



Palo Alto Networks Integration with LiveNX

LiveAction, Inc.
3500 WEST BAYSHORE ROAD
PALO ALTO, CA 94303

1. Introduction

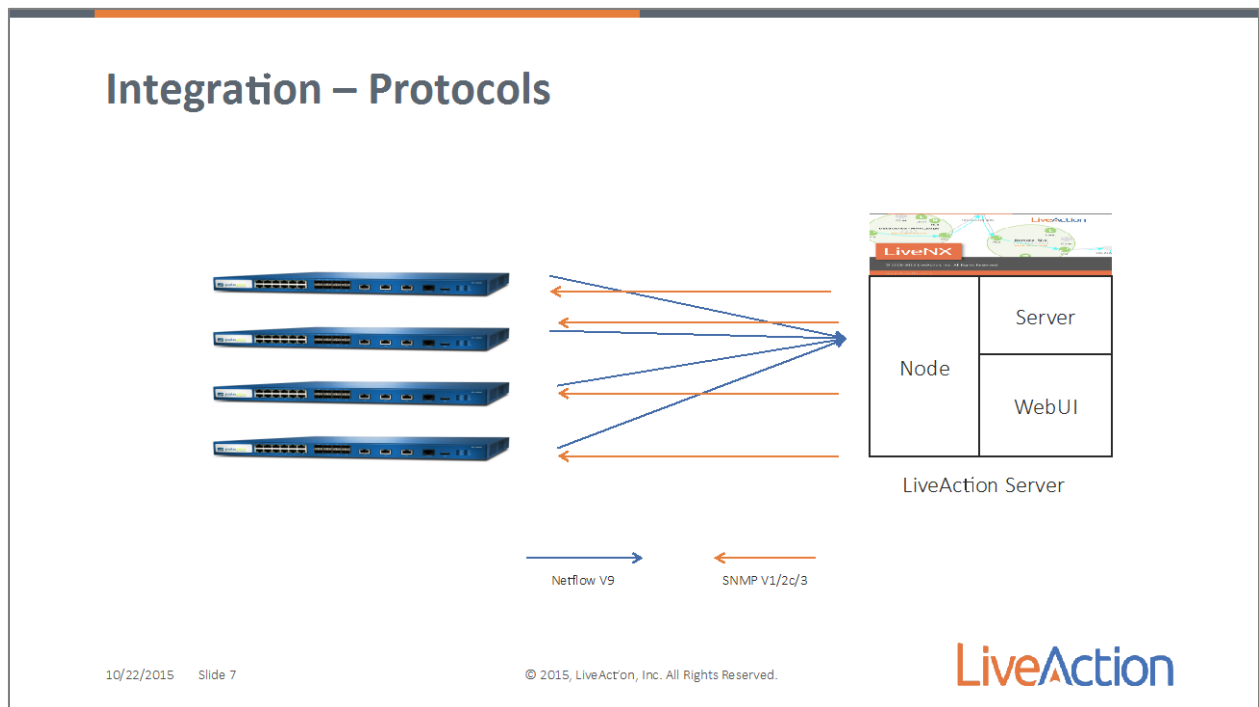
Palo Alto Network's Next Generation Firewall provides extensive information about sessions, websites and users visiting those sites. This information when displayed through LiveAction's LiveNX can help a network or security engineer visualize specific events that have happened at a specific time or is occurring at the present time.

This document will walk the administrator through the process of setting up NetFlow Export on the Palo Alto Networks device and how to visualize the information within LiveNX.

2 | Palo Alto Networks Integration with LiveNX

2. Integration Architecture

The integration between Palo Alto Networks devices and LiveNX is over standard protocols of NetFlow and the Simple Network Management Protocol (SNMP). Palo Alto Networks devices can export NetFlow information to LiveNX. In addition to the standard fields, Palo Alto Networks devices can also export Application ID and User ID within the NetFlow Packets.

