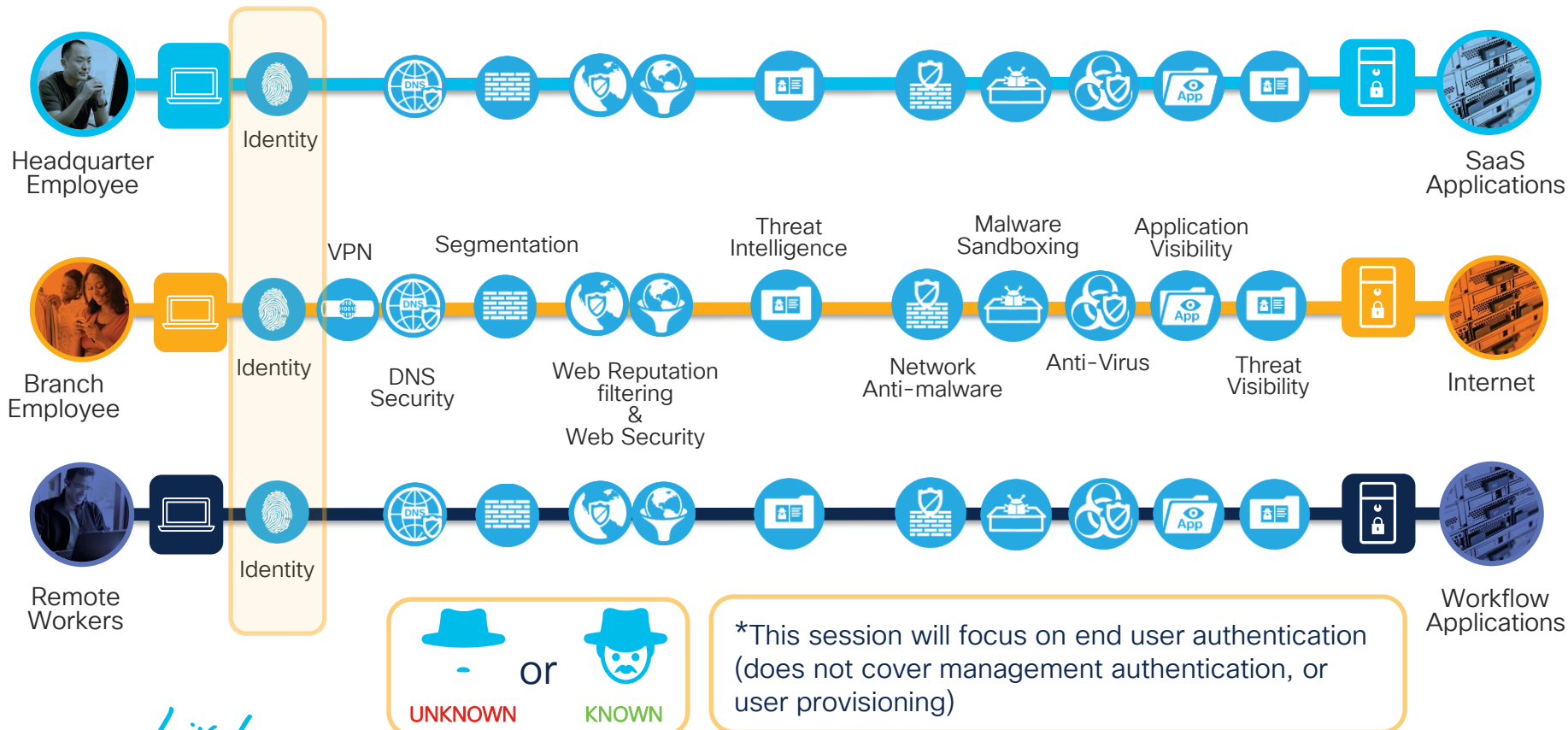
SAFE model: attack surfaces



SAFE model: threats

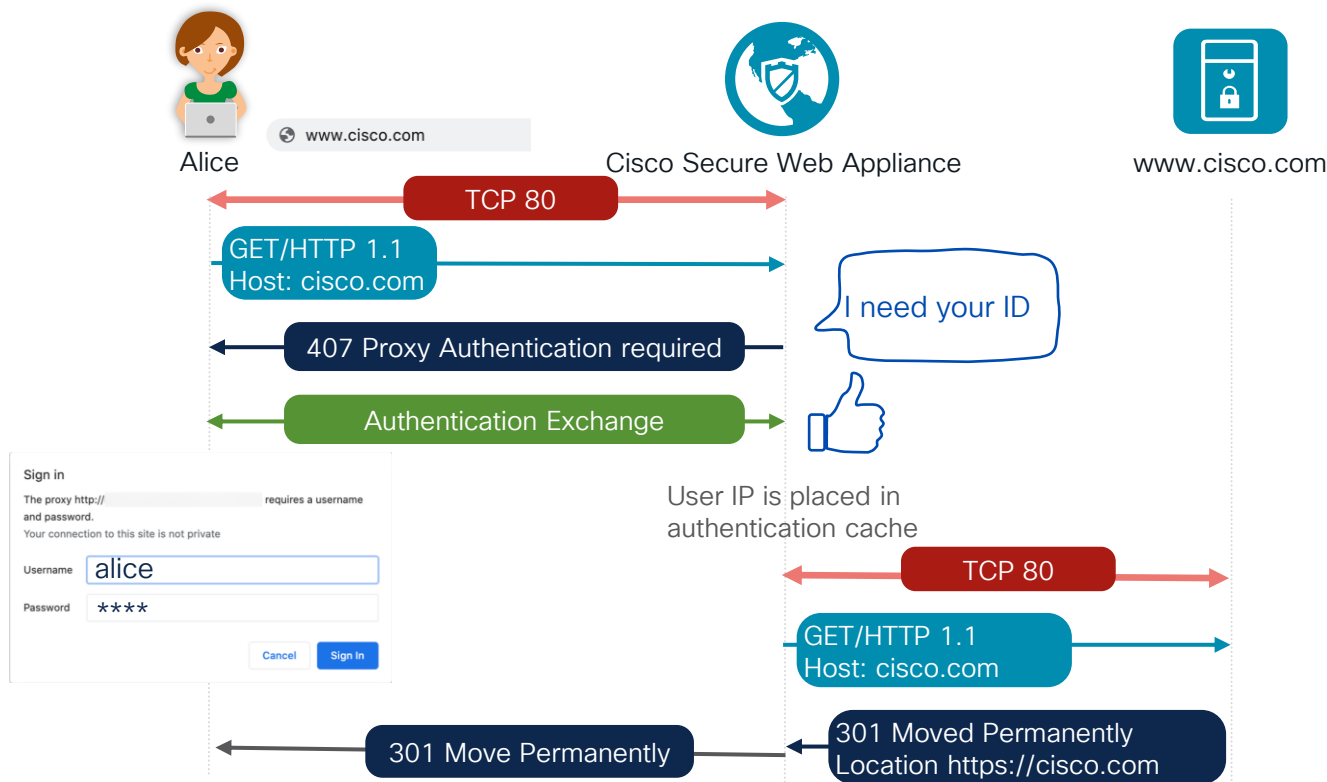


We will focus on User Identity



Traffic Flow: User Authentication

How proxy authenticates a user: explicit mode example



How proxy authenticates a user: explicit mode example



Alice's computer sends an HTTP GET request to the proxy.

```
hyperText Transfer Protocol
> GET http://cisco.com/ HTTP/1.1\r\n
Host: cisco.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
```

Destination IP address:

Secure Web Appliance IP

Requested resource:

<http://www.cisco.com>

Host header:

cisco.com

How proxy authenticates a user: explicit mode example



Secure Web Appliance responds with a 407 proxy authentication request.

```
> HTTP/1.1 407 Proxy Authentication Required\r\n
  Mime-Version: 1.0\r\n
  Date: Thu, 19 Jan 2023 12:31:40 GMT\r\n
  Via: 1.1 wsa.dcloud.cisco.com:80 (Cisco-WSA/14.5.0-537)\r\n
  Content-Type: text/html\r\n
  Proxy-Authenticate: Negotiate\r\n
  Proxy-Authenticate: NTLM\r\n
  Proxy-Authenticate: Basic realm="Cisco IronPort Web Security Appliance"\r\n
  Connection: close\r\n
  Proxy-Connection: close\r\n
> Content-Length: 2121\r\n
~ ~ ~
```

Includes **proxy authentication headers**. In this example it shows that Alice is allowed to authenticate using Kerberos which is mentioned as negotiate or NTLM, or Basic.

