
cisco Live!
Let's go

The bridge to possible

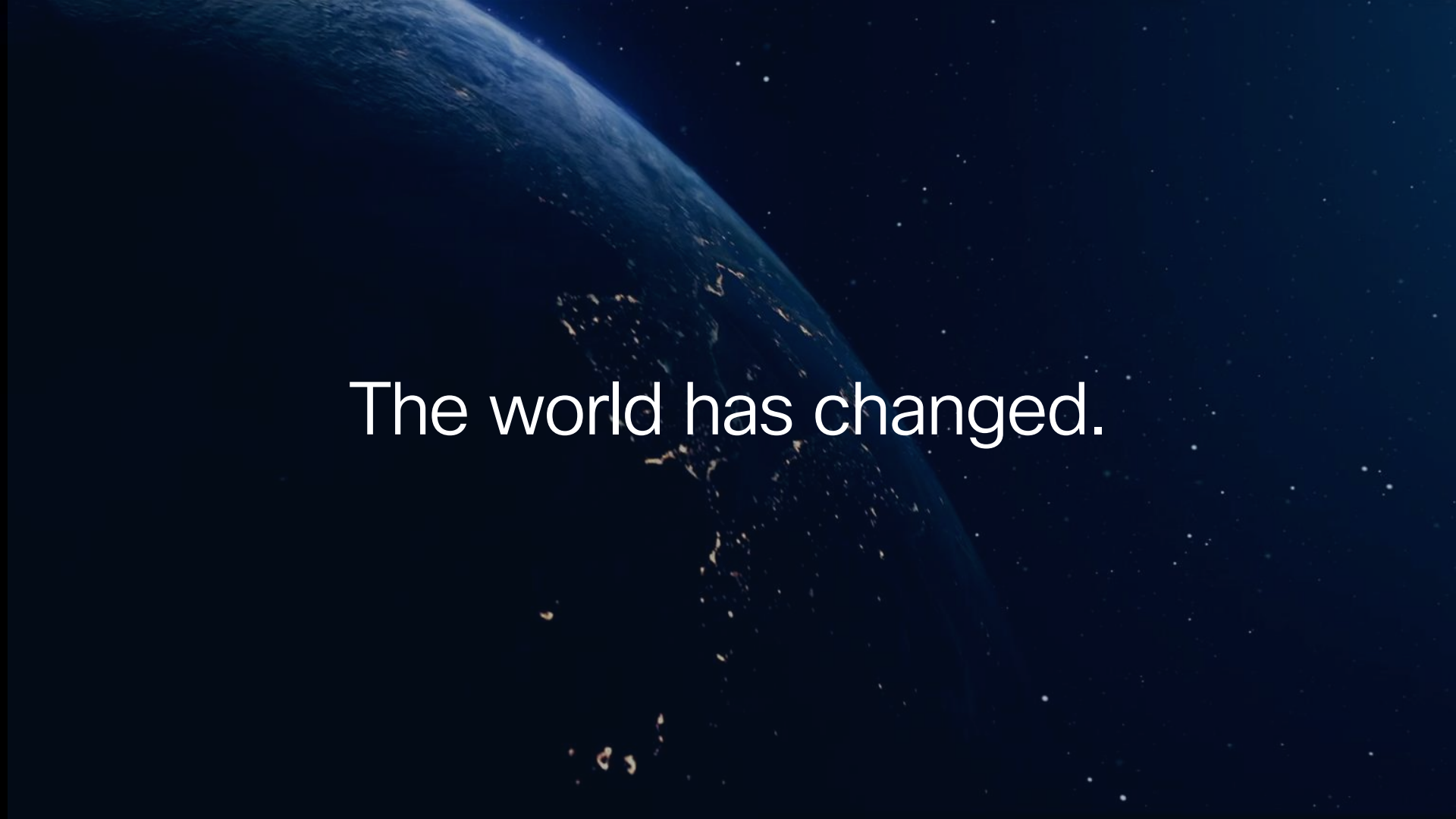
Who is Behind the Umbrella?

A View on User Authentication with Cisco Umbrella

Julia Sevostianova, Technical Projects Systems Engineer

cisco Live!

BRKSEC-2287


The world has changed.

89%

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

Accenture Future of Work Study 2021

63%

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

Cisco Hybrid Work Index 2022

77%

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”

