



You make **possible**



Designing security for the future of your network with Cisco Umbrella

James Brown, Product Strategy, Cisco Cloud Security
Meg Diaz, Product Marketing, Cisco Cloud Security

PSOSEC-4902

CISCO *Live!*

Barcelona | January 27-31, 2020



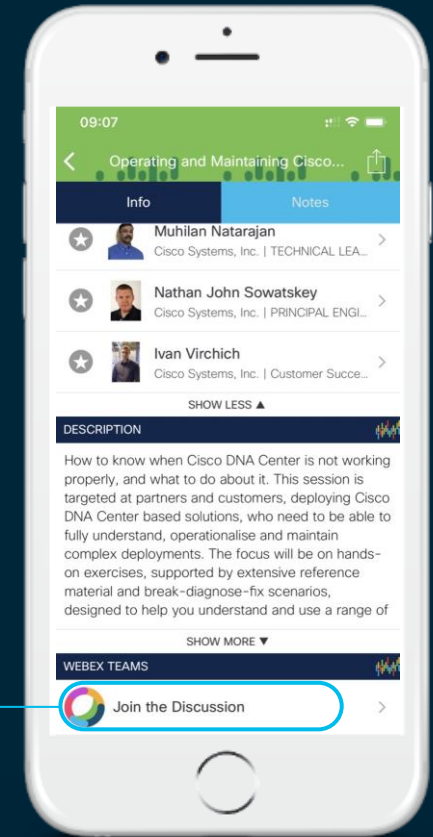
Cisco Webex Teams

Questions?

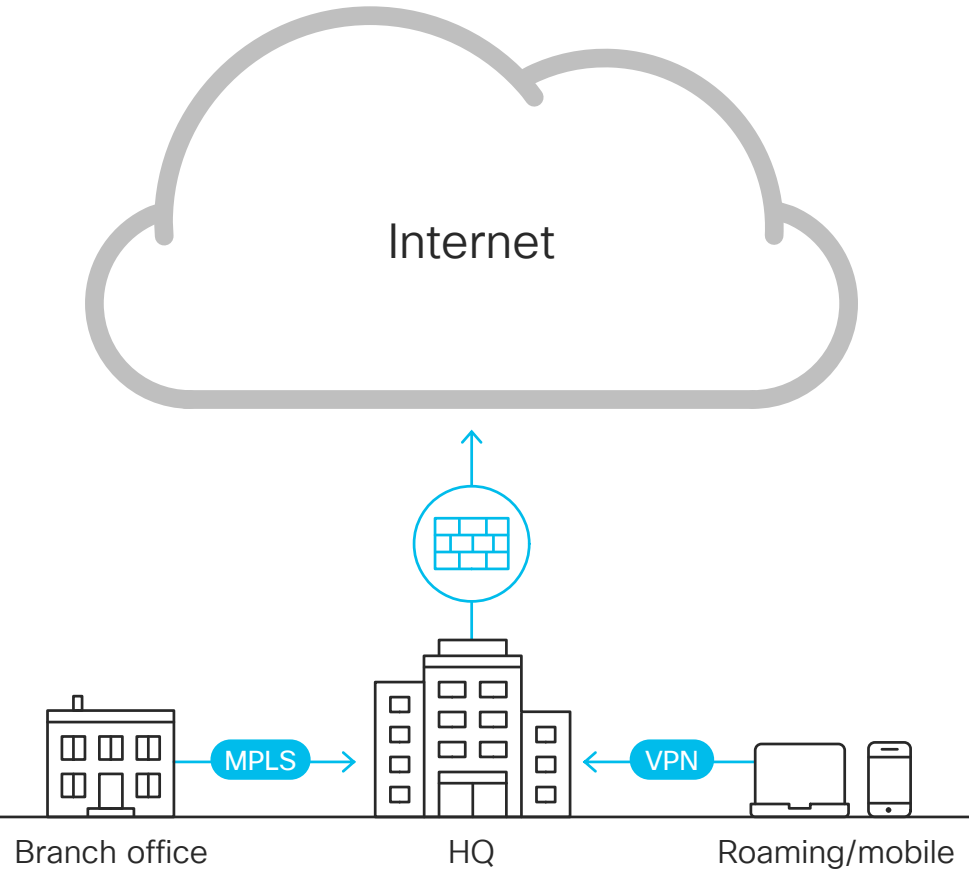
Use Cisco Webex Teams to chat with the speaker after the session

How

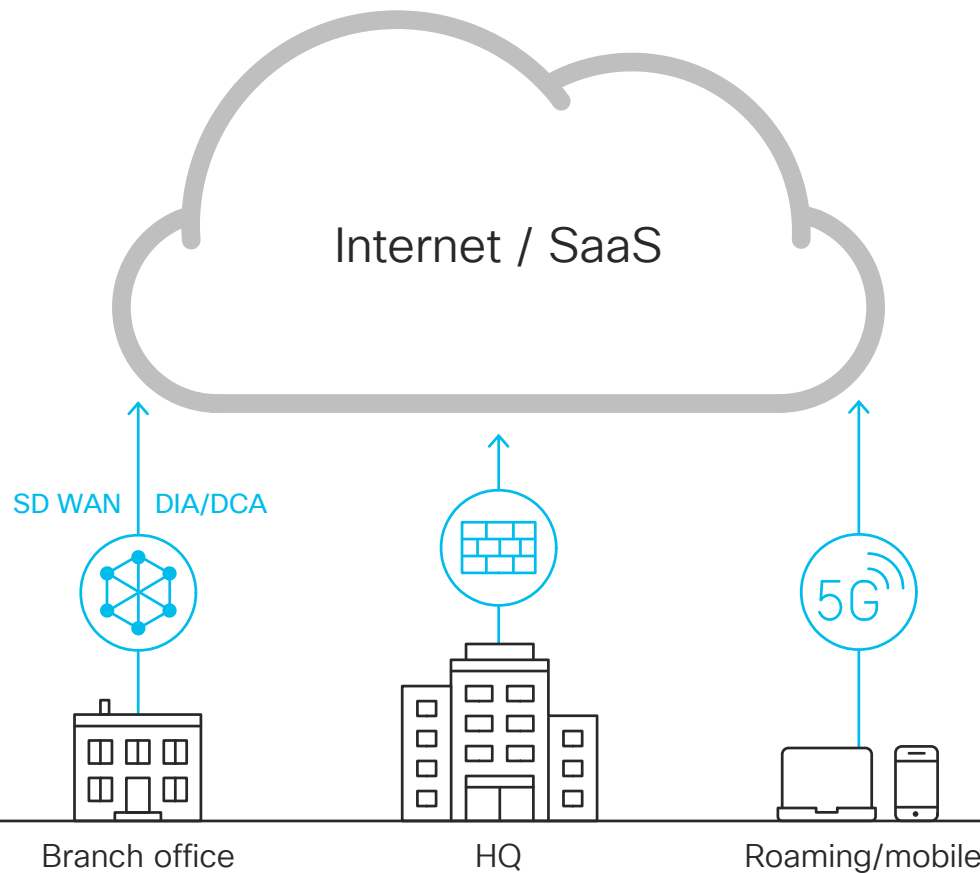
- 1 Find this session in the Cisco Events Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space



It was a simpler time...



The new model



Over the next hour, we'll explore...

- 1 Trends and resulting challenges
- 2 A new approach to securing your users
- 3 A demo of scenarios where Cisco Umbrella helps most

ESG market research



Access the report:
cs.co/ESG-SIG-research

- Surveyed 450 respondents
- North America & Western Europe
\$50M in annual revenue
- 500+ employees
- Cybersecurity, IT, and networking
security professionals

Poll

- A All applications are now SaaS
- B Majority of applications are moving to SaaS
- C Zero SaaS applications in use

Explosion of cloud apps



of applications are SaaS-based

Users install
own apps

Shadow IT

Expose
sensitive data

Roaming users



of employees considered
roaming users

While 82% mandate
use of VPNs...

8 out of 10

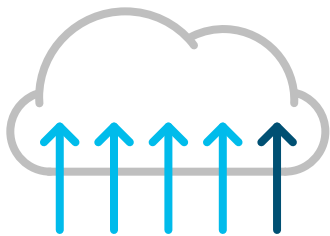
sometimes or frequently
avoid VPN use

Poll

- A Currently have direct internet access model at some sites
- B Plan to move to direct internet access in next 12 months
- C No plans to move to direct internet access

Poll

- A Using SD-WAN extensively or in some locations
- B Plan to deploy SD-WAN in next 12 months
- C No plans to deploy SD-WAN



4 out of 5

orgs are shifting to
direct internet access (DIA)



76%

of orgs use SD-WAN
extensively or selectively

DIA & SD-WAN pervasive in branch offices

Source: ESG Research Survey, Cisco Secure Internet Gateway Survey, January 2019



of branch office security deployments
take over a month

Branch offices are vulnerable to threats



of **remote offices and roaming users** found to
be **source of compromise** in recent attacks

Source: ESG Research Survey, Cisco Secure Internet Gateway Survey, January 2019

Biggest security challenges

Difficult to manage security with branch offices connecting to internal apps, cloud-based workloads, and SaaS apps


34%

Lack of visibility into branch office/roaming user activity for security monitoring

33%

Requires strong collaboration between security and network operations teams, which is challenging for my organization

31%



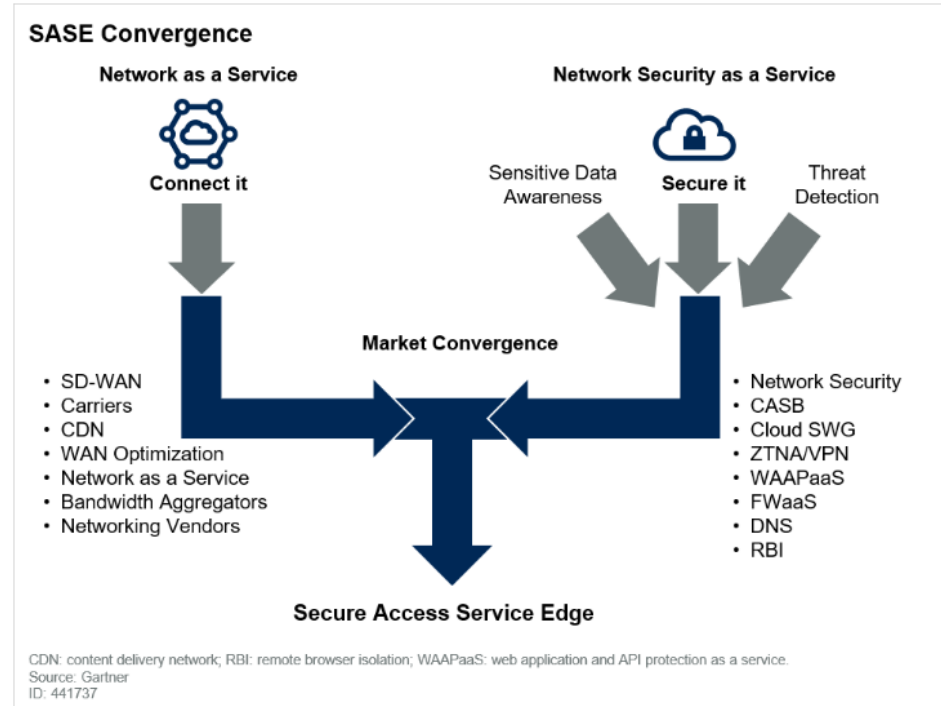
76% prefer a
multi-function
security platform
to solve the
remote security
challenge