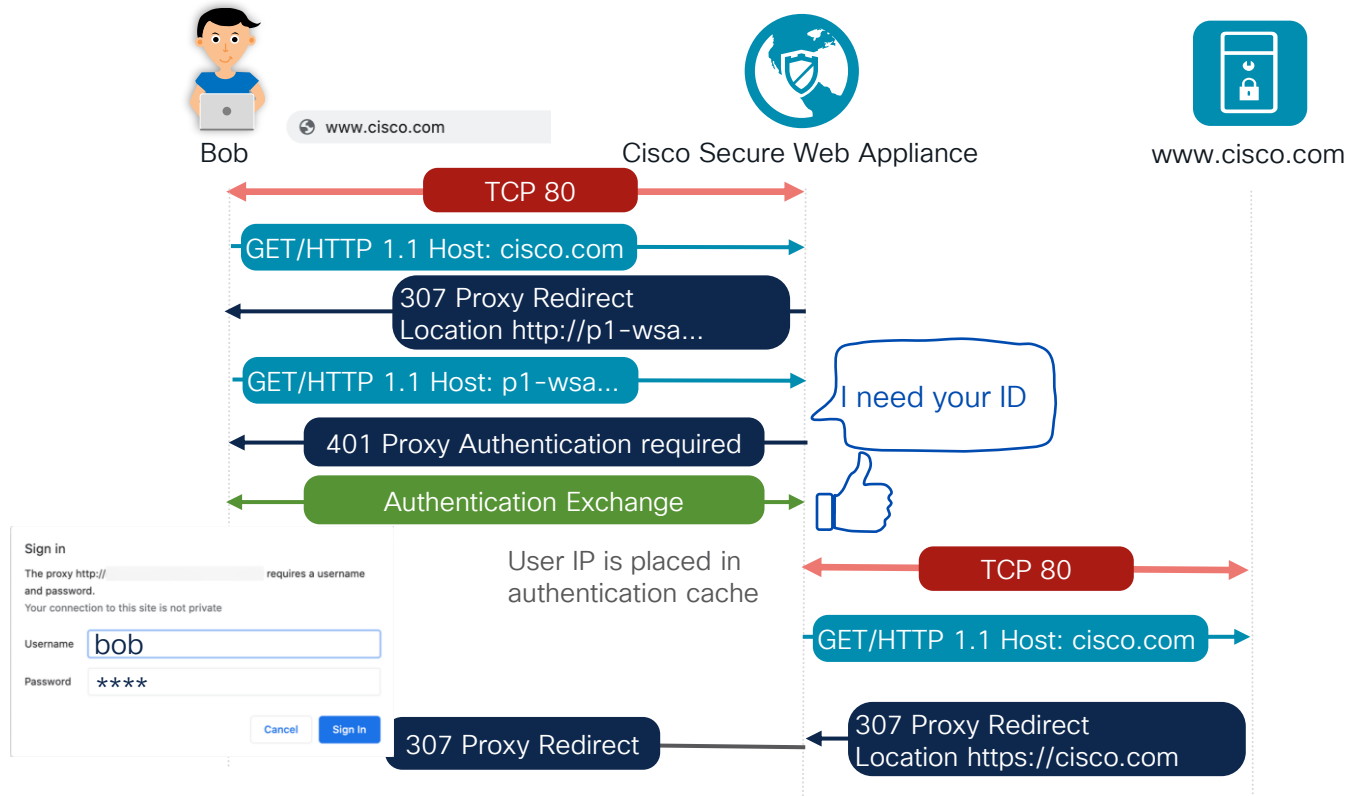
How proxy authenticates a user: explicit mode example



Since Alice only typed cisco.com and not https cisco.com, the server will return **301 Moved Permanently** that **upgrades** the connection to **HTTPS** and requires the TLS handshake before any data is exchanged.

```
Hyper-Text Transfer Protocol
> HTTP/1.1 301 Moved Permanently\r\n
  Location: https://cisco.com/\r\n
  Cache-Control: no-cache\r\n
  Pragma: no-cache\r\n
  Transfer-Encoding: chunked\r\n
  Date: Thu, 19 Jan 2023 12:31:45 GMT\r\n
  Via: 1.1 wsa.dcloud.cisco.com:80 (Cisco-WSA/14.5.0-537)\r\n
  Connection: close\r\n
  Proxy-Connection: close\r\n
  \r\n
```

How proxy authenticates a user: transparent mode example



How proxy authenticates a user: transparent mode example



When Bob types cisco.com into his browser, his computer makes a TCP connection to what it thinks is cisco.com. TCP SYN packet is redirected to the Secure Web Appliance.
Bob sends the **HTTP GET** request for cisco.com

```
▼ Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.cisco.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.cisco.com/]
    [HTTP request 1/1]
    [Response in frame: 195]
```

Destination IP address:

cisco.com IP

Requested resource:

http://www.cisco.com

Host header:

cisco.com

How proxy authenticates a user: transparent mode example



Secure Web Appliance responds with a 307 temporary redirect which contains a unique **location header**.

This header redirects Bob to the configured **redirect hostname** of the proxy, which is built with a **path from the UID**, Bob's IP address and the **originally requested site**.

```
▼ Hypertext Transfer Protocol
> HTTP/1.1 307 Proxy Redirect\r\n
  Mime-Version: 1.0\r\n
  Date: Thu, 19 Jan 2023 20:23:14 GMT\r\n
  Via: 1.1 wsa.dcloud.cisco.com:80 (Cisco-WSA/14.5.0-537)\r\n
  Content-Type: text/html\r\n
  Cache-Control: no-cache\r\n
  Location: http://wsa.dcloud.cisco.com/B0001D0000N0001N0001F0000S0000R0004/198.19.10.15/http://www.cisco.com/\r\n
  Connection: close\r\n
> Content-Length: 1857\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.012453000 seconds]
```

How proxy authenticates a user: transparent mode example



The Secure Web Appliance responds with a 401 Authorization Required that offers the available authentication mechanisms as the **authenticate headers**.

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 401 Authorization Required\r\n
    Mime-Version: 1.0\r\n
    Date: Thu, 19 Jan 2023 20:23:14 GMT\r\n
    Via: 1.1 wsa.dcloud.cisco.com:80 (Cisco-WSA/14.5.0-537)\r\n
    Content-Type: text/html\r\n
    WWW-Authenticate: Negotiate\r\n
    WWW-Authenticate: NTLM\r\n
    WWW-Authenticate: Basic realm="Cisco IronPort Web Security Appliance"\r\n
    Connection: keep-alive\r\n
  > Content-Length: 2195\r\n
    \r\n
```

How proxy authenticates a user: transparent mode example



Since Bob only typed cisco.com and not https cisco.com the server will return a **301 Moved Permanently** that **upgrades** the connection to HTTPS and requires the TLS handshake before any data is exchanged.

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 301 Moved Permanently\r\n
    Server: AkamaiGHost\r\n
    Location: https://www.cisco.com/\r\n
    Expires: Thu, 19 Jan 2023 20:23:17 GMT\r\n
    Cache-Control: max-age=0, no-cache, no-store\r\n
    Pragma: no-cache\r\n
    Date: Thu, 19 Jan 2023 20:23:17 GMT\r\n
    [truncated]Content-Security-Policy: upgrade-insecure-requests; frame-ancest
    Strict-Transport-Security: max-age=31536000\r\n
```

Kerberos

```
HTTP/1.1 407 Proxy Authentication Required\r\n
Mime-Version: 1.0\r\n
Date: Thu, 19 Jan 2023 12:31:40 GMT\r\n
Server: 1.1 wsa.dcloud.cisco.com:80 (Cisco-WSA/14.5.0-537)\r\n
Content-Type: text/html\r\n
Proxy-Authenticate: Negotiate\r\n
Proxy-Authenticate: NTLM\r\n
Proxy-Authenticate: Basic realm="Cisco IronPort Web Security Appliance"\r\n
Connection: close\r\n
Proxy-Connection: close\r\n
> Content-Length: 2121\r\n
...-
```

What a Proxy Needs to Know?

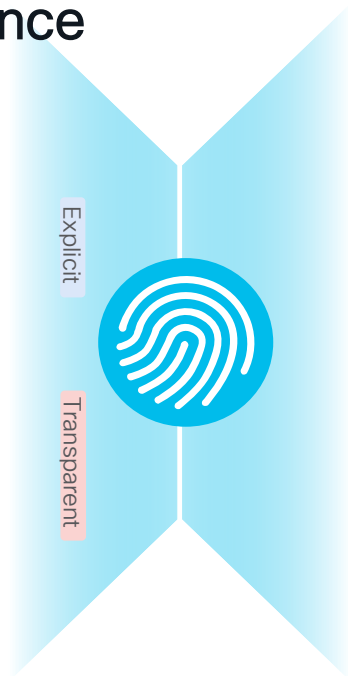
How does Secure Web Appliance and Umbrella SWG define Identity?

Secure Web Appliance

combinations of the following:

- Subnet
- Protocol
- Port
- URL Category
- Authentication Requirements

(Authentication Realm: Basic, NTLM, Kerberos or Transparent Identity-SGT)



Umbrella

WEB policy:

- Networks (or Internal IP in XFF HTTP header)

PAC File Proxy Chaining IPsec tunnel
Cisco Secure Client Roaming Security Module

- Users and Groups

PAC File Proxy Chaining IPsec tunnel
Cisco Secure Client Roaming Security Module

- Roaming Computer

Cisco Secure Client Roaming Security Module

Authentication Methods

We will focus on 3 main authentication types:

- 1 SAML Integrations (Duo, Azure, Okta, ADFS, PingID, etc.)
- 2 Remote User (Secure Client SWG, Umbrella Client)
- 3 Proxy Chaining with **Seamless Identity**