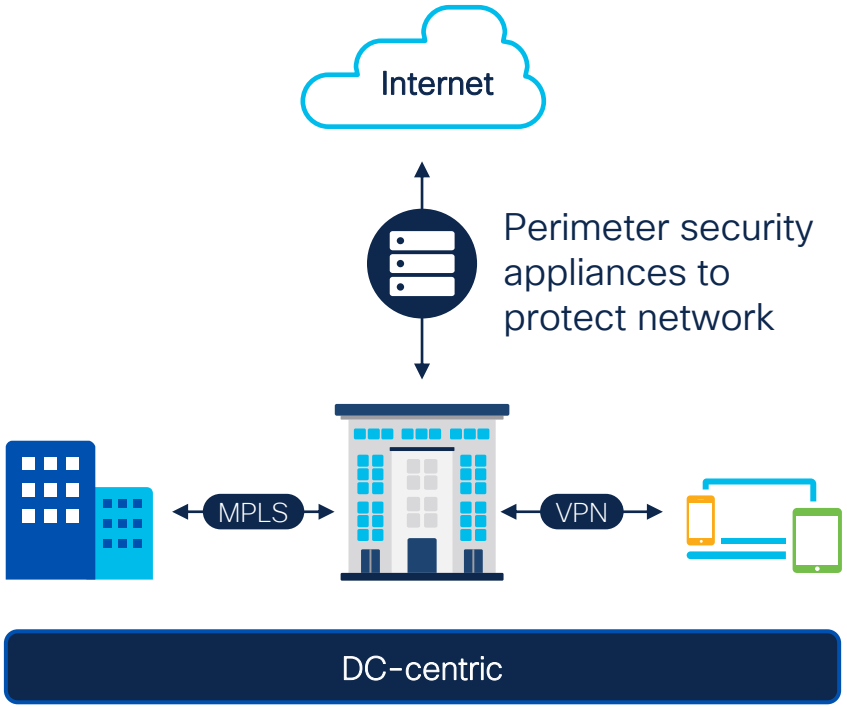
For Your Reference

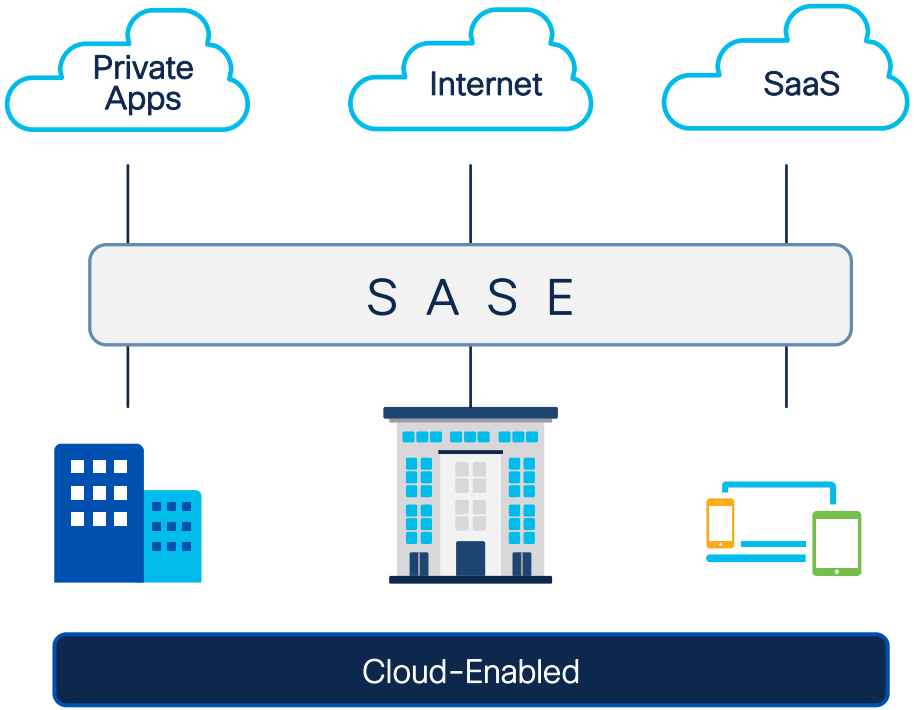
Agenda

- 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

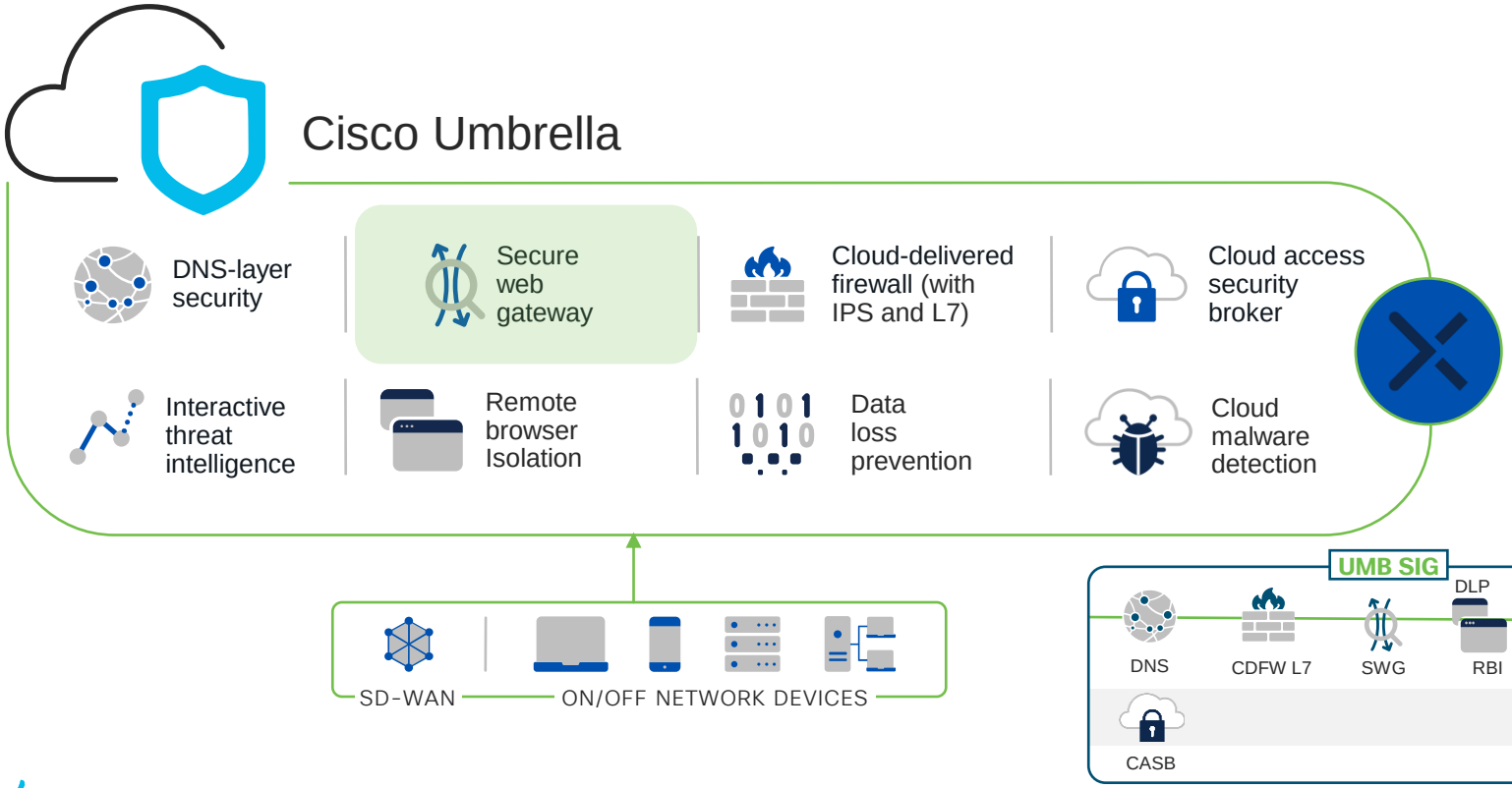
Umbrella for Beginners

From DC-centric topology to SASE





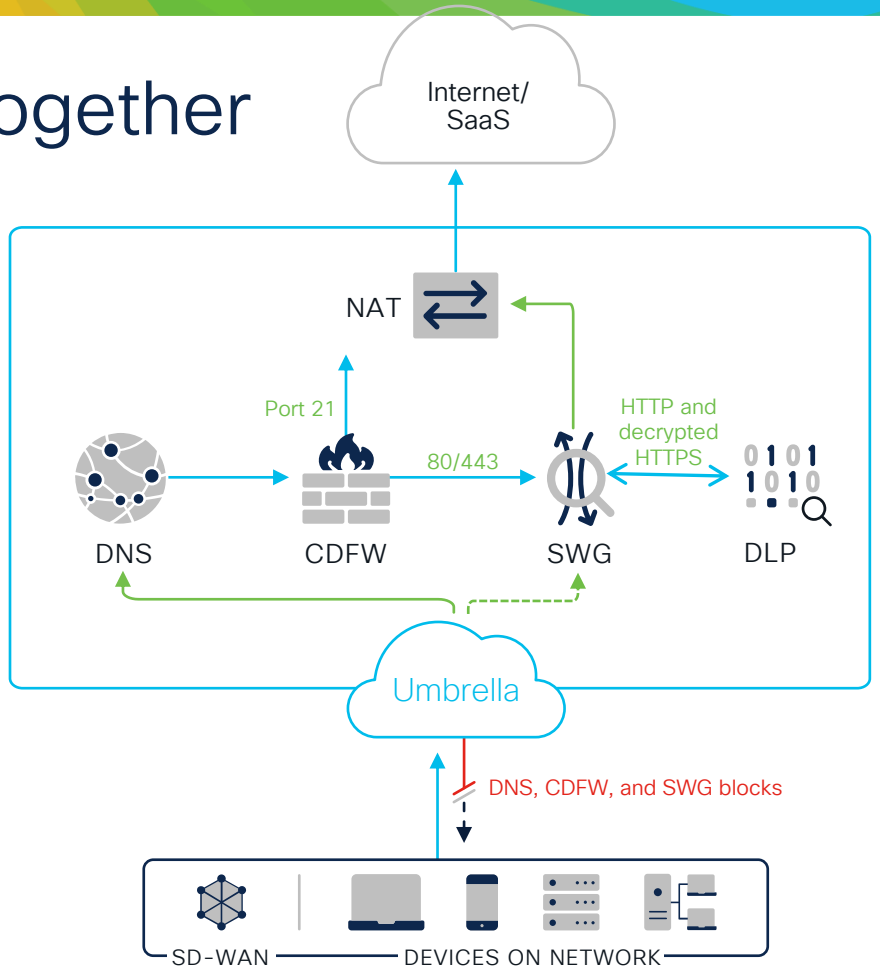
Cisco Umbrella – SIG overview



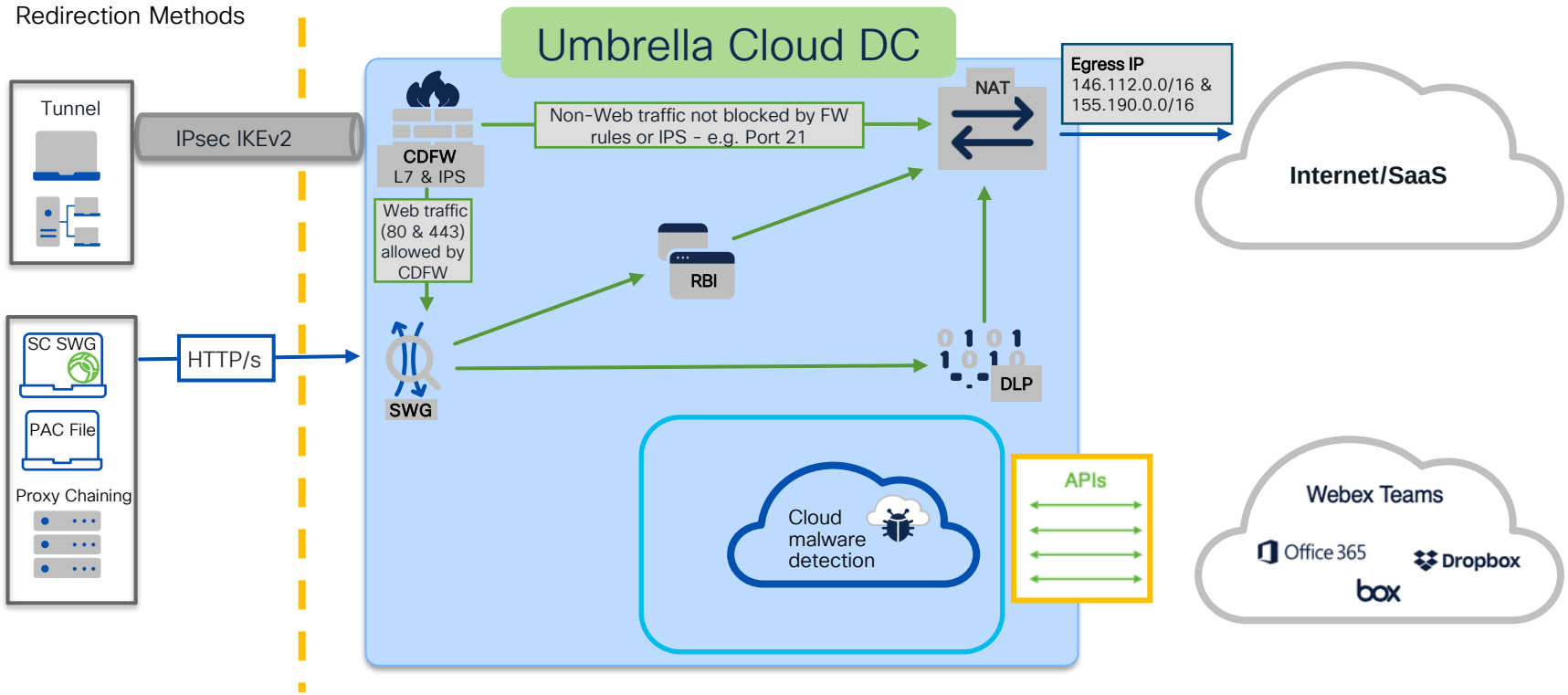
Enforcement that works together

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



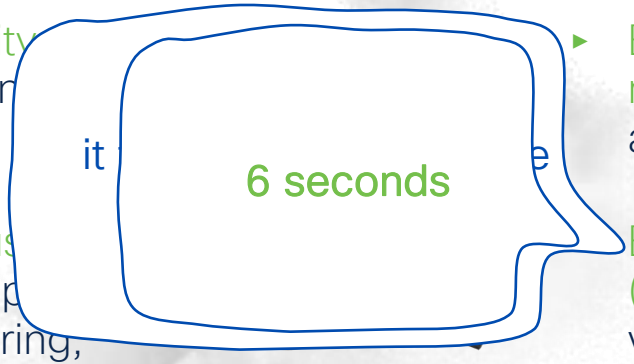
SIG Deployment Types & Traffic Flow Diagram



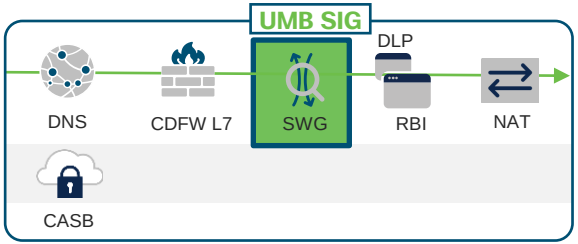
Secure web gateway: full web proxy

Deep inspection and control of web traffic

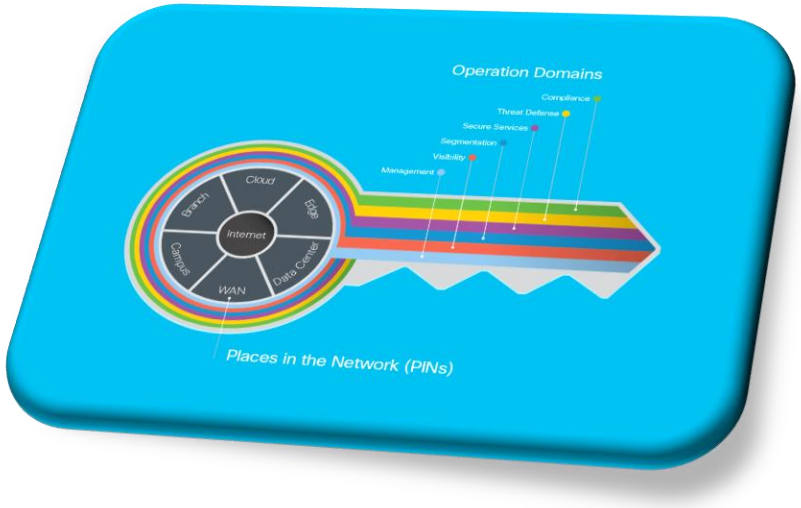
- Gain additional visibility via full URL logging and cloud app discovery
- Enforce acceptable use policy via granular app controls, content filtering, and URL block/allow lists



