ZIA Major release (Q1 CY20)

<NAME>| <ROLE>

Source IP Preservation

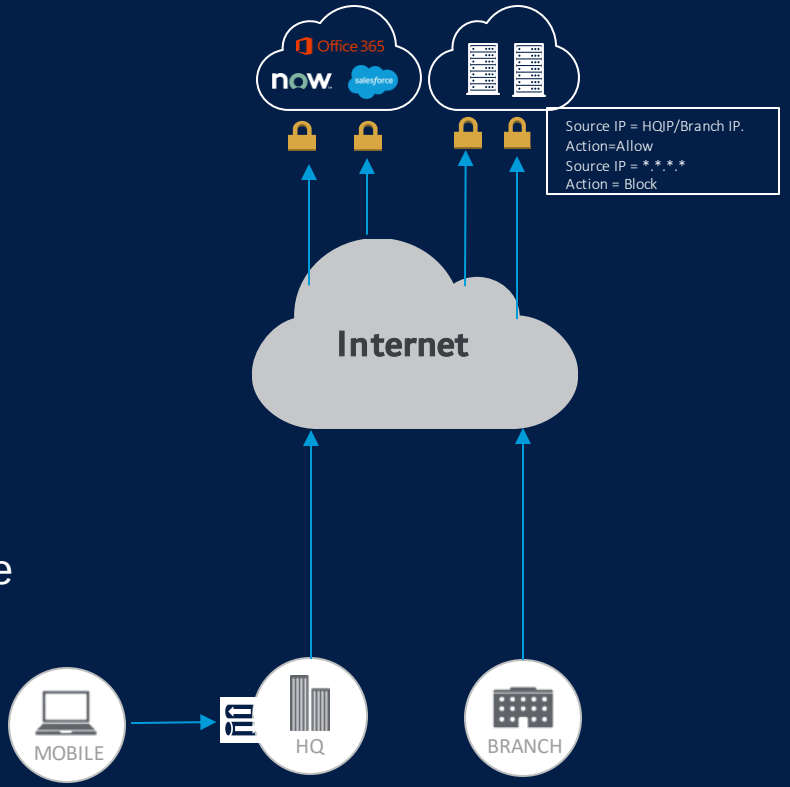
Source IP Anchoring

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

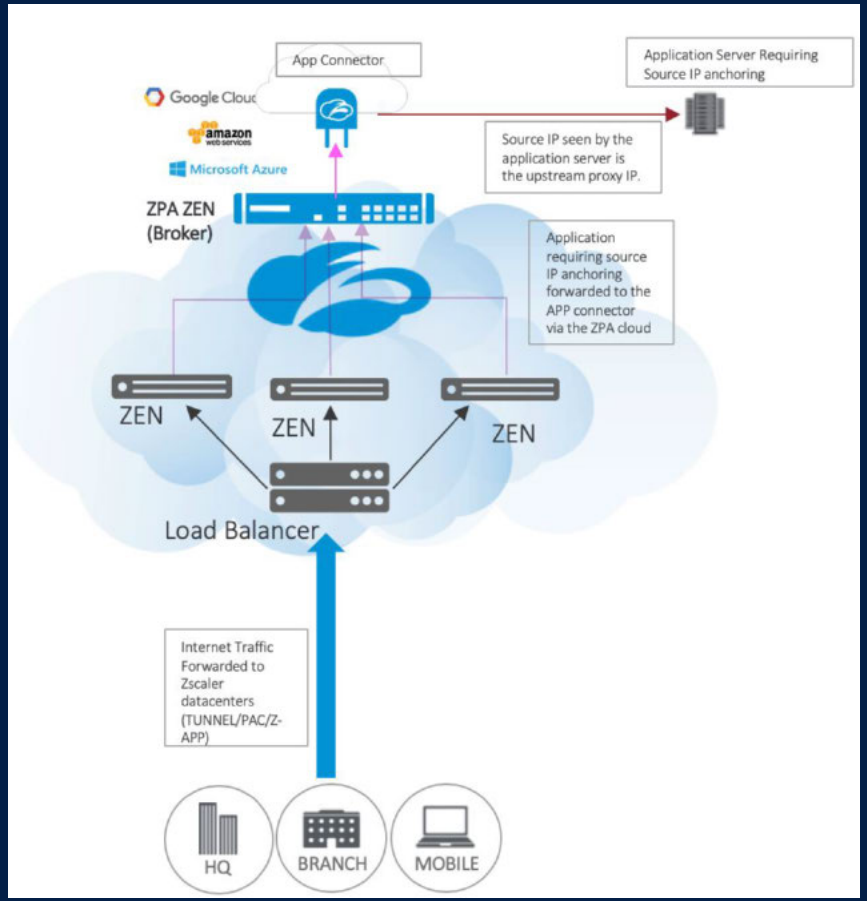
Proxy Chain *

- 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 it 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

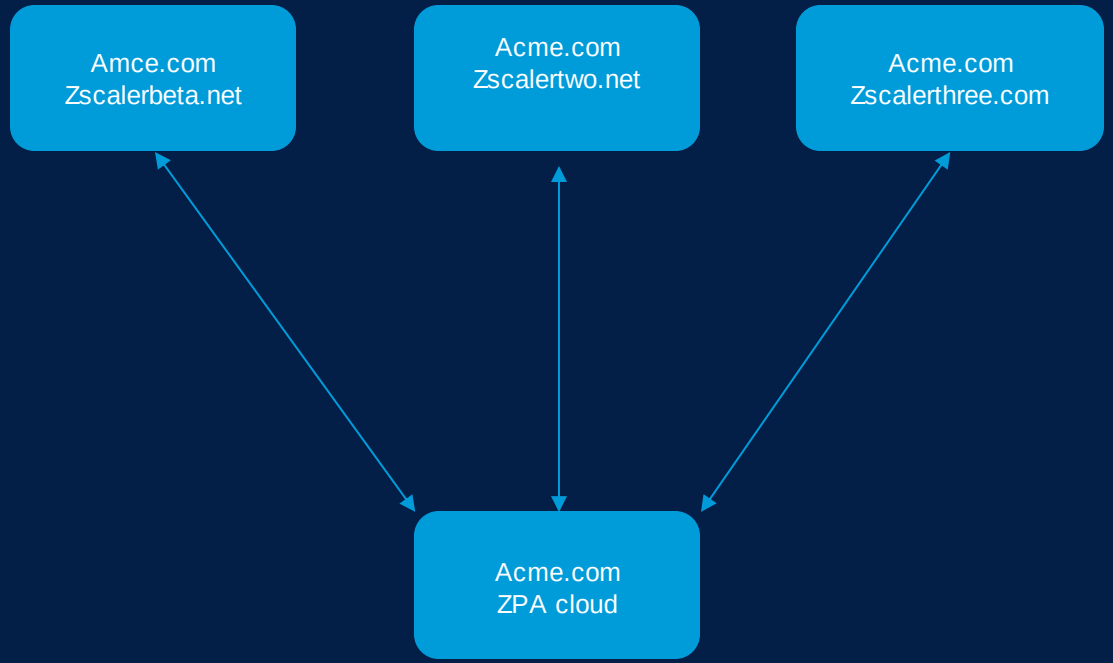


How does Source IP Anchoring work?