Gartner's view on convergence

Secure Access Service Edge

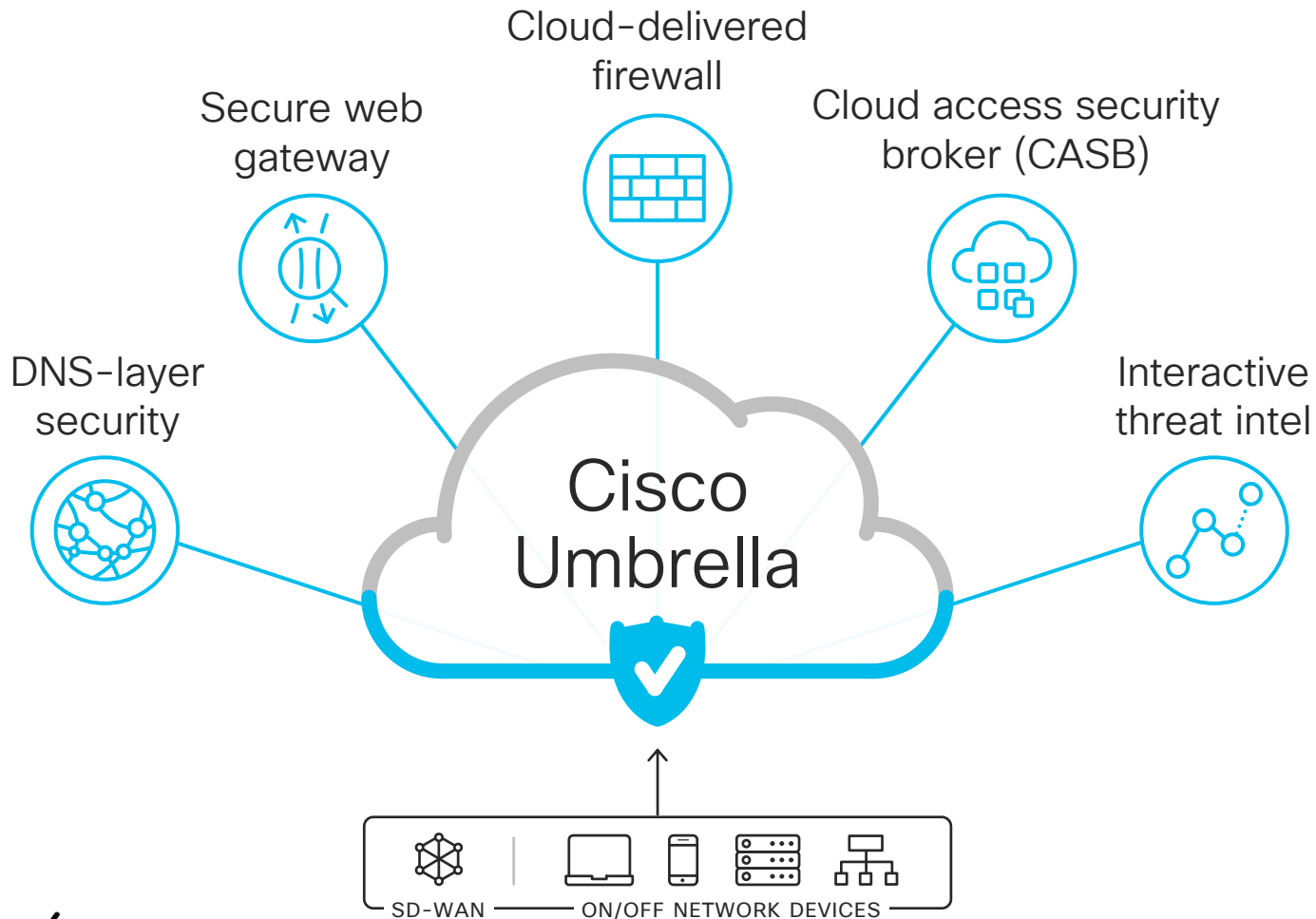
SASE capabilities delivered as a service based upon:

- Identity of the entity
- Real-time context
- Security and compliance policies
- Continuous assessment of risk/trust throughout the sessions



Source: Gartner, The Future of Network Security Is in the Cloud, Figure 1, August 2019

A new approach with Cisco Umbrella



DNS-layer security

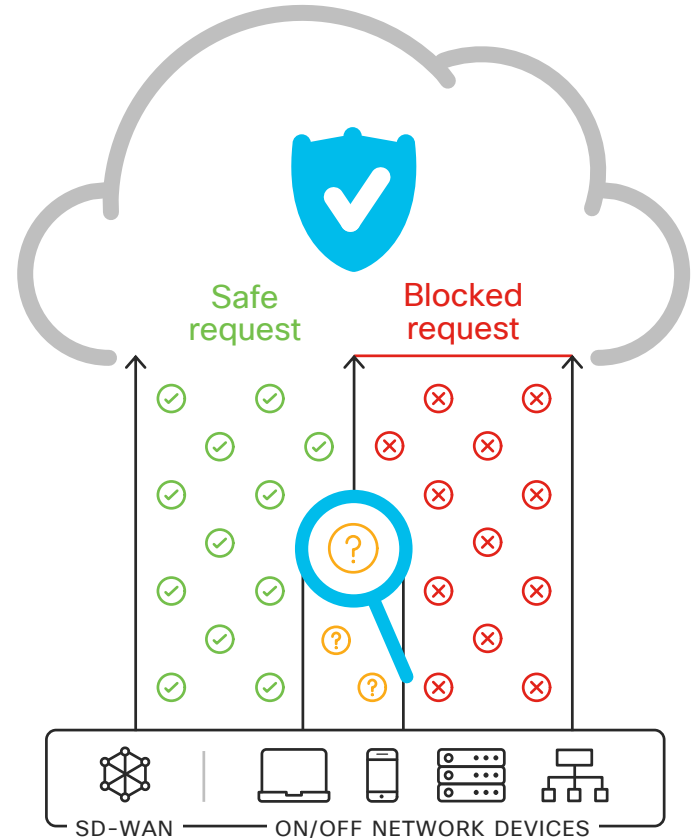
First line of defense

Deploy enterprise wide in minutes

Block domains associated with malware, phishing, command and control callbacks anywhere

Stop threats at the earliest point and contain malware if already inside

Amazing user experience – faster internet access; only proxy risky domains



DNS Tunneling

To attacker



From attacker



Bidirectional



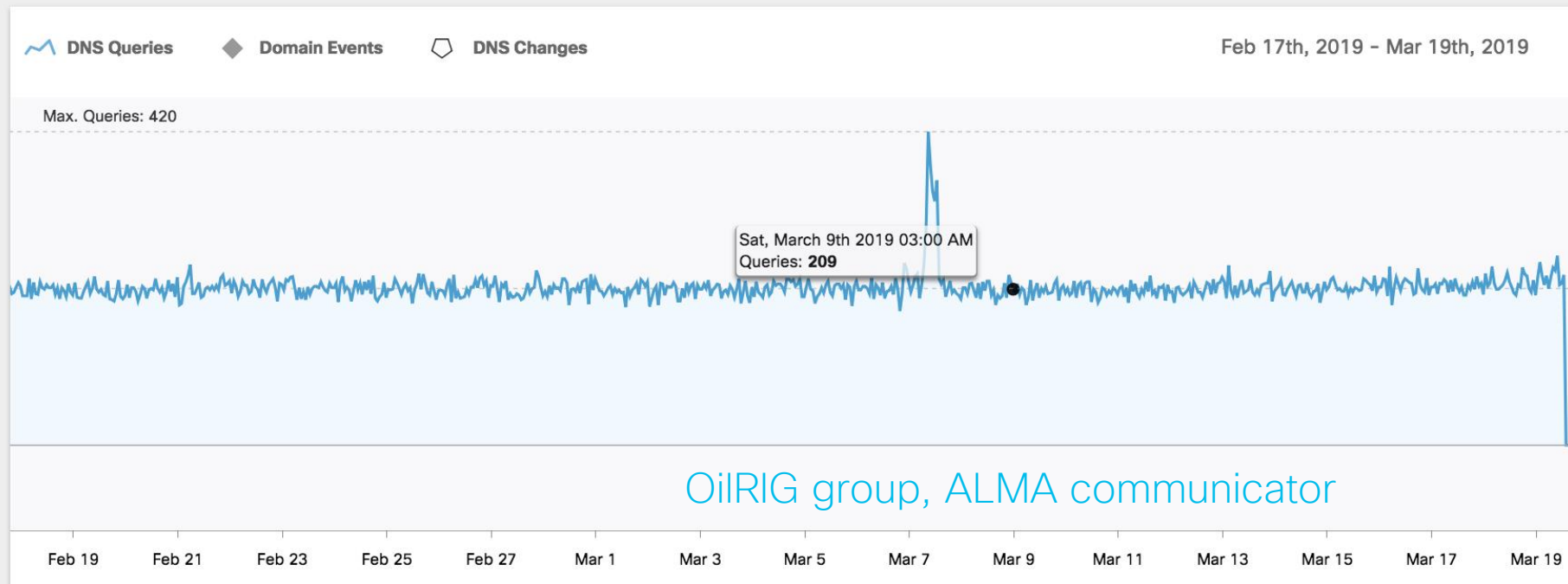
Attacker controls an authoritative name server

Details for prosalar.com

This domain is currently in the Umbrella block list

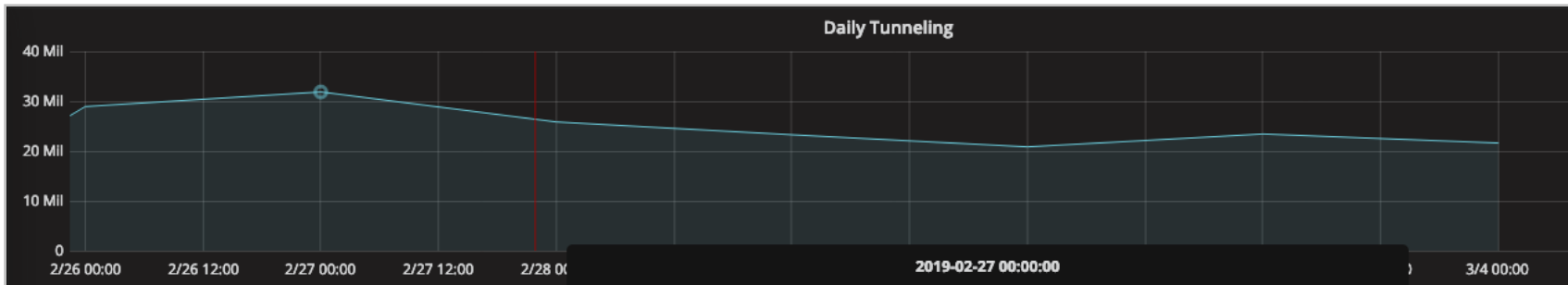
Umbrella Investigate Risk Score: 53 ?