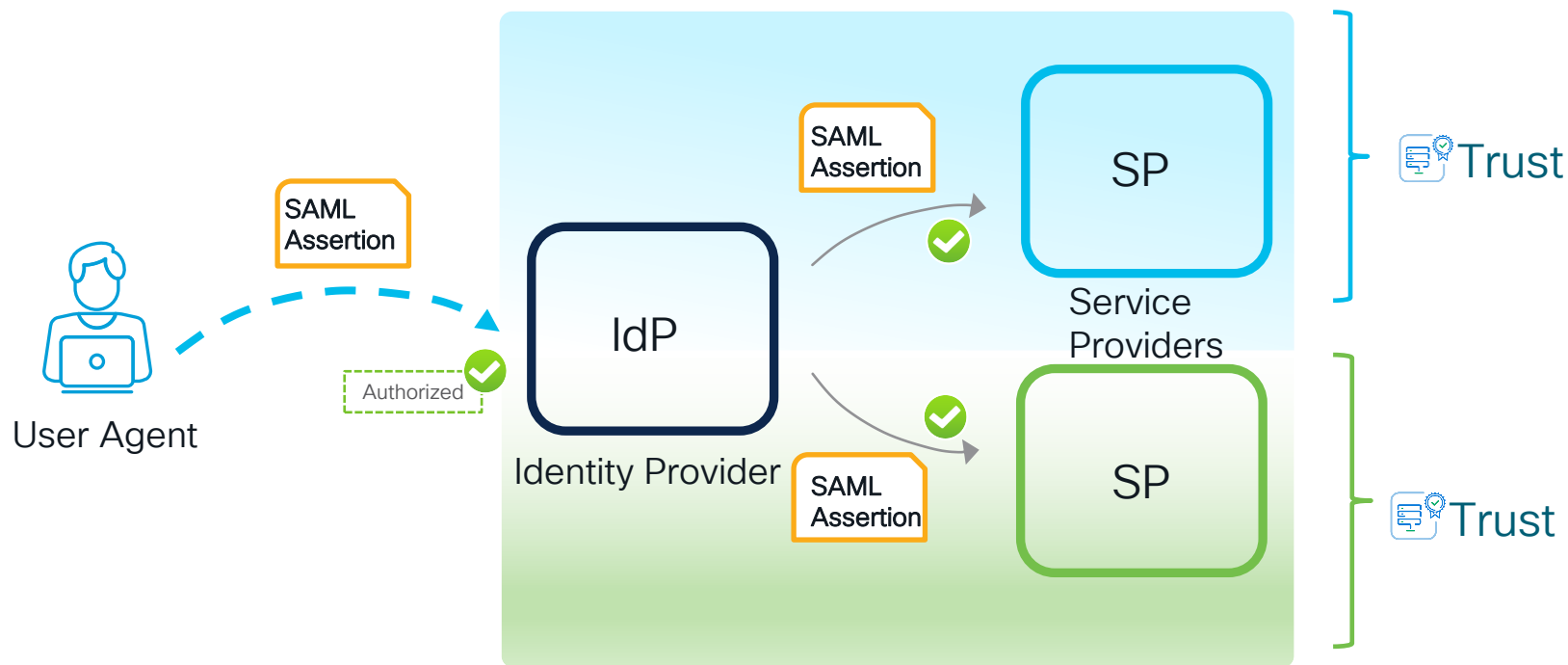
1. SAML

SAML recap

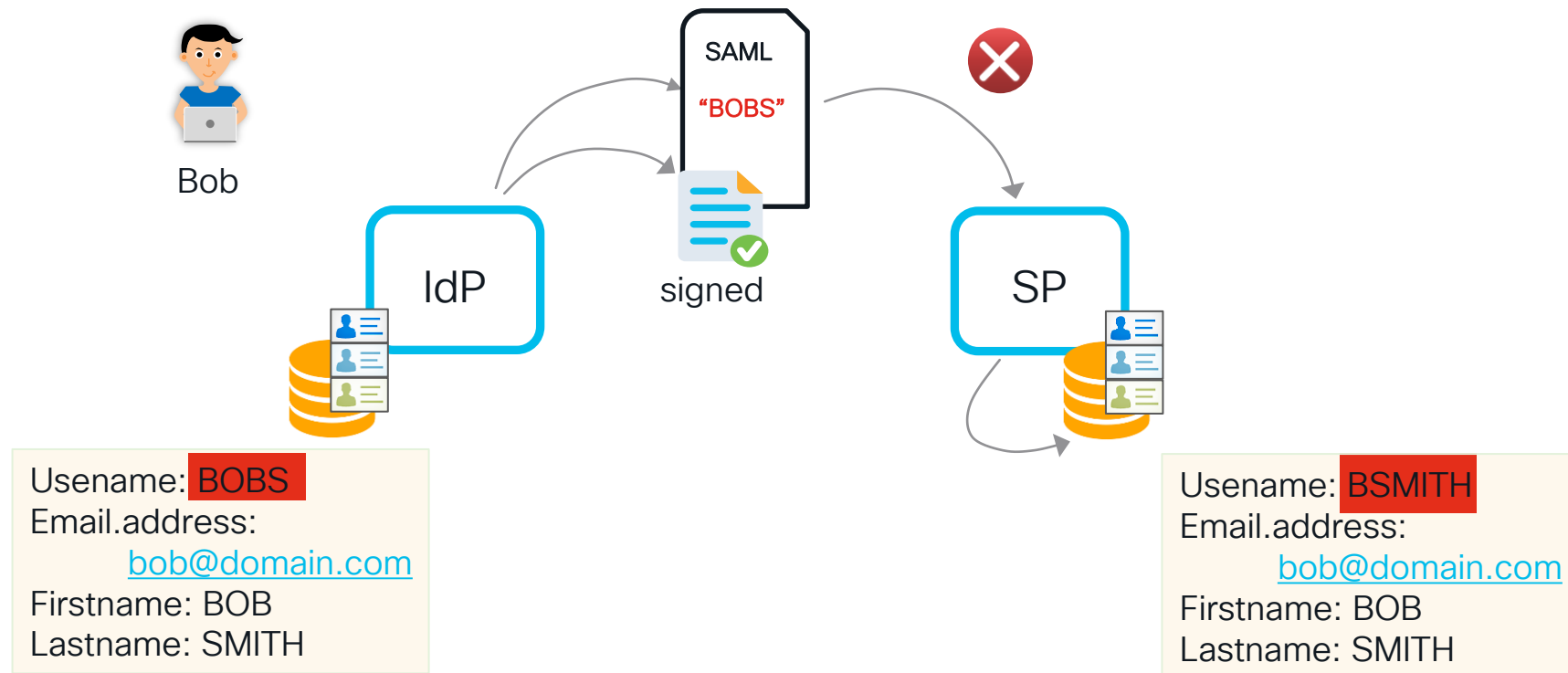
- Security Assertion Markup Language came in 2001
- Current version in use v2.0 (2005)
- SAML is an open standard
- Often used to provide single sign-on to web-based applications



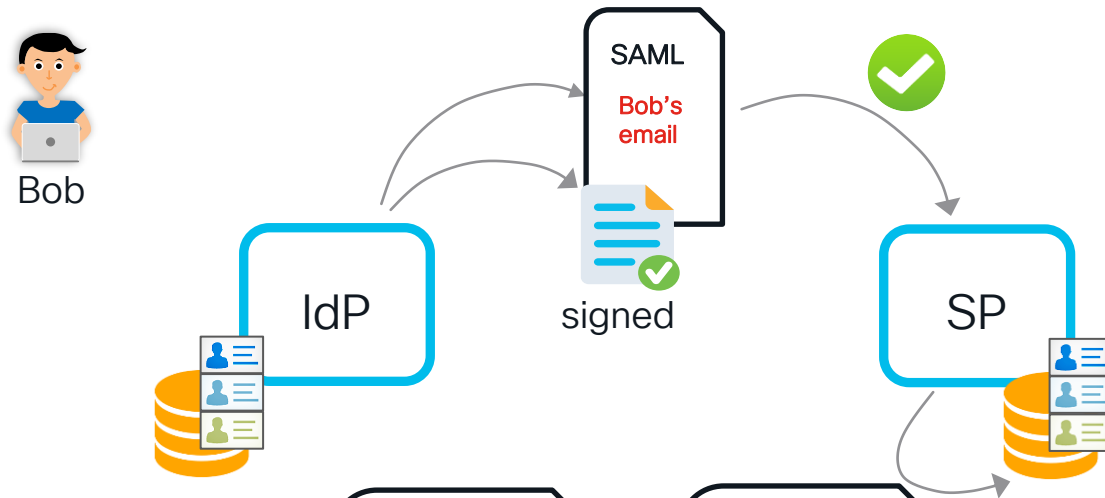
SAML high-level



SAML flow: user ID format



SAML flow: user ID format



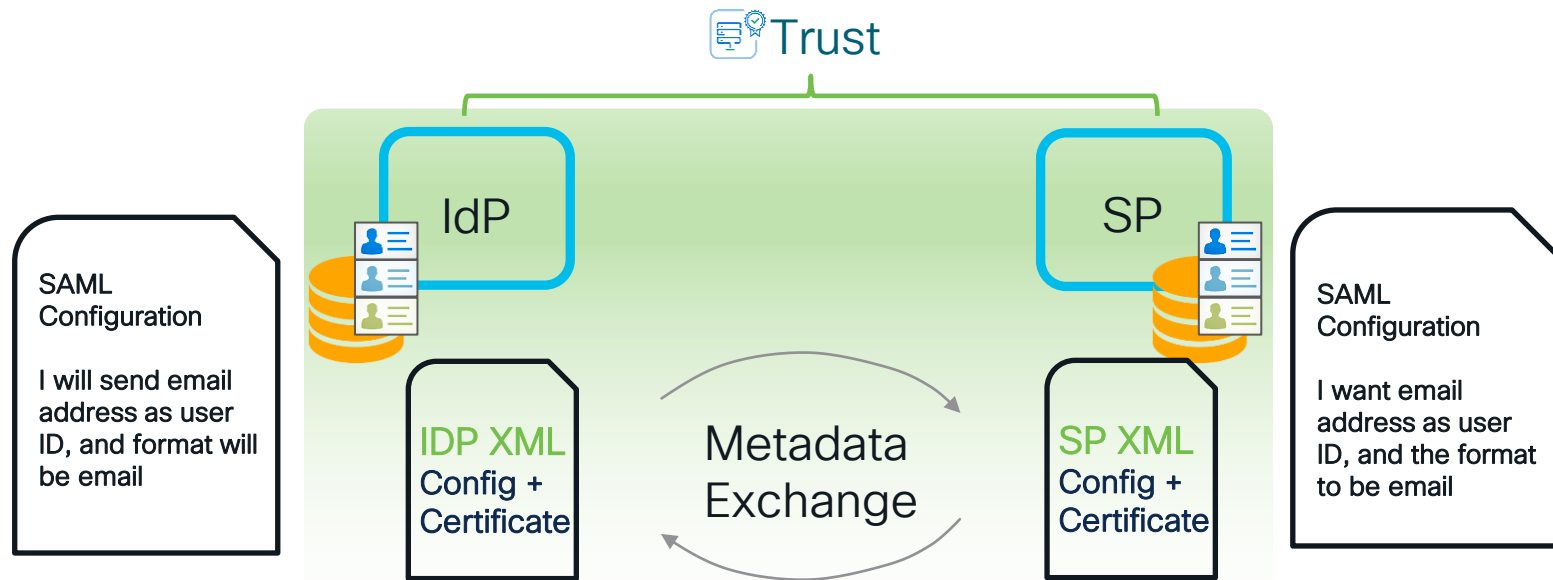
Username: BOBS
Email.address:
bob@domain.com
Firstname: BOB
Lastname: SMITH

SAML Configuration
I will send email address as user ID, and format will be email

SAML Configuration
I want email address as user ID, and the format to be email

Username: BSMITH
Email.address:
bob@domain.com
Firstname: BOB
Lastname: SMITH

SAML flow: Metadata Exchange



SAML Metadata for Umbrella



Umbrella URL for dynamic Metadata downloads:

https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml

SAML: Name ID requirements

Umbrella expects “User Principal NAME (UPN)” in NameID

METADATA

- Entity ID
- Certificate (or 2)
- Etc.