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

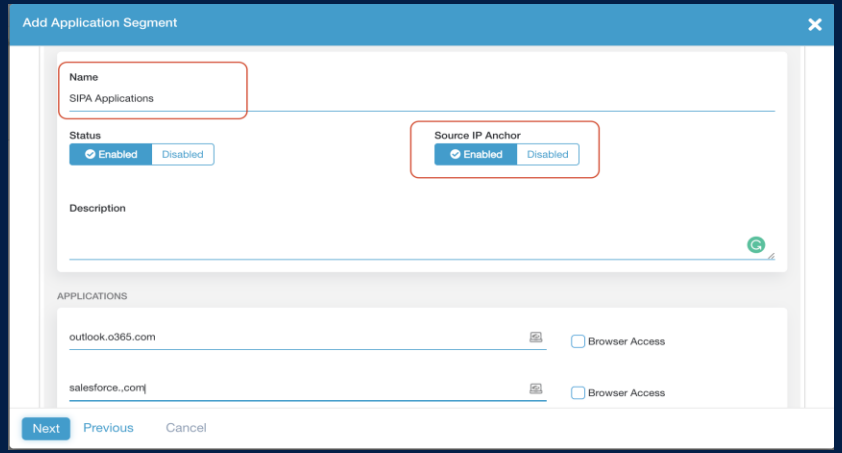
Tenant Bonding Between ZIA and ZPA

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



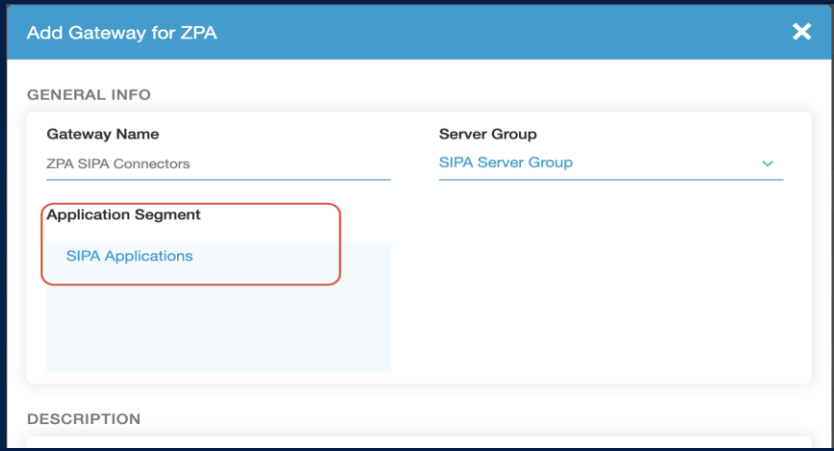
Interaction between ZIA and ZPA Tenants

ZPA UI



REST API

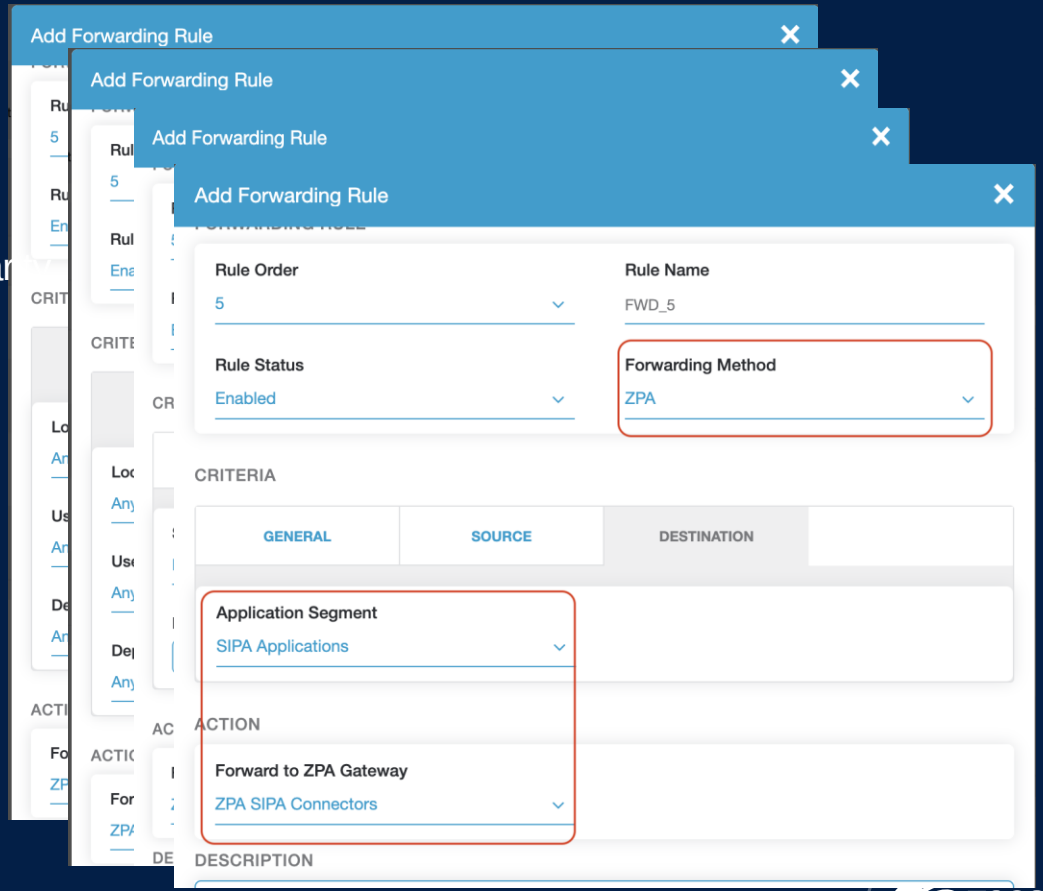
ZIA UI



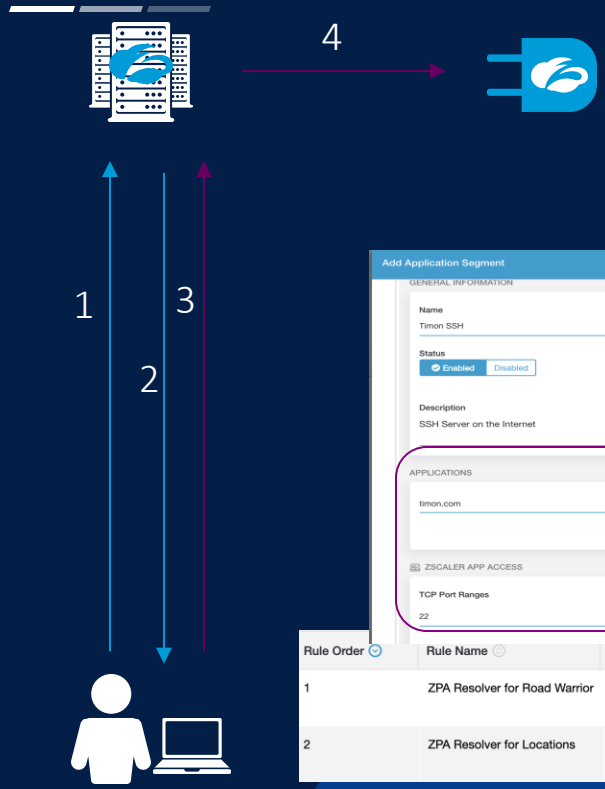
- Rest API based connectivity
- ZIA will fetch all Application Segments which has “Source Ip Anchor” flag enabled
- App segments and server group combinations are available to configure on ZIA

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/HTTPs and Web



1. User Makes DNS A-query for timon.com

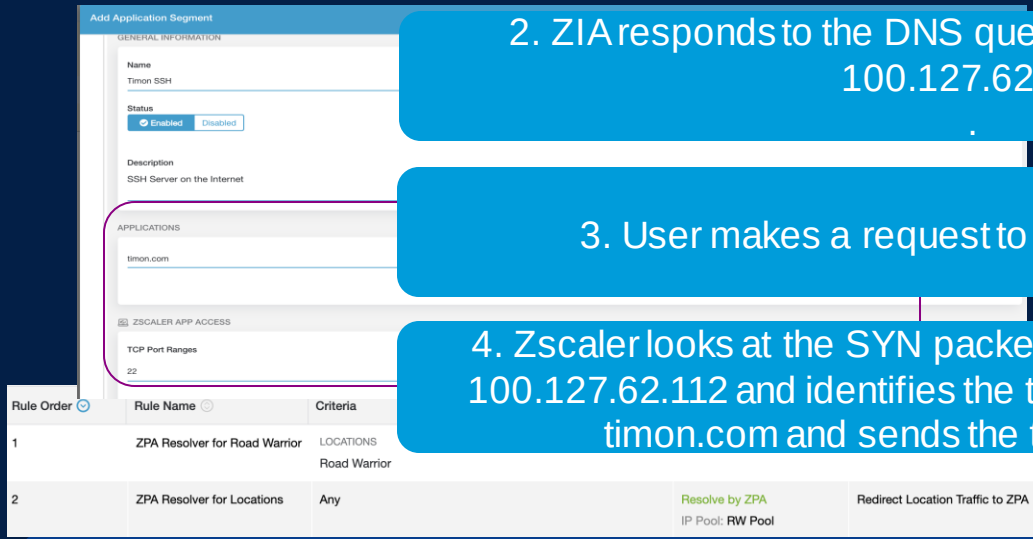
1a. The ZIA ZEN evaluates the Forwarding policies and checks and finds out that timon.com is defined as a SIPA application on ZPA.

2. ZIA responds to the DNS query with an Ephemeral IP 100.127.62.112

.

3. User makes a request to 100.127.62.112:22.

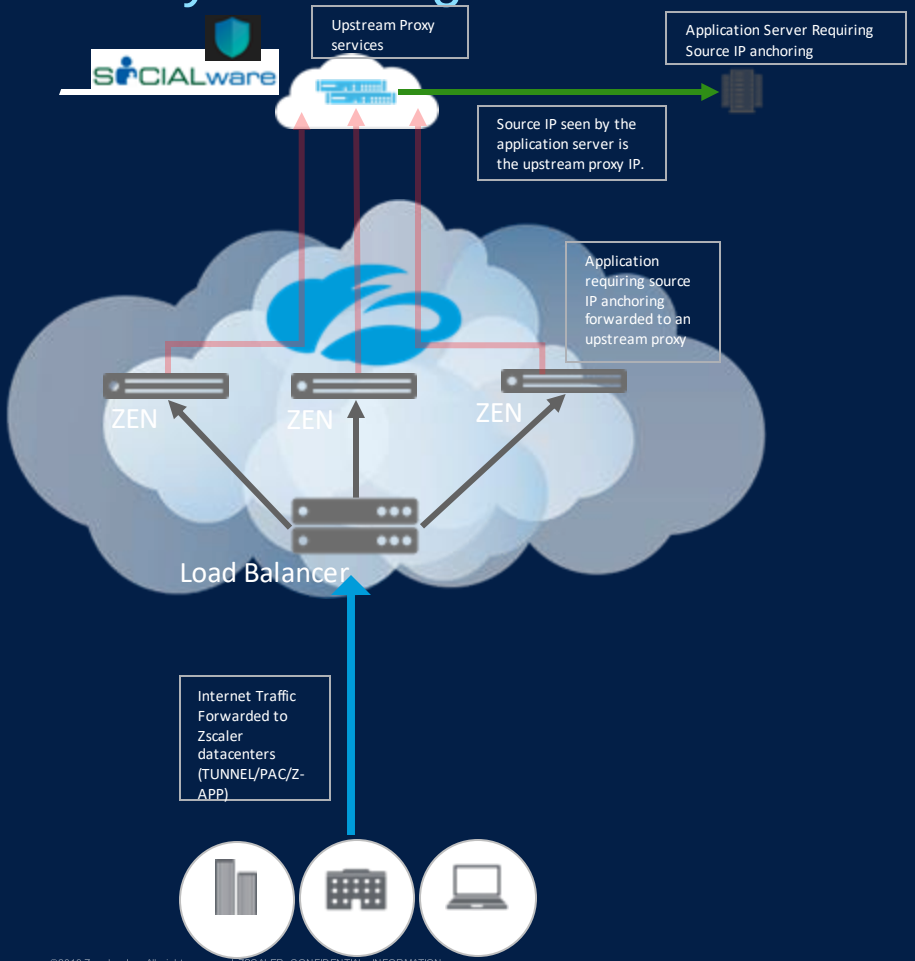
4. Zscaler looks at the SYN packet with the destination IP as 100.127.62.112 and identifies the traffic as traffic destined for timon.com and sends the traffic over to ZPA.



