1 Table of Contents

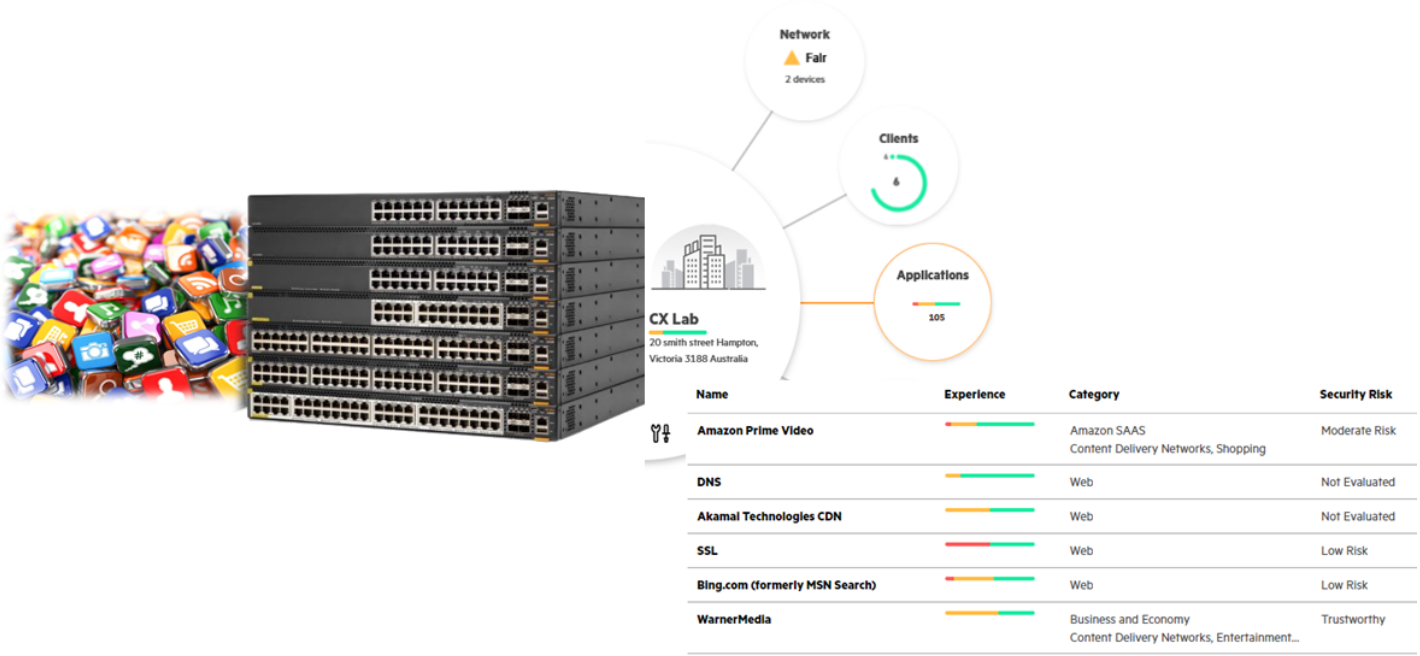
1 Table of Contents 1
1.1 Revision History 1
2 Application Recognition with CX Switches 2
2.1 Things you need 2
2.2 Assumptions 2
3 Application Recognition Configuration 3
3.1 App Recognition Modes 3
3.2 Port Level App Recognition with Fast Mode 3
3.3 IPFIX and Traffic Insight Configuration 5
3.4 IPFIX, Traffic Insight and Aruba Central Testing 7
3.5 Port Level App Recognition with Default mode 10
3.6 Application URLs 13
3.7 Best Practices 14

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
12 Oct 2024	0.1	Ariya Parsamanesh	Initial creation
20 Oct 2024	0.2	Ariya Parsamanesh	Added application URLs

2 Application Recognition with CX Switches

The Application Recognition and Control (ARC) is a relatively new feature in CX switches in which the switches perform Deep Packet Inspection (DPI) of the user traffic. Once the traffic is identified it then can be monitored and controlled. Currently it is supported on 6300 and 6400 switch series and for the latest iteration of the feature, you need to use 10.14.x firmware. In this technote I'll demonstrate ARC configuration and its application visibility information in New Aruba Central.



The advantages of ARC with Aruba Central are:

- It provides full layer 7 visibility of application (over 3,700) and various categories
- Display of application TLS version and certificate expiry date
- View connection establishment statistics
- Application based policy enforcement
- IPFIX integration to display flow statistics that can be exported to IPFIX collectors.
- Application summary card shows Top Application Categories
- Time travel support to display applications used at specific date and time.

2.1 Things you need

We need the following.

- Aruba 6300 or 6400 CX switches with 10.14.x firmware.
- Aruba Central account as IPFIX collector
- Foundational subscription for the switch.

2.2 Assumptions

- Here the CX switch is already added to Aruba Central account and has a valid subscription.
- The switch is configured for basic connectivity and is managed by Aruba Central.

3 Application Recognition Configuration

ARC feature uses DPI to identify the network apps and provides visibility and statistics to the administrator. The DPI engine runs on each line card in case of 6400 switches or stack member for 6300 series switches. It will process the first few packets of a TCP/UDP flow to identify the application. Even though IPFIX is not required for app-recognition to work, it is needed to report the flow statistics to the network administrator, IPFIX must be enabled since it exports the flow info to external/internal collector.

Traffic Insight (TI) is an internal IPFIX collector that monitors data collected from flow exporters like IPFIX and report. It can track multiple monitor requests simultaneously and displays it in the Switch WebUI and provides that info through APIs that Aruba Central uses.

Note that IPFIX is an open standard that is supported by many networking vendors. Except for a few additional fields added in IPFIX, the formats are nearly identical to Netflow.

Before we start, one should disable the following two feature

- IP Source lockdown – this is used to prevent IP source address spoofing on a per port basis
- IP Source lockdown resource extended – this is used to dynamically extend IP source lockdown hardware resources

It should be noted that, for Application visibility, one just need Aruba Central Foundational subscription for the switches, but Advance subscription is needed for Application control that includes generating client tags and building policies.

3.1 App Recognition Modes

There are two modes, one being the **default** mode and **Fast** mode. The main difference between the two is the number of packets required to recognise the applications. The default mode takes about 6 packets while the fast mode takes about 2 packets which results in 50mSec faster time to recognise an application.

Note that with Fast mode, the following application info will not be captured while it is captured with the default mode.