UPN in NameID from IdP

true by default for most IdPs

Edit Rule - UPN to email

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
UPN to Name ID

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	Name ID
*		

View Rule Language... OK Cancel

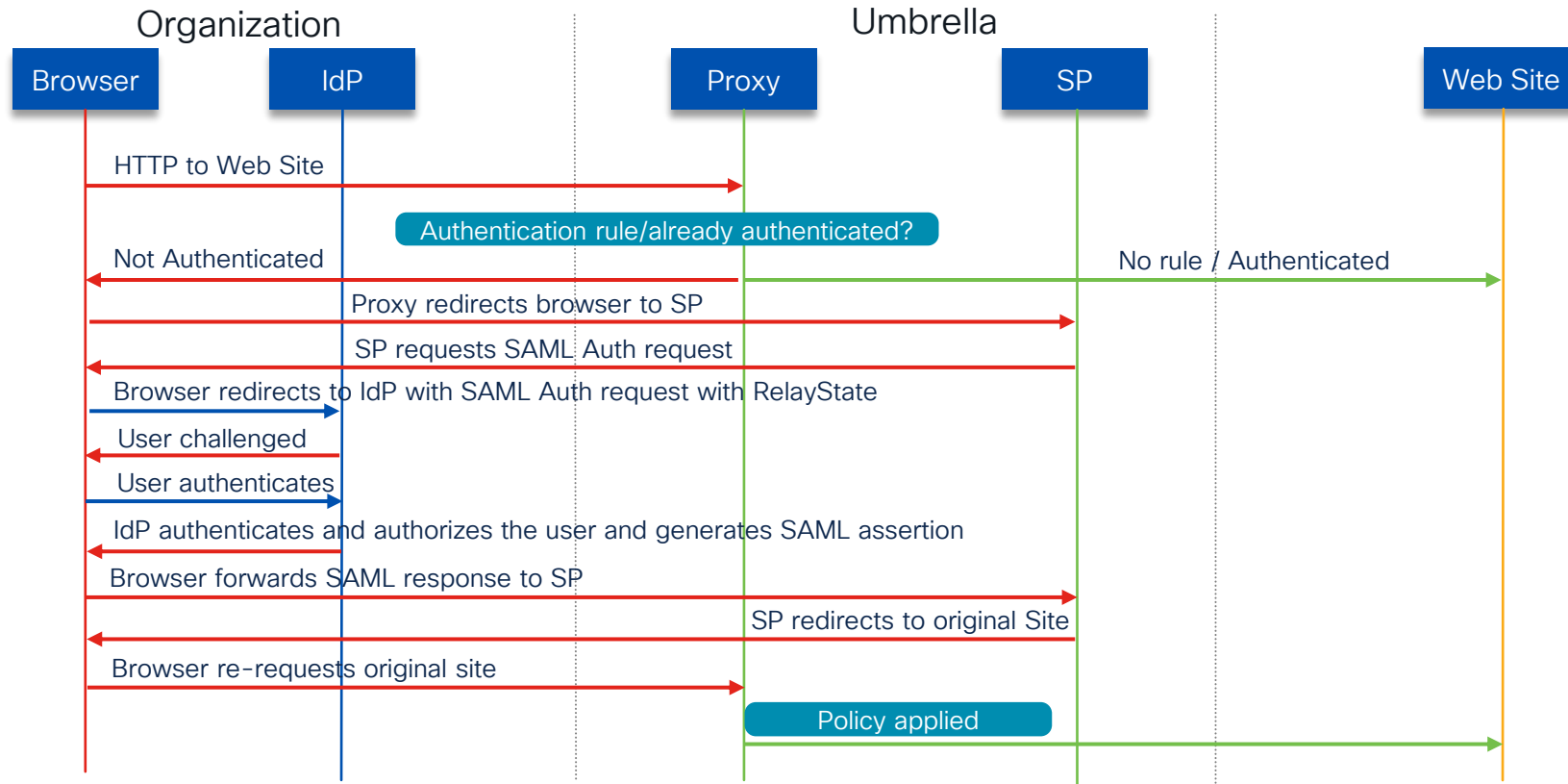
ADFS Claims Map Example



manual claims map is required in ADFS

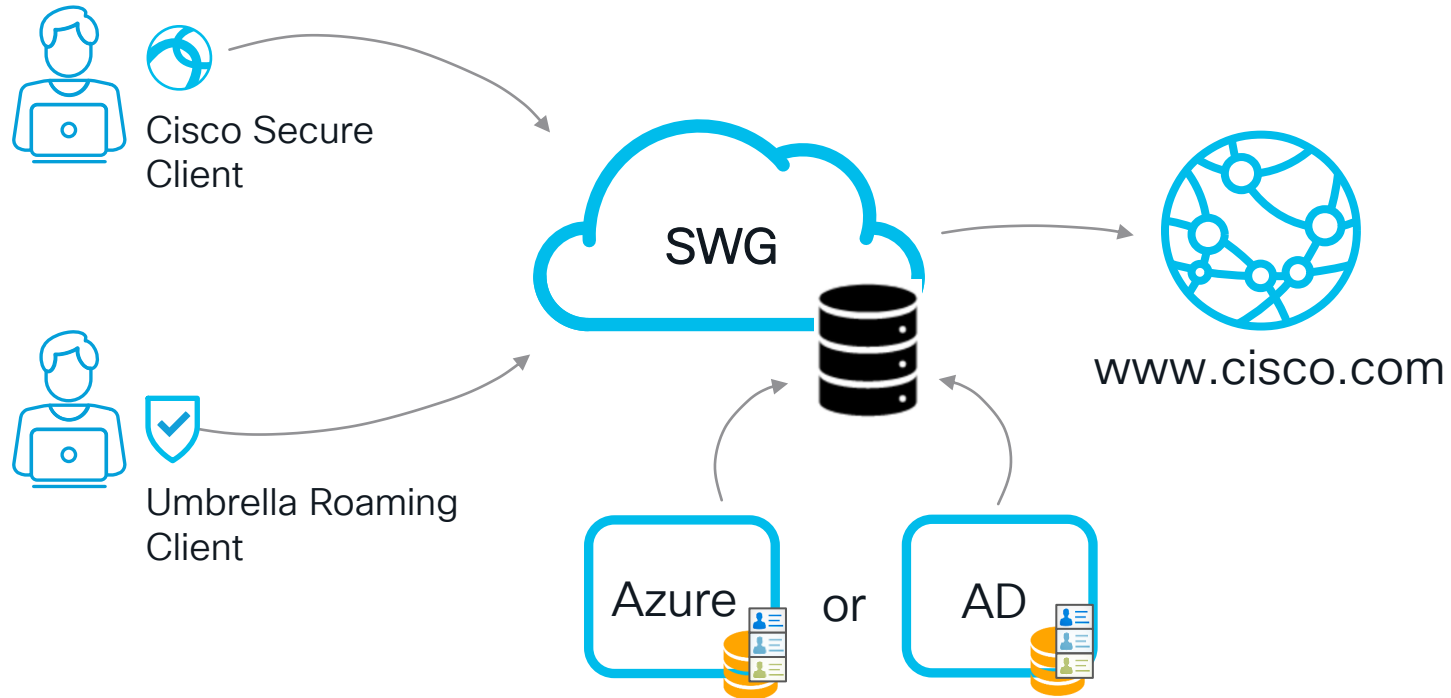
SAML Flow: Full Picture

SP and IdP never communicate directly!

