



ZIA Major release (Q1 CY20)

<NAME>| <ROLE>

Source IP Preservation

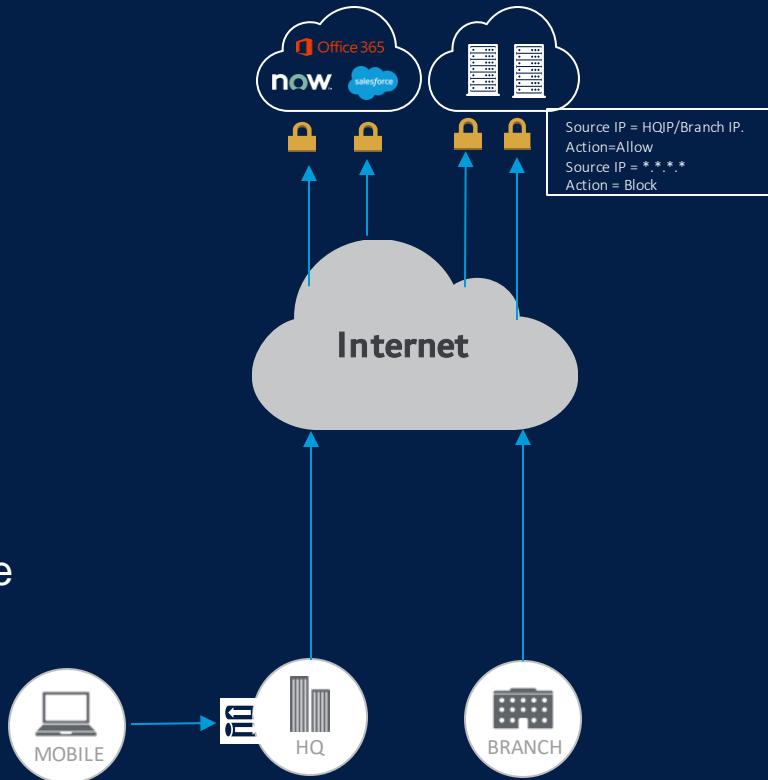
Source IP Anchoring

Use Case:

- Dedicated egress IP's
- Selective application steering
- Web & Non-web applications

Current Solutions:

- Virtual Service Edge/Physical Service Edge
- Whitelist Zscaler outbound IP's
- Bypass Zscaler



Source IP Anchoring – New Solutions!!!

Zscaler ZIA supports two modes

ZPA Connector

- Select traffic needs to come from a non Zscaler IP address,
a.k.a. Source IP Anchoring
- Supports web and non-web traffic

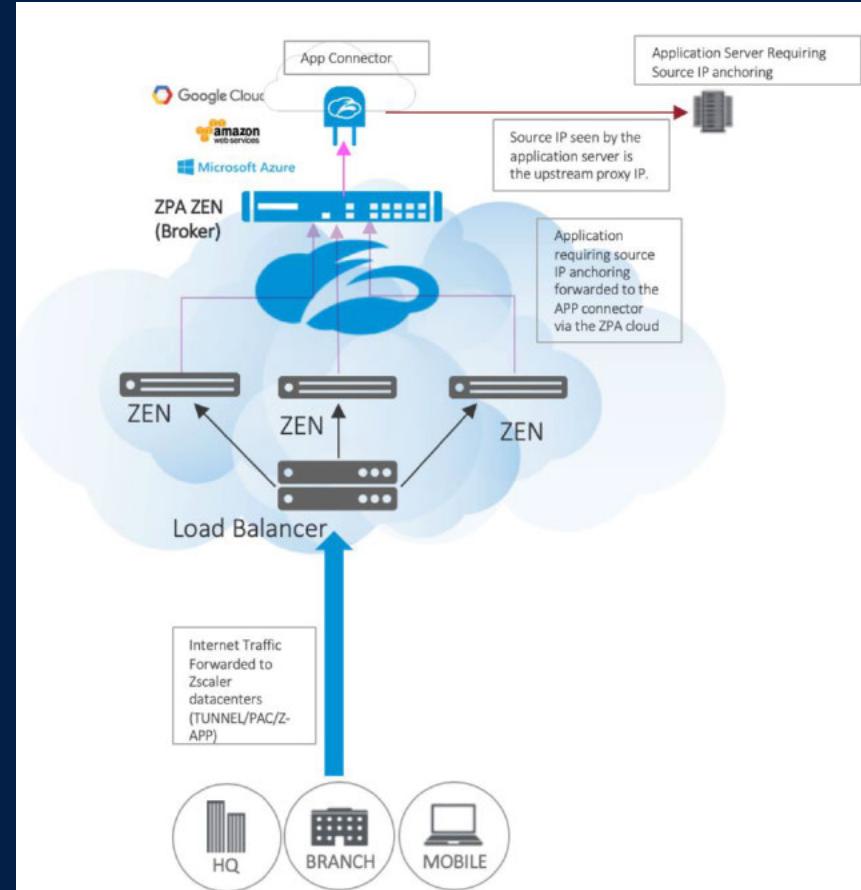
Proxy Chain *

- Third party upstream service may need select traffic sent for processing and archiving, e.g. Enterprise Information Archiving (EIA) solutions
- Web(80/443) Only traffic

* Proxy chain is not recommended for source-ip-anchoring as Zscaler cannot be held to SLA and it requires customer open attack surface (proxy listener)

Source IP Anchoring using Zscaler App Connector

- Public cloud hosted ZPA ZEN instance
- ZIA inspects traffic and enforce security before forwarding to connector
- Multiple connectors can be deployed
- Supports web and non-web application traffic
- Additional License required

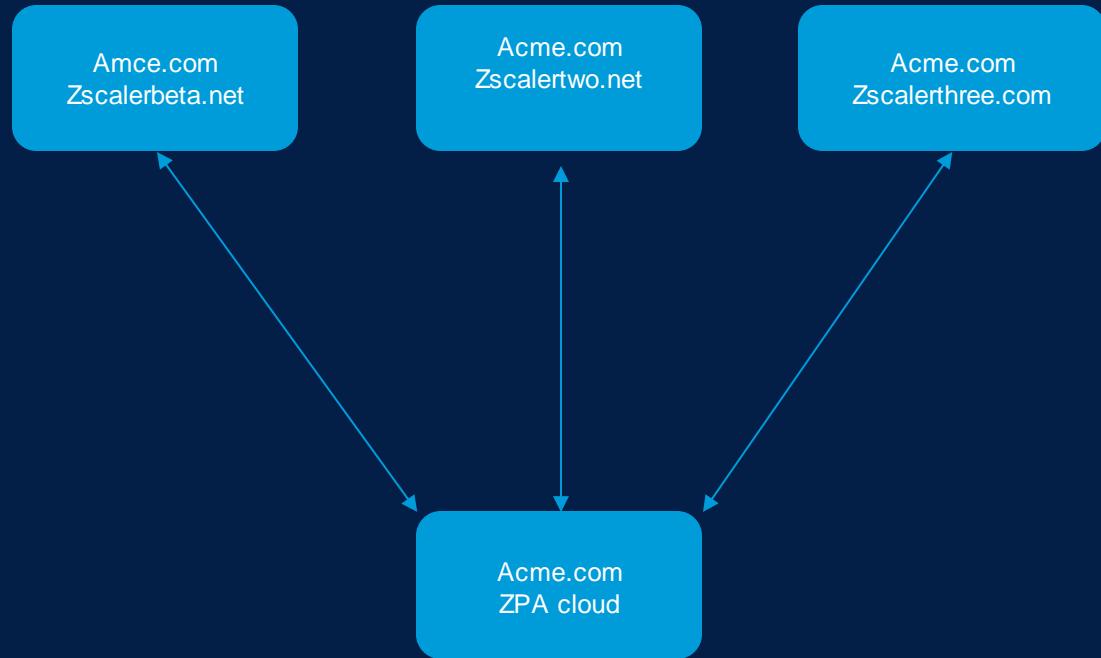


How does Source IP Anchoring work?

