The bridge to possible

Cisco Secure Hybrid SWG

Your First Step to Your SASE Journey

Tariq Bader, Cybersecurity Technical Solutions Architect
linkedin.com/in/tarbader/

Abstract

With the rapid movement to the cloud, relying more on SaaS applications, and adopting hybrid work model, so many organizations see the importance of shifting to SASE architecture.

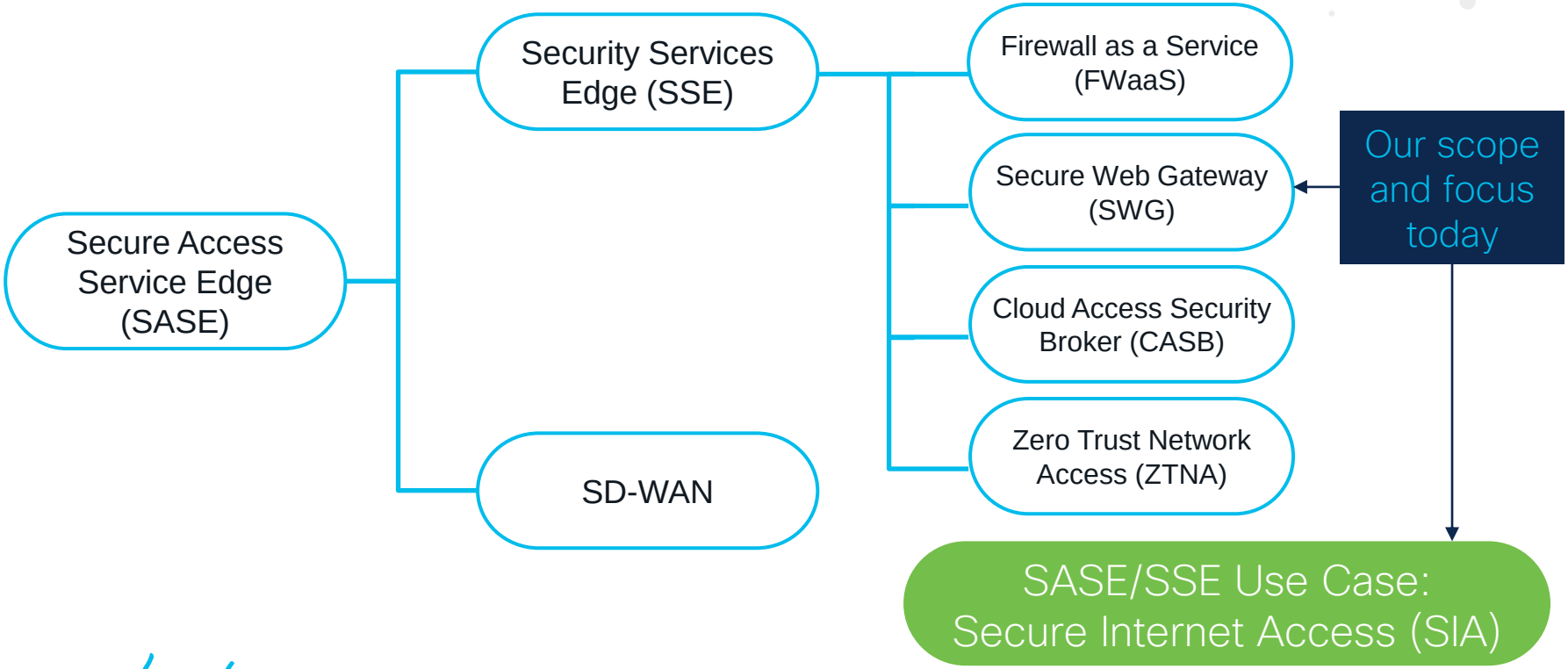
However, the journey into SASE architecture isn't an easy one and every organization is unique and requires a different path for the journey. While the SDWAN is pretty much defined, the Security Services Edge (SSE) part is where organizations have different requirements and require different paths. Some are driven by regulations and compliance (where cloud all-in is challenging), others driven by performance and design flexibility. Securing the internet access is one of the key important use cases that SSE/SASE covers and a great one to start with.

This session is to introduce Cisco Secure Hybrid SWG as a practical approach to start this journey smoothly by securing the internet access everywhere on and off the network while addressing the different requirements organizations need (regulations, geo restrictions, design flexibility .. etc).

You will walk out from this session understanding the advantages, design flexibility, requirements, feature details, use cases and configurations needed to deploy both Umbrella and Secure Web Appliance (aka WSA) together as a Hybrid SWG.

Note: Prior knowledge and familiarity to both Umbrella SIG and Secure Web Appliance (aka WSA) are highly recommended to attend this session.

How this is related to SASE/SSE ?



What do you expect from this session

- Undertand the value of Hybrid SWG approach and why it provides a good start for SASE/SSE transition covering the Secure Internet Access (SIA) use case for the enterprise/organization
- Understand the architecture and configuration of Hybrid SWG
- Understand the key practical use cases of Hybrid SWG

- *Note: We will not cover Umbrella and Secure Web Appliance (SWA) feature set in details, we assume existing knowledge and familiarity to both*

Brand Naming Changes

cisco SECURE

Web Security Appliance (WSA)	Cisco Secure Web Appliance (SWA)
AnyConnect	Cisco Secure Client (CSC)
	Cisco Umbrella SWG/SIG

Important: Hidden Slide Alert

Look for this “Reference” Symbol in your PDF’s

There is a good amount of hidden content that will not be presented, its for you to use later!

Icons Legend

Best Practice
Recommended

For Your Reference
Extra Content

Advantage
Benefit

Cisco Webex App

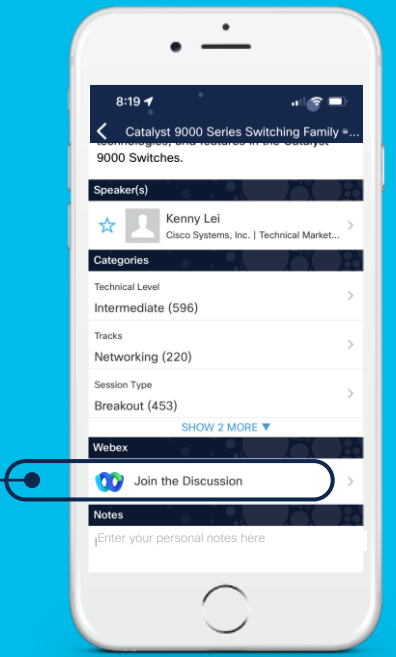
Questions?

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.



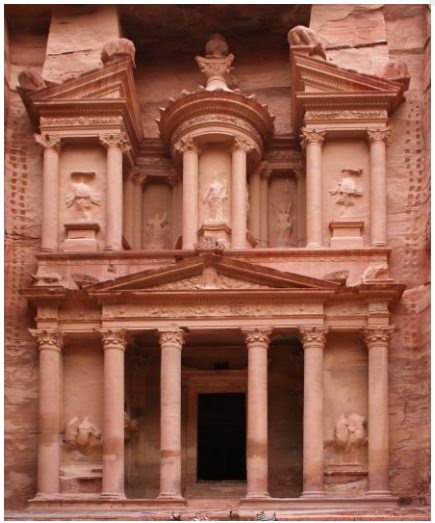
Agenda

- New Reality and New Challenges
- SWG Evolution
- Hybrid SWG
  - Proxy Chaining and Seamless Identity
  - Use Cases
  - Common Hybrid Policies
- Wrap Up

Who is your *Speaker* ?

Tariq Bader

- Cybersecurity Technical Solutions Architect
- 12+ years experience in Cybersecurity and Network
  - Previous Cisco TAC Security Engineer
  - Professional services and pre-sales experience previously with a Cisco partner
- From Jordan and based in Saudi Arabia
- CCIE Security #35627 since 2012



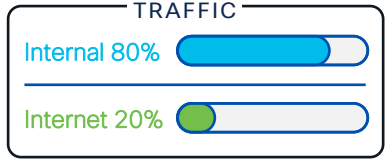
New Reality and New Challenges

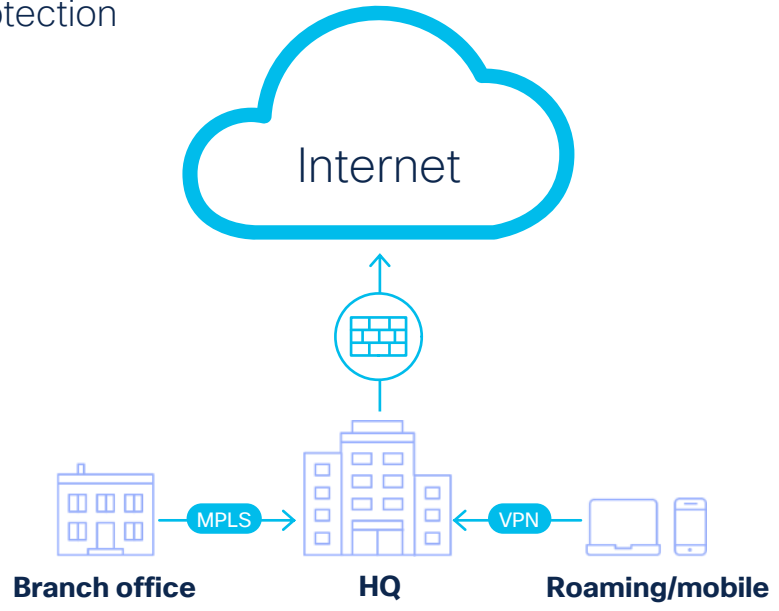
Internet Access Transformation

Transition from a centralized internet breakout to decentralized (Cloud/SASE ready)

Network: Centralized

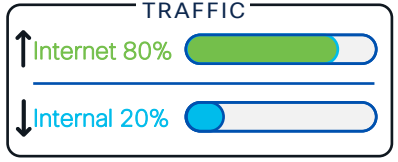
Security: Single place to enforce policies and protection

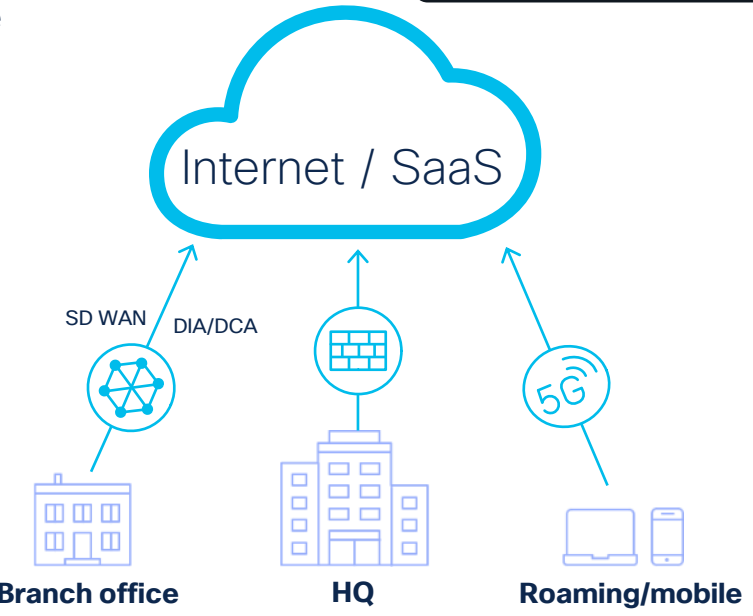




Network: Decentralized

Security: Protect at data center, cloud, and branch edge





New Reality and New Challenges

Move to the cloud

- More cloud services and SaaS
- Moving to SD-WAN and SASE
- More decentralization and DIA
- Lack of visibility and control
- Shadow IT

Hybrid Work

- Surge in remote users and work from anywhere approach
- Personal and unmanaged devices
- Higher threat exposure and new attack methods
- Shadow IT

Threats becoming more advanced

- Malware distributed by hacked legitimate sites
- 90% encrypted traffic
- Browser Infection
- Uncategorized URLs
- Risky SaaS

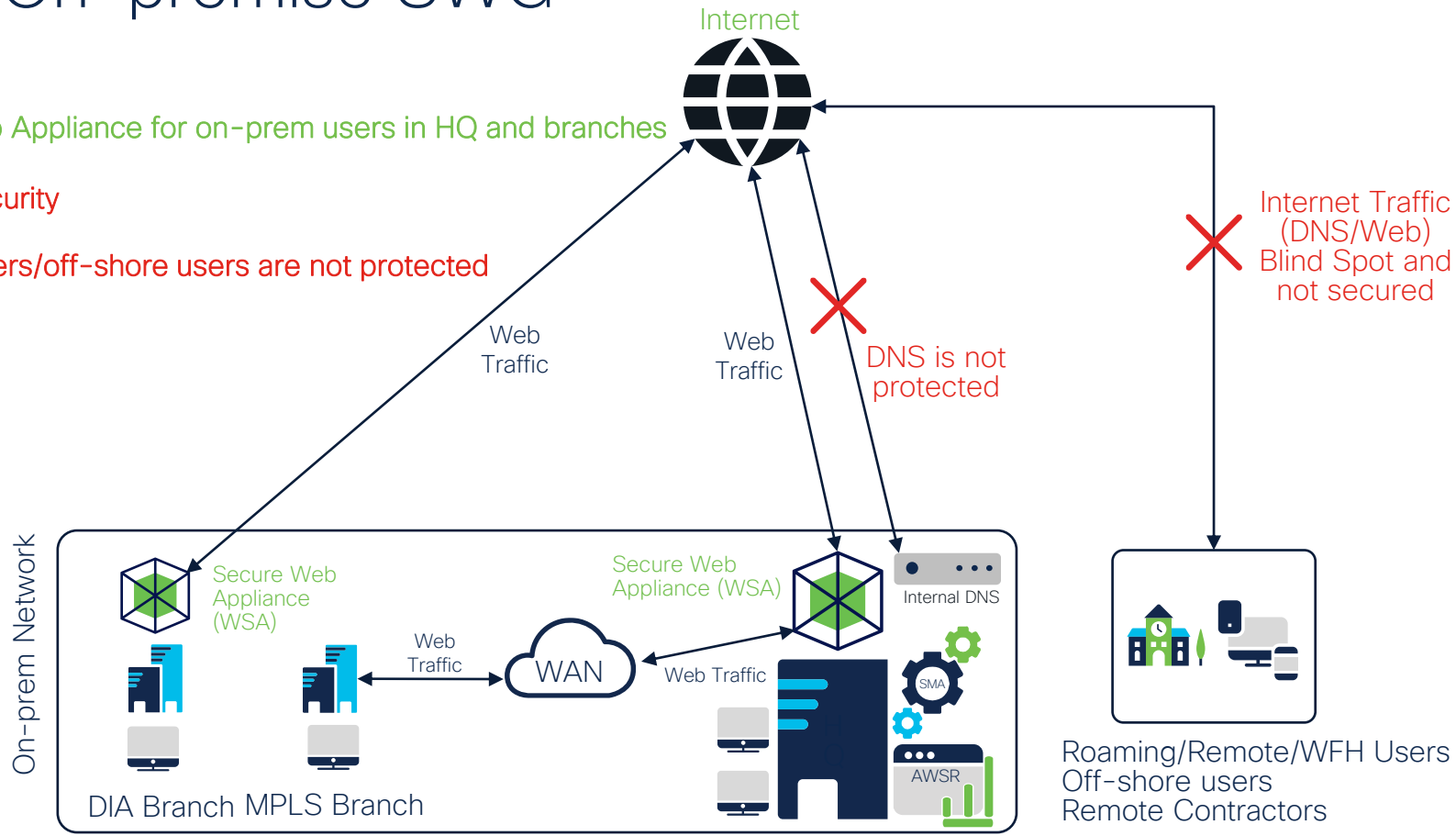
Regulation and Compliance

- Country specific regulations
- Industry specific regulations
- Cloud services are not allowed
- Data locality