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

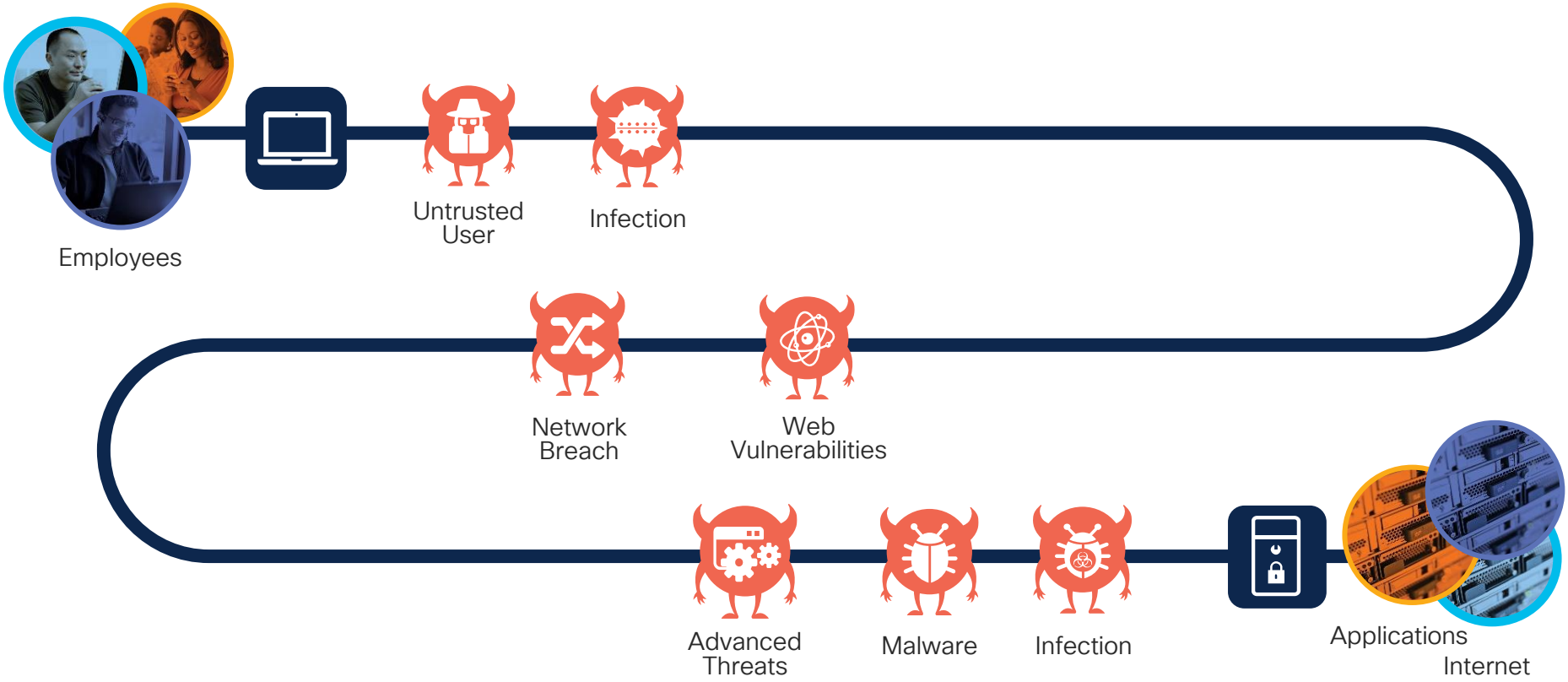


SAFE Framework

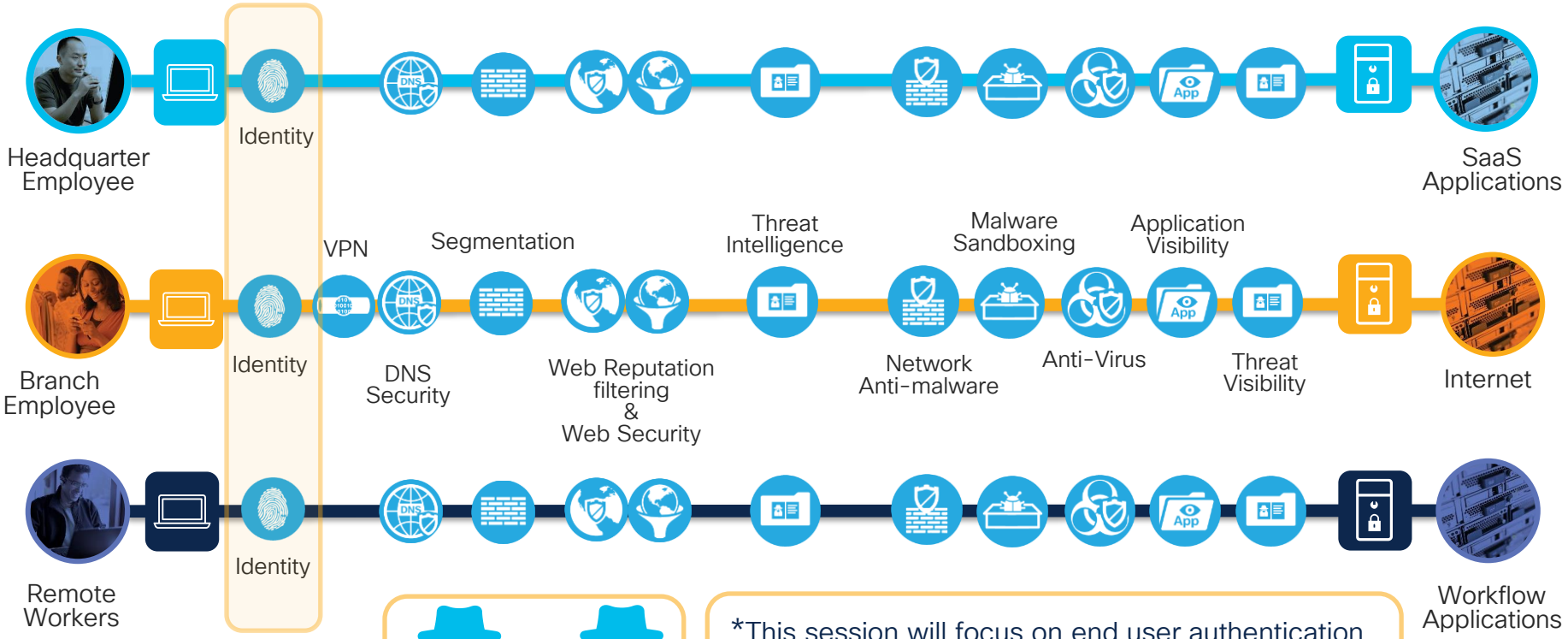


SAFE model: attack surfaces

SAFE model: threats



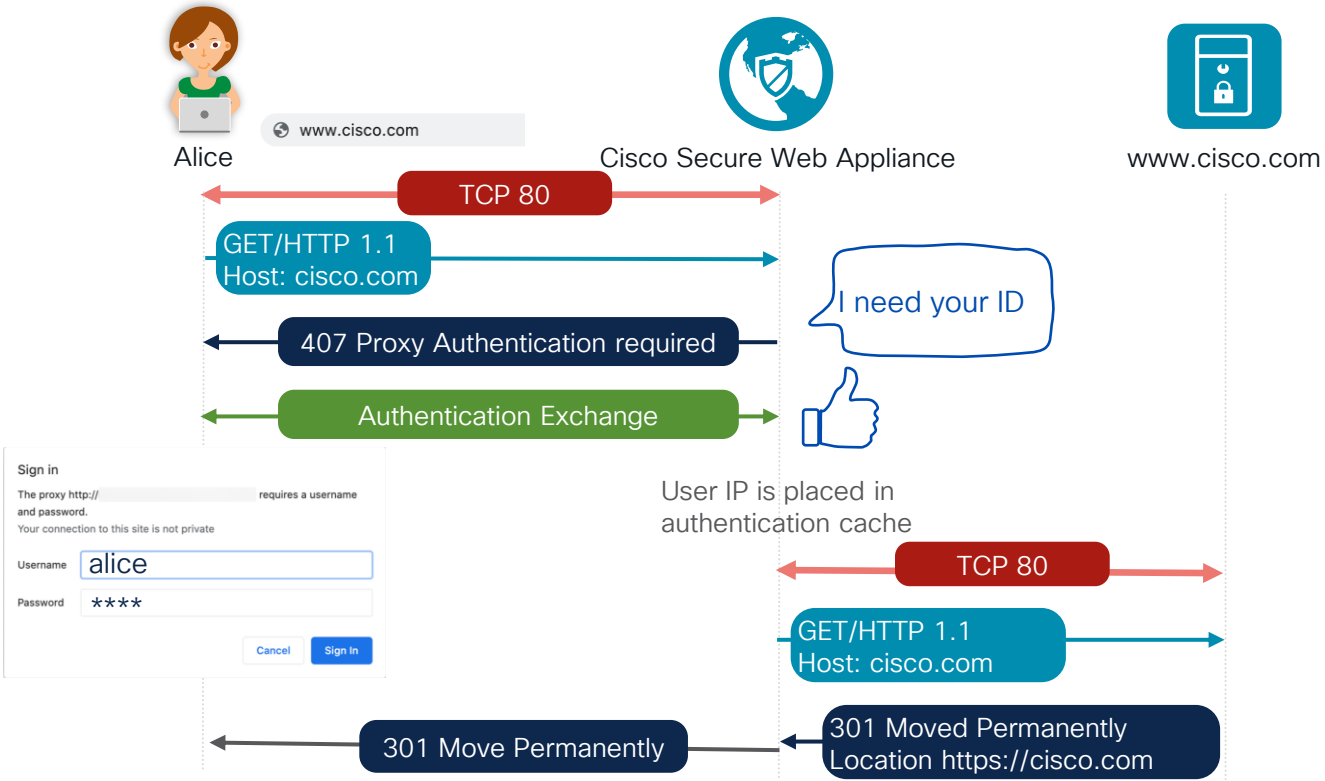
We will focus on User Identity



*This session will focus on end user authentication (does not cover management authentication, or user provisioning)

Traffic Flow:
User Authentication

How proxy authenticates a user: explicit mode example



How proxy authenticates a user: explicit mode example

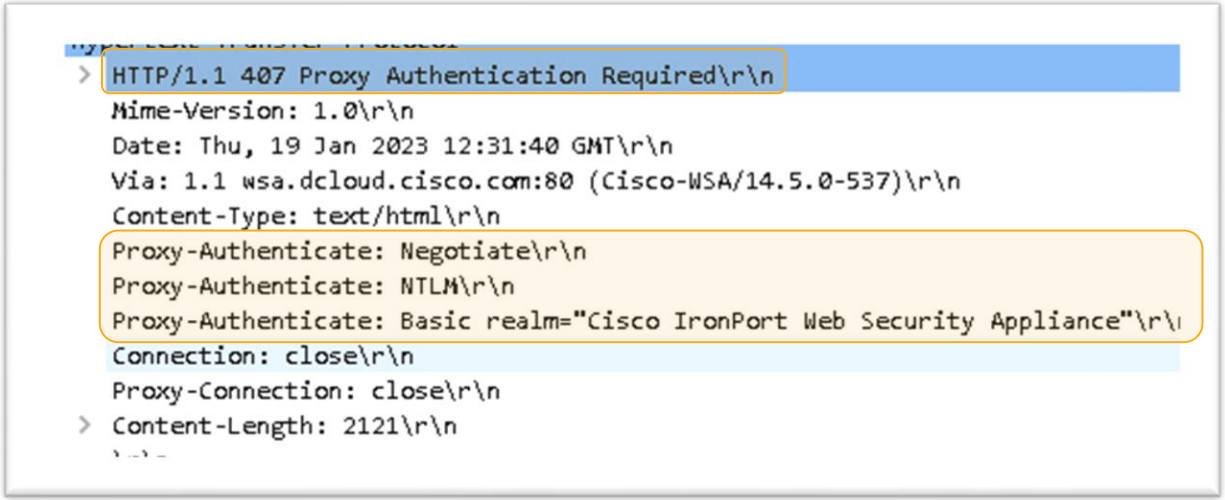
Alice's computer sends an HTTP GET request to the proxy.

```
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.



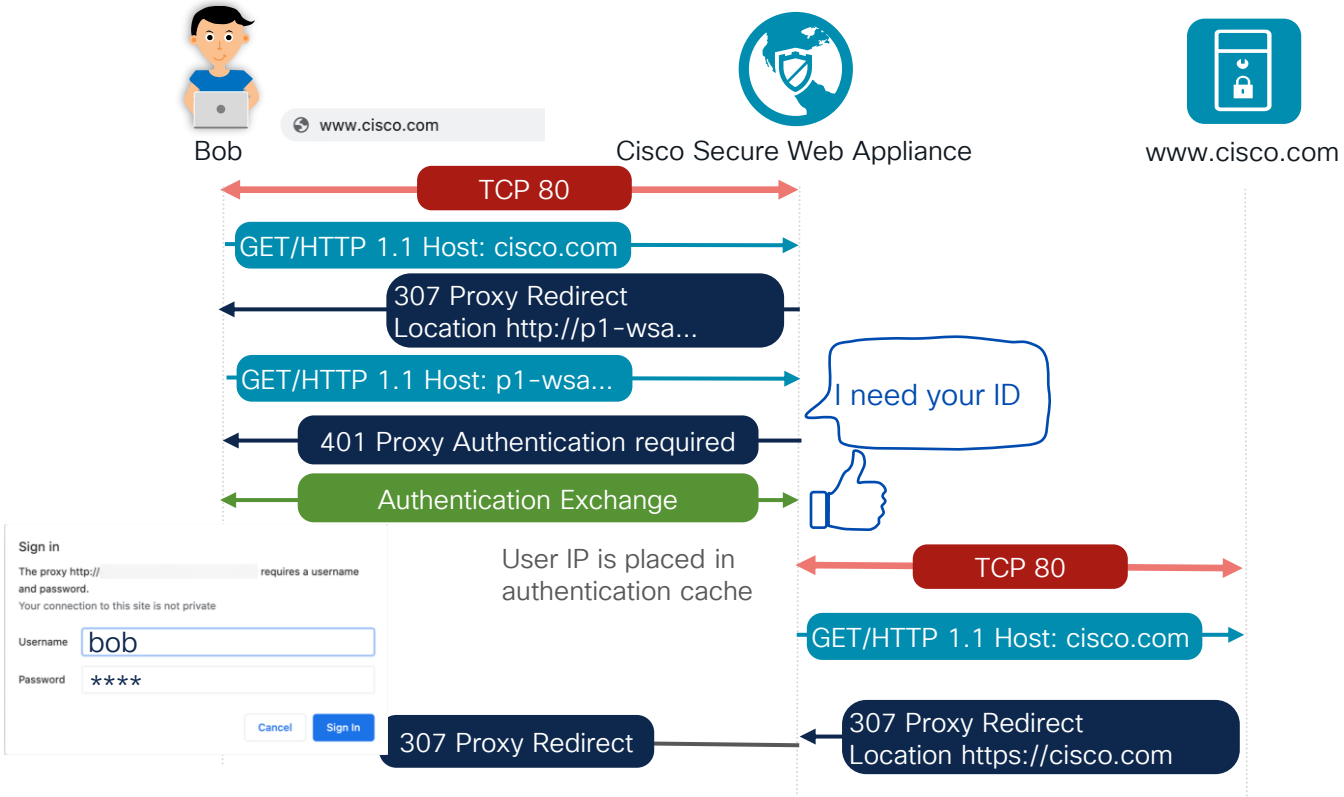
Includes **proxy authentication headers**. In this example it shows that Alice is allowed to authenticate using Kerberos which is mentioned as negotiate or NTLM, or Basic.

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.