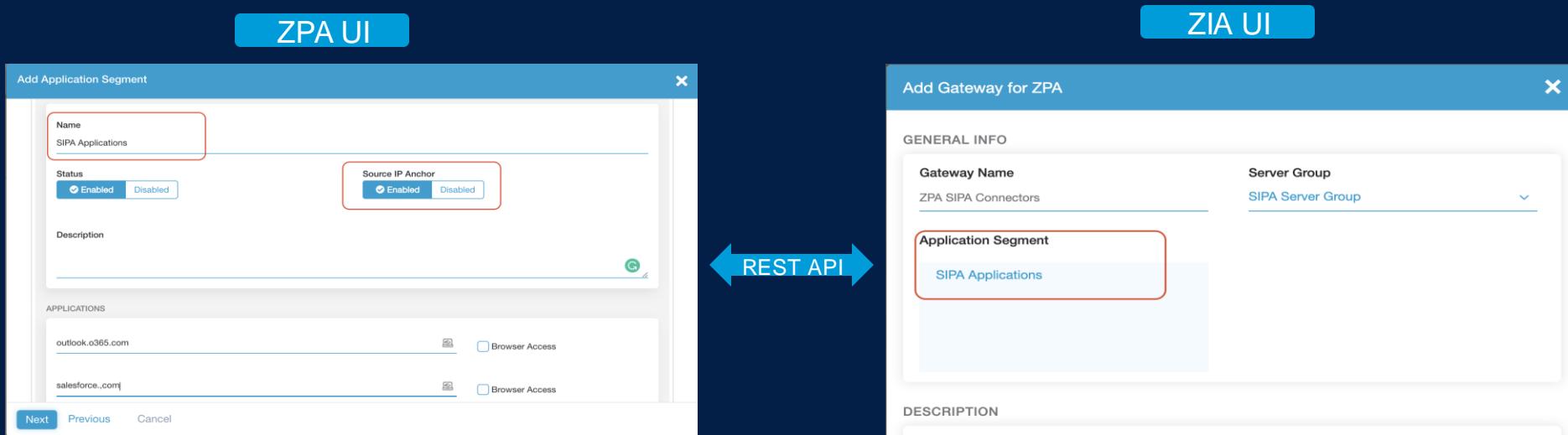
- 1 Create Application Segment , Server groups on ZPA portal
- 2 Create DNS gateway on ZIA portal
- 3 Create Forwarding rule policy on ZIA portal

Tenant Bonding Between ZIA and ZPA

- Primary Domain should be same for ZIA & ZPA
- Multiple ZIA tenants can be mapped to single ZPA tenant