Secure Web Gateway (SWG) Evolution

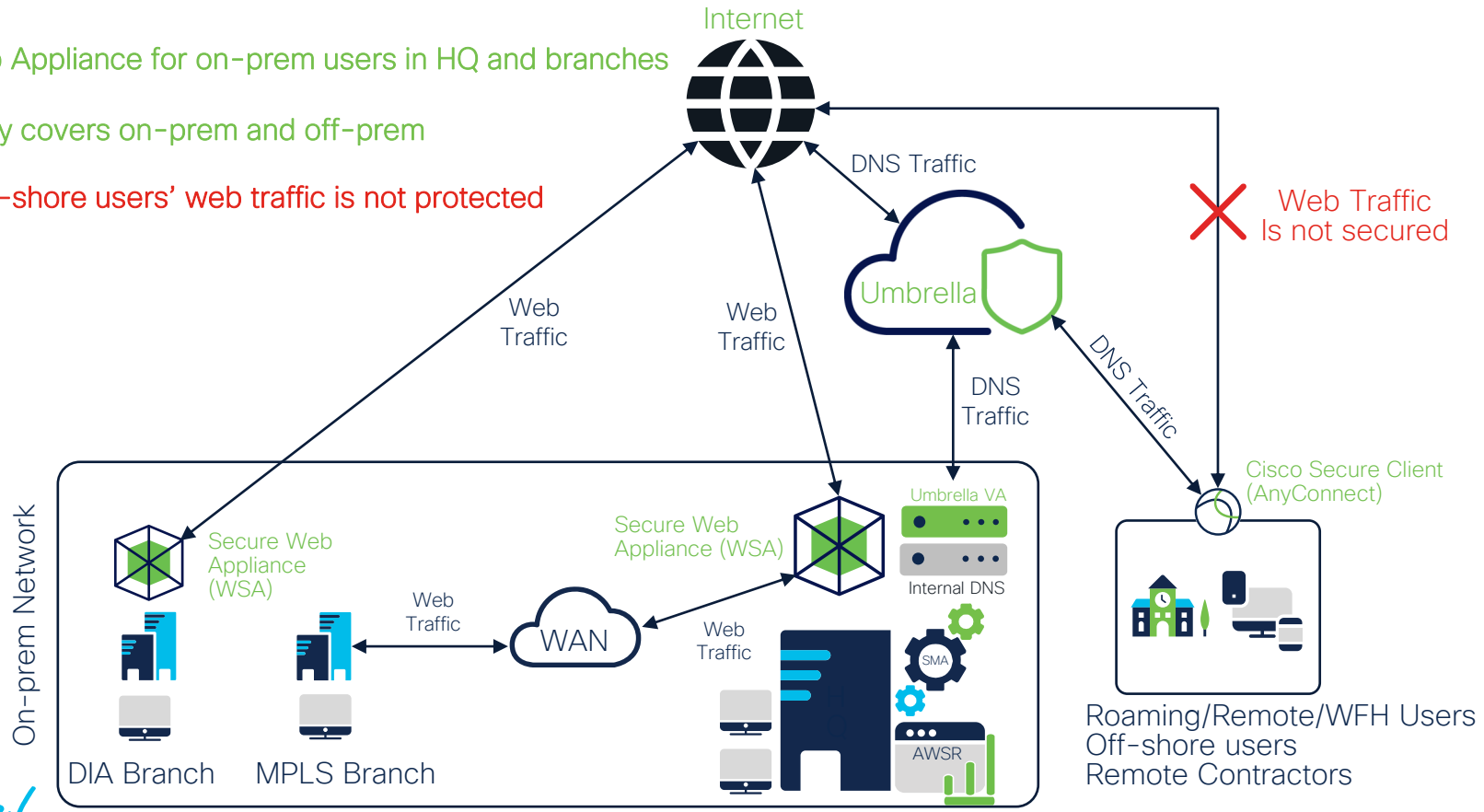
Fully On-premise SWG

- ✓ Secure Web Appliance for on-prem users in HQ and branches
- ✗ No DNS Security
- ✗ Roaming users/off-shore users are not protected



Fully On-premise SWG + DNS Security

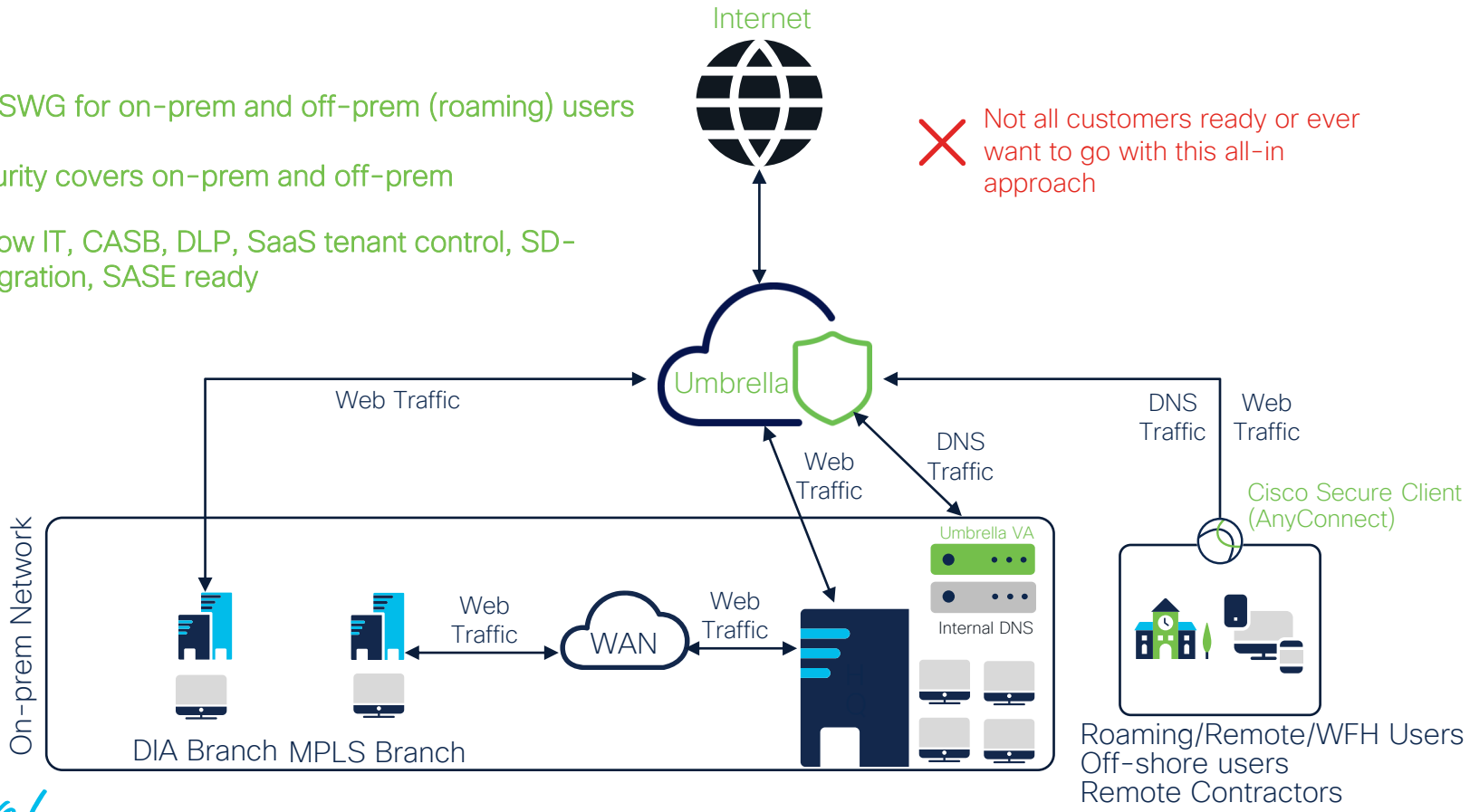
- ✓ Secure Web Appliance for on-prem users in HQ and branches
- ✓ DNS Security covers on-prem and off-prem
- ✗ Roaming/off-shore users' web traffic is not protected



Cloud Delivered SWG (Cloud all-in)

- ✓ Umbrella SWG for on-prem and off-prem (roaming) users
- ✓ DNS Security covers on-prem and off-prem
- ✓ RBI, shadow IT, CASB, DLP, SaaS tenant control, SD-WAN integration, SASE ready

✗ Not all customers ready or ever want to go with this all-in approach



"The reality is that the migration to a cloud-based future is a spectrum that every enterprise is on. It is not just a one-time event, it's a journey"

ESG whitepaper: **The Role and Benefits of a Hybrid Approach to Secure Web Gateway**

Why not go all-in Cloud SWG ?!

Regulations and Compliance

- Country/union specific regulations
- Industry specific regulations
- Data Locality

Geo Restrictions

- Cloud proxy don’t work in certain countries
- Local websites don't accept connections from outside

Organization is too complex for full cloud SWG

- Very large enterprise
- Globally distributed enterprise with multi country presence having different bandwidth, regulations, authentication methods .. etc

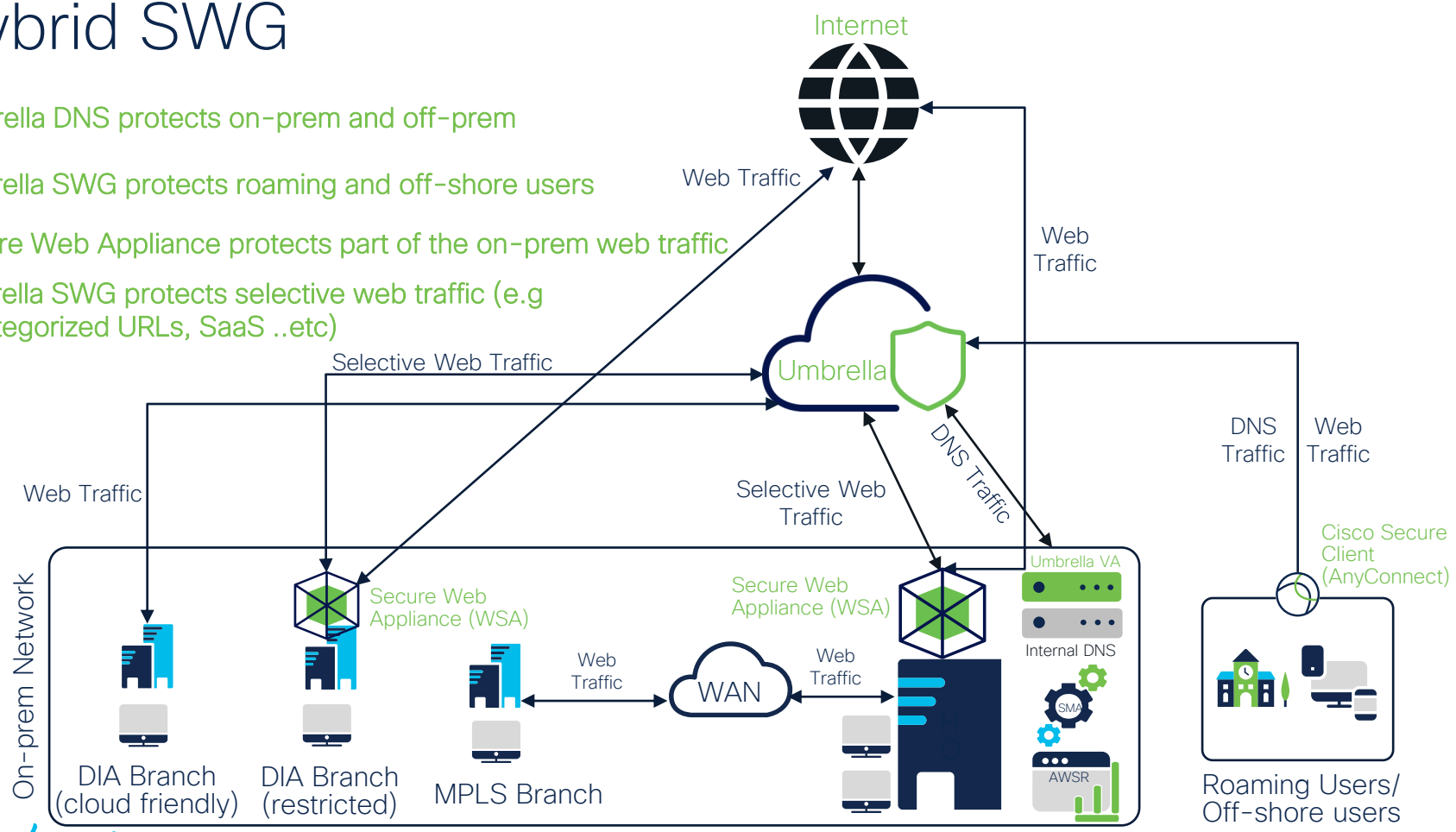
Need for flexibility

- Control what to be handled on-prem and what can be handled in cloud
- Moving to SASE approach gradually
- Design flexibility
- Proxy transparency option

Cisco Secure Hybrid SWG

Hybrid SWG

- ✓ Umbrella DNS protects on-prem and off-prem
- ✓ Umbrella SWG protects roaming and off-shore users
- ✓ Secure Web Appliance protects part of the on-prem web traffic
- ✓ Umbrella SWG protects selective web traffic (e.g uncategorized URLs, SaaS ..etc)



Hybrid SWG Benefits

More Flexibility

Smoother transition to cloud proxy and SSE/SASE architecture

More authentication options (no major identity changes)

More deployment and traffic redirection options (e.g proxy-chaining, on-premise, roaming users, PAC .. etc)

More Control

Decide what to be handled on-prem and what to be handled by cloud – great for regulations.

More Use Cases

Some examples:

- Integrating on-premise DLP
- CASB features on Umbrella
- Shadow IT
- DNS Security

Hybrid SWG is Perfect for the following organizations (not limited to)

Regulated & Agile

- Must meet regulations and compliance
- Cloud concerns or restrictions, want to control what to be handled in Cloud
- Moving to more hybrid work and SaaS usage

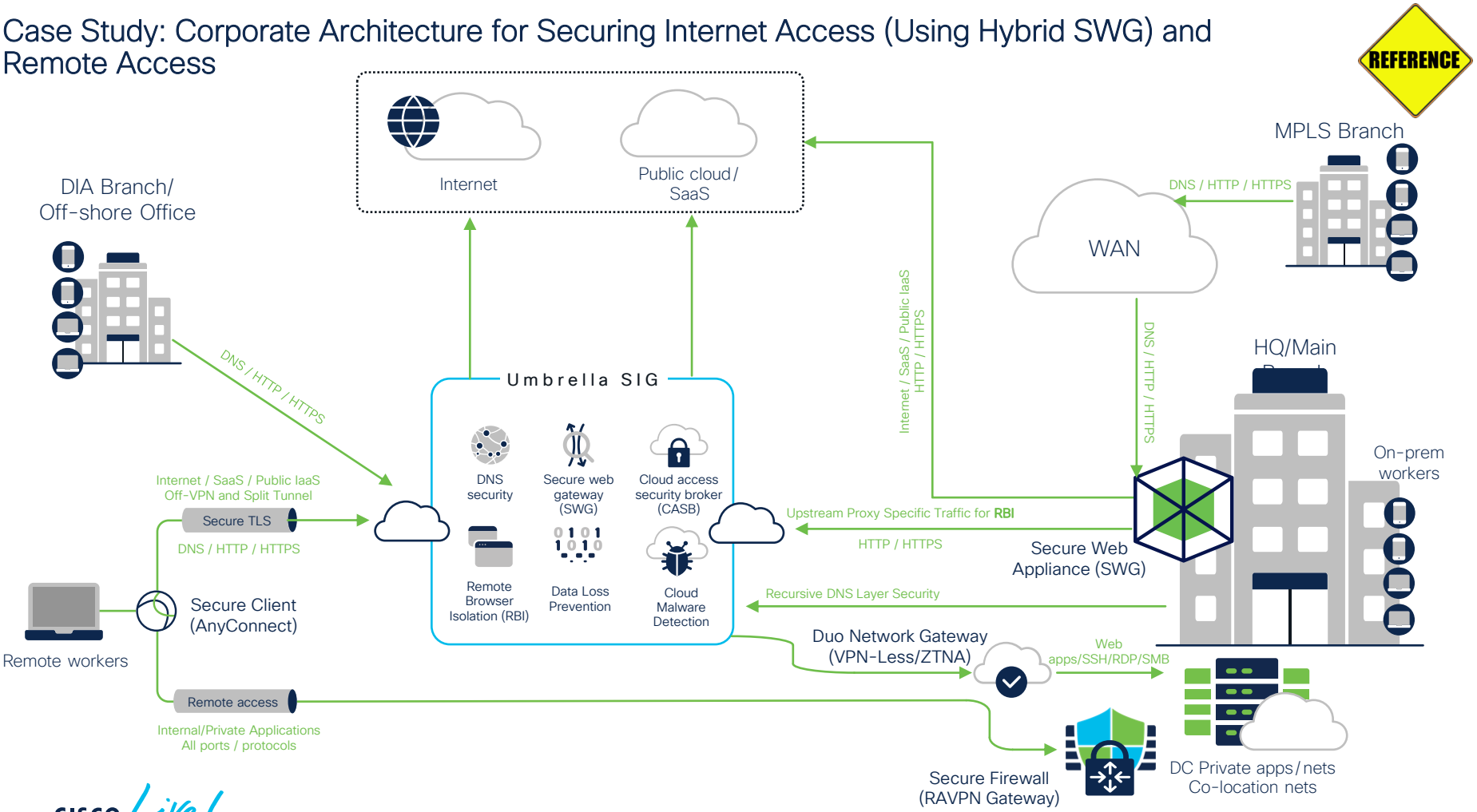
Smooth Transition

- Existing on-prem proxy moving to Cloud/SASE with phased approach and flexible deployment
- Start leveraging modern cloud only SWG/SASE features (e.g, DNS, RBI, CASB, Shadow IT .. etc) with minimal changes

Global Organization

- Wide geographical multi country presence
- Different regulations
- Different connectivity and bandwidth requirements
- Needs flexibility in design and traffic redirection

Case Study: Corporate Architecture for Securing Internet Access (Using Hybrid SWG) and Remote Access



Hybrid SWG
Proxy Chaining and Seamless Identity

Integrating SWA and Umbrella for Hybrid SWG

Proxy Chaining

Upstream Proxy – A node between the first proxy (downstream) in the network and the internet. In our case, the upstream proxy is Umbrella SWG.

- Routing Policies on SWA decides to forward traffic to the upstream proxy
- Traffic is sent in the form of explicit proxy requests.
- SWA can be deployed transparently or explicitly.