Timeline (Beta)



DNS Tunneling stats

Less than 1% of global traffic



NULL_QTYPE_TUNNELING

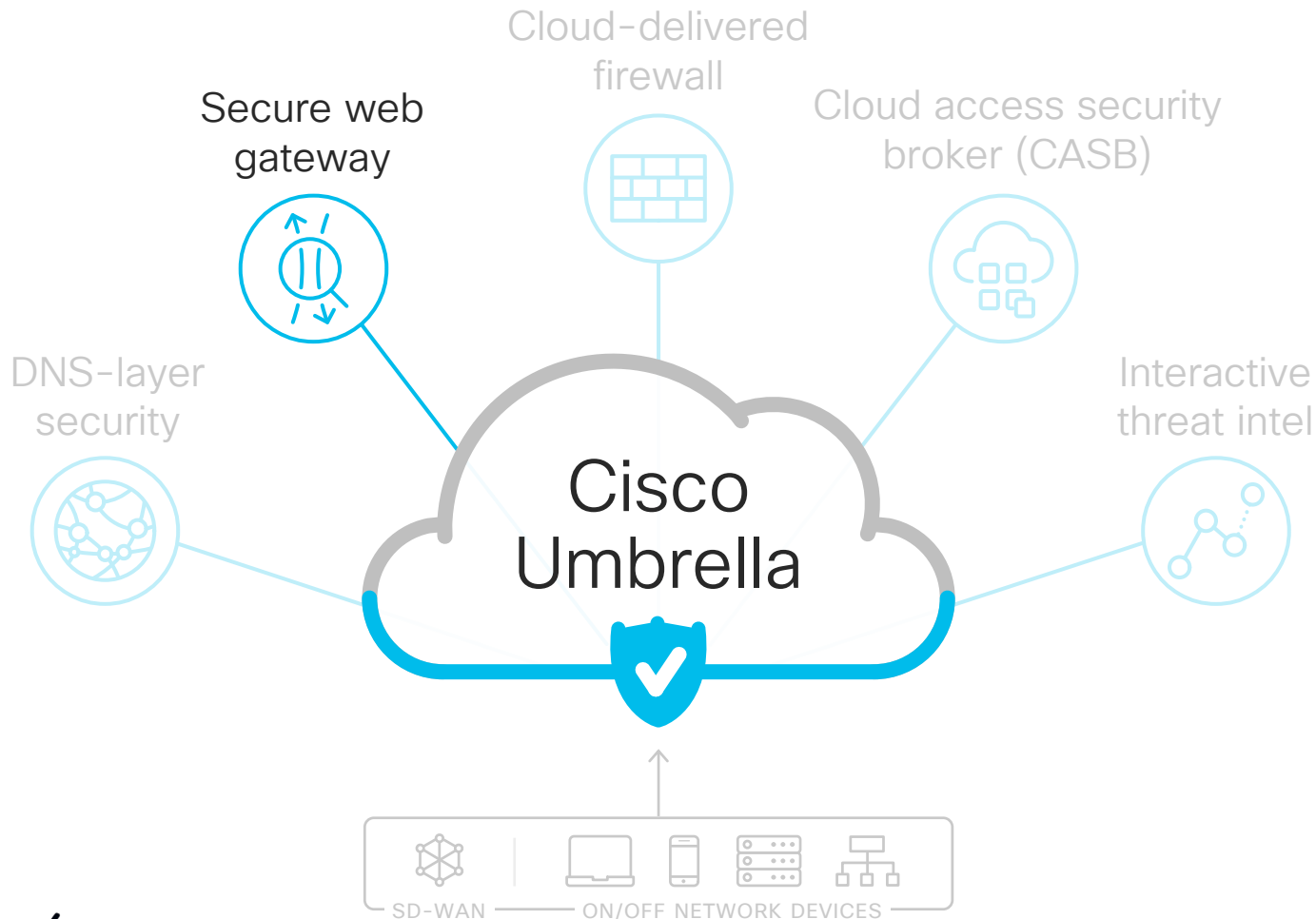
1198 nsquery.net
1198 jessicajoshua.com
1198 facebook-cdn.net
1197 phillippcliche.com
1193 thomaswaechter.com
1170 charlotteagnes.com
1168 poppyranken.com
1167 gl-appspot.org
1165 lotteagnesar.com
1153 tonholding.com
1150 teriava.com
875 tulationeva.com
486 5t2.be
406 notificeva.com
380 vieweva.com
41 getbring.de
35 shervin.org
31 89u.uk

TXT_QTYPE_NS_LABEL

1000 yomiuri.us
1000 voanews.hk
1000 nowpublic.us
1000 microsofurl.com
1000 microsoftner.com
1000 micorsoff.com
995 micrrsoft.net
733 flashplayerget.com
520 facebookcdn.com
319 microselver.com

100 UK orgs surveyed in 2017
21% impacted by data exfil
via DNS tunneling*

*https://www.infosecurityeurope.com/_novadocuments/445880?v=636554279131430000



Secure web gateway: full web proxy

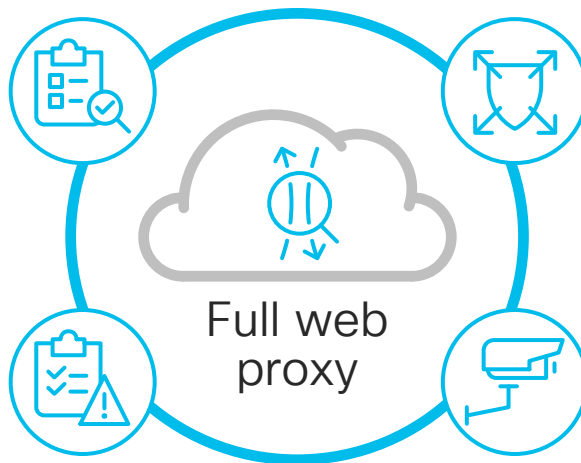
Deep inspection and control of web traffic

Gain additional visibility

via full URL logging and
cloud app discovery

Enforce acceptable use policy

via app controls,
content filtering, and URL
block/allow lists



Extend protection against malware

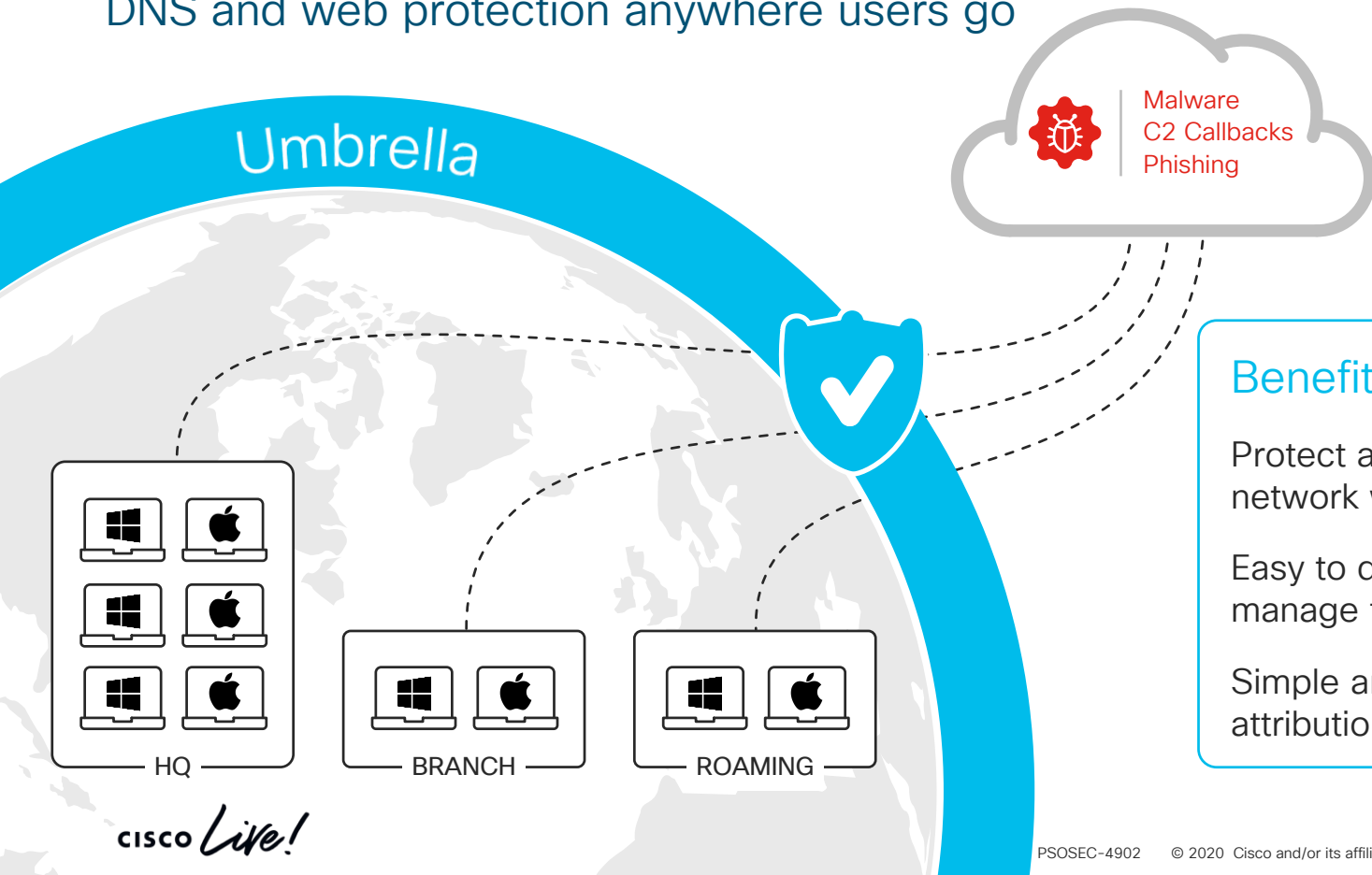
via SSL decryption
and file inspection

Enrich file inspection (with retrospective alerts)

