

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 | 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.

palo<u>alto</u>	Dashboard ACC	Manitar Polic	ies Objects N	letwork Device	1			aa	🗑 Save
	((i) Hep
Gill Setup Garling Audit	-1								
Pataword Profiles	Name	Packets	Minutes	Active Timeout	PAN-OS Field Types	Name	Host	Port	
Administrators User Identification WH Information Sources WH Information Sources WH Information Sources With High Availability Vige Continuate Management Get Certificates	export to LA	1 NetFlow Server Profi	1. No	5		PA-Sampleator	10.1.10.247	2055	
CCSP Responder		1000	Name						
© Response Pages ▼ 12 Log Settings		Template Refresh	Rate						
System Config HP Match			Packets 20						
Alarms		Active Time	Active Timeout (min) 5						
V 1 Server Profiles			PAN-OS Field 1	lypes					
Systep		Name	NetFlow	Server	Port				
Sevies Tenal Sevies Rethere Rethere Rethere Sevies Se	Tass Doole	And Destru	it of the Helfflow server	30 10	06	Cancel			

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

		Loopback Terrind									
ANS shall Wires	5.										
rtual Routers	Interface	Interface Type	Management Profile	Link. State	IP Address	Virtuel Router	Тьр	VLAN / Virtual- Wire	Security Zone	Features	Comment
HCP	3322 ethnike(1/3 -	. Amywell		in	avaids.	definit;	Lintaged.	none	1.3-Trust	10	Inside
S Prony Automation	and ethicsvirts/2	-	U.M. MARKSHOWING	1967		11110	Carolinean -		a starter and s		
Portals	and ethemists/3	Ethernet Znierlau									
Datzwarys	data with second 1/4	Interface Na	ne ethemet1/1						one		
1DM	E\Limitetimetimeta	Interface Ty	pe Layer3						one		
work Profiles	size wither rest 1/6	Netflow Pro	ile export to LA					1	one		
KE Goteways	saul ethnimet 1/7	Comme	inside						one		
HE Crypto	and ethicsmint 170	Config 19v	Config 19v4 19v6 Advanced								
tonitor	same ethnomet 1/0	Assign Interface To							one		
nterface Mgort	and ethornat 1/10	Victorial	Virtual Router default						one		
205 Profile	and othernat1/11	Security Zone 13 Tout					191	0MZ-2 kb	助	imide	
	and ethernet1/12	2003	y Long (C) hog						3 Unitrust	To	outside
		-									
	and ethnemist 1/13						OK	Carcel	one		
	and effortenet 1714						ON	Curreer	one		
	and ethnemist 1/15			0		none		HOUSE	nune		
	and ethumiet1/16			100	Instan	Inches	Unitaggest	and a second	Tanan .		
	and other st1/17			[th]	nonit	borin	Untagger	none	none.		
	and ethemat 1/18			100	rionit	barie	Untagged	none	none		
	and other et1/19				nonii	incrist	Untagged	none	0008		
	and atherent1/20				none	none		0006	none		

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

, palo <u>alto</u>	Dashboard AC	C Monitor Policies Objects	Network Device		🍰 Commit 💰 🗟 Save
					5 Q (ie
Sotup	User Mapping User ID	Agents Territorial Services Agents Group Mappin 10 Agent Satur Enable Security Log Server Seniori Rose Proguercy (orc) 2 Server Seniori Rose Proguercy (orc) 30 Novel e0instro; Query Intervel (orc) 30 Enable Poting Probe Intervel (orc) 30 Enable Poting Probe Intervel (orc) 30 Enable Homan Enable ATIM Collector Name	Stitlings Captive Purch See Palo Aho Networks User 10 WHI Authentication 9 U Confirm	Agent Setup Agent Setup Inver Honitor Client Probing Cache F asr Name Password	NTLM Redistribution Systog Filters
Alarms	Server Nonitoring				
♥ 10 Server Profiles 10 SHVP Trap 10 SHVP Trap 10 Email 10 Trail 10 Trail 10 Trail 10 Trail 10 Trail 10 Trail	Name	Exabled Type Microsoft Active Directory	Network Address	Status Connected	
C Kerboros	Add - Denne De	scover			
V UM Local User Database S Users	Include (Exclude Nation				
Loren Lorongs Line Groups Line Groups Line Groups Line Groups Line Groups Line Groups Line Group Lin	Name	Enabled Discovery	Network Address		
	(+)Add (+)Device Cud	tom Include/Exclude Network Sequence			