Integrating SWA and Umbrella for Hybrid SWG

User Authentication Options with Proxy Chaining

SAML Authentication

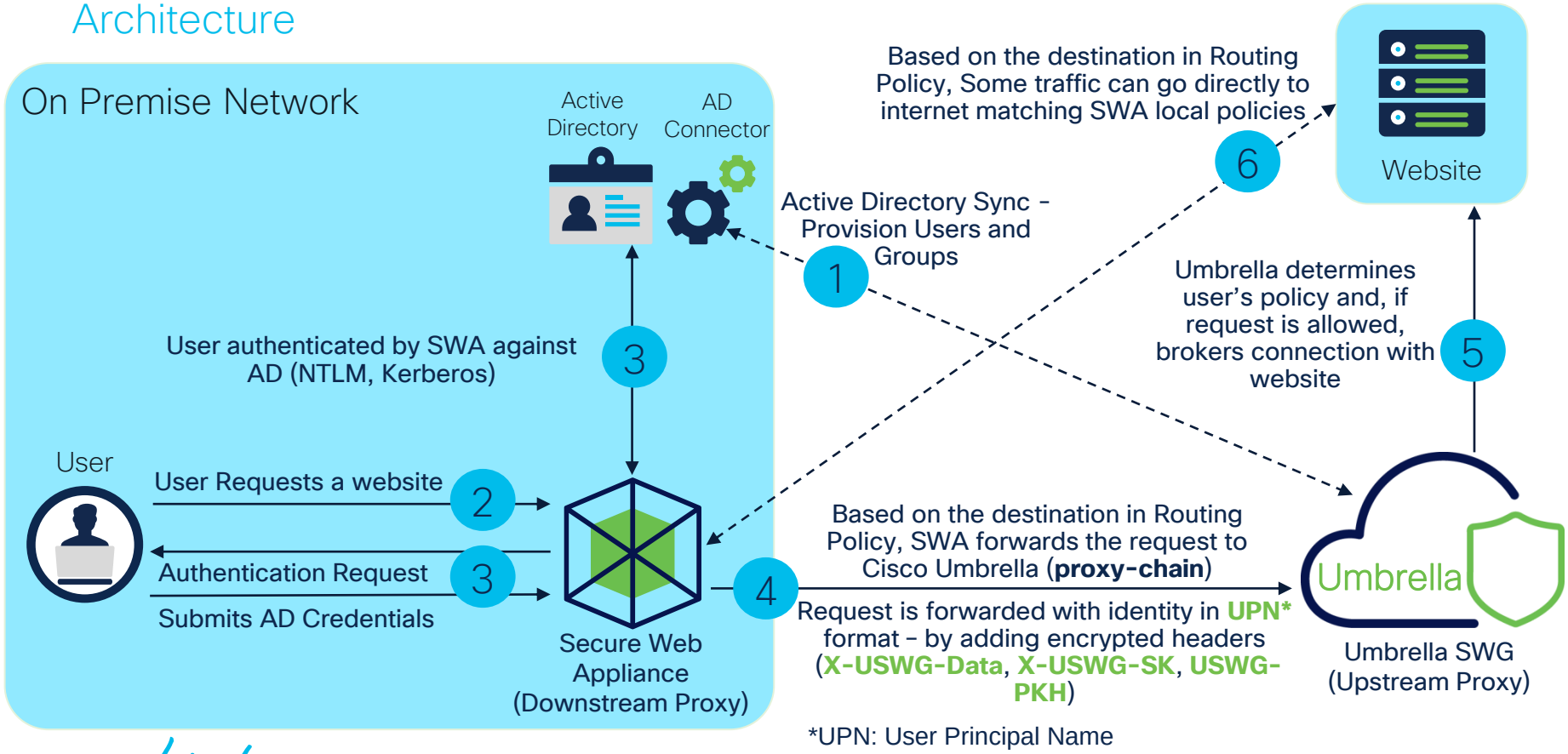
- User gets authenticated directly with Umbrella SWG as Service Provider and IdP of your choice
- Surrogate support options
  - Cookie surrogate: Requires HTTP/HTTPS inspection, requires cookie enabled
  - IP surrogate: more consistent userID auths, needs internal IP visibility through XFF (hence decryption on both SWA/SWG)
- Intended support for browsers, may not work for “desktop apps”

Seamless Identity Sharing

- Share user identity information authenticated by SWA with Umbrella SWG
- Leverage SWA’s user authentication using Active Directory (Basic, NTLM, Kerberos)
- Shared identity is used for policy enforcement and reporting on Umbrella
- Needs SWA v14.1 and later

Seamless Identity Sharing

Architecture



Seamless Identity Sharing

Benefits

- Minimal changes and smooth transition for existing SWA customers moving to hybrid and cloud proxies – leverage existing identity for on-prem users
- Improves the user experience by using transparent authentication (TUI)
- Expand the authentication and identity options on Umbrella SWG for policy enforcement and reporting beyond SAML.*
- Works better with desktop applications vs SAML authentication

*Check the following breakout for more information on Umbrella authentication methods:
Who is Behind the Umbrella? A View on User Authentication with Cisco Umbrella - BRKSEC-2287

Seamless Identity Sharing HTTP Headers

- Identity Headers are sent by SWA for CONNECT, HTTP Methods.
  - " **X-USWG-PKH**" : Public Key Hash Header field, contains the SIG public key identifier to be shared by the SWA.
  - "**X-USWG-SK**" : Value of X-USWG-SK http header field is a shared key, which is a symmetric key, created by SWA and encrypted with RSA public key followed by base-64 encoding.
  - " **X-USWG-Data**" : Value of X-USWG-Data http header fields contains all identity attributes shared by SWA in JSON format encrypted by symmetric key followed by base-64 encoding

Seamless Identity Sharing:
Configuration Walk-through

cisco Live!

Seamless Identity Sharing
Configuration Summary

On Umbrella Portal:

1. Add SWA's public IP (NAT) as network deployment
2. AD User and Groups provisioning (AD Connecter integration)
3. Export the Umbrella Root Certificate or CA (Certificate Authority) signed certificate from Umbrella dashboard.

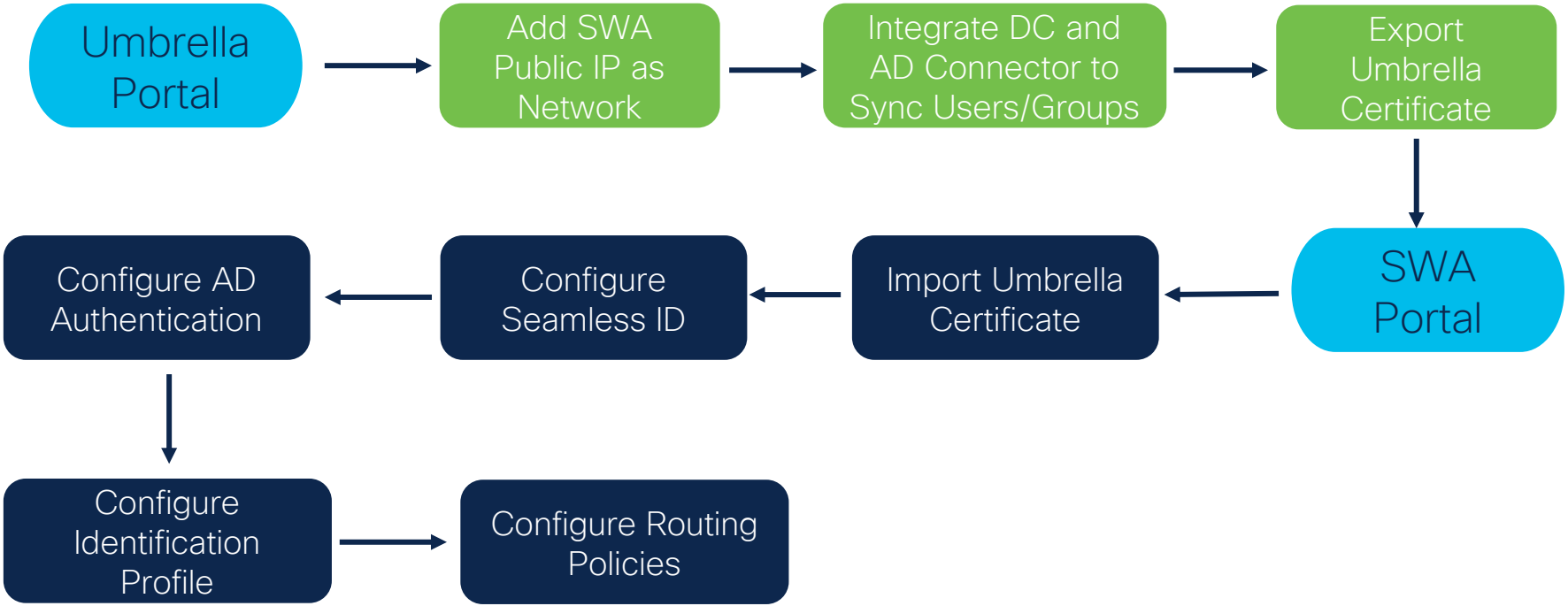
On Secure Web Appliance Portal – *(SWA needs to be v14.1 or later):*

1. Add Umbrella Root Cert CA to SWA's trusted certificate store.
2. Configure the **Cisco Umbrella Seamless ID settings** using **FQDN Anycast** (proxy.sig.umbrella.com) or **TCP Anycast** IP (146.112.255.50) with appropriate listening port(s), and specify Umbrella Org ID
3. Enable AD authentication and configure the needed identification profile(s)
4. Configure **Routing Policies** to use 'Cisco Umbrella Seamless ID profile' with appropriate port(s) as upstream proxy group and specify the suitable identification profile and **traffic match criteria**
5. (Recommended) Enable '**Decrypt for Auth**' in HTTPs Proxy settings to support identity for all HTTPS traffic

Detailed Configuration Guide: https://www.cisco.com/c/dam/en/us/products/se/2021/6/Collateral/swa-async-os.pdf

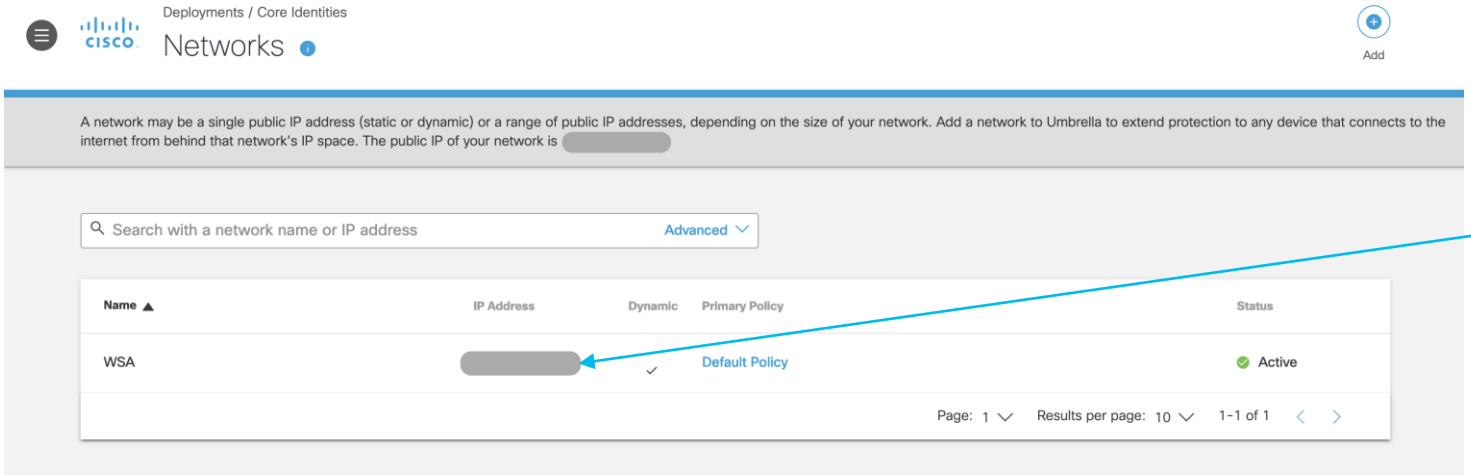
Seamless Identity Sharing

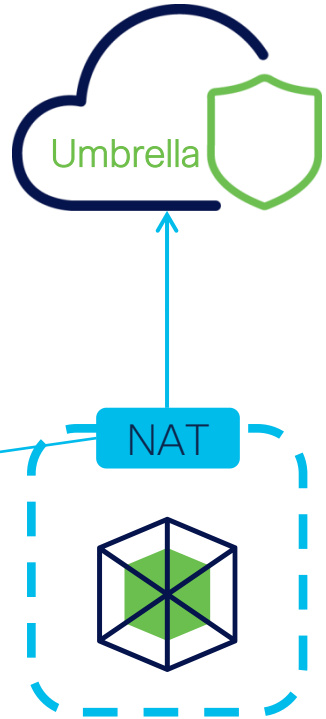
Configuration Flow



Add SWA Public Address as a Network on Umbrella

Add the SWA IP address (NAT Public Address) to the Umbrella Account as a Network, login to the Umbrella Dashboard then Deployment > Core Identities > Networks and add a new network



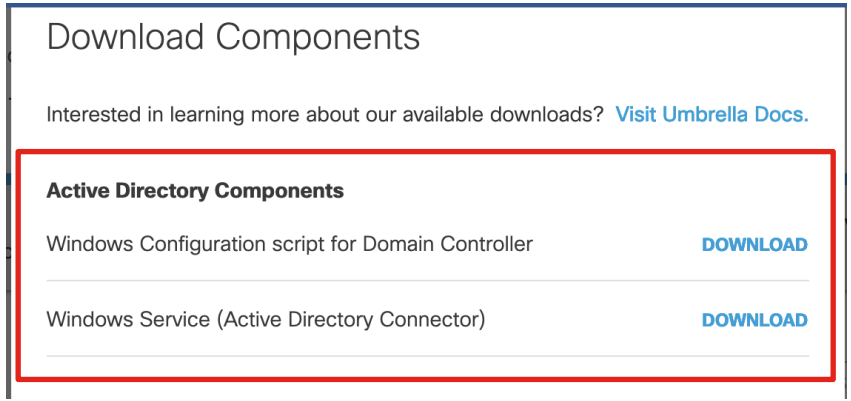


AD User and Groups provisioning

AD Connecter integration

Integrate Active Directory to the Umbrella Account for user database synchronization

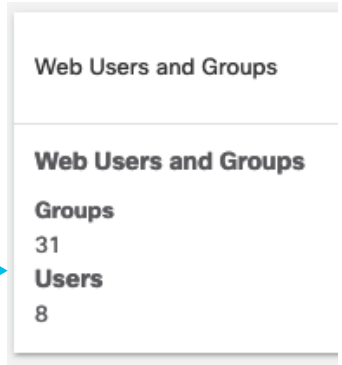
1. From Umbrella Dashboard go to Deployments > Configuration > Sites and Active Directory click on the Download button at the top right corner, download both Active Directory components
2. Register Domain controller and Install AD Connector, full installation steps from here
3. Verify That the Connector Syncs with the Umbrella Dashboard from Deployments > Core Identities > Users and Groups



Active Directory Domain Controller

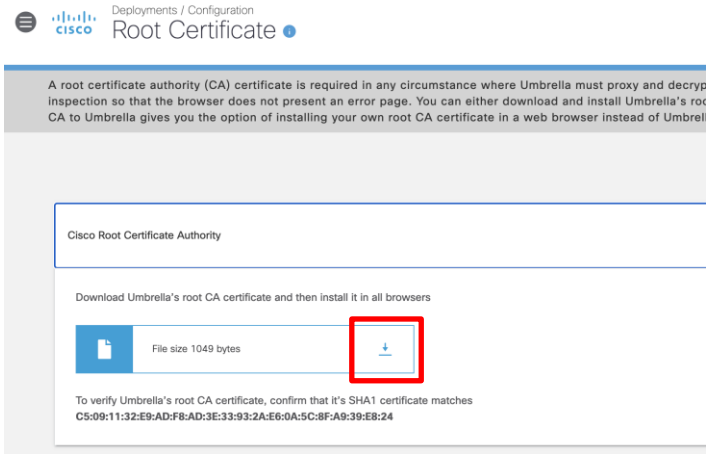
Umbrella AD Connector (runs on domain joined server)

Deployments > Core Identities > Users and Groups



Import Umbrella Certificate into SWA

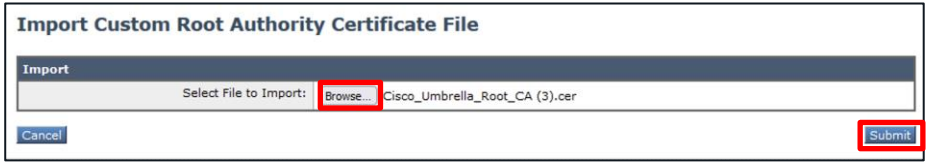
On Umbrella
Deployments > Configuration > Root Certificate
Download the certificate



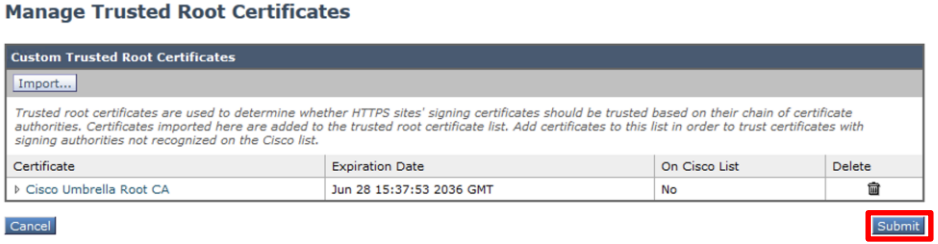
Note: You can use Umbrella Root Certificate or optionally customer provided CA Root Certificate

On SWA
Network > Certificate Management > Custom Trusted Root Certificate
Click on Import