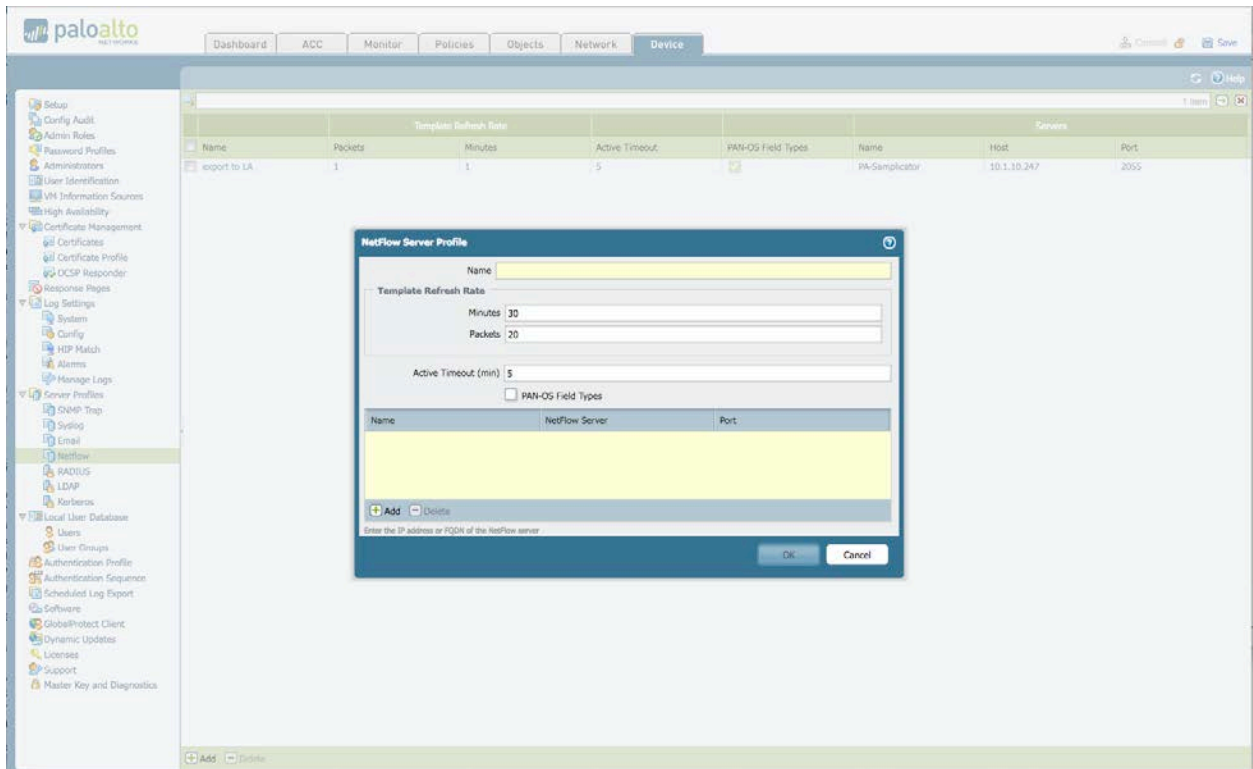


3 | Palo Alto Networks Integration with LiveNX

3. Enabling NetFlow Export on Palo Alto Networks Firewalls

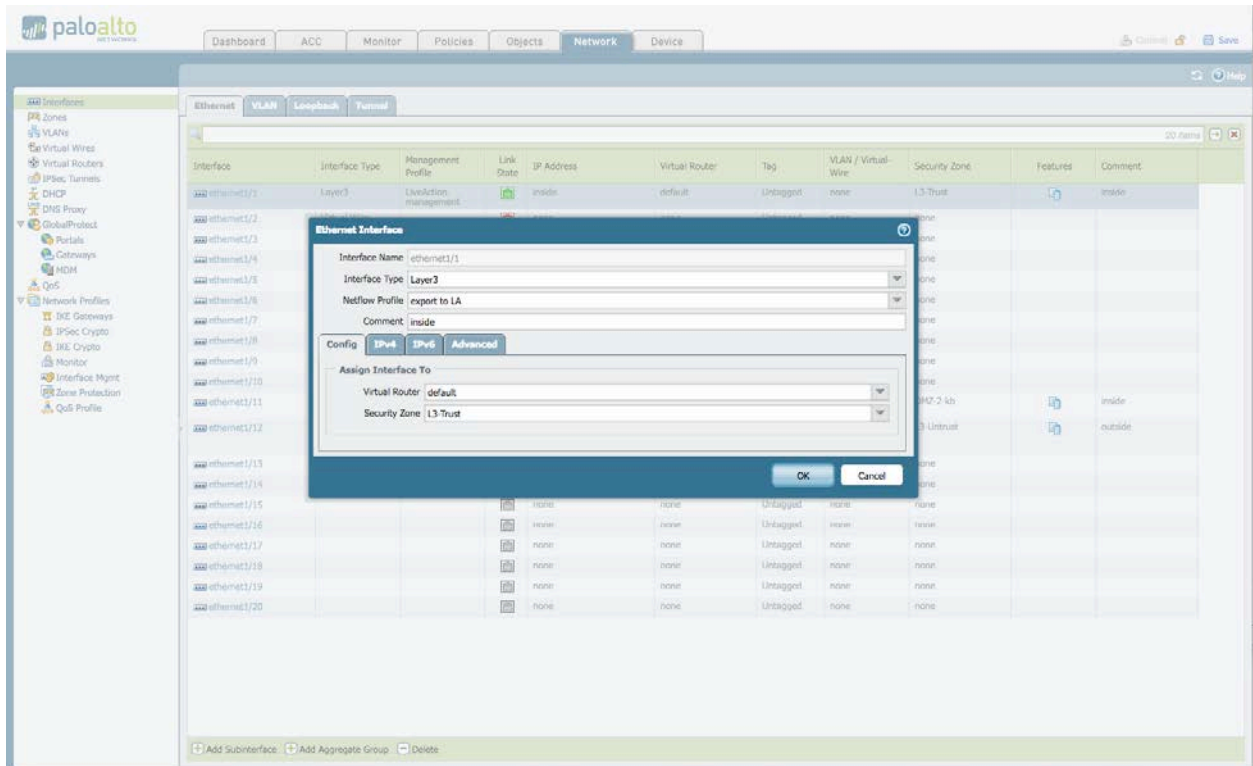
To enable NetFlow Export on the Palo Alto Networks device, log into the Palo Alto Networks WebUI.

Navigate to “Device,” expand the Sever Profile accordion, and select “NetFlow.” Click on “Add” and enter the correct information for the LiveNX server or node. To include the extra Palo Alto Networks fields, User ID and Application ID, check the PAN-OS Field Types box.



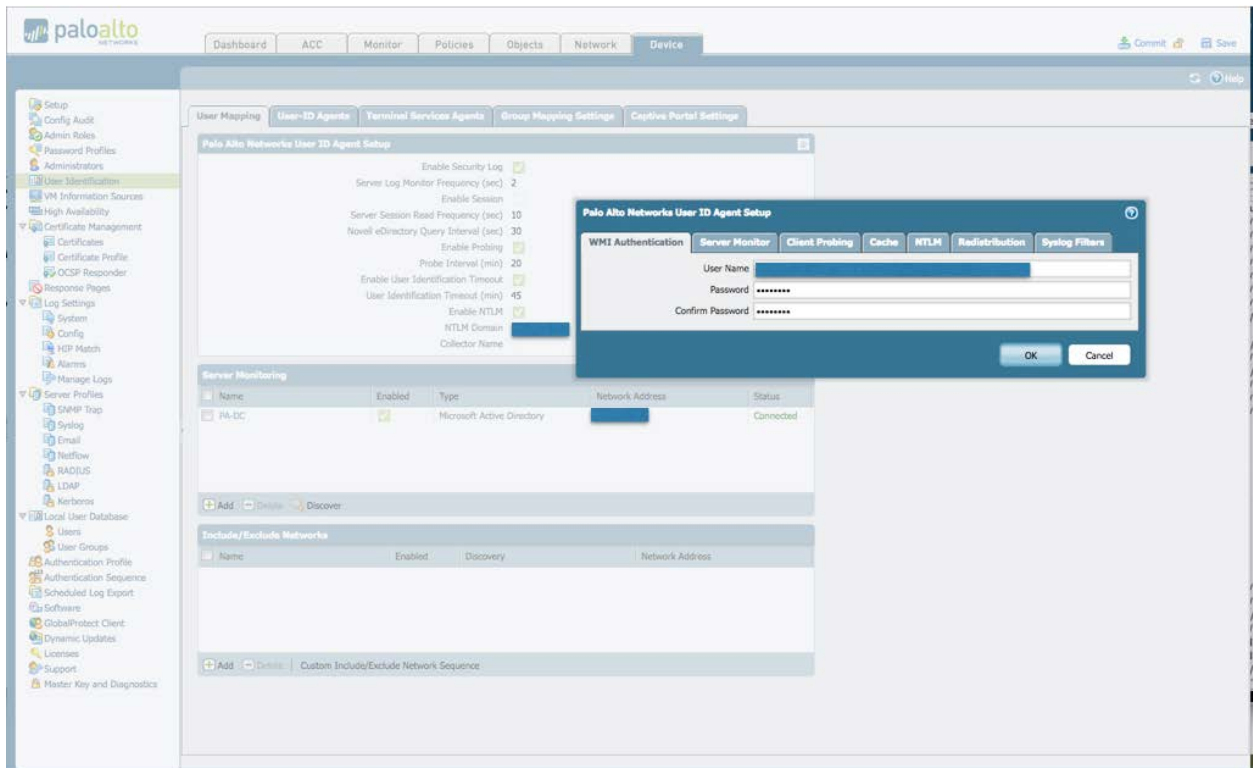
Select “OK” and the Exporter has been set up. Now we need to activate the export of the flows. This is done on an interface level. Now navigate to the Network Tab, and Interfaces. Select the Interface(s) that will be used to generate the NetFlow data. In the NetFlow Profile section add the Exporter that we just set up.

4 | Palo Alto Networks Integration with LiveNX



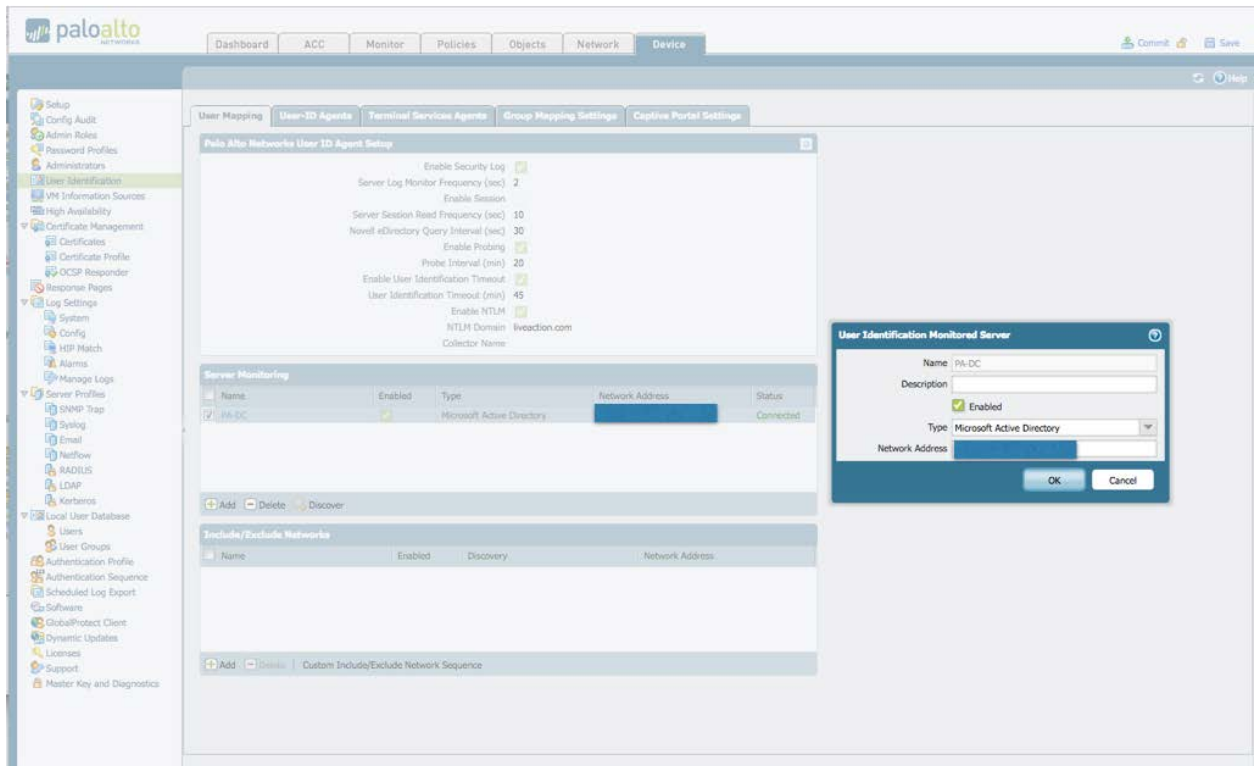
Once completed, commit the configuration. The Palo Alto Networks device should now be exporting flows to LiveNX. The next step is to enable the Palo Alto Networks device to use the Microsoft Active Directory to pull the User ID to IP address mapping. Palo Alto Networks can pull this information from other sources as well, please refer to the Palo Alto Networks documentation to enable the other sources. On the Device Tab, navigate to “User Identification” and in User Mapping select the gear icon (top right) to set up the agent. We are going to use the Agentless method and enable Windows Management Interface (WMI). Enter the name and password that will be used for WMI connectivity. We will presume that this User ID has already been set up by your AD administrator with the correct security level.