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

GLUBD T INTERVOIDER	Dashboard ACC Monitor Policies Objects Network Device	👗 Commit: 💰 🛅 Save
		S (0)#4
Sohip Sohip Config Audit Sohip Config Audit Sohin Relea Anni Relea Anni Relea Anni Relea Anni Relea Anni Relea Sohip Sohip	Uter Happing User-DD Agenda Terminal Generation Agenda Group Phasping Settings Capilian Poundal Settings Mate Material Dubands Secure Log Photoper Pressure (sec) 2 Each After Material Security Log 2 Secure Log Photoper Pressure (sec) 3 Secure Log Photoper Pressure (sec) 3 Secure Log Photoper Pressure (sec) 3 Secure Each Photoper (sec) 3 Secure Each Photoper (sec) 3 Secure Each Photoper (sec) 3 Secure Each Photoper (sec) 3 Secure Each Photoper (sec) 3 Secure Each Photoper (sec) 3 Secure Each Photoper (sec) 3 Secure Each Photoper (sec) 3 Secure Each Photoper (sec) 3 Each Photoper (secure) Secure Thread Secure Thread Secure Thread Photo Photoper (secure) Secure Thread Secure Thread Secure Thread Photoper (secure) Secure Thread Type Network Address Secure Thread Photoper (secure) Secure Thread Secure Thread Secure Thread Secure Thread Photoper (secure) Secure Thread Secure Thread Secure Thread Secure Thread	User Identification Manitored Server Name PA-DC Description Frabled Type Microsoft Active Directory Network Address OK

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

, palo <mark>alto</mark>	Dashboard	ACC Monitor Po	licies Objects N	etwork	Device					🖄 Cammit 💰 🗟 Sava
										S @Hap
and Interfaces										1.10mm 🕀 🛞
PR/Zones										
En Virtual Wires	ET Name	Type	Interfaces / Virtual Systems	Zone Pr	obection Profile	Log Setting	Enabled	μ. Έ	ncluded Networks	Excluded Networks
Virtual Routers	V LI Orient	lener)	ethomist1712							
DHCP	DMZ 2-4h	layer3	ethernet1/1							
2 DNS Provy										
Contrais		Zone					(D		
Coteways MDM		Name	L3-Untrust		User Identific	ation ACL				
V Cos		Туре	Type Layer3		Include List					
F IKE Gateways B IPSec Crypto D IKE Crypto		Interfaces a			Select an address or address group or type in your own address Exc 192 168 1 20 or 193 168 1 1024					
		ethernet1/12								
interface Mgmt										
Pit Zone Protection										
						setas				
					Exclude List		-			
		(+)Add (-)thelete	(+)Add (-) (belota)			Select an address or address group or type in your own				
					address, Exc 31	92.168.1.20 or 192.168.1.	0/24			
		Zone Protection Profile	None							
		Log Setting	None	w	+ Add - Dr	leter				
			Carlo Ser Identification		Users from these ad-	inmen/subrets will not be iden	07ed.			
							and a second			
							Cancel			
	+ Add = Delete									
	🔿 Add . 📼 Delete									

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.

• • •		Add Device				
Steps	Device Connect	tion Information				
1. Device Connection Information	Enter the SNMP connection information.					
 CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces Select VLANs Select Features Enable Polling Review Configuration Device Updated 	Node IP Address Non SNMP LiveSensor Use the De Enter SNMP SNMP Versio Community	Local x.x.x.x device such as NetFlow probes fault SNMP connection settings connection settings for this device on Version 2c String public	C Edit			
	< Back	Next > Finish	Cancel 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."

9 | Palo Alto Networks Integration with LiveNX

• • •	Add Device - PA-3020 (10.1.2.10)
Steps	Select VLANs
 Device Connection Information CLI Settings (Configuring) CLI Settings (Monitoring) Select Interfaces Select VLANs Select Features Enable Polling Review Configuration Device Updated 	Select the VLANs you want to monitor on this device (maximum 25 VLANs).
	< Back Next > Finish Cancel Help

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."