- TLS attributes
- DNS reason code
- URL

3.2 Port Level App Recognition with Fast Mode

ARC can be enabled on a port level and on a role level. Here are the 6300 configuration you need to enable ARC at port level. Note that One does not enable it on the uplink ports. When using Fast mode, the Application name, category and descriptions are identified.

```
flow-tracking
    enable
!
app-recognition
    enable
    mode fast
!
interface 1/1/4-1/1/5
    description clients-ports
    no shutdown
    no routing
    vlan access 150
    app-recognition enable
    exit
```

Here is a quick show command to check if ARC is operational.

```
primary1-Stack# sh app-recognition

  Application Recognition Global Configuration
     Configuration status             : Enabled
     Operational status               : Disabled
     ABP Session Limit Exceed Action  : Drop New Flows
     Operational Mode                 : Fast
     Failure Reason                   : flow_tracking_oper_status_disabled

  Application Recognition Port Configuration

    Interface       User-config       Port-access-config      Oper-status
    -----------     -----------       ------------------      ----------
   1/1/1              Disabled            Disabled            Disabled
   1/1/2              Disabled            Disabled            Disabled
   1/1/3              Disabled            Disabled            Disabled
   1/1/4              Disabled            Disabled            Disabled
   1/1/5              Enabled             Disabled            Disabled
   1/1/6              Disabled            Disabled            Disabled

   <<<<<<<<<<<<<<<<<<<<< output removed >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
```

Notice that the operational status is disabled. That is because IP source lockdown is enabled by default that needs to be disabled.

```
primary1-Stack(config)# flow-tracking
primary1-Stack(config-flow-tracking)# enable
Warning: IP source lockdown extended mode needs to be disabled for
flow tracking feature to be operational
primary1-Stack(config-flow-tracking)#
```

Now we'll disable "IP source lockdown".

```
primary1-Stack(config)# no ip source-lockdown resource-extended
primary1-Stack(config)# flow-tracking
primary1-Stack(config-flow-tracking)# enable
primary1-Stack(config-flow-tracking)#
```

Let's check ARC again and this time, it is operation status is enabled as shown below.

```
primary1-Stack# sh app-recognition

  Application Recognition Global Configuration
     Configuration status             : Enabled
     Operational status               : Enabled
     ABP Session Limit Exceed Action  : Drop New Flows
     Operational Mode                 : Fast
     Failure Reason                   : NA

  Application Recognition Port Configuration

    Interface       User-config       Port-access-config      Oper-status
    -----------     -----------       ------------------      ----------
   1/1/1              Disabled            Disabled            Disabled
   1/1/2              Disabled            Disabled            Disabled
   1/1/3              Disabled            Disabled            Disabled
   1/1/4              Enabled             Disabled            Enabled
   1/1/5              Enabled             Disabled            Enabled
   1/1/6              Disabled            Disabled            Disabled

   <<<<<<<<<<<<<<<<<<<<< output removed >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
```

One can check the feature pack that indicates that we can use Application based Policy and recognition.

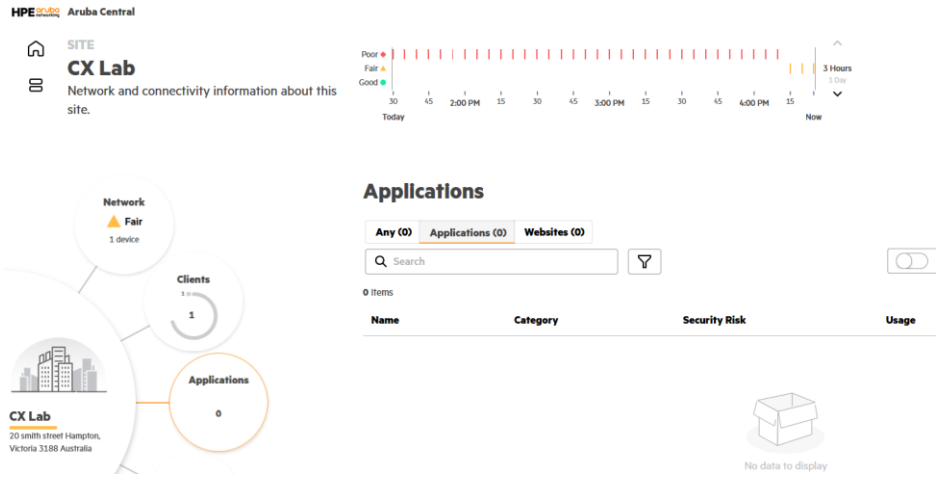
```
primary1-Stack# show feature-pack
```

```
Feature Pack Summary
====================
Name              : --
Expiration Date   : --
Serial Number(s)  : --
MAC Address       : --
Hostname          : --
Platform          : --
Type              : --
Mode              : --
State             : Subscription through Aruba Central is connected
Error Reason      : none
                                                    Subscription  Feature
Feature                                             Status        Status
-------------------------------------------------------------------------------
Application Based Policy                            active        allowed
Audio Video Bridging                                active        unsupported on SKU
Application Recognition                             active        allowed
MACsec extensions for WAN                           active        allowed
Reflexive Policies for Port Access GBP Clients      active        allowed
Reflexive Policies for Port Access Clients          active        allowed

primary1-Stack#
```

Now a client (10.150.0.46) is connected to interface 1/1/5, the flows should be visible with “show ip flow” command.

```
primary1-Stack# sh ip flows
Source IP            Dest IP           Source  Dest    Proto  VRF     App   App                        App
                                       Port    Port                   ID    Name                       Category
-------------------------------------------------------------------------------------------------------------------
10.150.0.46          192.168.1.131     51315   53      udp    default 32    dns                        network-service
44.240.0.217         10.150.0.46       443     50538   tcp    default 2328  twitch                     web
10.150.0.46          40.70.77.177      50574   443     tcp    default 1111  windows-marketplace        mobile-app-store
65.8.33.108          10.150.0.46       443     50532   tcp    default 205   tcp                        network-service
10.150.0.46          44.240.0.217      50538   443     tcp    default 2328  twitch                     web
74.125.68.188        10.150.0.46       5228    50326   tcp    default 1441  gtalk                      instant-messaging
40.70.77.177         10.150.0.46       443     50574   tcp    default 1111  windows-marketplace        mobile-app-store
10.150.0.46          74.125.68.188     50326   5228    tcp    default 1441  gtalk                      instant-messaging
34.212.147.224       10.150.0.46       443     50542   tcp    default 2328  twitch                     web
10.150.0.46          34.212.147.224    50542   443     tcp    default 2328  twitch                     web
10.150.0.46          192.168.1.131     58555   53      udp    default 32    dns                        network-service
192.168.1.131        10.150.0.46       53      51315   udp    default 32    dns                        network-service
10.150.0.46          192.168.1.131     64175   53      udp    default 32    dns                        network-service
10.150.0.46          151.101.66.214    50407   443     tcp    default 4     unknown                    standard
<<<<<<<<<<<<<<<<<<<<<< output removed >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

primary1-Stack#
```

Even though the flows are visible here in the CLI, it is not displayed in New Aruba Central



This is because we have not yet configured IPFIX exporter which is needed for Aruba Central to display the information.

3.3 IPFIX and Traffic Insight Configuration

As explained in the previous section, we need to configure IPFIX so that the flow information is available to Aruba Central using the API. To summarise

- ARC is applied and enabled on client-facing ports
- IPFIX is enabled for both client-facing and uplink ports
- IPFIX export app information and details to Traffic Insight which is an internal IPFIX collector

Traffic Insight supports 5 monitor types for 6300 CX switches: raw flows, topN flows, application-flows, DNS onboarding latency and DNS average latency.