5 | Palo Alto Networks Integration with LiveNX



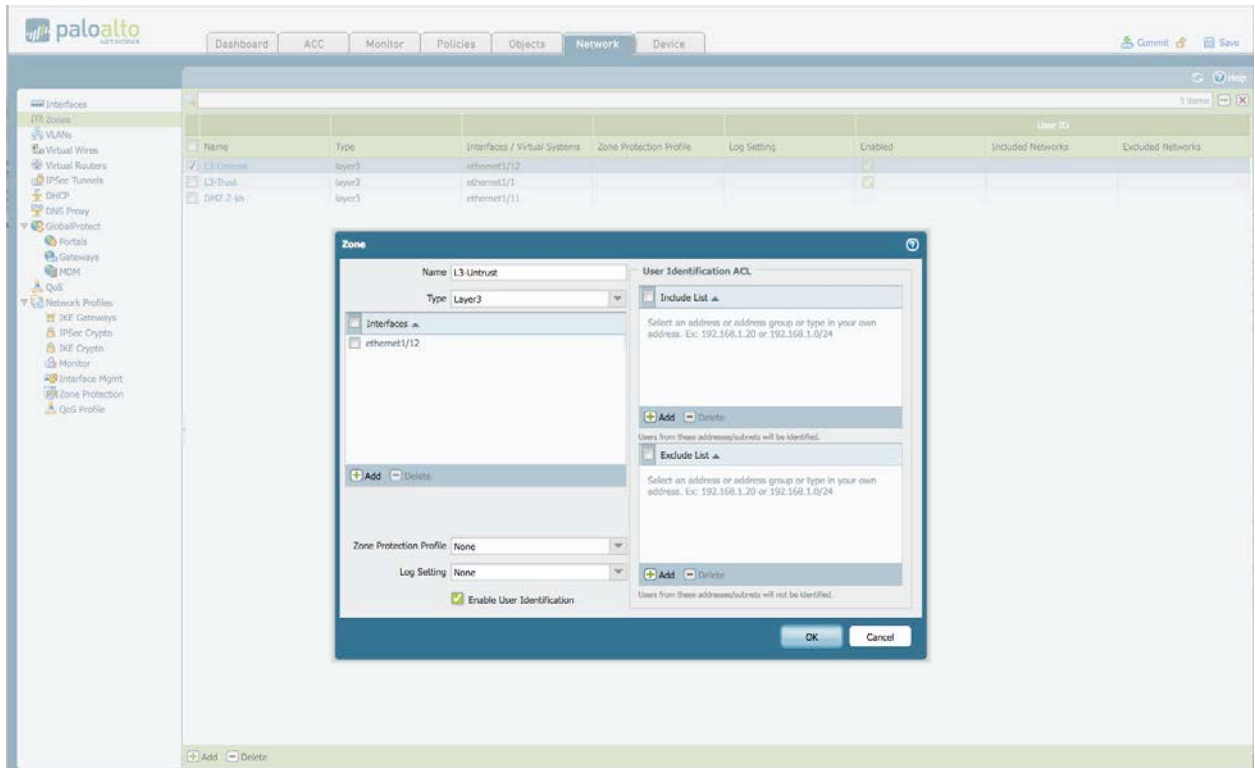
Make sure that you also enable Server Monitoring, Client Probing and NTLM. Next click “OK” and then in the Server Monitoring section add the domain controllers that need to be accessed by this Palo Alto Networks Device. This list may be different depending on the AD architecture and geographic location, as AD security audit logs are local to the domain controllers that are used for authentication.

6 | Palo Alto Networks Integration with LiveNX



Once you have added the User Identification server, you must enable User ID identification on the Zones. To accomplish this, navigate to Network, Zones and edit each of the Zones that you want the User ID to be displayed on.

7 | Palo Alto Networks Integration with LiveNX



Now commit the changes, and we have finished setting up the Palo Alto Networks device.

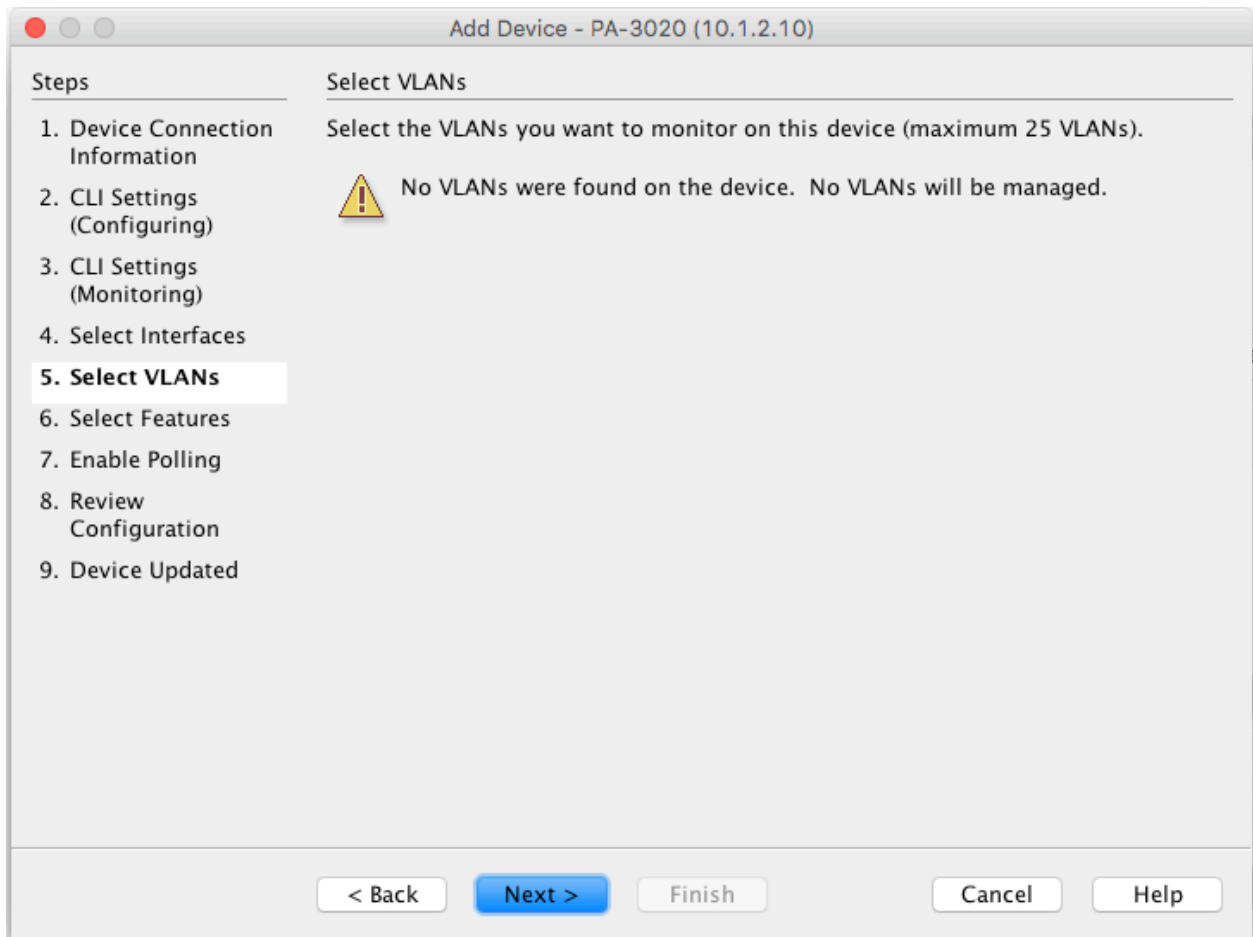
8 | Palo Alto Networks Integration with LiveNX

4. Adding the Palo Alto Networks Device(s) to LiveNX

Open the LiveNX Java Client and log into the system. Navigate to File -> Add device and the Add Device Wizard will start. This is a 9-step wizard that will ask and interrogate the device to find the Interfaces and other information about the system. You must have the IP address of any Layer 3 interface that will be exporting Flow data, and the Management IP address. You must also have the SNMP community string that will be used to collect the interface Table.