10 | Palo Alto Networks Integration with LiveNX

00	Add Device - PA-3020 (10.1.2.10)
Steps	Enable Polling
1. Device Connection Information	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.
2. CLI Settings (Configuring)	
3. CLI Settings (Monitoring)	Polling Rate 1 minute
4. Select Interfaces	
5. Select VLANs	Poll the following features
6. Select Features	Z Flows
7. Enable Polling	TIOWS
8. Review Configuration	O QoS
9. Device Updated	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

11 | Palo Alto Networks Integration with LiveNX

• • •	Add Device - PA	-3020 (10.1.2.10)
Steps	Device Updated	
 Device Connection Information CLI Settings (Configuring) CLI Settings 	You have configured this do want to save the current co settings will not be lost wh Device Settings	evice successfully with the following settings (You may nfiguration to the device's startup config, so your en the device is restarted):
3. CLI Settings (Monitoring)	Setting Bolling Bate	Description
4. Select Interfaces	Flow Monitoring	Flow Collector
5. Select VLANs	Flow Polling Adjacency Polling	Enabled N/A
6. Select Features	, agacency ronning	
7. Enable Polling		
8. Review Configuration		
9. Device Updated	Interfaces	
	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."

12 | Palo Alto Networks Integration with LiveNX

R	eports	•
F	low	►
E A R R Z	dit Device Settings dd or Remove Interfac efresh Device emove Device oom to Device	es
D	Device Tools	►
S	tatistics	►
v	/iew	►
G	roup Management	•

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.

13 | Palo Alto Networks Integration with LiveNX

	Edit Non-	Cisco - PA-3020 (10.1.2.10)					
Steps	Device Connection	Information					
1. Device Connection Information	Enter the SNMP connection information.						
2. Select Interfaces	Node	Demo-node-HQ		\$			
3. Select VLANs	IP Address	10.1.2.10					
4. Enable Polling	Non SNMP dev	ice such as NetFlow probes					
5. Device Updated	O Use the Defau	It SNMP connection settings		Edit			
	Enter SNMP co	nnection settings for this device	•				
	SNMP Version	Version 2c	0	Target Port	161		
	Community Stri	ng liveaction					
	< Back Ne	ext > Finish	C	Cancel	Help		

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.

• • •		Edit Virtual Dev	vice					
*System Name:	PA-3020							
*IP Address:	10.1.2.10							
Description:	Palo Alto Networks PA-300	0 series firewall						
*Map Interface	s to Ifindexes:							
*lfIndex	*Interface	Description	IP Address	Subnet Mask				
	2 mgmt 3 ethernet1/1	inside	10.10.20.5	255.255.255.0				
	13 ethernet1/11 14 ethernet1/12	inside outside		255.255.255.248				
Remove Add row Note - Interfaces and ifindexes must be unique.								
				Finish Cancel				

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.