Here we are creating the following monitors for traffic insight TI-01 profile, note that we have two TopN flows and that TopN-2 is "group-by" app-id. We'll see the difference in the show output commands. Finally you can have a maximum of 5x monitors defined in a traffic-insight like we do have here.

```
traffic-insight TI-01
    enable
    source ipfix
    monitor TopN-1 type topN-flows entries 20
    monitor TopN-2 type topN-flows entries 20 group-by appid
    monitor apps type application-flows
    monitor dns-avg-latency type dns-average-latency
    monitor dns-ob-latency type dns-onboarding-latency
```

You should note that there are three parts to Flow command

1. Flow Exporter >> 2. Flow Record >> 3. Flow Monitor

The flow Exporter and flow Record gets referenced in the flow Monitor which then gets applied to the interfaces. Then it is the flow Exporter that references Traffic Insight (internal IPFIX collector) that displays the information.

```
flow exporter app-vis-export
    description Export app data to central insight
    destination type traffic-insight
    destination traffic-insight TI-01
    template data timeout 30
    transport udp 2055  <<<<< you don't need this but gets added to the config

flow record app-vis-record
    description Record ipv4 flows for app visibility
    match ipv4 protocol
    match ipv4 version
    match ipv4 destination address
    match ipv4 source address
    match transport destination port
    match transport source port
    collect application name
    collect application dns response-code
    collect forwarding-status
    collect application https url
    collect application tls-attributes
    collect counter bytes
    collect counter packets
    collect timestamp absolute first
    collect timestamp absolute last

flow monitor app-vis-monitor
    cache timeout active 30
    exporter app-vis-export
    record app-vis-record
```

Now we have to apply the flow monitor app-vis-monitor to our uplinks and client access interfaces as shown below.

```
interface lag 256
    description to-core-sw
    no shutdown
    no routing
    ip flow monitor app-vis-monitor in
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active

interface 1/1/4-1/1/5
    no shutdown
    no routing
    vlan access 150
    app-recognition enable
    ip flow monitor app-vis-monitor in
```

3.4 IPFIX, Traffic Insight and Aruba Central Testing

Once this is done the flow information should get displayed in CLI, the local WebUI of the switch and Aruba Central. We'll start with the output of the CLI commands which you can execute using remote console through Aruba Central.

```
primary1-Stack# show traffic-insight TI-01 monitor-type topN-flows TopN-1

Name       : TopN-1
Group By   : None
Entries    : 20
Filter By  : None
Running Statistics Timeout   : 600
Dataset    : Running Statistics
Rank    srcip                    dstip            ipproto     srcport     dstport     appname     Bytes
-------------------------------------------------------------------------------------------------------
1       23.199.68.130            10.150.0.46      tcp         443         65353       abc-au      74991092
2       202.7.223.140            10.150.0.46      udp         443         51680       unknown     39219367
3       23.199.70.163            10.150.0.46      tcp         443         49540       akamai      17658164
4       199.232.210.172          10.150.0.46      tcp         80          49705       ms-edge     9982134
5       10.150.0.46              202.7.223.140    udp         51680       443         unknown     4825227
6       151.101.1.140            10.150.0.46      tcp         443         49623       reddit      3615832
7       104.97.188.138           10.150.0.46      tcp         443         65396       news-au     1353159
8       10.150.0.46              23.199.68.130    tcp         65353       443         abc-au      1096568
9       216.239.38.120           10.150.0.46      udp         443         58673       google-gen  1092148
10      151.101.129.140          10.150.0.46      tcp         443         49621       reddit      917547
11      142.250.70.206           10.150.0.46      udp         443         52205       google-gen  904636
12      151.101.81.91            10.150.0.46      udp         443         51934       fastly      810995
13      23.60.148.139            10.150.0.46      tcp         443         65403       news-au     776176
14      104.71.131.91            10.150.0.46      udp         443         57848       akamai      729269
15      204.79.197.220           10.150.0.46      tcp         443         49603       bing        681901
16      204.79.197.220           10.150.0.46      tcp         443         49548       bing        668993
17      104.71.131.91            10.150.0.46      tcp         443         49549       microsoft   576709
18      10.150.0.46              34.120.195.249   udp         55839       443         unknown     527923
19      99.86.212.44             10.150.0.46      tcp         443         49246       https       510930
20      142.250.70.230           10.150.0.46      udp         443         59282       google-gen  481372

primary1-Stack#
```

Note the difference between the two topN-flows outputs. As stated earlier, TopN-2 is configured with "group-by" app-id and here we see it sorted by App Id. This is to illustrate the flexibility of traffic insights.

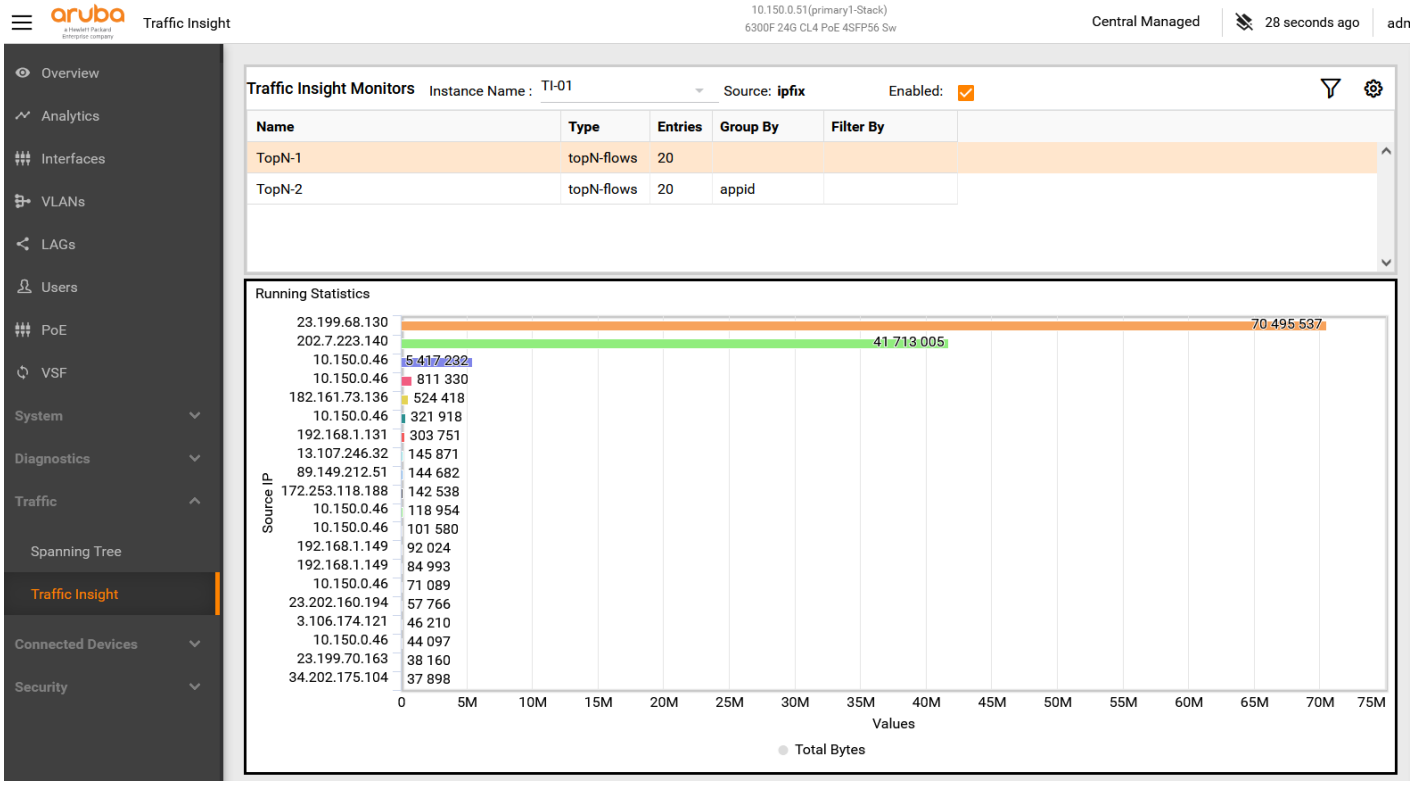
```
primary1-Stack# show traffic-insight TI-01 monitor-type topN-flows TopN-2

Name       : TopN-2
Group By   : appid
Entries    : 20
Filter By  : None
Running Statistics Timeout   : 600

Dataset    : Running Statistics
Rank    appid       Bytes
```

```
-----------------------------------
1        2537          76195357
2        4             48423797
3        1284          18925604
4        4355          10289007
5        943           5251133
6        1479          4917244
7        2199          2555752
8        68            2415562
9        547           1804050
10       2660          955342
11       2821          833683
12       968           701214
13       2531          547357
14       2652          505734
15       2599          360347
16       2524          348312
17       32            342595
18       1288          324168
19       247           309203
20       2484          262064

primary1-Stack#
```