The screenshot shows the 'Add Device' wizard window. On the left, a 'Steps' list shows 9 steps: 1. Device Connection Information, 2. CLI Settings (Configuring), 3. CLI Settings (Monitoring), 4. Select Interfaces, 5. Select VLANs, 6. Select Features, 7. Enable Polling, 8. Review Configuration, and 9. Device Updated. Step 1 is currently selected. The main area is titled 'Device Connection Information' and contains the instruction 'Enter the SNMP connection information.' Below this, there are several fields: 'Node' with a dropdown menu showing 'Local', 'IP Address' with a text field containing 'X.X.X.X', and three radio buttons: 'Non SNMP device such as NetFlow probes', 'LiveSensor', and 'Use the Default SNMP connection settings'. The 'Enter SNMP connection settings for this device' radio button is selected. Below the radio buttons, there are two more fields: 'SNMP Version' with a dropdown menu showing 'Version 2c', and 'Target Port' with a text field containing '161'. At the bottom, there is a 'Community String' text field containing 'public'. At the very bottom of the window, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Select “Next” and LiveNX will now go through and find the interfaces in the Palo Alto Networks Device. Once you have selected the interfaces that NetFlow will be exported from, click “Next,” and as LiveNX will not know of any VLANs defined within the Palo Alto Networks select “Next.”



Now we can change the Polling Rate, leave it at one minute, and select Flows and click next to review the configuration and then select "Finish."

Add Device - PA-3020 (10.1.2.10)

Steps

1. Device Connection Information

2. CLI Settings (Configuring)

3. CLI Settings (Monitoring)

4. Select Interfaces

5. Select VLANs

6. Select Features

7. Enable Polling

8. Review Configuration

9. Device Updated

Enable Polling

Select the features you want to actively monitor and the polling rate for all the features on this device. Learn more about polling in the Help section.

Polling Rate

1 minute

Poll the following features

☒ Flows

☐ QoS

☐ IP SLA

☐ Routing

☐ LAN*

* LAN polling occurs every 15 minutes

* For SNMP v3, please see the User Guide on configuring LAN polling.

< Back

Next >

Finish

Cancel

Help

Add Device - PA-3020 (10.1.2.10)

Steps

1. Device Connection Information

2. CLI Settings (Configuring)

3. CLI Settings (Monitoring)

4. Select Interfaces

5. Select VLANs

6. Select Features

7. Enable Polling

8. Review Configuration

9. Device Updated

Device Updated

You have configured this device successfully with the following settings (You may want to save the current configuration to the device's startup config, so your settings will not be lost when the device is restarted):

Device Settings

Setting	Description
Polling Rate	1 minute
Flow Monitoring	Flow Collector
Flow Polling	Enabled
Adjacency Polling	N/A

Interfaces

mgmt
ethernet1/12
ethernet1/11
ethernet1/1

< Back

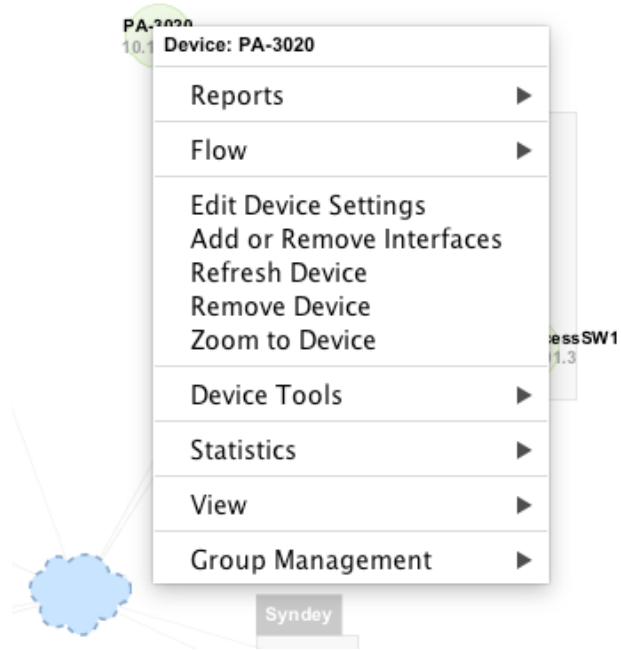
Next >

Finish

Cancel

Help

The device will now appear on the Main Screen and should be green, meaning that LiveNX has contacted the device. We now need to run the device setup again. This is an issue with retrieving the IP addresses from the interfaces. Palo Alto Networks devices do not update the Interface MIB table with IP addresses, and therefore LiveNX cannot associate the flow data with the correct interface or, connect it to the correct networks. This is remedied by modifying the device. Right click on the Palo Alto Networks device and open “Edit Device Settings.”



The Device Wizard will start and this time we are going to change the Device type to Non SNMP device, select “Next” and the Interface Table will be presented.

Enter the IP addresses of the Interfaces that will be exporting the flows and select “Finish.”

The Device will now connect to the correct networks. If the Palo Alto Networks Device is running in Layer 2 mode, enter the Management IP address.

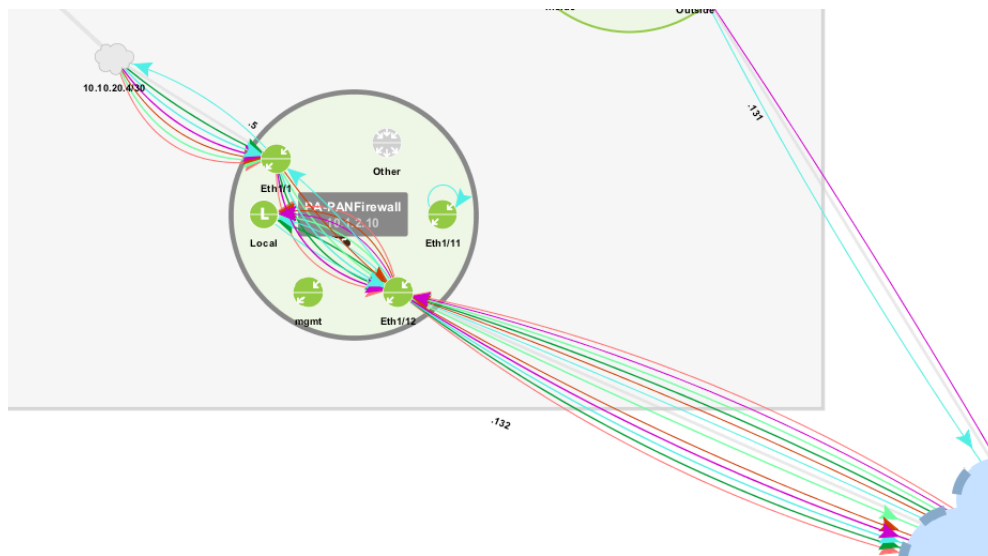
*Ifindex	*Interface	Description	IP Address	Subnet Mask
2	mgmt			
3	ethernet1/1	inside	10.10.20.5	255.255.255.0
13	ethernet1/11	inside		
14	ethernet1/12	outside		255.255.255.248

14 | Palo Alto Networks Integration with LiveNX

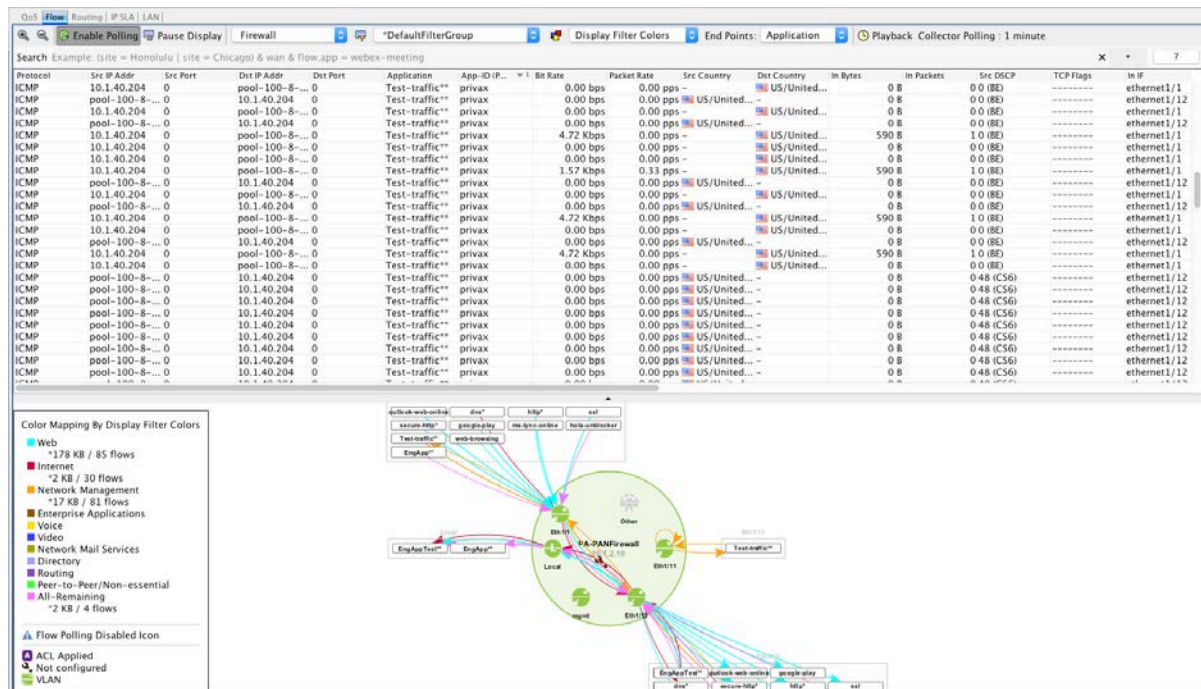
5. Reports

LiveNX currently has a rich set of reports and visual aids that can help the network/security engineer to view traffic that is traversing the Palo Alto Networks device and be able to understand the applications and users that maybe effecting the stability of the network.

