




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  
6 years in Cisco, 10 years in IT

CCIE (RS & Security) #53290

# Cisco Webex App

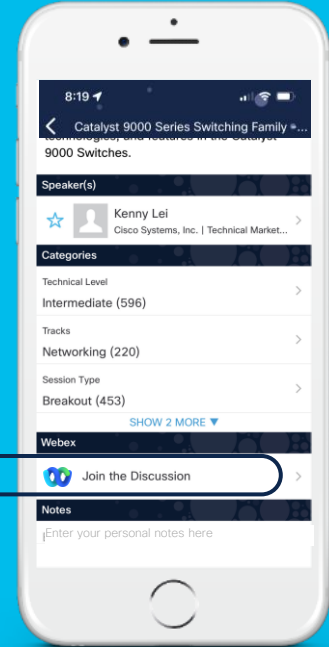
## Questions?

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

## How

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

Webex spaces will be moderated until February 24, 2023.



# For Your Reference

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



For Your  
Reference



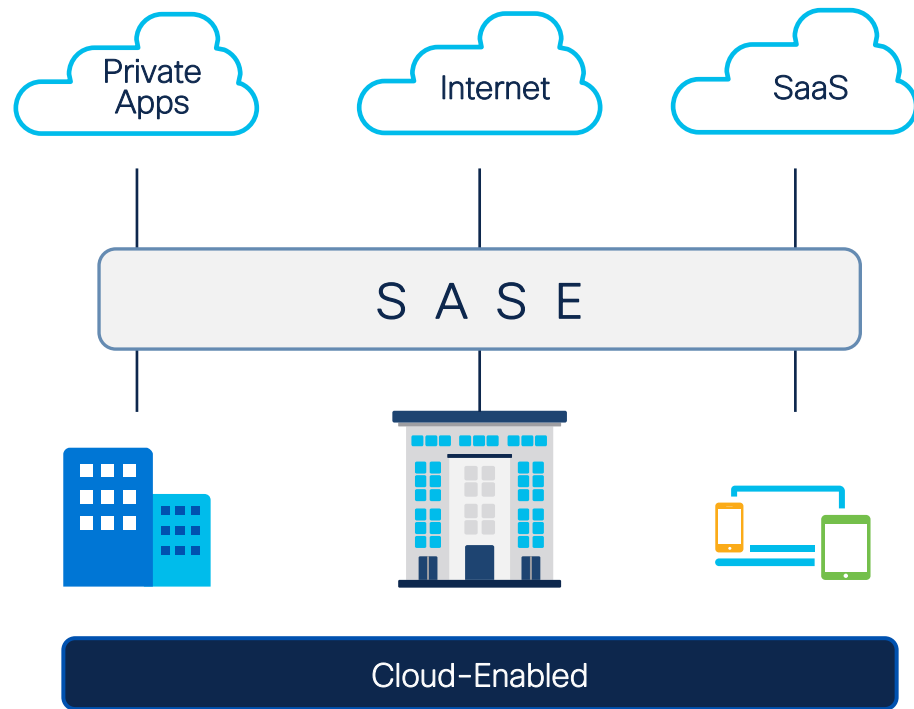
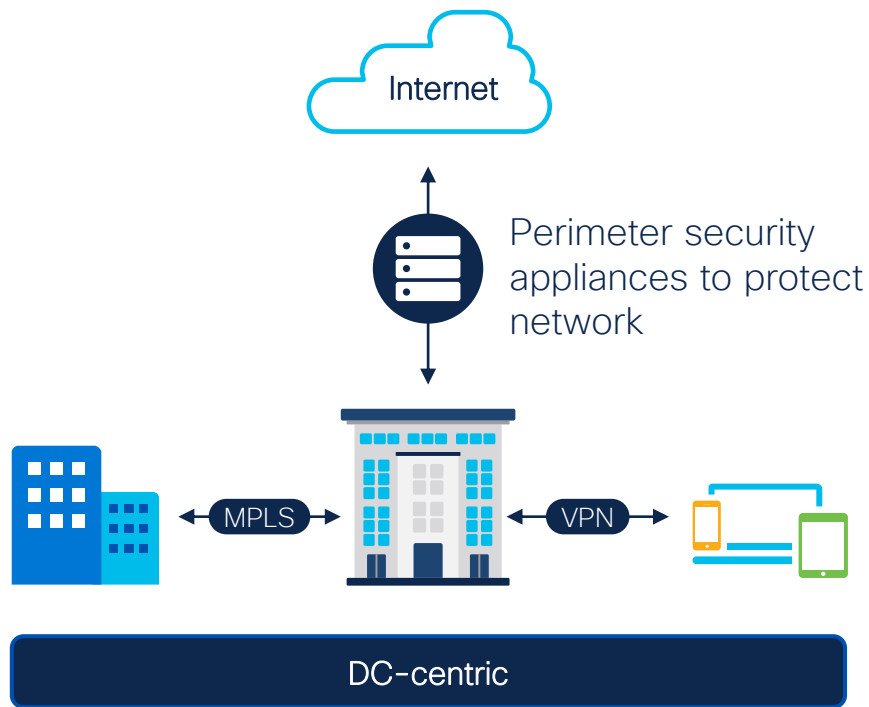
# Agenda

- 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

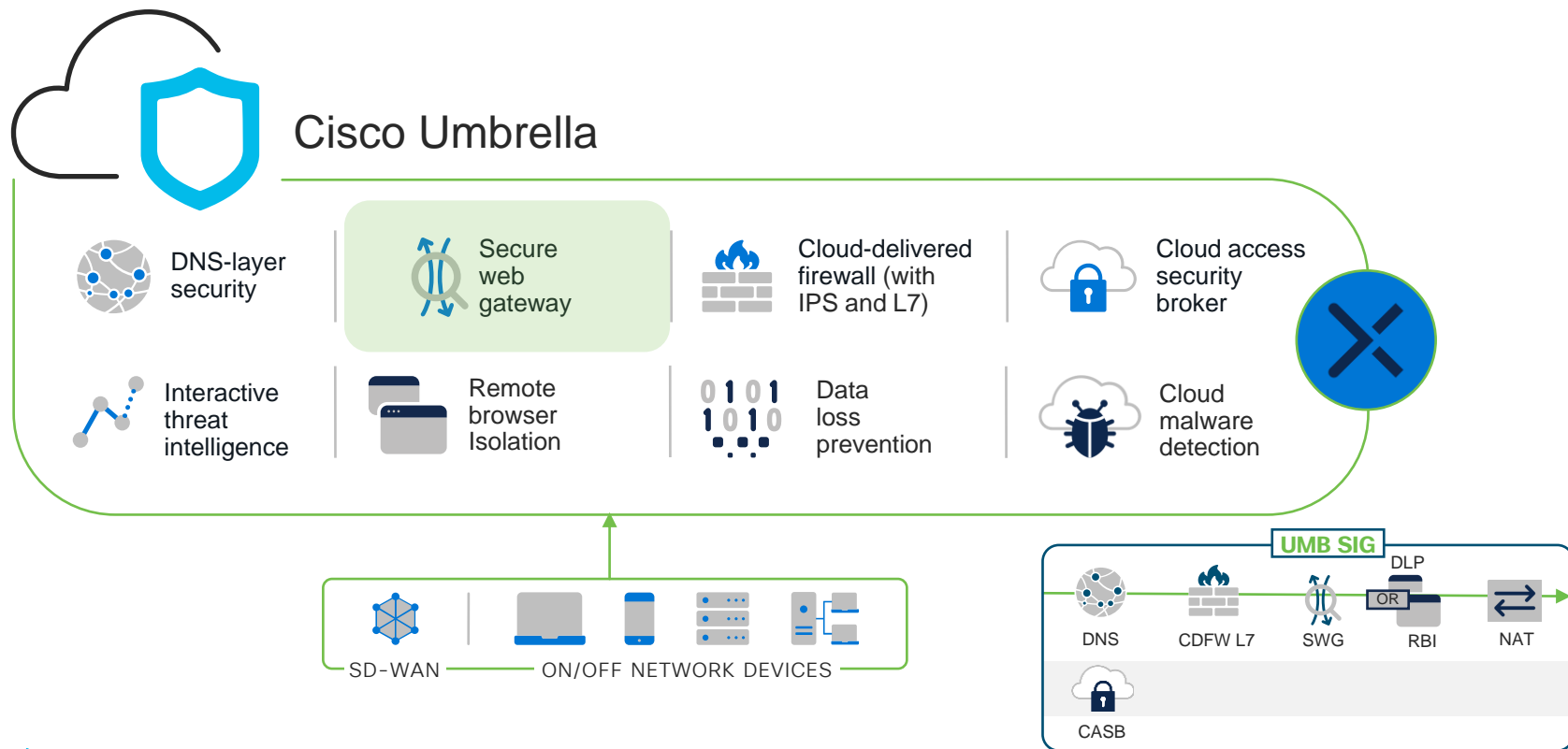


# Umbrella for Beginners

# 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)

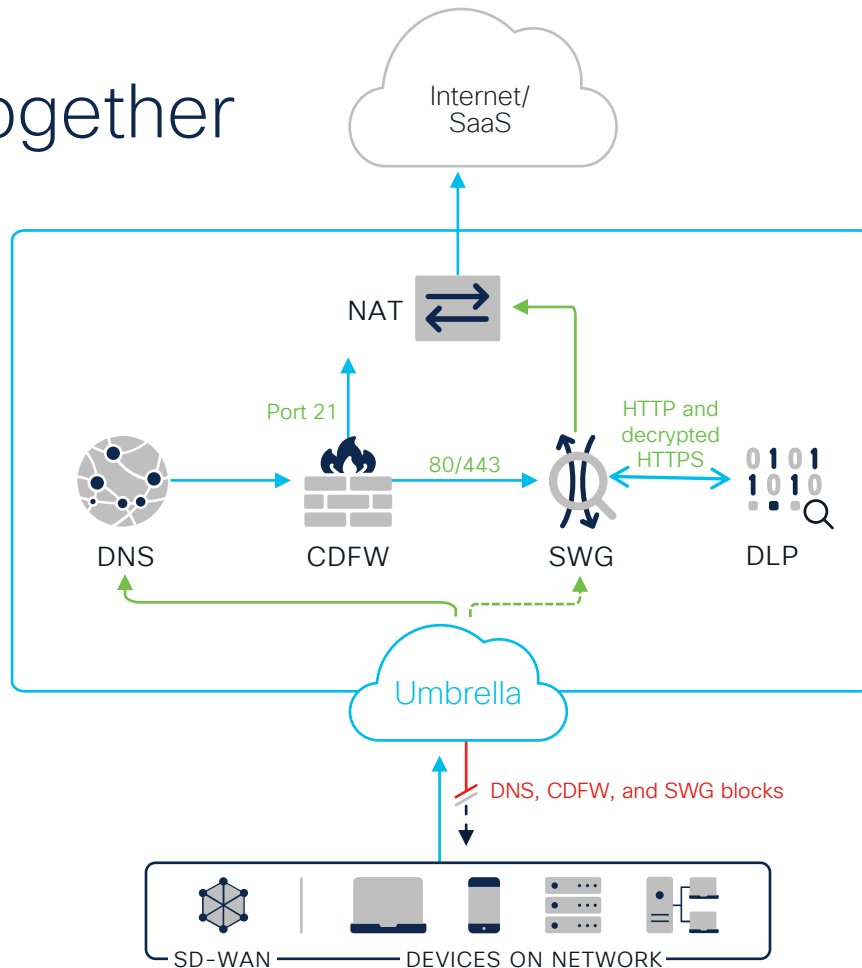
Next check for IP, port, protocol and application rules