Upload the Umbrella exported CA certificate, then click Submit



Another Submit, then commit the changes



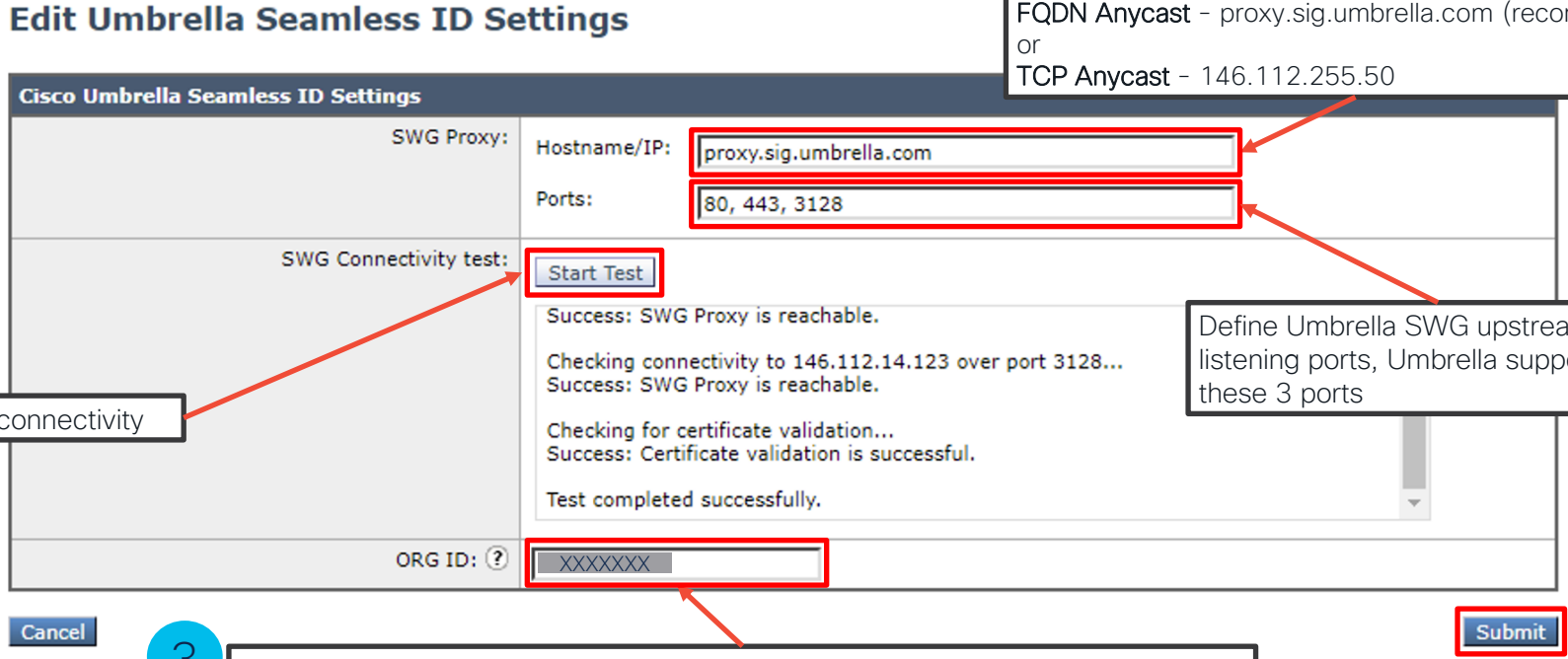
Configure the Cisco Umbrella Seamless ID Settings

From the SWA portal go to Web Security Manager > Cisco Umbrella Seamless ID then click on Edit Settings

Note: this configures the seamless ID feature along with the proxy chaining settings

1

Define Umbrella SWG upstream proxy:
FQDN Anycast - proxy.sig.umbrella.com (recommended)
or
TCP Anycast - 146.112.255.50



2

Define Umbrella SWG upstream listening ports, Umbrella supports these 3 ports

3

Specify Umbrella Org ID which ca be extracted from Umbrella dashboard URL:
https://dashboard.umbrella.com/o/<ORG ID>/#/overview

4

Test the connectivity

5

FQDN vs TCP Anycast

- **FQDN anycast (proxy.sig.umbrella.com) – Recommended**
  - Uses Umbrella DNS to discover the best datacenter to forward web traffic to and is the primary anycast method used across Umbrella.
  - If Umbrella DNS can be used, and the on-premises proxy can use an FQDN-based URL (SW has this ability) to define the upstream proxy, then FQDN anycast should be used.

- **TCP anycast (146.112.255.50)**
  - Does not use Umbrella DNS, and therefore can be employed by on-premises proxies that require the upstream proxy to be defined as an IP address.
  - TCP anycast is also appropriate for environments in which the on-premises proxy does not have DNS configured and all traffic forwarding decisions are made by IP address, offloading DNS lookups to the upstream proxy.

AD Authentication and Identification Profile on SWA

1 From the SWA portal go to Network > Identification Services > Authentication and add Active Directory realm

Authentication Realms

Add Realm...

Realm Name	Server Type	Scheme(s)	Servers	Transparent User Identification	Base DN or NetBIOS Domain	Delete
tarbader.com	Active Directory	Kerberos, NTLMSSP, Basic	192.168.15.200	Not Enabled	TARBADER	

2 From the SWA portal go to Web Security Manager > Authentication > Identification Profile and add an Identification Profile to authenticate the users against the AD realm you created

Client / User Identification Profiles

Add Identification Profile...

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Clone Policy	Delete
1	**Inside Subnet** Subnets: 192.168.150.0/24 Protocols: HTTP/HTTPS	Authenticate: Realm: tarbader.com (Scheme: Basic, NTLMSSP, Kerberos)	(global profile)		
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available		

Edit Order...

Configure the Routing Policies

From the SWA portal go to Web Security Manager > Routing Policies

1. **Add Policy** to specify the Routing Policy name and traffic membership/matching criteria

Routing Policies

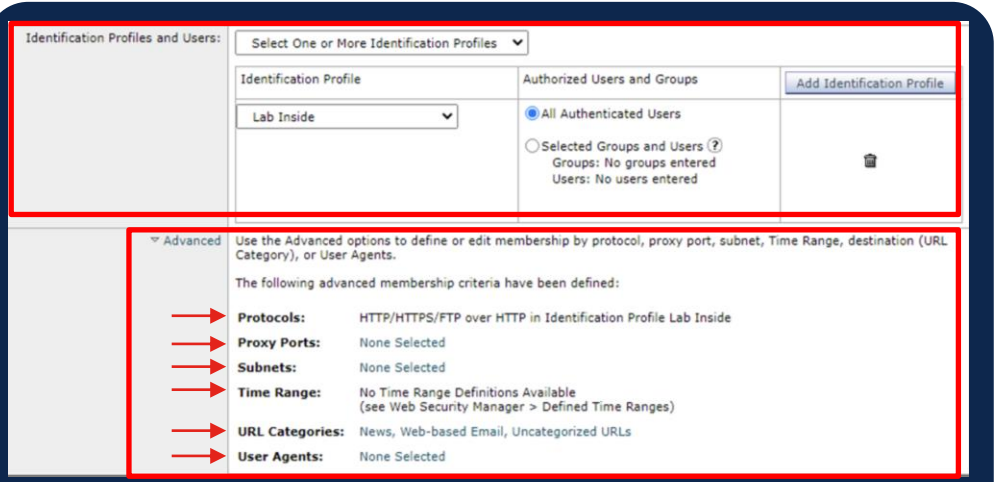
Routing Definitions

Add Policy...

Order	Members	Routing Destination
1	**BypassProxyChain** Identification Profile: All URL Categories: ProxyChainBypassList	Direct Connection
2	**SIG HTTPS Traffic** Identification Profile: Lab Inside All identified users	Cisco Umbrella Seamless ID 443 proxy.sig.umbrella.com:443
3	**SIG HTTP Traffic** Identification Profile: All Protocols: HTTP	Cisco Umbrella Seamless ID 80 proxy.sig.umbrella.com:80
	Global Routing Policy	Direct Connection

Edit Policy Order...

2. Specify the proxy that will handle the matching traffic:
   - **Direction Connection** → Handle locally on SWA
   - **Cisco Umbrella Seamless ID** → Proxy Chain to Umbrella SWG upstream proxy and share identity. We create a routing policy for each Umbrella listening port configured in the Seamless ID Settings



Matching Criteria

1. Identification Profile and Users/Groups
2. Protocols
3. Proxy Ports
4. Subnets
5. Time Range
6. URL Categories*
7. User Agents

*URL category membership requires explicit proxy for HTTPs traffic

Routing Policy based on URL Categories

Explicit vs Transparent Proxy Mode

- Defining Routing Policies to redirect traffic to upstream proxy like Umbrella based on URL Categories **works only with Explicit** SWA mode for HTTPs traffic, it **does not work with Transparent** SWA mode

- **Why?**

  For transparently redirected HTTPS requests, the Web Proxy must contact the destination server to determine the server's name and therefore the URL category in which it belongs. Due to this, when the Web Proxy evaluates Routing Policy Group membership, it cannot yet know the URL category of an HTTPS request because it has not yet contacted the destination server. If the Web Proxy does not know the URL category, it cannot match the transparent HTTPS request to any user-defined Routing Policy because of insufficient information.

- **What Happened for such traffic?**

  As a result, transparently redirected HTTPS transactions only match Routing Policies if no Routing Policy Group and no identification profile has a membership criteria. If any user-defined Routing Policies or identification profiles define their membership by URL category, then the transparent HTTPS transactions match the Default Routing Policy Group.

- **You can use SWA in transparent mode in Hybrid SWG only if you need traffic to be authenticated using Seamless ID against on-premise AD, and you need everything to be handled in Umbrella.**

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa-14-5/user-guide/wsa-userguide-14-5/b_WSA_UserGuide_11_7_appendix_010111.html?bookSearch=true#con_1316471

Routing Policy Configuration Approaches

1- Conservative Mode (More On-premise)

- Default policy is to handle traffic by SWA directly
- Selective traffic and destinations to be sent to Umbrella based on routing policy traffic membership
- Both Umbrella and SWA are used to configure relevant policy and features needed as per use cases (*this will change with the coming Common Hybrid Policies feature*)
- Gives more control, use cases and features
- Explicit proxy mode is needed for the URL category traffic matching

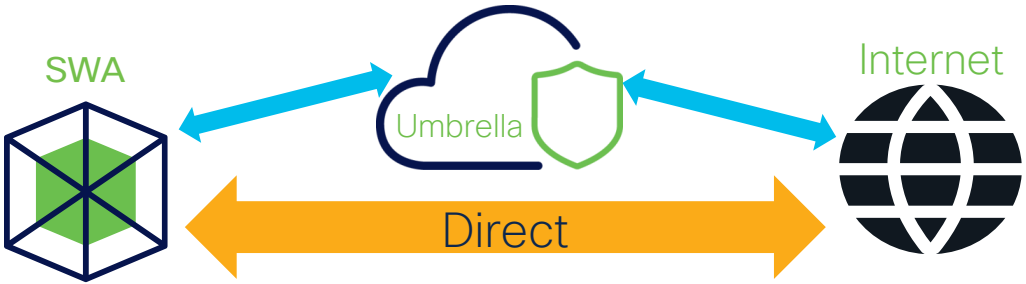
Routing Policies

Routing Definitions

Add Policy...

Order	Members	Routing Destination
1	**BypassProxyChain** Identification Profile: All URL Categories: ProxyChainBypassList	Direct Connection
2	**SIG HTTPS Traffic** Identification Profile: All URL Categories: Umbrella Policy Debug, Umbrella RBI, News, Sports...	Cisco Umbrella Seamless ID 443 proxy.sig.umbrella.com:443
3	**SIG HTTP Traffic** Identification Profile: All URL Categories: News, Sports and Recreation, Web-based Email	Cisco Umbrella Seamless ID 80 proxy.sig.umbrella.com:80
	Global Routing Policy	Direct Connection

Edit Policy Order...



Routing Policy Configuration Approaches

2- Cloud Friendly Mode (More Cloud)

- Default policy is to send to Umbrella with selective exceptions to be handled locally by SWA
- Umbrella is the main portal used day to day to configure the policy and see reporting, simpler operation
- For any selective exceptions to be handled locally, needed SWA configurations should be done
- Explicit proxy mode is needed for the URL category traffic matching
- Transparent proxy mode is possible if we only need SWA for Seamless ID and no URL category membership is defined

Routing Policies

Routing Definitions

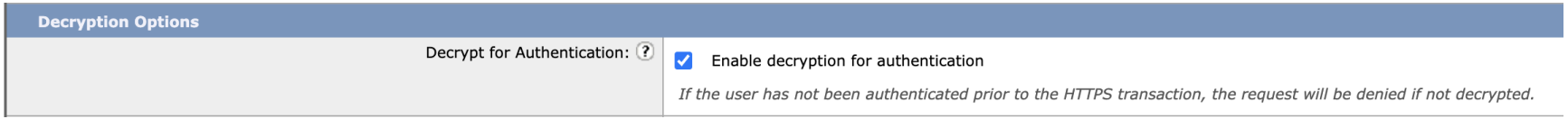
Add Policy...

Order	Members	Routing Destination
1	**BypassProxyChain** Identification Profile: All URL Categories: ProxyChainBypassList	Direct Connection
2	**SIG HTTPS Traffic** Identification Profile: Lab Inside All identified users	Cisco Umbrella Seamless ID 443 proxy.sig.umbrella.com:443
3	**SIG HTTP Traffic** Identification Profile: All Protocols: HTTP	Cisco Umbrella Seamless ID 80 proxy.sig.umbrella.com:80
	Global Routing Policy	Cisco Umbrella Seamless ID 3128 proxy.sig.umbrella.com:3128

Edit Policy Order...

Enable Decrypt for Authenticaiton

From the SWA portal go to Security Services > Proxy Settings > HTTPS Proxy then click on Edit Settings, then check Enable decryption for authentication



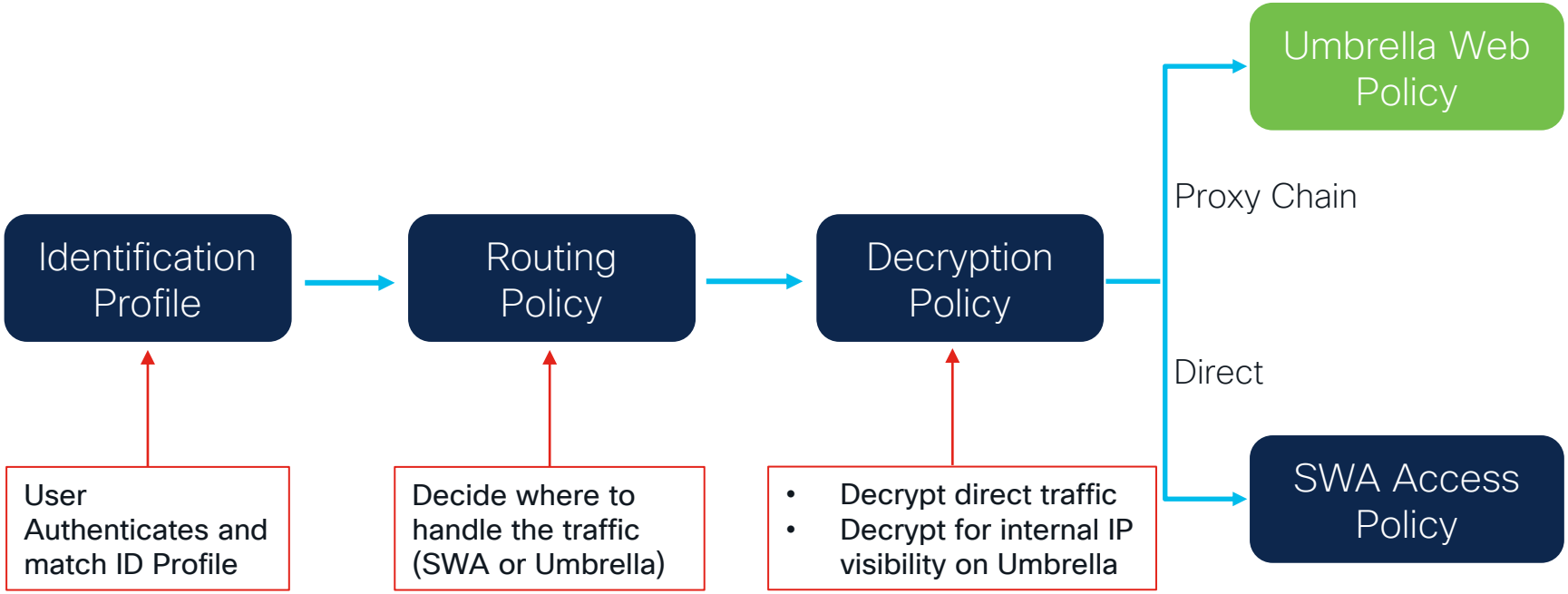
- This will ensure to authenticate all HTTPs traffic in all scenarios
- It allows decryption to do the authentication for users/traffic who have not been authenticated prior to current HTTPs request.
- It determines how the Web Proxy handles an HTTPS request that comes before any HTTP request, when authentication is enabled and uses an IP-based surrogate.
- This applies to all transparent requests, and to explicit forward requests when credential encryption is enabled (see Network > Authentication).