via Cisco Advanced Malware
Protection (AMP) and Cisco
Threat Grid sandboxing

AnyConnect integration with Umbrella

DNS and web protection anywhere users go

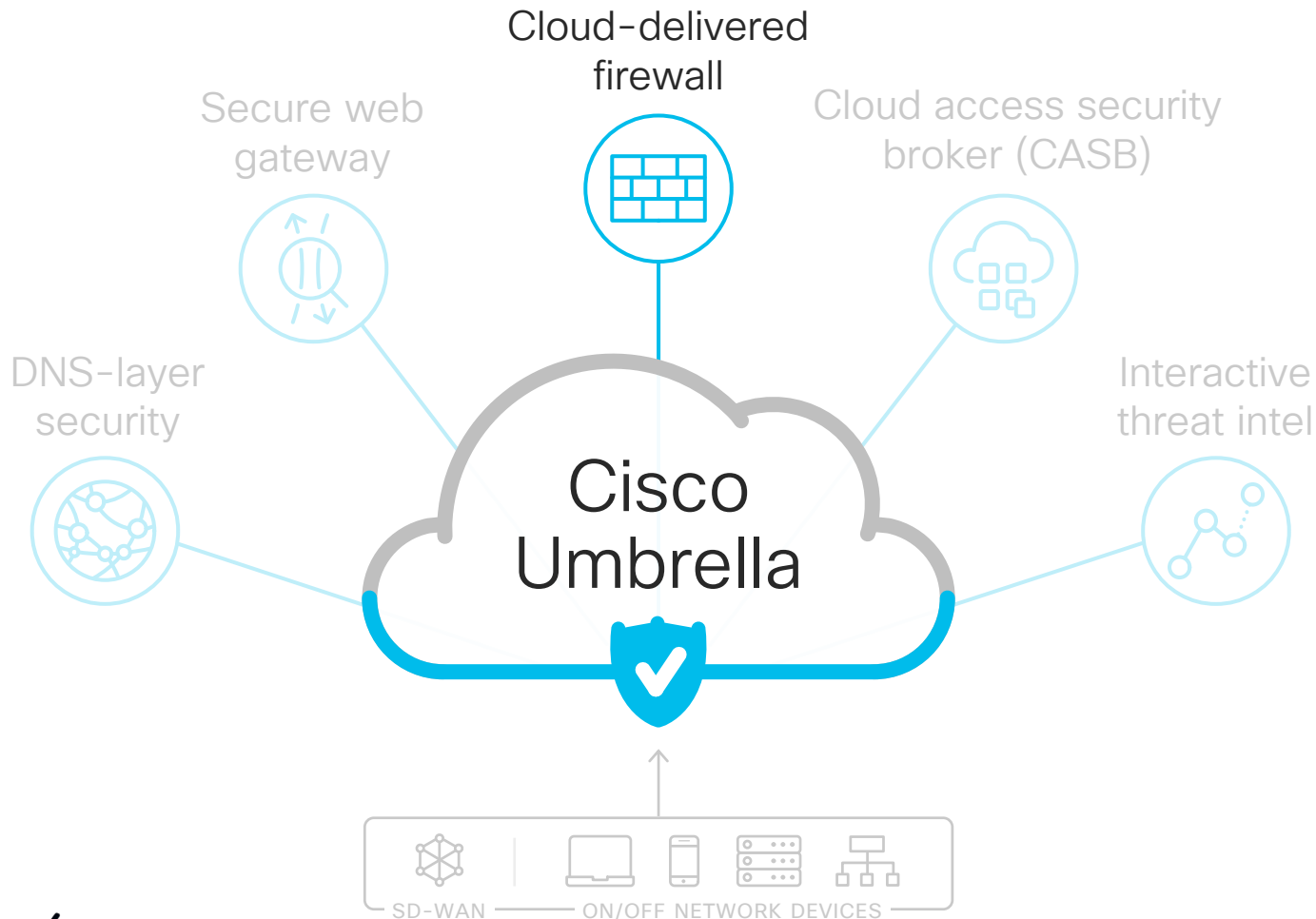


Benefits

Protect assets on and off network with consistent policies

Easy to deploy, simple to manage for AnyConnect users

Simple and consistent user attribution



Cloud-delivered firewall

Firewall for the cloud edge

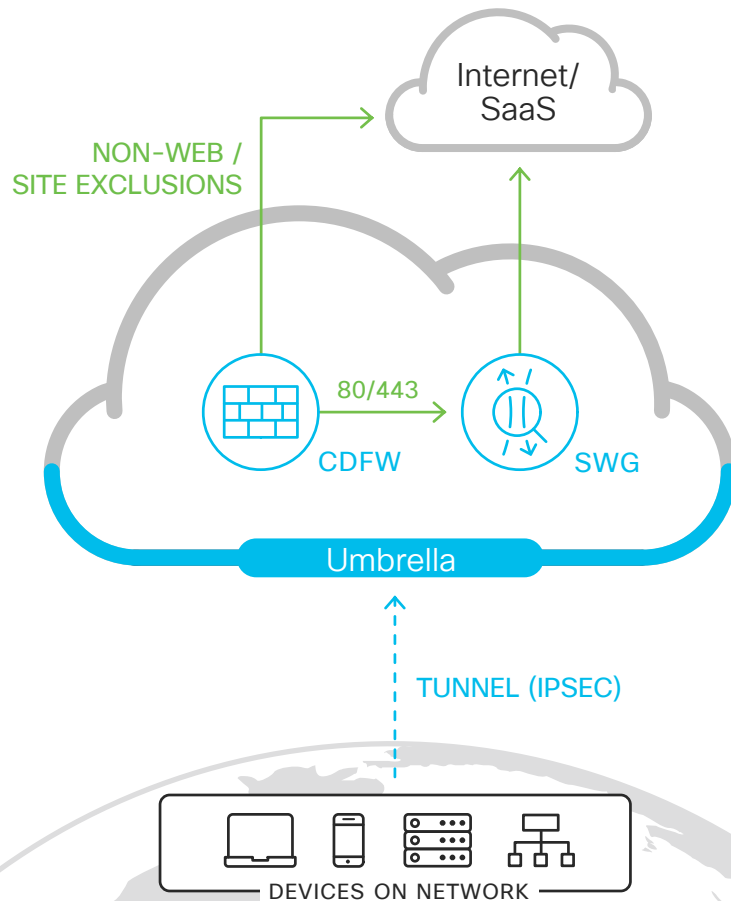
Tunnel all outbound traffic to Umbrella

Block high risk, non-web applications

Centrally manage IP, port, and protocol rules (L3/L4)

IPsec tunnel termination

Use cases: Protect guest WiFi and dev environments, provide IP obfuscation



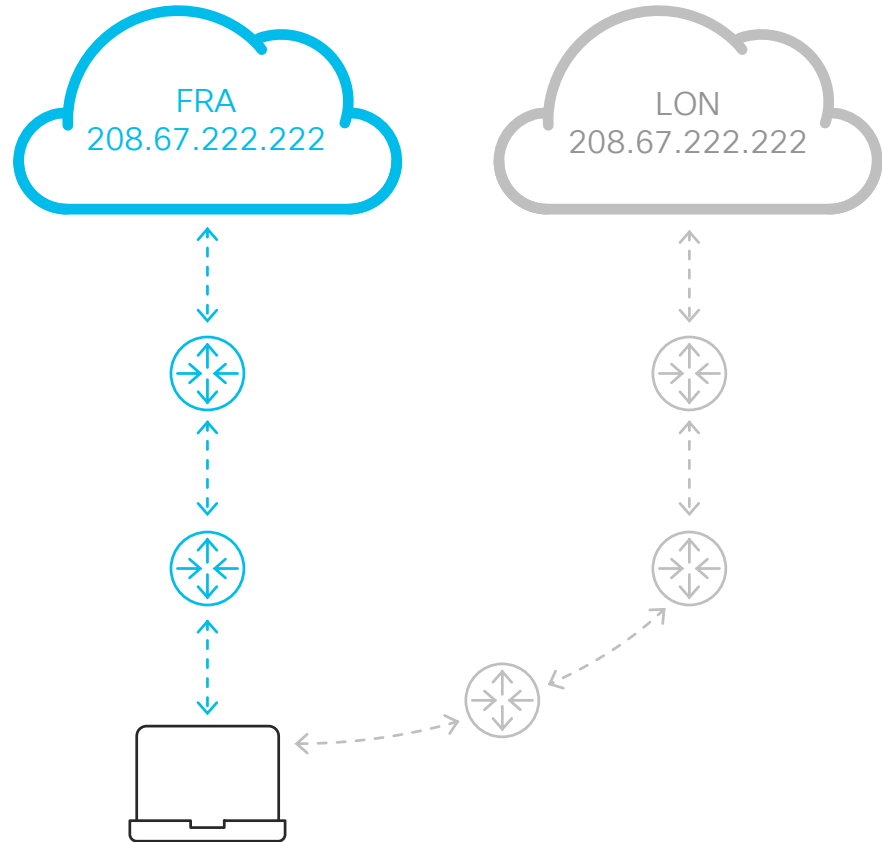
DNS-layer security

Anycast IP routing for reliability

All data centers announce same IP address

Customer points DNS traffic to our IP address

Requests transparently sent to fastest available with automated failover

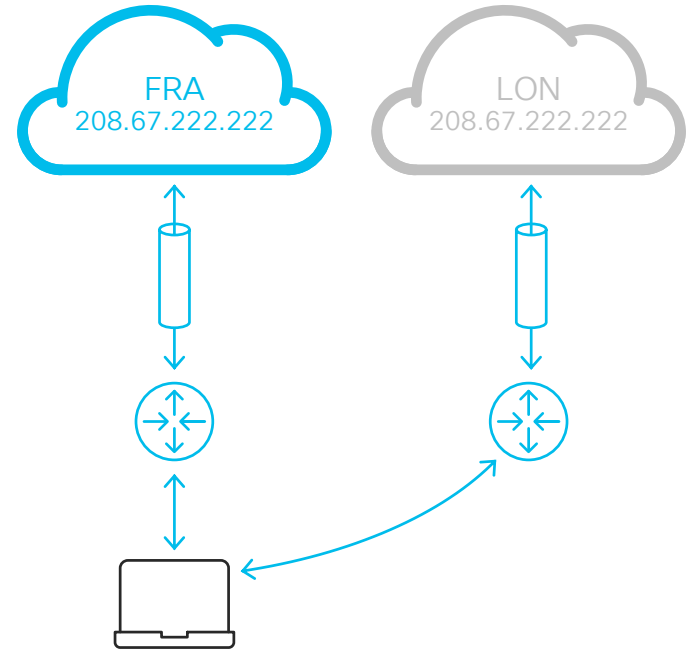


Leveraging Anycast for IPSec tunnel reliability and resilience

Customers choose data center to handle requests

Customers do not have to build a backup IPSec tunnel

If data center fails, customers' IPSec tunnel automatically moves with minimal downtime