### 3. Secure web gateway (SWG)

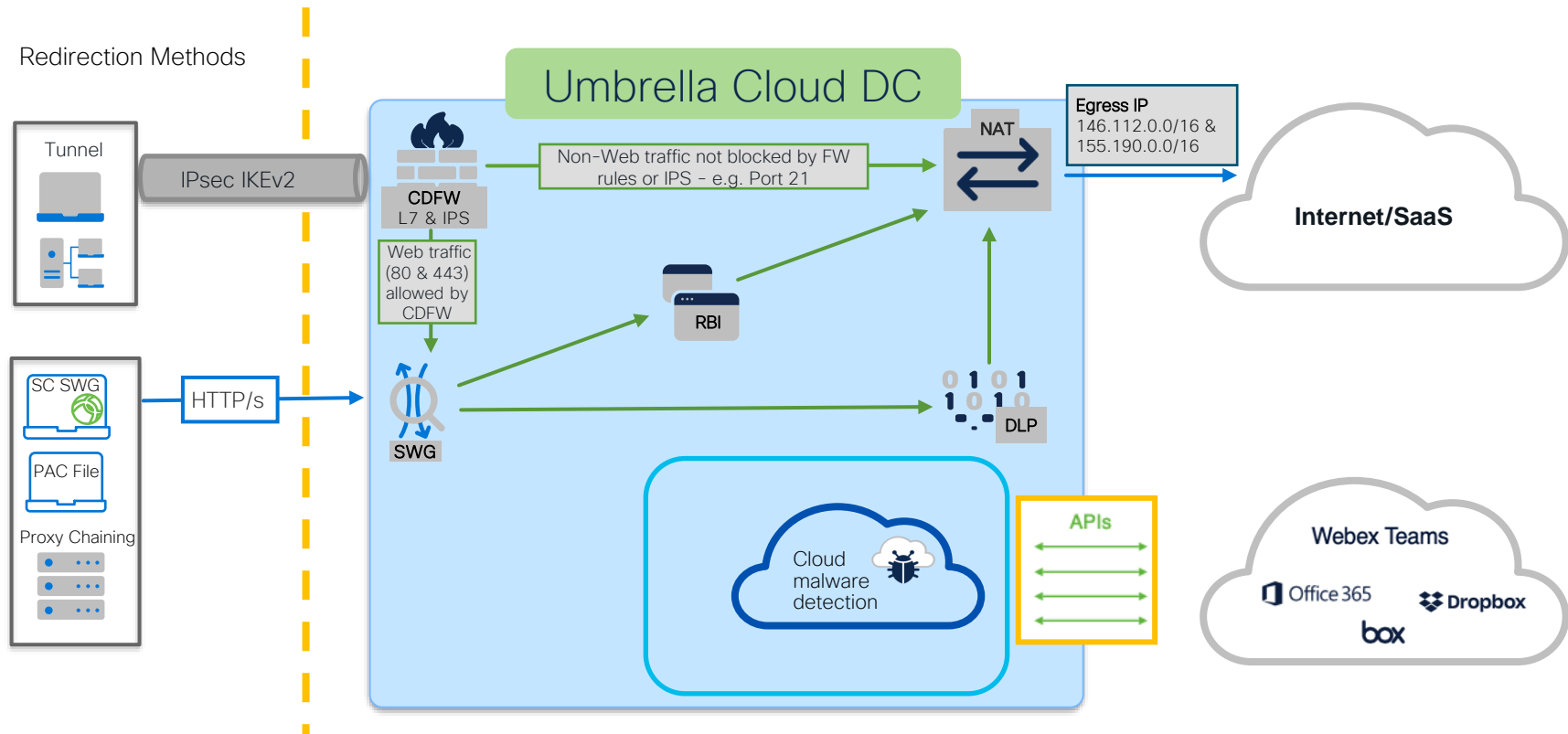
Final check of all web traffic for malware and policy violations

### 4. Data loss prevention (DLP)

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



# SIG Deployment Types & Traffic Flow Diagram



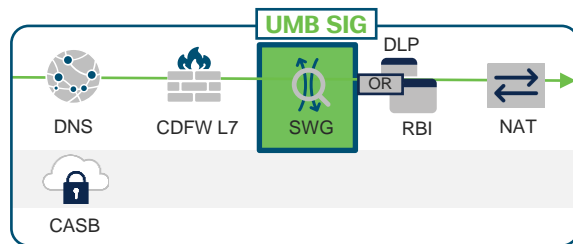
# Secure web gateway: full web proxy

## Deep inspection and control of web traffic

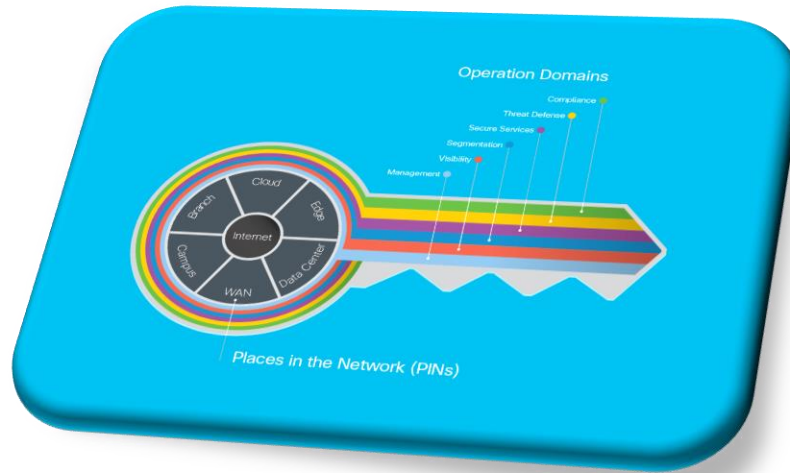
- ▶ Gain additional visibility via full URL logging and cloud app discovery
- ▶ Enforce acceptable use policy via granular app controls, content filtering, and URL block/allow lists



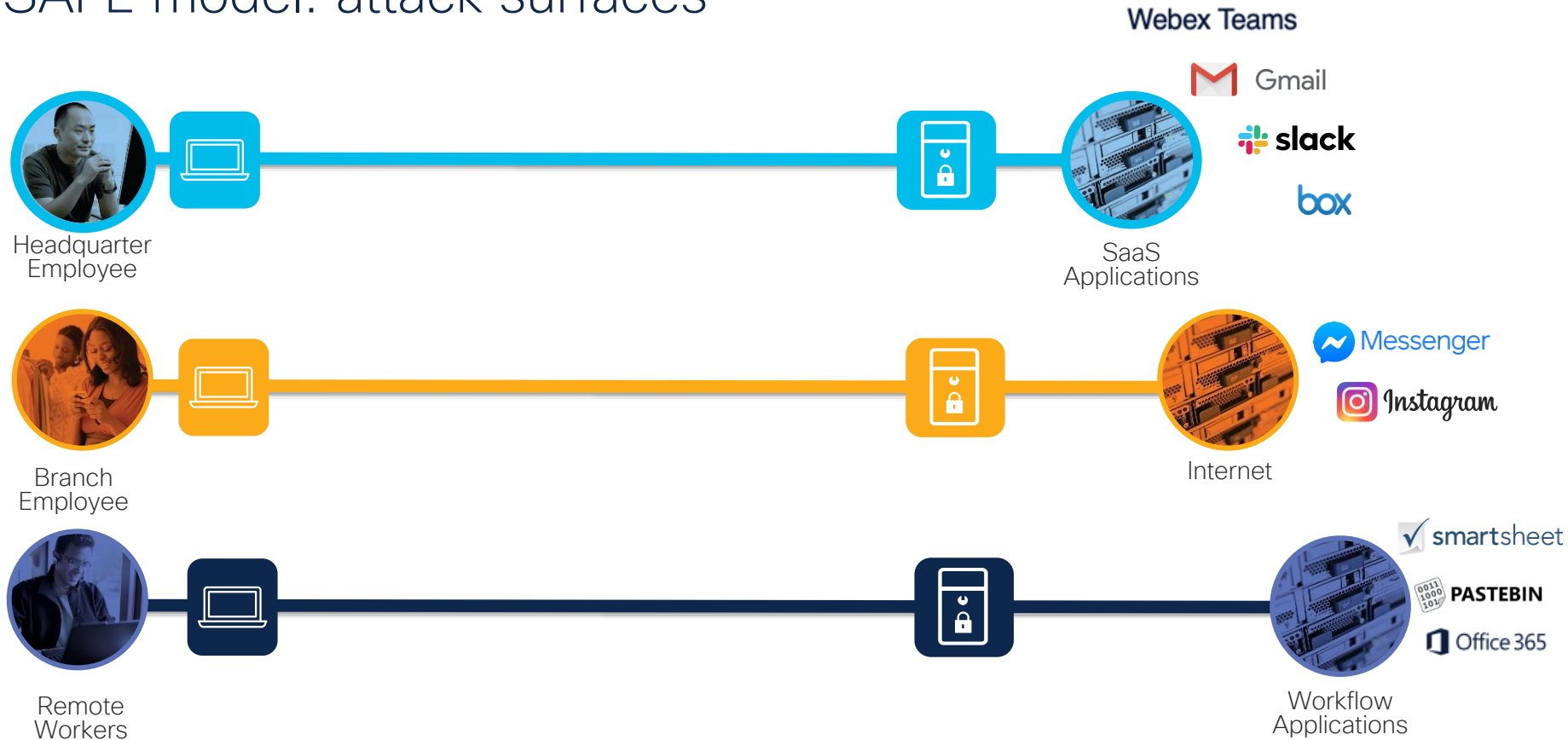
- ▶ Extend protection against malware via SSL decryption and file inspection
- ▶ Enrich file inspection (with retrospective alerts) via malware defense and analytics