```
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.**

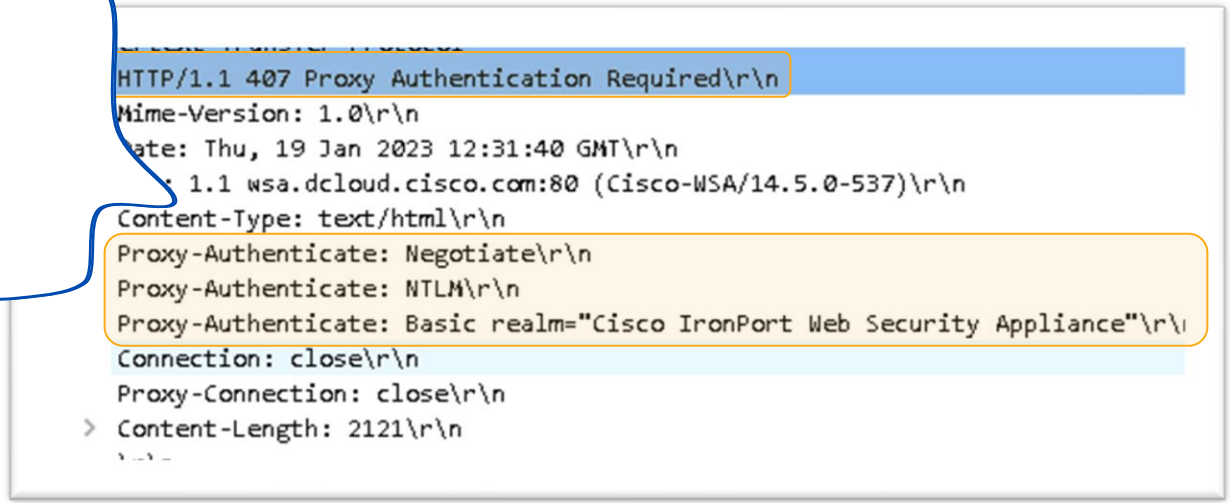
```
Hypertext Transfer Protocol
  HTTP/1.1 401 Authorization Required\r\n
  Mime-Version: 1.0\r\n
  Date: Thu, 19 Jan 2023 20:23:14 GMT\r\n
  Via: 1.1 wsa.dcloud.cisco.com:80 (Cisco-WSA/14.5.0-537)\r\n
  Content-Type: text/html\r\n
  WWW-Authenticate: Negotiate\r\n
  WWW-Authenticate: NTLM\r\n
  WWW-Authenticate: 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



What a Proxy Needs to Know?

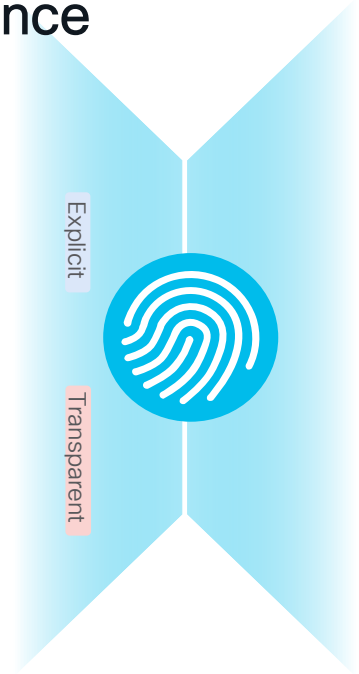
How does Secure Web Appliance and Umbrella SWG define Identity?

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:

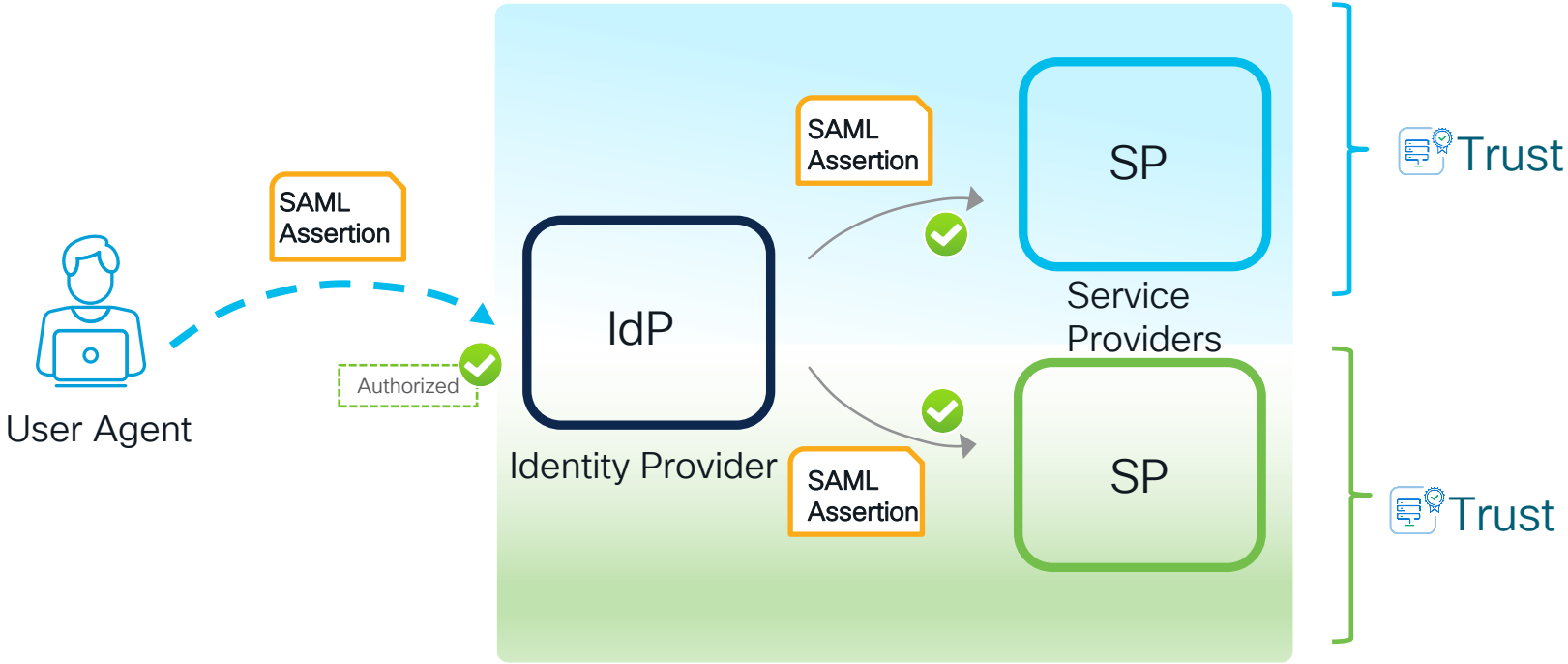
1. SAML Integrations (Duo, Azure, Okta, ADFS, PingID, etc.)
2. Remote User (Secure Client SWG, Umbrella Client)
3. Proxy Chaining with Seamless Identity

1. SAML

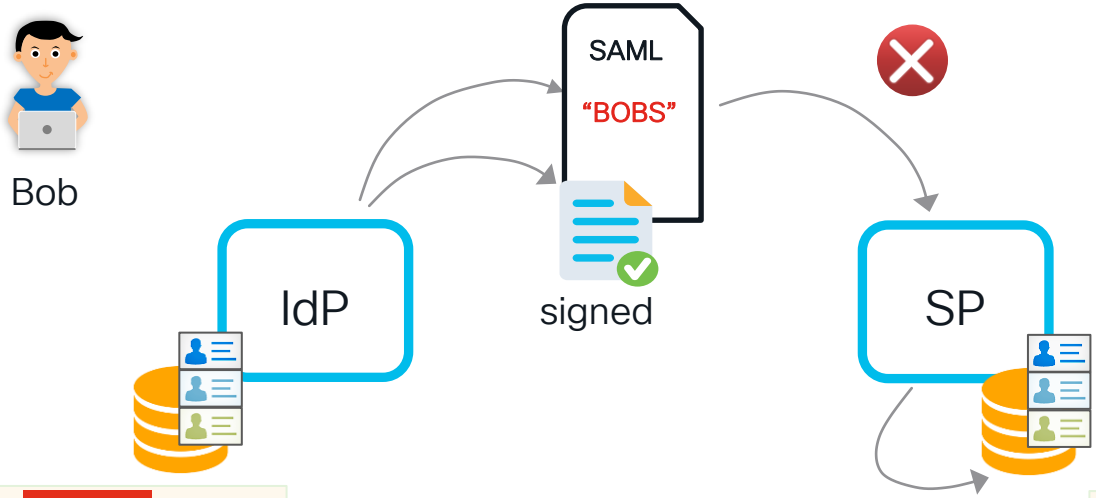
SAML recap

- 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



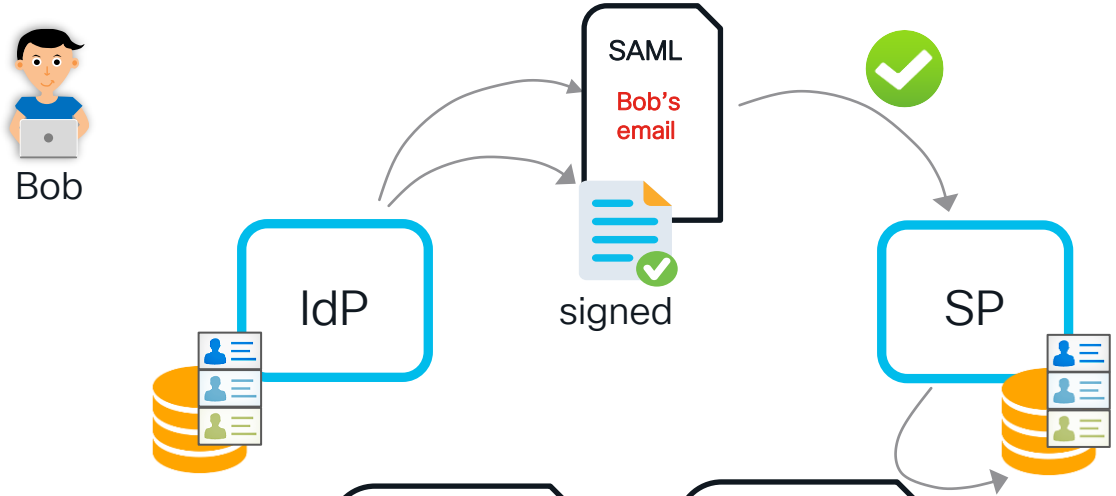
SAML flow: user ID format



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

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

SAML flow: user ID format



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

SAML Configuration

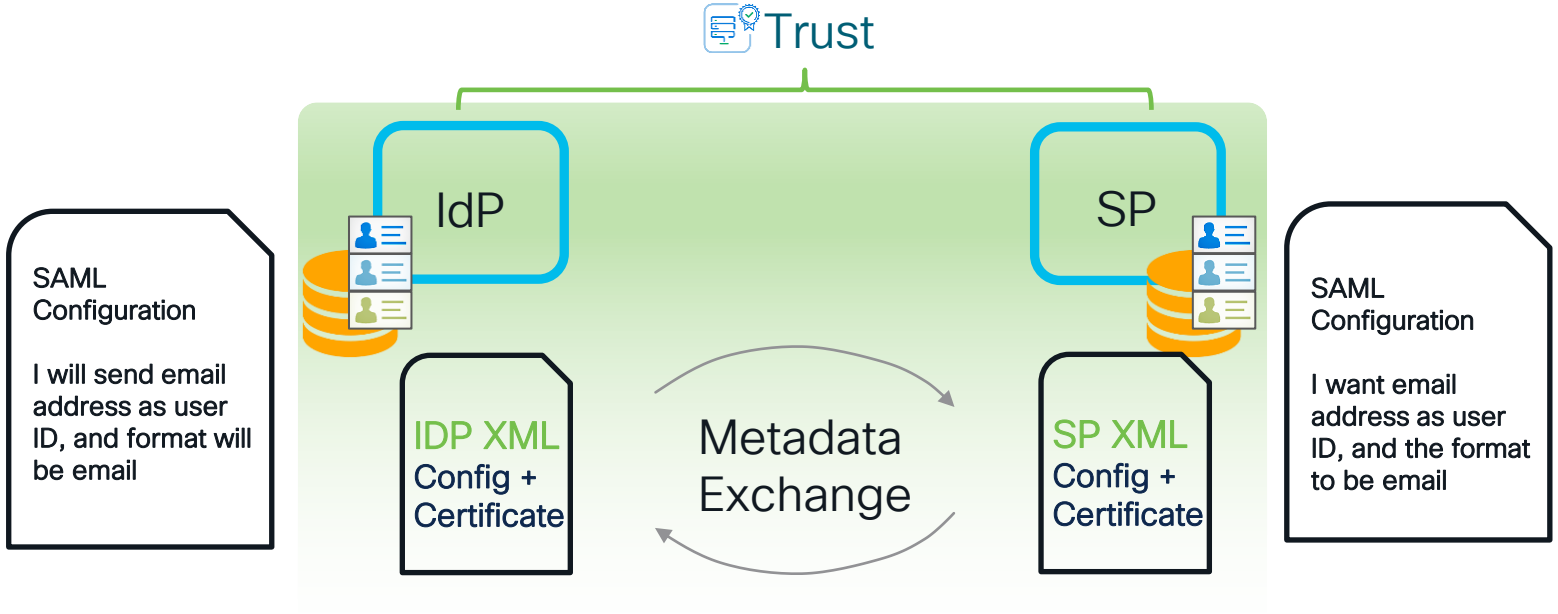
I will send email address as user ID, and format will be email

SAML Configuration

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

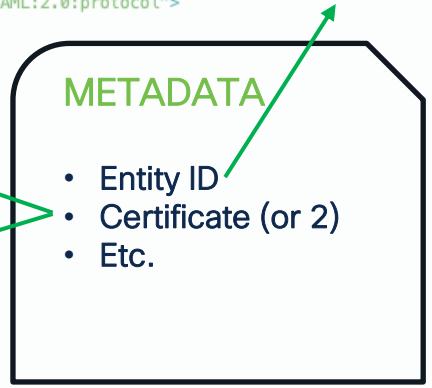
Usename: BSMITH
Email.address: bob@domain.com
Firstname: BOB
Lastname: SMITH

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
               ...
               O7ZRC/RQQpcU+vqTfj0aM7Hqn5No+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>
```