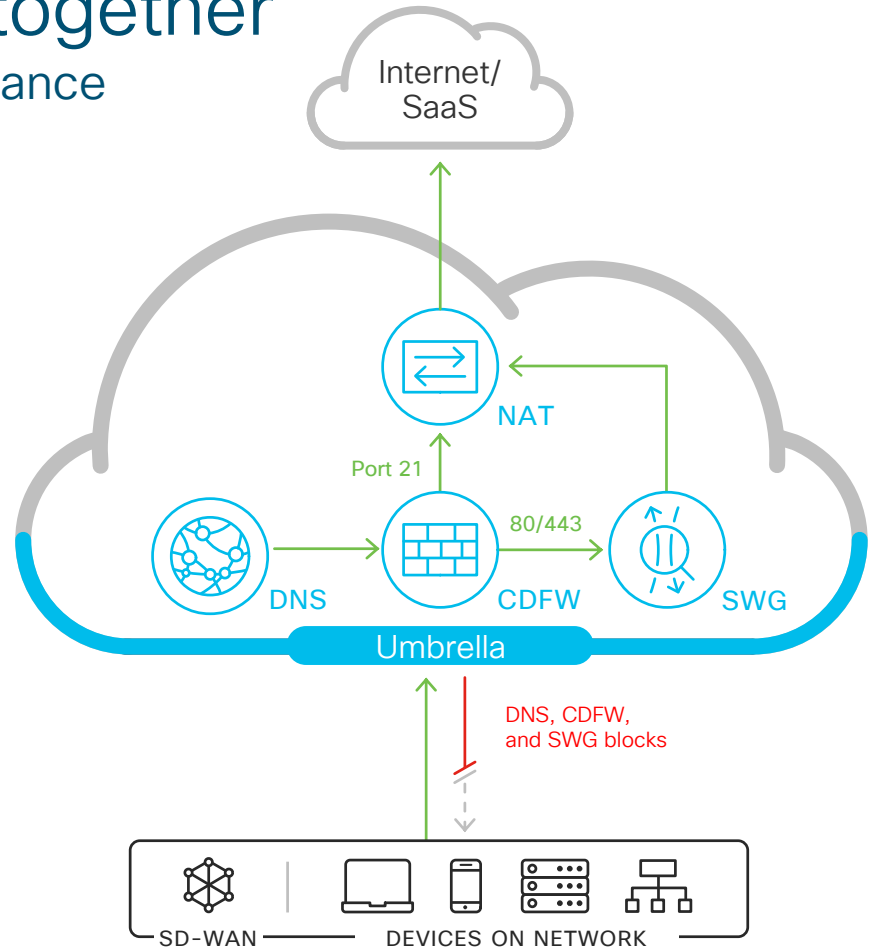
Enforcement that works together

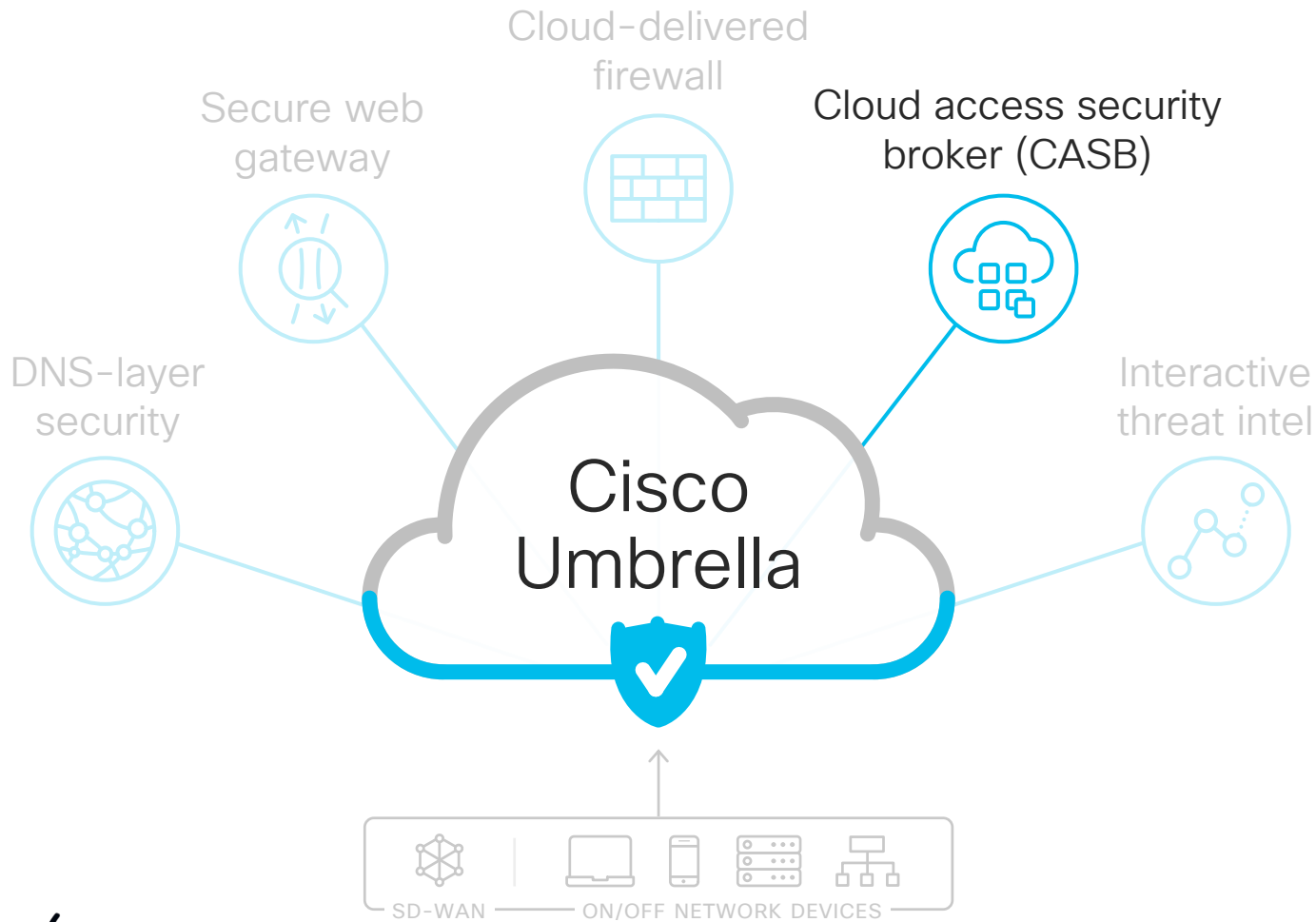
Improved responsiveness and performance

DNS-layer security: First check for domains associated with malware

Cloud-delivered firewall (CDFW): Next check for IP, port, and protocol rules

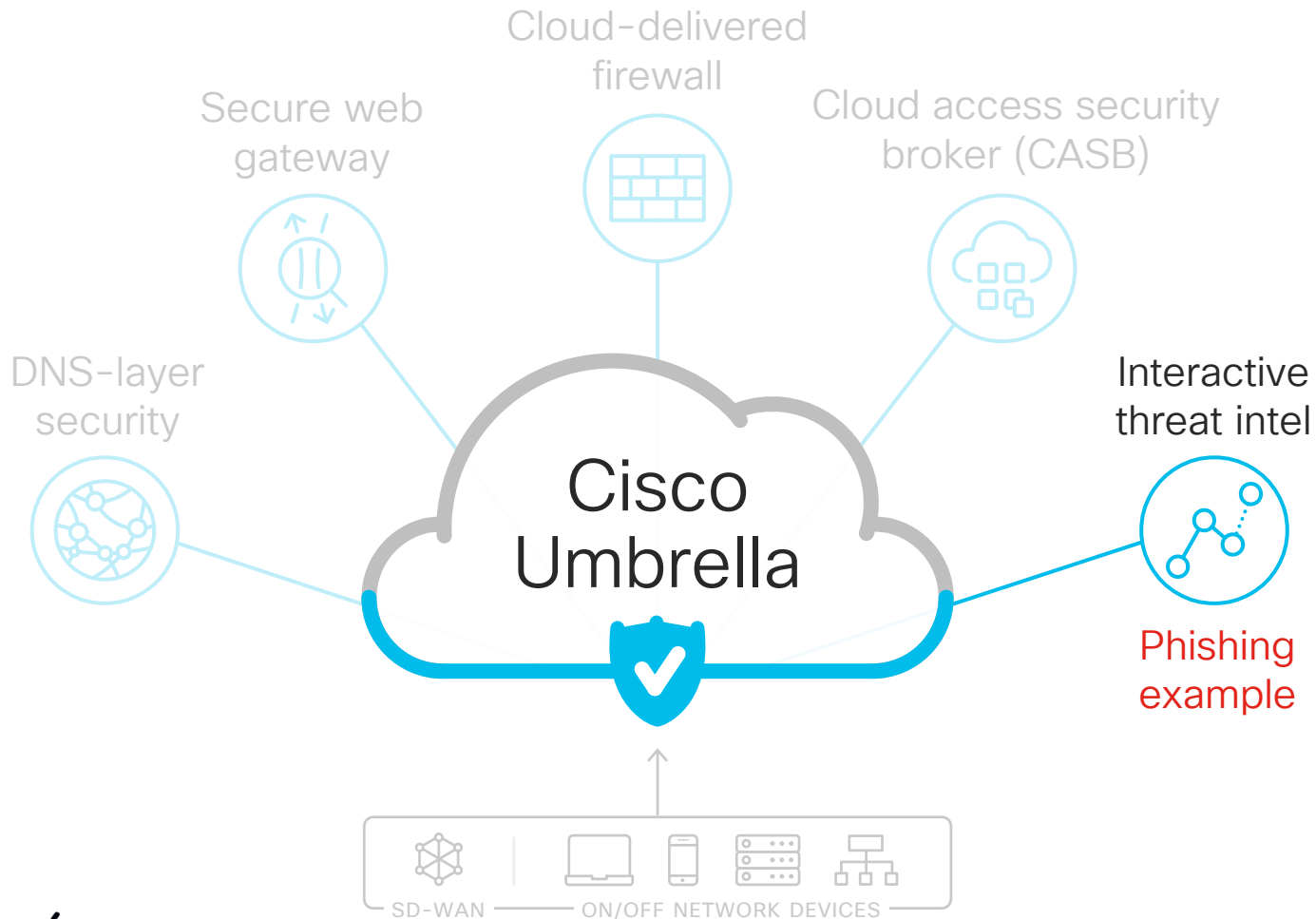
Secure web gateway (SWG): Final check of all web traffic for malware and policy violations





Shadow IT visibility and blocking





Details for paypal.co.uk.9u7t.icu

This domain is currently in the Umbrella block list.