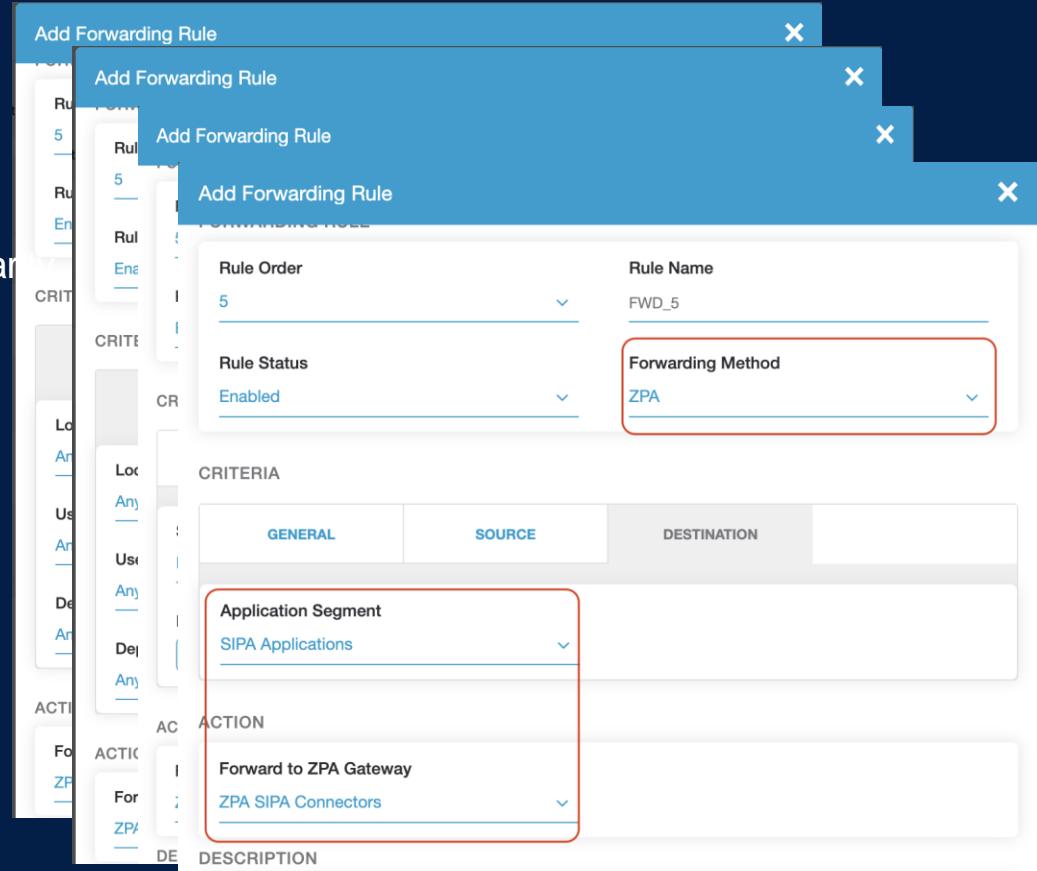
Interaction between ZIA and ZPA Tenants



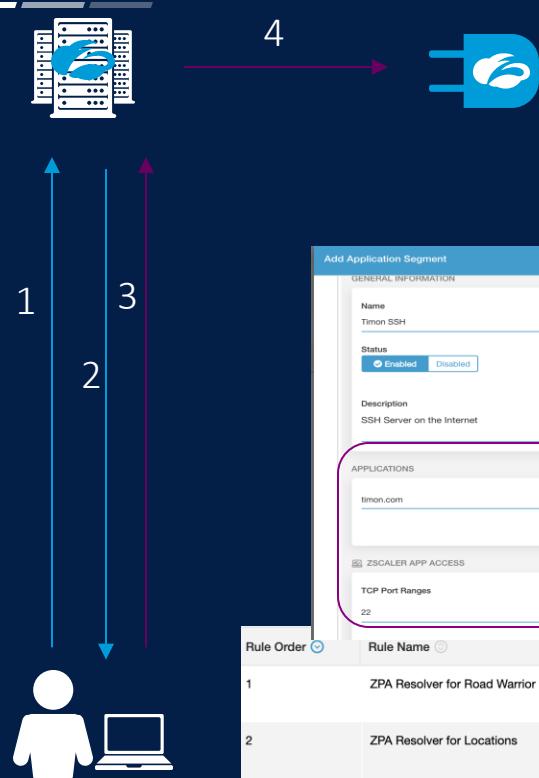
- Rest API based connectivity
- ZIA will fetch all Application Segments which has “Source Ip Anchor” flag enabled
- App segments and server group combinations are available to configure on ZIA

Forwarding Rule Policy on ZIA

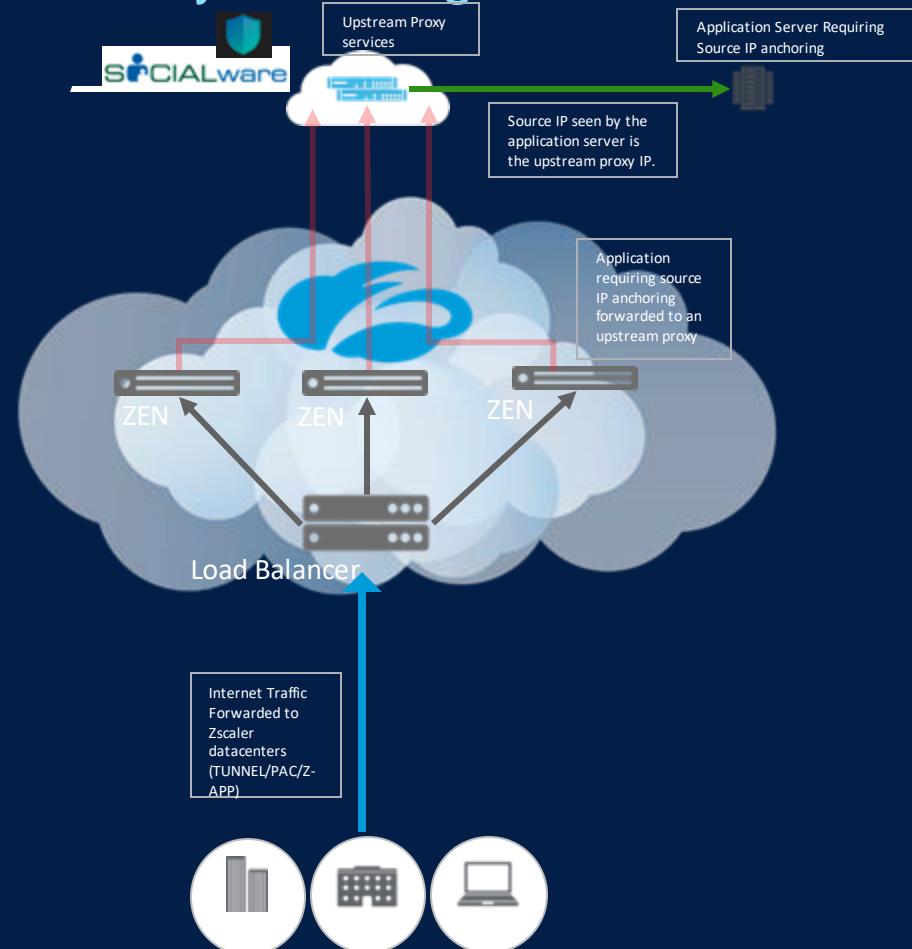
1. Choose the Forwarding Method
2. Criteria
 - User/Group/Dept/Location granular
 - Src IP groups/Src IP address
 - Application segment
3. Action – Choose ZPA gateway



Traffic Handling – Non HTTP/HTTPPs and Web



Proxy Chaining from Zscaler



- Integration with 3rd party services e.g. Enterprise Information Archiving (EIA), RBI etc
 - Features:
 - Redundant proxies
 - support for dual SSL decryption
 - Granular policies for proxy chaining.

Security

CrowdStrike and Zscaler

Unifying Endpoint and Network Security Detection and Response



ENDPOINT POSTURE
DRIVEN ACCESS POLICY
ENFORCEMENT



THREAT VISIBILITY
ACROSS NETWORK AND
ENDPOINT



FAST AND EFFECTIVE
THREAT RESPONSE AND
CONTAINMENT

Unifying Endpoint and Network

ZERO DAY, MALWARE & ADVANCED THREAT PROTECTION

ACCESS CONTROL

REPORTING

ENDPOINT DETECTION & RESPONSE



CROWDSTRIKE
AGENT Z-APP



- IOCs
- ENDPOINT POSTURE

Zscaler API | Falcon API

BEHAVIOR & POSTURE ANALYSIS

ENDPOINT INFORMATION



Threat detection and response across the Network and Endpoint

Easy One-time Setup

The screenshot shows the Zscaler API key management interface. On the left, there's a sidebar with various icons and sections like 'API key', 'Account Information', 'API UUID', 'Edit API client', 'API client', 'Client ID', 'SECRET', 'Copy this', 'Prevention policies', and 'Date and Time'. A red box highlights the 'Edit API client' section. The main area is titled 'User Profile' with 'User Details' sub-sections for 'EMAIL' (rupalekar@zscaler.com), 'CUSTOME ID' (redacted), 'FIRST NAME' (Rohan), and 'LAST NAME' (Upalekar). Below these are 'Cancel' and 'Save' buttons. At the bottom, there's a 'Privacy Policy' link and a 'SELECT TIMEZONE' dropdown. A red arrow points from the text 'Clicking here will reveal the CS Customer ID' to the 'Customer ID' input field.

The screenshot shows the Zscaler Partner Integration interface under the 'MCAS' tab. It has a sidebar with 'Dashboard', 'Analytics', 'Policy', 'Administration' (selected), 'Activation', 'Search', and 'Help'. The main area is titled 'Partner Integration' with tabs for 'MCAS', 'SD-WAN PARTNER', 'AZURE VIRTUAL WAN', and 'CROWDSTRIKE' (selected). The 'CROWDSTRIKE' tab contains two sections: 'CrowdStrike Authentication Tokens' (with fields for 'API Auth URL' (api.crowdstrike.com/), 'Client ID' (redacted), 'Secret' (redacted), and 'Customer ID' (redacted)) and 'CrowdStrike Sync' (with a 'Sync' button and a note 'Last synced on: Tuesday, August 25, 2018 3.12.08 pm'). A green line with numbered circles indicates a workflow: step 1 is 'CrowdStrike Authentication Tokens' and step 2 is 'CrowdStrike Sync'.