Auto Created DNS Policies

Note: This method is used only for Non HTTP/HTTPS traffic. The domai
HTTP/HTTPS traffic is destined to is identified by looking at the GET/CONNECT or SNI.

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

- IOCs
- ENDPOINT POSTURE

Zscaler API | Falcon API

ENDPOINT DETECTION & RESPONSE

CROWDSTRIKE AGENT

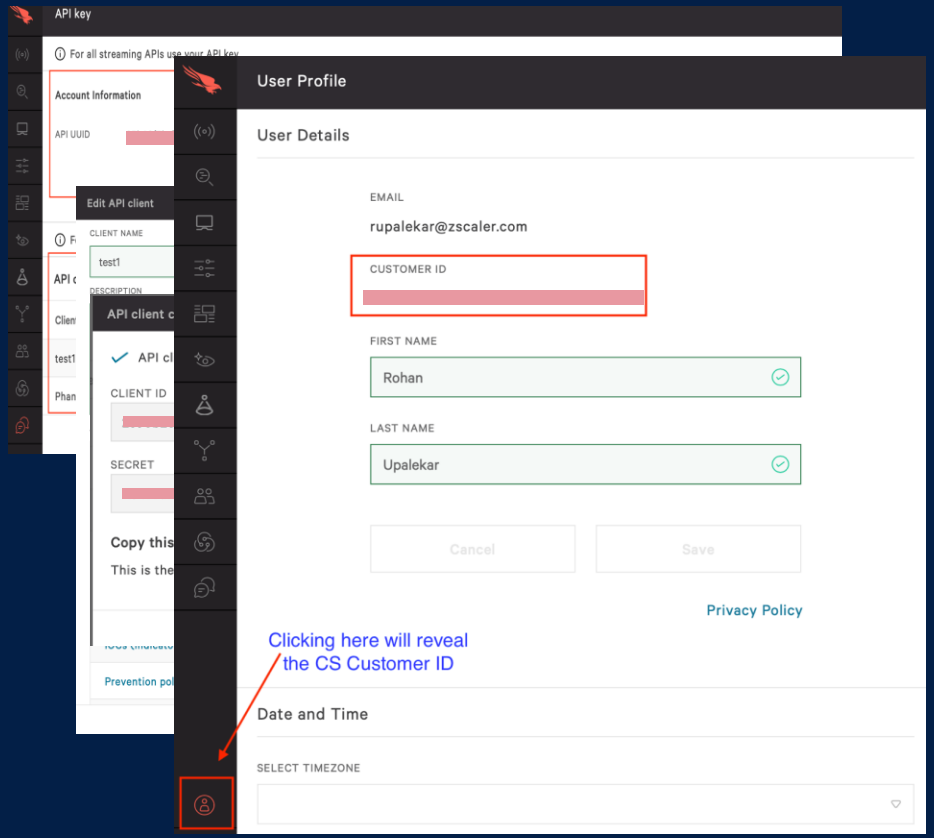
Z-APP

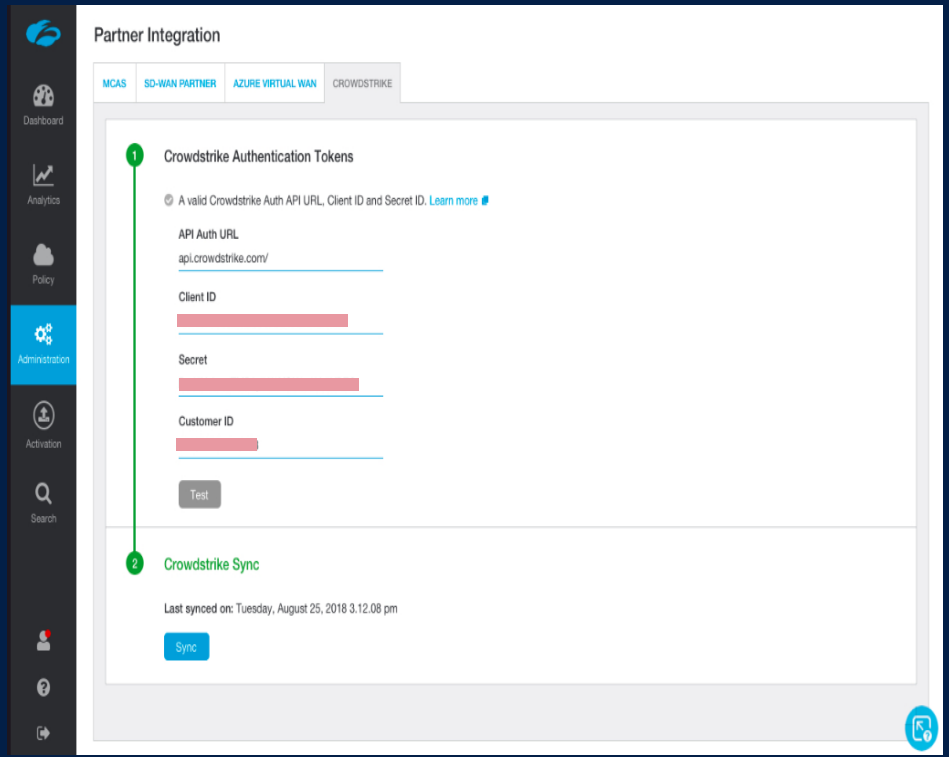
BEHAVIOR & POSTURE ANALYSIS

ENDPOINT INFORMATION

Threat detection and response across the Network and Endpoint

