Palo Alto Networks Integration with LiveNX

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

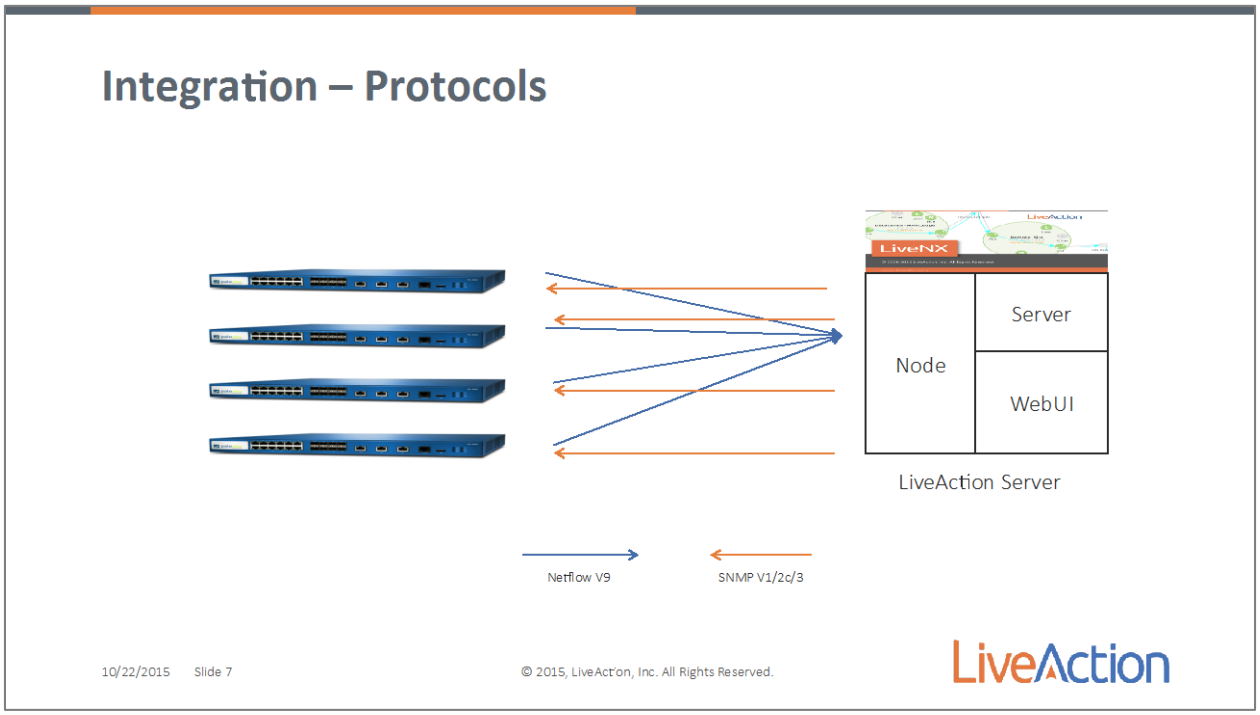
1. Introduction

Palo Alto Network's Next Generation Firewall provides extensive information about sessions, websites and users visiting those sites. This information when displayed though 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. Integration Architecture

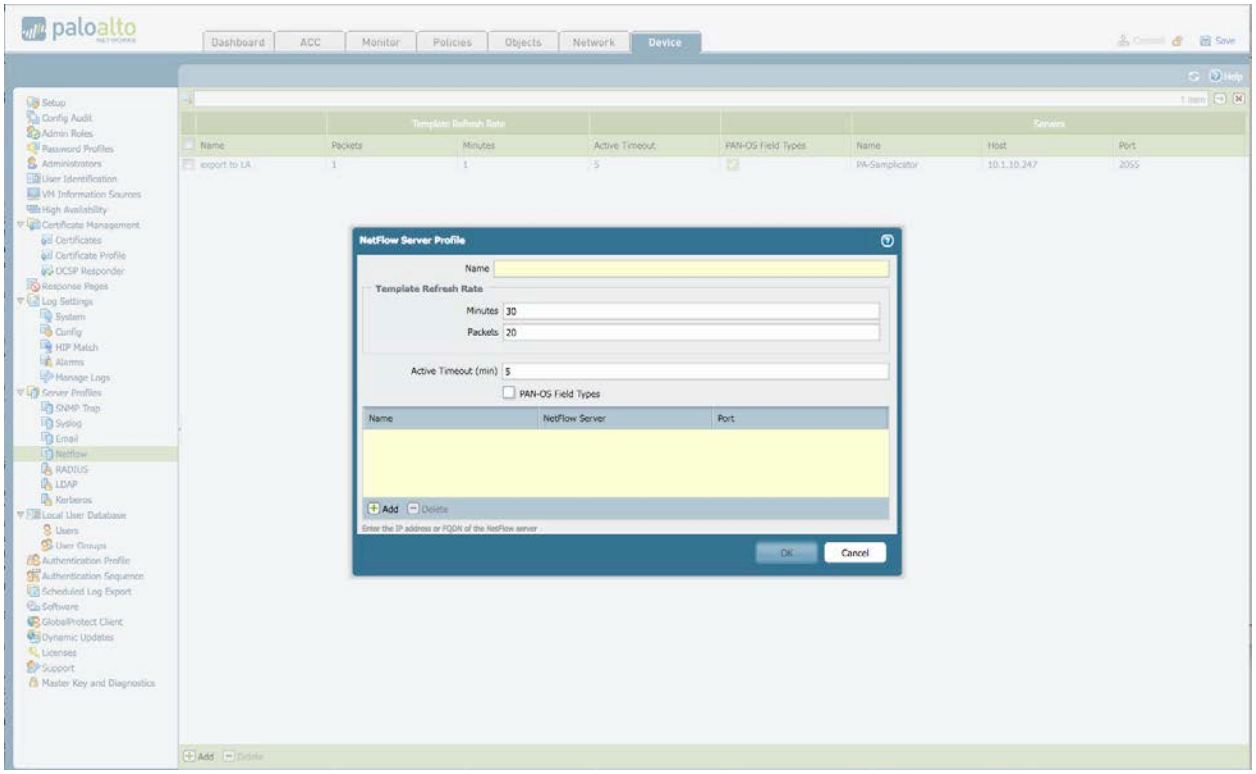
The integration between Palo Alto Networks devices and LiveNX is over standard protocols of NetFlow and the Simple Network Management Protocol (SNMP). Palo Alto Networks devices can export NetFlow information to LiveNX. In addition to the standard fields, Palo Alto Networks devices can also export Application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