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

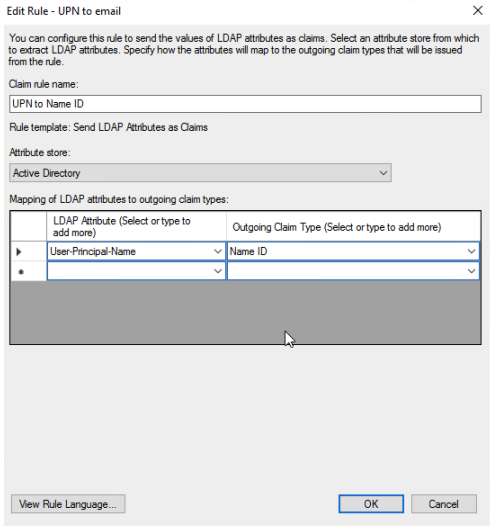
METADATA

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

+

UPN in NameID from IdP

true by default for most IdPs

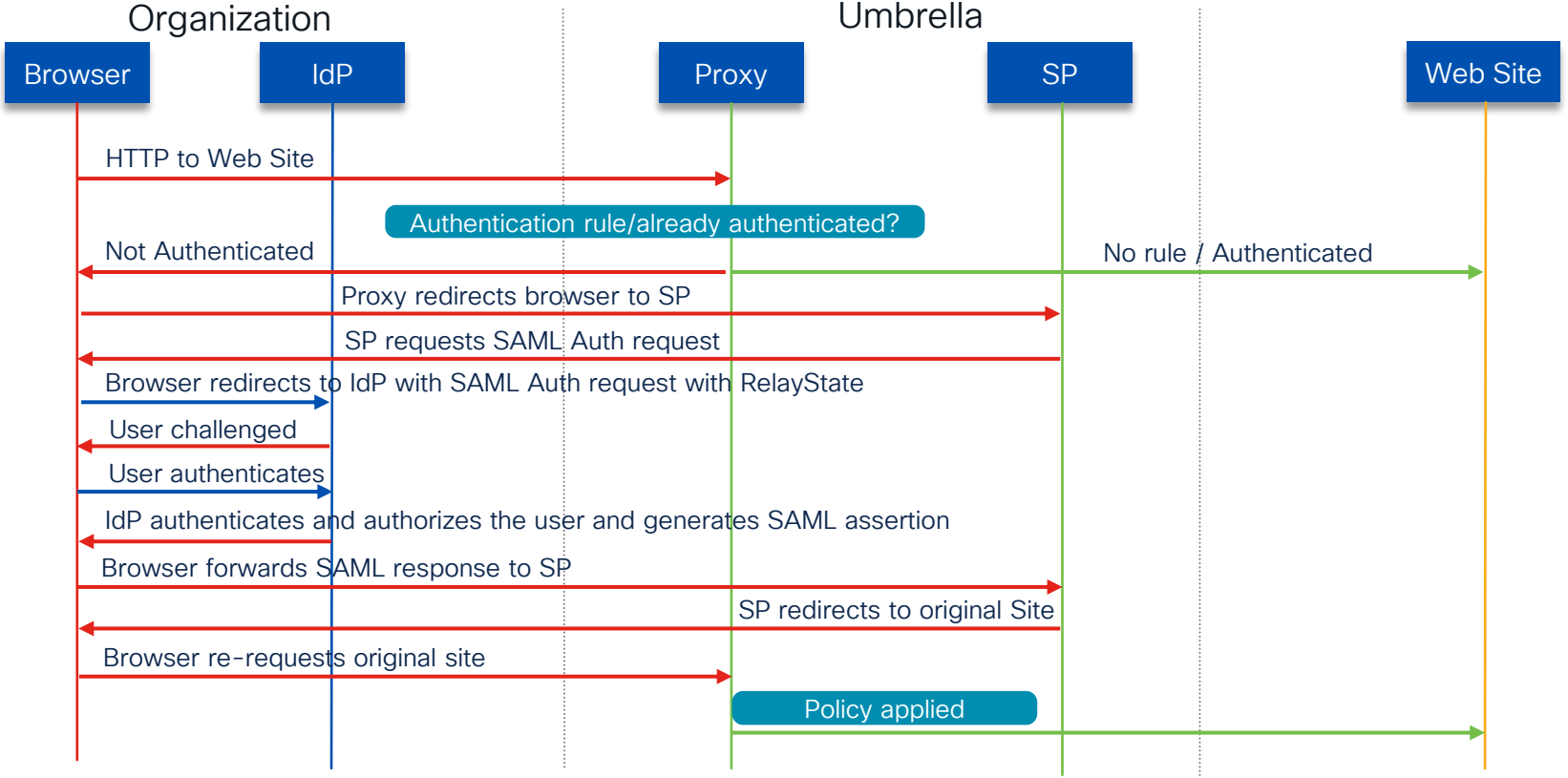


ADFS Claims Map Example

manual claims map is required in ADFS

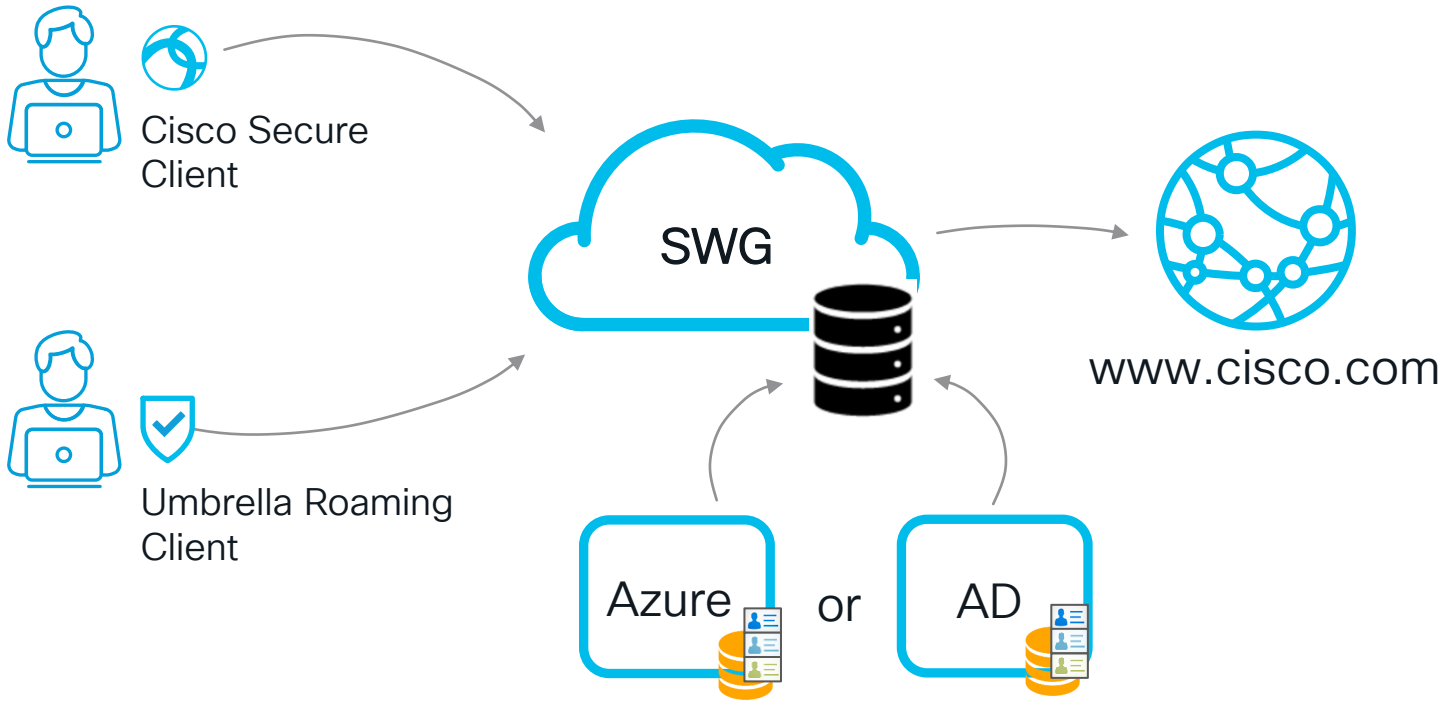
SAML Flow: Full Picture

SP and IdP never communicate directly!

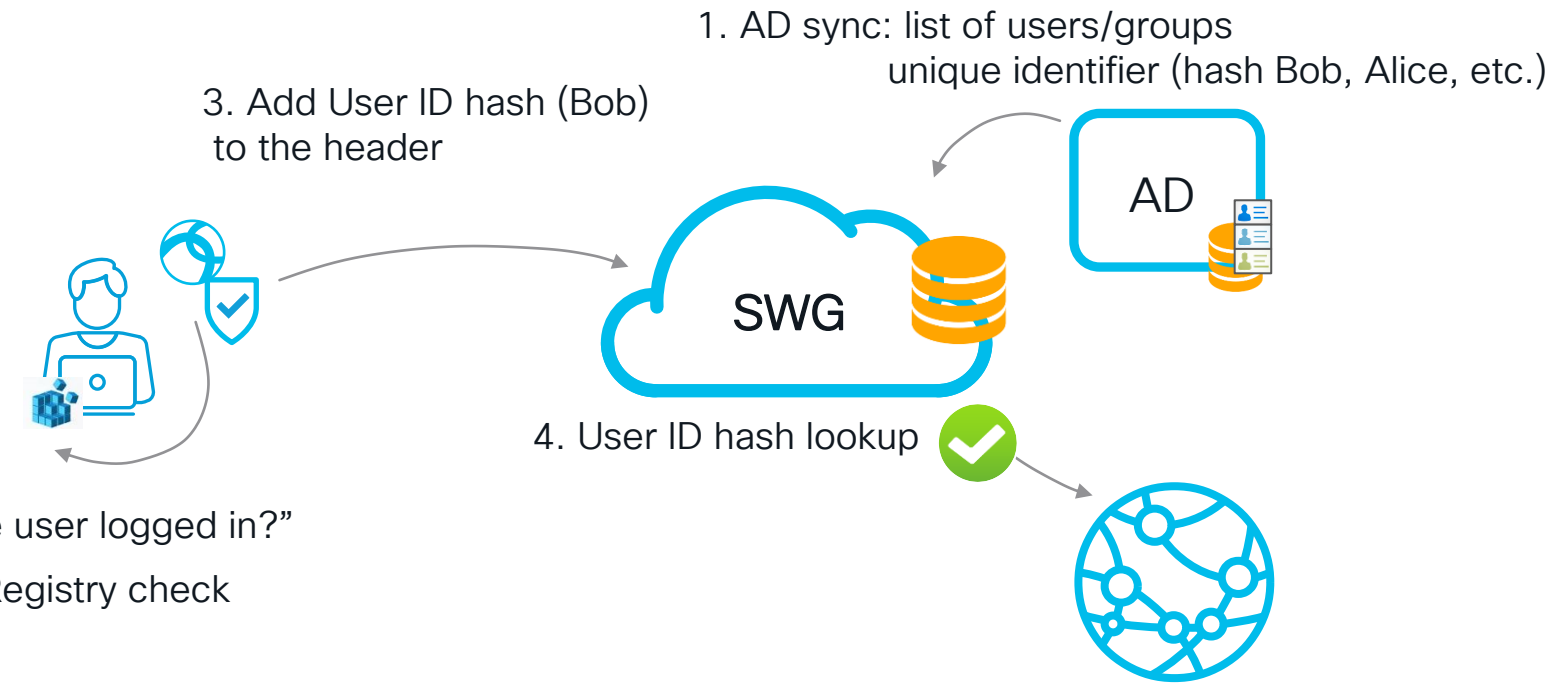


2. Remote Users

Remote User Connection Options



Remote User: Traffic Flow



Remote User: Hash Generation

objectGuid

- 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.

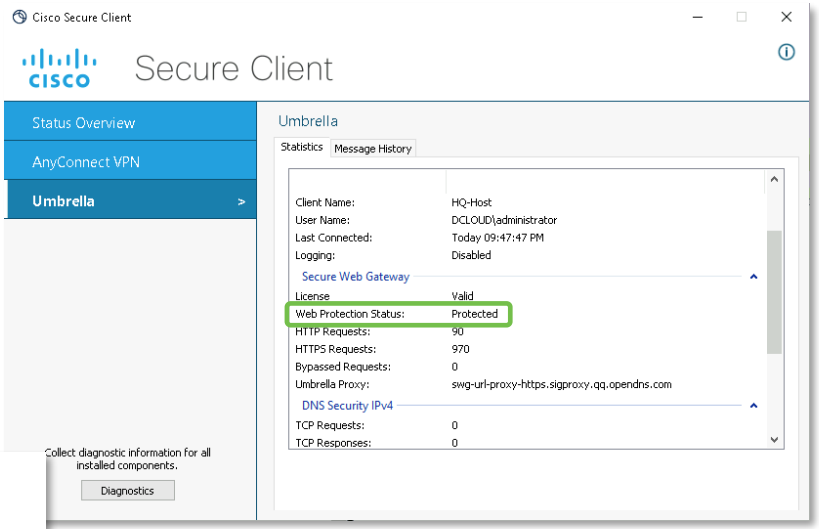
UPN

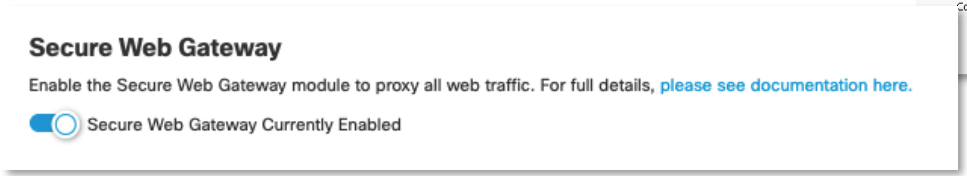
- “userPrincipalName” AD attribute
- **user@domain** format
- usually is the same as the users' email address but does not have to be
- works in pure and hybrid AZURE environment
- **preferred method starting**
  - AC 4.10 MR6+ / AC 5.0+ (Cisco Secure Client)
  - Standalone 3.0.328+

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”