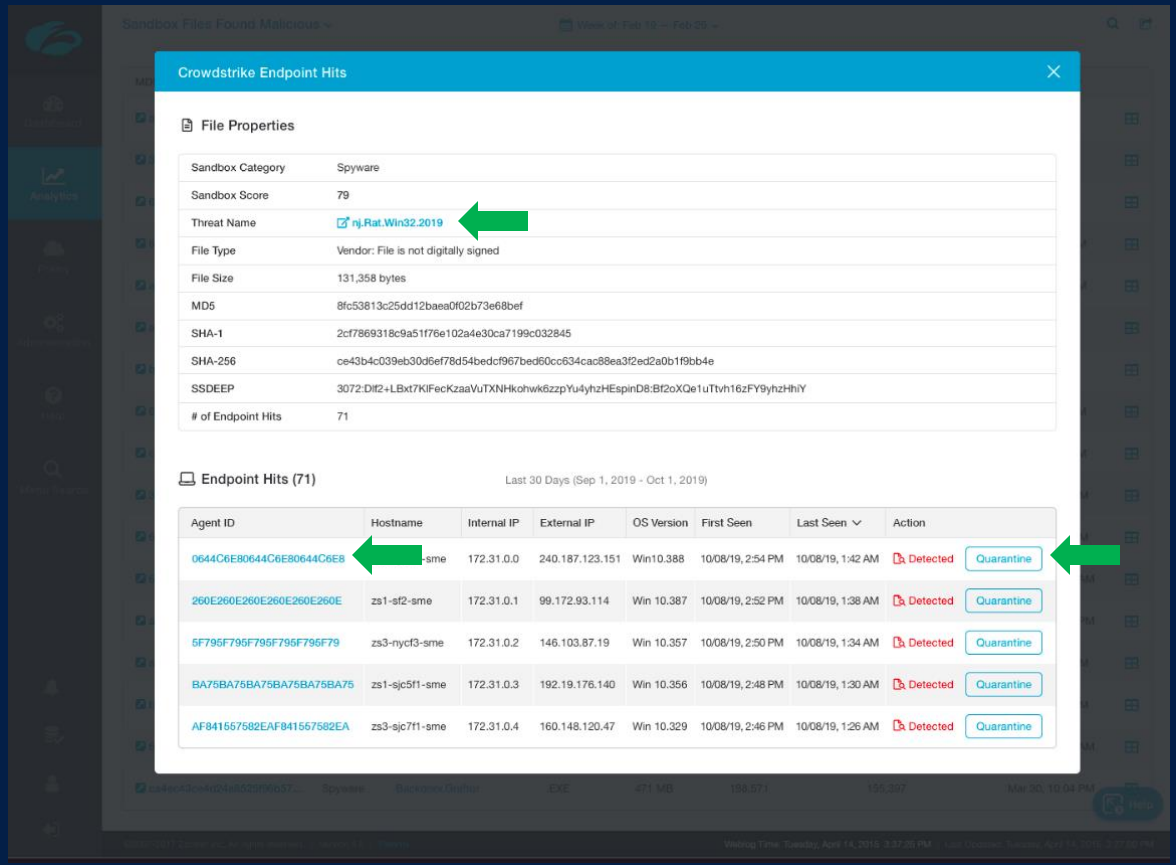
Easy One-time Setup





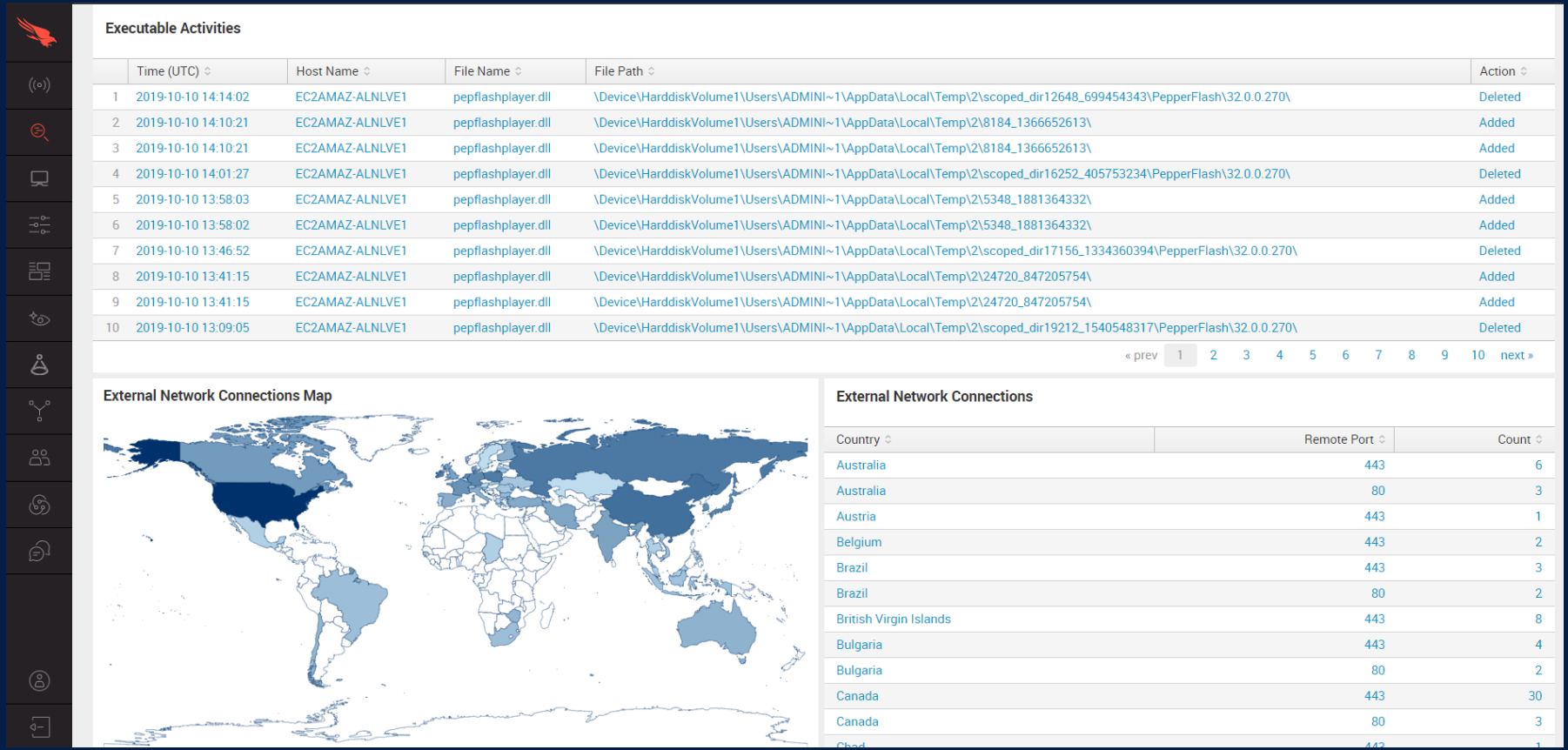
ZIA: Threat detection and response across the Network and Endpoint

Integrated Visibility and Response



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\32.0.0.270\	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\32.0.0.270\	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\32.0.0.270\	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\32.0.0.270\	Deleted

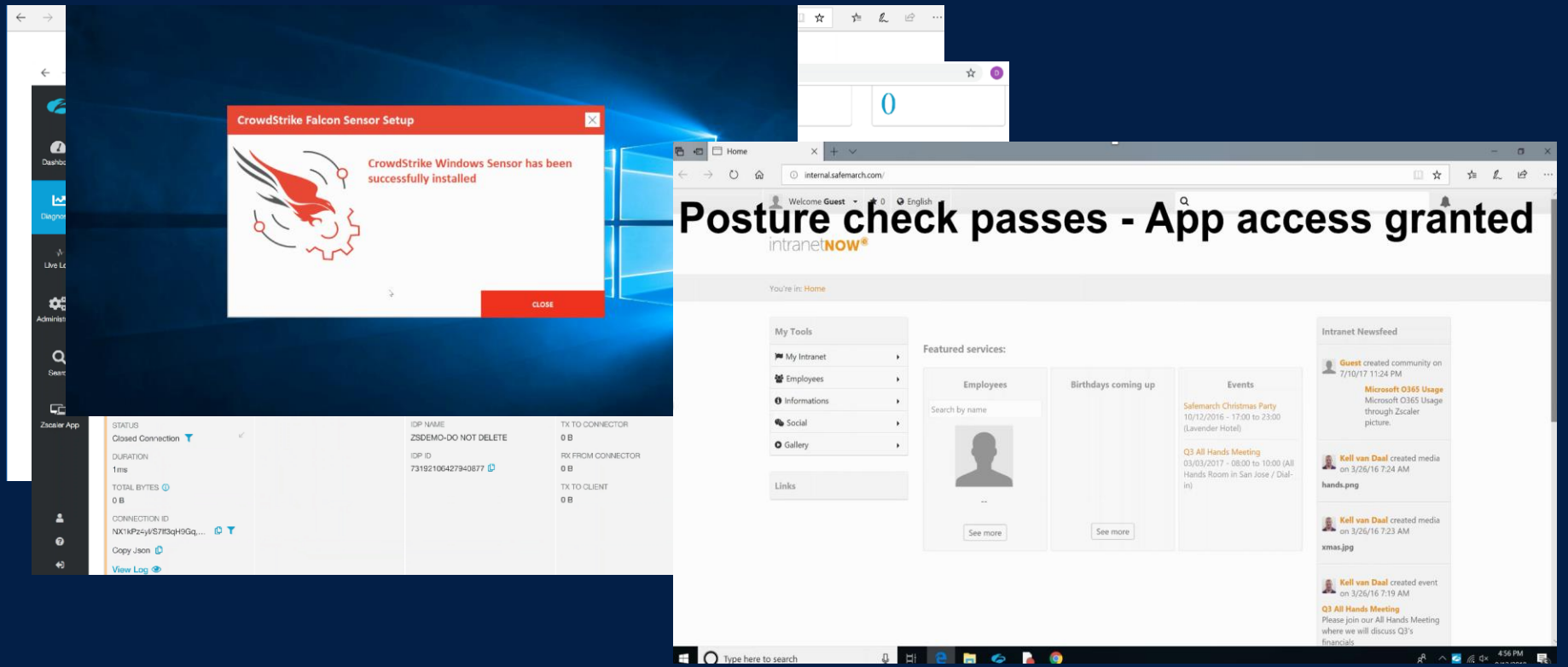
« prev 1 2 3 4 5 6 7 8 9 10 next »