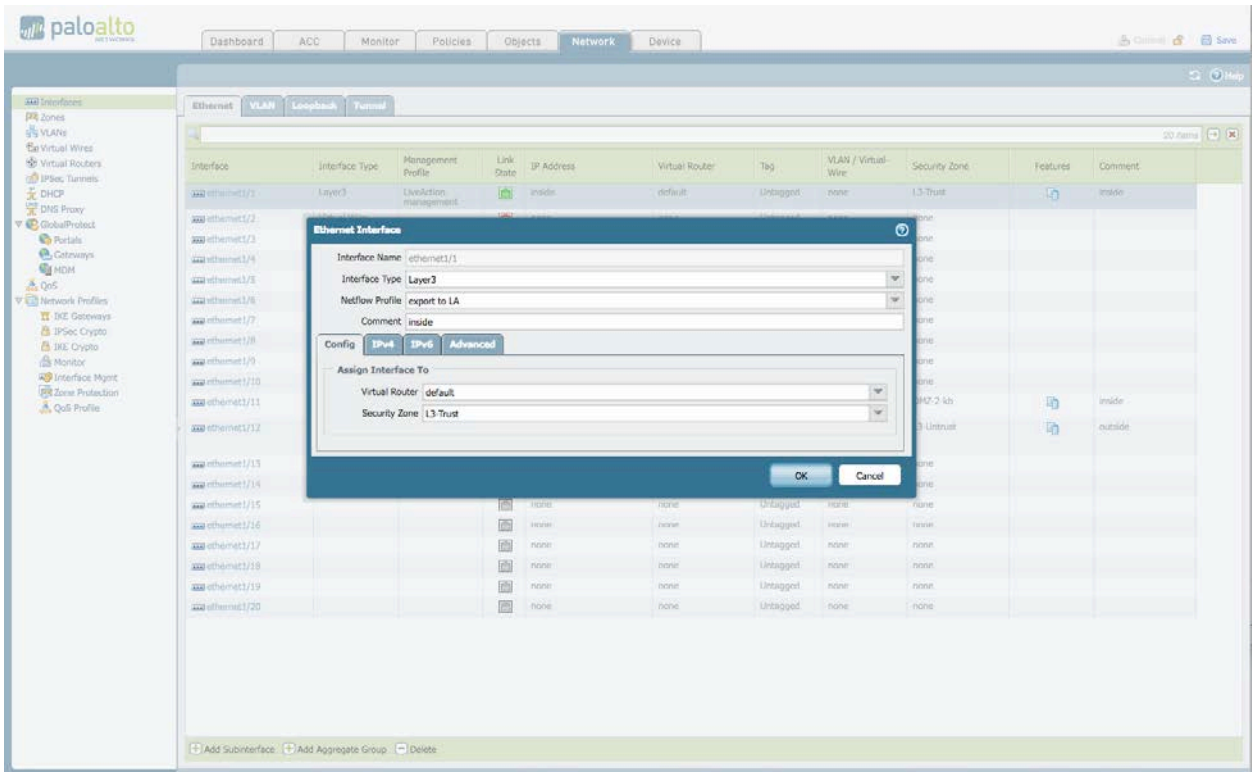
3. Enabling NetFlow Export on Palo Alto Networks Firewalls

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

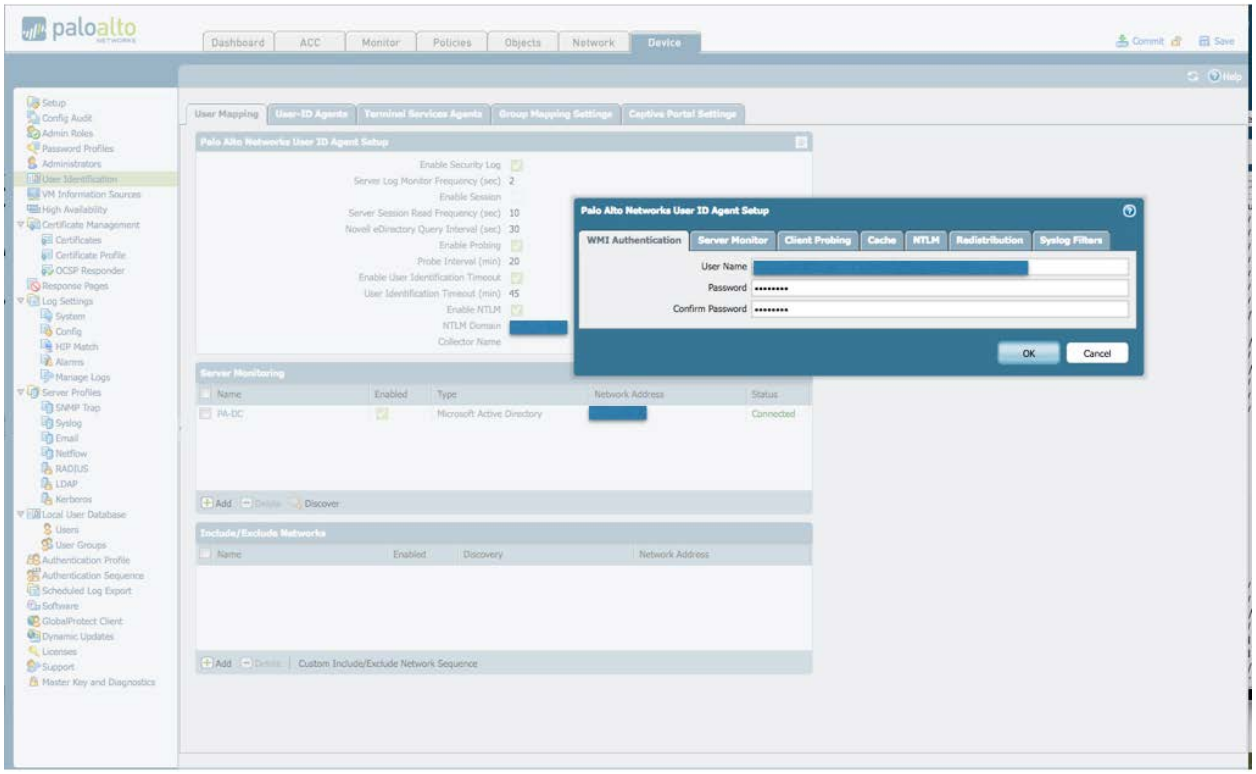
Navigate to “Device,” expand the Sever Profile accordion, and select “NetFlow.” Click on “Add” and enter the correct information for the LiveNX server or node. To include the extra Palo Alto Networks fields, User ID and Application ID, check the PAN-OS Field Types box.



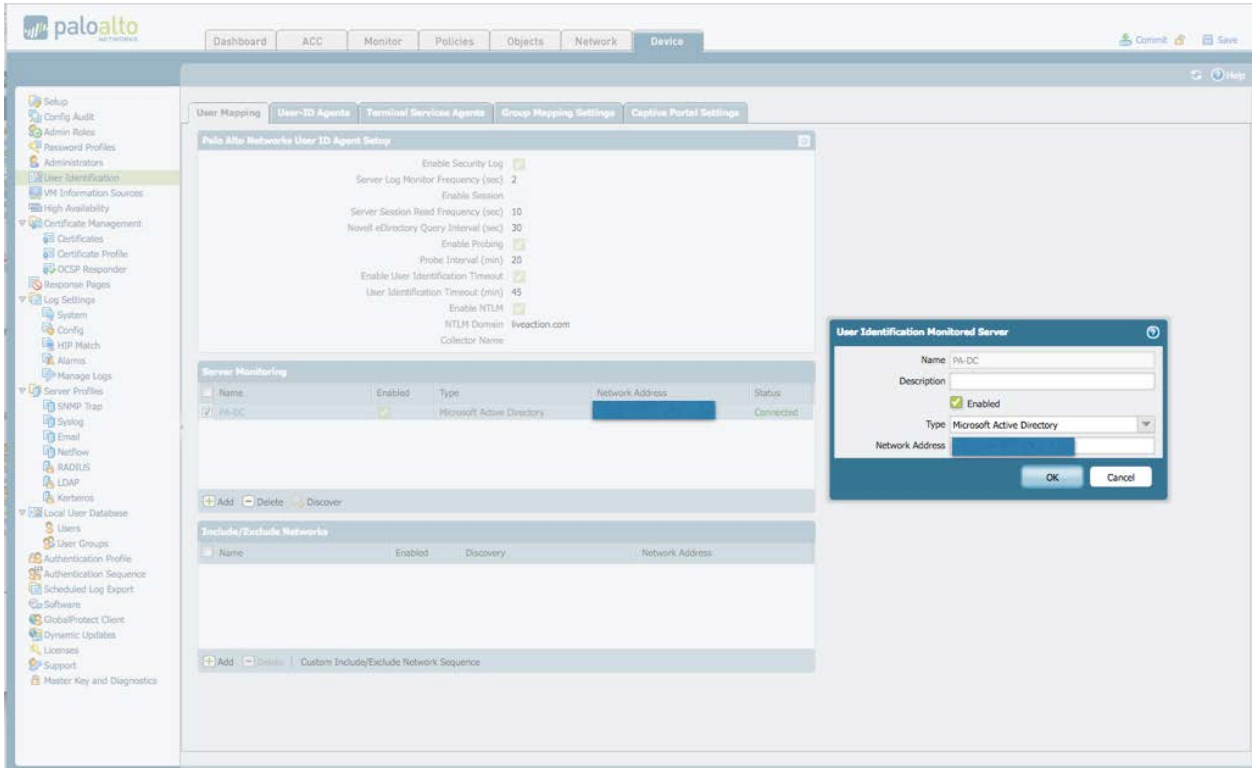
Select “OK” and the Exporter has been set up. Now we need to activate the export of the flows. This is done on an interface level. Now navigate to the Network Tab, and Interfaces. Select the Interface(s) that will be used to generate the NetFlow data. In the NetFlow Profile section add the Exporter that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