ZIA: Threat detection and response across the Network and Endpoint

Integrated Visibility and Response

The screenshot displays the CrowdStrike Falcon interface, specifically the 'Sandbox Files Found Malicious' section. A modal window titled 'CrowdStrike Endpoint Hits' is open, showing detailed file properties for a Spyware sample. The threat name is highlighted with a green arrow pointing to the 'nj.Rat.Win32.2019' entry. Below the modal, a table lists 71 endpoint hits over the last 30 days. The first hit in the table is also highlighted with a green arrow pointing to the '0644C6E80644C6E80644C6E8' Agent ID entry. The table includes columns for Agent ID, Hostname, Internal IP, External IP, OS Version, First Seen, Last Seen, and Action (with 'Detected' and 'Quarantine' buttons).

Sandbox Files Found Malicious - Week of Feb 10 — Feb 29 —

CrowdStrike Endpoint Hits

File Properties

Sandbox Category	Spyware
Sandbox Score	79
Threat Name	nj.Rat.Win32.2019
File Type	Vendor: File is not digitally signed
File Size	131,358 bytes
MD5	8fc53813c25dd12baea0f02b73e6bbef
SHA-1	2cf7869318c9a51f76e102a4e30ca7199c032845
SHA-256	ce43b4c039eb30d6ef78d54bedc967bed60cc634cac88ea3f2ed2a0b19bb4e
SSDEEP	3072.DlF2vLBx7KIfecKzaaVuTXNHiokhwk6zzpYu4yzHEspnD8.Bf2oXQe1uTvh16zFY9yzHhiY
# of Endpoint Hits	71

Last 30 Days (Sep 1, 2019 - Oct 1, 2019)

Agent ID	Hostname	Internal IP	External IP	OS Version	First Seen	Last Seen	Action
0644C6E80644C6E80644C6E8	zs1-sf2-sme	172.31.0.0	240.187.123.151	Win 10.388	10/08/19, 2:54 PM	10/08/19, 1:42 AM	D Detected Quarantine
260E260E260E260E260E260E	zs1-sf2-sme	172.31.0.1	99.172.93.114	Win 10.387	10/08/19, 2:52 PM	10/08/19, 1:38 AM	D Detected Quarantine
5F795F795F795F795F795F79	zs3-ncf3-sme	172.31.0.2	146.103.87.19	Win 10.357	10/08/19, 2:50 PM	10/08/19, 1:34 AM	D Detected Quarantine
BA75BA75BA75BA75BA75BA75	zs1-sjc5f1-sme	172.31.0.3	192.19.176.140	Win 10.356	10/08/19, 2:48 PM	10/08/19, 1:30 AM	D Detected Quarantine
AF841557582EAFB41557582EA	zs3-sjc7f1-sme	172.31.0.4	160.148.120.47	Win 10.329	10/08/19, 2:46 PM	10/08/19, 1:26 AM	D Detected Quarantine

ZIA: Threat detection and response across the Network and Endpoint

- Integrated Visibility and Response

Executable Activities

	Time (UTC) ◁	Host Name ◁	File Name ◁	File Path ◁	Action ◁
1	2019-10-10 14:14:02	EC2AMAZ-ALNLVE1	pepflashplayer.dll	\Device\HarddiskVolume1\Users\ADMINI~1\AppData\Local\Temp\2\scoped_dir12648_699454343\PepperFlash\32.0.270\	Deleted
2	2019-10-10 14:10:21	EC2AMAZ-ALNLVE1	pepflashplayer.dll	\Device\HarddiskVolume1\Users\ADMINI~1\AppData\Local\Temp\2\8184_1366652613\	Added
3	2019-10-10 14:10:21	EC2AMAZ-ALNLVE1	pepflashplayer.dll	\Device\HarddiskVolume1\Users\ADMINI~1\AppData\Local\Temp\2\8184_1366652613\	Added
4	2019-10-10 14:01:27	EC2AMAZ-ALNLVE1	pepflashplayer.dll	\Device\HarddiskVolume1\Users\ADMINI~1\AppData\Local\Temp\2\scoped_dir16252_405753234\PepperFlash\32.0.270\	Deleted
5	2019-10-10 13:58:03	EC2AMAZ-ALNLVE1	pepflashplayer.dll	\Device\HarddiskVolume1\Users\ADMINI~1\AppData\Local\Temp\2\5348_1881364332\	Added
6	2019-10-10 13:58:02	EC2AMAZ-ALNLVE1	pepflashplayer.dll	\Device\HarddiskVolume1\Users\ADMINI~1\AppData\Local\Temp\2\5348_1881364332\	Added
7	2019-10-10 13:46:52	EC2AMAZ-ALNLVE1	pepflashplayer.dll	\Device\HarddiskVolume1\Users\ADMINI~1\AppData\Local\Temp\2\scoped_dir17156_1334360394\PepperFlash\32.0.270\	Deleted
8	2019-10-10 13:41:15	EC2AMAZ-ALNLVE1	pepflashplayer.dll	\Device\HarddiskVolume1\Users\ADMINI~1\AppData\Local\Temp\2\24720_847205754\	Added
9	2019-10-10 13:41:15	EC2AMAZ-ALNLVE1	pepflashplayer.dll	\Device\HarddiskVolume1\Users\ADMINI~1\AppData\Local\Temp\2\24720_847205754\	Added
10	2019-10-10 13:09:05	EC2AMAZ-ALNLVE1	pepflashplayer.dll	\Device\HarddiskVolume1\Users\ADMINI~1\AppData\Local\Temp\2\scoped_dir19212_1540548317\PepperFlash\32.0.270\	Deleted

« prev 1 2 3 4 5 6 7 8 9 10 next »

External Network Connections Map

External Network Connections

Country ◁	Remote Port ◁	Count ◁
Australia	443	6
Australia	80	3
Austria	443	1
Belgium	443	2
Brazil	443	3
Brazil	80	2
British Virgin Islands	443	8
Bulgaria	443	4
Bulgaria	80	2
Canada	443	30
Canada	80	3
Chad	443	1