External Network Connections Map

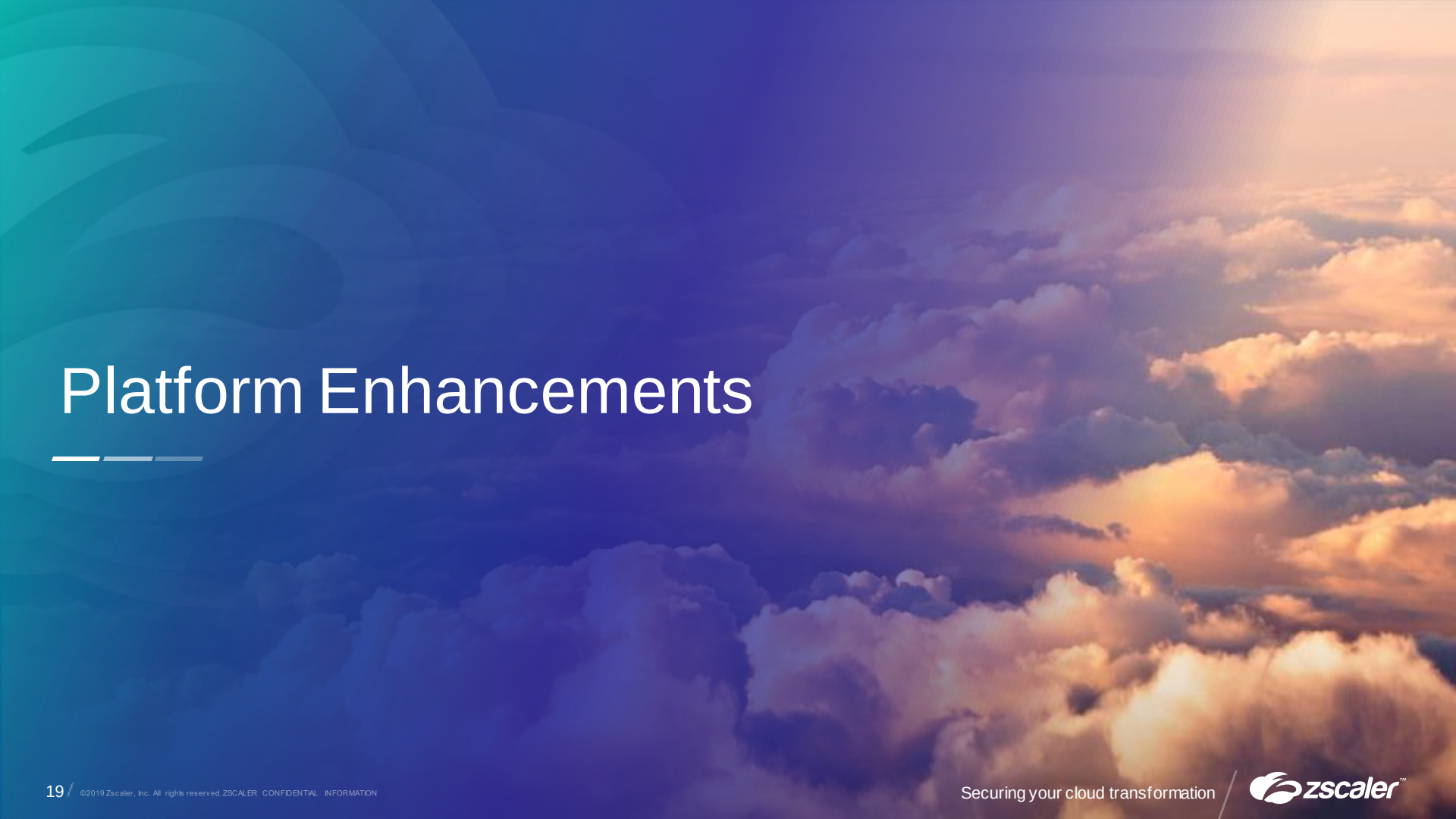
External Network Connections

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

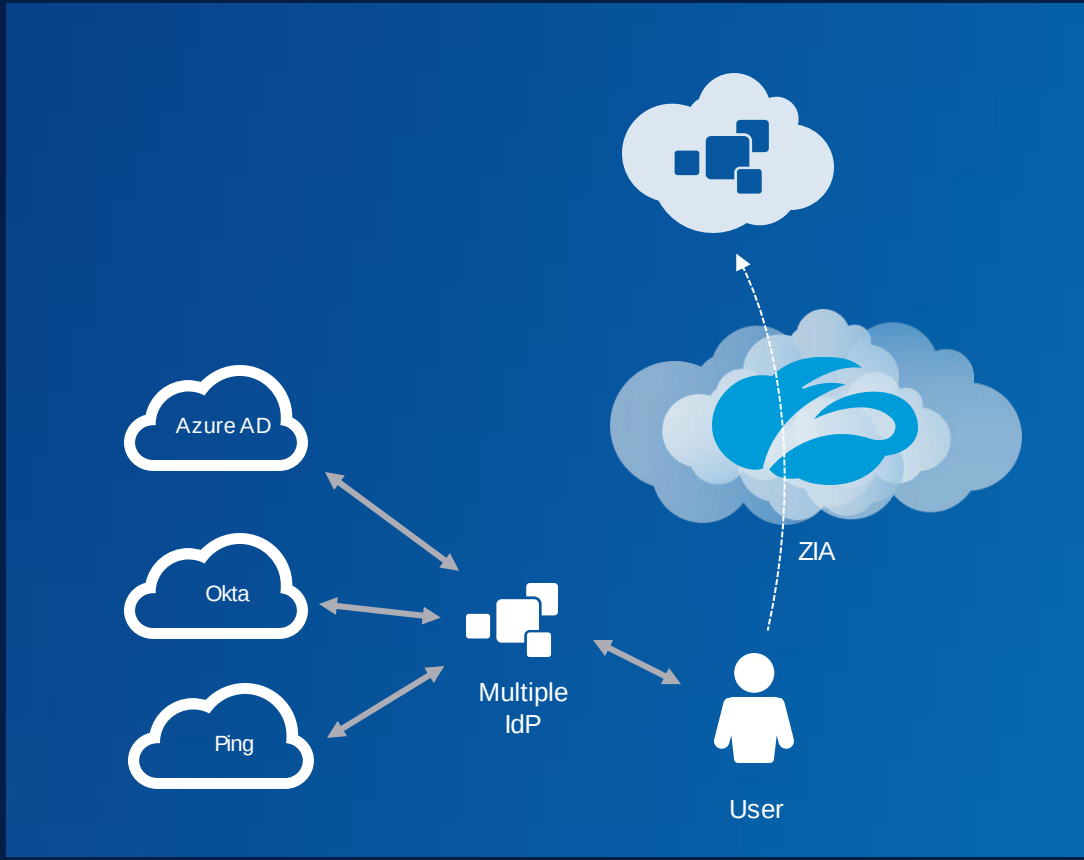


Platform Enhancements



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



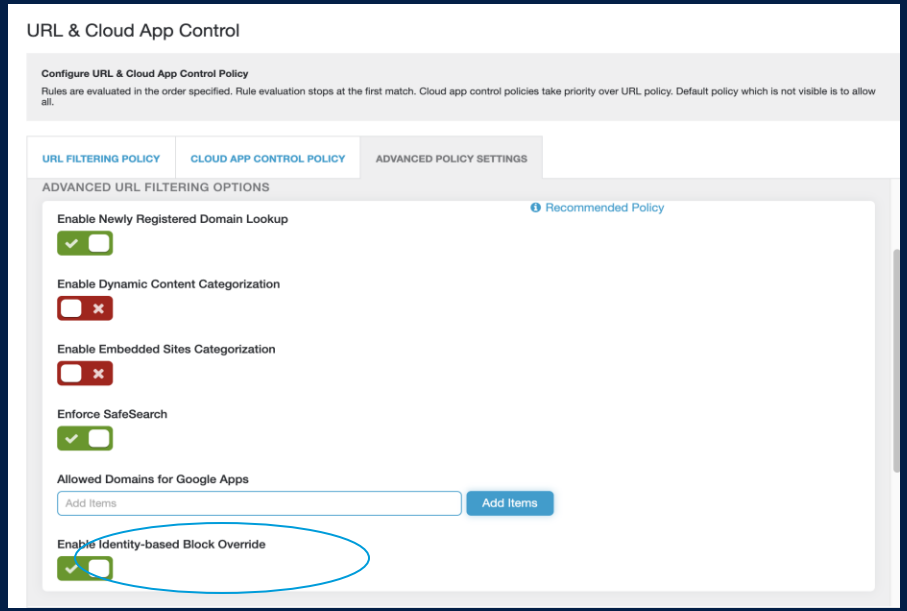
Support for Company Auth in Block Overrides for URL filtering

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

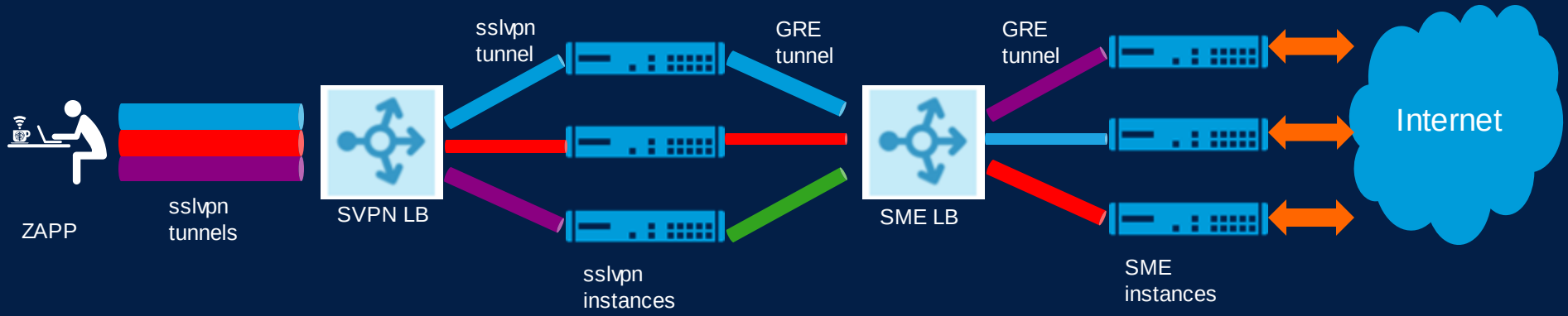
What

- 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

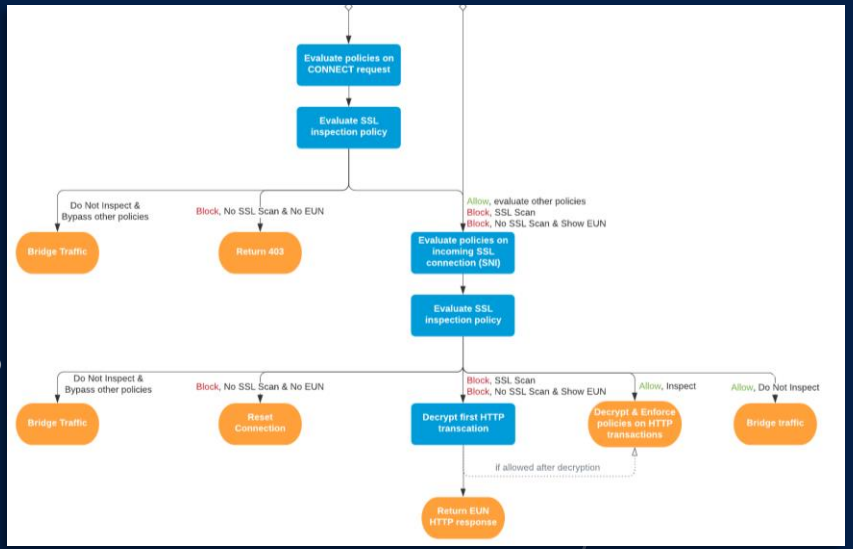
Why?

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

What?