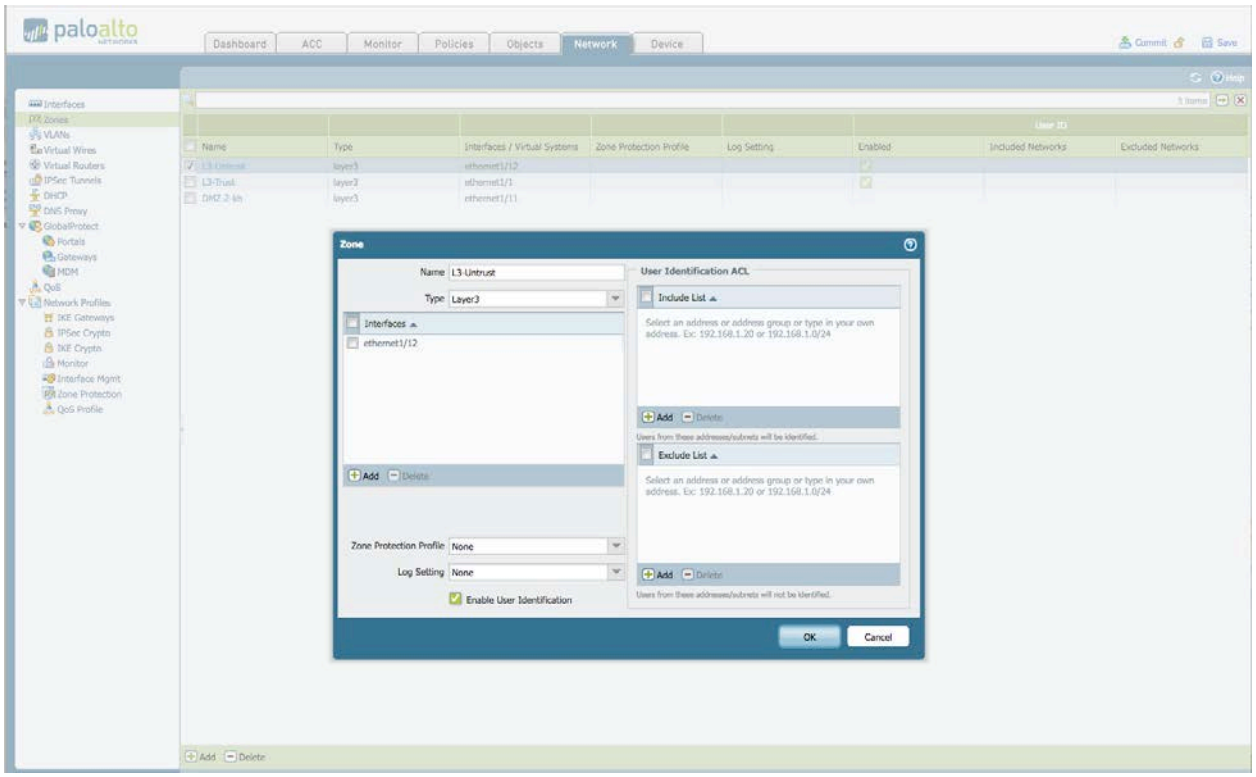
Once completed, commit the configuration. The Palo Alto Networks device should now be exporting flows to LiveNX. The next step is to enable the Palo Alto Networks device to use the Microsoft Active Directory to pull the User ID to IP address mapping. Palo Alto Networks can pull this information from 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.



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.



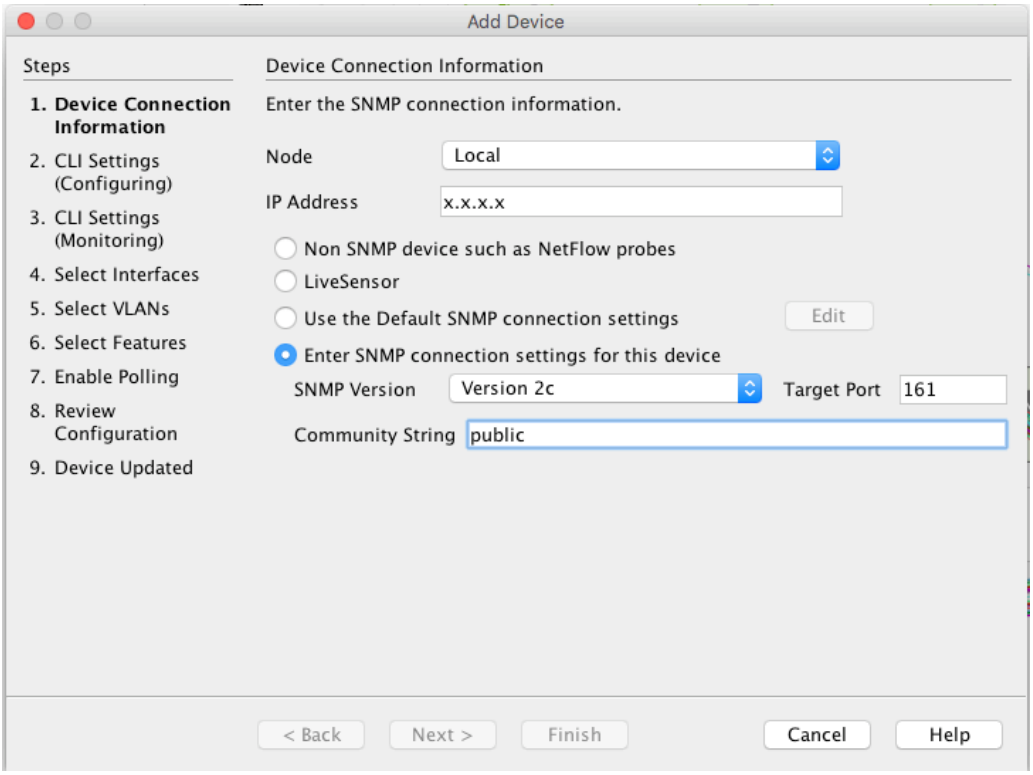
Once you have added the User Identification server, you must enable User ID identification on the Zones. To accomplish this, navigate to Network, Zones and edit each of the Zones that you want the User ID to be displayed on.