Seamless ID HTTPs Traffic Behavior

Deployment Mode	Surrogate	Decrypt for Authentication	Secure Web Appliance Authentication	Cisco Umbrella Seamless ID Sharing
Explicit	IP surrogate	Yes/No	Yes	Yes
Transparent	IP surrogate	Yes	Yes	Yes
Transparent	IP surrogate	No	Skips authentication	No
Explicit	Cookie, without credential encryption	Yes/No	Yes	Yes
Explicit	Cookie, with credential encryption	Yes/No	Yes	No
Transparent	Cookie with/without credential encryption	Yes/No	Skips authentication	No

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa-14-5/user-guide/wsa-userguide-14-5/b_WSA_UserGuide_11_7_chapter_0100.html?bookSearch=true#Cisco_Concept.dita_8fa3b857-af44-403f-be9c-9cf71f82aa7d

Hybrid SWG Policy Matching Flow



Use Internal IPs for Enforcement and Visbility

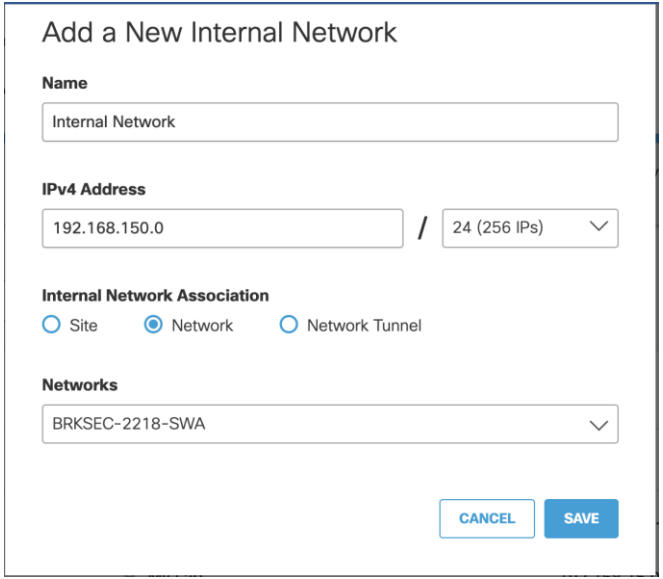
REFERENCE

1. Enable XFF to be sent
SWA Portal > Security Services > Proxy Settings > Web Proxy > Edit Settings > Advanced Settings)

Generate Headers:	X-Forwarded-For:	Send	Do Not Send

2. Configure Internal Subnet on Umbrella dashboard (Deployments > Configuration > Internal Networks then Add a new Internal Network and associate it with the SWA Public Address that is registered as a Network identity on Umbrella

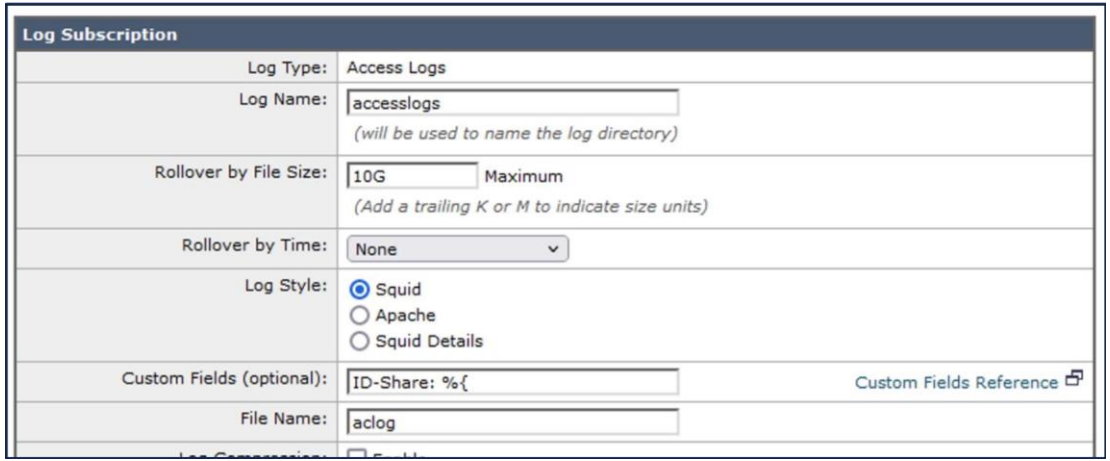
3. Make sure that any HTTPs traffic that you need to be identified on Umbrella using Internal IP to be **decrypted** on SWA using the Decryption Policies



Validation Tips

To check the Seamless ID-Sharing headers were added for a given request, add optional formatter “%{“ in the access logs custom field.

SWA Portal > **System Administration** > **Log Subscriptions** > Click on **accesslogs** to edit



Seamless ID is shared

```
1621509856.915 387 192.168.104.103 TCP_MISS_SSL/200 132 CONNECT
tunnel://edition.cnn.com:443/ "DC1\testuser123@AD"
DEFAULT_PARENT/146.112.255.50 - DECRYPT_WEBCAT_7-
Org1_Decryption_Policy-Org1_HTTPS_Test_Traffic-NONE-NONE-NONE-
HTTPS_SIG_Traffic-NONE <"IW_news",2.0,-,"-",-,-,-,-,"-",-,-,-,"-",-
,-,"-","-",-,- ,"IW_news",-,"-","News","-","Unknown","Unknown","-
","-",2.73,0,-,"-","-",-,"-",-,-,"-","- ",-,-,"-",-,-> - - - NTLMSSP
User-Agent : "curl/7.68.0" IP Spoofing Profile : - Header Profile :
None ID-Share: ID_SHARED
```

Seamless ID is not shared

```
1621509859.222 2305 192.168.104.103 TCP_MISS_SSL/200 1122223 GET
https://edition.cnn.com:443/ "DC1\testuser123@AD"
DEFAULT_PARENT/146.112.255.50 text/html DEFAULT_CASE_12-
Org1_Access_Policy-Org1_HTTPS_Test_Traffic-NONE-NONE- NONE-
HTTPS_SIG_Traffic-NONE <"IW_news",2.0,1,"-",0,0,0,1,"-",-,-,-,"-
",1,-,"-","- ",-,-,"IW_news",-,"Unknown","News","-
","Unknown","Unknown","-","-",3894.92,0,- ,"Unknown","-",1,"-",-,-
,"-","-",-,-,"-",-,-> - - - NTLMSSP User-Agent : "curl/7.68.0" IP
Spoofing Profile : - Header Profile : None ID-Share: -
```

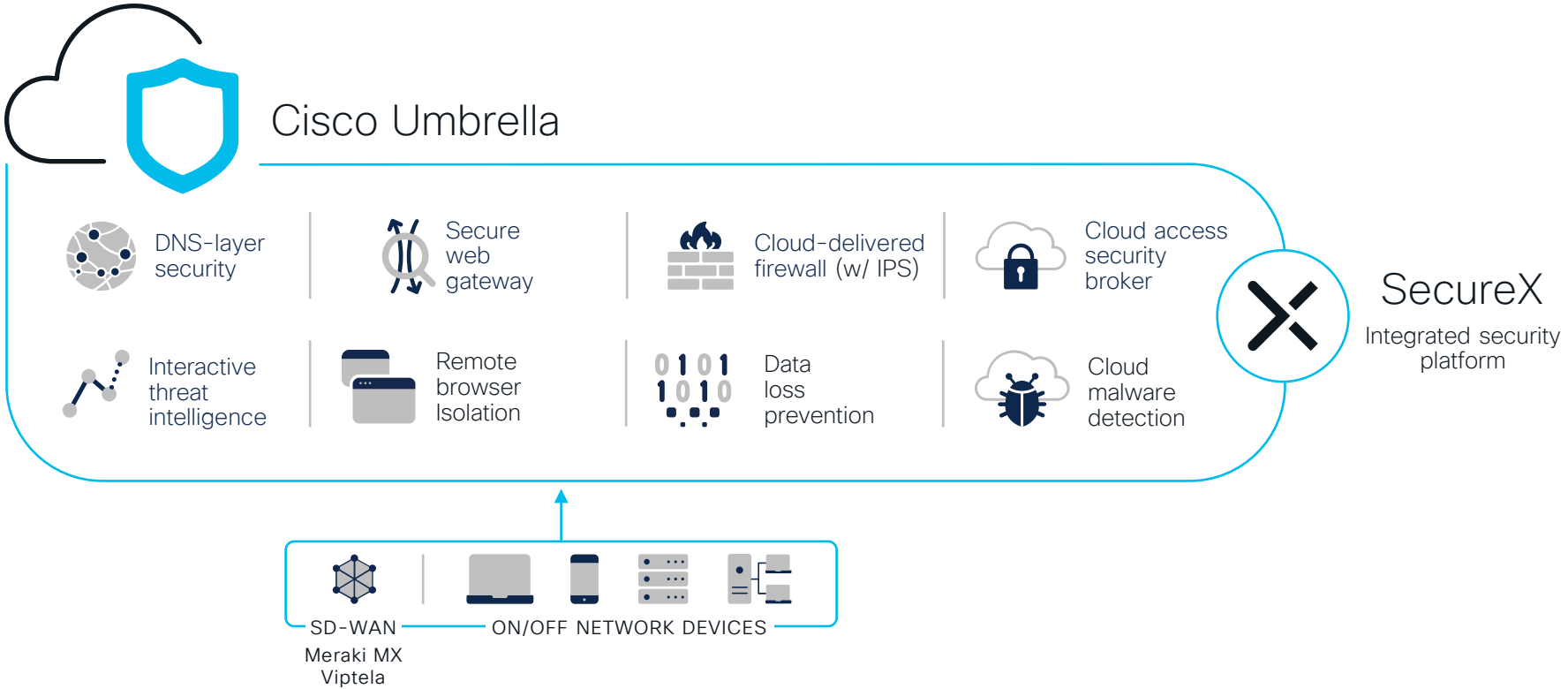
Validation Tips

Use the http://policy-debug.checkumbrella.com URI to check the applied end-user web policy, which returns the Web-Policy, OrgID, and User-Info / Type.

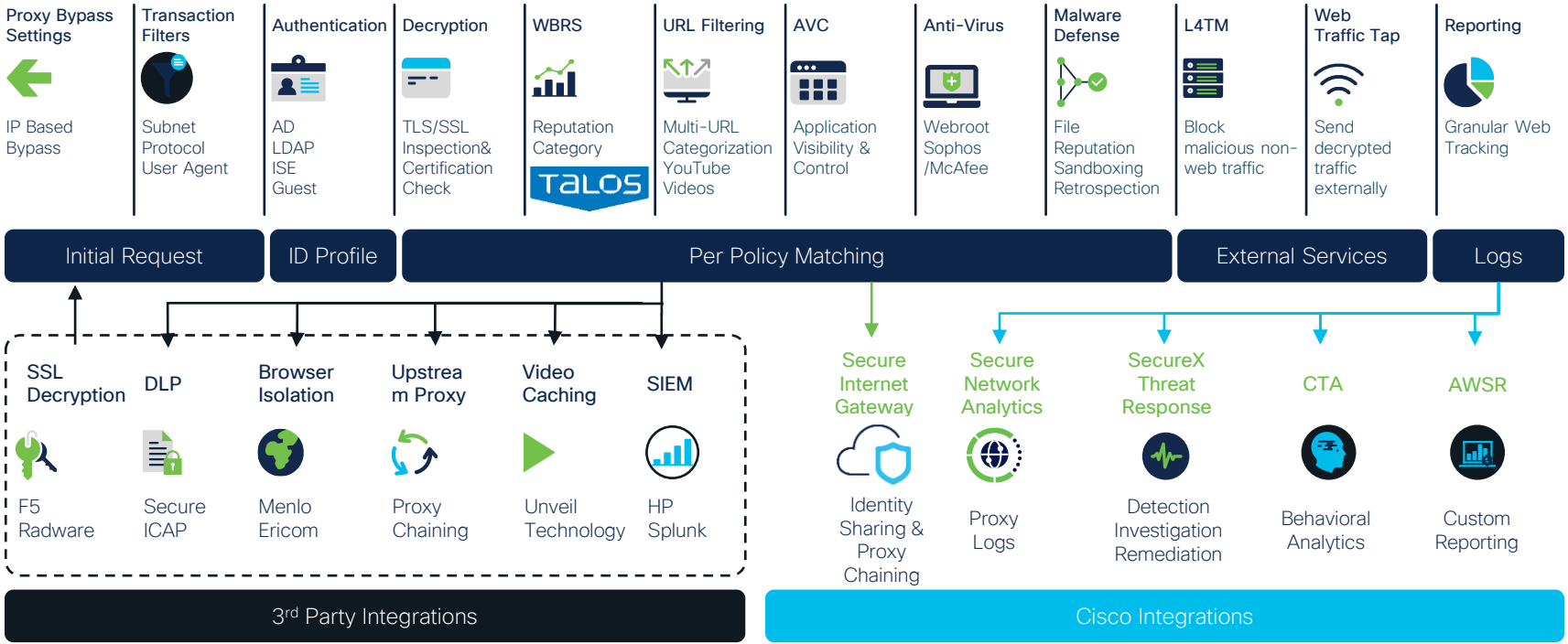
Based on it, you can verify if the machine is protected by Umbrella SWG, and you can differentiate if its through SWA downstream proxy or directly to Umbrella

Hybrid SWG
Use Cases

Cisco Umbrella



Cisco Secure Web Appliance Pipeline



Umbrella SWG Use Cases

1. Remote Browser Isolation
2. SaaS/Cloud applications to be handled using Umbrella
3. Offload SSL Decryption to cloud scale
4. Multimode CASB/DLP with unified policy and reporting
5. Roaming clients web traffic

Secure Web Appliance Use Cases

1. Handle Restricted destinations
2. Web traffic to be scanned by internal DLP (ICAP integration)
3. Layer 4 Traffic Monitor
4. Global Threat Alerts (aka CTA)
5. Decrypted Web Traffic Tap to monitoring systems (SIEM, NDR, IDS)
6. Bandwidth Control

SWG Use Case: Remote Browser Isolation

Remote Browser Isolation

- Provide air gap between user device and browser-based threats
- Choose from three levels of protection
- Deploy rapidly without changing existing browser configurations