# SAFE Framework

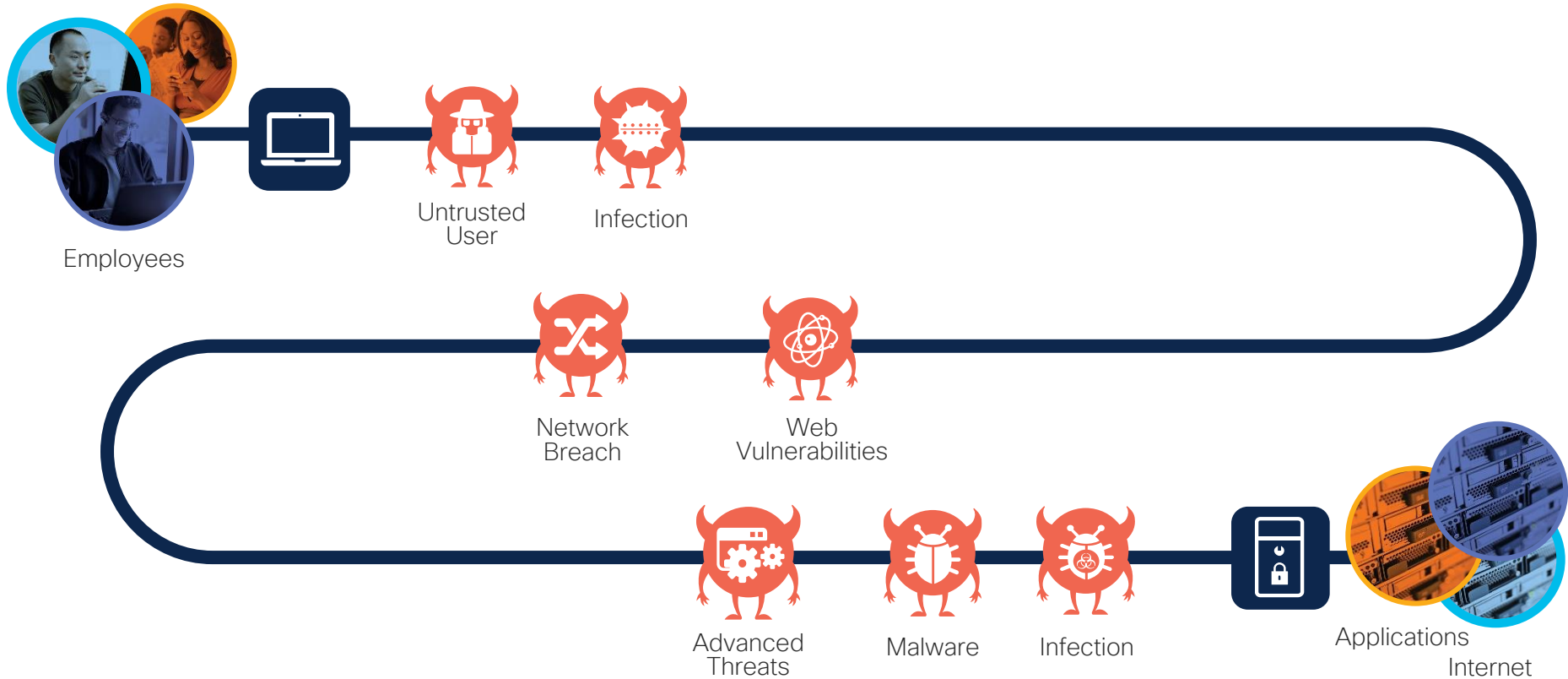


# SAFE model: attack surfaces

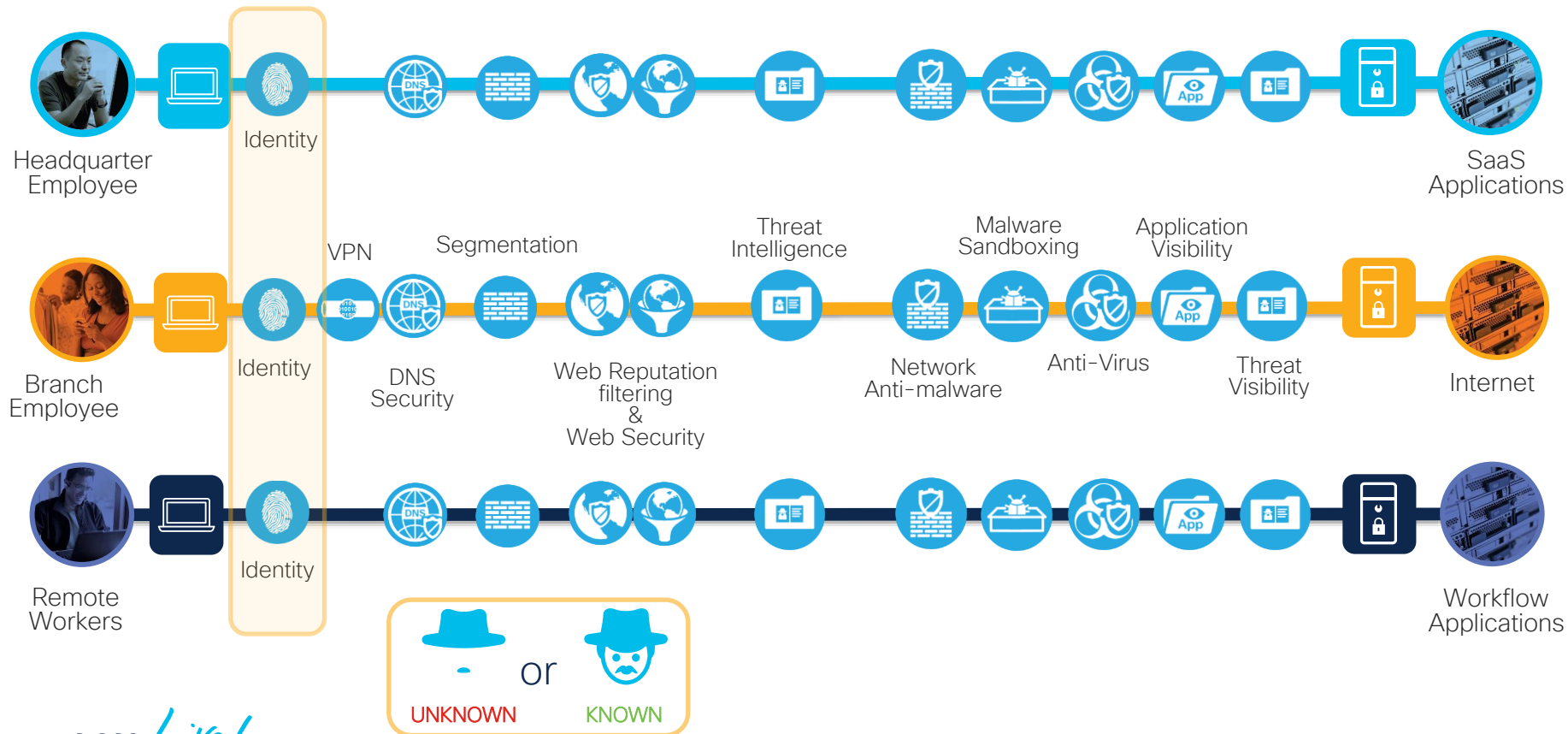




# SAFE model: threats

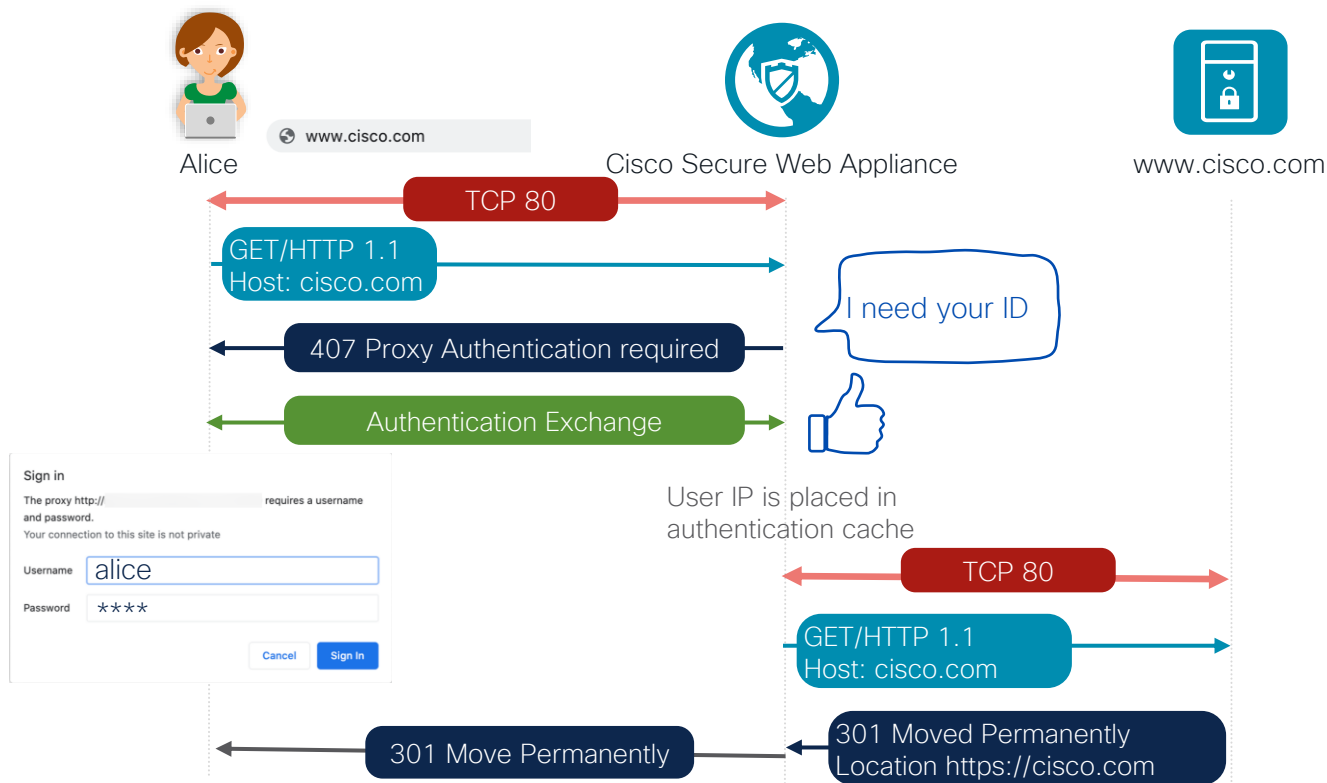


# We will focus on User Identity



# 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.

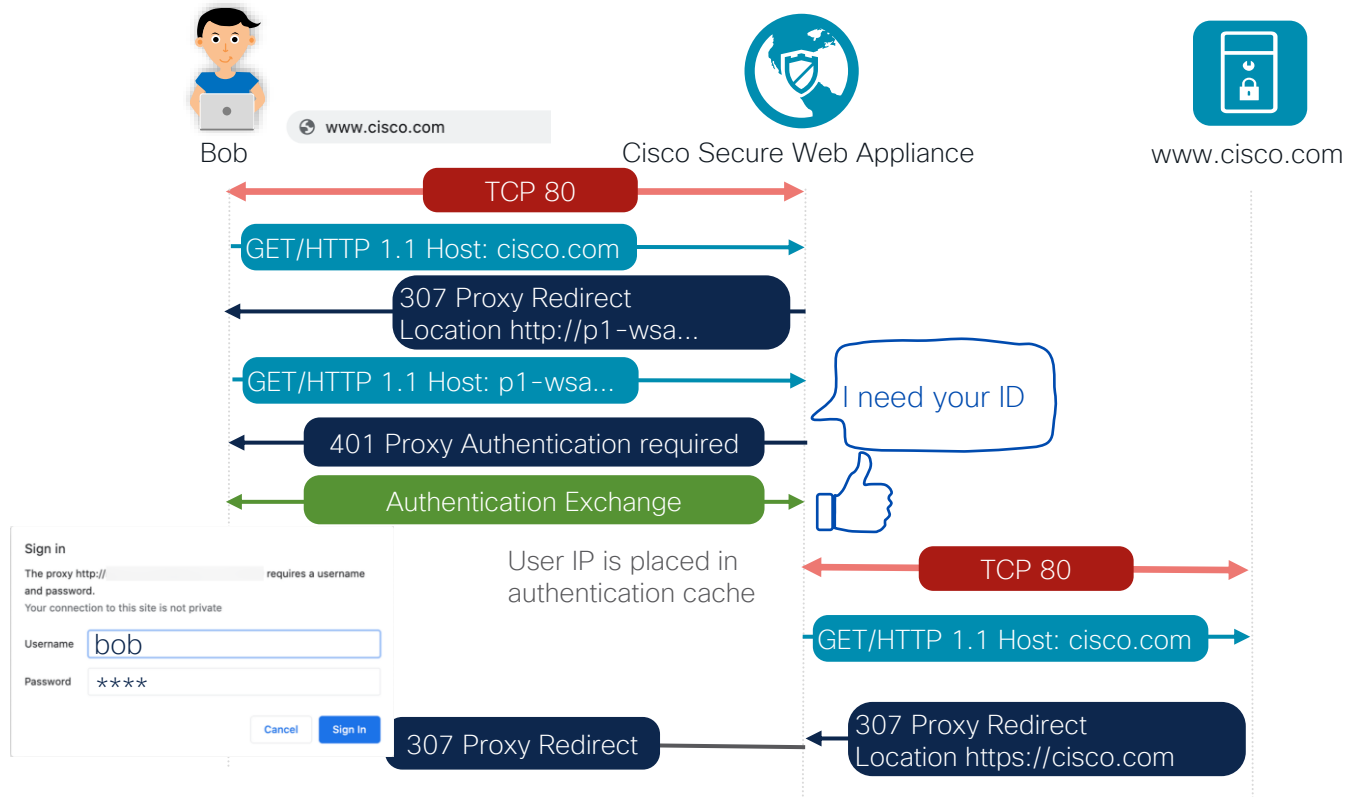
# How proxy authenticates a user: **explicit mode** example