Umbrella Investigate Risk Score: 100 ⓘ

This domain might be a fast flux.

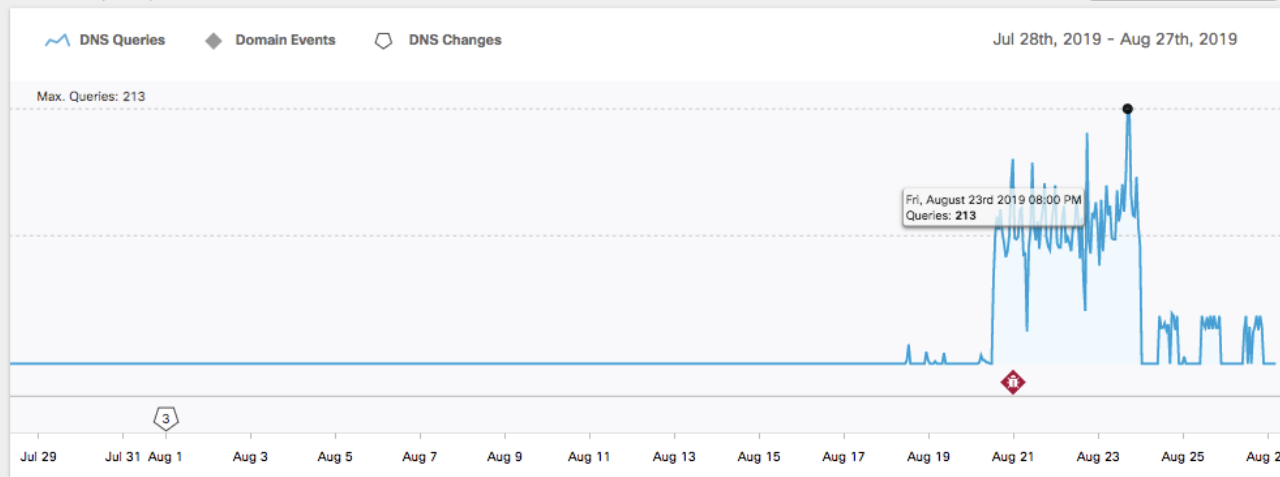
This domain has a suspicious prefix score.

This domain has a suspicious prefix score.

This domain may have been created using a domain generation algorithm (DGA).

Timeline (Beta)

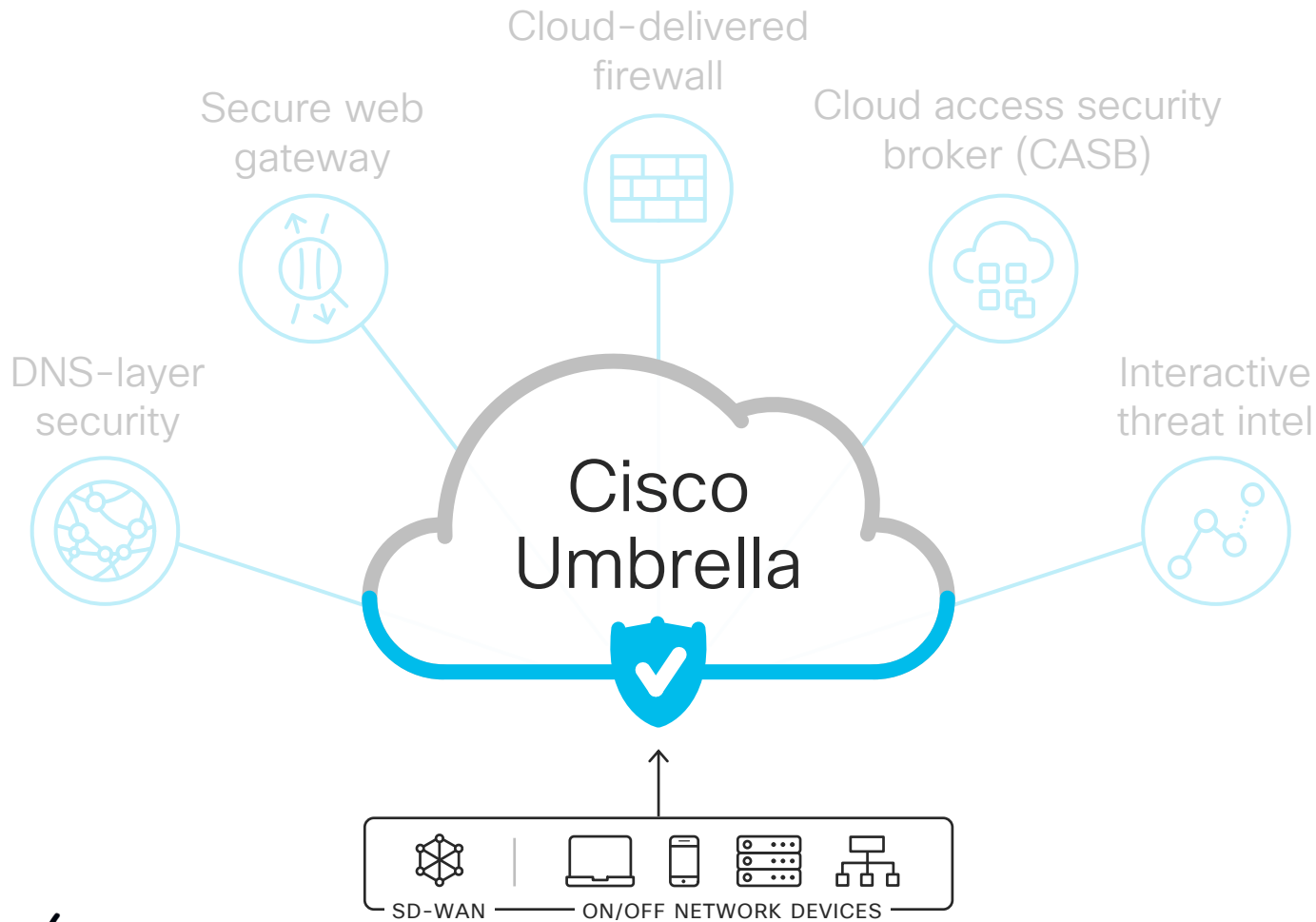
Current Content Category: None



DNS Resolution (Beta)

ADDRESSES					NAME SERVER (NS)	DNS (OTHERS)
IP Malicious: 1 IP Total: 16 TTL(s): 600						
IP	Security Category	TTL (seconds) ▼	First Seen ▼	Last Seen ▼		
176.105.252.88	Malware	600	August 20, 2019	August 20, 2019		
<u>193.124.117.45</u>	Malware	600	August 20, 2019	August 20, 2019		
195.133.147.138	Malware	600	August 19, 2019	August 20, 2019		
212.109.218.122	Malware	600	August 20, 2019	August 20, 2019		
185.193.141.185	Malware	600	August 20, 2019	August 20, 2019		
1 - 5 < >						

Paypal UK phish hosted on a bulletproof
hosting infrastructure we've been tracking



Tested/integrated Cisco deployment options

DNS, SWG, & CDFW



AnyConnect



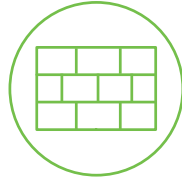
ISR



CSR



SD-WAN
(Viptela)