Let's start with a set of Visual Aids—the first is to monitor the Palo Alto Networks device itself and see what flow are active in real-time. From the main screen in the Java Client, change the flow display to Firewall. This will display all flows traversing the Palo Alto Networks.



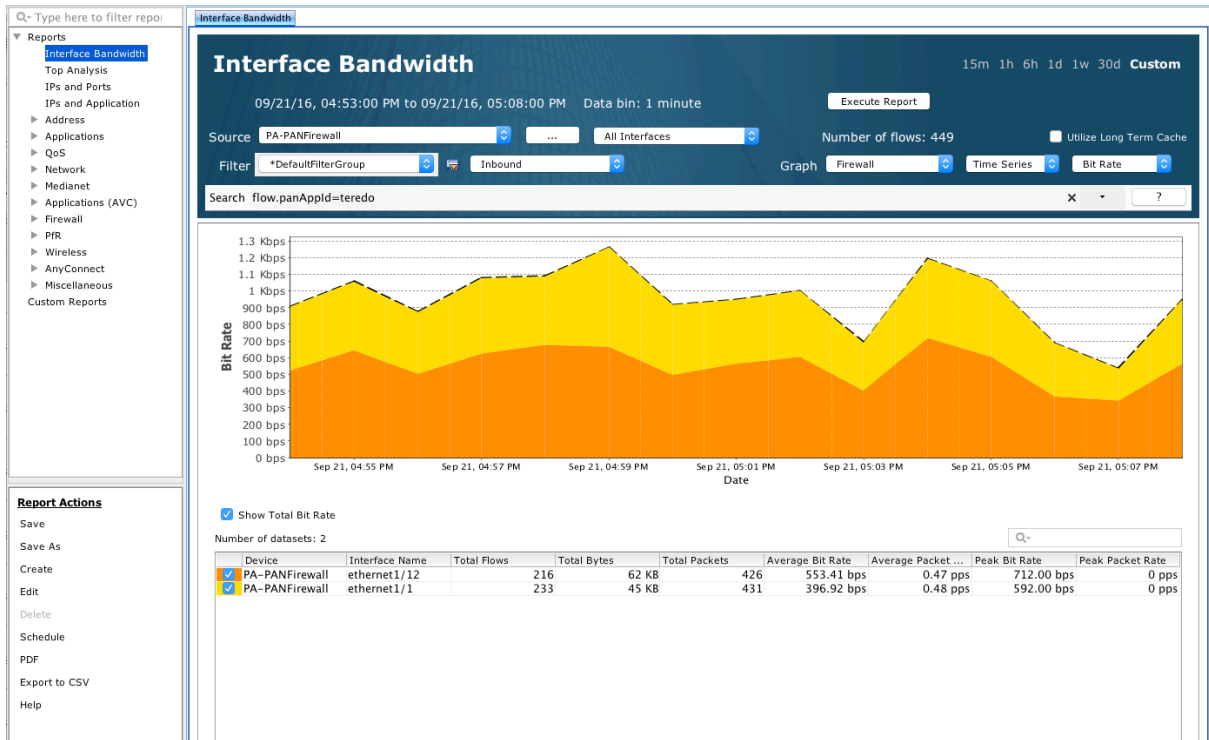
Now, if we double click onto the device we will see a real-time display of all the flows the Palo Alto Networks device is exporting. This view is updated every minute and can be used to find specific flows and drill down into more specific reports.



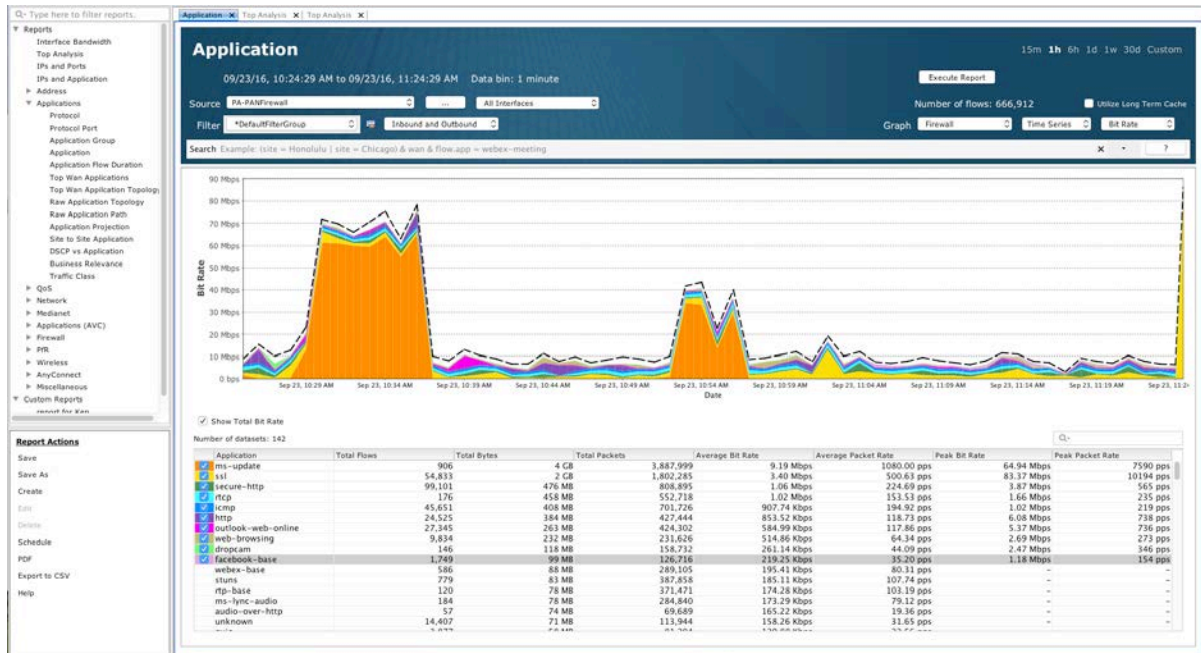
If we select a specific flow, it can be added to the search filter, and then only information destined to that application or IP address can be displayed. Or, we can drill down into more specific reports, like Top Analysis, or Interface Bandwidth reports.

The screenshot displays the Palo Alto Networks LiveNX interface. At the top, a table lists traffic flows with columns: Application, App-ID (P...), Bit Rate, Packet Rate, Src Country, Dst Country, In Bytes, In Packets, Src DSCP, and TCP Flags. Below the table is a network diagram showing a central 'PA-PANFirewall' node connected to various external nodes like 'outlook-web-online', 'secure-http*', 'teredo-ipv6-tunnel*', 'Test-traffic**', 'EngAppTest**', 'web-browsing', 'salesforce-base*', 'github-base', 'dns*', 'ssl', 'hold-unblocker', 'ntp*', and 'Other'. A context menu is open over the 'EngAppTest**' application, listing various reports such as 'Top Analysis Report', 'Interface Bandwidth Report', 'Top Conversations Report', 'Bidirectional Source/Destination Pair Report', 'Source or Destination Address Report', 'Address Pair Report', 'Destination Address Report', 'Source Address Report', 'Destination Address Popularity Report', 'Source Address Popularity Report', 'Site Traffic Report', 'Destination Site Traffic Report', 'Source Site Traffic Report', 'Protocol Report', 'Protocol Port Report', 'Application Group Report', 'Application Report', 'Application Flow Duration Report', 'DSCP vs Application Report', 'Business Relevance Report', 'Traffic Class Report', 'User Filter DSCP Audit Report', 'Application DSCP Audit Report', 'Site to Site User Filter DSCP Audit Report', 'Site to Site Application DSCP Audit Report', 'Type of Service Report', 'DSCP Report', 'Interface Bandwidth Summary Report', 'Bandwidth Summary Report', 'Traffic Volume Pair Report', 'Outbound Bandwidth Utilization Report', 'Network Security Denied Events Report', 'App Group (DSCP) Bandwidth Report', 'App Group (DSCP) Bandwidth by Site Report', 'App Group (DSCP) Bandwidth by Service Provider Report', 'Site Capacity Utilization Report', and 'Site Capacity Utilization by App Group (DSCP) Report'.