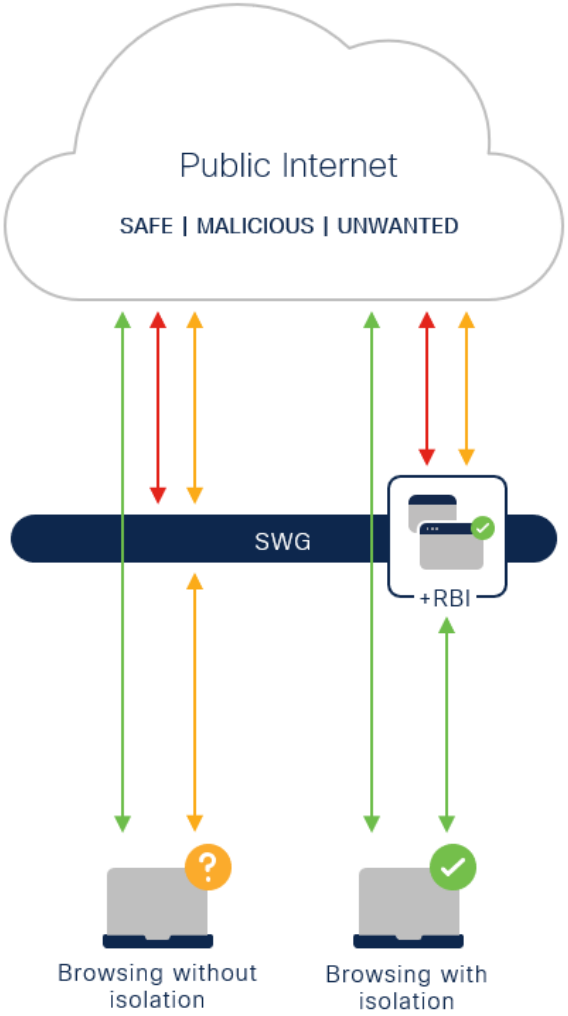
Results

✓ Protect from browser-based attacks

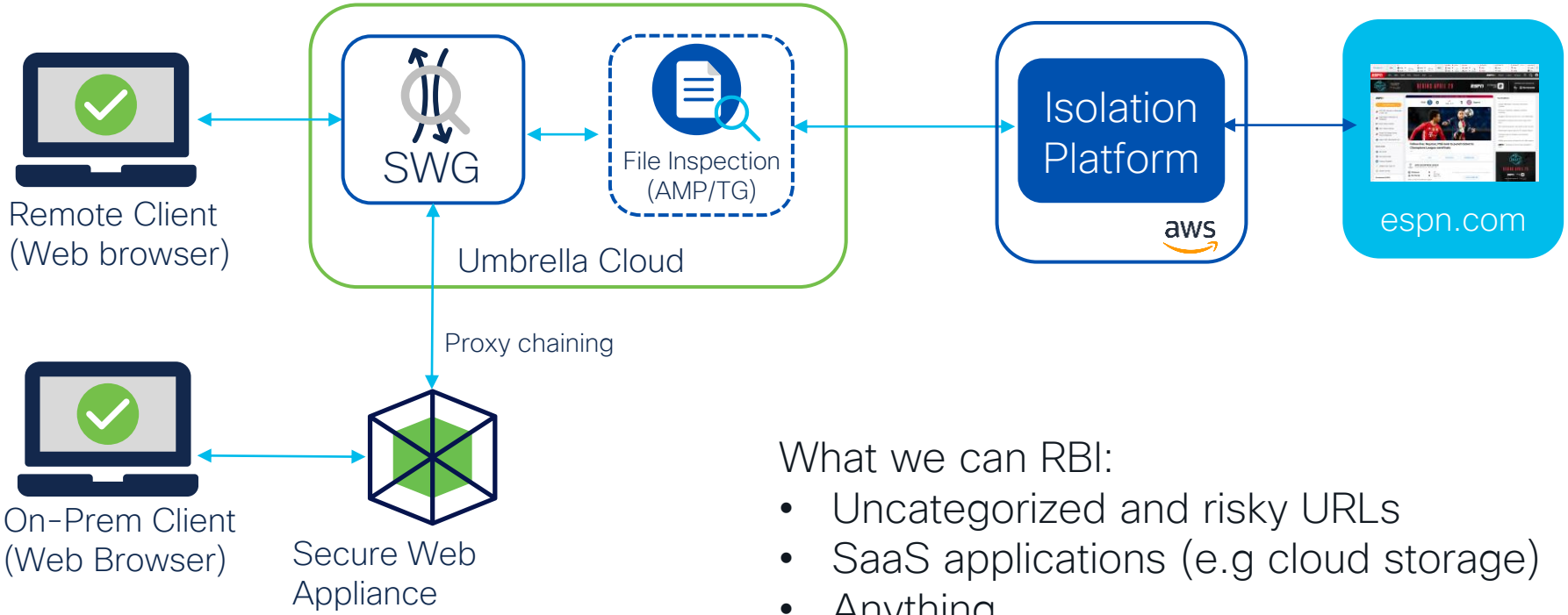
✓ Improve productivity

✓ Reduce alerts and incidents

✓ Support compliance goals



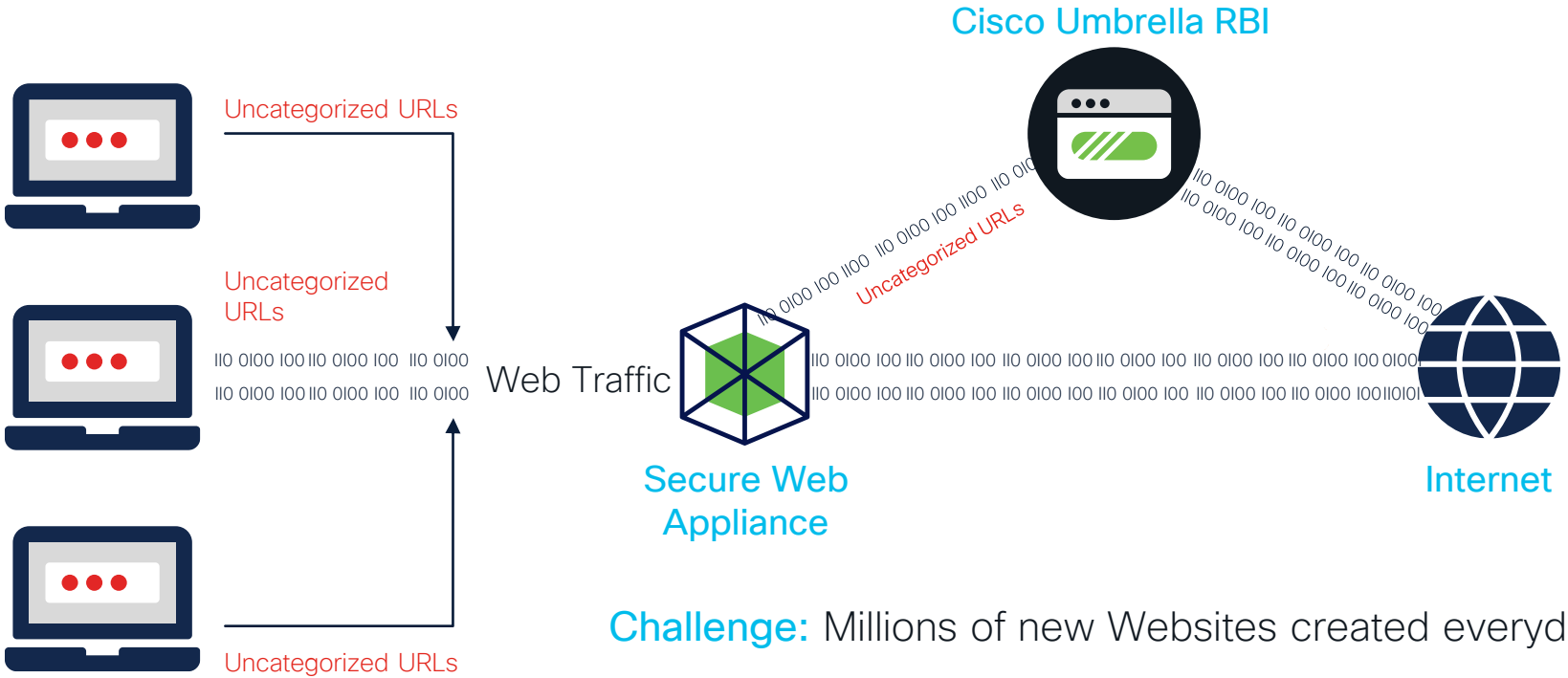
Leveraging RBI in Hybrid SWG



What we can RBI:

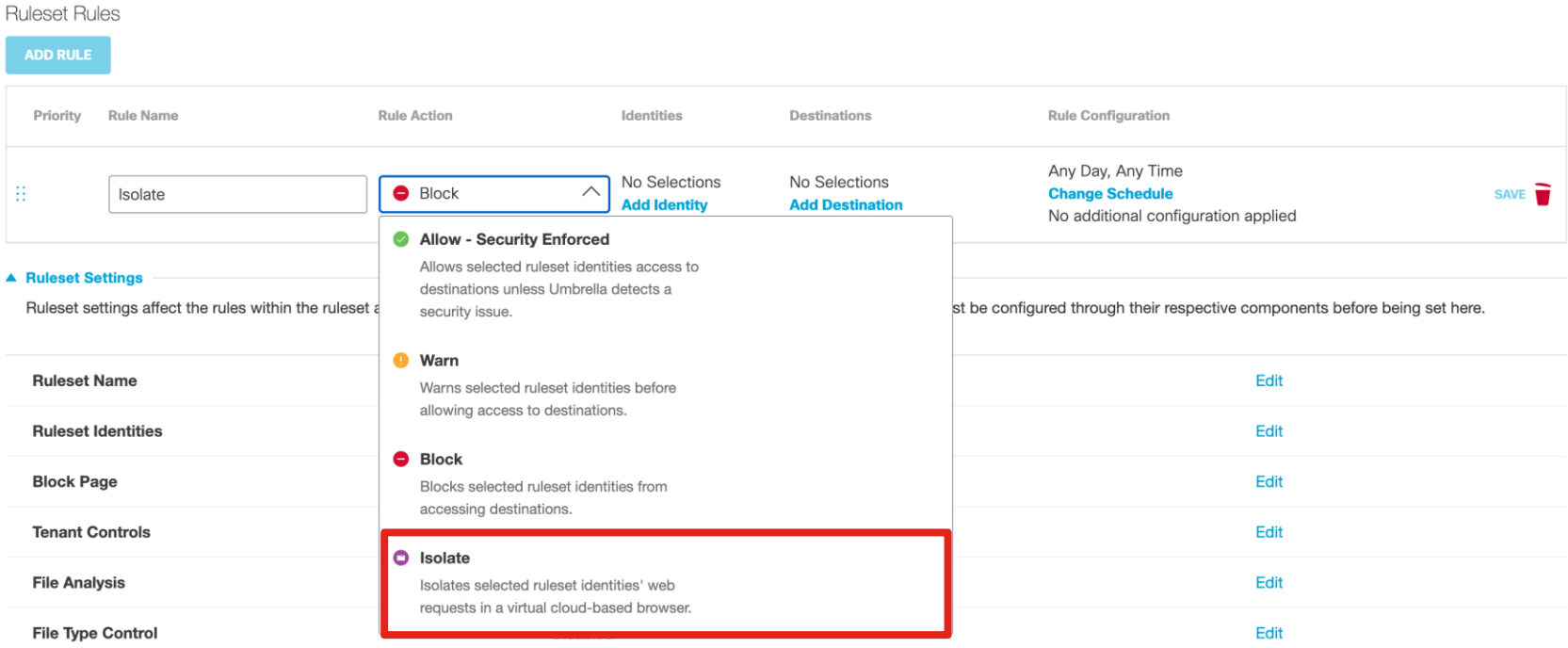
- Uncategorized and risky URLs
- SaaS applications (e.g cloud storage)
- Anything

Key Use Case: Uncategorized URLs



Challenge: Millions of new Websites created everyday

RBI integrated in a very simple way



SWG Use Case: SaaS/Cloud Applications

Handling SaaS/Cloud Applications by Umbrella SWG

A perfect match in the cloud !

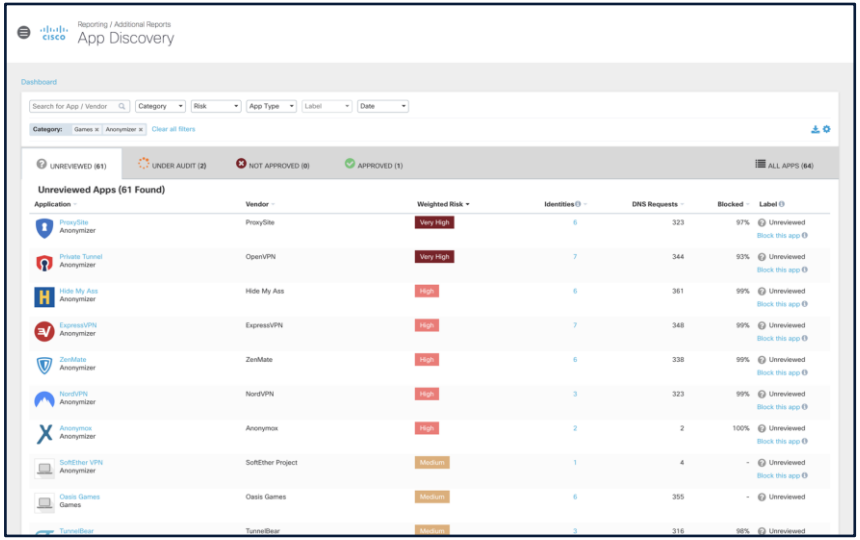
Why using Umbrella for SaaS:

- Umbrella is faster for SaaS
- Shadow IT visbility and control
- Advanced App Controls
- SaaS Tenant Control
- Multimode CASB/DLP with unified policy and reporting
- O365 compatability mode
- Remote Browser Isolation (RBI)

App discovery and controls

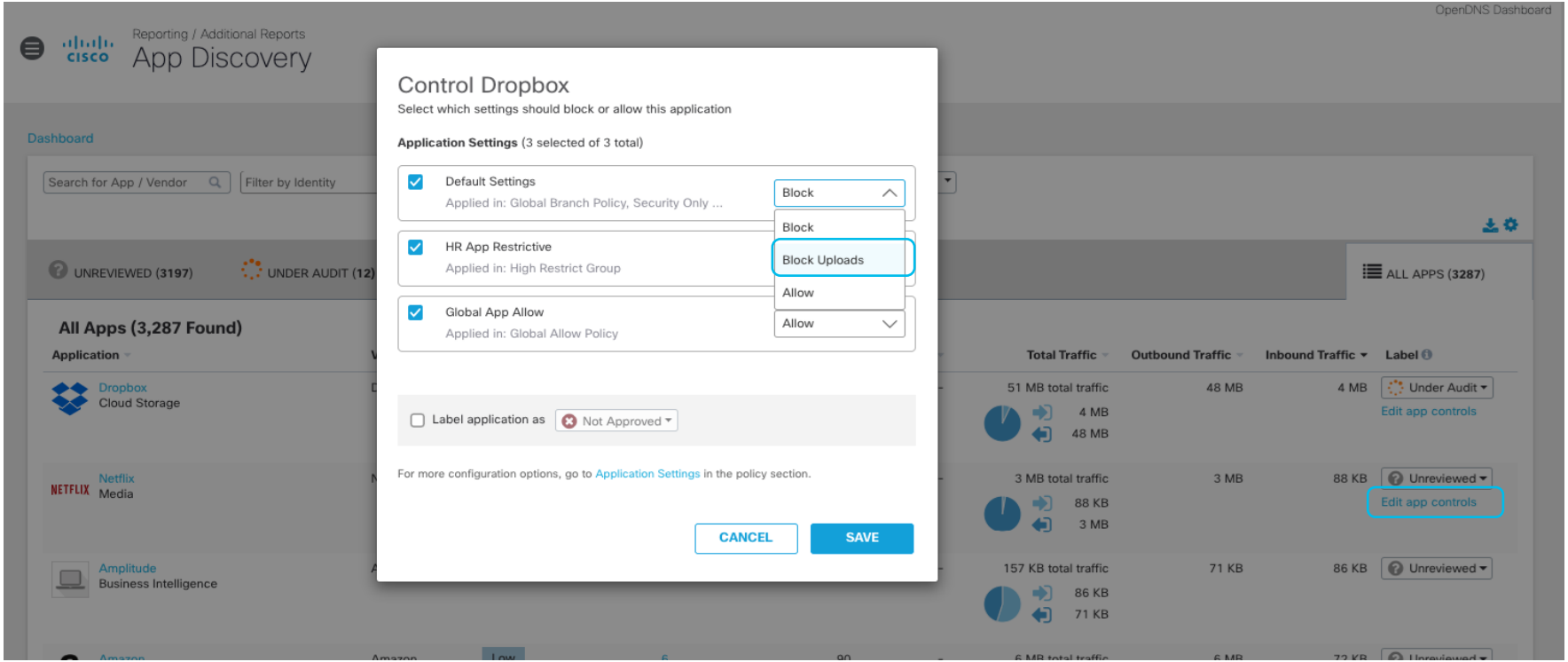
Visibility into shadow IT and control of cloud apps

- Full list of cloud apps in use
- Reports by category and risk level
- Number of users and amount of incoming and outgoing traffic
- Blocking of high-risk categories or individual apps



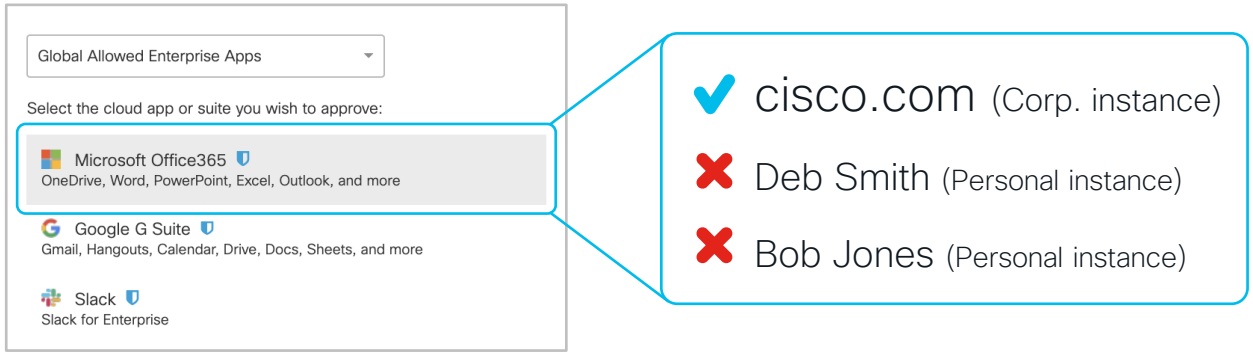
Granular app controls

e.g Block uploads (i.e. Dropbox/Box)
e.g Block attachments (i.e. webmail)



Tenant controls

Select the instance(s) of Core SaaS applications that can be accessed by all users or by specific groups/individuals



Key Use Cases

Security
Ensure, sensitive data is created and stored in approved instances of cloud apps

Productivity
Only provide access to corporate instances of core SaaS apps

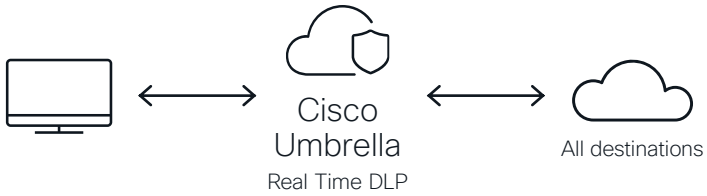
*Check BRKSEC-2143 for more details

Multimode Cloud Data Loss Prevention (DLP)

Unified policies and reporting for a single customer experience

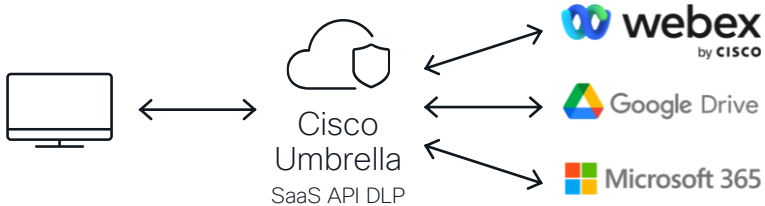
Real-time (inline) DLP

- Works via Umbrella Secure Web Gateway proxy
- Scans web traffic inline for real-time enforcement
- All application coverage: Sanctioned and unsanctioned



SaaS API (out-of-band) DLP

- Works via cloud APIs for data at rest; no web proxy required
- Scans traffic out-of-band with near real-time enforcement
- Sanctioned app coverage