15 | Palo Alto Networks Integration with LiveNX

	Enable Polling 🖙 Pause Display	Firewall	🖸 📪 (*DefaultFilterG	roup	0	🛃 Displa	y Filter Colors	End Point	s: Application	Bayback Collect	or Polling : 1 minut	c	
Search Ex	ample: (site = Honolulu site = Ch	icago) & wan & flow,a	app = webes	-meeting									×	• 7
Protocol	Src IP Addr Src Port	Dst IP Addr Ds	t Port	Application	App-ID (P	w1 Bit	Rate	Packet Rate	Src Country	Dst Country	In Bytes In Packets	Ste DSCP	TCP Flags	In IF
ICMP	10.1.40.204 0	pool-100-8 0		Test-traffic**	privax		0.00 bps	0.00 pp	ps -	US/United	0.6	0 0 (BE)		ethernet1/1
ICMP	pool-100-8 0	10.1.40.204 0		Test-traffic**	privax		0.00 bps	0.00 pp	os 🔜 US/United		0 B	0 0 (8E)		ethernet1/12
ICMP	10.1.40.204 0	pool-100-8 0		Test-traffic**	privax		0.00 bps	0.00 pp	os -	US/United	. 0 B	0.0 (BE)		ethernet1/1
ICMP	pool-100-8 0	10.1.40.204 0		Test-traffic**	privax		0.00 bps	0.00 pp	os 🔜 US/United		0.8	0 0 (BE)		ethernet1/12
ICMP	10.1.40.204 0	pool-100-8 0		Test-traffic**	privax		4.72 Kbps	0.00 pp	os -	US/United	. 590 B	1 0 (BE)		ethernet1/1
ICMP	10.1.40.204 0	pool-100-8 0		Test-traffic**	privax		0.00 bps	0.00 pp	05 -	US/United	0.8	0.0 (BE)	Ar 10 Ar 10 Ar 10 Ar 10	ethernet1/1
ICMP	10.1.40.204 0	pool-100-8 0		Test-traffic**	privax		0.00 bps	0.00 pp	ps -	US/United	0.6	0 0 (BE)		ethernet1/1
ICMP	10.1.40.204 0	pool-100-8 0		Test-traffic**	privax		1.57 Kbps	0.33 pp	- 25	US/United	590 B	1 0 (BE)	10000000	ethernet1/1
ICMP	pool-100-8 0	10.1.40.204 0		Test-traffic**	privax		0.00 bps	0.00 pp	os MUS/United		0.8	0 0 (BE)	*******	ethernet1/12
ICMP	10.1.40.204 0	pool-100-8 0		Test-traffic**	privax		0.00 bps	0.00 pp	- 25	U\$/United	08	0 0 (BE)		ethernet1/1
ICMP	pool-100-8 0	10.1.40.204 0		Test-traffic"	privax		0.00 bps	0.00 pp	os s US/United	-	0.8	0.0 (BE)		ethernet1/12
ICMP	10.1.40.204 0	pool-100-8 0		Test-traffic**	privax		4.72 KBps	0.00 pp	ps -	US/Onited	590 8	10(8)		ethernet1/1
ICMP	10.1.40.204 0	pool-100-8 0		Test-traffic"	privax		0.00 bps	0.00 pp	as -	US/United	. 08	0.0 (BE)		ethernet1/1
ICMP	pool-100-80	10.1.40.204 0		Test-traffic**	privax		0.00 bps	0.00 pp	os mu US/United	THE LIF (Included	08	0 0 (BE)		ethernet1/12
ICMP	10.1.40.204 0	pool-100-80		Test-traffic**	privax		4.72 KDp1	0.00 pp	os -	US/United	. 590 B	10(85)		ethernet1/1
ICMP ICMP	10.1.40.204 0	10.1.40.204 0		Test-traffic**	privax		0.00 bps	0.00 pp	as all the itleited	US/United	. 08	0.48 (056)		ethernet1/1
ICMP	pool-100-80	10.1.40.204 0		Test-traffictt	privax		0.00 bps	0.00 pp	us/United		0.8	0.48 (CSG)		ethemet1/12
ICMP	pool-100-8- 0	10.1.40.204 0		Test-traffic##	privax		0.00 bps	0.00 pp	is US/United		0.0	0.48 (056)		ethemet1/12
ICMP	pool-100-80	10.1.40.204 0		Test-traffictt	privat		0.00 bps	0.00 pt	IS US/United		0.8	0.48 (C30)		ethemet1/12
CMP	pppl-100-8- 0	10.1.40.204 0		Test-traffic**	privax		0.00 bps	0.00 pg	as the US/United.		0.8	0.48 (CS6)		ethernet1/12
ICMP	pool-100-8- 0	10.1.40.204 0		Test-trafficett	privax		0.00 bps	0.00 pp	or In US/United.	1	0.8	0.48 (CS0)		othernot1/12
ICMP	ppol-100-8- 0	10.1.40.204 0		Test-traffic**	privax		0.00 bps	0.00 ps	IS US/United.		0.0	0.48 (056)		ethernet1/12
ICMP	pool-100-8- 0	10.1.40.204 0		Tast_trafficts	privax		0.00 bps	0.00 ps	s IIS/IInited.	2	0.8	0.48 (CS6)		atharnat1/12
ICMP	ppol-100-8- 0	10 1 40 204 0		Test-traffic**	privax		0.00 bps	0.00 p	is a US/United		0.8	0.48 (CS6)		ethemet1/12
10110	1 100 0 0	10.1.40.204 0		T	privax		0.00 000	0.00 pp	and the first for the			0.40 (000)		-1 +1.11%
Color Mag Web 17 Interm 22 Netwo 17 Enterp Voice Voice Voice Voice Netwo Direct Routin Peer-1 All-Re 22 All-Re 24 Color Mag 10 10 10 10 10 10 10 10 10 10	pping By Display Filter Colors 8 KB / 85 flows 8 / 85 / 30 flows 9 / 4 flows 9 / 4 flows 9 / 4 flows 9 / 4 flows			Englag Inter	des" gas give by web-towering Beyleys"	Billion and	al Br Nebulko Diff Da Ta Ta Ta Ard	Aar Oliver Ufficewalt East12	Track					
ACL A	pplied onfigured							Eng	AppTest" stationk amb	entin) geogle-play				

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.