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

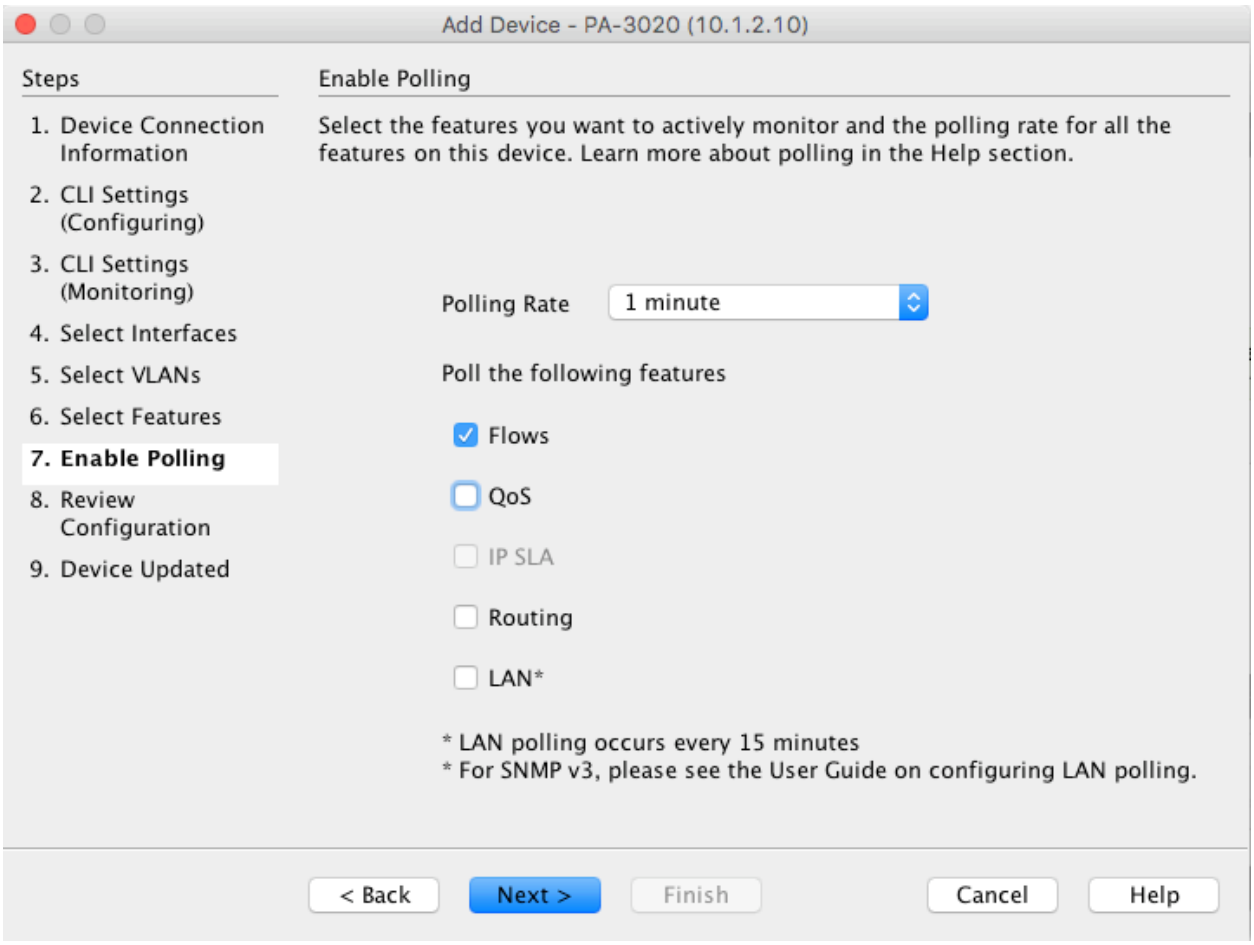
4. Adding the Palo Alto Networks Device(s) to LiveNX

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.

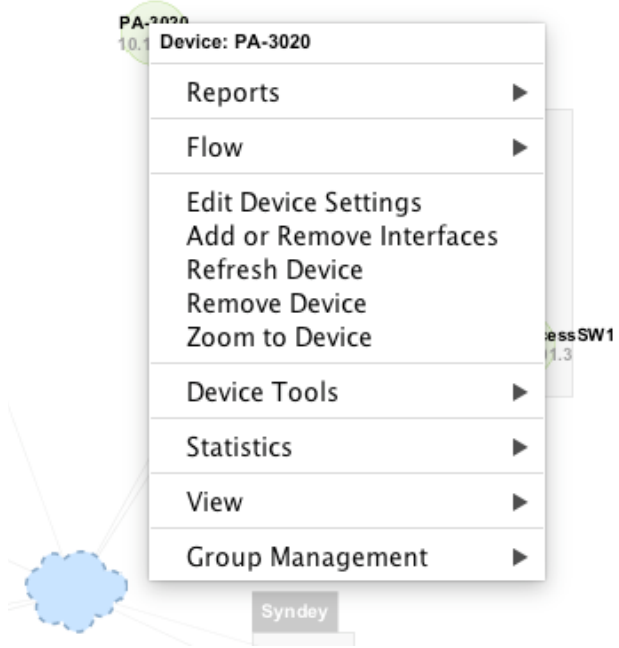


Select “Next” and LiveNX will now go through and find the interfaces in the Palo Alto Networks Device. Once you have selected the interfaces that NetFlow will be exported from, click “Next,” and as LiveNX will not know of any VLANS defined within the Palo Alto Networks select “Next.”

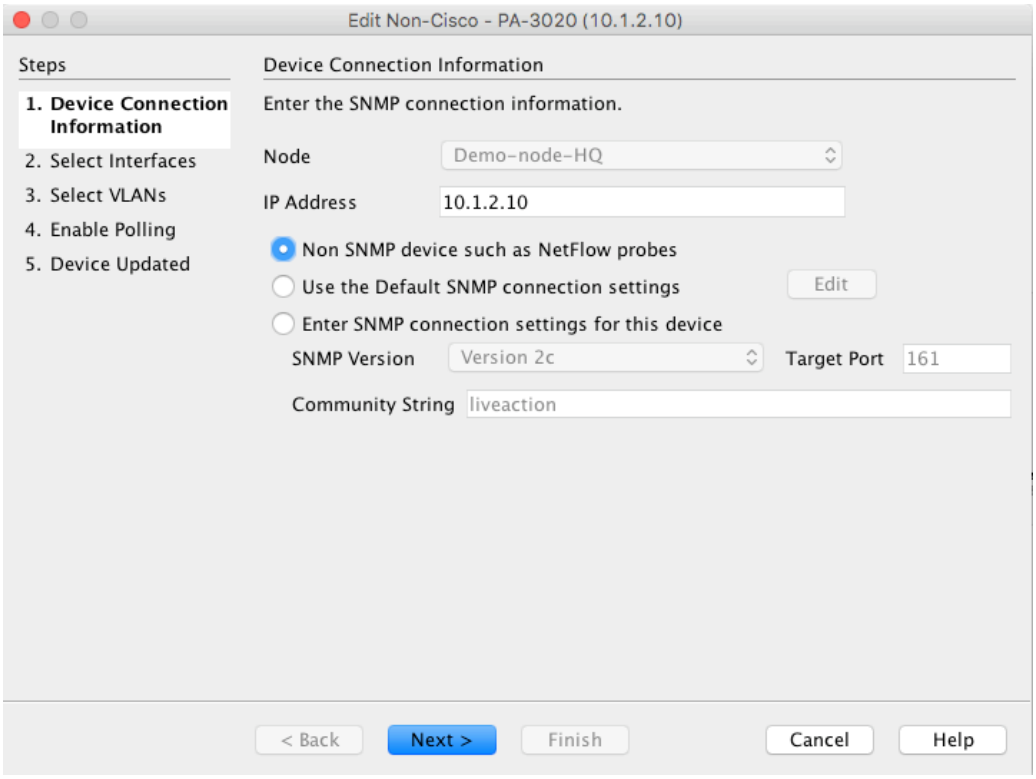
Now we can change the Polling Rate, leave it at one minute, and select Flows and click next to review the configuration and then select “Finish.”



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.”