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/B0001D000W0001N0001F0000S0000R0004/198.19.10.15/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
```

# What a Proxy Needs to Know?



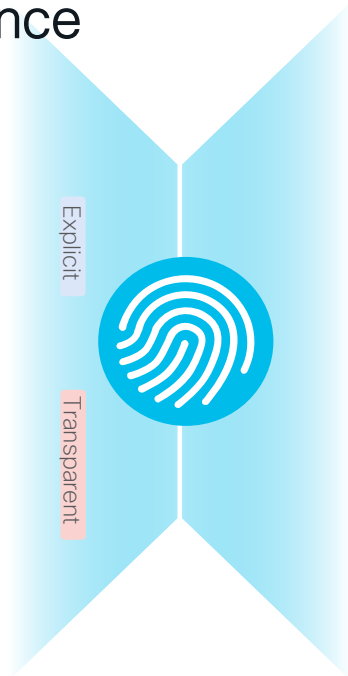
# How does Secure Web Appliance and Umbrella SWG define Identity?

## 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**



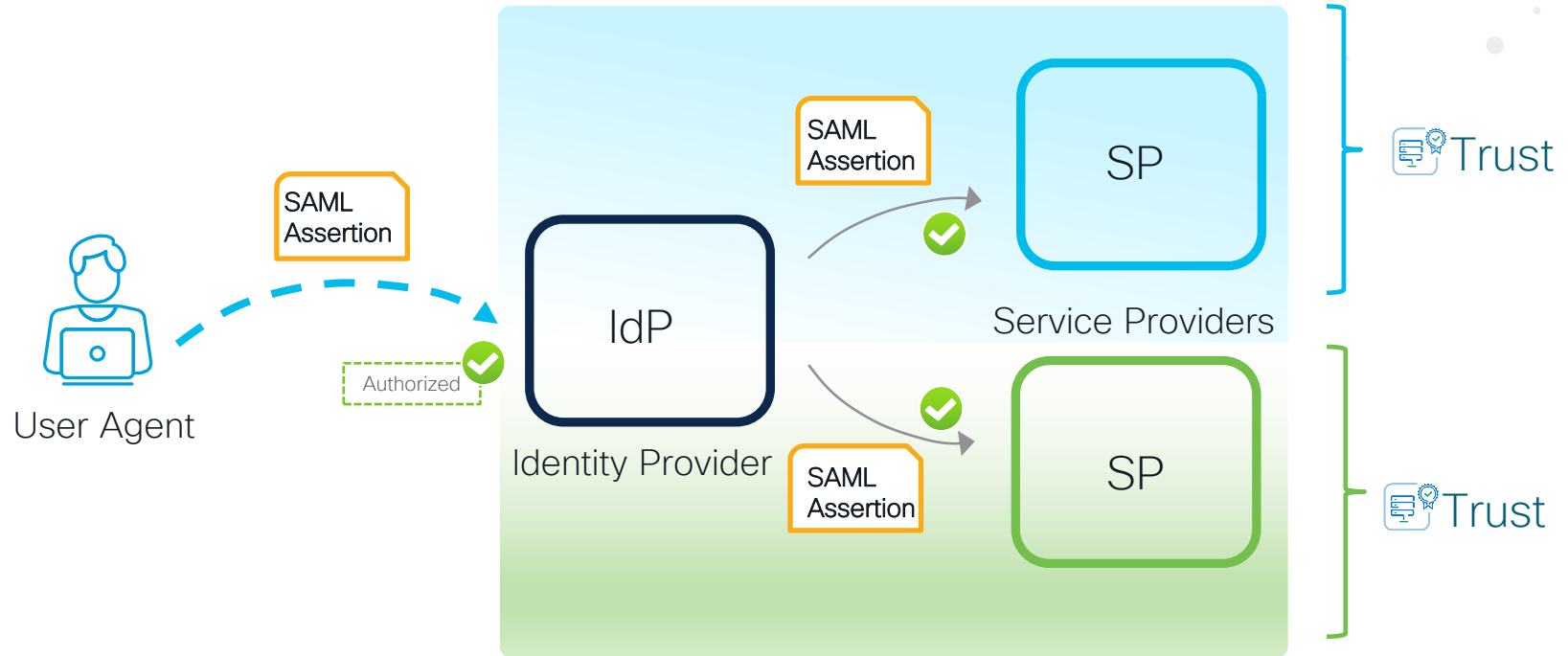
# 1. SAML

# SAML recap

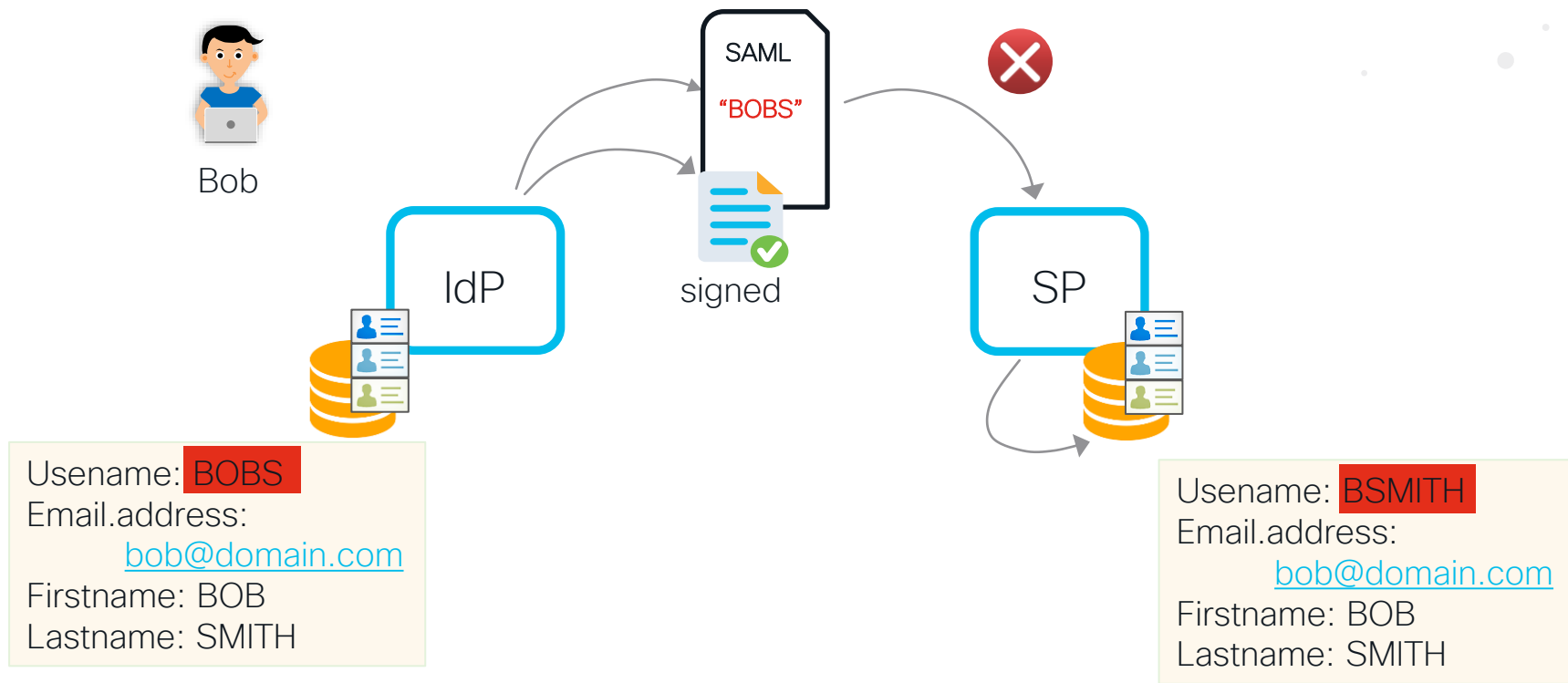
- Security Assertion Markup Language came in 2001
- Current version in use v2.0 (2005)
- SAML is an open standard
- Often used to provide single sign-on to web-based applications



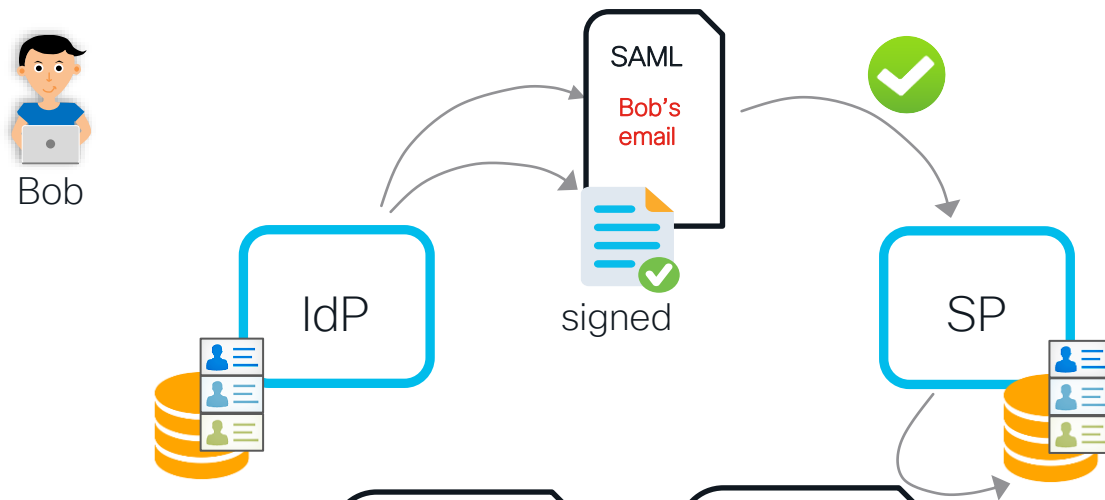
# SAML high-level



# SAML flow: user ID format



# SAML flow: user ID format



Username: BOBS

Email address:

[bob@domain.com](mailto: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

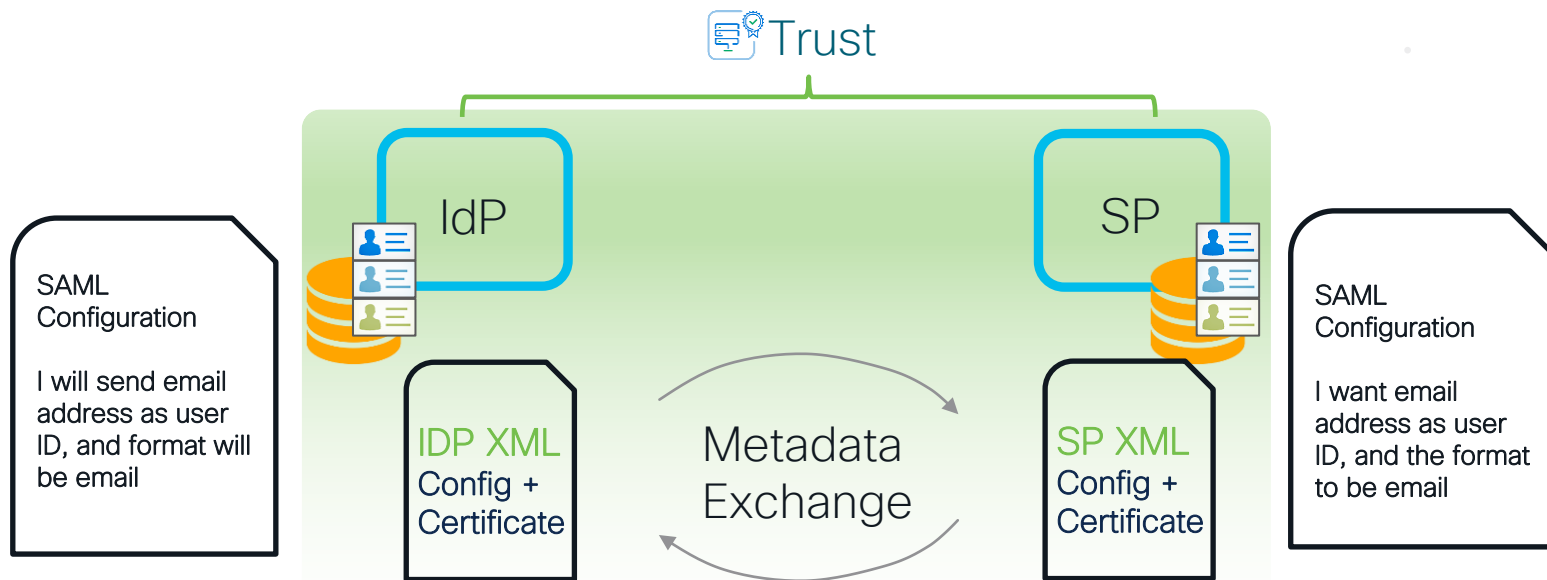
Email address:

[bob@domain.com](mailto:bob@domain.com)

Firstname: BOB

Lastname: SMITH

# SAML flow: Metadata Exchange



# SAML Metadata for Umbrella

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2023-08-12T06:44:04Z" cacheDuration="PT604800S" entityID="saml.gateway.id.swg.umbrella.com">
  <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIHmTCCBoGgAwIBAgIQQAF8JguwYwQLXswRTMhcBzANBgkqhkiG9w0BAQsFADBy
          ...
          07ZRC/RQQpcU+vgTfj0aM7Hqn5No+9iM2Qhwino=</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIHlzCCBn+gAwIBAgIQQAGCKMyZ4ruqIPPGozm1dDANBgkqhkiG9w0BAQsFADBy