By right clicking on specific columns in this display we can drill down and look at specific issues that could be happening, if we choose the Source IP address we can drill down to the interface report and see the amount of traffic that is being generated that is traversing through the firewall by that specific address, or by right clicking on the APP-ID (Palo Alto Networks) we can choose the same report and see the amount of traffic that is specific application is generating.



From LiveNX's Flow Reports we can also look at all the applications and the bandwidth each is consuming. Open Flow Reports and choose the Application report, choose the Palo Alto Networks device and make the Graph Type "Firewall," select the time frame and execute the report.



From this view, we can also drill down on specific applications and gather more information on Network Activity.

6. Use Cases

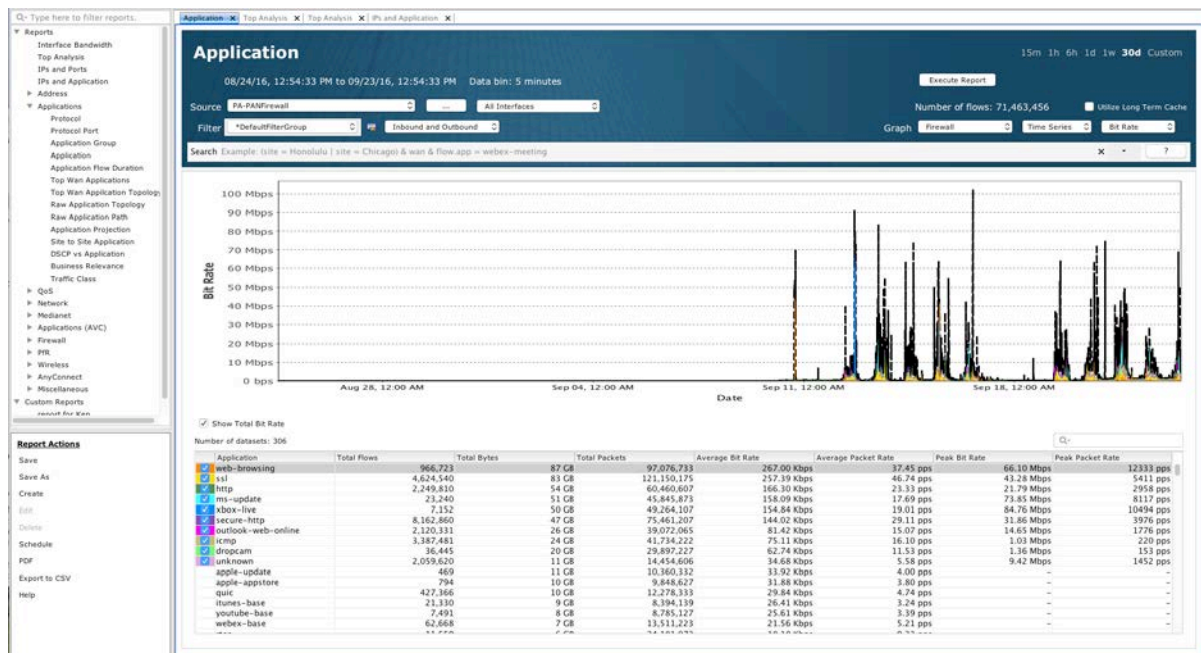
Let's look at some specific use cases that can help solve specific issues that may be generated within an organization.

1) What was Done?

In this specific use case, we need to understand what an employee did during a specific time period and what applications were used, and if any large amounts of data were transferred outside the of the company's infrastructure. Information that we have are the user's ID and the time frame that the event happened. In LiveNX, we can run Flow reports on the time frame and then as the user's ID appears in the reports we can use the associated IP address to add to the filter list. Execute the report and now we have all the external activity for that user over the selected time period.

Time	Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	User-ID (PAN)	Application	App-ID (PAN)	Bit Rate	Packet Rate	Src Country	Dst Country
Sep 23, 2016, 10:24:29 AM	TCP	xx-fbcdn-shv-01-sjc2.fbcdn.net	443	12.33.223.132	43,604	liveaction.com/testime	facebook-base facebook-base	2.49 Kbps	0.00 pps	0.00 pps	IE/Ireland	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,517	edge-star-m... 443	liveaction.com/testime	facebook-base facebook-base	26.46 Kbps	3.67 pps	3.67 pps	3.67 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	4,348	liveaction.com/testime	facebook-base facebook-base	5.47 Kbps	2.67 pps	2.67 pps	2.67 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,482	edge-star-m... 443	liveaction.com/testime	facebook-base facebook-base	347.17 bps	0.13 pps	0.13 pps	0.13 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	51,643	liveaction.com/testime	facebook-base facebook-base	693.89 bps	16.00 pps	16.00 pps	16.00 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,457	xx-fbcdn-sh... 443	liveaction.com/testime	facebook-base facebook-base	17.51 Kbps	51.00 pps	51.00 pps	51.00 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	xx-fbcdn-shv-01-sjc2.fbcdn.net	443	12.33.223.132	56,965	liveaction.com/testime	facebook-base facebook-base	549.47 Kbps	2.83 Kbps	2.83 Kbps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	42,315	liveaction.com/testime	facebook-base facebook-base	36.70 Kbps	4.07 pps	4.07 pps	4.07 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,465	xx-fbcdn-sh... 443	liveaction.com/testime	facebook-base facebook-base	4.54 Kbps	4.20 pps	4.20 pps	4.20 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	xx-fbcdn-shv-01-atl3.fbcdn.net	443	12.33.223.132	50,215	liveaction.com/testime	facebook-base facebook-base	107.59 Kbps	10.00 pps	10.00 pps	IE/Ireland	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,545	xx-fbcdn-sh... 443	liveaction.com/testime	facebook-base facebook-base	6.62 Kbps	10.00 pps	10.00 pps	10.00 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	52,704	liveaction.com/testime	facebook-base facebook-base	224.70 Kbps	7.00 pps	7.00 pps	7.00 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,545	xx-fbcdn-sh... 443	liveaction.com/testime	facebook-base facebook-base	6.62 Kbps	10.00 pps	10.00 pps	10.00 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	xx-fbcdn-shv-01-atl3.fbcdn.net	443	12.33.223.132	11,374	liveaction.com/testime	facebook-base facebook-base	224.70 Kbps	20.00 pps	20.00 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,547	edge-star-m... 443	liveaction.com/testime	facebook-base facebook-base	2.78 Kbps	0.62 pps	0.62 pps	0.62 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	23,459	liveaction.com/testime	facebook-base facebook-base	3.18 Kbps	0.67 pps	0.67 pps	0.67 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,526	xx-fbcdn-sh... 443	liveaction.com/testime	facebook-base facebook-base	670.24 bps	0.12 pps	0.12 pps	0.12 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	11,896	liveaction.com/testime	facebook-base facebook-base	273.49 bps	0.14 pps	0.14 pps	0.14 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,456	xx-fbcdn-sh... 443	liveaction.com/testime	facebook-base facebook-base	30.77 bps	0.04 pps	0.04 pps	0.04 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	xx-fbcdn-shv-01-sjc2.fbcdn.net	443	12.33.223.132	29,825	liveaction.com/testime	facebook-base facebook-base	369.54 bps	0.08 pps	0.08 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,401	xx-fbcdn-sh... 443	liveaction.com/testime	facebook-base facebook-base	284.57 bps	0.20 pps	0.20 pps	0.20 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	xx-fbcdn-shv-01-sjc2.fbcdn.net	443	12.33.223.132	2,275	liveaction.com/testime	facebook-base facebook-base	3.93 Kbps	0.46 pps	0.46 pps	IE/Ireland	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,402	xx-fbcdn-sh... 443	liveaction.com/testime	facebook-base facebook-base	303.43 bps	0.26 pps	0.26 pps	0.26 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	xx-fbcdn-shv-01-sjc2.fbcdn.net	443	12.33.223.132	56,737	liveaction.com/testime	facebook-base facebook-base	7.65 Kbps	0.73 pps	0.73 pps	IE/Ireland	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,466	xx-fbcdn-sh... 443	liveaction.com/testime	facebook-base facebook-base	31.17 bps	0.04 pps	0.04 pps	0.04 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	xx-fbcdn-shv-01-atl3.fbcdn.net	443	12.33.223.132	61,138	liveaction.com/testime	facebook-base facebook-base	374.44 bps	0.08 pps	0.08 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,483	edge-star-m... 443	liveaction.com/testime	facebook-base facebook-base	1.22 Kbps	0.53 pps	0.53 pps	0.53 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	60,171	liveaction.com/testime	facebook-base facebook-base	8.33 Kbps	1.13 pps	1.13 pps	1.13 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,546	edge-star-m... 443	liveaction.com/testime	facebook-base facebook-base	2.69 Kbps	0.62 pps	0.62 pps	0.62 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	23,998	liveaction.com/testime	facebook-base facebook-base	3.64 Kbps	0.46 pps	0.46 pps	0.46 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,377	edge-star-m... 443	liveaction.com/testime	facebook-base facebook-base	270.46 bps	0.08 pps	0.08 pps	0.08 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	22,972	liveaction.com/testime	facebook-base facebook-base	657.85 bps	0.14 pps	0.14 pps	0.14 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,534	edge-star-m... 443	liveaction.com/testime	facebook-base facebook-base	401.66 bps	0.13 pps	0.13 pps	0.13 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	55,979	liveaction.com/testime	facebook-base facebook-base	1.41 Kbps	0.24 pps	0.24 pps	0.24 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,544	xx-fbcdn-sh... 443	liveaction.com/testime	facebook-base facebook-base	2.56 Kbps	1.67 pps	1.67 pps	1.67 pps	IE/Ireland	US/United
Sep 23, 2016, 10:24:29 AM	TCP	xx-fbcdn-shv-01-atl3.fbcdn.net	443	12.33.223.132	16,774	liveaction.com/testime	facebook-base facebook-base	11.06 Kbps	2.00 pps	2.00 pps	IE/Ireland	US/United
Sep 23, 2016, 10:24:29 AM	TCP	edge-star-mini-shv-07-ash4... 443	12.33.223.132	23,998	liveaction.com/testime	facebook-base facebook-base	8.83 bps	0.01 pps	0.01 pps	0.01 pps	US/United	US/United
Sep 23, 2016, 10:24:29 AM	TCP	10.1.2.205	49,482	edge-star-m... 443	liveaction.com/testime	facebook-base facebook-base	6.23 bps	0.01 pps	0.01 pps	0.01 pps	US/United	US/United