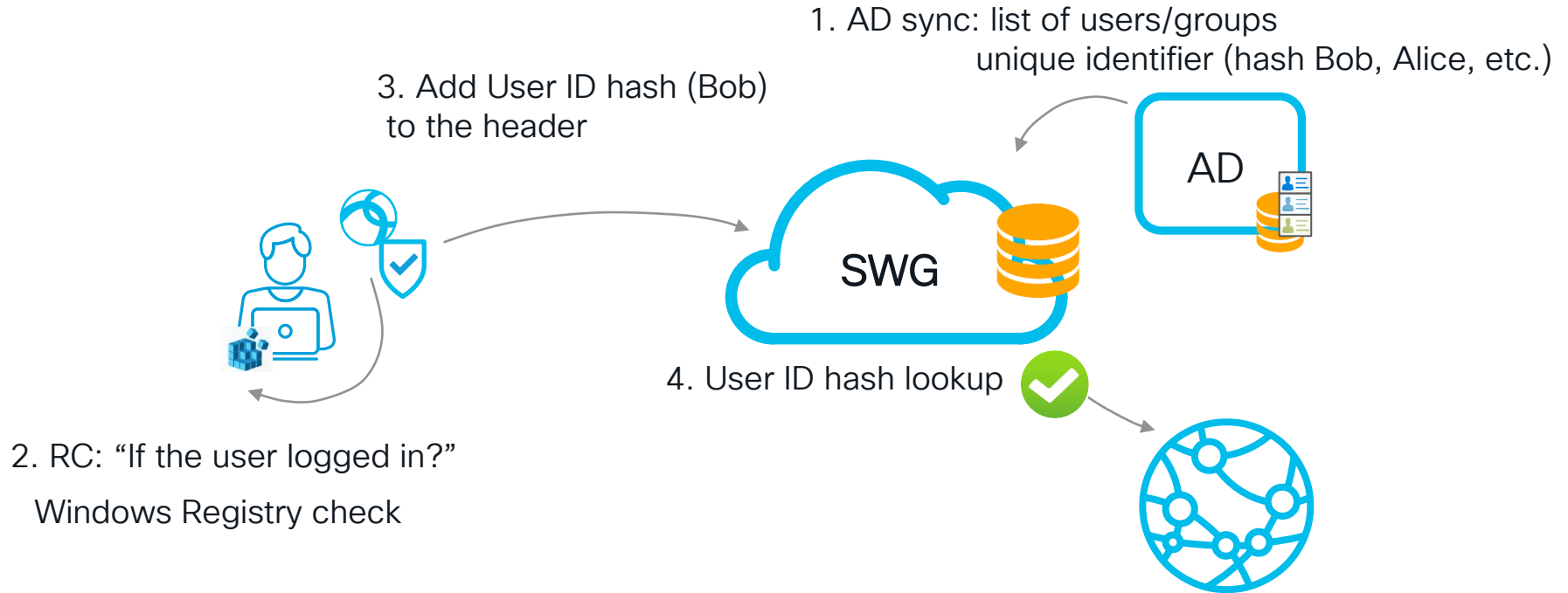


2. Remote Users

Remote User Connection Options



Remote User: Traffic Flow



Remote User: Hash Generation



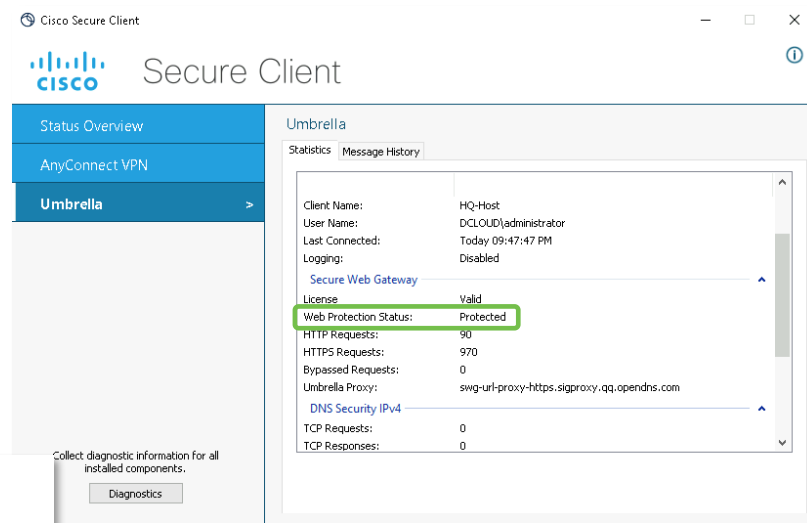
- globally unique ID for each object in Active Directory
- the client gets it from Windows Registry
- should match the value detected on the AD server by the Connector.

- “userPrincipalName” AD attribute
- **user@domain** format
- usually is the same as the users' email address but does not have to be
- works in pure and hybrid AZURE environment
- **preferred method starting**
 - AC 4.10 MR6+ / AC 5.0+ (Cisco Secure Client)
 - Standalone 3.0.328+

Cisco Security Client (Any Connect)

Entitlement is included for use with an Umbrella subscription
(excludes VPN functionality)

- AnyConnect can be used across an entire enterprise
- Both Umbrella DNS and Secure Web Gateway services can co-exist
- Needs to be enabled in Umbrella Portal:
“Deployments > Roaming Clients > Settings”



Secure Web Gateway

Enable the Secure Web Gateway module to proxy all web traffic. For full details, [please see documentation here](#).



Secure Web Gateway Currently Enabled



Supports Windows and Mac desktops

Remote User: AnyConnect SWG closer look

- The config is delivered from the cloud to the client during API sync.
- Settings are copied to C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG\SWGConfig.json

- Includes:

- identity settings
- exception list
- special settings
- proxy address
- SWG parameters

```
{
  "identity": {
    "orgId": "8073397",
    "deviceId": "01015C3B6CF1790B",
    "adUserIdUpn": "c7df1cd1507cc7853e465f5714f12c11"
  },
  "deviceConfig": {},
  "orgConfig": {
    "exceptionList": [
      {
        "failOpen": "1",
        "swgAnycast": "146.112.255.50",
        "swgDomain": "swg-url-proxy-https.sigproxy.qq.opendns.com",
        "swgEchoService": "http://www.msftconnecttest.com/connecttest.txt",
        "swgHonorTND": "1"
      }
    ],
    "commonConfig": {
      "rsaPubKey": "LS0tLS1CRUdJTiBQVUJMSUMgSOVZLS0tLS0KU1JQklqQU5CZ2txaGtpRzl3MEJBUUWVGQUPPQ0FRRC",
      "rsaPubKeyId": "52379614bb86e028bbdcfeeabe2d743e",
      "swgHosts": "swg-url-proxy-https.sigproxy.qq.opendns.com"
    },
    "dnsBackoff": {
      "isAnyConnectTND": false,
      "dns4": {
        "backedOff": false,
        "reason": "none"
      },
      "dns6": {
        "backedOff": true,
        "reason": "noNetwork"
      }
    },
    "vpnDetails": {

```

Remote User: Web Interception

1. **acswgagen.exe** runs a kind of proxy process locally on the machine (TCP:5002):

```
TCP    [::1]:5002    [::]:0    LISTENING
[acswgagent.exe]
```

4. inserts encrypted headers in the user HTTP request and sends request to Umbrella
5. Umbrella proxy applies policies and Makes forward/block decision

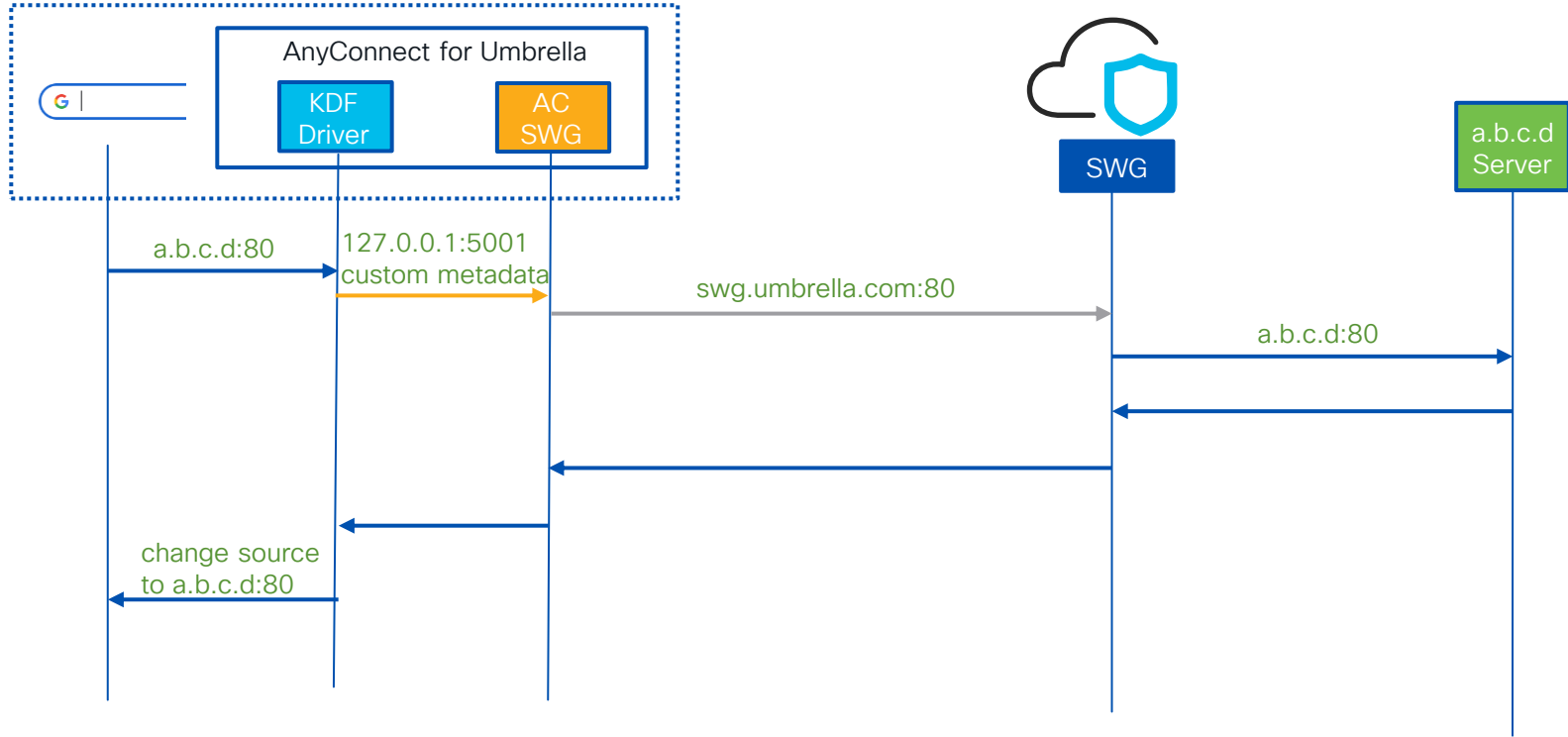


2. process intercepts any web requests TCP 80/443

3. looks at destination address and makes forwarding decision (exclusions)

```
X-USWG-SK: tz39AYT/UEk3oaaMbX0G2crg35Agu15gXwP3H+1E7wYdw0d7+bGRux7e1mqhO/
o3nU2a3JQo6XqDYQ3XvxybTsTHCwdaP6hFEUVGHzcVEgW0wP8XofzFOIf+OSRTgWLAfdg0vUNeyLSiEexrV1PLEtkc5m8D3Yw6hN
d1AY07DUJZ/h63PDucktgW27YI11JLZDf538LjExlpFZ04sFm+1W2FTPyashCa8Spw==
X-USWG-Data:
CQY10wvcwjnRmpBqYzj67VvKlQneNlAqKi7WkrEwB507ghnAUJGTfV4GCl0RwDROc5Q+6WNS4okDHQmZkc67sQFnq1L2kXC6XXS61
nyuICE5w+DEhImzDkS9qxD5gFNqKc04Lyjh/2gvEdUdbVfphr8YNUcxP/1ez1wdd0NL2G1Z273K94fzqH1dNu3zRXwLxR+d0m0E
Zgve63/6zt3qfd30LHjL1g3uGwr1YLK+HyEx6LTvW3qsvxyh6350P21ZbK9r+6RXedwgv9QNWVsc8051zD8K17fZ45fsTAy535
X-USWG-PKH: 52379614bb86e028bbdcfeeabe2d743e
```