ZPA: Endpoint posture driven conditional access to sensitive apps

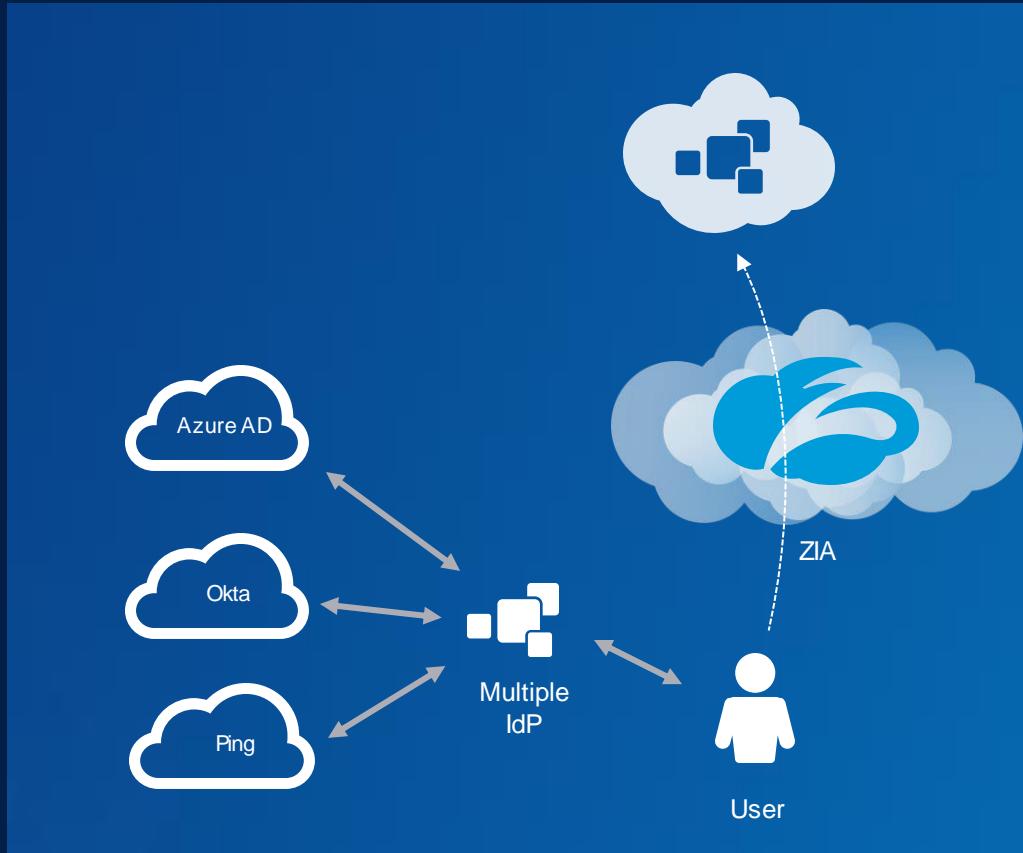
The image is a composite of three screenshots illustrating the integration of CrowdStrike Falcon with Zscaler App Access (ZAA).

- ZAA Interface:** On the left, the ZAA dashboard shows a "Zscaler App" card. It displays connection details: STATUS (Closed Connection), DURATION (1ms), TOTAL BYTES (0 B), and CONNECTION ID (N1X1Kp2z-jS7t3qH9Gq...). Buttons for "Copy json" and "View Log" are visible.
- CrowdStrike Falcon Sensor Setup:** A central window titled "CrowdStrike Falcon Sensor Setup" shows a red falcon logo and the message "CrowdStrike Windows Sensor has been successfully installed". A "CLOSE" button is at the bottom right.
- Posture Check Result:** On the right, a web browser window shows the URL "internal.safemarch.com/". The main content reads "Posture check passes - App access granted" in large bold letters, with "intranetNOW®" below it. The browser's address bar shows "internal.safemarch.com/".

Platform Enhancements

Multiple IdP support on ZIA

- ZIA will support multiple IdP on the same cloud instance
- IdP selection criteria based on location and/or domain
- One domain or location can be mapped to one unique IdP
- Allows different countries or different sub-orgs to have different IdPs
- Support with Z App mobile portal as IdP



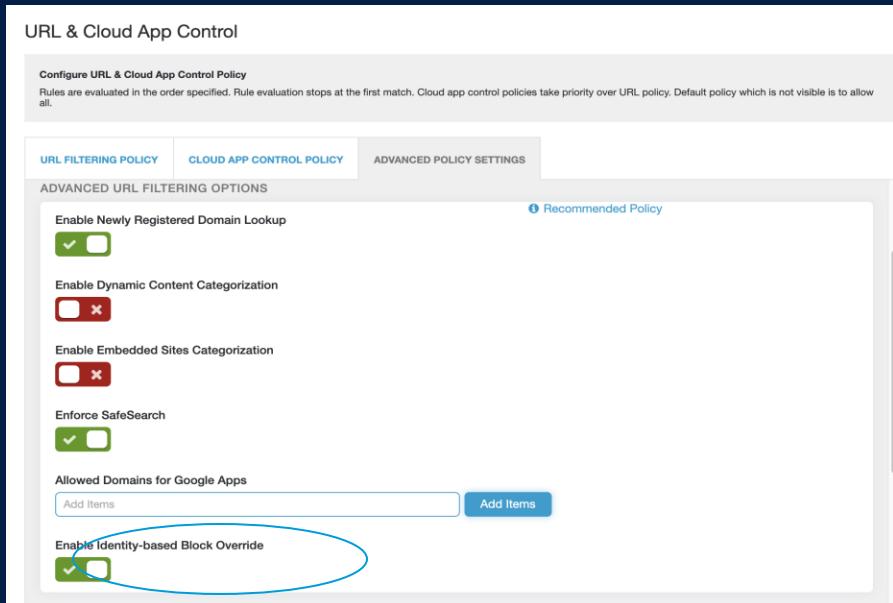
Support for Company Auth in Block Overrides for URL filtering

Prior to 6.0:

- The block-override feature in ZIA is applicable for hosted database users. The user who could override a policy should be a hosted user. This restricts the feature mainly to orgs that have auth-type as hosted-user. A complex workaround exists for orgs with non-hosted auth type by means of a One Time Password (OTP).

With 6.0:

- This feature removes the restriction by allowing the override user to provide access to blocked pages by using company provided credentials (like single sign-on credentials)
- Different auth-types the company could have are 'Hosted DB', 'Zab/Authbridge', LDap(active directory/open ldap) and SAML.



SSLVPN Clustering Overview

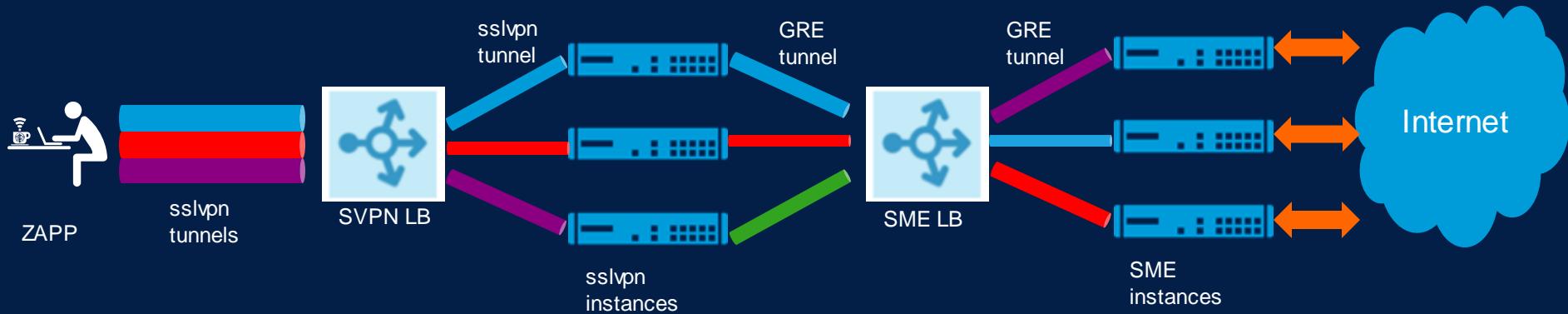
What

- New cloudnode type SVPN
- Dedicated SVPN clusters for independent scaling
- Load-balancer improvements
- Upgrade in SVPN server discovery mechanism for ZAPPs