Not only can we see what external apps and systems were touched, but we can also see all the internal activity from that address, while the user was associated with that IP address. Select "All Devices" and the timeframe, set the graph to "Basic Flow" and execute the report.



From this report we can drill down into the application where the data leakage was reported. So if we right click on the application, then drill down and run the Top Analysis we can now see the individual flows over this specific time frame and the users that generated the traffic. In this example, we will look for something going to Facebook. Even though it's not a data export tool, the same principle applies.

Reports

Interface Bandwidth

Top Analysis

Flows and Ports

IPs and Application

Address

Applications

Protocol

Predefined Port

Application Group

Application

Application Flow Duration

Top View Applications

Top View Application Topology

Raw Application Topology

Raw Application Path

Raw Application Projection

Site to Site Application

DSCP vs Application

Business Relevance

QoS

Network

MacAddress

Applications (AVC)

Firewall

IPS

Sniffers

AnyConnect

Miscellaneous

Custom Reports

Report Raw Data

Save

Save As

Create

Edit

Details

Schedule

PDF

Export to CSV

Help

Application: *Top Analysis

Time: 09/23/16, 09:32:34 AM to 09/23/16, 03:32:34 PM

Source: PA-PANFWireless

Filter: *DefaultFilterGroup

Inbound and Outbound

All Interfaces

Number of flows: 5,000+

CSV File Reader

Flow app=facebook-base

15m 1h 6h 1d 1w 30d Custom

Execute Report

Firewall

Time Sorted

Unique Flows

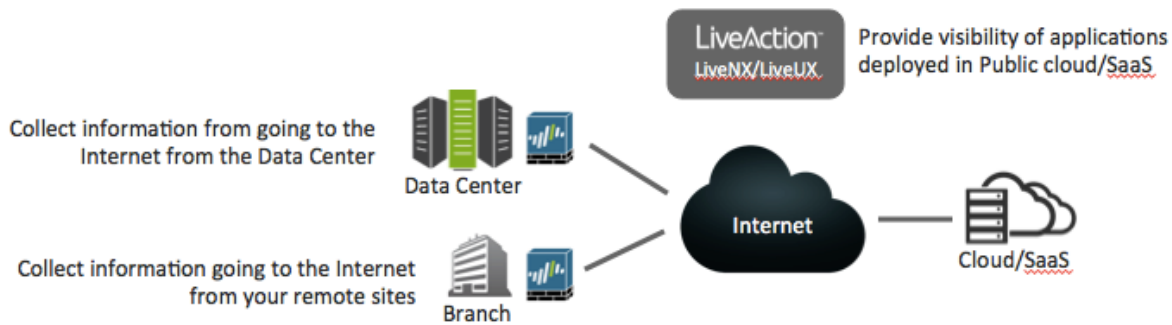
1

2

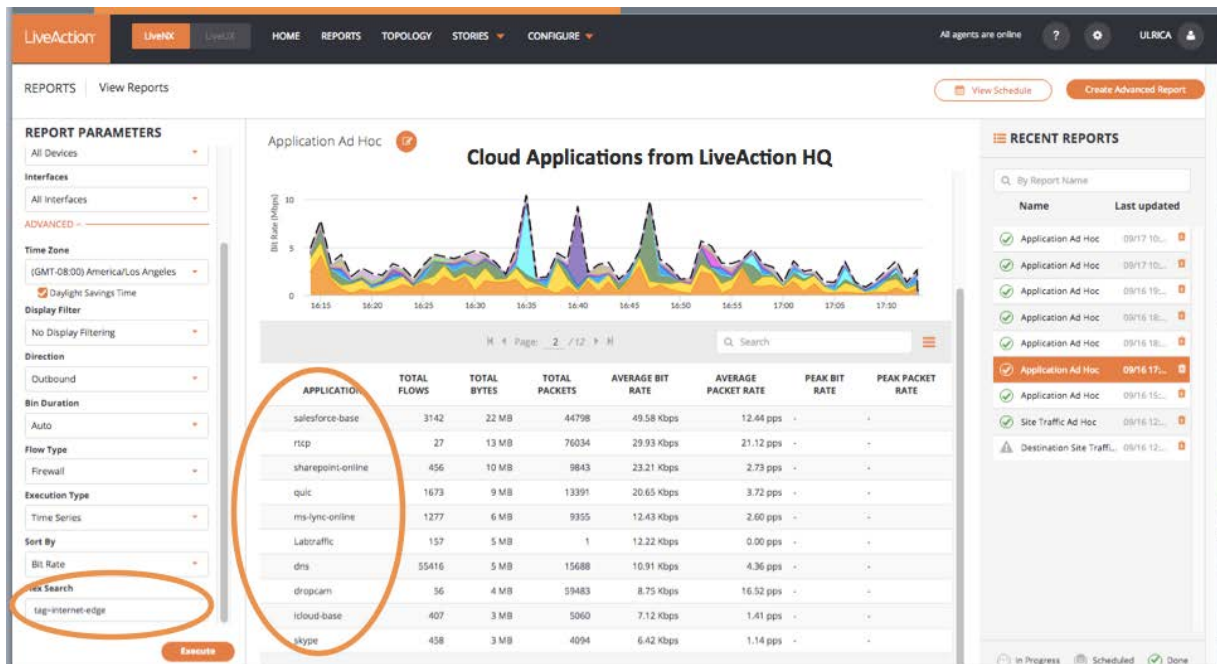
Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	User-ID (RAN)	Application	App-ID (RAN)	Bit Rate	Packet Rate	Src Country	Dst Country	In Bytes	In Packets	Src DSCP	Tx
TCP	10.1.2.205	49,534	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	36.70 Kbps	4.07 pps	4.07 pps	US/United States	US/United States	124 KB	110 (BE)	---	---
TCP	10.1.2.205	49,465	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	4.54 Kbps	4.20 pps	4.20 pps	US/United States	US/United States	3 KB	21 (BE)	---	---
TCP	10.1.2.205	49,534	12.31.223.132	50,215	liveaction.com/testme	facebook-base facebook-base	107.59 Kbps	10.00 pps	10.00 pps	US/United States	US/United States	67 KB	50 (BE)	---	---
TCP	10.1.2.205	49,534	12.31.223.132	50,215	liveaction.com/testme	facebook-base facebook-base	22.74 Kbps	8.00 pps	8.00 pps	US/United States	US/United States	3 KB	8 (BE)	---	---
TCP	10.1.1.52	59,197	12.31.223.132	52,704	liveaction.com/testme	facebook-base facebook-base	25.54 Kbps	7.00 pps	7.00 pps	US/United States	US/United States	3 KB	7 (BE)	---	---
TCP	10.1.1.86	58,474	12.31.223.132	54,489	liveaction.com/testme	facebook-base facebook-base	308.16 Kbps	0.21 pps	0.21 pps	US/United States	US/United States	3 KB	15 (BE)	---	---
TCP	10.1.1.86	58,475	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	275.40 Kbps	0.23 pps	0.23 pps	US/United States	US/United States	3 KB	17 (BE)	---	---
TCP	10.1.1.86	58,475	12.31.223.132	63,140	liveaction.com/testme	facebook-base facebook-base	21.69 Kbps	0.03 pps	0.03 pps	US/United States	US/United States	160 B	2 (BE)	---	---
TCP	10.1.1.86	58,475	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	13.56 Kbps	0.02 pps	0.02 pps	US/United States	US/United States	100 B	1 (BE)	---	---
TCP	10.1.2.205	49,545	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	21.69 Kbps	0.03 pps	0.03 pps	US/United States	US/United States	160 B	2 (BE)	---	---
TCP	10.1.2.205	49,545	12.31.223.132	47,391	liveaction.com/testme	facebook-base facebook-base	6.62 Kbps	10.00 pps	10.00 pps	US/United States	US/United States	2 KB	30 (BE)	---	---
TCP	10.1.2.205	49,547	12.31.223.132	11,374	liveaction.com/testme	facebook-base facebook-base	224.70 Kbps	20.00 pps	20.00 pps	US/United States	US/United States	112 KB	80 (BE)	---	---
TCP	10.1.2.205	49,547	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	2.78 Kbps	0.62 pps	0.62 pps	US/United States	US/United States	8 KB	15 (BE)	---	---
TCP	10.1.2.205	49,547	12.31.223.132	23,459	liveaction.com/testme	facebook-base facebook-base	3.18 Kbps	0.67 pps	0.67 pps	US/United States	US/United States	10 KB	16 (BE)	---	---
TCP	10.1.2.205	49,526	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	670.24 Kbps	0.12 pps	0.12 pps	US/United States	US/United States	5 KB	7 (BE)	---	---
TCP	10.1.2.205	49,516	12.31.223.132	13,896	liveaction.com/testme	facebook-base facebook-base	273.49 Kbps	0.14 pps	0.14 pps	US/United States	US/United States	2 KB	8 (BE)	---	---
TCP	10.1.2.205	49,516	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	30.77 Kbps	0.04 pps	0.04 pps	US/United States	US/United States	300 B	3 (BE)	---	---
TCP	10.1.2.205	49,401	12.31.223.132	29,825	liveaction.com/testme	facebook-base facebook-base	369.54 Kbps	0.08 pps	0.08 pps	US/United States	US/United States	4 KB	6 (BE)	---	---