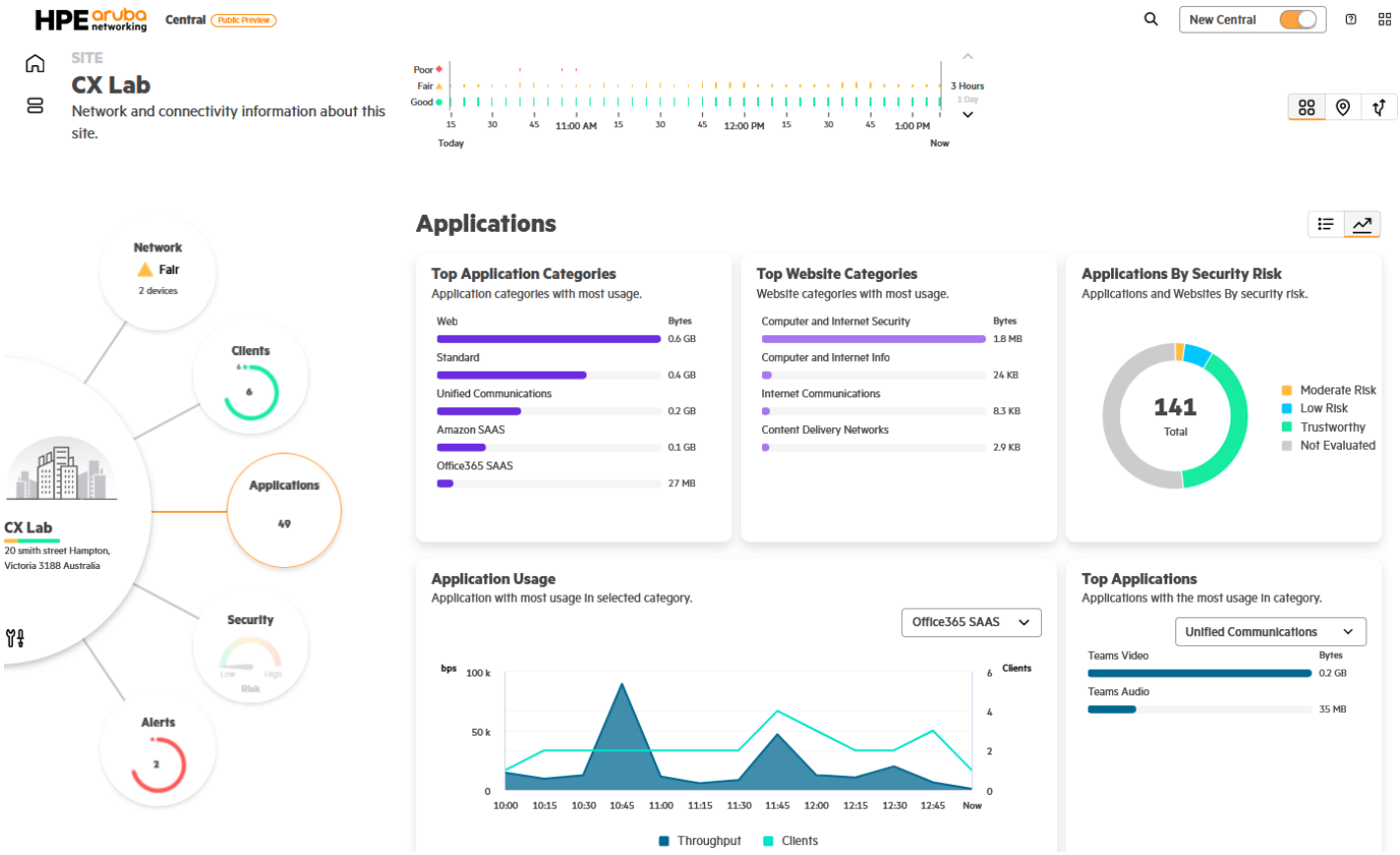
One can also use “filter-by” option either on its own or along with “group-by” like this example.

```
traffic-insight TI-example
   enable
   source ipfix
   monitor mon1-example type topN-flows group-by appid filter-by dstport 443
```