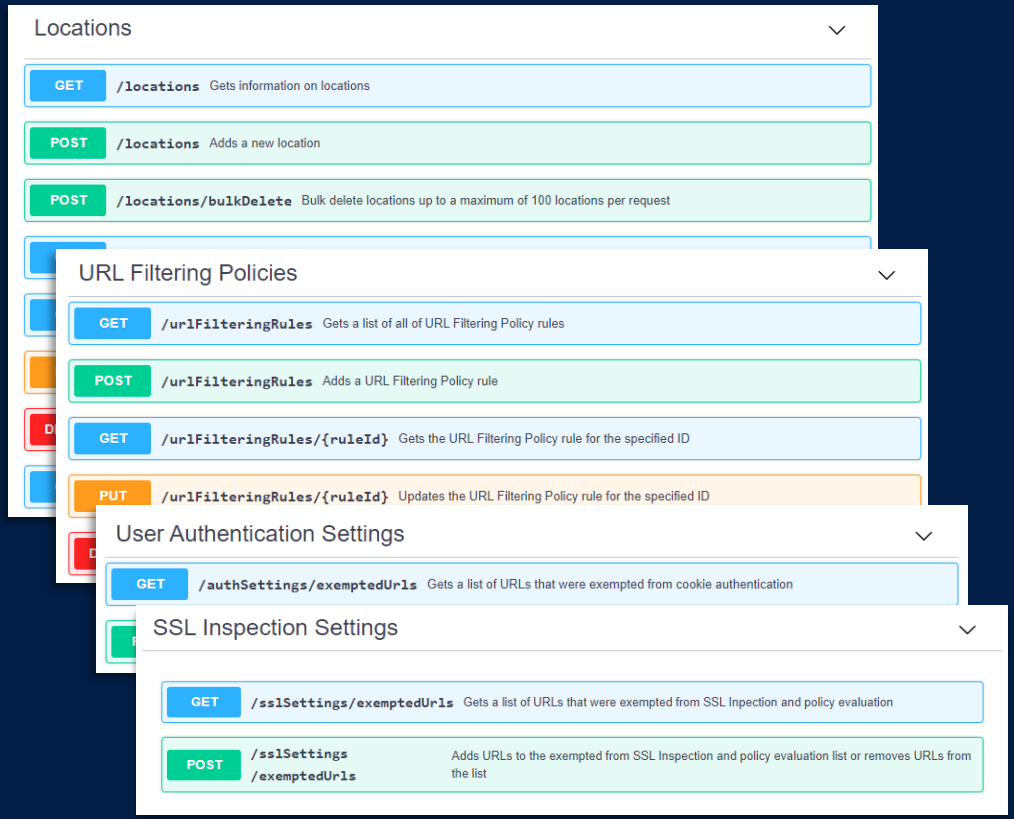
- New protocol types: HTTP-PROXY, TUNNEL-SSL
- Additional round of policy evaluation and weblog record for SSL session after CONNECT
- Support for common HTTP methods in URL policy
- More “N/A” in weblogs, since SSL session is not HTTP
- Granular SSL policy reason field (hidden initially)

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 Client Hello	SSL	Any / “N/A”
HTTP after SSL	HTTPS	Actual Method
Binary after SSL	TUNNEL-SSL	Any / “N/A”



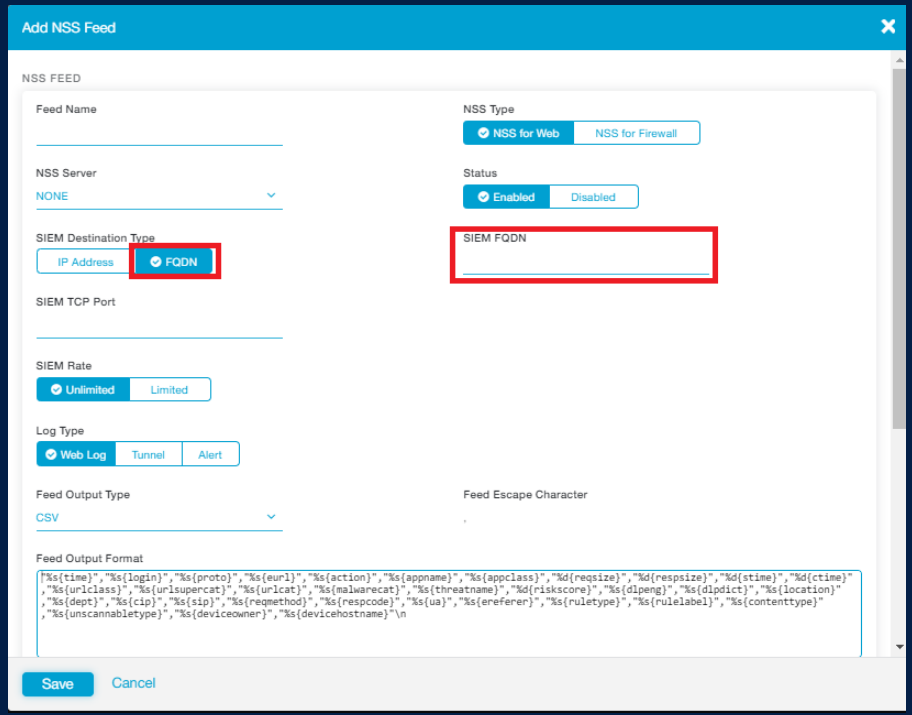
New Public APIs for customers and technology partners