          ...
          jNRR7ZM7DNqJJ2y7UMMKq67+PUTHPwDucRo+</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://gateway.id.swg.umbrella.com/gw/auth/acs/response" index="0"
      isDefault="true" />
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

**METADATA**

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

Umbrella URL for dynamic Metadata downloads:

[https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco\\_Umbrella\\_SP\\_Metadata.xml](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

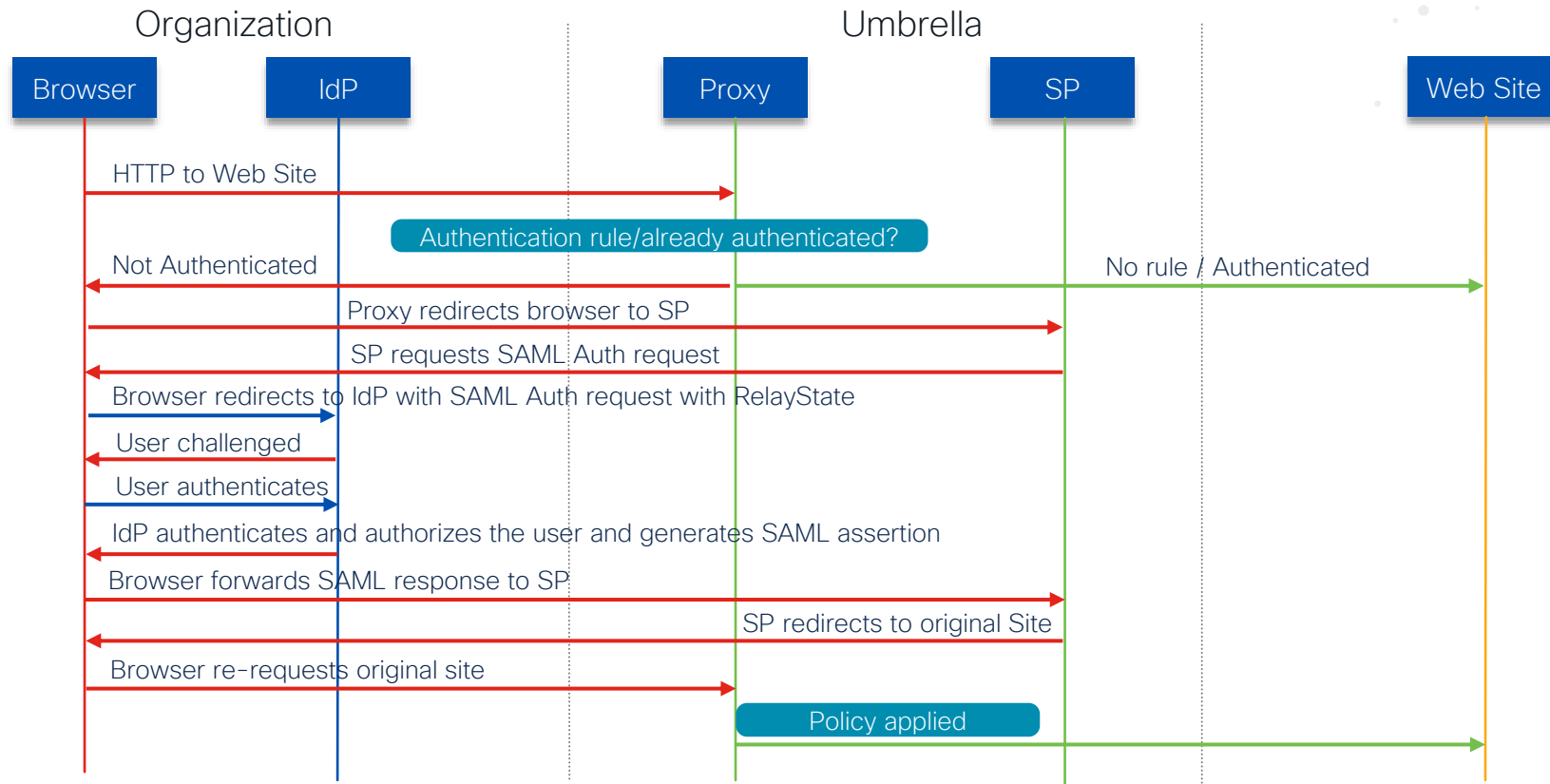


manual claims map is required in ADFS



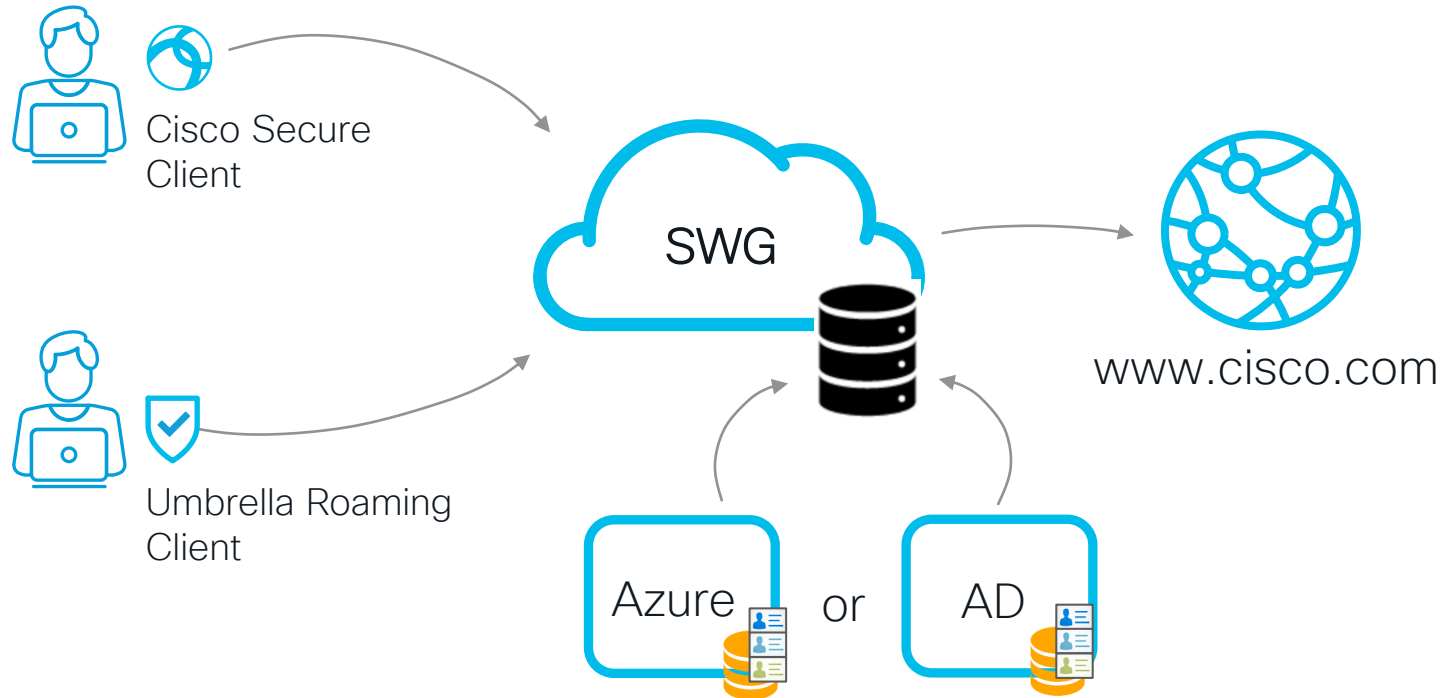
# SAML Flow: Full Picture

SP and IdP never communicate directly!

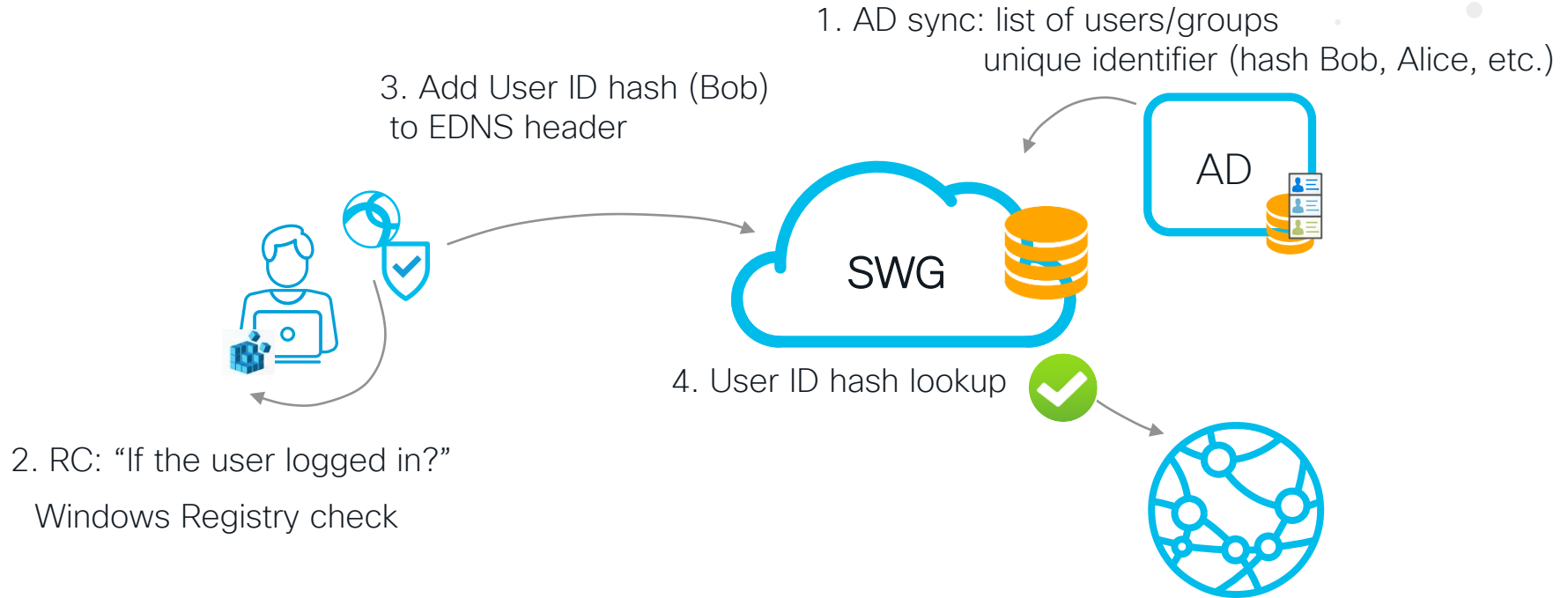


## 2. Remote Users

# 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)

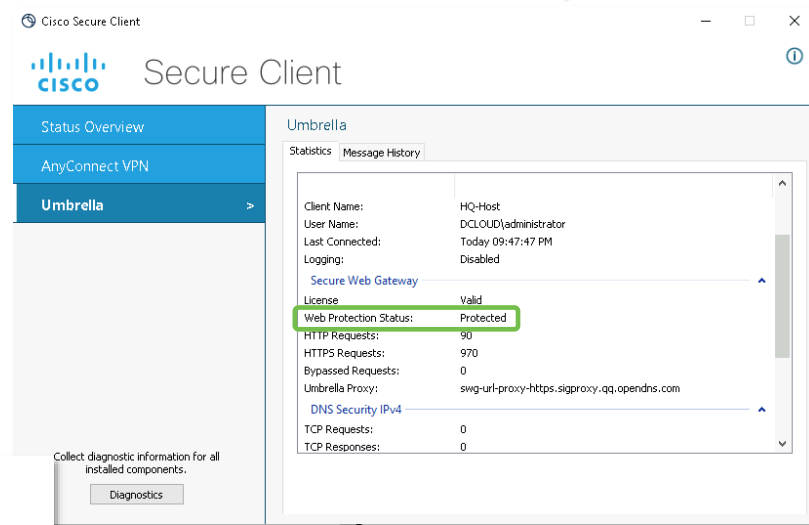
- AnyConnect can be used across an entire enterprise
- Both Umbrella DNS and Secure Web Gateway services can co-exist
- Needs to be enabled in Umbrella Portal:  
“Deployments > Roaming Clients > Settings”

## 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": "LS0tLS1CRUdJTiBQVUJMSUMgSOVZLS0tLS0KU1JQK1qQU5CZ2txaGtpRz13MEJBUUQGU0FPOFRRC",
      "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



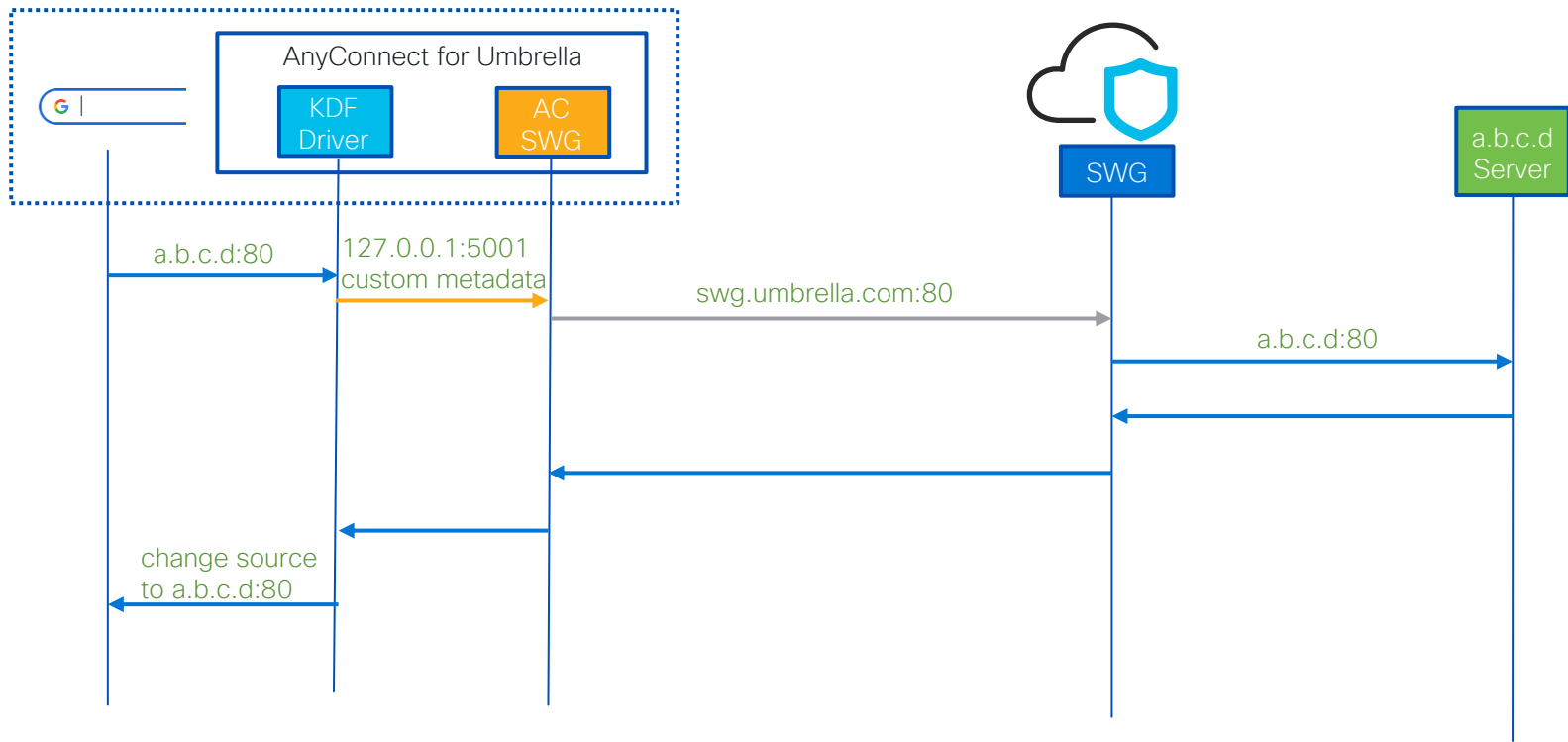
2. process intercepts any web requests TCP 80/443

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