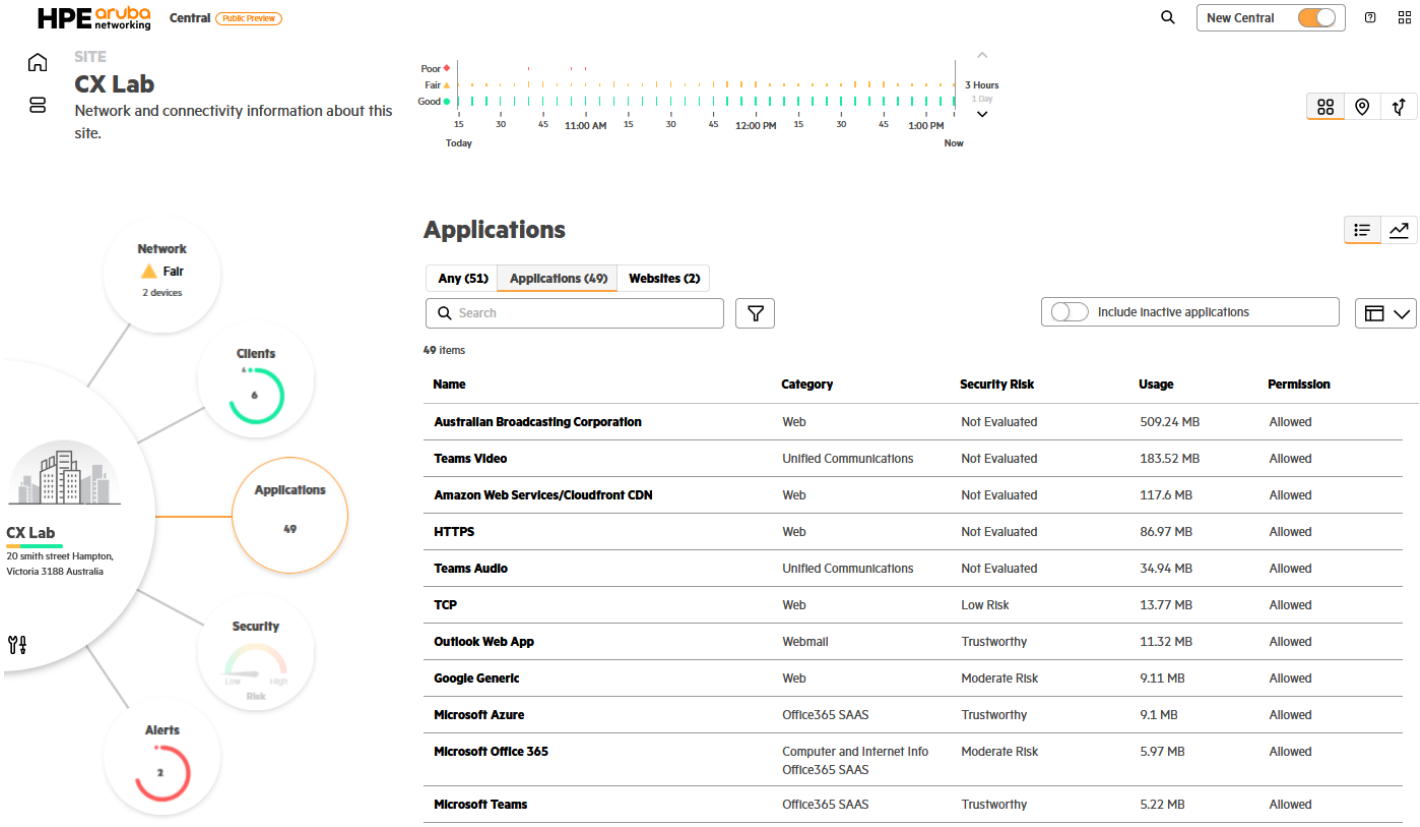
Next we browse to it and after login you need to go to Traffic Insight as shown below.



Soon after this info should also be visible in the New Central.



Note that Web site categories and application security is performed by DPI/WebCC functionalities on APs and gateways and not CX switches. Application Visibility can also be viewed from the Client context. And here is the table view where you can sort and search for specific application, etc.



3.5 Port Level App Recognition with Default mode

Here we'll change the application recognition mode from fast to default. This is so that we can get more information from the DPI than the 5x tuple, like the URL and TLS attributes of the flow.

```
app-recognition
    enable
    mode default
```

With this change we can do a quick check with the following command to ensure it is using default mode.

```
primary1-Stack# sh app-recognition

  Application Recognition Global Configuration
     Configuration status             : Enabled
     Operational status               : Enabled
     ABP Session Limit Exceed Action  : Drop New Flows
     Operational Mode                 : Default
     Failure Reason                   : NA

  Application Recognition Port Configuration

    Interface       User-config       Port-access-config      Oper-status
    -----------     -----------       ------------------      ----------
   1/1/1              Disabled            Disabled            Disabled
   1/1/2              Disabled            Disabled            Disabled
   1/1/3              Disabled            Disabled            Disabled
   1/1/4              Enabled             Disabled            Enabled
   1/1/5              Enabled             Disabled            Enabled
   1/1/6              Disabled            Disabled            Disabled
   <<<<<<<<<<<<<<<<<<<< output removed >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
```

Now that we have enabled default mode, we should be able to see the TLS attributes and URLs.

```
primary1-Stack# show traffic-insight TI-01 monitor-type application-flows apps ?
  app-details          Shows traffic insight flows with application details.
  client-role          Shows role assigned to the client.
  denied               Specifies traffic insight flows that are denied
  permitted            Specifies traffic insight flows that are permitted
  tls-cert-visibility  Shows traffic insight flows with application TLS Certificate Visibility.
  tls-visibility       Shows traffic insight flows with application TLS Visibility.
  url-details          Shows traffic insight flows with application URL details.
```

This is to display the TLS information.