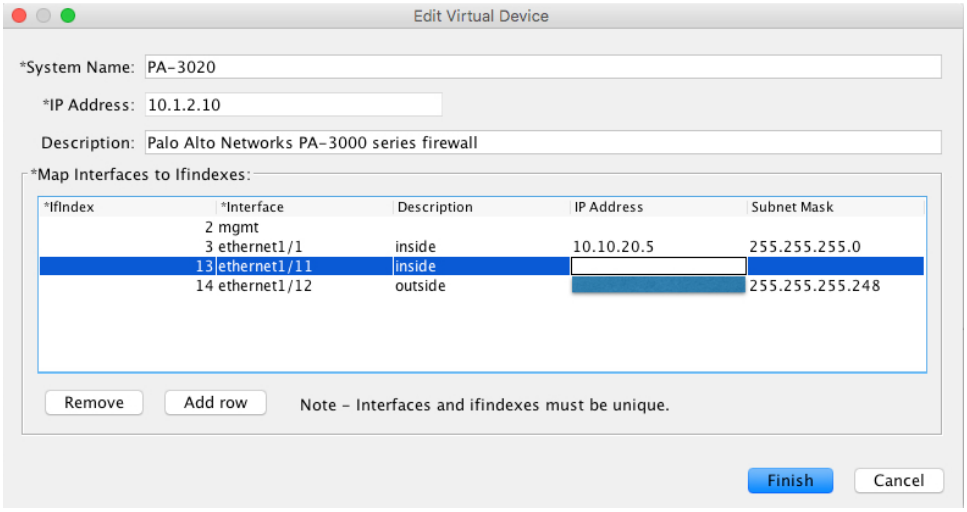


The Device Wizard will start and this time we are going to change the Device type to Non SNMP device, select “Next” and the Interface Table will be presented.



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

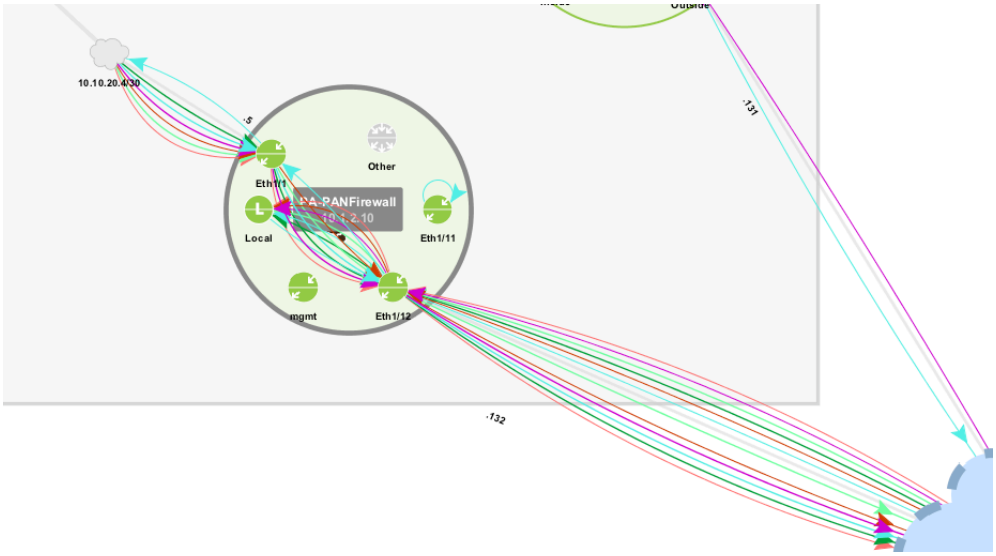
The Device will now connect to the correct networks. If the Palo Alto Networks Device is running in Layer 2 mode, enter the Management IP address.



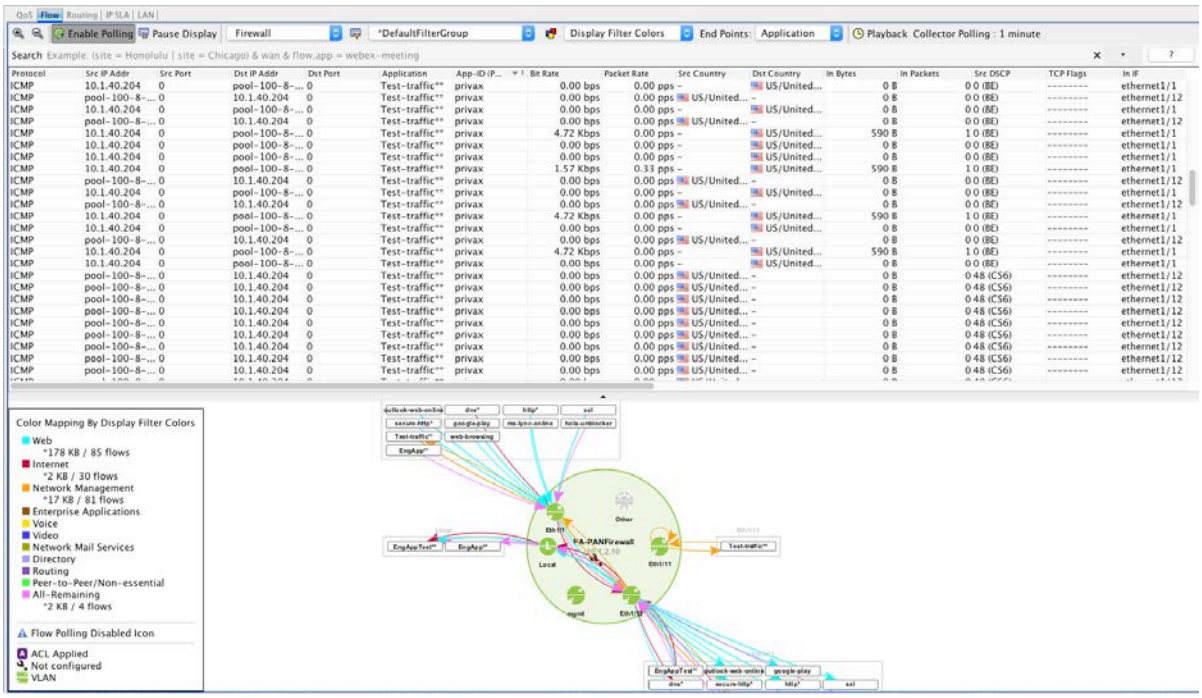
5. Reports

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.