ASA

DNS only



WLAN
controller



Meraki
MX



Security
Connector for iOS

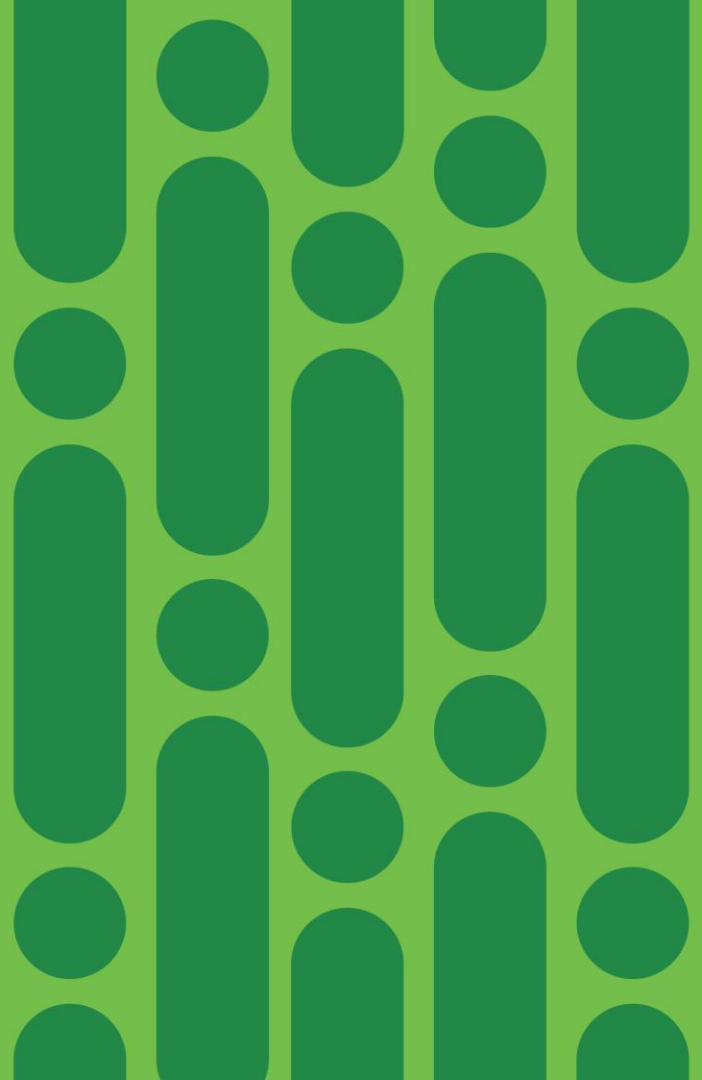


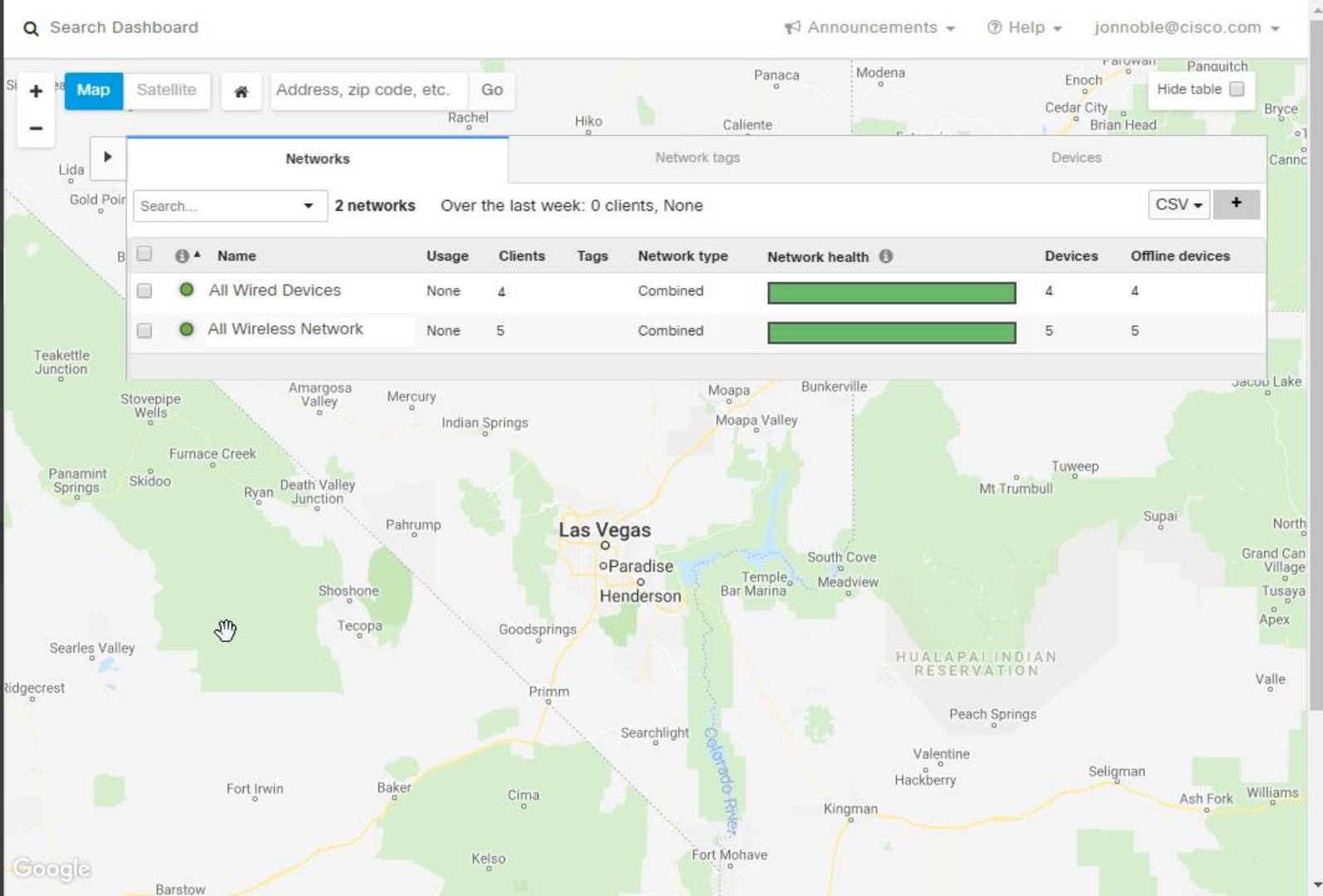
Mobility
Express



Meraki
MR

Let's look at how
this works together





Firewall & traffic shaping

SSID: Guest Connect ▾

Block IPs and ports

Layer 2 LAN isolation Disabled ▾ (bridge mode only)

Layer 3 firewall rules ⓘ

#	Policy	Protocol	Destination	Port	Comment	Actions
	Deny ▾	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

[Add a layer 3 firewall rule](#)

Block applications and content categories

Layer 7 firewall rules

There are no rules defined for this SSID.

[Add a layer 7 firewall rule](#)

DNS layer protection
(Cisco Umbrella)

To enable DNS layer protection using Cisco Umbrella, you'll need to link a Cisco Umbrella account.

Route DNS requests
through Cisco Umbrella
DNS and deny DNS
requests by linking
Umbrella policies.

[Link Umbrella policies](#)

Firewall & traffic shaping

SSID: Guest Connect ▾

Block IPs and ports

Layer 2 LAN isolation Disabled ▾ (bridge mode only)

Layer 3 firewall rules ⓘ

#	Policy	Protocol	Destination	Port	Comment	Actions
	Deny ▾	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

[Add a layer 3 firewall rule](#)

Block applications and content categories

Layer 7 firewall rules

There are no rules defined for this SSID.

[Add a layer 7 firewall rule](#)

DNS layer protection
(Cisco Umbrella)

Select an Umbrella policy to apply.

Route DNS requests
through Cisco Umbrella
DNS and deny DNS
requests by linking
Umbrella policies.

Default Policy (indirectly applied) ▾

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

ex:
meraki.com

You have unsaved changes.

Save or cancel

Firewall & traffic shaping

SSID: Guest Connect ▼

ORGANIZATION

All Wireless Network ▼

NETWORK

Guest Wireless Protect ▼

Network-wide

Security & SD-WAN

Wireless

Organization

Block IPs and ports

Layer 2 LAN isolation Disabled ▼ (bridge mode only)

Layer 3 firewall rules ⓘ

#	Policy	Protocol	Destination	Port	Comment	Actions
	Deny ▼	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

[Add a layer 3 firewall rule](#)

Block applications and content categories

Layer 7 firewall rules

There are no rules defined for this SSID.

[Add a layer 7 firewall rule](#)

DNS layer protection
(Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Select an Umbrella policy to apply.

Security Only - Guest Networks ▼

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

ex:
meraki.com
meraki.net
....

This configuration is linked to a Cisco Umbrella account.

You have unsaved changes.

Save or cancel

Firewall & traffic shaping

Changes saved. ✕

SSID: Guest Connect ▾

Block IPs and ports

Layer 2 LAN isolation

Disabled ▾ (bridge mode only)

Layer 3 firewall rules ⓘ

#	Policy	Protocol	Destination	Port	Comment	Actions
	Deny ▾	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

[Add a layer 3 firewall rule](#)

Block applications and content categories

Layer 7 firewall rules

There are no rules defined for this SSID.

[Add a layer 7 firewall rule](#)

DNS layer protection
(Cisco Umbrella)

Select an Umbrella policy to apply.

Security Only - Guest Networks ▾

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

ex:
meraki.com
meraki.net
...

Overview

Deployments

Core Identities

Networks

Network Devices

Roaming Computers

Mobile Devices

Chromebook Users

Network Tunnels

User Provisioning

Configuration

Internal Domains

Sites and Active Directory

Internal Networks

Service Account Exceptions

Root Certificate

SAML Configuration

SAML Users Groups Delete

Policies

Reporting

Admin

Active Networks
20% 1 / 5 Active

Active Roaming Clients
100% 2 / 2 Active

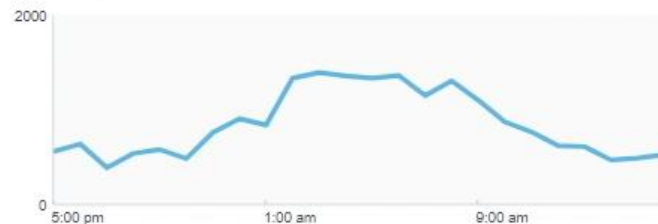
Active Virtual Appliances
100% 2 / 2 Active

Active Network Tunnels
14% 1 / 7 Active

Network Request Breakdown

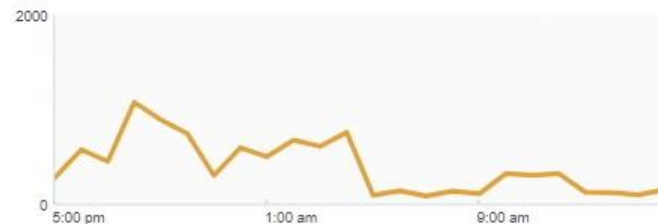
Total DNS Requests

20.8K Total, ▲ 1%

[VIEW ACTIVITY](#)

Total Proxy Requests

9633 Total, ▲ 749%

[VIEW ACTIVITY](#)

Total Blocks

7615 Total, ▲ 504%

[VIEW ACTIVITY](#)

Security Blocks

1115 Total, ▲ 6%

[VIEW ACTIVITY](#)



A Network Device is a physical piece of hardware that forwards DNS requests from client computers to Cisco Umbrella. After registering the device with Cisco Umbrella, the device becomes an identity you can manage and set policies for, with no need for any client device configuration at all. Device integration is done by providing authentication (either by entering your Cisco Umbrella username and password directly on your device or entering an API token), and having a serial number added automatically or manually. The API token can be generated under Admin > API keys in the navigation bar. To learn more about how to integrate your devices with Cisco Umbrella, read [here](#).

🔍 Search by device name or serial number.

2 Total

Device Name	Serial Number	Primary Policy	Status
SD-WAN Employees VPN - Main HQ	FGL189914GG	SD-WAN Employees Policy	● Active
SD-WAN Guests VPN - Guest Branch	FGL18991399	Security Only - Guest Networks	● Active

1-2 of 2 < >

Core Identities

Networks

Network Devices

Roaming Computers

Mobile Devices

Chromebook Users

Network Tunnels

User Provisioning

Configuration

Internal Domains

Sites and Active Directory

Internal Networks

Service Account Exceptions

Root Certificate



8 Total

Network Tunnels ▼	Status	Device Type	Last Active
US HQ	✓ Active	ASA	Just Now
EMEA HQ	✓ Active	ISR	Just Now
APAC HQ	✓ Active	ISR	Just Now
Germany Branch	✓ Active	Meraki MX	Just Now
Mexico Branch	✓ Active	Meraki MX	Just Now
Japan Branch	✓ Active	Meraki MX	Just Now
Spain Guests	✓ Active	Viptela vEdge	Just Now
Australia Guests	✓ Active	Viptela vEdge	Just Now



Add New Tunnel

Tunnel Name

Device Type

ASA

ISR

Viptela vEdge

Other

CANCEL

SAVE



8 Total

Network Tunnels ▼	Status	Device Type	Last Active
US HQ	✓ Active	ASA	Just Now
EMEA HQ	✓ Active	ISR	Just Now
APAC HQ	✓ Active	ISR	Just Now
Germany Branch	✓ Active	Meraki MX	Just Now
Mexico Branch	✓ Active	Meraki MX	Just Now
Japan Branch	✓ Active	Meraki MX	Just Now
Spain Guests	✓ Active	Viptela vEdge	Just Now
Australia Guests	✓ Active	Viptela vEdge	Just Now



Overview

Deployments >

Policies >

Management

DNS Policies

Firewall Policy

Web Policies

Policy Components

Destination Lists

Content Categories

Application Settings

Security Settings

Block Page Appearance

Integrations

Reporting >

Admin >

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. More policy info can be found in [this article](#).