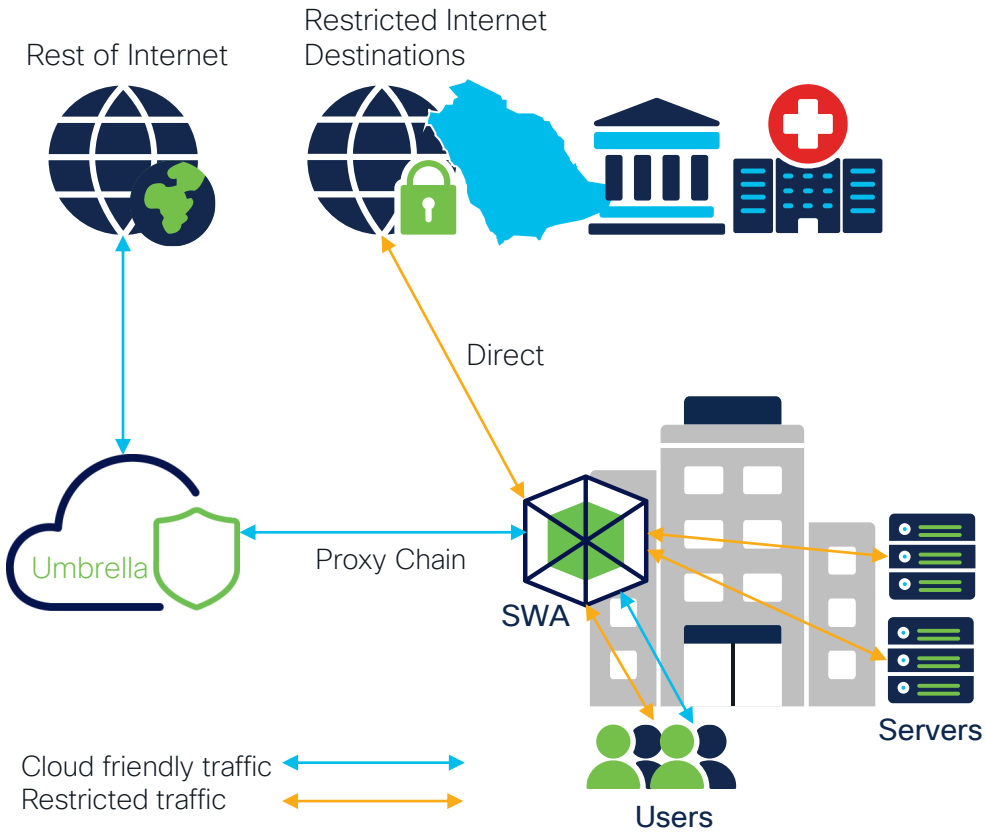
Same management interface

SWA Use Case: Handle Restricted Traffic

Use Case: SWA for Restricted Traffic

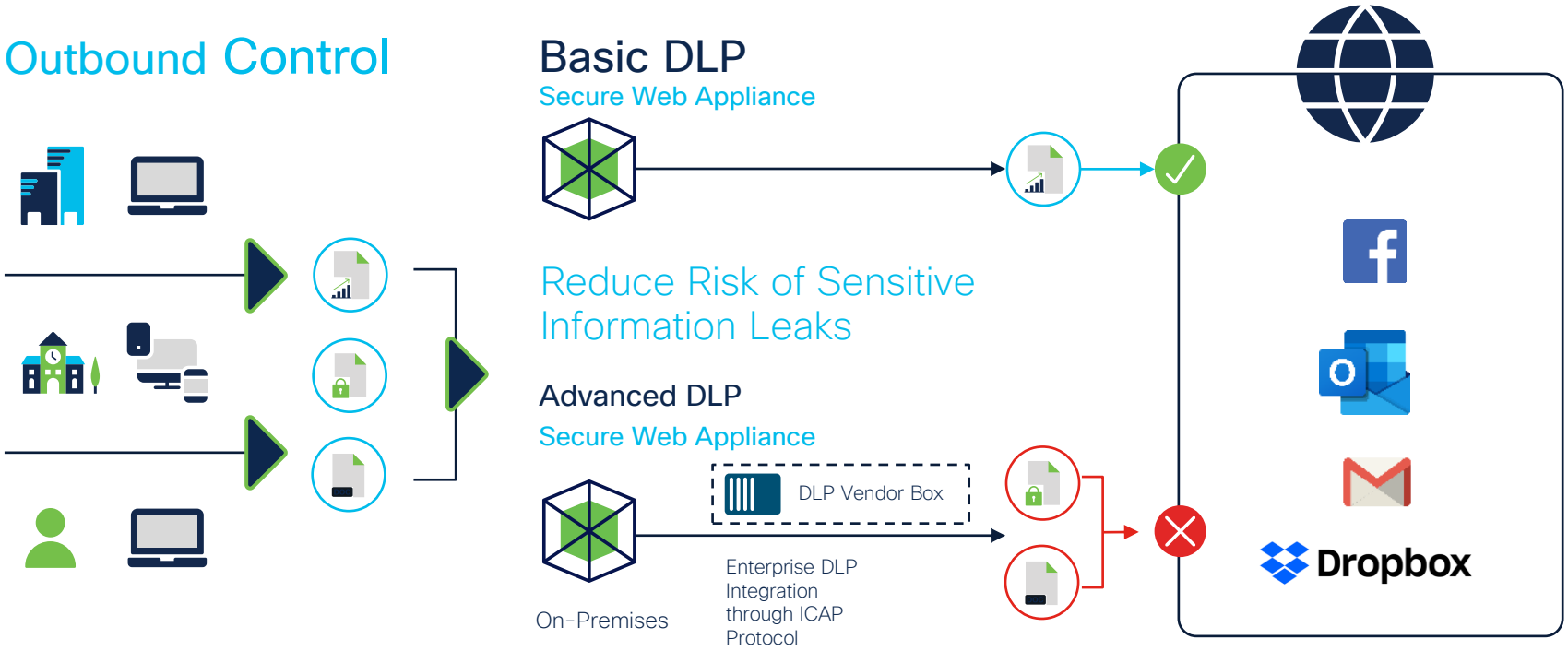
Examples:

- Servers Web Traffic
- Restrited countries -with no Umbrella DC- local traffic
- Government services traffic
- Healthcare/Financial services traffic
- Traffic to countries don't not allow from cloud proxies



SWA Use Case: Internal/On-prem DLP integration

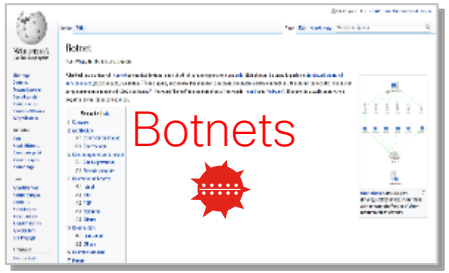
Data Security & Data-Loss Prevention

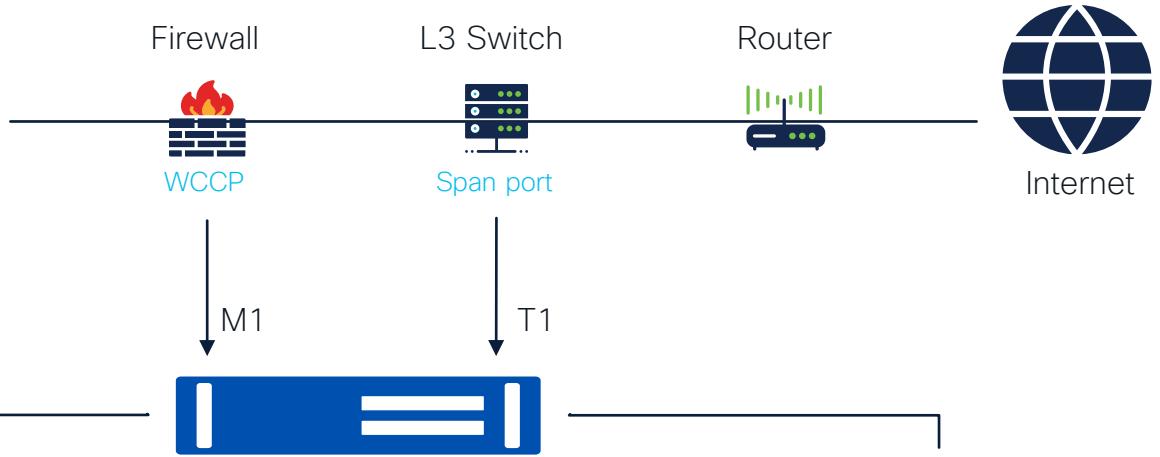


SWA Use Case: L4 Traffic Monitor

Layer 4 Traffic Monitoring

Protect against C2 and botnets traffic on non-web and non-standard ports





- Sends RSTs for TCP sessions
- Sends ICMP unreachable messages for UDP sessions
- Packets are sent out the Proxy Port

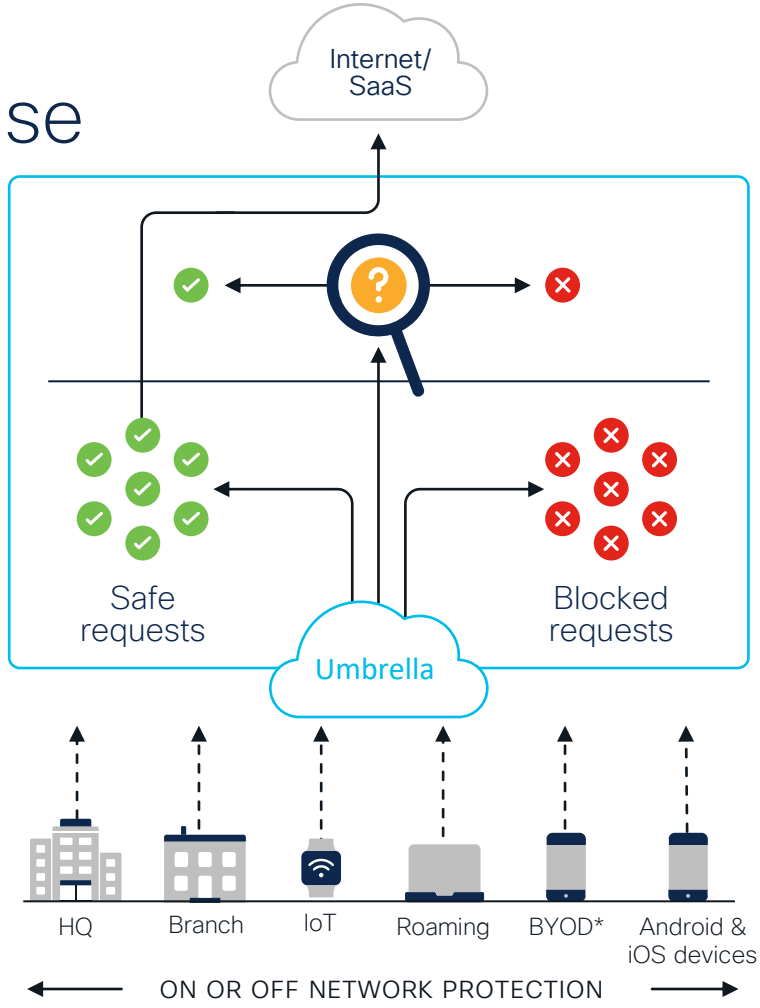
- Packet capture from Switch
- All TCP/UDP Traffic
- No IP address assigned

Cherry on the Cake: DNS Security

A versatile first line of defense

- All office locations
- Any device on your network
- Roaming laptops and mobile devices
- Every port and protocol

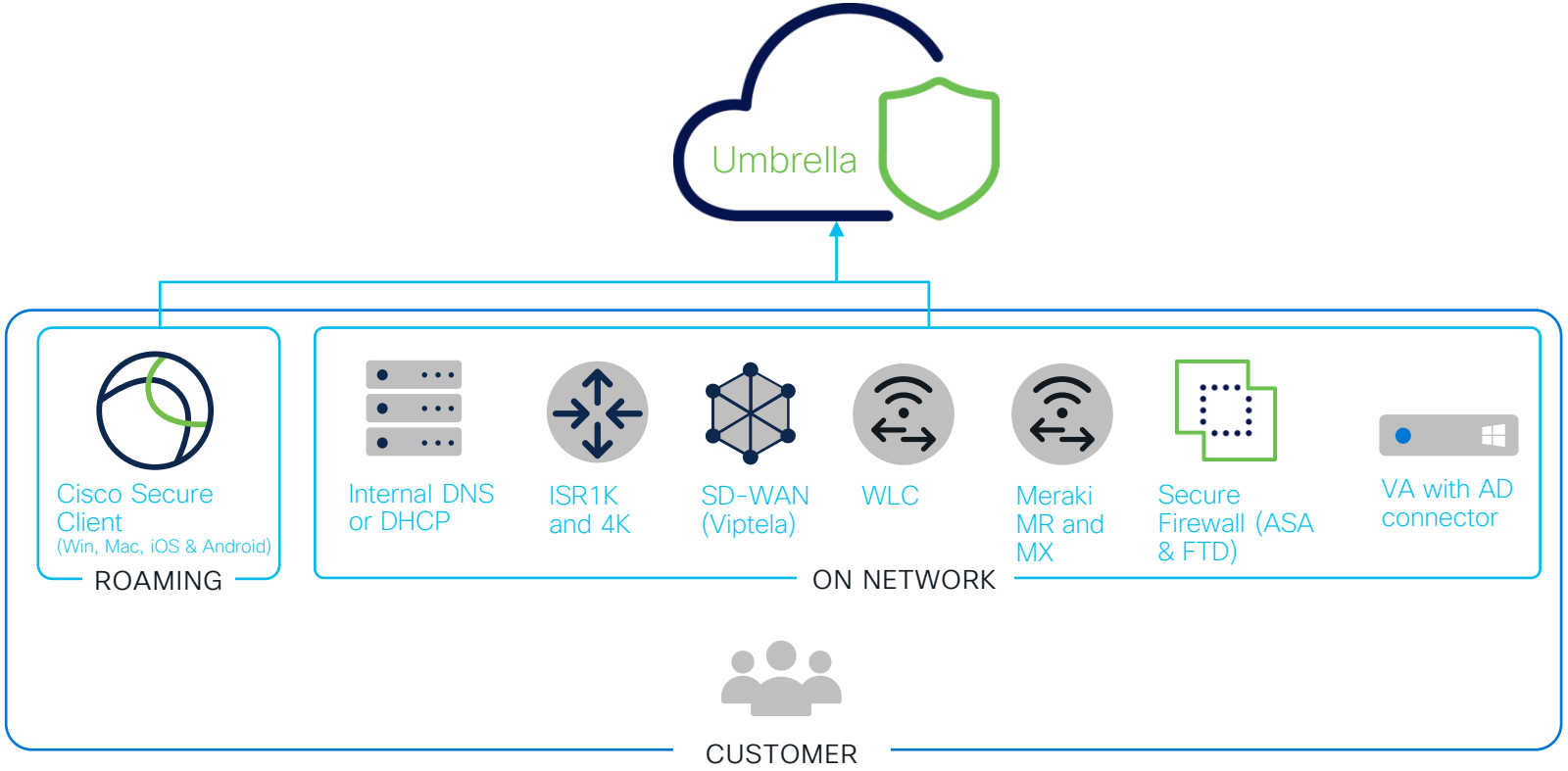
✓ DNS-layer security provides unique protection



Umbrella DNS Security Value in Hybrid SWG

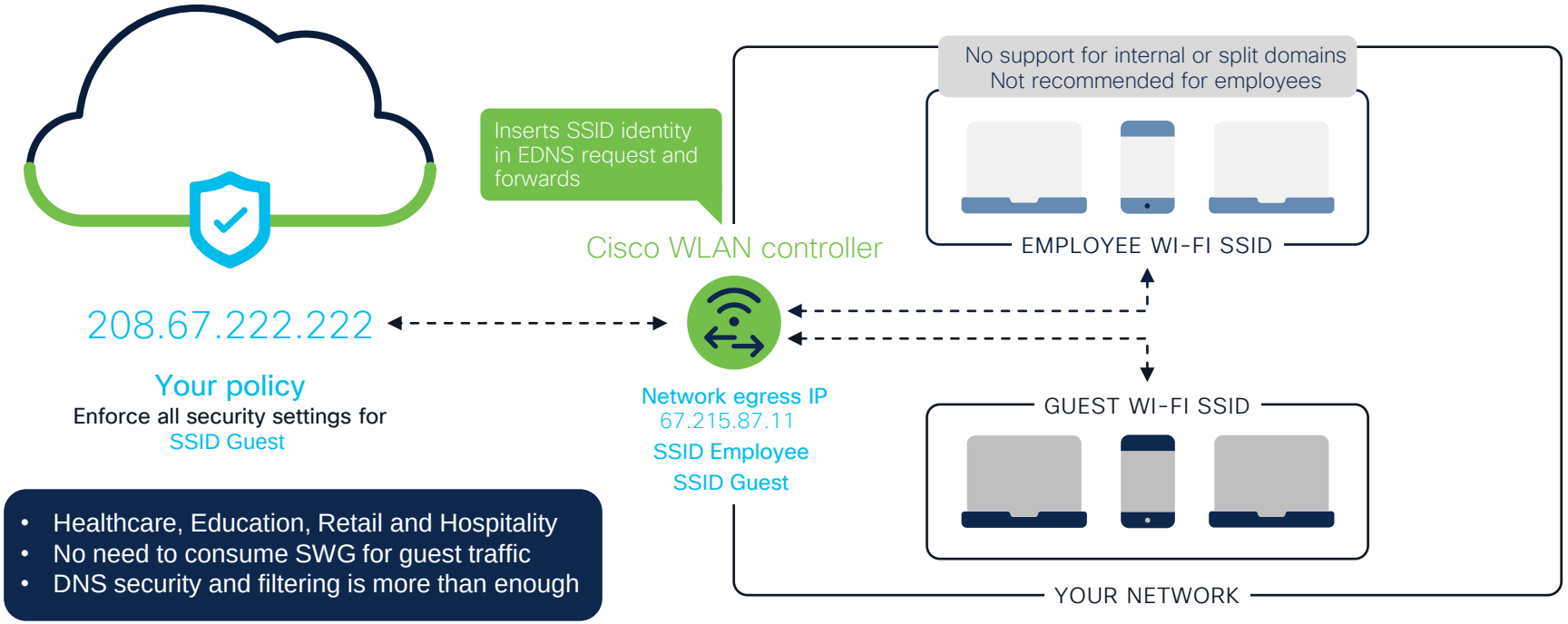
- Early enforcement and without delay
  - Get rid of security issues (malicious destinations) on DNS layer (port agnostic)
  - Filter unwanted traffic and content early in the pipeline
  - Enhance the overall performance of network and on-prem security appliances.
- Faster time to value in implementation
  - No need to wait rolling out the SWG across the enterprise to get protection, secure the whole network in 5 minutes.
- Adds great unique use cases in Hybrid SWG architecture:
  1. Guest WiFi
  2. Mobile devices security protection (iOS and Android) – Managed and Unmanaged
  3. Newly Seen Domains
  4. DNS Tunneling
  5. Secure small branches in restricted countries that don't allow cloud proxy use with minimal footprint