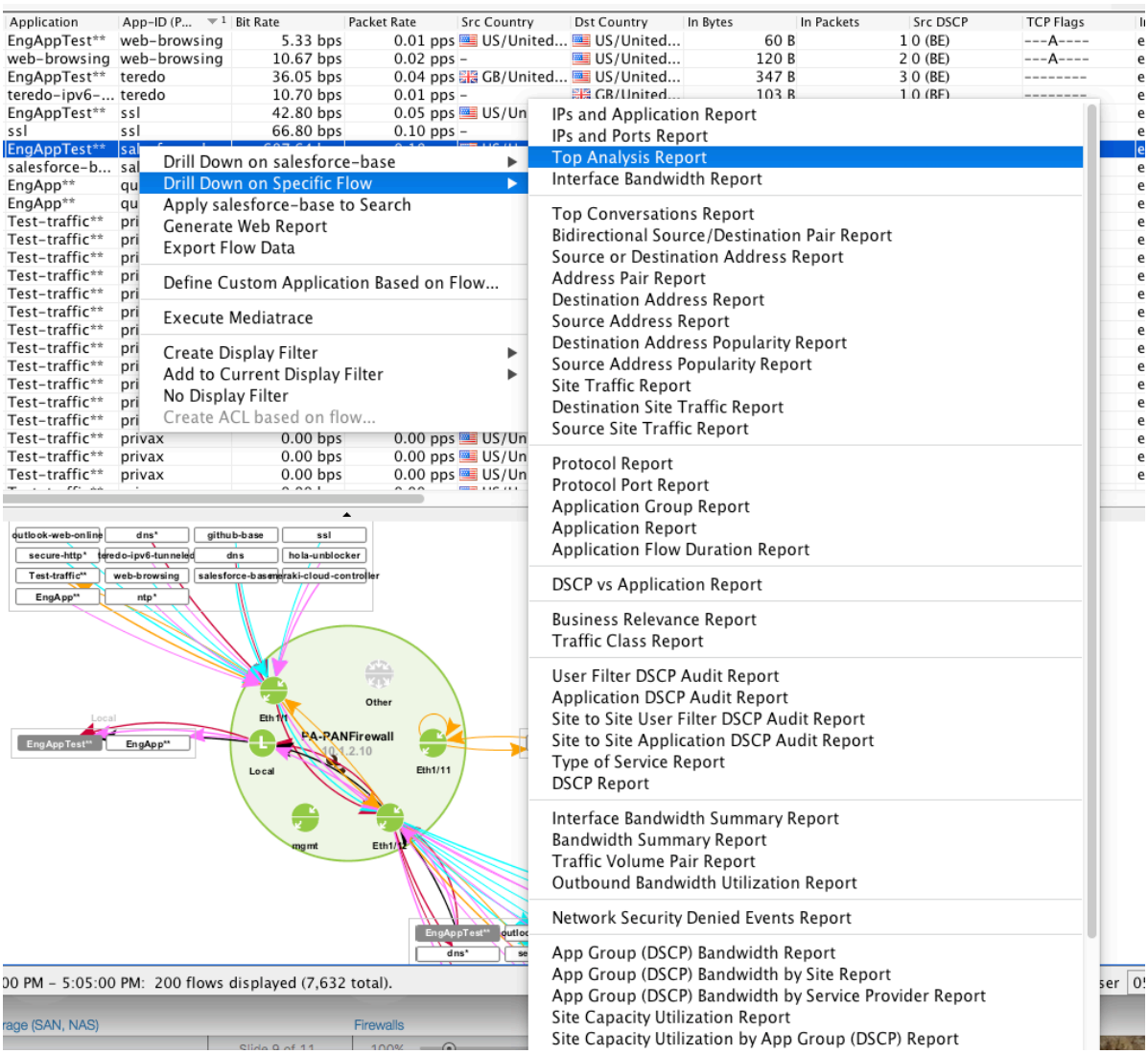
Let's start with a set of Visual Aids—the first is to monitor the Palo Alto Networks device itself and see what flow are active in real-time. From the main screen in the Java Client, change the flow display to Firewall. This will display all flows traversing the Palo Alto Networks.



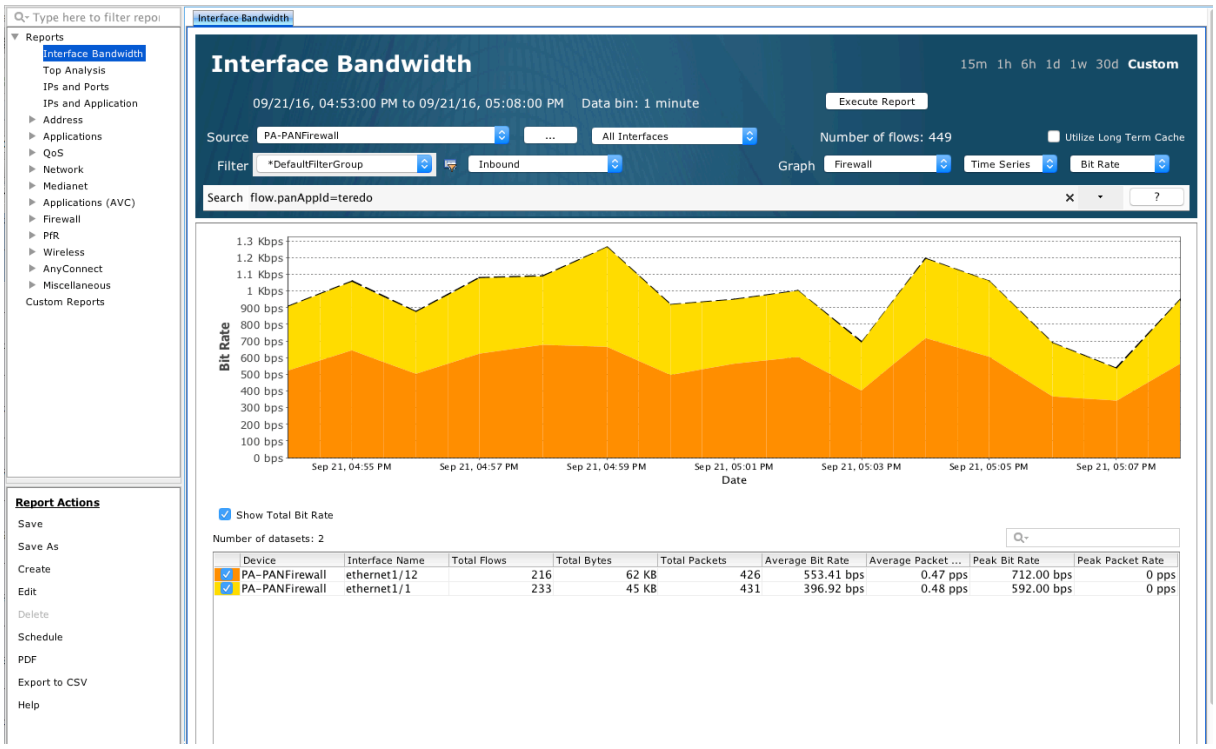
Now, if we double click onto the device we will see a real-time display of all the flows the Palo Alto Networks device is exporting. This view is updated every minute and can be used to find specific flows and drill down into more specific reports.



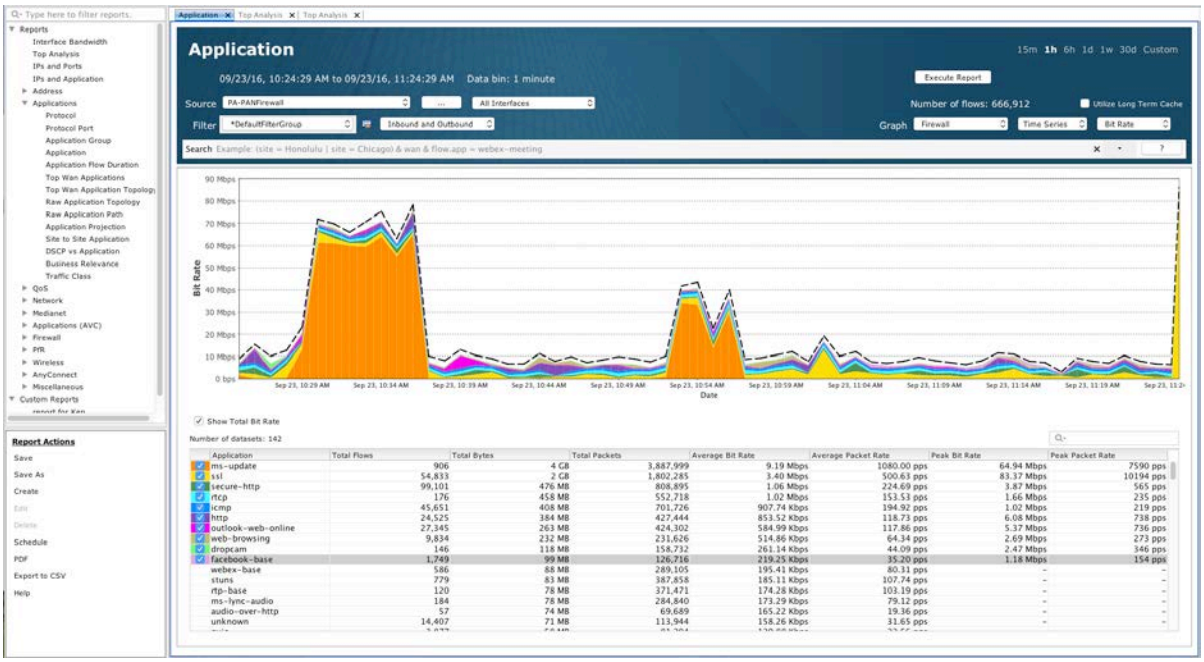
If we select a specific flow, it can be added to the search filter, and then only information destined to that application or IP address can be displayed. Or, we can drill down into more specific reports, like Top Analysis, or Interface Bandwidth reports.