16 | Palo Alto Networks Integration with LiveNX

Application	App-ID (P 🔍 1	Bit Rate Packet	t Rate Src Country	Dst Country In Bytes	In Packets	Src DSCP	TCP Flags	
EngAppTest**	web-browsing	5.33 bps	0.01 pps 🚟 US/Unit	ed 🔤 US/United	60 B	1 0 (BE)	A	e
web-browsing	web-browsing	10.67 bps	0.02 pps -	🔤 US/United	120 B	2 0 (BE)	A	e
EngAppTest**	teredo	36.05 bps	0.04 pps 🚟 GB/Unit	ed 🔜 US/United	347 B	3 0 (BE)		e
teredo-ipv6	teredo	10.70 bps	0.01 pps –	GB/United	103 B	1.0 (BF)		e
EngAppTest**	ssl	42.80 bps	0.05 pps 🔤 US/Un	IPs and Application Repo	rt			e
ssl	ssl	66.80 bps	0.10 pps –	IPs and Ports Report				e
EngAppTest**	sal Drill Dow	n on salesforce-bas	se 🕨	Top Analysis Report				e
salestorce-b	sal Drill Dow	un on Specific Flow		Interface Bandwidth Repo	ort			e
EngApp**	qu Annhu ca	lasforso, base to See	reh					e
EngApp Tost_traffic**	qu Appiy sa	lestorce-base to Sea	arcn	Top Conversations Repor	t			e
Test_traffic**	Generate	e Web Report		Bidirectional Source/Dest	ination Pair Repor	t		0
Test-traffic**	Export F	low Data		Source or Destination Ad	dress Report			e
Test-traffic**	pri p.c. c			Address Pair Report	aress nepore			e
Test-traffic**	pri Define C	ustom Application B	ased on Flow	Destination Address Done				e
Test-traffic**	pri Evocuto	Madiatraca		Destination Address Repo	ort			e
Test-traffic**	pri	meulatiace		Source Address Report				e
Test-traffic**	pri Create D	isplay Filter		Destination Address Popu	alarity Report			e
Test-traffic**	pri Add to C	'urrent Display Filter		Source Address Popularit	y Report			e
Test-traffic**	pri Na Diaul	urrent Display Filter		Site Traffic Report				e
Test-traffic**	pri No Displ	ay Filter		Destination Site Traffic Re	eport			e
Test-traffic**	pri Create A	CL based on flow		Source Site Traffic Report				e
Test-traffic**	privax	0.00 bps	0.00 pps 🔤 US/Un	source site frame kepon	•			e
Test-traffic**	privax	0.00 bps	0.00 pps 🔤 US/Un	Protocol Report				e
Test-traffic**	privax	0.00 bps	0.00 pps US/Un	Protocol Port Report				e
				Application Group Report				
				Application Group Report	L			
outlook-web-online	dns* githu	ib-base ssl		Application Report	Dement			
secure-http* tere	do-ipv6-tunneled o	dns hola-unblocker		Application Flow Duration	h Keport			
Test-traffic**	web-browsing salesfo	orce-basemeraki-cloud-controller		DSCP vs Application Repo	ort			
EngApp**	ntp*		_	bber vs Application Repe				
				Business Relevance Repo	rt			
				Traffic Class Report				
			÷	User Filter DSCP Audit Re	port			
		Othe	er	Application DSCP Audit R	eport			
Loca		Eth 1/1		Site to Site User Filter DS0	P Audit Report			
		PA-PANFirewa	all 💽	Site to Site Application D	CP Audit Report			
EngAppTest**	EngApp~	101.2.10		Type of Service Report	CI Addit Report			
		Local	Eth1/11	Type of Service Report				
				DSCP Report				
		\ 🔷 🛸		Interface Bandwidth Sum	mary Report			
		N 19 19 19 19 19 19 19 19 19 19 19 19 19		Bandwidth Summany Dan	ant vicepoir			
		ang mt Eti	h1/12	Bandwidth Summary Rep				
				Traffic Volume Pair Repoi	rt			
				Outbound Bandwidth Util	ization Report			
				Network Security Denied	Events Report			
			EngApprest outloc	Ann Group (DSCD) Brade	idth Donort			
			ans" se	App Group (DSCP) Bandw	ideb by Cite Domoni			-
00 PM - 5:05:00	PM: 200 flows	displayed (7,632 total).	App Group (DSCP) Bandw	inter by Site Report		-	ser 0
				App Group (DSCP) Bandw	idth by Service Pro	wider Report		
rage (SAN, NAS)		Firew	alls	Site Capacity Utilization R	eport			
		Slide 9 of 11 10	0%	Site Capacity Utilization b	y App Group (DSC	P) Report		A 10.5

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.