```
X-USWG-SK: tz39AYT/UEk3oaaHbX0G2crg35Agu15gXwP3H+1E7wYdw0d7+bGRux7eImqH0/
d3nU2aJ3Qo6XqDYQ3XvxybsTHCwdaP6hFEUVGHzcVEgW0wP8XofzFOIf+OSRTgWLAfDg0VUNeyLSiEexrV1PLEtkc5m8D3Yw6Hn
d1AY07DUJZ/h63PDucktgW27YI113LZDf538LjEx1pFZ04sFm+1W2FTPyashCa8Spw==
X-USWG-Data:
CQY10wvcwjnRmpBqYzj67VvkUQneNAqki7WkrEwB507ghnAUJGTfV4GCl0RwDROc5Q+6W54okDHQmZkc67sQFnq1L2kXC6XXS61
nyuICE5w+DEhImzDkS9qxD5gFNqkC04Lyjh/2gVEduDbVfphr8YNUcxP/1ez1wdd0NL2GIZ273JK94fzqH1dNu3zRkxLxR+d0m0E
Zgve63/6zt3qfd30LHjL1g1uGwr1YLK+HyEx6LTvW3q5xvYh6350P21ZbK9r+6RXedwgv9QNWVsc8051zD8K17fZ45fsTAy535
X-USWG-PKH: 52379614bb86e028bbdcfeeabe2d743e
```



# Remote User: Traffic Flow



# Remote User: AC-SWG Headers

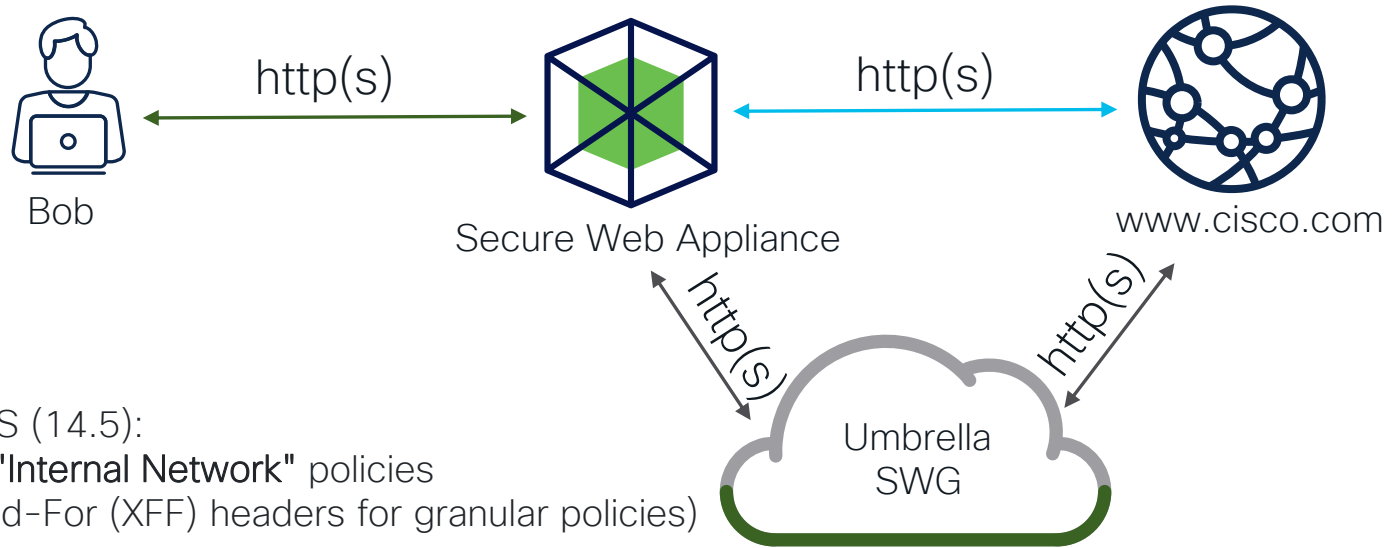
- **X-USWG-SK** – Encrypted Session Key
- **X-USWG-Data** – Org ID + Identity (Device/User) + 'timestamp'
- **X-USWG-PKH** – Hash of RSA Private Key