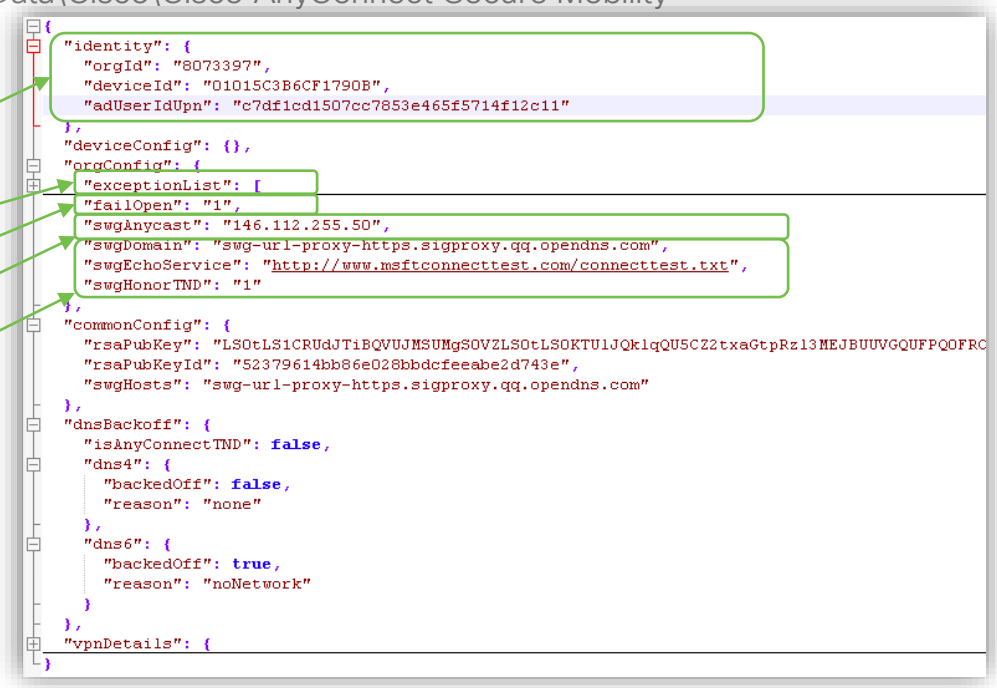


Supports Windows and Mac desktops

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



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

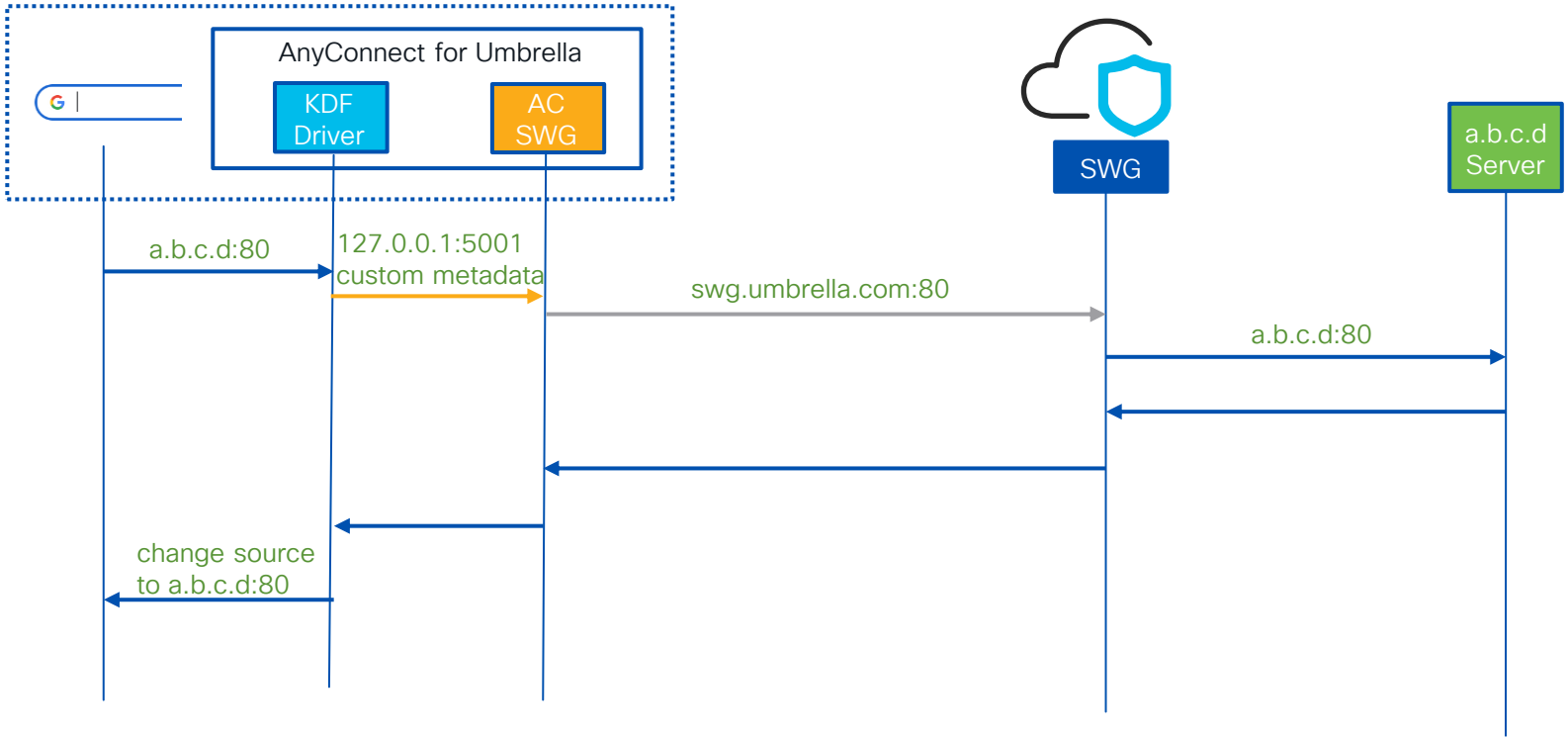
5. Umbrella proxy applies policies and Makes forward/block decision

2. process intercepts any web requests TCP 80/443

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

```
X-USWG-SK: tzJ9AYT/UEkJoaaMbX0G2crg35Agui5gXwPJH+1E7wYdw0d7+bGRux7elmqhO/
oJnU2aJJQo6XqDYQJXvxvbsTHCwdaP6hfELWGHzcVEgW0wP8XofzFOif+OSRTgWLAFdg6VUNeyLSiEexrV1PLEtkc5m8DJYw6hN
dlAY07DUjZ/h63PDuckTgN27YIl1JLZDf538LjExlpFZd4sFm+1W2FTPYashCaBSpw==
X-USWG-Data:
CQYl0wvcwjnRNpBqYzj67VkUQneNAqKi7WkrEwB507gHnRUJGTfV4GCloRwDROc5Q+6uNG4okDHQmZkc67sQFnqlL2kXC6XXS6l
nyuWCE5w+DEhlmzDkS9qxLSgFNqKcO4Lyjh/2gVEdWdBvfphr8YNWCxP/1ezIwdd0NLZGIZ27JK94fzqHidNu3zRXwIxR+d0m0E
ZgveG3/6zt3qfd3O1HjL1gJuGwr1YLK+HyEx6LTVw3qsxvYh635OP21ZbK9r+6RXedwgv9QNWWVsc805lzD8KT7fZ45fsTAy535
X-USWG-PKH: 52379614bb86e028bbdcfeeabe2d743e
```

Remote User: Traffic Flow



Remote User: AC-SWG Headers

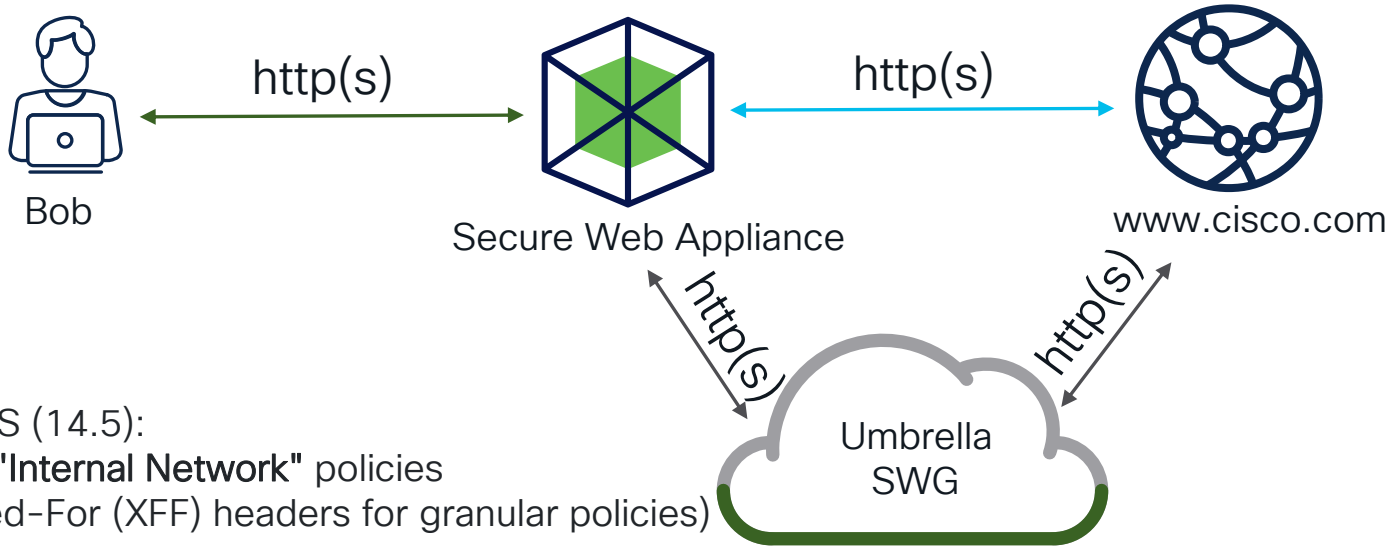
- X-USWG-SK – Encrypted Session Key
- X-USWG-Data – Org ID + Identity (Device/User) + 'timestamp'
- X-USWG-PKH – Hash of RSA Private Key

```
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: lG1F8+WYfKA0tvrzlhKp4hngOMCeE9Lf1Q1/
Pmrj8DrZAFCv1VcRDjeuBNWnTOhrgnK2qb45A9JPM60TuDQdc1KTqqoQ9ntVEZv0SnOMBen99jzsiNislKgSfHx2HZCiHfqt+LDQDUans
4HUw0FnCzWHSHsKzFLm8FOmI5tdMC38viwxYJnyU/BrVCc3HiKgAZt1H8TslJnEa6OVwqyE1NVN+szF3DJXxvYge4lz3kdzVh0HJnLhRT
X-USWG-Data: SLNHC82h9OlAsArTN+z8wLwnBc5tjzkPKFzxXzDiehC6PlWH+70EhXDkrNZMkZWR+xyxDZvCBN947GcRSRanpiMuJKwf
XN9yWYS1InDxSrZJXTOjRoZkCTX17GHaBY9I3BlvjfdiwVxNYG7ZKIGt5cuW4+bVMNNQ1pt6VENvOjFuHCowYymLjdSL859e2cweIftSl
rhf6Aao371vL1VLcV3hYu102IXnHze4KKvLFo4gQQKHXEBRrmRHb1wPyjUeSnf5ihZaWfYIDqAssdoy29XtBPhooMDsdeX+iJNBvaUz4P
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

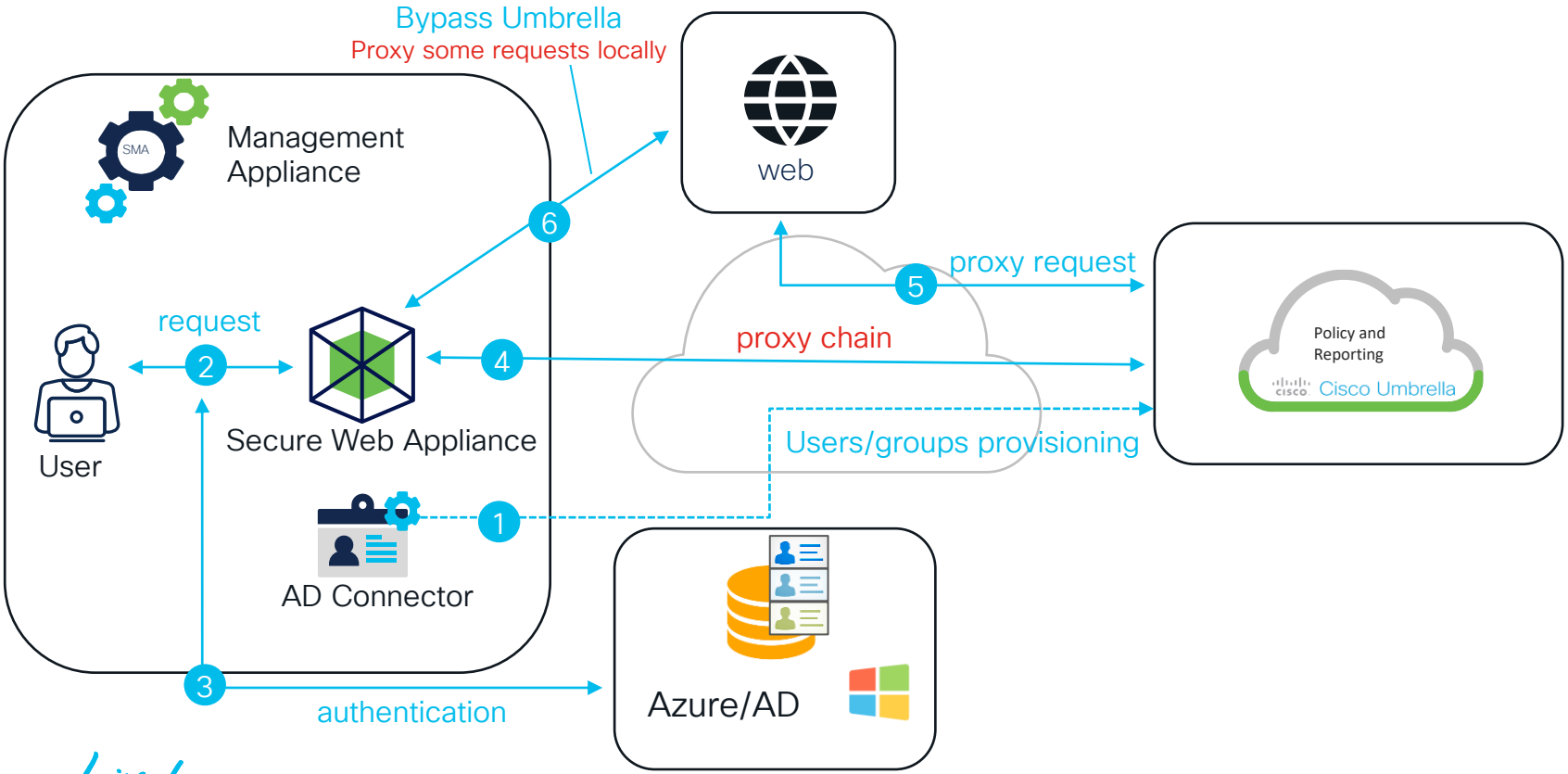


Before AsyncOS (14.5):
WSA provides **"Internal Network"** policies
(or X-Forwarded-For (XFF) headers for granular policies)

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