17 | Palo Alto Networks Integration with LiveNX



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.

18 | Palo Alto Networks Integration with LiveNX



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

19 | Palo Alto Networks Integration with LiveNX

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.

Q- Type here to filter reports.	Application X Top Analysis	K Top Analysis X							
Reports				The left is the second s					
Interface Bandwidth	and the second second								
Top Analysis	l op Analys	SIS						15m 1h 6h 1d 1w 3	Od Custom
10x and Bosts									
ins and norts	an institute water						English Ran		
IPs and Application	09/23/16, 10:2	24:29 AM to 09/23/16, 11:24:21	AM				Execuse Rep	2015	
► Address			100	the second s					
▼ Applications	Source PA-PANFirewall		All 1	Interfaces C			Number of flo	ws: 1,707	CSV File Results
Protocol		and the second s	10				and the second second		
Protocol Port	Filter *DefaultFilterGr	roup 🔁 🔄 Inbound and	Outbound C				Frewall	Time Sorted - Uni	que Flows 😑
Analization Group		and an an an and a state of the			the second s		2.5		
Application	Search flow.app=facebo	ok-base						х -	7
Appreciation		An order to have							
Application How Duration								0	
Top Wan Applications	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1							14	
Top Wan Application Topology	Time Protocol	Src IP Addr	Src Port	Dst IP Addr Dst Port	User-ID (PAN)	* 1 Application App-ID (PAN)	Bit Rate 1	Packet Rate Src Country	Dst Country
Raw Application Topology	Sep 23, 2016 TCP	10.1.2.205	49,458	xx-fbcdn-sh 443	liveaction.com\testme	facebook-base facebook-base	1.32 Kbps	0.00 pps -	I IE/Ireland
Raw Application Path	Sep 23, 2016 TCP	xx-fbcdn-shv-01-sjc2.fbcdn.	. 443	12.33.223.132 43,604	liveaction.com\testme	facebook-base facebook-base	2.49 Kbps	0.00 pps II IE/Ireland	MUS/United
Application Projection	Sep 23, 2016 TCP	10.1.2.205	49,517	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	26.46 Kbps	3.67 pps -	MUS/Uniter
City in City Application	Sep 23, 2016 TCP	edge-star-mini-shv-07-ash4.	. 443	12.33.223.132 8,348	liveaction.com\testme	facebook-base facebook-base	5.47 Kbps	2.67 pps M US/United.	🔜 US/Uniter
ane to ane application	Sep 23, 2016 TCP	10.1.2.205	49,482	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	347.17 bps	0.11 pps =	S/Uniter
DSCP vs Application	Sep 23, 2016 TCP	edge-star-mini-shv-07-ash4.	_ 443	12.33.223.132 51,643	liveaction.com\testme	facebook-base facebook-base	693.89 bps	0.13 pps 🔜 US/United.	📑 US/Unitec
Business Relevance	Sep 23, 2016 TCP	10.1.2.205	49,457	xx-fbcdn-sh 443	liveaction.com\testme	facebook-base facebook-base	17.51 Kbps	16.00 pps -	E IE/Ireland
Traffic Class	Sep 23, 2016 TCP	xx-fbcdn-shv-01-sjc2.fbcdn.	443	12.33.223.132 56,965	liveaction.com\testme	facebook-base facebook-base	549.47 Kbps	51.00 pps I IE/Ireland	S/Uniter
▶ Qo5	Sep 23, 2016 TCP	10.1.2.205	49,378	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	2.83 Kbps	3.37 pps -	MUS/Uniter
in Nationale	Sep 23, 2016 TCP	edge-star-mini-shv-07-ash4.		12.33.223.132 42,315	liveaction.com\testme	facebook-base facebook-base	36.70 Kbps	4.07 pps 🔜 US/United.	🔜 US/Uniter
h Medicael	Sep 23, 2016 TCP	10.1.2.205	49,465	xx=fbcdn=sh 443	liveaction.com\testme	facebook-base facebook-base	4.54 Kbps	4.20 pps -	E E/Ireland
P Reparet	Sep 23, 2016 TCP	xx-fbcdn-shv-01-atl3.fbcdn.	. 443	12.33.223.132 50,215	liveaction.com\testme	facebook-base facebook-base	107.59 Kbps	10.00 pps I I IE/Ireland	US/Uniter
 Applications (AVC) 	Sep 23, 2016 TCP	10.1.2.205	49,534	edge-star-m 443	liveaction.com\testime	facebook-base facebook-base	22.74 Kbps	8.00 pps -	US/Uniter
Frewall	Sep 23, 2016 TCP	edge-star-mini-shv-07-ash4.	. 443	12.33.223.132 52,704	liveaction.com\testme	facebook-base facebook-base	25.54 Kbps	7.00 pps M US/United.	🔜 US/Uniter
► PIR	Sep 23, 2016 TCP	10.1.2.205	49,545	xx-fbcdn-sh 443	liveaction.com\testme	facebook-base facebook-base	6.62 Kbps	10.00 pps -	E IE/Ireland