```
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/
Pmrj8DrZAFcv1VcRDjeuBNWnTOhrgnK2qb45A9JPM60TuDQdc1KTqqQ9ntVEZv0SnQMBen99jzsiNis1KgSfHx2HZCiHfqt+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

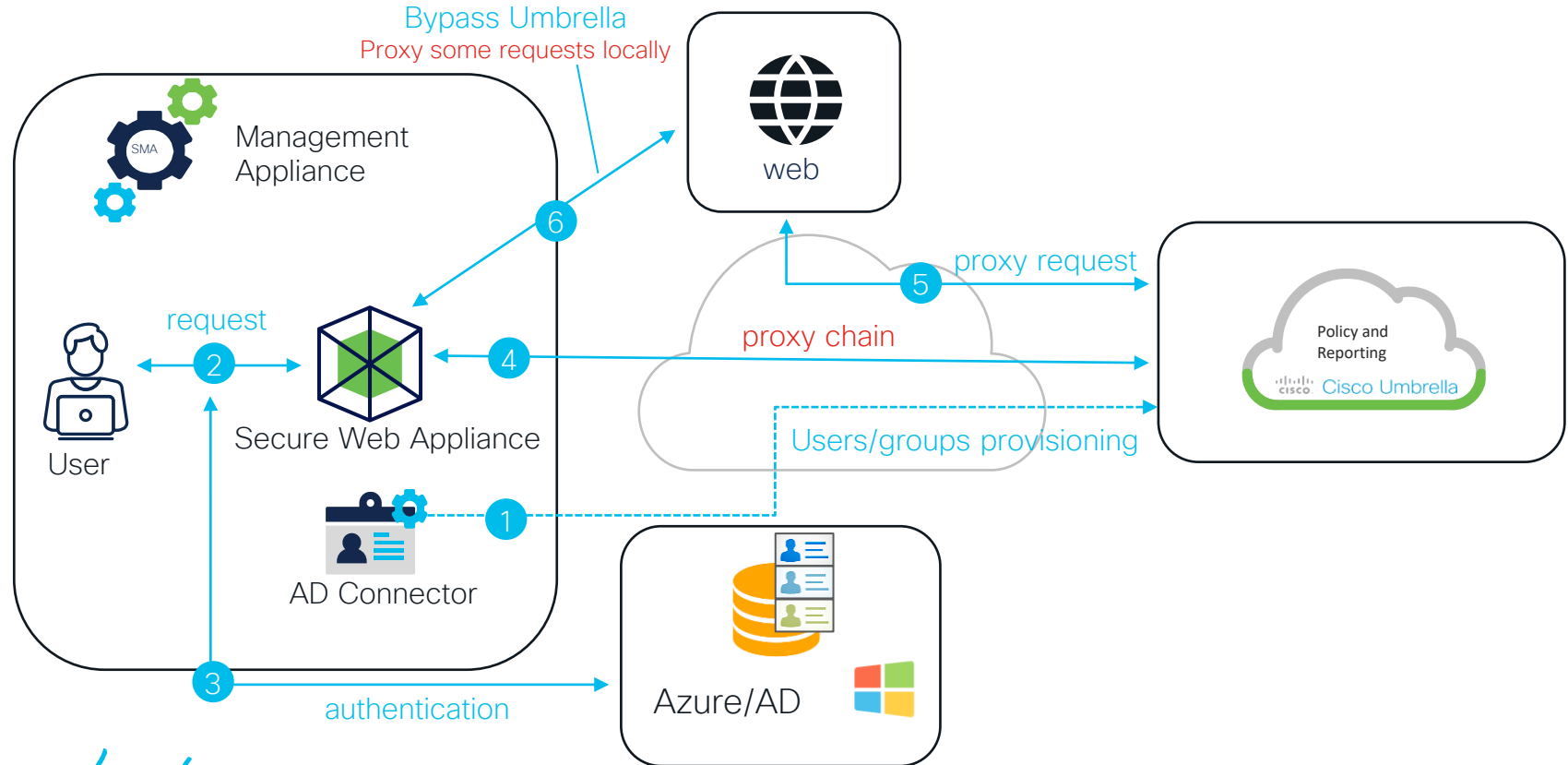


Before AsyncOS (14.5):  
WSA provides "**Internal Network**" policies  
(or X-Forwarded-For (XFF) headers for granular policies)

# Seamless Identity: Adding UserID to proxy Chaining

- **Granular** policy/reporting based on User Identity
- WSA Customers can take advantage of authentication methods they may already be using in the WSA such as **Kerberos/NTLM** or ISE.
- **Consistent** user identity between WSA 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



## Demo Scenario 1:

- User is trying to access blocked category “News” ([www.bbc.com](http://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-42179F8366CDAEAF0946-4F277AA9A29C-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)

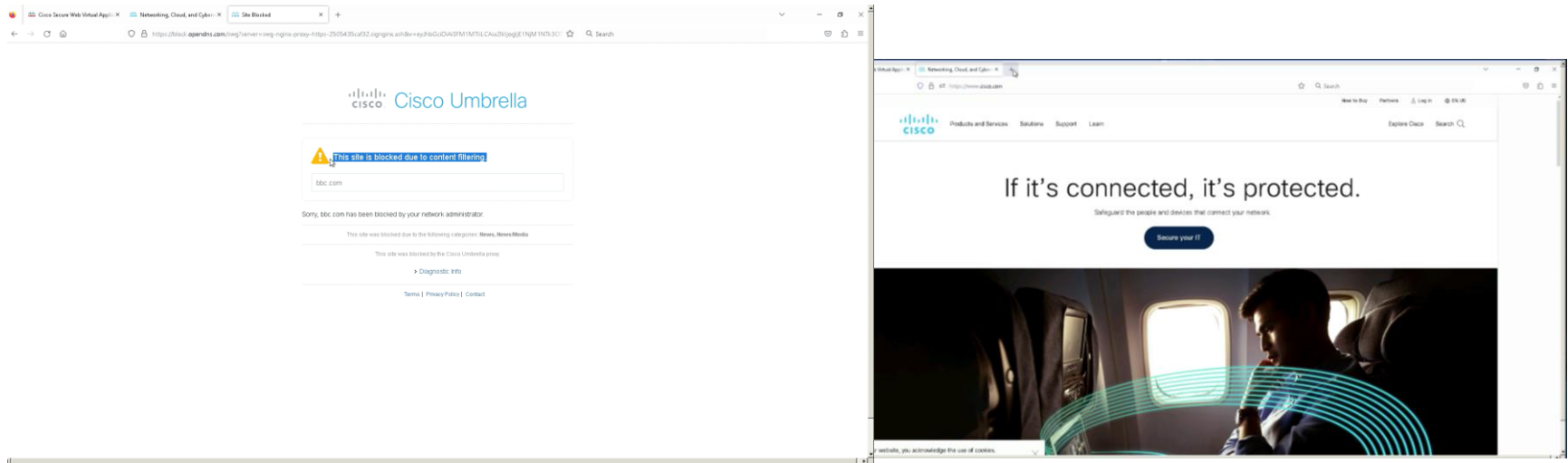
[Edit Settings...](#)



## 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](http://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
<input checked="" type="checkbox"/> 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 ▼
<input type="checkbox"/> 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.