Why

- Fault tolerance. Decouple tunneling from Proxy/Firewall
- Horizontal scaling of sslvpn capacity
- Load-balance tunnels from an IP uniformly across cluster
- Faster tunnel setup

Traffic Flow via SSLVPN Instances



Improvements to SSL & CONNECT policy evaluation & logging

Consistent evaluation and recording based on what we see in the traffic

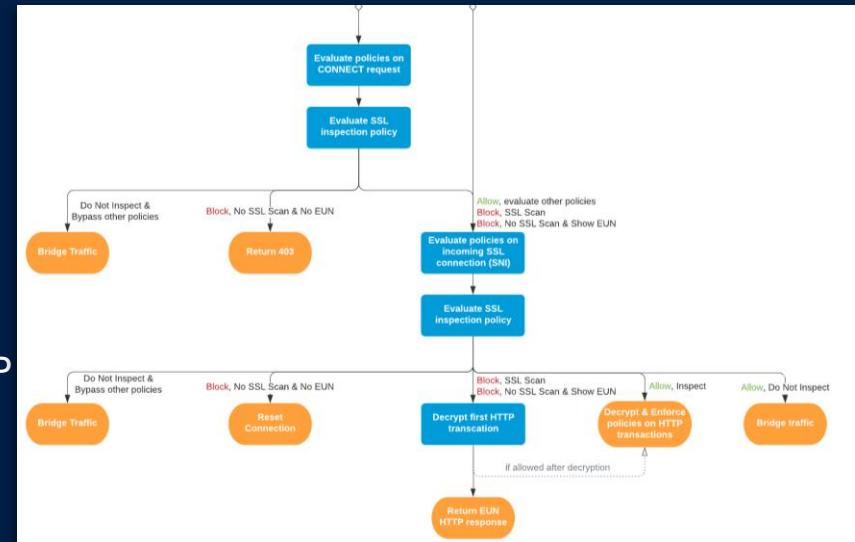
Why?

- Unreliable accounting of decrypted SSL traffic
- HTTP CONNECT in transparent proxy !?
- Is HTTP CONNECT in explicit proxy SSL or HTTPS or HTTP !?

What?

- New protocol types: HTTP-PROXY, TUNNEL-SSL
- Additional round of policy evaluation and weblog record for SSL session after CONNECT
- Support for common HTTP methods in URL policy
- More “N/A” in weblogs, since SSL session is not HTTP
- Granular SSL policy reason field (hidden initially)

Traffic Type	Protocol for evaluation/logging	Request Method for evaluation/logging
CONNECT to ZEN	HTTP-PROXY	CONNECT
CONNECT to 3PP	HTTP	CONNECT
Binary after CONNECT	TUNNEL	Any / “N/A”
SSL ClientHello	SSL	Any / “N/A”
HTTP after SSL	HTTPS	Actual Method
Binary after SSL	TUNNEL-SSL	Any / “N/A”



New Public APIs for customers and technology partners

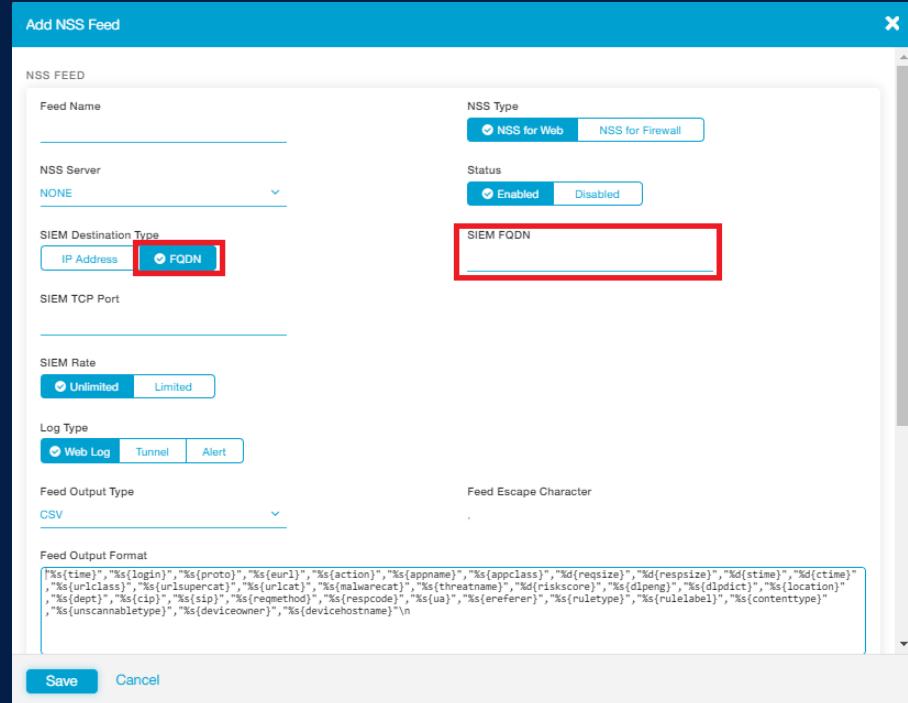
- Locations / Sub-locations enhancements
 - Full CRUD of sub-locations
 - Including gateway options (SSL, Firewall)
 - Available both for **customers** and partners
- URL Filtering Policies
 - Full CRUD
- Authentication Bypass List management
- SSL Bypass List management
- Admin User management
 - Full CRUD of admin users
 - Read-only admin roles

The screenshot shows a user interface for managing public APIs. It features three main sections: "Locations", "URL Filtering Policies", and "SSL Inspection Settings". Each section contains a list of RESTful endpoints with their methods and descriptions.

- Locations**
 - GET /locations** Gets information on locations
 - POST /locations** Adds a new location
 - POST /locations/bulkDelete** Bulk delete locations up to a maximum of 100 locations per request
- URL Filtering Policies**
 - GET /urlFilteringRules** Gets a list of all of URL Filtering Policy rules
 - POST /urlFilteringRules** Adds a URL Filtering Policy rule
 - GET /urlFilteringRules/{ruleId}** Gets the URL Filtering Policy rule for the specified ID
 - PUT /urlFilteringRules/{ruleId}** Updates the URL Filtering Policy rule for the specified ID
- SSL Inspection Settings**
 - GET /sslSettings/exemptedUrls** Gets a list of URLs that were exempted from SSL Inspection and policy evaluation
 - POST /sslSettings/exemptedUrls** Adds URLs to the exempted from SSL Inspection and policy evaluation list or removes URLs from the list

FQDN for NSS Feed Destination

- Today, only IP:PORT can be used for destination TCP connection
- IPs can change → Ability to configure FQDN as destination
- FQDN is resolved when establishing TCP connection or after TCP connection drops
- If DNS resolution has multiple IP addresses, only first one is selected
- Cannot use for DNS-based load balancing!