- 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



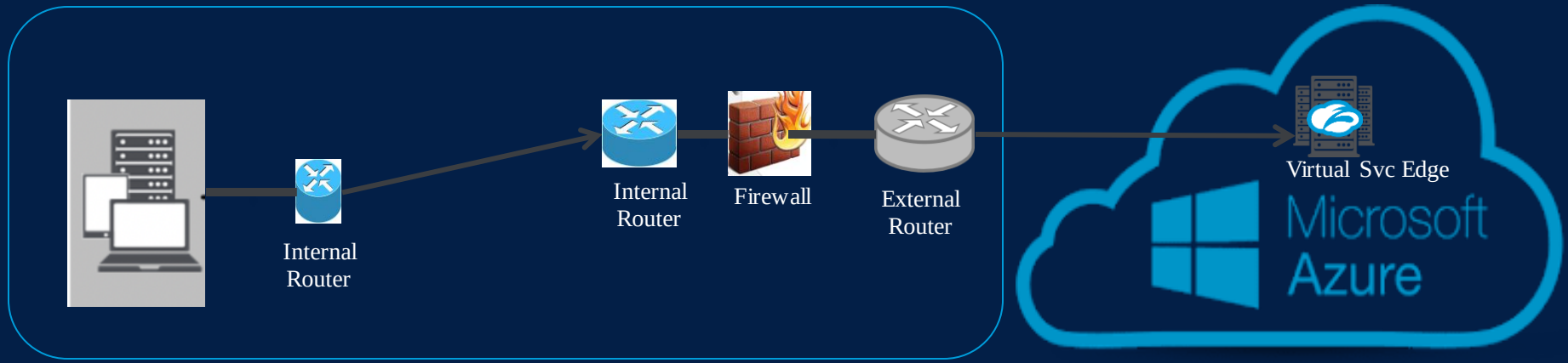
FQDN for NSS Feed Destination

- 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

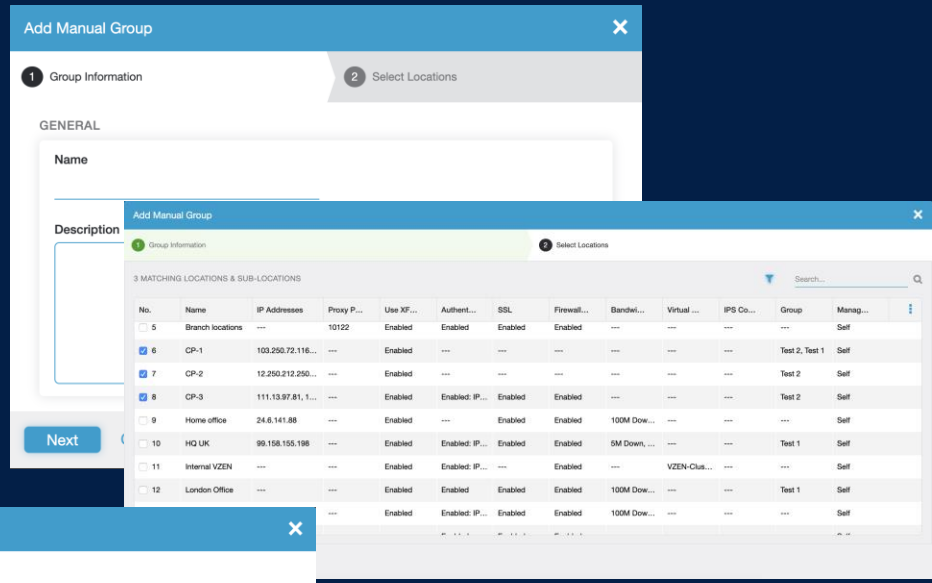
New

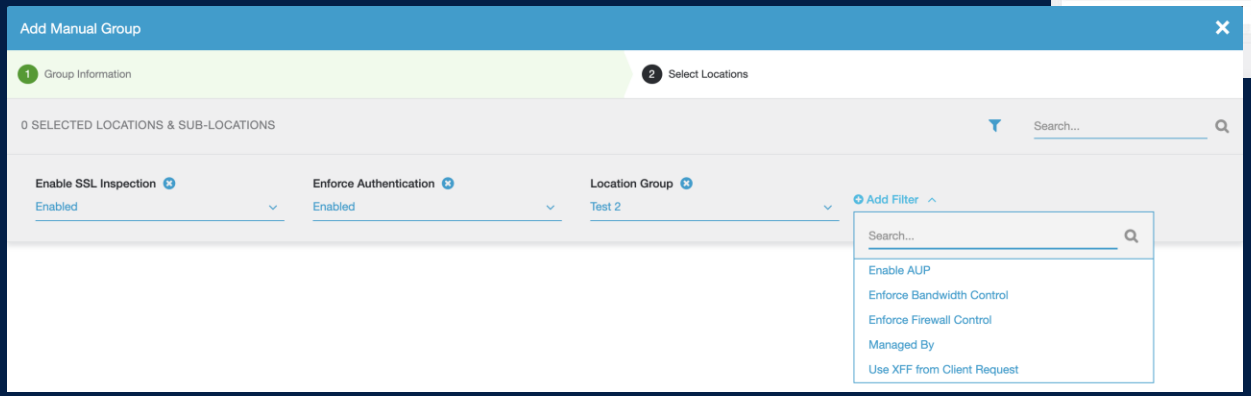


Policy & Access Control

Location Groups

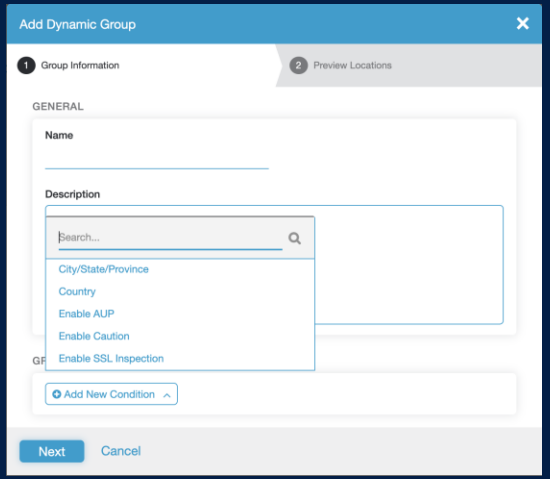
- Types of groups – Manual & Dynamic Groups
- **Manual Group**: Manually pick locations and/or sub-locations to add to the group.
  - Filter list: The list of locations to select from, can be filtered using

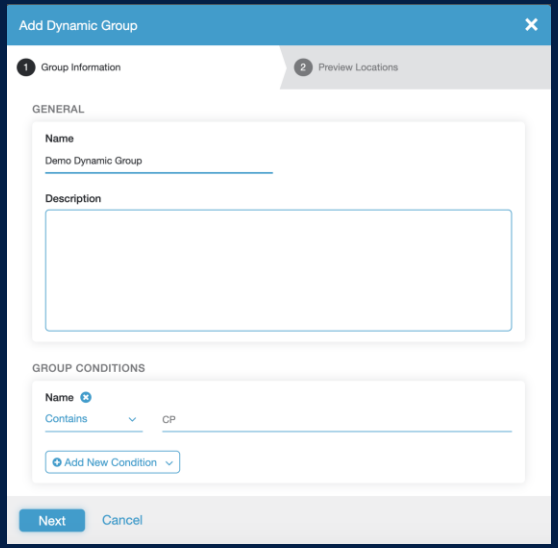


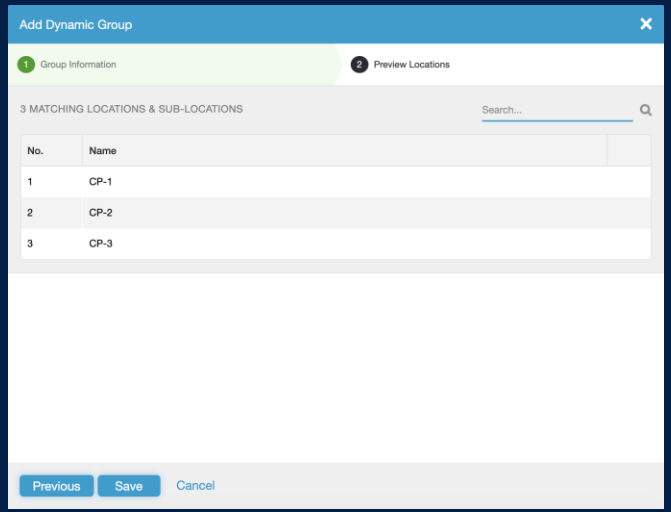


Location Groups

- **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.

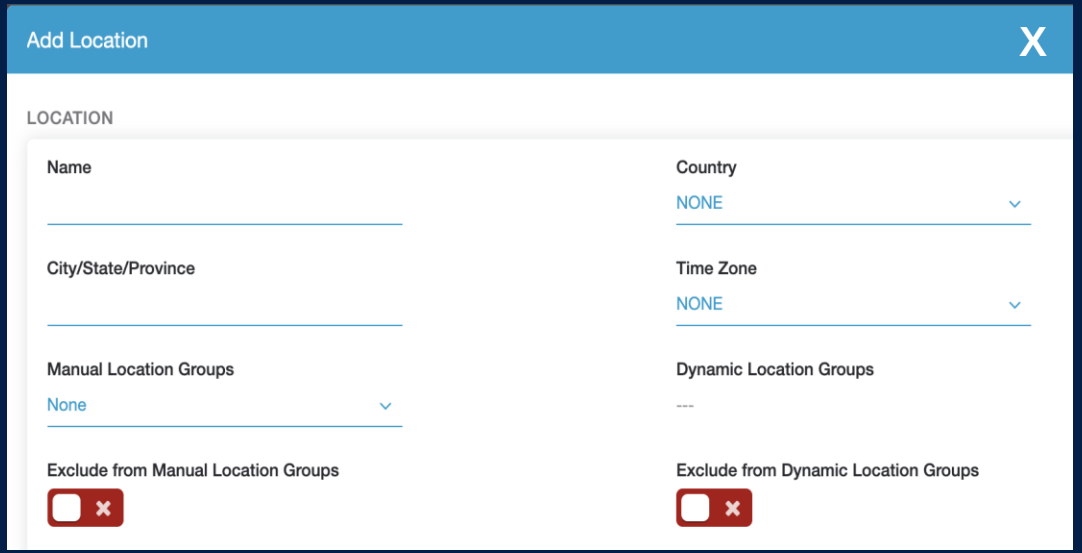






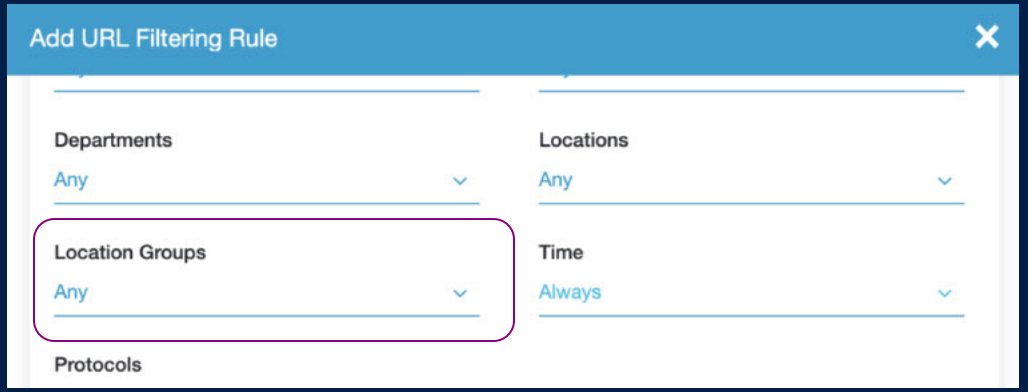
Location Groups

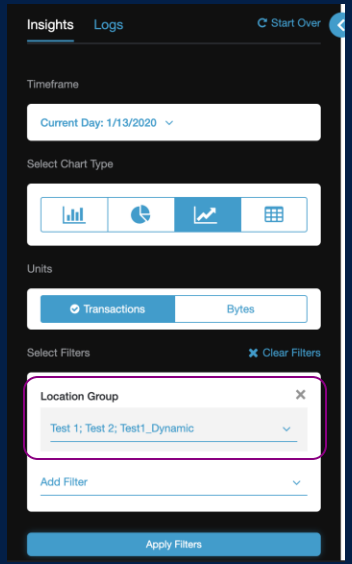
- **Location Attributes**
  - **Manual Location Groups**: Manage and view manual locations groups that this location or sub-location is a member of.
  - **Dynamic Location Groups**: View the dynamic location groups that this location/sub-location is a member of.
  - **Exclude from Manual Location Groups**: 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.