The screenshot shows the Cisco Secure Client window. The left sidebar has three items: 'Status Overview' (selected), 'AnyConnect VPN', and 'Umbrella'. The main area is titled 'Status Overview' and contains two sections. The first section is 'AnyConnect VPN (Disconnected)' with details: Bytes Sent: 0, Bytes Received: 0, Time Connected: 00:00:00, Client Address (IPv4): Not Available, Client Address (IPv6): Not Available, Server Address: Not Available, and Session Disconnect: None. The second section is 'Umbrella' with details: IPv4 DNS Protection Status: Protected, IPv6 DNS Protection Status: Disabled (no network), **Web Protection Status: Disabled** (highlighted with a blue bar), and Last Connected: Today 08:33:54 PM. At the bottom, there is a button labeled 'Diagnostics' and a note: 'Collect diagnostic information for all installed components.'



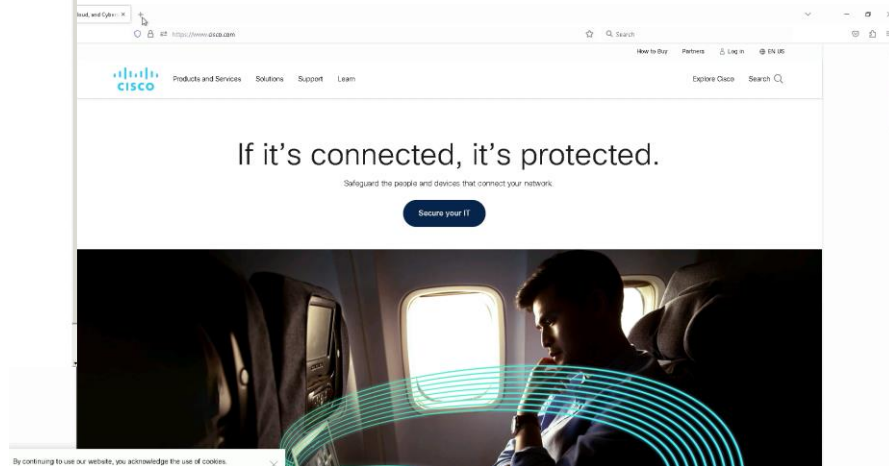
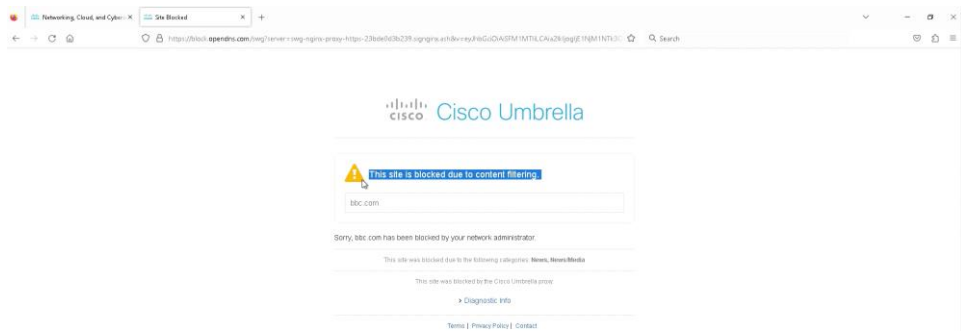
The screenshot shows the Cisco Secure Client window. The left sidebar has three items: 'Status Overview', 'AnyConnect VPN', and 'Umbrella' (selected). The main area is titled 'Umbrella' and contains two tabs: 'Statistics' and 'Message History'. The 'Statistics' tab is active and shows a table of client information: Client Name: HQ-Host, User Name: DCLoud/administrator, Last Connected: Today 08:38:11 PM, and Logging: Disabled. Below this is a section for 'Secure Web Gateway' with a table: License: Valid, **Web Protection Status: Protected** (highlighted with a blue bar), HTTP Requests: 0, HTTPS Requests: 9, Bypassed Requests: 0, and Umbrella Proxy: swg-url-proxy-https.sigproxy.qq.opendns.com. At the bottom, there is a button labeled 'Diagnostics' and a note: 'Collect diagnostic information for all installed components.'

## 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

No.	Time	Source	Destination	Protocol	Length	Info
14620	4.248980	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	5.308184	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.ca/wp-content/
45030	22.820250	198.19.10.201	198.19.10.52	HTTP	438	GET http://k20xb9meqz7a.924329928.com
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?ip=4 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-Forwarded-For: 201\r\n
Via: 1.1 wsa.cloud.cisco.com:80 (Cisco-WSA/14.5.0-537)\r\n
[truncated]X-USWG-Data: 1UP50TJue1Q7r9f5bmcqhcUpqR2AKMqA2EtQTQ/obeaP6nS0M3ES3qQUcWLB09NoDM/SPYPSY6mJG/rp3Ng8bXkK
[truncated]X-USWG-SK: LQY7rNjV81ankjcgAuAY2ZrWm8tHn2jPY3F0H+DN1jW/qD9pLmPl1fXxfS3ALRpUOm9OePrkU9oWdXUNKX0XgnzPr
X-USWG-PKH: f0d78ed86ebc390157ca14ba10978cfar\r\n
\r\n
[Full request URI: http://bbc.com/]
[HTTP request 1/1]
[Response in frame: 47562]

No.	Time	Source	Destination	Protocol	Length	Info
660	10.510156	198.19.10.15	146.112.43.24	HTTP	1325	GET / HTTP/1.1
3007	32.340423	198.19.10.15	146.112.43.240	HTTP	357	GET /canonical.html HTTP/1.1
3019	32.384677	198.19.10.15	146.112.239.215	HTTP	359	GET /success.txt?ip=4 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_B6:94:85 (00:50:56:B6:94:85), Dst: VMware_b8:14:fd (00:50:56:b8:14:fd)
> Internet Protocol Version 4, Src: 198.19.10.15, Dst: 146.12.43.24
> 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, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
[truncated]X-USWG-Data: sIUdEdHb+h5u5QW4pCAlxH09wssChetter8LUnARAIzUGC6+ku+/BNY41rN3adB1Rda8gf7v1VRHdxisk6yEc/asx3VB5DFHWE4Y
[truncated]X-USWG-SK: K4p282BTjHtH9bomfmx0UCljPycBTZ3axHv08LeERjPiowUy+Dlmply0h8Hr2gQnF8H8qFhJ845QWFHjG93Igl/SyLwhoeFF0bQ
X-USWG-PKH: 52379614bb86e028bbdcfeeb2d743e\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

# Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand).

# Security Technologies

## Secure Access Service Edge (SASE)

Learn how Secure Access Service Edge combines networking and security functions in the Cloud to deliver seamless, secure access to applications, anywhere users work. Core functions include software-defined wide area network, secure web gateway, firewall as a service, cloud access security broker, and zero-trust network access. The SASE model aims to consolidate these functions in a single, integrated cloud service.

START

Feb 6 | 08:30

### **TECSEC-3780**

Cisco SASE for Architects and Implementation Engineers

Feb 7 | 08:30

### **BRKSEC-2128**

SASE the SOC's New Best Friend

Feb 7 | 14:45

### **BRKSEC-2238**

Getting SASE with Umbrella and Meraki - Understand best practices for simple and flexible integrations between Meraki and Umbrella

Feb 7 | 15:30

### **BRKSEC-2143**

Do You Know Where Your Data Is? A Deep Dive on Cisco Umbrella CASB and DLP and How to Protect your Locations, Data and Users

Feb 7 | 15:30

### **BRKSEC-2129**

Deploy & Scale SASE for Secure Remote Worker in the Cloud with Cisco+ Secure Connect

Feb 7 | 17:00

### **BRKSEC-2438**

Solving Today's Challenges with the Newest Features in Cisco Umbrella

Feb 8 | 08:30

### **BRKOPS-2857**

Deploy Visibility in Your SASE Architecture With ThousandEyes

Feb 8 | 08:45

### **BRKSEC-2644**

Secure Access Service Edge - From Home to the Office with Cisco SASE!

Feb 8 | 10:30

### **BRKSEC-2287**

Who is Behind the Umbrella? A View on User Authentication with Cisco Umbrella

Feb 9 | 12:00

### **BRKENT-2312**

Evolution of Cisco SD-WAN Security and Journey Towards SASE

If you are unable to attend a live session, you can watch it [On Demand](#) after the event

**CISCO** *Live!*



- 
- Feb 9 | 14:00  
**LTRSEC-2272**  
SASE - The best of 2 worlds  
(Networking and Security)
- Feb 9 | 14:20  
**PSOSEC-1214**  
How to Reach the Full Promise  
of SSE
- Feb 9 | 15:45  
**BRKMER-1003**  
Cisco+ Secure Connect  
- Connect and Secure with Meraki
- FINISH** Feb 10 | 11:00  
**BRKSEC-2218**  
Cisco Secure Hybrid SWG  
- Your First Step to Your  
SASE Journey

If you are unable to attend a live session, you can watch it [On Demand](#) after the event

**CISCO** *Live!*

# Security Technologies

## Zero Trust

Learn how Cisco will help you deploy a broad range of technologies in order to deploy your end to end Zero Trust strategy.

START

- Feb 5 | 16:00  
**LABSEC-2089**  
Multi-factor Authentication:  
Integration of DUO with ISE for MFA
- Feb 6 | 08:45  
**TECSEC-2007**  
Find Your Zen with Cisco Secure  
Workload for Zero Trust Segmentation
- Feb 6 | 08:45  
**TECSEC-2781**  
Zero Trust: From understanding the  
risks to architecting a practical solution
- Feb 6 | 15:20  
**PSOSEC-1210**  
A global view on Zero-Trust  
- mapping your business resilience  
requirements
- Feb 7 | 08:45  
**BRKSEC-2445**  
The Art of ISE Posture, Configuration  
and Troubleshooting

- Feb 7 | 16:45  
**BRKSEC-2053**  
Zero Trust: Securing the  
Evolving Workplace
- Feb 7 | 17:00  
**BRKSEC-1139**  
Application Security  
- The Final Frontier
- Feb 8 | 10:45  
**BRKSEC-2096**  
Securing Industrial Networks:  
Where do I start?
- Feb 8 | 13:30  
**BRKSEC-2748**  
Taking Authentication to the Next Level  
with Cisco Secure Access by Duo
- Feb 8 | 17:00  
**BRKSEC-2123**  
Solving the Segmentation Puzzle!  
Secure Workload and Secure  
Firewall Integration

If you are unable to attend a live session, you can watch it [On Demand](#) after the event

**CISCO** *Live!*

# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from 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 Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>



# Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand).

# Please Fill Out The Survey!





The bridge to possible

# Thank you

CISCO *Live!*

Q&A time



CISCO *Live!*

ALL IN