Virtual Service Edge on Azure Cloud

New



Policy & Access Control

Location Groups

- Types of groups – Manual & Dynamic Groups
- **Manual Group:** Manually pick locations and/or sub-locations to add to the group.
 - Filter list: The list of locations to select from, can be filtered using

The screenshot shows the 'Add Manual Group' interface in two stages:

Stage 1: Group Information

This stage is titled '1 Group Information'. It contains a 'Name' input field and a 'Description' input field. A preview window shows a list of 3 matching locations: CP-1, CP-2, and CP-3. A 'Next' button is at the bottom.

No.	Name	IP Addresses	Proxy P...	Use XFF...	Authent...	SSL	Firewall...	Bandwi...	Virtual ...	IPS Co...	Group	Manag...
5	Branch locations	---	10/22	Enabled	Enabled	Enabled	Enabled	---	---	---	---	Self
6	CP-1	103.250.72.116...	---	Enabled	---	---	---	---	---	---	Test 2, Test 1	Self
7	CP-2	12.250.212.256...	---	Enabled	---	---	---	---	---	---	Test 2	Self
8	CP-3	111.13.97.81, 1...	---	Enabled	Enabled: IP...	Enabled	Enabled	---	---	---	Test 2	Self
9	Home office	24.6.141.88	---	Enabled	---	Enabled	Enabled	100M Dow...	---	---	---	Self
10	HQ UK	99.158.155.198	---	Enabled	Enabled: IP...	Enabled	Enabled	5M Down...	---	---	Test 1	Self
11	Internal VZEN	---	---	Enabled	Enabled: IP...	---	Enabled	---	VZEN-Clus...	---	---	Self
12	London Office	---	---	Enabled	Enabled	Enabled	Enabled	100M Dow...	---	---	Test 1	Self

Stage 2: Select Locations

This stage is titled '2 Select Locations'. It shows a list of selected locations: CP-1, CP-2, and CP-3. A 'Search...' input field is at the top right. A dropdown menu labeled 'Add Filter' is open, showing options: Search..., Enable AUP, Enforce Bandwidth Control, Enforce Firewall Control, Managed By, and Use XFF from Client Request.

Location Groups

- **Dynamic Group:** Define the location attributes to be used as criteria to automatically add locations/sub-locations.
 - Future proofed model: Any location/sub-location created will automatically be added to one or more dynamic location groups provided all conditions are met.

Add Dynamic Group

1 Group Information 2 Preview Locations

GENERAL

Name
Demo Dynamic Group

Description

GROUP CONDITIONS

Name Contains CP

Add New Condition

Next Cancel

Add Dynamic Group

1 Group Information 2 Preview Locations

3 MATCHING LOCATIONS & SUB-LOCATIONS

No.	Name
1	CP-1
2	CP-2
3	CP-3

Search...

Previous Save Cancel

Add Dynamic Group

1 Group Information 2 Preview Locations

GENERAL

Name

Description

Search... GF

City/State/Province
Country
Enable AUP
Enable Caution
Enable SSL Inspection

Add New Condition

Next Cancel

Location Groups

• Location Attributes

- **Manual Location Groups:** Manage and view manual locations groups that this location or sub-location is a member of.
- **Dynamic Location Groups:** View the dynamic location groups that this location/sub-location is a member of.
- **Exclude from Manual Location Groups:** Setting this control to “On” will disassociate this location or sub-location from any Manual Location Groups that it may be a member of, and will not allow it to be added to any Manual Location Groups in the future.
- **Exclude from Dynamic Location Groups:** Setting this control to “On” will disassociate this location or sub-location from any Dynamic Location Groups that it may be a member of, and will not allow it to be added to any Dynamic Location Groups in the future.

Add Location

X

LOCATION	
Name	Country
City/State/Province	NONE
Manual Location Groups	Time Zone
None	NONE
Exclude from Manual Location Groups	Dynamic Location Groups
<input type="checkbox"/> <input checked="" type="checkbox"/>	---
Exclude from Dynamic Location Groups	Exclude from Dynamic Location Groups
<input type="checkbox"/> <input checked="" type="checkbox"/>	---

Location Groups

- **Use in Policy:** All policies and rules will now support selection of manual and dynamic location groups
- **Reporting**
 - Use in Insights and Logs
 - Use in Dashboards and Reports

Add URL Filtering Rule

Departments

Any

Locations

Any

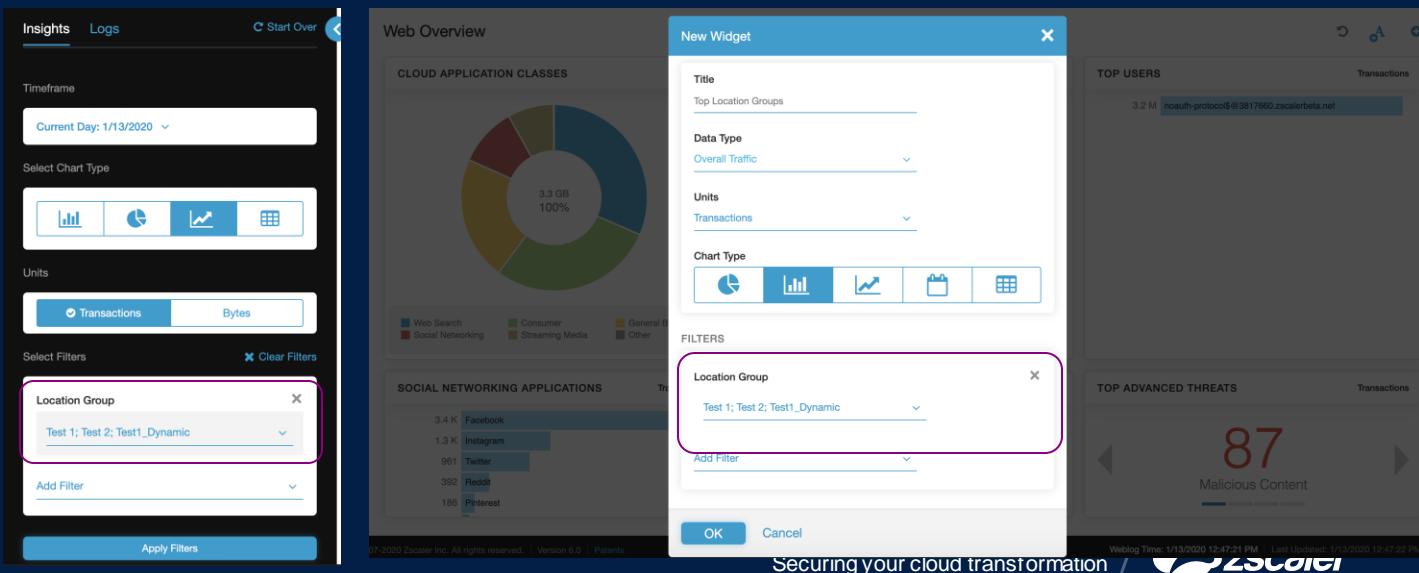
Location Groups

Any

Time

Always

Protocols



Custom URLs Limit Increase

- Limit of custom categories is now increased from 64 to 256. Default limit remains as 64 and can be increased upon request.
- Limit increase from 25,000 to up to 275,000 with additional SKUs. Default limit is 25,000.
- Each SKU gives 50,000 additional custom URLs limit