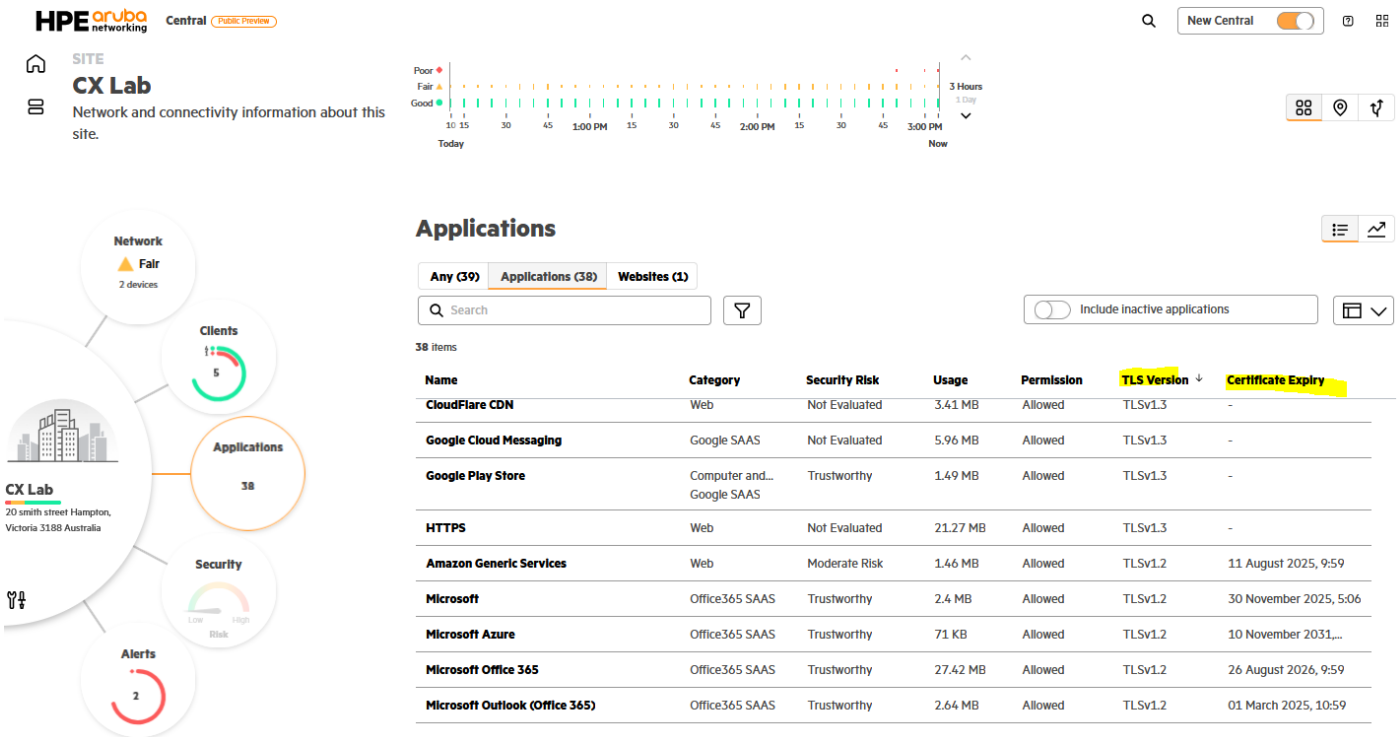
```
primary1-Stack# show traffic-insight TI-01 monitor-type application-flows apps tls-visibility
Name           : apps
Type           : application-flows

client_mac          src_ip                  dest_ip                 app_name                tls_version
next_protocol       bytes(Rx+Tx)
-------------------------------------------------------------------------------------------------------------
28:d2:44:52:c2:38   10.150.0.46             172.172.255.218         microsoft               TLSv1.2
-                   28293
28:d2:44:52:c2:38   10.150.0.46             10.150.0.255            Unrecognized            -
-                   243
28:d2:44:52:c2:38   10.150.0.46             52.167.163.114          windows-marketplace     TLSv1.2
HTTP/2              5732
28:d2:44:52:c2:38   10.150.0.46             142.251.221.67          google-gen              -
-                   9407
28:d2:44:52:c2:38   10.150.0.46             89.149.212.51           https                   TLSv1.3
-                   624246
28:d2:44:52:c2:38   10.150.0.46             54.153.189.86           amazon                  TLSv1.2
-                   130988
28:d2:44:52:c2:38   10.150.0.46             54.253.69.181           nielsen                 TLSv1.2
HTTP/2              2898
28:d2:44:52:c2:38   10.150.0.46             54.174.200.5            amazon                  TLSv1.3
-                   25333
<Output removed>
-------------------------------------------------------------------------------------------------------------
Total Traffic      : 142927808(bytes)
```

```
Encrypted Traffic  : 142927808(bytes)
Percentage of Encrypted Traffic : 100.000000

primary1-Stack#
```

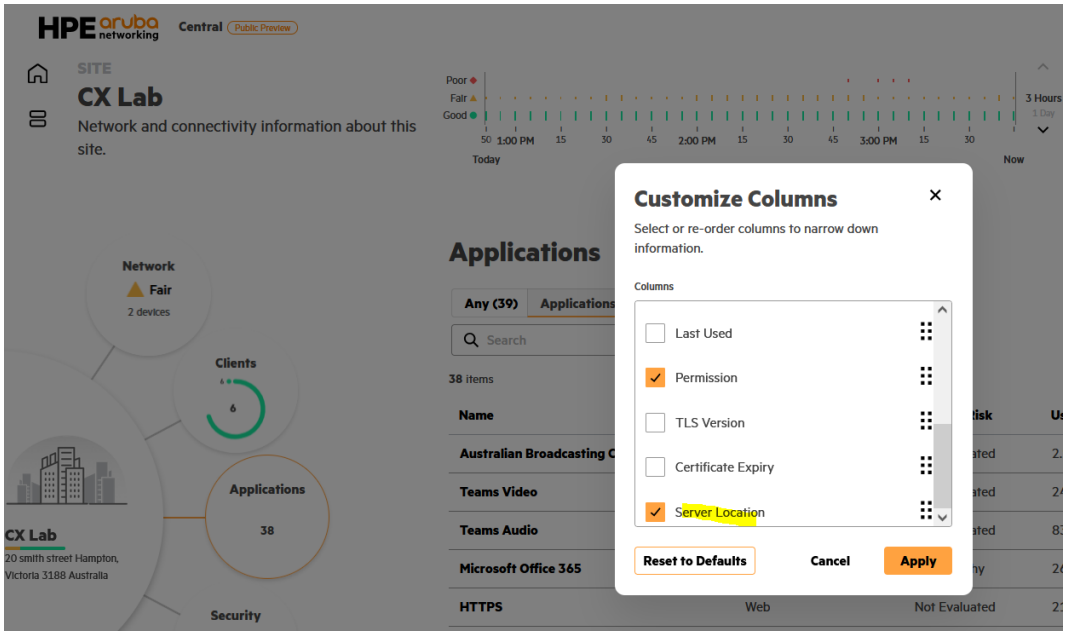
This is to display Server certificate information.

```
primary1-Stack# show traffic-insight TI-01 monitor-type application-flows apps tls-cert-visibility
Name            : apps
Type            : application-flows

client_mac         src_ip                    dest_ip                   app_name          cert_issuer
cert_issued_date      cert_expiry_date

(DD/MM/YY HH:MM:SS)   (DD/MM/YY HH:MM:SS)
-------------------------------------------------------------------------------------------------------
28:d2:44:52:c2:38  10.150.0.46               18.155.88.113             amazon            -
-                     -
28:d2:44:52:c2:38  10.150.0.46               104.19.158.19             cloudflare        GlobalSign Root
CA       15/11/23  03:43:21    28/01/28  00:00:42
28:d2:44:52:c2:38  10.150.0.46               131.253.33.237            bing              -
-                     -
28:d2:44:52:c2:38  10.150.0.46               204.79.197.239            ms-edge           Microsoft Azure
RSA TLS  16/07/24  11:56:27    11/07/25  11:56:27
28:d2:44:52:c2:38  10.150.0.46               23.34.236.111             news-au           DigiCert TLS RSA
SHA256   06/12/23  00:00:00    05/12/24  23:59:59
28:d2:44:52:c2:38  10.150.0.46               23.60.148.139             news-au           DigiCert TLS RSA
SHA256   06/12/23  00:00:00    05/12/24  23:59:59
28:d2:44:52:c2:38  10.150.0.46               34.124.209.251            simpli-fi         DigiCert Global
G2 TLS R 07/11/23  00:00:00    07/12/24  23:59:59
28:d2:44:52:c2:38  10.150.0.46               69.173.151.100            rubiconproject    DigiCert TLS RSA
SHA256   30/07/24  00:00:00    03/04/25  23:59:59
28:d2:44:52:c2:38  10.150.0.46               172.64.149.180            cloudflare        -
-                     -
28:d2:44:52:c2:38  10.150.0.46               13.107.21.239             ms-edge           Microsoft Azure
RSA TLS  16/07/24  11:56:27    11/07/25  11:56:27
28:d2:44:52:c2:38  10.150.0.46               23.34.236.194             pubmatic          DigiCert TLS RSA
SHA256   26/11/23  00:00:00    26/11/24  23:59:59
<Output removed>

primary1-Stack#
```