TCP	10.1.2.205	49,401	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	284.57 Kbps	0.20 pps	0.20 pps	US/United States	US/United States	3 KB	17 (BE)	---	---
TCP	10.1.2.205	49,402	12.31.223.132	2,275	liveaction.com/testme	facebook-base facebook-base	3.93 Kbps	0.46 pps	0.46 pps	US/United States	US/United States	41 KB	39 (BE)	---	---
TCP	10.1.2.205	49,402	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	303.43 Kbps	0.26 pps	0.26 pps	US/United States	US/United States	3 KB	22 (BE)	---	---
TCP	10.1.2.205	49,402	12.31.223.132	56,737	liveaction.com/testme	facebook-base facebook-base	7.65 Kbps	0.73 pps	0.73 pps	US/United States	US/United States	80 KB	61 (BE)	---	---
TCP	10.1.2.205	49,466	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	31.17 Kbps	0.04 pps	0.04 pps	US/United States	US/United States	3 KB	3 (BE)	---	---
TCP	10.1.2.205	49,466	12.31.223.132	63,138	liveaction.com/testme	facebook-base facebook-base	374.44 Kbps	0.08 pps	0.08 pps	US/United States	US/United States	4 KB	6 (BE)	---	---
TCP	10.1.2.205	65,038	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	13.26 Kbps	0.00 pps	0.00 pps	US/United States	US/United States	2 KB	18 (BE)	---	---
TCP	10.1.2.205	49,483	12.31.223.132	31,042	liveaction.com/testme	facebook-base facebook-base	498.39 Kbps	0.00 pps	0.00 pps	US/United States	US/United States	62 KB	48 (BE)	---	---
TCP	10.1.2.205	49,483	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	1.22 Kbps	0.53 pps	0.53 pps	US/United States	US/United States	2 KB	8 (BE)	---	---
TCP	10.1.2.205	49,483	12.31.223.132	60,371	liveaction.com/testme	facebook-base facebook-base	8.33 Kbps	1.13 pps	1.13 pps	US/United States	US/United States	16 KB	17 (BE)	---	---
TCP	10.1.1.86	65,046	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	17.87 Kbps	12.00 pps	12.00 pps	US/United States	US/United States	2 KB	12 (BE)	---	---
TCP	10.1.2.205	49,483	12.31.223.132	46,238	liveaction.com/testme	facebook-base facebook-base	23.82 Kbps	14.00 pps	14.00 pps	US/United States	US/United States	3 KB	14 (BE)	---	---
TCP	10.1.1.116	48,468	edge-mgmt-1	443	liveaction.com/testme	facebook-base facebook-base	3.91 Kbps	0.01 pps	0.01 pps	US/United States	US/United States	425 B	5 (BE)	---	---
TCP	10.1.2.205	49,546	12.31.223.132	59,142	liveaction.com/testme	facebook-base facebook-base	2.00 Kbps	0.69 pps	0.69 pps	US/United States	US/United States	6 KB	10 (BE)	---	---
TCP	10.1.2.205	49,546	12.31.223.132	21,988	liveaction.com/testme	facebook-base facebook-base	2.69 Kbps	0.62 pps	0.62 pps	US/United States	US/United States	8 KB	15 (BE)	---	---
TCP	10.1.2.205	49,546	12.31.223.132	21,988	liveaction.com/testme	facebook-base facebook-base	3.64 Kbps	0.06 pps	0.06 pps	US/United States	US/United States	11 KB	11 (BE)	---	---
TCP	10.1.2.205	49,577	12.31.223.132	443	liveaction.com/testme	facebook-base facebook-base	270.46 Kbps	0.08 pps	0.08 pps	US/United States	US/United States	4 KB	8 (BE)	---	---
TCP	10.1.2.205	49,543	12.31.223.132	22,972	liveaction.com/testme	facebook-base facebook-base	657.85 Kbps	0.14 pps	0.14 pps	US/United States	US/United States	9 KB	15 (BE)	---	---
TCP	10.1.2.205	49,534	12.31.223.132	31,042	liveaction.com/testme	facebook-base facebook-base	401.66 Kbps	0.13 pps	0.13 pps	US/United States	US/United States	4 KB	11 (BE)	---	---
TCP	10.1.2.205	49,544	12.31.223.132	55,979	liveaction.com/testme	facebook-base facebook-base	1.41 Kbps	0.24 pps	0.24 pps	US/United States	US/United States	14 KB	20 (BE)	---	---
TCP	10.1.2.205	49,544	12.31.223.132	55,979	liveaction.com/testme	facebook-base facebook-base	2.56 Kbps	1.67 pps	1.67 pps	US/United States	US/United States	960 B	5 (BE)	---	---

3) Shadow IT/Cloud Application Visibility

The cloud is transforming the way business is done. But IT teams do not always have visibility of these business critical applications and yet they are still responsible for making sure these applications are performing well and meeting users' needs.



The first step is to collect information from the Internet edges across your network. Schedule a weekly report to provide you a list of Cloud applications on an ongoing basis.



From this report, you can see the list of Cloud applications and the amount of traffic each application is consuming your resources. Network congestion can be an issue for many businesses today. You want to be sure that critical applications are not impacted when competing with recreational traffic. In the new Internet-based world, it is important to identify which applications are on your network and where your resources are being consumed to align with your business policy.

7. Conclusion

Combining Palo Alto Networks Next Generation Firewalls and LiveAction's LiveNX gives both network engineers and Security Engineers more visibility into traffic that is in the network, and exiting a segment or the perimeter of the network.