URL Categories

Max: 275k Used: 26

The custom URL count displayed here shows how many custom URLs your organization is using across all policies. You can see the count in the following places: Advanced Settings, Advanced Threat Protection, Bandwidth Classes, FTP Control, SSL Inspection, and URL Categories. To learn more, see [Ranges & Limitations](#).

Maximum: 275000 | Used: 26 | Remaining: 274974

Custom URLs

Add Items

Search...

.espn.com
.ndtv.com
faq.whatsapp.com
www.securityweek.com
www.thrillophilia.com

1-5 of 5 < 1 / 1 > Remove

URLs retaining parent category

Add Items

Search...

www.netflix.com
www.primevideo.com
www.youtube.com

1-3 of 3 < 1 / 1 > Remove

URL filtering enhancements

- Categorization accuracy improvements
 - New 3rd party feed
 - Reduction in Miscellaneous URLs
 - Better coverage of non-English and regional URLs
 - More accurate categorization
- New URL Categories

URL Category Name	Super Category
Web Conferencing	Internet Communication
Operating System and Software Updates	Information Technology
DNS over HTTPS	Information Technology
Online Trading, Brokerage, Insurance	Business and Economy
Marijuana	Drugs
Malicious TLDs	Security
Encrypted Web Content	Security



External DB integrated in Zscaler



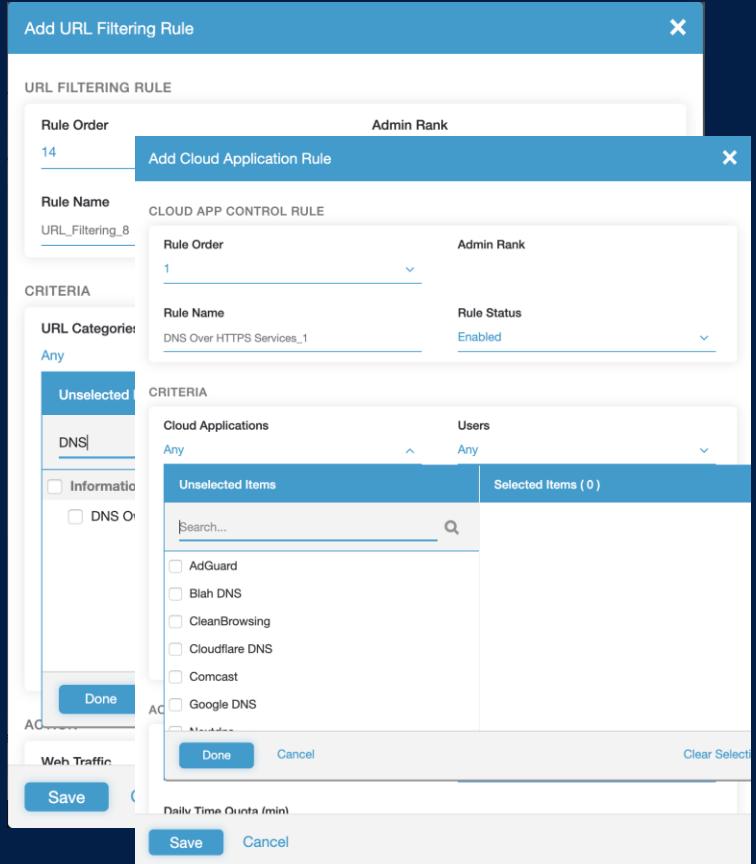
New 3rd party URL categorization engine

DNS over HTTPS (DoH) Support

A new URL category and cloud app category are added for DoH servers

- *Without SSL Inspection:*
 - SNI based
 - Allow/Block DoH servers
 - ~90 domains added
- *With SSL Inspection:*
 - Inspect GET and POST headers
 - Signature: based on MIME(content-type: application/dns-message or application/dns-json)

Granular reporting on DOH is available



Multi-Select Capability

- Supported in Dashboard, Interactive Reports, Insights & Logs
- Select up to 200 values in a single filter
- **Include or Exclude** the selected values
- Dashboards, Interactive Reports and Insights supports multi-select for users, departments, locations, cloud app categories, cloud apps
- Log view supports multi-select on above fields, as well as provides additional operators like “Does not contain”, “Does not start with”, “is Null”, “is Not Null” for filters that perform string match like Domain search.

The image displays three screenshots of the Zscaler interface illustrating the multi-select capability across different modules:

- Top Left:** A screenshot of the "New Widget" configuration dialog. It shows a circular chart with data and various filter settings. A modal window titled "New Widget" is open, showing "Data Type: Overall Traffic" and "Units: Transactions". Below these are buttons for "INCLUDE" and "EXCLUDE", and dropdown menus for "Any" and "Add Filter". Buttons for "OK" and "Cancel" are at the bottom.
- Top Right:** Another "New Widget" dialog, similar to the one above, but with a different set of selected items in the "Selected Items" list. The list includes "ANZ Office", "ANZ Office->Branch", "ANZ Office->Test Sublocation", and "Head Quarter". There are also sections for "Unselected Items" and "Selected Items (4)". Buttons for "Done" and "Cancel" are present.
- Bottom Left:** A screenshot of the "Logs" tab in the Insights module. It shows a sidebar with "Analytics" selected. The main area has tabs for "Logs" (which is active) and "Logs". Below the tabs are "Timeframe" and "Number of Records Displayed" filters. Under "Select Filters", there are two sections: "User" and "Cloud Application", each with "INCLUDE" and "EXCLUDE" buttons. A dropdown menu lists "admin123@safemarch.com; admin2@safem...". Buttons for "Apply Filters" and "Start Over" are at the bottom.
- Bottom Right:** A screenshot of the "Logs" tab in the Insights module, similar to the one above. It highlights a dropdown menu under "Select Filters" for "URL Search". This menu includes operators like "Not Null", "Is Null", "Does Not Contain", "Does Not End With", and "Does Not Start With". Buttons for "Domain", "URL", "Path", and "Host" are at the top of the dropdown.

Platform Improvements

- Improvements to SSL & CONNECT Policy evaluation & logging
- Enhancement to FW policy handling of HTTP CONNECT
- Full CRUD support for location and sublocation in public API
- PAC Enhancements
- EDNS0 Support
- ZSCM enhancements



Thank You