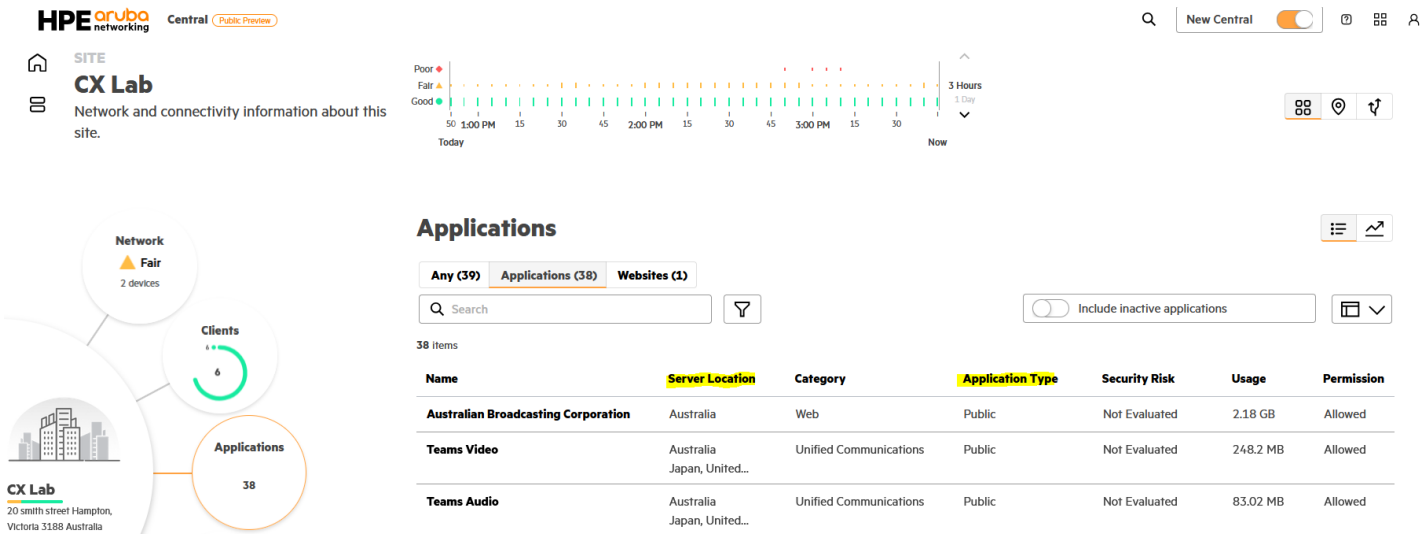
Here is the New Central view.



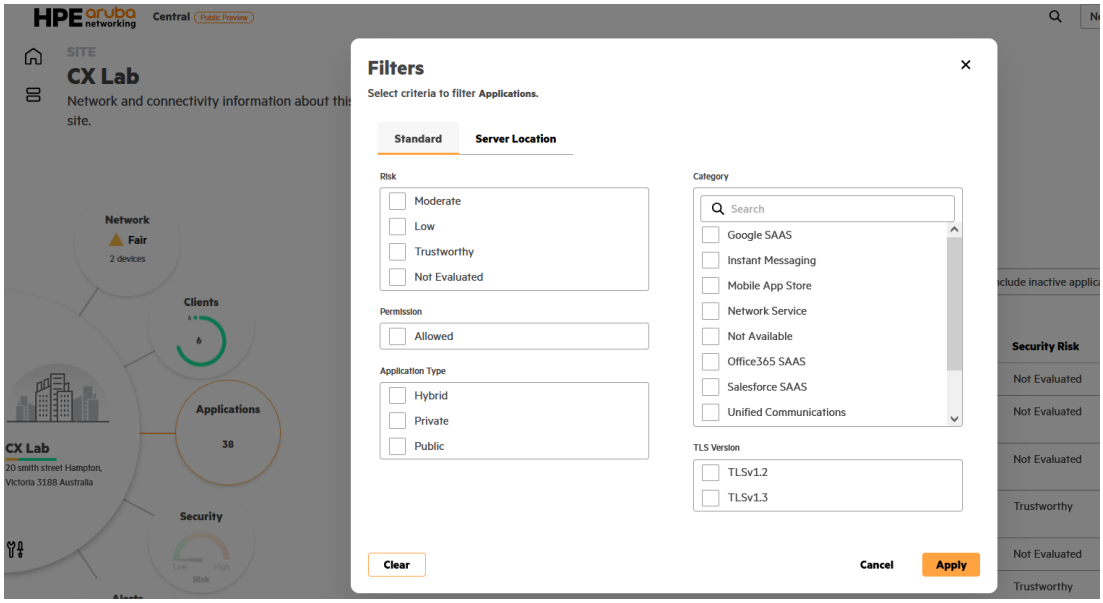
We can also get the geo location of the applications



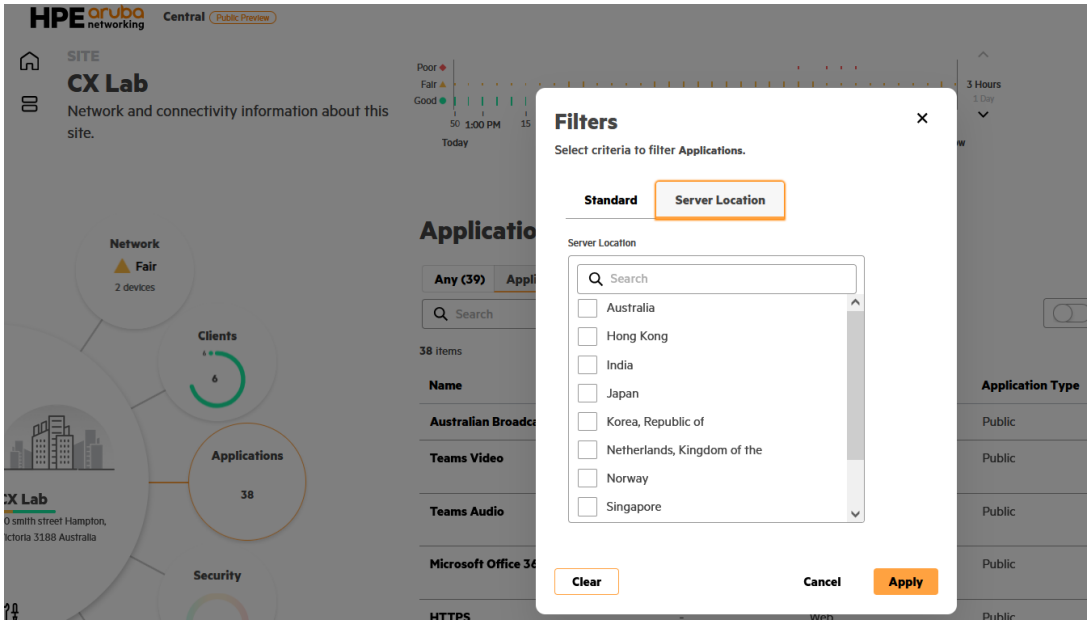
And once you apply the new customised columns, you get the geo locations.