Remote User: Traffic Flow



Remote User: AC-SWG Headers

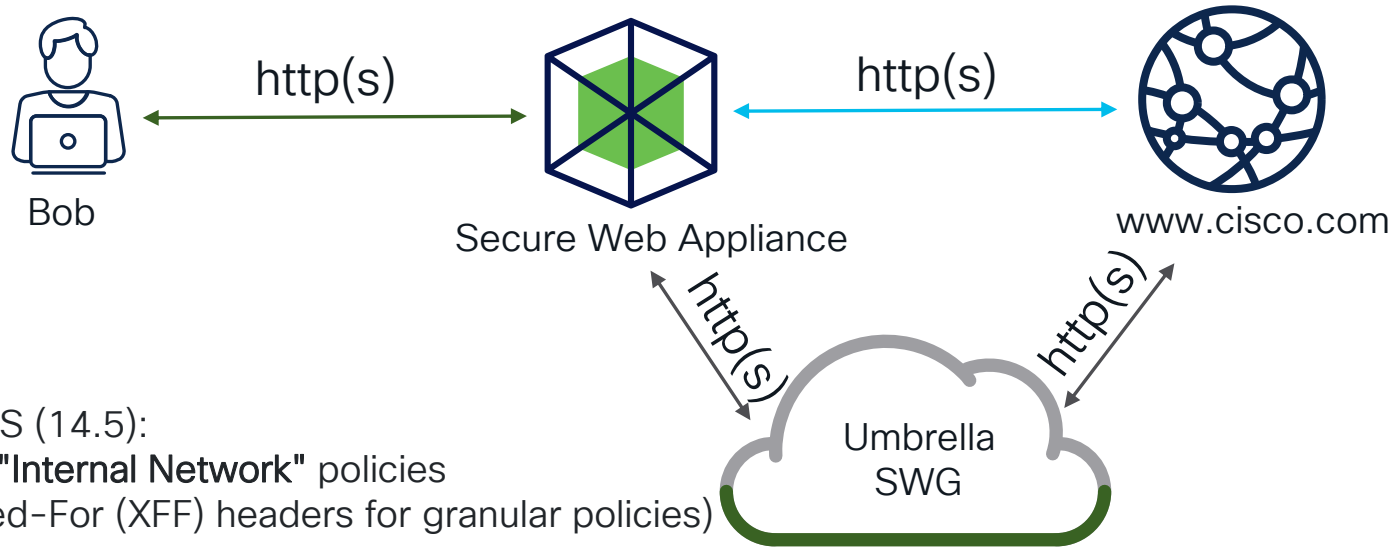
- **X-USWG-SK** – Encrypted Session Key
- **X-USWG-Data** – Org ID + Identity (Device/User) + 'timestamp'
- **X-USWG-PKH** – Hash of RSA Private Key

```
CONNECT 13.64.180.106:443 HTTP/1.0
Content-Length: 0
Proxy-Connection: Keep-Alive
Host: 13.64.180.106:443
X-USWG-SK: 1G1F8+WyfKA0tvrzlhKp4hngOMCeE9Lf1Q1/
Pmrj8DrZAFcv1VcRDjeuBNWnTOhrgnK2qb45A9JPM60TuDQdc1KTqqQ9ntVEZv0SnOMBen99jzsiNis1KgSfHx2HZCiHfqt+LDQDUans6
4HUw0FnCzWHSKzFLm8FCmI5tdMC38viVxYJnyU/BrVCc3HiKgAZt1H8Ts1JnEa6OVwgyE1NVN+szF3DJXxvYge41z3kdzVh0HJnLhRTJ
X-USWG-Data: SLNHC82h901AsArTN+z8wLnBc5tjzkPKFzxXzD1ehC6P1WH+70EhXDKrNZHkZWR+xyxDZvCBN947GcRSRanpiMuJkwtJ
XN9yWYS1InDxSrZJXT0jRoZkCTX17GHABY9I3B1vjfdiWvXNYG7ZKIGt5cuW4+bVMNNQ1pt6VENvOjFuHCowYmLjdSL859e2cweIftS1f
rhf6Aao371vL1VLcV3hYu102IXnHze4KKvLFo4gQQKHxEBRrmRHb1wPyjUeSnf5ihZaWfYIDqAssdoy29XtBPhooNDsdeX+iJNBvaUz4P9
X-USWG-PKH: 52379614bb86e028bbdcfeeabe2d743e

HTTP/1.1 200 Connection established
Via:HTTP/1.1 s_proxy_ash
```

3. Seamless Identity

Seamless Identity: Proxy Chaining Concept

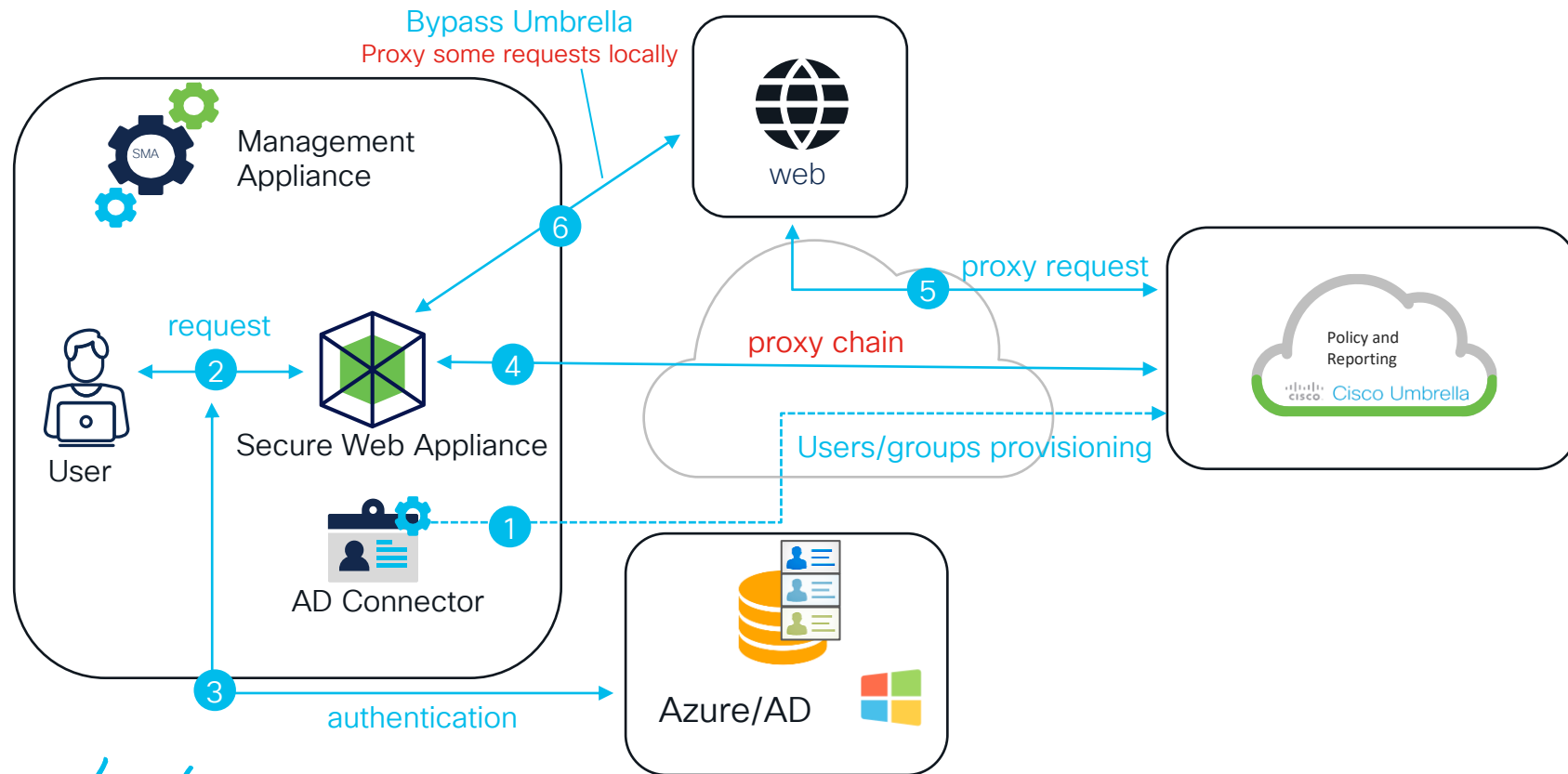


Before AsyncOS (14.5):
WSA provides "**Internal Network**" policies
(or X-Forwarded-For (XFF) headers for granular policies)

Seamless Identity: Adding UserID to proxy Chaining

- Granular policy/reporting based on User Identity
- Secure Web Appliance Customers can take advantage of authentication methods they may already be using in the Secure Web Appliance such as Kerberos/NTLM or ISE.
- Consistent user identity between Secure Web Appliance and Umbrella
- Better user experience compared with SAML

Seamless Identity: Traffic Flow



Seamless Identity: HTTP Headers

- X-USWG-Data
 - Org ID
 - Identity (Device/User)
 - 'timestamp'
- X-USWG-SK
 - Encrypted Session Key
- X-USWG-PKH
 - Hash of RSA Private Key

[illegible]

Headers in Authentication Process



Demo

CISCO *Live!*



Demo Scenario 1:

- User is trying to access blocked category “News” (www.bbc.com).
- Cisco Web Security Appliance is deployed in transparent mode.
- Kerberos authentication is enabled for domain users.
- Web Security Appliance is configured to pass traffic to Umbrella: proxy chaining with seamless identity feature enabled



Demo Scenario 1:

1. Traffic from default gateway is redirected to Secure Web Appliance

```
198.19.10.254 - PuTTY
ASAv# sho run | i wccp
access-list wccp-traffic extended permit ip host 198.19.10.15 any
access-list wccp-servers extended permit ip host 198.19.10.52 any
wccp 15 redirect-list wccp-traffic group-list wccp-servers
wccp interface inside 15 redirect in
ASAv# sho wccp 15

Global WCCP information:
  Router information:
    Router Identifier:      198.19.10.254
    Protocol Version:      2.0

  Service Identifier: 15
    Number of Cache Engines: 1
    Number of routers:      1
    Total Packets Redirected: 147414
    Redirect access-list:   wccp-traffic
    Total Connections Denied Redirect: 0
    Total Packets Unassigned: 0
    Group access-list:      wccp-servers
    Total Messages Denied to Group: 0
    Total Authentication failures: 0
    Total Bypassed Packets Received: 0
ASAv#
```



Demo Scenario 1:

2. We start capture on Secure Web Appliance to check the headers

**Cisco Secure Web Appliance**
S600V

Secure Web Appliance is getting a new look. Try it!