► Wireless	Sep 23, 2016 TCP	xx-fbcdn-shv-01-atl3.fbcdn.	. 443	12.33.223.132 11,374	liveaction.com/testme	facebook-base facebook-base	224.70 Kbps	20.00 pps 1 It/Ireland	US/United
 AnvConnet 	Sep 23, 2016 TCP	10.1.2.205	49,547	edge-star-m 443	liveaction.com/testme	facebook-base facebook-base	2.78 Kbps	0.62 pps -	US/Uniter
h Macallanana	Sep 23, 2016 TCP	edge-star-mini-shv=07-ash4.	_443	12.33.223.132 23,439	liveaction.com\testme	facebook-base facebook-base	3.18 Kbps	0.67 pps su US/United.	US/United
P Piscelaneurs	Sep 23, 2016 ICP	10.1.2.205	49,520	eoge-star-m 443	Inveaction.com/testime	facebook-base facebook-base	670.24 bps	0.12 pps -	US/United
Custom Reports	Sep 23, 2016 TCP	edge-star-mini-shv-0/-ash4.	493	12.33.223.132 13,896	Inveaction.com\testime	facebook-base facebook-base	273.49 bps	0.14 pps su US/United.	Solution of the second
record for Ken	Sep 23, 2016 TCP	10.1.2.203	49,430	XX-10C01-51	inveaction.com/testine	racebook-base racebook-base	30.77 bps	0.04 pps -	I IE/retand
	Sep 23, 2016 TCP	xx-rocon-snv-01-sjc2.rocon.	443	12.33.223.132 29,823	inveaction.com/testine	racebook-base racebook-base	309.54 bps	0.08 pps a sic/ireland	us/united
	Sep 23, 2016. TCP	up flying shu fill sig? flying	49,401	13 32 332 123 3 376	liveoction com/testine	facebook base facebook base	2 02 Khud	0.45 pps	115 /lieiter
eport Actions	Sep 23, 2010 TCP	10.1.2.205	40.402	se ssees as ears	Investion comitestine	facebook - base facebook - base	303.43 hors	0.36 pps	I If ileland
ave	Sep 23, 2016 TCP	10.1.2.205	49,402	xx-10c0n-sn 443	Inveaction.com/testine	facebook-base facebook-base	303.43 Dps	0.26 pps -	E IE/Ireland
	Sep 23, 2016 TCP	10.1.2.205	445	12.55.225.152 30,737	Investion.com/testine	facebook - base facebook - base	21.17 box	0.04 pps - ic/ireland	I I E // reland
ave As	Sep 23 2016 TCP	xx-fbrdn-shy-01-atl3 fbrdn	443	12 33 223 132 61 138	liveaction com/testme	facebook - base facebook - base	374.44 hos	0.08 nos 11E/ireland	US/Uniter
reate	Sep 23, 2016 TCP	10.1.2.205	49 483	edge-star-m 443	liveaction com/testme	farebook-base farebook-base	1.22 Khos	0.53 005 -	III US/Uniter
	Sep 23 2016 TCP	edoe_star_mini_shy_07_ash4	443	12 13 223 132 60 171	liveration comitestme	Facebook -base facebook -base	8 33 Khos	1.13 pps IIIS/IInited	IIS/IIniter
	Sep 23, 2016 TCP	10.1.2.205	49.546	edge-star-m., 443	liveaction.com\testme	facebook-base facebook-base	2.69 Kbos	0.62 pps -	US/Uniter
	Sep 23 2016 TCP	edoe-star-mini-shy-07-ash4	443	12 33 223 132 23 998	liveaction com\testme	farebook-base farebook-base	3.64 Khos	0.46 pos IIIS/United	III US/Uniter
	Sep 23, 2016, TCP	10.1.2.205	49 377	edne-star-m. 443	liveaction com\testme	facebook-base facebook-base	270.46 bos	0.08.005 -	III US/Uniter
chedule	Sep 23, 2016 TCP	edge-star-mini-shy-07-ash4	443	12.33.223.132.22.972	liveaction.com\testme	facebook-base facebook-base	657.85 bps	0.14 pps MUS/United.	US/Uniter
	Sep 23, 2016 TCP	10.1.2.205	49,514	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	401.66 bps	0.13 pps -	US/Uniter
N.O	Sep 23, 2016 TCP	edge-star-mini-shy-07-ash4.	. 443	12.33.223.132 55.979	liveaction.com\testme	facebook-base facebook-base	1.41 Kbps	0.24 pps 🔜 US/United.	SUS/United
	Sep 23, 2016 TCP	10.1.2.205	49,544	xx-fbcdn-sh 443	liveaction.com\testme	facebook-base facebook-base	2.56 Kbps	1.67 pps -	E IE/Ireland
	Sep 23, 2016 TCP	xx-fbcdn-shv-01-atl3.fbcdn.	. 443	12.33.223.132 36,774	liveaction.com\testme	facebook-base facebook-base	11.06 Kbps	2.00 pps I IE/Ireland	US/Uniter
lelp .	Sep 23, 2016 TCP	edge-star-mini-shv-07-ash4.	_443	12.33.223.132 23.998	liveaction.com\testme	facebook-base facebook-base	8.83 bps	0.01 pps MUS/United.	MUS/United
	Sep 23, 2016 TCP	edge-star-mini-shv-07-ash4.	. 443	12.33.223.132 23.459	liveaction.com\testme	facebook-base facebook-base	8.83 bps	0.01 pps MUS/United.	MUS/Uniter
	Sep 23, 2016 TCP	10.1.2.205	49,482	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	6.23 bps	0.01 pps -	US/Uniter
			100000						
								e final de fierre t	1.262
									ALCONE CONTRACTOR