Sorted by Order of Enforcement

1

All HQ and Branches Web Policy

Protection
Web PolicyApplied To
1 IdentityContains
3 Policy SettingsLast Modified
Sep 12, 2019 ✓

2

Guests Web Policy

Protection
Web PolicyApplied To
18 IdentitiesContains
4 Policy SettingsLast Modified
Sep 12, 2019 ✓

3

Roaming Users Web Policy

Protection
Web PolicyApplied To
1 IdentityContains
4 Policy SettingsLast Modified
Sep 12, 2019 ✓



Overview

Deployments >

Policies >

Management

DNS Policies

Firewall Policy

Web Policies

Policy Components

Destination Lists

Content Categories

Application Settings

Security Settings

Block Page Appearance

Integrations

Reporting >

Admin >

The Firewall Policy allows you to control network traffic based on IP, port, and protocol. Rules within the policy are evaluated in descending order.

FILTERS

4 Total

<input type="checkbox"/>	Priority	Name	Status	Protocol	Source Criteria	Destination Criteria	Action	
<input type="checkbox"/>	1	Block Dangerous IPs	Enabled	Any	AnyIPs AnyPorts	2 IPs AnyPorts	Block	...
<input type="checkbox"/>	2	Block SQL Server Access	Enabled	Any	AnyIPs AnyPorts	3 IPs 1 Port	Block	...
<input type="checkbox"/>	3	Protect our BitSight Score	Enabled	Any	AnyIPs AnyPorts	AnyIPs 1 Port	Block	...
<input type="checkbox"/>	4	Default Rule	Enabled	Any	AnyIPs AnyPorts	AnyIPs AnyPorts	Allow	...

Core Reports

Security Overview

Security Activity

Activity Search

Destinations

Identities

Additional Reports

Total Requests

Activity Volume

Top Domains

Top Categories

Top Identities



Q Search request activity

Advanced ▾

CLEAR

Columns

All Requests ▾

Identity	Destination	Action	Categories	>
Mexico Branch	clikerz.net	Blocked	Gambling	
Australia Guests	34.201.37.125:5558	Blocked		
US HQ	full-streaming.fr	Blocked	Phishing	
Spain Guests	34.196.255.167:10034	Blocked		
EMEA HQ	moonbit.co.in	Blocked	Cryptomining	
EMEA HQ	full-streaming.fr	Blocked	Phishing	
Spain Guests	http://d2bq.cl.net/9e.crx/tntwring.html	Blocked	DNS Tunneling	
Mexico Branch	https://djpunjab.video/NATEON60.exe	Blocked	Cryptomining	
US HQ	http://imgtiger.com/SMSetup.exe	Blocked	Pornography	
Mexico Branch	https://poker.co.ru/ru-en/information/preparation	Blocked	Gambling	
APAC HQ	https://vpnoverdns.com/OC313_SCR_.exe	Blocked	DNS Tunneling	



Security Activity

Activity Search

Destinations

Identities

Additional Reports

Total Requests

Activity Volume

Top Domains

Top Categories

Top Identities

App Discovery

Cloud Malware

Management

Exported Reports

Scheduled Reports

Admin Audit Log

3,327 apps discovered

2,321
unreviewed apps27
apps under audit662
apps not approved317
apps approved

Flagged Categories

Category:
Anonymizer7
unreviewed apps

Anonymizer apps introduce risk to your network because they enable users to bypass security controls.

[DETAILS](#)Category:
P2P5
unreviewed apps

P2P apps represent high risk because they can be used to transmit files infected with viruses and malware.

[DETAILS](#)Category:
Cloud Storage106
unreviewed apps

Discover what **cloud storage** apps are in use - sensitive data may be stored in unreliable services or unsecured environments.

[DETAILS](#)

Flagged Apps (3 of 19)



Redbooth

High



Collaboration app used by 5 identities



Jumpshare

High



P2P app used by 4 identities



Fonality

High



Collaboration app used by 5 identities



Security Activity

Activity Search

Destinations

Identities

Additional Reports

Total Requests

Activity Volume

Top Domains

Top Categories

Top Identities

App Discovery

Cloud Malware

Management

Exported Reports

Scheduled Reports

Admin Audit Log

Dashboard

Search for App / Vendor



Filter by Identity

Category



Risk



App Type



Label



Date



Category:

Anonymizer x

[Clear all filters](#)

UNREVIEWED (7)



UNDER AUDIT (6)



NOT APPROVED (0)












APPROVED (0)



ALL APPS (13)

Under Audit Apps (6 Found)

Application	Vendor	Weighted Risk	Identities	Total Traffic	Label
 ProxySite Anonymizer	ProxySite	High	4	0 B total traffic  0 B 0 B	 Under Audit Edit app controls
 Private Tunnel Anonymizer	OpenVPN	High	4	51 MB total traffic  4 MB 48 MB	 Under Audit Edit app controls
 DotVPN Anonymizer	Smart Security Ltd	Medium	4	0 B total traffic  0 B 0 B	 Under Audit Edit app controls



Security Activity

Activity Search

Destinations

Identities

Additional Reports

Total Requests

Activity Volume

Top Domains

Top Categories

Top Identities

App Discovery

Cloud Malware

Management

Exported Reports

Scheduled Reports

Admin Audit Log

Control Private Tunnel

Select which settings should block or allow this application

Application Settings (2 selected of 3 total)

**Default Settings**

Applied in: Global Branch Policy, Security Only ...

Block

**HR App Restrictive**

Applied in: High Restrict Group

Block

**Global App Allow**

Applied in: Global Allow Policy

Block



Label application as

Not Approved

For more configuration options, go to [Application Settings](#) in the policy section.

CANCEL

SAVE

DotVPN
Anonymizer

Smart Security Ltd

Medium

4

Total Traffic ▾ Label ⓘ

0 B total traffic

Under Audit ▾



0 B

[Edit app controls](#)

0 B

51 MB total traffic

Under Audit ▾



4 MB

[Edit app controls](#)

48 MB

0 B total traffic

Under Audit ▾



0 B

[Edit app controls](#)

0 B



Security Activity

Activity Search

Destinations

Identities

Additional Reports

Total Requests

Activity Volume

Top Domains

Top Categories

Top Identities

App Discovery

Cloud Malware

Management

Exported Reports

Scheduled Reports

Admin Audit Log

3,327 apps discovered

2,321
unreviewed apps27
apps under audit662
apps not approved317
apps approved

Flagged Categories

Category:
Anonymizer7
unreviewed apps

Anonymizer apps introduce risk to your network because they enable users to bypass security controls.

[DETAILS](#)Category:
P2P5
unreviewed apps

P2P apps represent high risk because they can be used to transmit files infected with viruses and malware.

[DETAILS](#)Category:
Cloud Storage106
unreviewed apps

Discover what **cloud storage** apps are in use - sensitive data may be stored in unreliable services or unsecured environments.

[DETAILS](#)

Flagged Apps (3 of 19)



Redbooth

High



Collaboration app used by 5 identities



Fonality

High



Collaboration app used by 5 identities



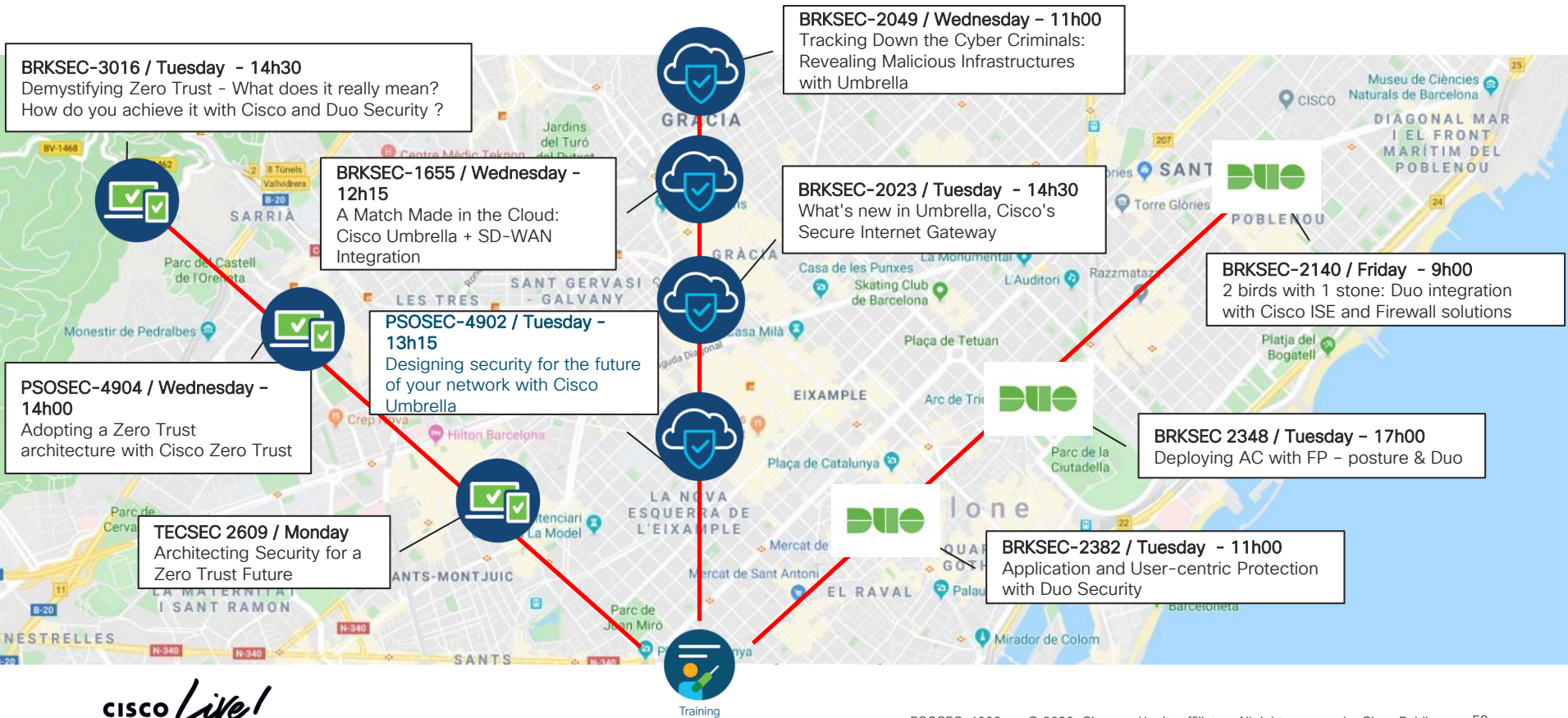
ooVoo

High



Collaboration app used by 5 identities

Umbrella, DUO and Zero Trust Learning maps



Continue your education



Demos in the
Cisco Showcase



Walk-In Labs



Meet the Engineer
1:1 meetings



Related sessions



Start a free trial of Cisco Umbrella: signup.umbrella.com

Complete your online session survey



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

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



Thank you





You make **possible**