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.



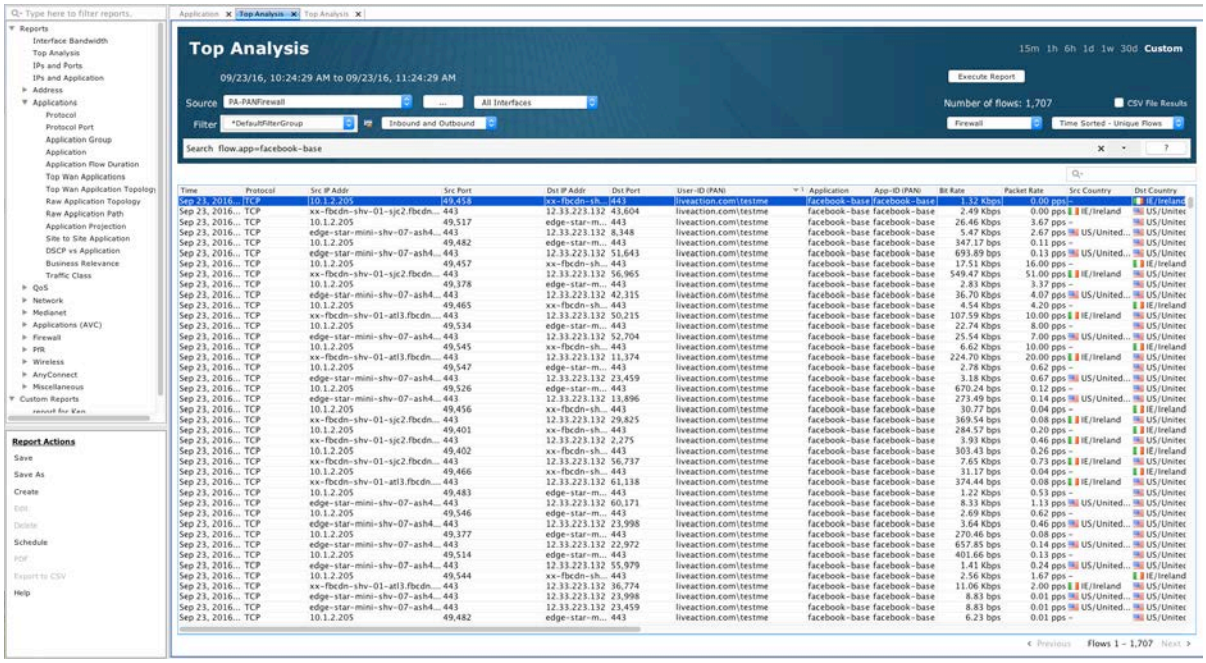
From this view, we can also drill down on specific applications and gather more information on Network Activity.

6. Use Cases

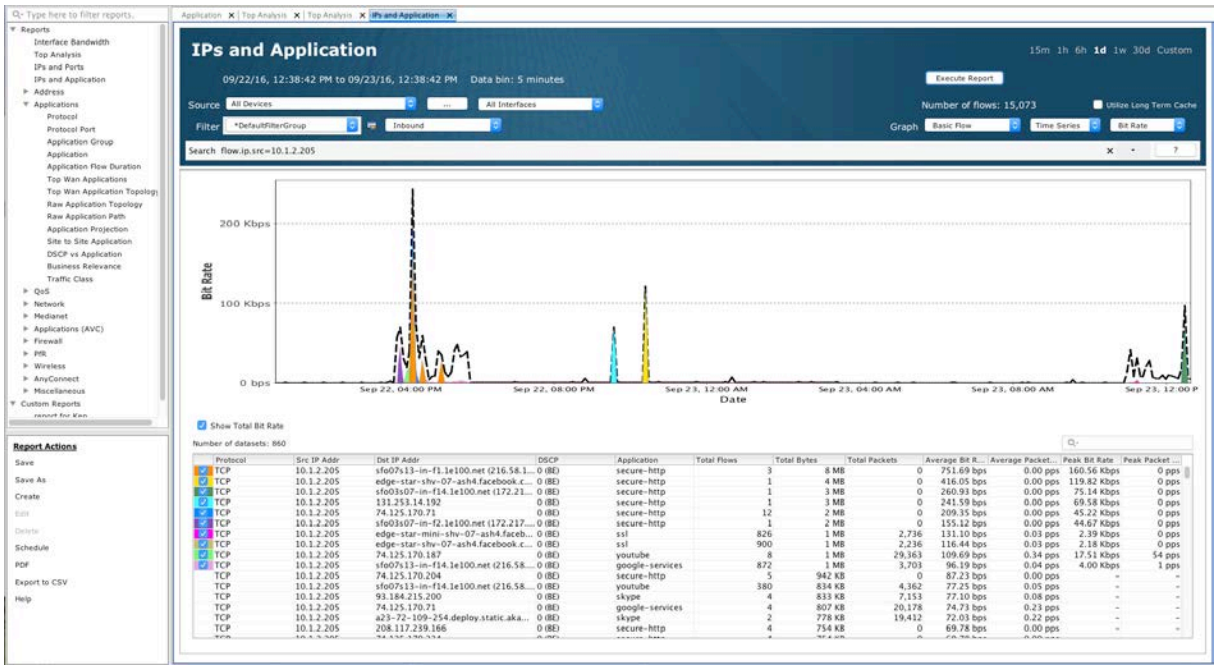
Let's look at some specific use cases that can help solve specific issues that may be generated within an organization.

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.

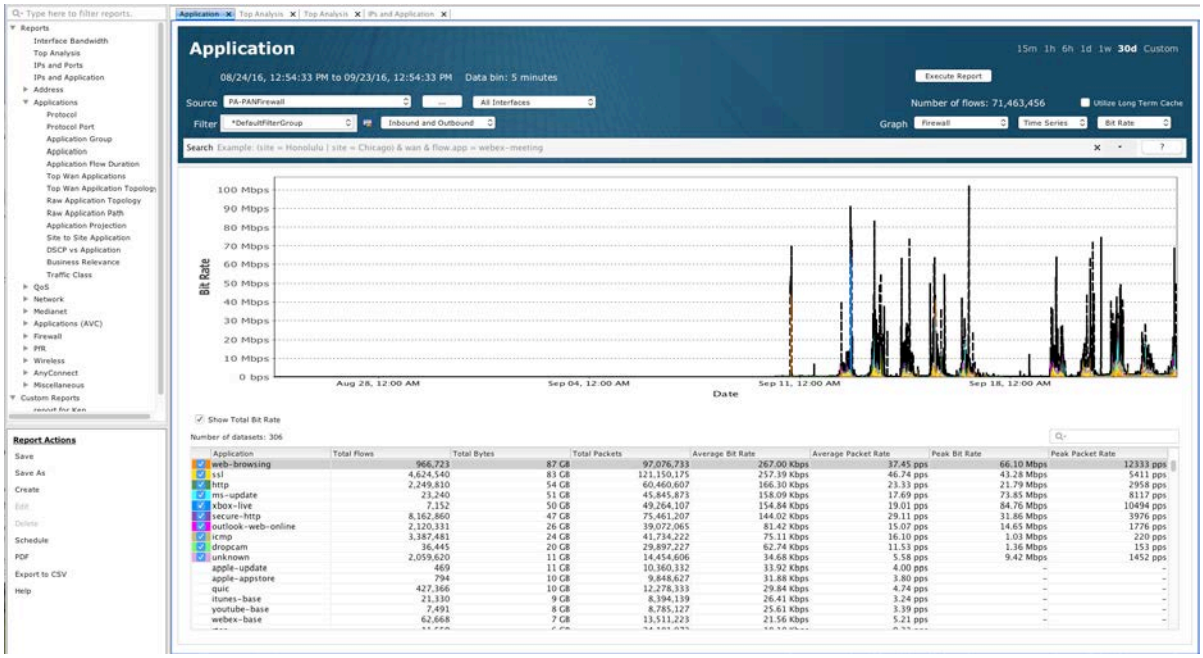


Not only can we see what external apps and systems were touched, but we can also see all the internal activity from that address, while the user was associated with that IP address. Select "All Devices" and the timeframe, set the graph to "Basic Flow" and execute the report.