There is also a comprehensive filtering options that gives you 2x options. One Standard and the other based on the application server geo-location. The standard option is shown below



And here is the Server location option that quickly allows you to filter on a specific location.



Finally you need to be aware of the capacities for the exact switch model when you are configuring Traffic Insight. You can use the following command to check.

```
primary1-Stack# show capacities traffic-insight

System Capacities: Filter TRAFFIC_INSIGHT
Capacities Name                                                                  Value
-------------------------------------------------------------------------------------
Maximum number of Traffic-insight application flow cache entries               75000
Maximum number of Traffic-insight application flow table entries                2000
Maximum number of Traffic-insight instances                                        1
Maximum number of Traffic-insight monitors                                         5
Maximum number of Traffic-insight TopN monitor reports                           100
Maximum number of Traffic-insight TopN monitor reports per monitor                20
Maximum number of Traffic-insight raw flow cache entries                        8000
Maximum number of Traffic-insight raw flow table entries                        5000
```

3.6 Application URLs

To show the URL info we need to use the diagnostic mode with the following CLI commands.

```
diagnostic
diag-dump flow-tracking basic
```

```
primary1-Stack# diagnostic
primary1-Stack# diag-dump flow-tracking basic
================================================================================
[Start] Feature flow-tracking Time : Mon Oct  7 16:53:47 2024
================================================================================
--------------------------------------------------------------------------------
[Start] Daemon ipfmd
--------------------------------------------------------------------------------

===  IPFMD Global data  ===
=========================================
 IPFM Global Configuration  : ENABLED
 MQTT Publisher Status      : CONNECTED
```

```
===  IPFMD Global FLOW Data  ===

=========================================
 Client MAC        SRC IP                  DST IP                  SRC Port  Dst Port  Proto  VRF  Agent  State   App Id  App URL
-------------------------------------------------------------------------------------------------------------------------------------------------
 28:d2:44:52:c2:38  10.150.0.46             192.168.1.131           63470     53        17     1    0      READY   32      ping.chartbeat.net
 94:60:d5:da:5a:20  23.60.148.119           10.150.0.46             443       63910     6      1    0      READY   2537    collector.abc.net.au
 28:d2:44:52:c2:38  10.150.0.46             69.173.158.92           49353     443       6      1    0      READY   2527    prebid-server.rubiconproject.com
 28:d2:44:52:c2:38  10.150.0.46             54.153.189.86           49587     443       6      1    0      READY   968     deliver.oztam.com.au
 28:d2:44:52:c2:38  10.150.0.46             142.250.70.238          55027     443       17     1    0      READY   943
 94:60:d5:da:5a:20  192.168.1.131           10.150.0.46             53        63470     17     1    0      READY   32      ping.chartbeat.net
 94:60:d5:da:5a:20  192.168.1.131           10.150.0.46             53        61818     17     1    0      READY   32      play.google.com
 28:d2:44:52:c2:38  10.150.0.46             142.250.70.142          57328     443       17     1    0      READY   943
 94:60:d5:da:5a:20  44.207.247.4            10.150.0.46             443       65482     6      1    0      READY   968     ping.chartbeat.net
 28:d2:44:52:c2:38  10.150.0.46             23.199.68.130           65353     443       6      1    0      READY   2537    abc-iview-mediapackagestreams-2.akamaized.net
 28:d2:44:52:c2:38  10.150.0.46             52.167.163.114          63903     443       6      1    0      READY   1111    *.prod.do.dsp.mp.microsoft.com
 28:d2:44:52:c2:38  10.150.0.46             202.7.223.140           51680     443       17     1    0      READY   4
 28:d2:44:52:c2:38  10.150.0.46             13.107.5.93             63906     443       6      1    0      READY   2821    *.exp-tas.com
 28:d2:44:52:c2:38  10.150.0.46             192.168.1.131           50036     53        17     1    0      READY   32      play.google.com
 94:60:d5:da:5a:20  89.149.212.51           10.150.0.46             443       65356     6      1    0      READY   68      infinity-c32.youboranqs01.com
 28:d2:44:52:c2:38  10.150.0.46             172.253.118.188         64659     5228      6      1    0      READY   2484    mtalk.google.com
 94:60:d5:da:5a:20  202.7.223.140           10.150.0.46             443       51680     17     1    0      READY   4
 28:d2:44:52:c2:38  10.150.0.46             54.174.200.5            63901     443       6      1    0      READY   968     ping.chartbeat.net
 94:60:d5:da:5a:20  172.253.118.188         10.150.0.46             5228      64659     6      1    0      READY   2484    mtalk.google.com
 28:d2:44:52:c2:38  10.150.0.46             23.202.160.194          65333     443       6      1    0      READY   2537    res.abc.net.au
 28:d2:44:52:c2:38  10.150.0.46             89.149.212.51           65356     443       6      1    0      READY   68      infinity-c32.youboranqs01.com
 28:d2:44:52:c2:38  10.150.0.46             192.168.1.131           64542     53        17     1    0      READY   32      ping.chartbeat.net
 94:60:d5:da:5a:20  54.174.200.5            10.150.0.46             443       63901     6      1    0      READY   968     ping.chartbeat.net
 94:60:d5:da:5a:20  54.153.189.86           10.150.0.46             443       49588     6      1    0      READY   968     deliver.oztam.com.au
 94:60:d5:da:5a:20  23.199.68.130           10.150.0.46             443       65353     6      1    0      READY   2537    abc-iview-mediapackagestreams-2.akamaized.net
```

From the CLI we can use this command to show the TopN apps based on app id.

```
primary1-Stack# show traffic-insight TI-01 monitor-type topN-flows TopN app-details

Name        : TopN
Group By    : appid
Entries     : 20
Filter By   : None
Running Statistics Timeout    : 600

Dataset     : Running Statistics
Rank    appid       appname                         appcategory                     Bytes
-------------------------------------------------------------------------------------------
1       2537        abc-au                          web                             87673731
2       4           unknown                         standard                        21757299
3       32          dns                             network-service                 264830
4       943         google-gen                      web                             155878
5       2484        gcm                             web                             106618
6       68          https                           web                             72267
7       0           Unrecognized                    Unrecognized                    69351
8       968         amazon                          web                             43857
9       205         tcp                             network-service                 23255
10      2821        microsoft                       web                             13914
11      562         windows-update                  web                             372
```

3.7 Best Practices

Here are the best practices as published in user guide.

- Use it for wired clients, IP Phone an PC/laptop connected to the IP Phone is also supported.
- Use ARC Default mode if you want URL and TLS attribute information.
- Also check this video for Scalability and Performance information.