```
GET http://bbc.com/ HTTP/1.1
Connection: keep-alive
Host: bbc.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip
Upgrade-Insecure-Requests: 1
X-IMForwards: 20
Via: 1.1 wsa.dcloud.cisco.com:80 (Cisco-WSA/14.5.0-537)
X-USWG-Data:
C8Innyb1Eq8169KRipx0hdV724DVaBz59ma1nLNh2rbWwHb80AiyEPj5vJ44AFNc4g+Qsyjpf7NnoXXo7b9W3+z67BLeeEFe4
hLI/OsA9Yt0BATIgjrKd4zRcQXgLMKjrFycSSyu638dpq7JZyGtkOWYV4ga7DK7QOz0rVSmBSyDfBbukbMsxrBuM3DsOEo6Sj
X-USWG-SK: R0SqiGQuzDfVwQvYBaqFzAshaVgdaayKhaZOUpMtutAWFwrn+yI0n8PORfwIYHiHX9bygEiZc2m+u525v6aDr2
d9PCo+1olfl/kRxP6MYpYlTQevATkyZgLqXfxBYhXgpvzlB2Emneer5+SxywDwYn69m+d3seItEpel+c7XBYHJlA1PP/g==
X-USWG-PKH: f0d78ed86bcb390157ca14ba10978cfa