Connecting to Umbrella DNS



Protect guest Wi-Fi

Using Cisco Wireless LAN Controller or Meraki MR



- Healthcare, Education, Retail and Hospitality
- No need to consume SWG for guest traffic
- DNS security and filtering is more than enough

Protect against DNS-Tunneling

- DNS traffic widely used and trusted.
- DNS tunneling allows malware authors to communicate in a covert channel.
  - Data is encoded into DNS queries and responses
- Used to:
  - Bypass security (firewalls, web proxies)
  - Exfiltrate sensitive data
  - Command & Control instructions
  - Free WiFi

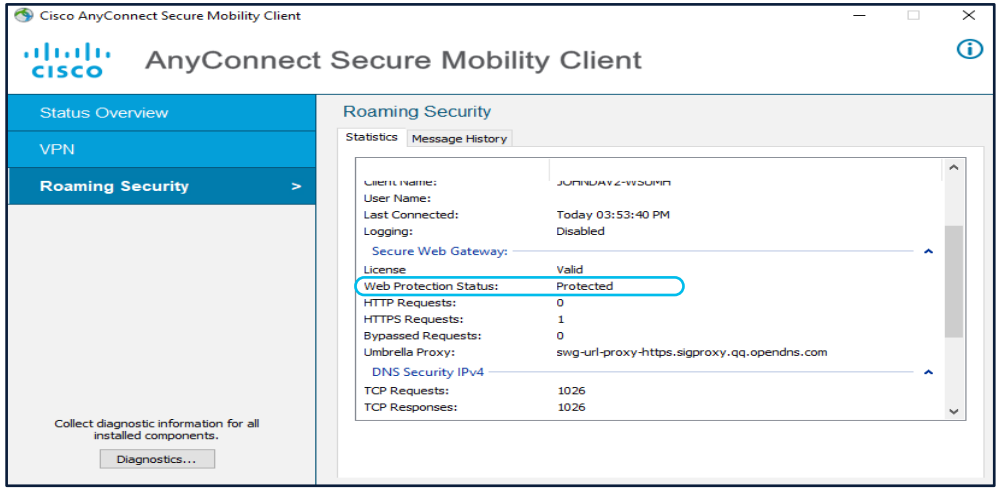
Cisco Secure Client

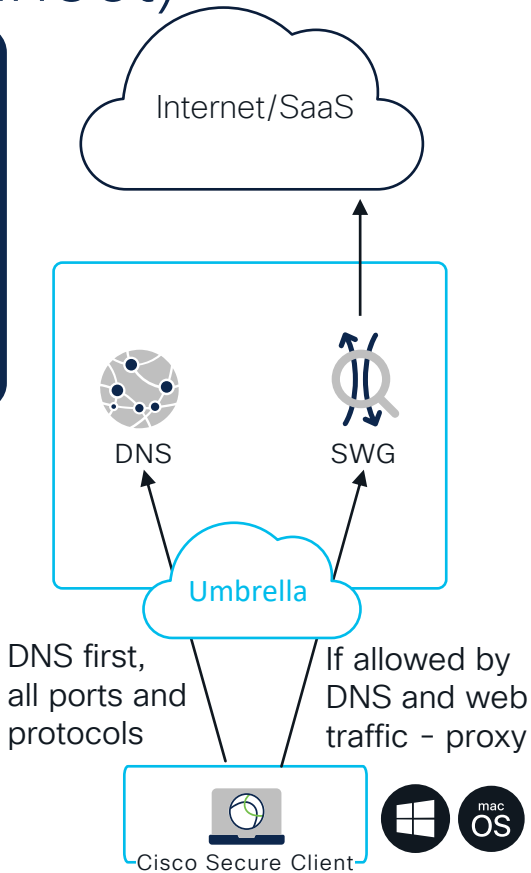
Cisco Secure Client (formerly AnyConnect)

- CSC can be used across an entire enterprise
  - Protect assets on or off network
  - Trusted Network Detection:

    Option to disable DNS and SWG when on-premise (perfect for Hybrid SWG to force using SWA when on-network)

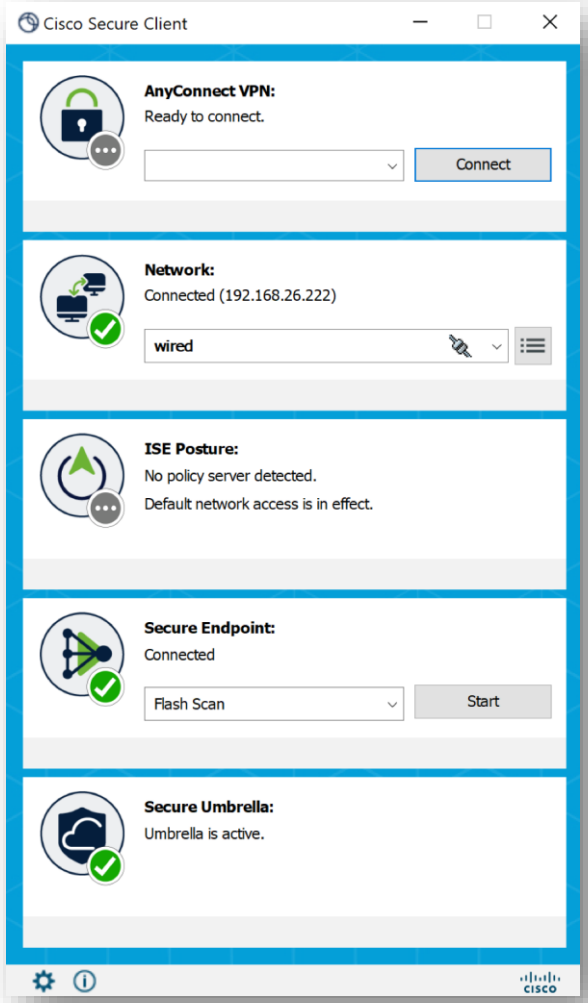
- Both Umbrella DNS and Secure Web Gateway services can co-exist (Win and Mac)
  - DNS only for iOS and Android
- Simple and consistent user attribution
- Choice of fail open or fail closed
- Selective SWG enablement per client





Cisco Secure Client

- AnyConnect VPN (Core)
- Network Access Manager (NAM)
- ISE Posture
- Secure Firewall Posture (No UI)
- Secure Endpoint (EPP/EDR)
- Umbrella (DNS/SWG)
- Cloud Management Module (No UI)
- Network Visibility Module (NVM) (No UI)
- Diagnostics and Reporting Tool (DART)

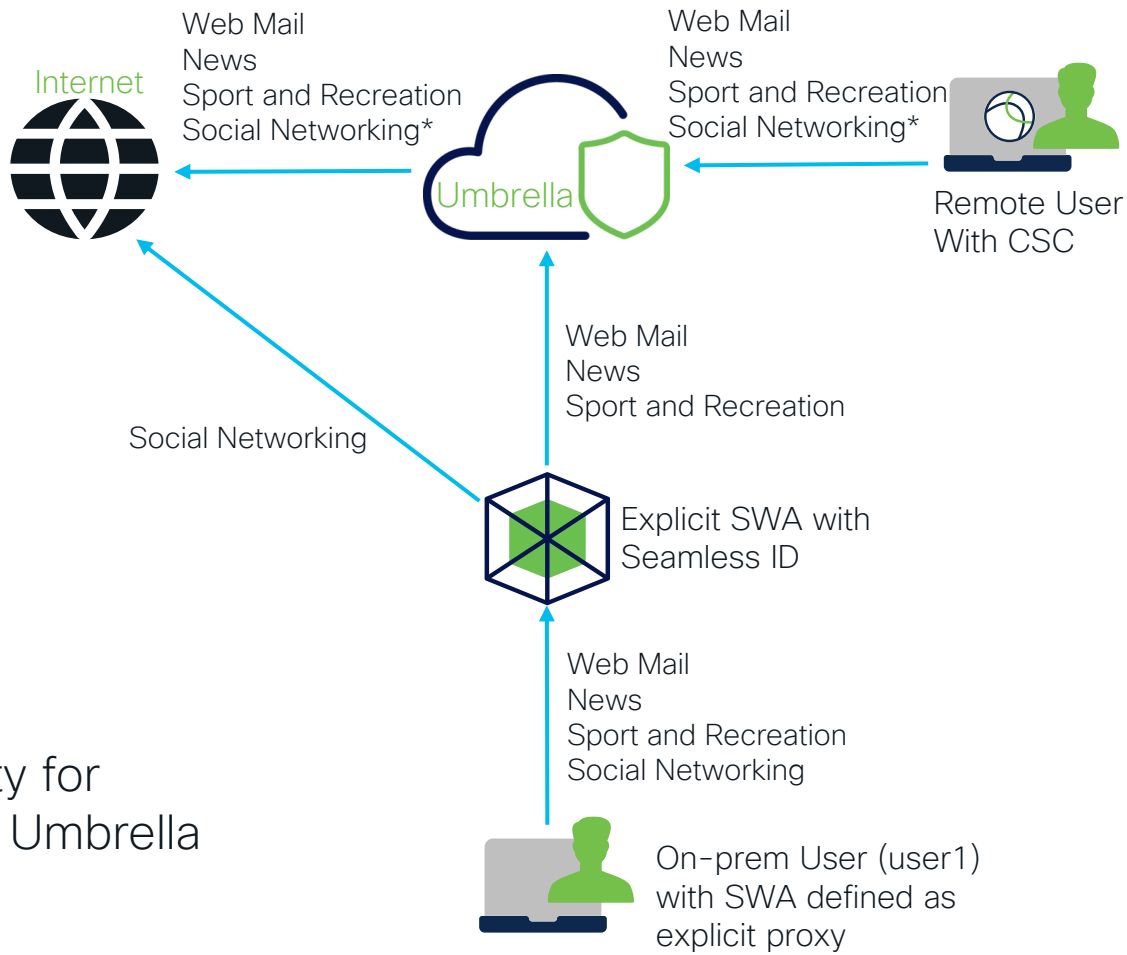


Demo:
Hybrid SWG – Seamless Identity

Demo Scenario

- ✗ Web Mail
- ✗ Sports and Recreation
- ✗ Social Networking
- RBI News

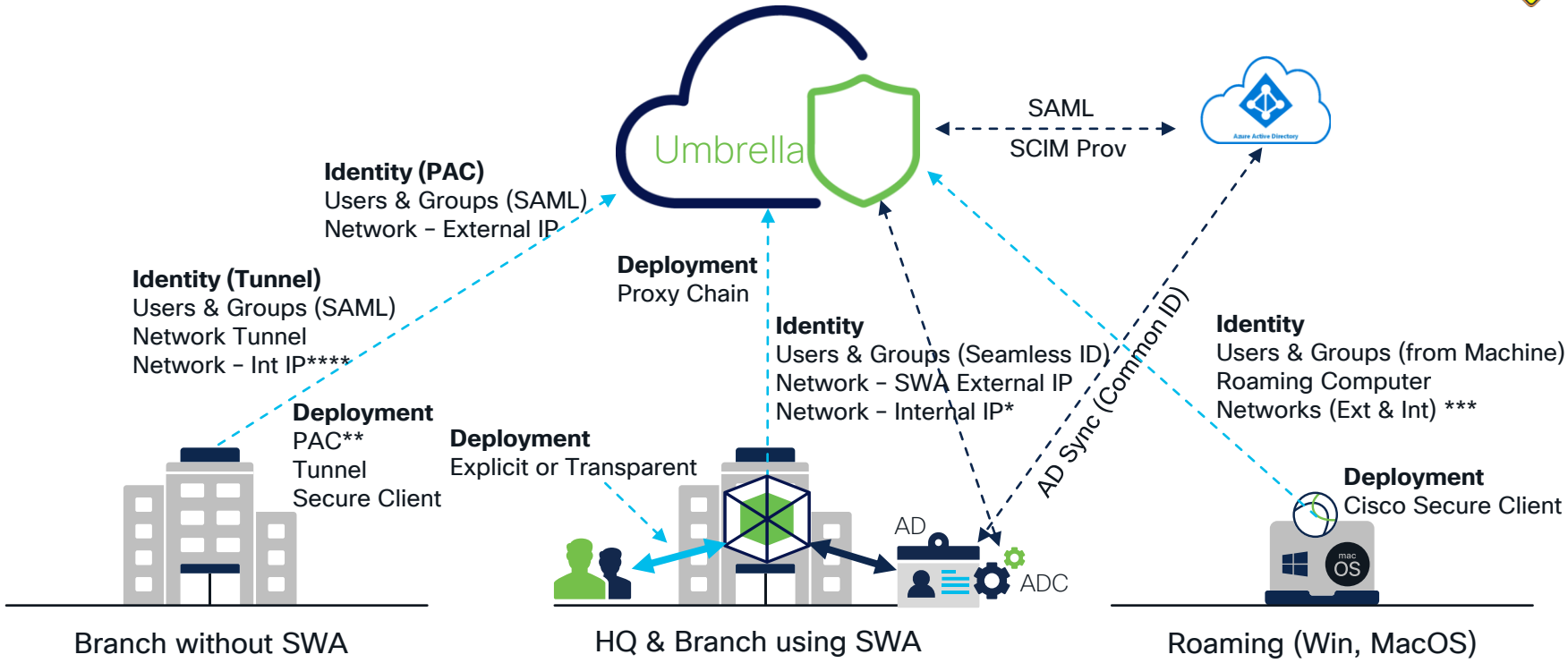
Note: Needs Internal IP visbility for Web Mail and News traffic on Umbrella



*Needs XFF enabled, needs decryption for HTTPs traffic on SWA

Hybrid SWG
Traffic Redirection and Identity Methods

Hybrid SWG Traffic Redirection & Identity Methods



*Needs XFF enabled, needs decryption for HTTPs traffic on SWA
** Cloud PAC or optional customer hosted PAC
*** Needs AD provisioning to map internal IP to Roaming Computer
**** Needs AD provisioning to map internal IP to User

Wrap Up

Wrap Up

- Secure Internet Access (SIA) is a great use case to start your SASE/SSE transition and protect user's internet access everywhere
- Hybrid SWG is a perfect approach to achieve this SASE/SSE start smoothly and provides flexibility, control and tons of capabilities and use cases.
- Seamless ID Sharing allows you to leverage your exiting SWA AD authentication with proxy chaining to Umbrella
- Common Hybrid Policies and reporting let you manage the Hybrid SWG architecture from one console which is Umbrella dashboard

Hybrid SWG Resources

- YouTube Videos:
  - Cisco Umbrella SWG: WSA Proxy Chain (Base Configuration)
  - Cisco Umbrella SWG: WSA Proxy Chain (Internal Network ID Based Policies and IP based Attribution)
  - Cisco Secure Web Appliance Async OS 14.1 – Umbrella Seamless Identity Sharing
- Manage Proxy Chaining in Umbrella: https://docs.umbrella.com/umbrella-user-guide/docs/manage-proxy-chaining
- Configuration guide for the proxy chain between WSA and SWG: https://support.umbrella.com/hc/en-us/articles/360039805572-Configuration-guide-for-the-proxy-chain-between-WSA-and-SWG
- Seamless Identity Sharing: https://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/umbrella-seamless-identity-wsa-async.html
- Seamless ID from SWA User Guide
- Umbrella Identity and SIG Deployments: https://docs.umbrella.com/umbrella-user-guide/docs/identity-and-sig-deployment

Continue your Education

Learn more with SASE Learning Map (check next two slides) breakout sessions when they are available On Demand Library post-event

Check the resources for more details

Please ask your questions in the Webex space

Visit the products page at
www.cisco.com/go/umbrella
www.cisco.com/go/secure-web

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 SOCs 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

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

Feb 10 | 11:00

FINISH

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

Complete your Session Survey

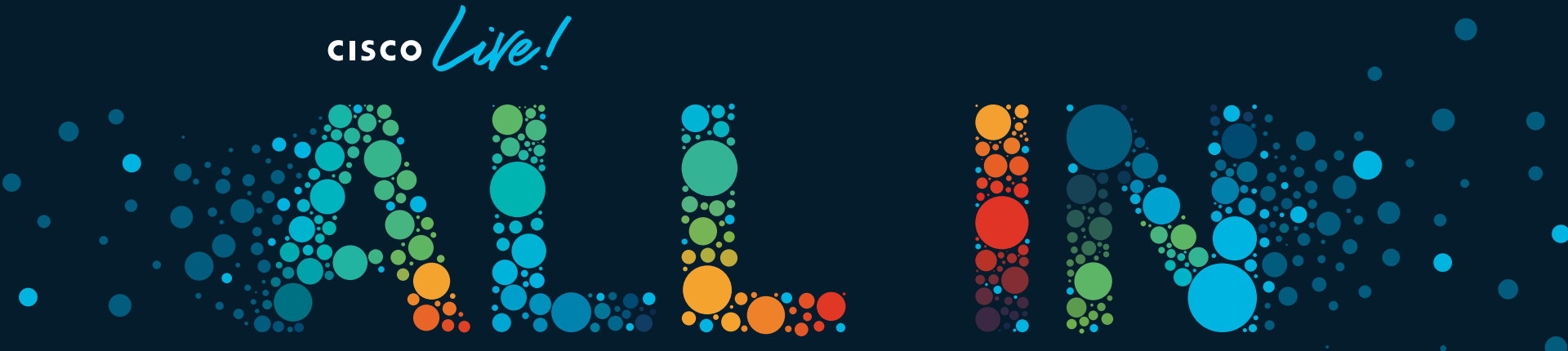
- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- 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

The bridge to possible

Thank you

cisco Live!


CISCO Live!
ALL IN