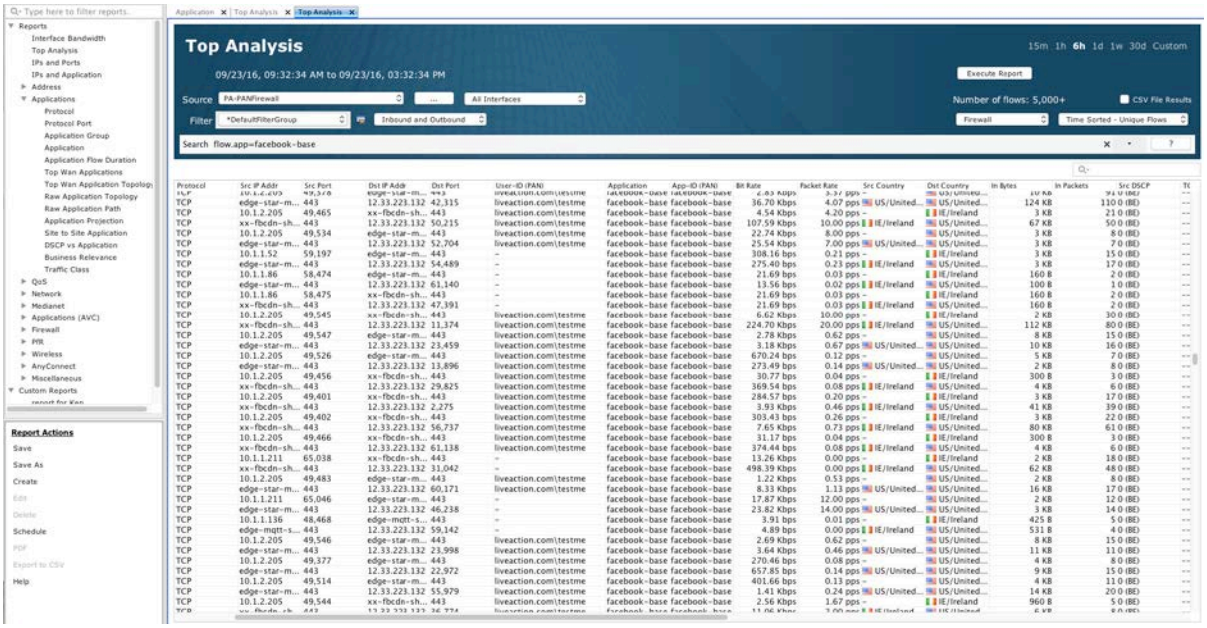


2) Data Leakage

Report of a large Data Leakage has occurred. Your mission as a network/security engineer is to try and find out who, what and when it occurred. You know the Application, but you don't know who did it, or when it was done. How do you figure it out? The first step is to look at the applications going through the firewall(s) over a period of time. Navigate to flow reports in LiveNX, select the period of time that you want to monitor, select the firewall that you will use as the source, select graph type to be firewall and execute the report.

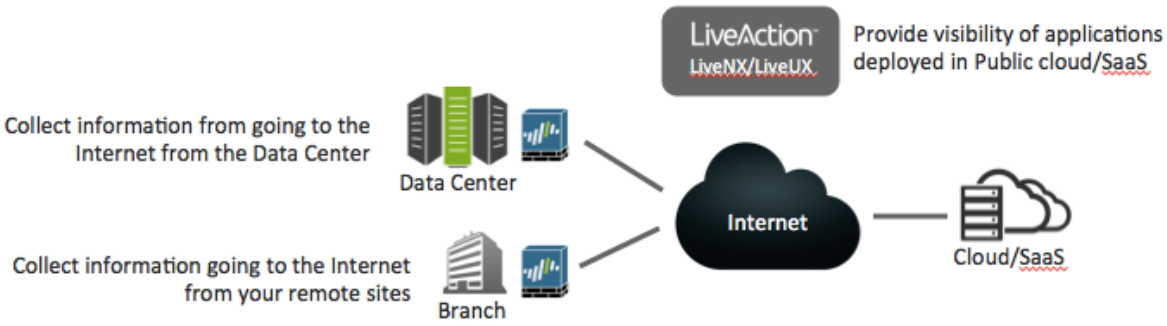


From this report we can drill down into the application where the data leakage was reported. So if we right click on the application, then drill down and run the Top Analysis we can now see the individual flows over this specific time frame and the users that generated the traffic. In this example, we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

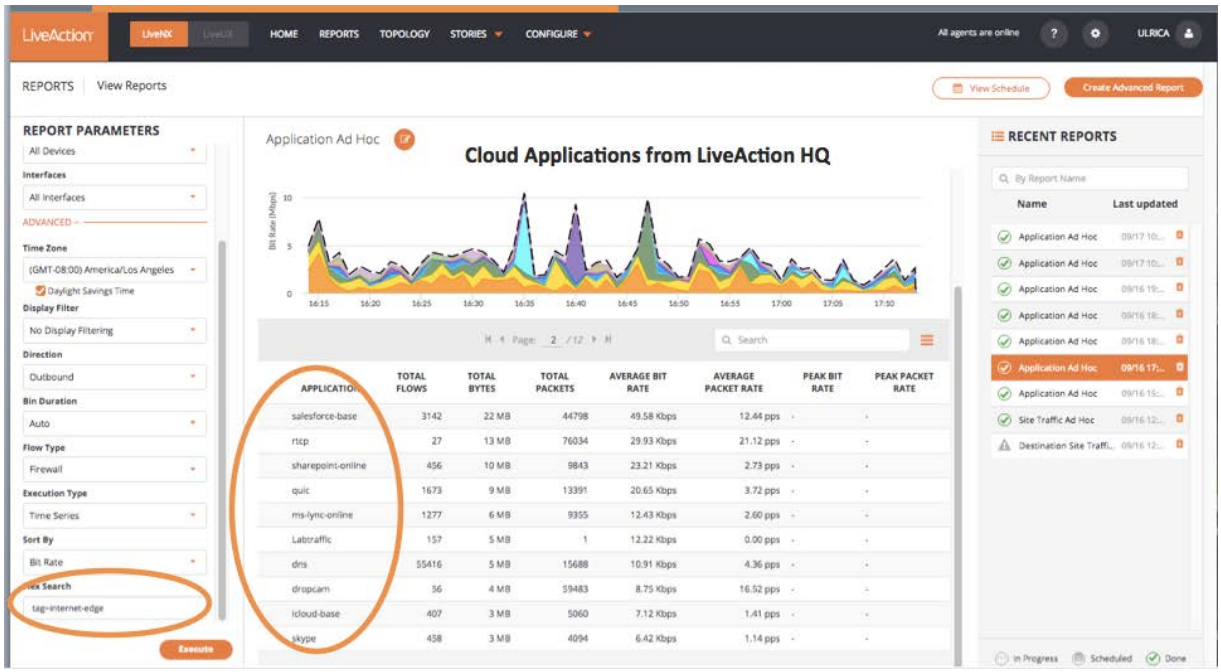


3) Shadow IT/Cloud Application Visibility

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.