HTTP/1.1 303 See Other
Server: Cisco Umbrella
Date: Fri, 20 Jan 2023 00:28:05 GMT
Content-Type: text/html
Content-Length: 172
Connection: keep-alive
Location: https://block.opendns.com/swg?server=swg-nginx-proxy-https-
c9c89ebfa871.signginx.ash&v=eyJhbGciOiAiSFM1MTIiLCAia2lkIjogIjE1NjM1NTk3OTYifQ.eyJidHlwZSI6ICIiLC
ICI4MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwNDAwMDAiLCAidXJsIjogImh0dHA6Ly9iYmMuY29tL
Via: HTTP/1.1 s_proxy_ash
```

forwarding device

Headers in Authentication Process

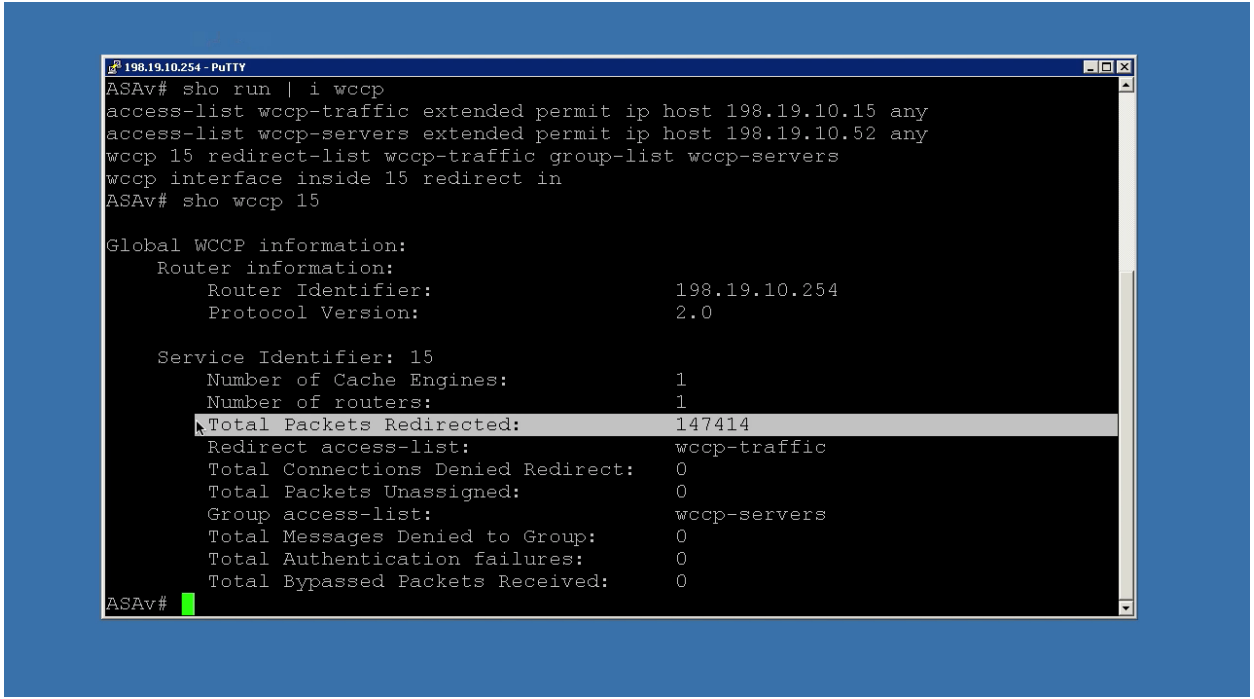
Demo

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

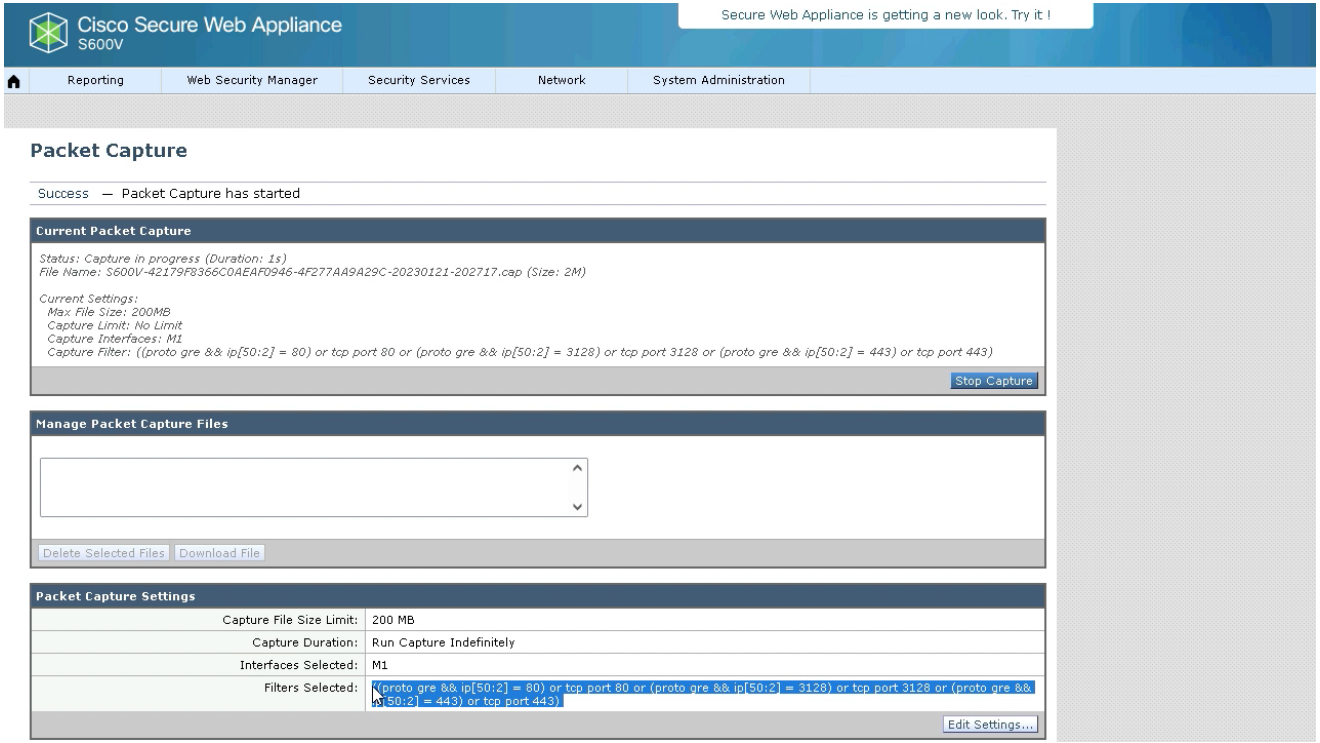
Demo Scenario 1:

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



Demo Scenario 1:

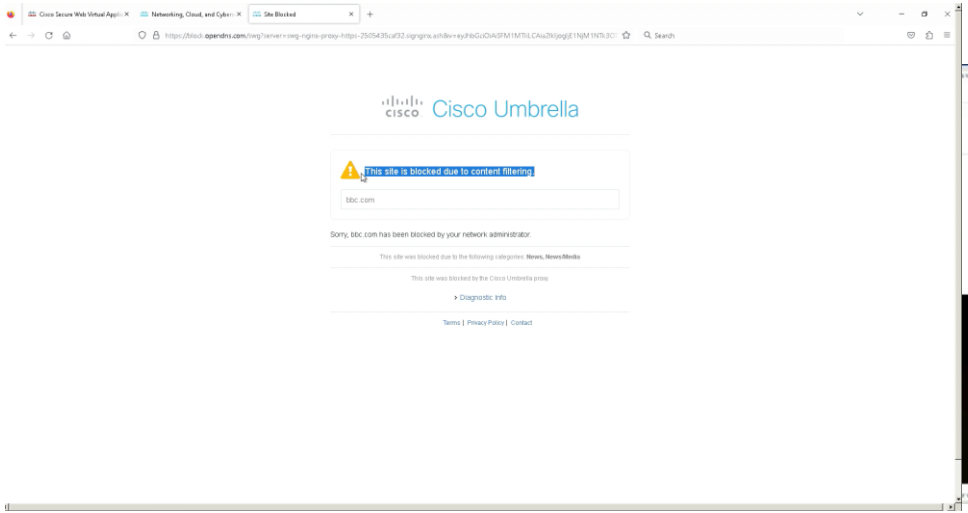
2. We start capture on Secure Web Appliance to check the headers

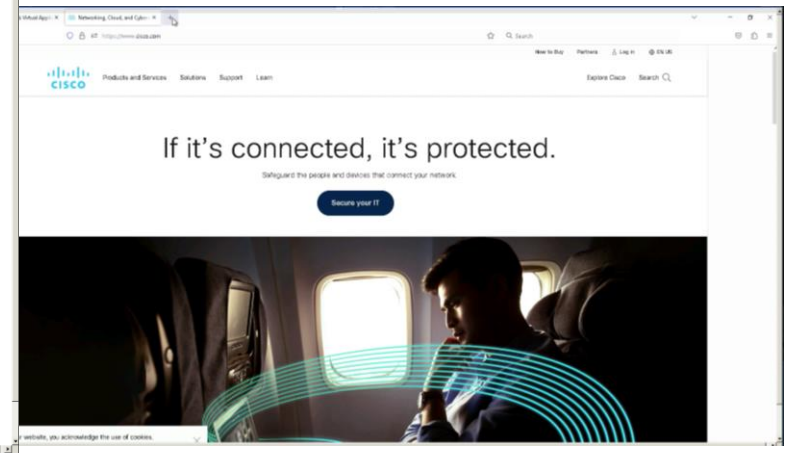


Demo Scenario 1:

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.



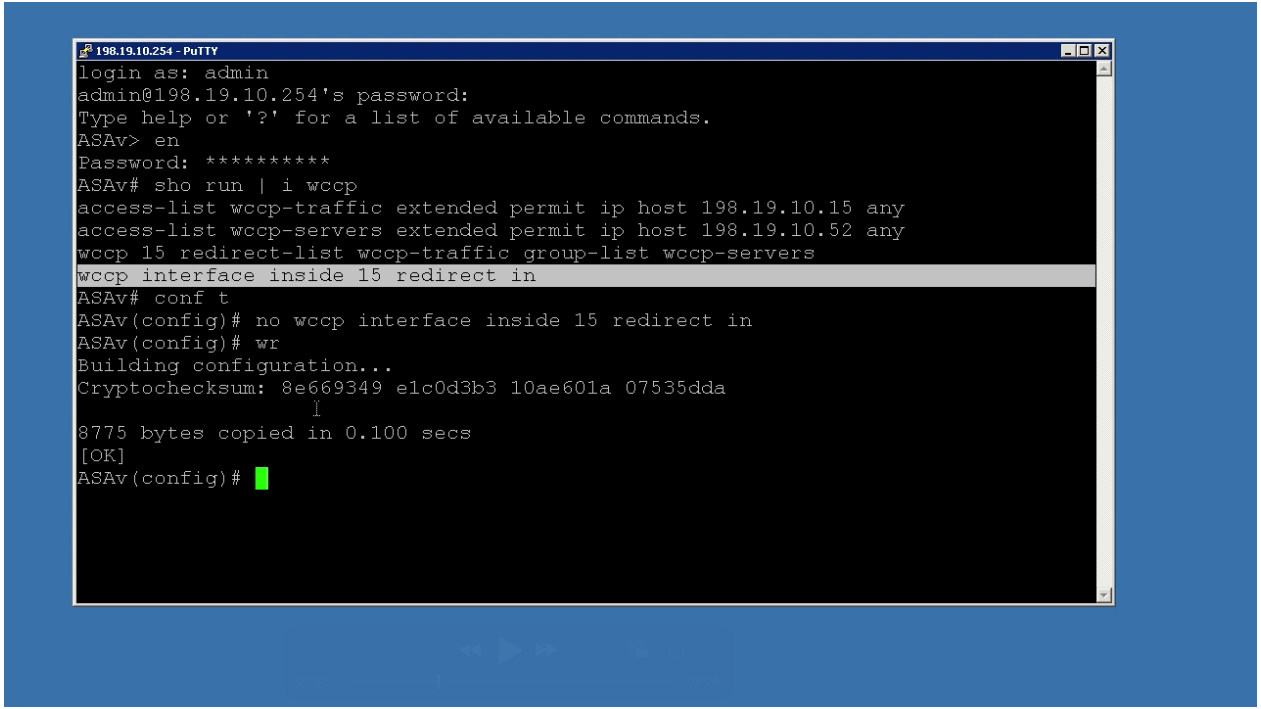


Demo Scenario 2:

- 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

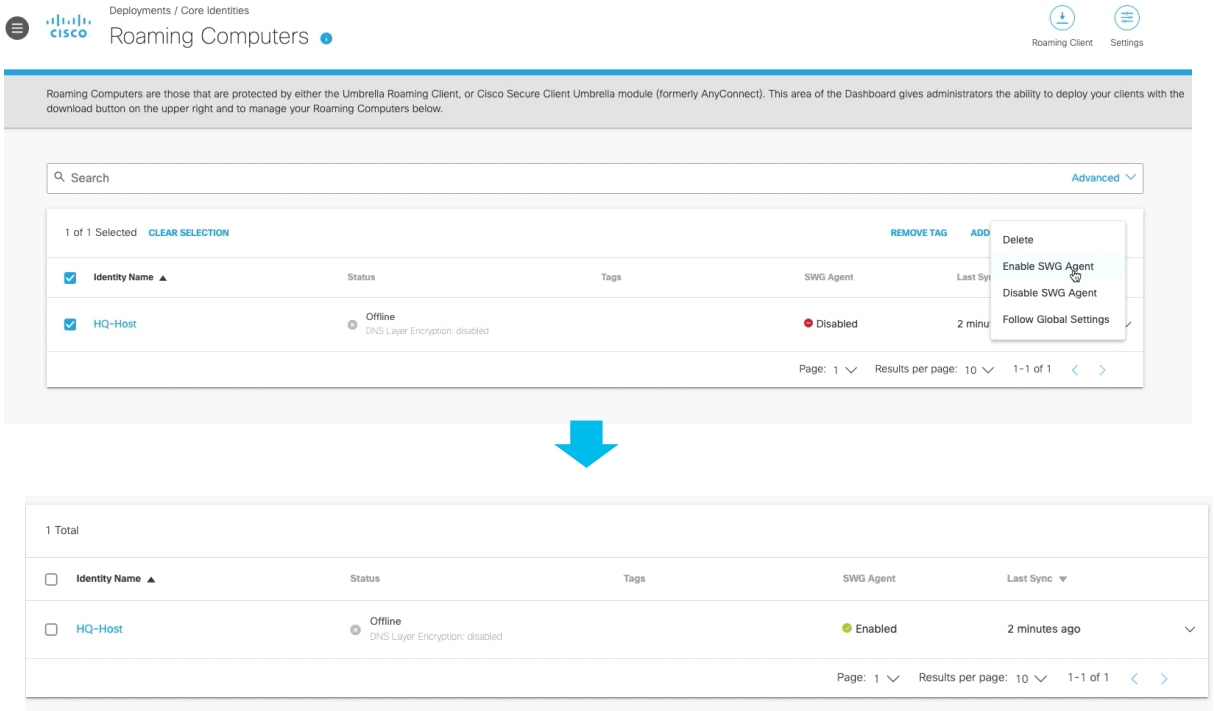
Demo Scenario 2:

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



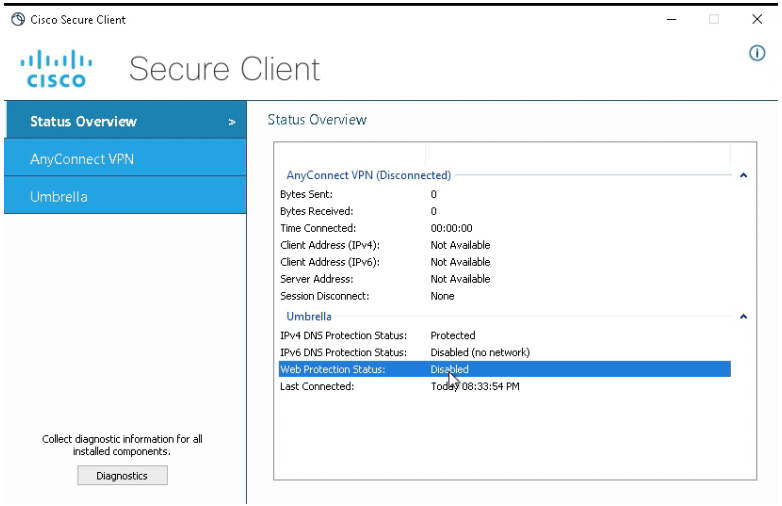
Demo Scenario 2:

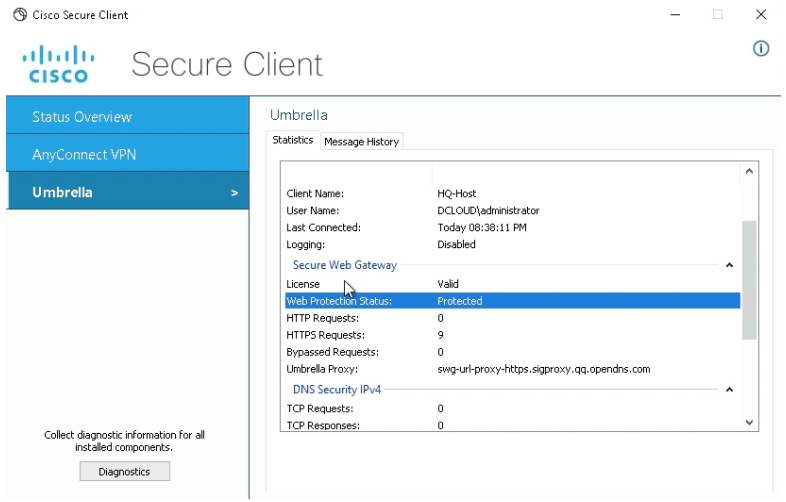
2. Secure Client status changes from Umbrella Web Protection disabled to Enabled, after enabling the feature it on Umbrella portal.



Demo Scenario 2:

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

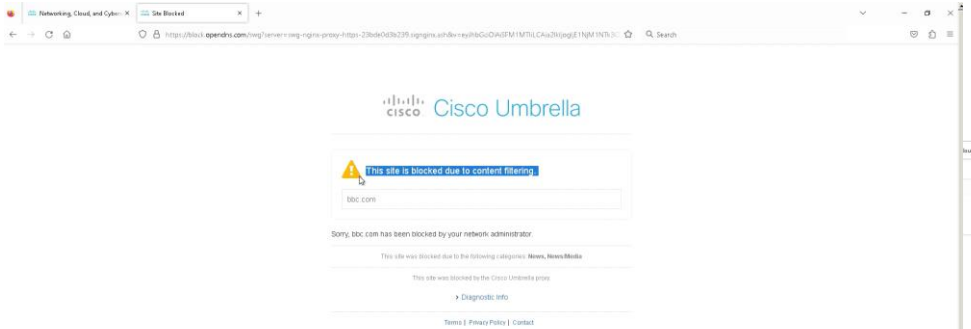


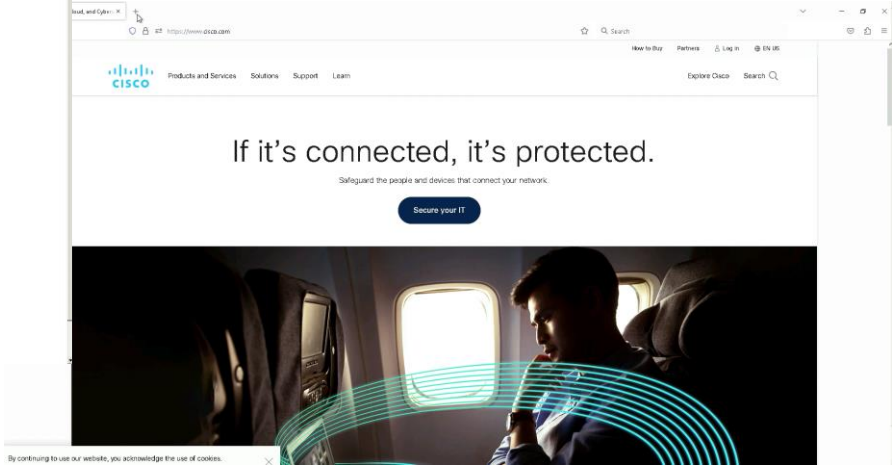


Demo Scenario 2:

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.

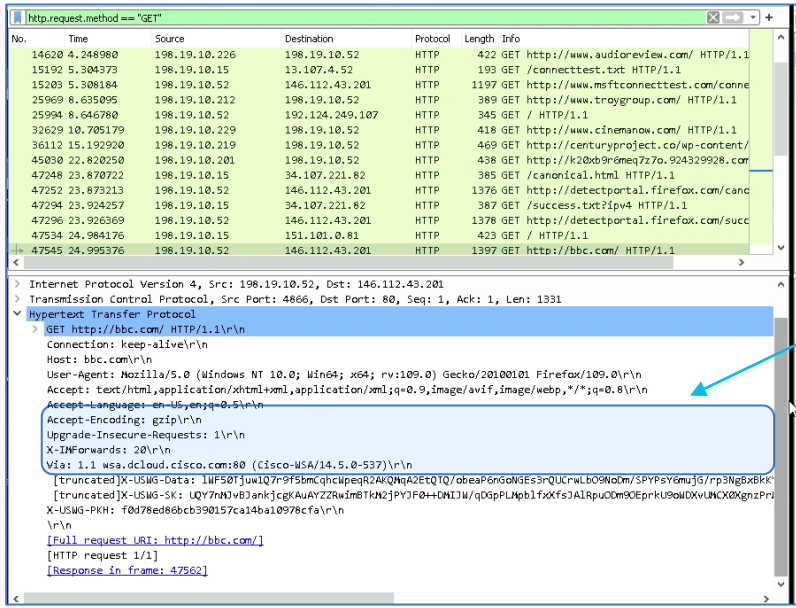




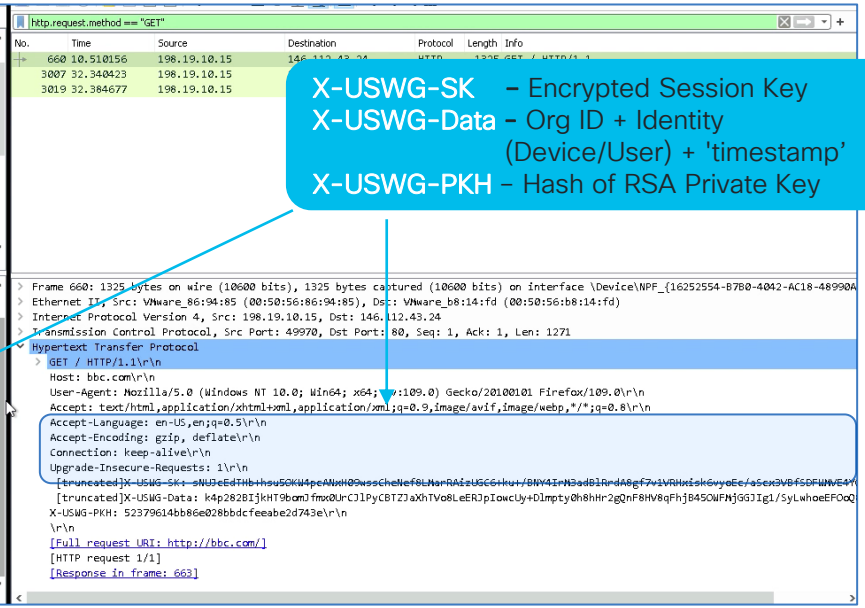
HTTP headers play important role in authentication process.

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

Seamless Identity



Cisco Secure Client



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

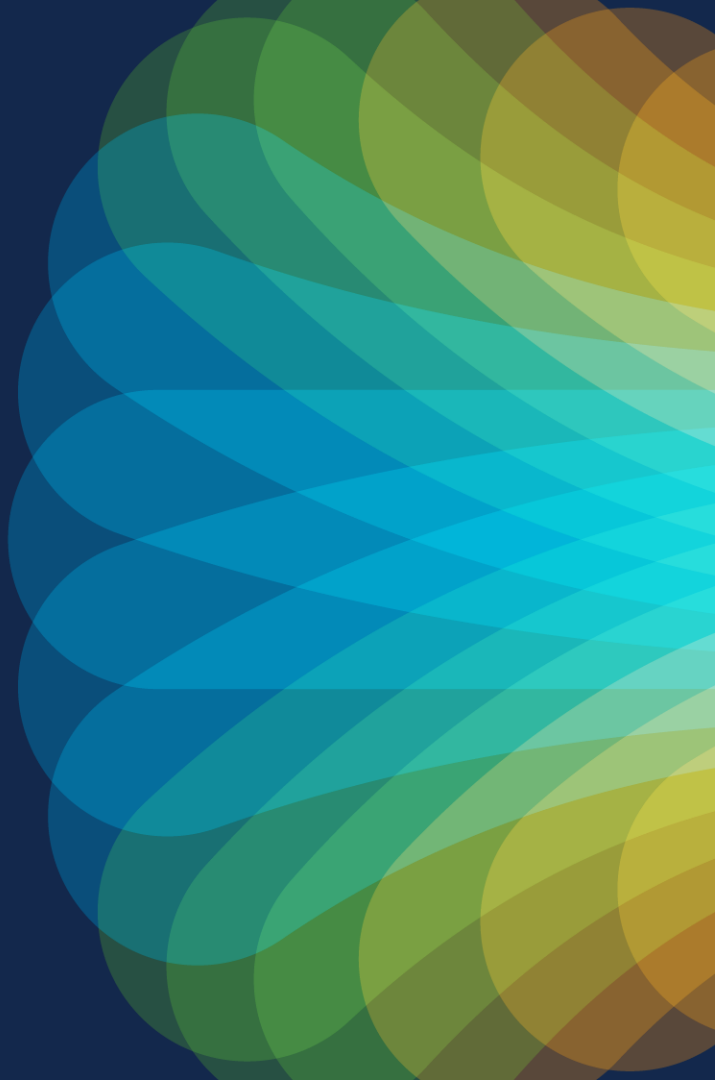
Azure: Configure Cisco Umbrella User Management for automatic user provisioning

Please Fill Out The Survey!

Q&A time

The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go