[Home](#) [Reporting](#) [Web Security Manager](#) [Security Services](#) [Network](#) [System Administration](#)

Packet Capture

Success — Packet Capture has started

Current Packet Capture

Status: Capture in progress (Duration: 1s)
File Name: S600V-42179F8366C0AEAF0946-4F277AA9A29C-20230121-202717.cap (Size: 2M)
Current Settings:
Max File Size: 200MB
Capture Limit: No Limit
Capture Interfaces: M1
Capture Filter: ((proto gre && ip[50:2] = 80) or tcp port 80 or (proto gre && ip[50:2] = 3128) or tcp port 3128 or (proto gre && ip[50:2] = 443) or tcp port 443)

[Stop Capture](#)

Manage Packet Capture Files

[Delete Selected Files](#) [Download File](#)

Packet Capture Settings

Capture File Size Limit:	200 MB
Capture Duration:	Run Capture Indefinitely
Interfaces Selected:	M1
Filters Selected:	((proto gre && ip[50:2] = 80) or tcp port 80 or (proto gre && ip[50:2] = 3128) or tcp port 3128 or (proto gre && ip[50:2] = 443) or tcp port 443)

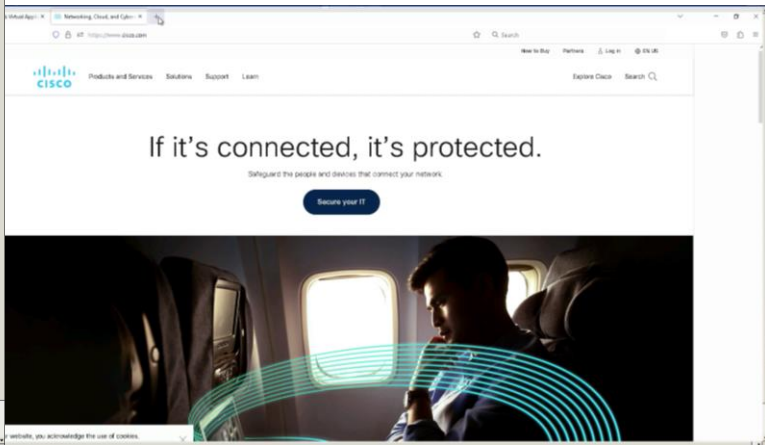
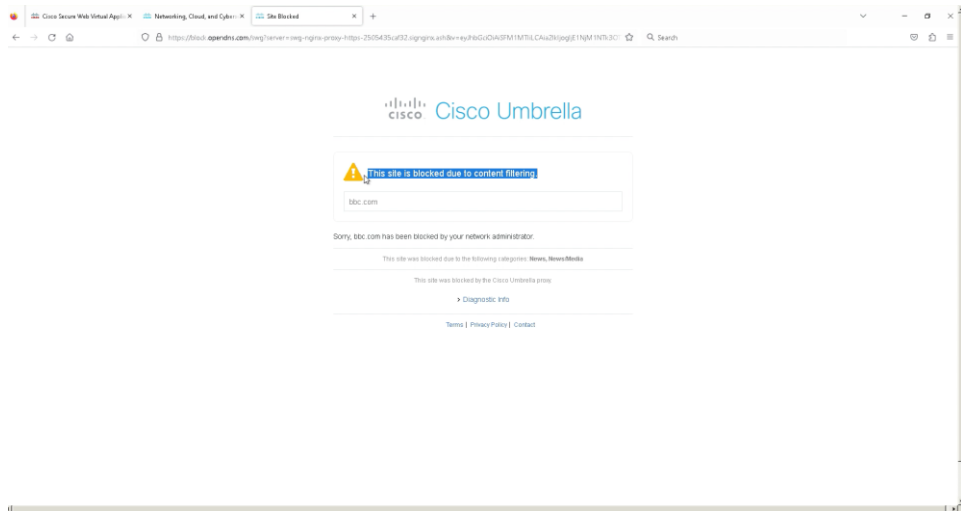
[Edit Settings...](#)



Demo Scenario 1:

3. User access to web category "News" is blocked by Umbrella configured policy, access to allowed web categories is working as expected.

4. Capture on Secure Web Appliance is stopped and saved.





Demo Scenario 2:

- User is trying to access blocked category “News” (www.bbc.com).
- There is no proxy in the network, Secure Client is installed with Umbrella module
- Secure Web Gateway is enabled for the user PC in Umbrella portal



Demo Scenario 2:

1. We disable transparent redirection on the default gateway. All traffic from the user is going directly to the Internet.

```
198.19.10.254 - PuTTY
login as: admin
admin@198.19.10.254's password:
Type help or '?' for a list of available commands.
ASAv> en
Password: *****
ASAv# sho run | i wccp
access-list wccp-traffic extended permit ip host 198.19.10.15 any
access-list wccp-servers extended permit ip host 198.19.10.52 any
wccp 15 redirect-list wccp-traffic group-list wccp-servers
wccp interface inside 15 redirect in
ASAv# conf t
ASAv(config)# no wccp interface inside 15 redirect in
ASAv(config)# wr
Building configuration...
Cryptochecksum: 8e669349 e1c0d3b3 10ae601a 07535dda
8775 bytes copied in 0.100 secs
[OK]
ASAv(config)#
```



Demo Scenario 2:

2. Secure Client status changes from Umbrella Web Protection disabled to Enabled, after enabling the feature it on Umbrella portal.

Deployments / Core Identities

Roaming Computers

Roaming Client Settings

Roaming Computers are those that are protected by either the Umbrella Roaming Client, or Cisco Secure Client Umbrella module (formerly AnyConnect). This area of the Dashboard gives administrators the ability to deploy your clients with the download button on the upper right and to manage your Roaming Computers below.

Search Advanced

1 of 1 Selected CLEAR SELECTION REMOVE TAG ADD

☒	Identity Name ▲	Status	Tags	SWG Agent	Last Sync
☒	HQ-Host	Offline DNS Layer Encryption: disabled		Disabled	2 min

Page: 1 Results per page: 10 1-1 of 1

Context menu for HQ-Host:

- Delete
- Enable SWG Agent
- Disable SWG Agent
- Follow Global Settings



1 Total

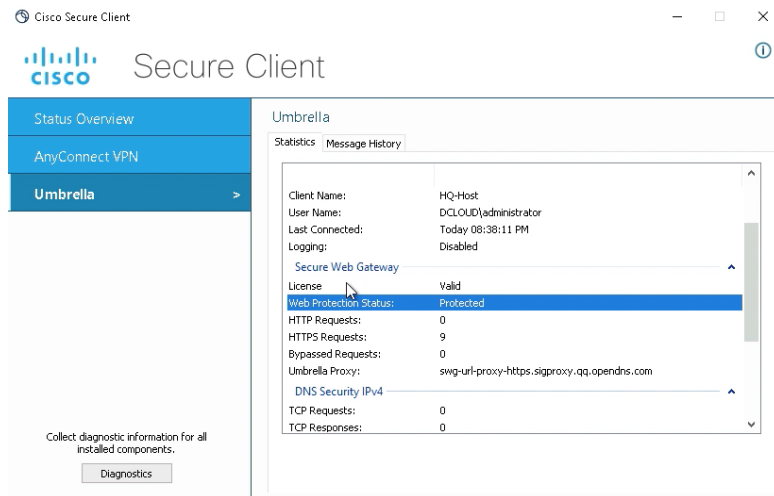
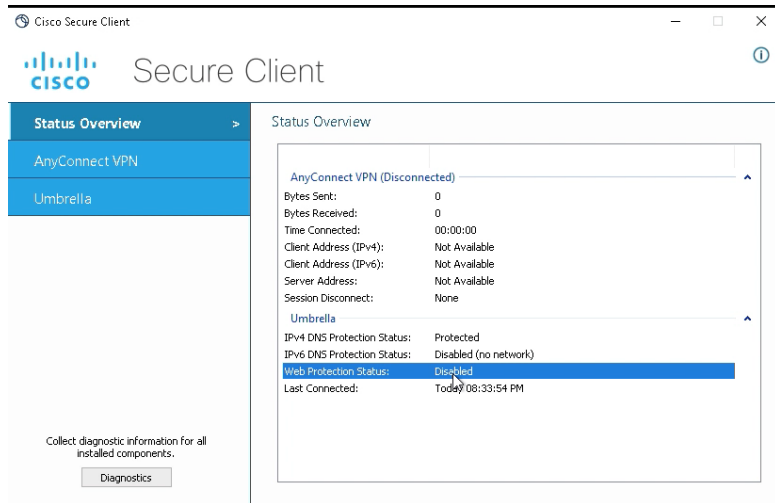
☐	Identity Name ▲	Status	Tags	SWG Agent	Last Sync ▼
☐	HQ-Host	Offline DNS Layer Encryption: disabled		Enabled	2 minutes ago

Page: 1 Results per page: 10 1-1 of 1



Demo Scenario 2:

2. Secure Client status changes from Umbrella Web Protection disabled to Enabled, after enabling the feature it on Umbrella portal.