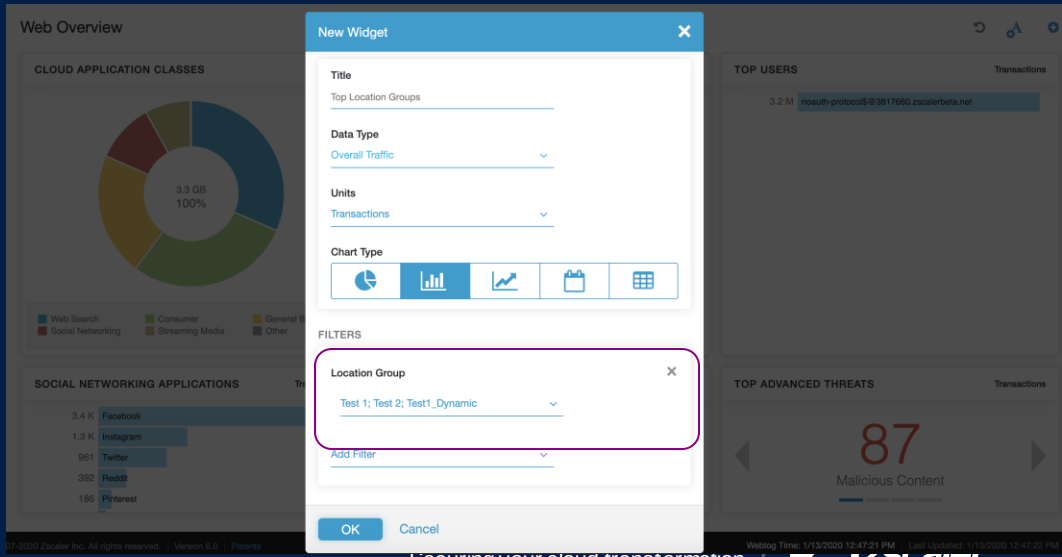


Location Groups

- **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**

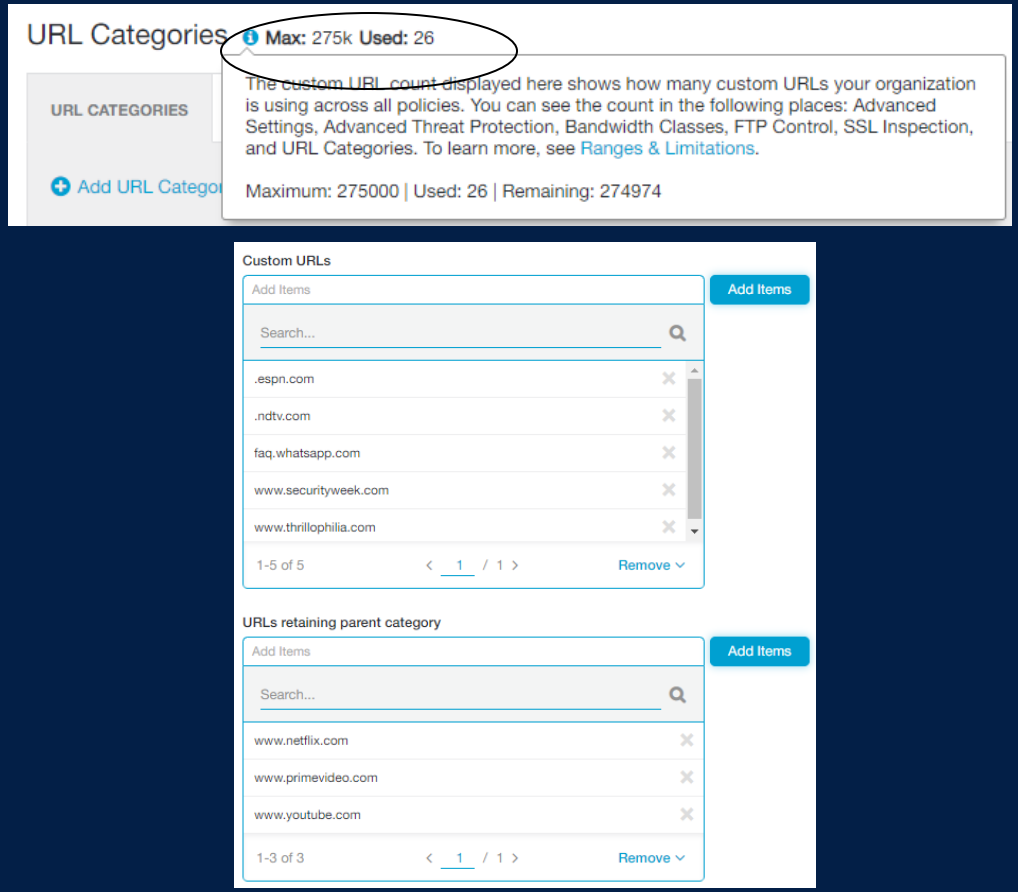






Custom URLs Limit Increase

- 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 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

External DB integrated in Zscaler

New 3rd party URL categorization engine

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

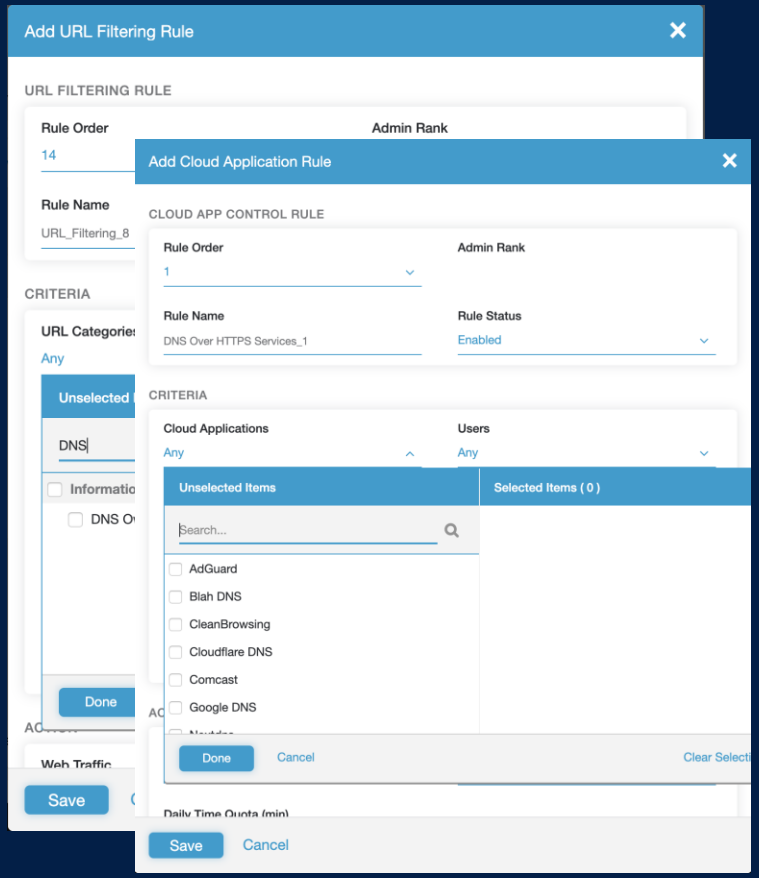
DNS over HTTPs (DoH) Support

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

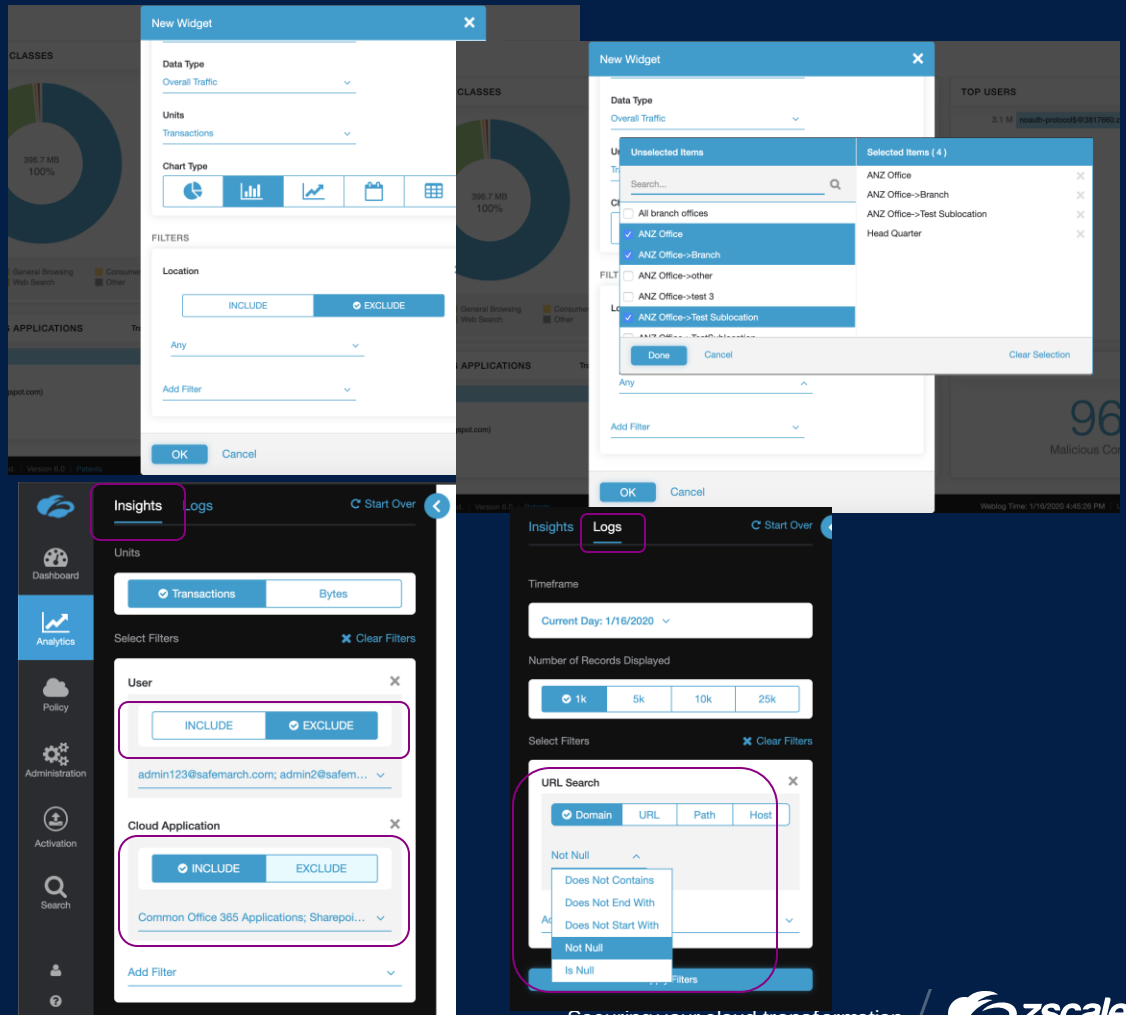
- *With SSL Inspection*:
  - Inspect GET and POST headers
  - Signature: based on MIME(content-type: application/dns-message or application/dns-json)

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.



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