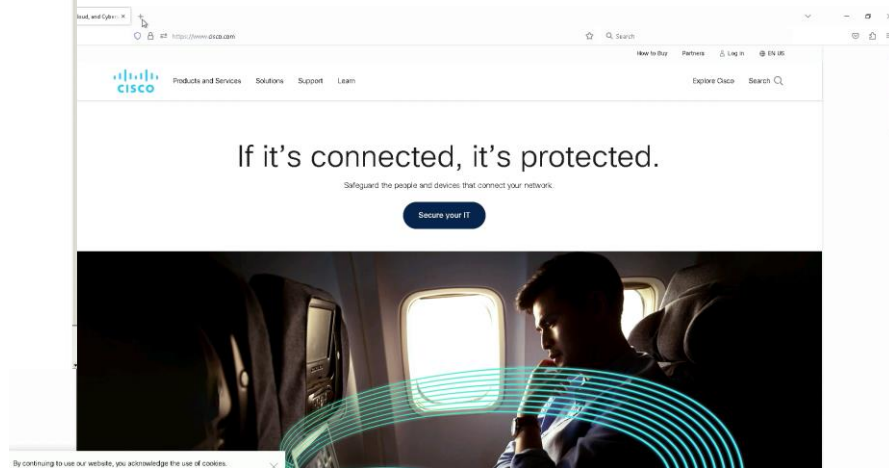
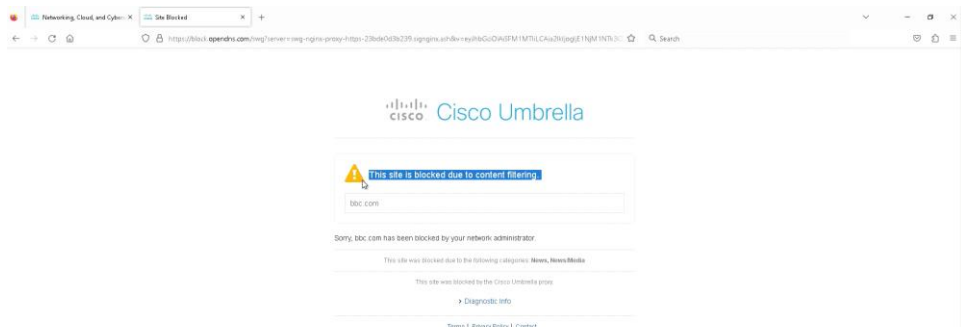




Demo Scenario 2:

3. Once the status changed to “protected”, we start packet capture on user PC and test restricted web category “News”. Site is blocked, as expected.

4. Capture on user PC is stopped and saved.



HTTP headers play important role in authentication process.

Authentication headers **are the same** for Seamless Identity and Cisco Secure Client connection scenarios.

Seamless Identity

Cisco Secure Client

```
http.request.method == "GET"
No. Time Source Destination Protocol Length Info
14630 8.248980 198.19.10.226 198.19.10.52 HTTP 422 GET http://www.audioreview.com/ HTTP/1.1
15192 5.304373 198.19.10.15 13.107.4.52 HTTP 193 GET /connecttest.txt HTTP/1.1
15203 5.306184 198.19.10.52 146.112.43.201 HTTP 1197 GET http://www.msftconnecttest.com/conne
25969 8.635095 198.19.10.212 198.19.10.52 HTTP 389 GET http://www.troygroup.com/ HTTP/1.1
25994 8.646780 198.19.10.52 192.124.249.107 HTTP 345 GET / HTTP/1.1
32629 10.705179 198.19.10.229 198.19.10.52 HTTP 418 GET http://www.cinemanow.com/ HTTP/1.1
36112 15.192920 198.19.10.219 198.19.10.52 HTTP 469 GET http://centuryproject.com/wp-content/
45030 22.820250 198.19.10.201 198.19.10.52 HTTP 438 GET http://k2qdb9r0meq7z7o.924329928.car
47248 23.870722 198.19.10.15 34.107.221.82 HTTP 385 GET /canonical.html HTTP/1.1
47252 23.873213 198.19.10.52 146.112.43.201 HTTP 1376 GET http://detectportal.firefox.com/canc
47294 23.924257 198.19.10.15 34.107.221.82 HTTP 387 GET /success.txt?ipv4 HTTP/1.1
47296 23.926369 198.19.10.52 146.112.43.201 HTTP 1378 GET http://detectportal.firefox.com/succ
47534 24.984176 198.19.10.15 151.101.0.81 HTTP 423 GET / HTTP/1.1
47545 24.995376 198.19.10.52 146.112.43.201 HTTP 1397 GET http://bbc.com/ HTTP/1.1

> Internet Protocol Version 4, Src: 198.19.10.52, Dst: 146.112.43.201
> Transmission Control Protocol, Src Port: 4866, Dst Port: 80, Seq: 1, Ack: 1, Len: 1331
Hypertext Transfer Protocol
> GET http://bbc.com/ HTTP/1.1\r\n
Connection: keep-alive\r\n
Host: bbc.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip\r\n
Upgrade-Insecure-Requests: 1\r\n
X-Infowards: 20\r\n
Via: 1.1 wsa.cloud.cisco.com:80 (Cisco-WSA/14.5.0-537)\r\n
[truncated]X-USWG-Data: Ulf50TjwLQ7r9f5bmghcLpeR2AK0gA2EQ1Q/0heaPong0m5Es3QUcrWLB09NoOm/SPYPsY6mJG/rp3Ng8xBKk
[truncated]X-USWG-SK: UQY7N0v80ankjcgKAuAY2ZrWm8tKN2jY3F8+DNL1W/qQ9pLmPl1xXfs)ALRp0Om0EprkU0aDXUkXG0znPr
X-USWG-PKH: f0d78ed86cb390157ca14ba18978cf\r\n
\r\n
[Full request URI: http://bbc.com/]
[HTTP request 1/1]
[Response in frame: 47562]
```

```
http.request.method == "GET"
No. Time Source Destination Protocol Length Info
660 10.510156 198.19.10.15 146.112.43.201 HTTP 1326 GET / HTTP/1.1
3007 32.340423 198.19.10.15 146.112.43.201 HTTP 1326 GET / HTTP/1.1
3019 32.384677 198.19.10.15 146.112.43.201 HTTP 1326 GET / HTTP/1.1

> Frame 660: 1325 bytes on wire (10600 bits), 1325 bytes captured (10600 bits) on interface \Device\NPF_{16252554-B780-4042-AC18-48990A}
> Ethernet II, Src: VMware_R6:94:85 (00:50:56:86:94:85), Dst: VMware_b8:14:fd (00:50:56:b8:14:fd)
> Internet Protocol Version 4, Src: 198.19.10.15, Dst: 146.112.43.24
> Transmission Control Protocol, Src Port: 49970, Dst Port: 80, Seq: 1, Ack: 1, Len: 1271
Hypertext Transfer Protocol
> GET / HTTP/1.1\r\n
Host: bbc.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip\r\n
Upgrade-Insecure-Requests: 1\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
[truncated]X-USWG-SK: k4p28B2j3HT9ban7fmwDnUcJ1PyCBT27aXhTv08LEaR3pIowUy+Dlmyt0h8hHr2gQnF8H8qfhj8450WFH93Igl/SylwhoeEFOOQ
X-USWG-PKH: 52379614bb6e02bbdcf6eebe2d743e\r\n
\r\n
[Full request URI: http://bbc.com/]
[HTTP request 1/1]
[Response in frame: 663]
```

- X-USWG-SK – Encrypted Session Key
- X-USWG-Data – Org ID + Identity (Device/User) + 'timestamp'
- X-USWG-PKH – Hash of RSA Private Key

Key take aways

Summary: user authentication options

- 1 SAML Integrations (Duo, Azure, Okta, ADFS, PingID, etc.)
- 2 Remote User (AnyConnect SWG, Umbrella Client)
- 3 Proxy Chaining with **Seamless Identity**

Key takeaways

- 1 SAML Integrations are wildly used in Umbrella deployments.
Umbrella expects “User Principal NAME (UPN)” in NameID
- 2 Remote User (AnyConnect SWG, Umbrella Client)
injects encrypted HTTP headers with authentication status (with other info)
- 3 Proxy Chaining with **Seamless Identity** is a new feature.
Allows **consistent** user identity between on prem proxy and Umbrella in Hybrid networks. Allows to use Kerberos or ISE for user authentication.
- 4 Authentication methods can be used in parallel for different user scenarios



Useful links:

3d Party SAML integration configuration:

[Using Duo as the IdP for Umbrella SWG SAML](#)

[Using PingID as the IdP for Umbrella SWG SAML](#)

[Using Okta to Configure SAML 2.0 for Cisco Umbrella](#)

[Azure: Configure Cisco Umbrella User Management for automatic user provisioning](#)

Please Fill Out The Survey!



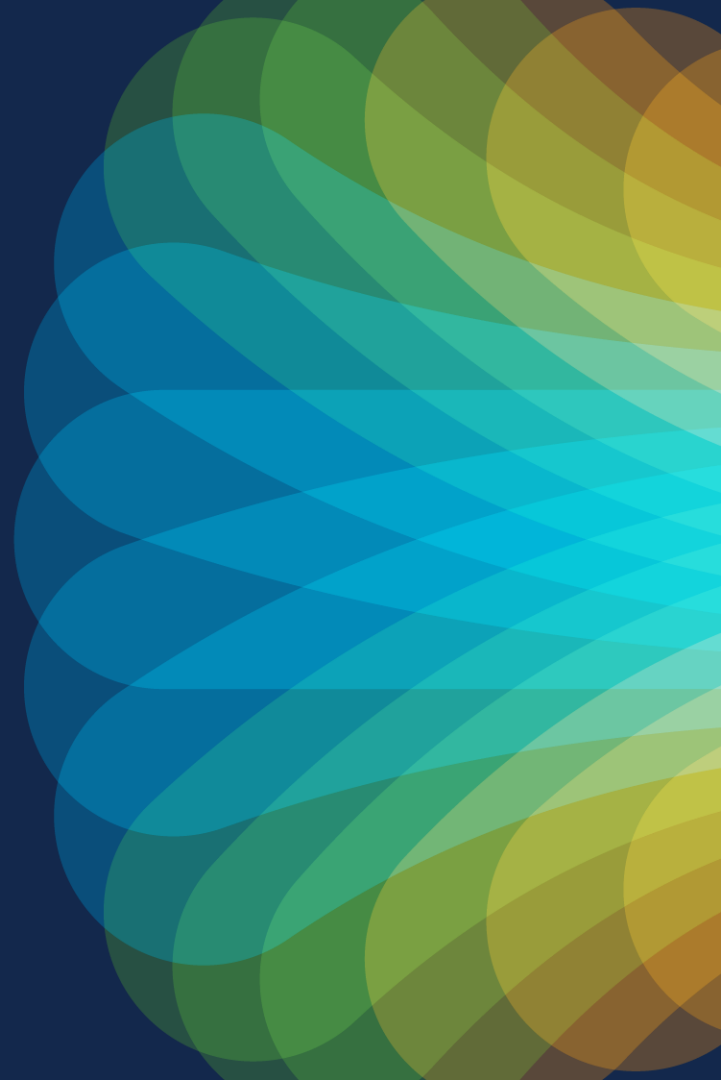
Q&A time



The bridge to possible

Thank you

CISCO *Live!*



The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, radiating lines in various colors, including blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go