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.

20 | Palo Alto Networks Integration with LiveNX



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.

21 | Palo Alto Networks Integration with LiveNX

and a set the set of t	the second se							
Enace Bandwidth	Application						15m (1b) 6b	otherwo sol on
o Analysis	Application							
and Ports	200 (Carles - 2012) 201					() and the second second	12	
and Application	08/24/16, 12:54:33	PM to 09/23/16, 12:54:33 PM Data bi	in: 5 minutes			Execute Report		
ress			Contraction of the local division of the loc					
lications	Source PA-PANFirewall	- Al IA	sterføces 0			Number of flows:	71,463,456	Usize Long Terr
votocol	Profestilitation	C I Takened and Orthored C				Crash Result	2 Time Louise	C Bit Date
votocol Port	Pilter Census Herorosp	C Instant and Obsound C				Graph	C THINK SEPTRE	U DI KUIE
pplication Group	Search Example Jaite - Honolu	lo Latte - Chicanol & was & Environment	-meeting					* *
pplication	Staren Example. tine - Honord	nu i site a cincagova nani u non app a nebe	ix-meening					
pplication Flow Duration	17							
op Wan Applications	Destances in the							
op Wan Application Topology	100 Mbps							
aw Application Tepology	90 Mbor							
aw Application Path	20 mops							
pplication Projection	80 Mbps					and the second second second second		
te to Site Application	20 Mbos					and the state of the second state		non partition and the
SCP vs Application	o o trops							j l
usiness Relevance	60 Mbps							
raffic Class	SO Mbos							
	a somers				The second s		101000000000000000000000000000000000000	
Jrk .	40 Mbps							
net	30 Million						1	
cations (AVC)	30 Mbps						l,	
cations (AVC) all	30 Mbps						<u> </u>	
anet cations (AVC) all	30 Mbps							
anet cations (AVC) vall	30 Mbps 20 Mbps 10 Mbps							
anet cations (AVC) eail less connect	30 Mbps 20 Mbps 10 Mbps 0 bps	Aug 75, 1205 AM	5-0 M 12-00 AM		500.11.12.00			
inet cations (AVC) all ess onnect illaneous	30 Mbps 20 Mbps 10 Mbps 0 bps	Aug 28, 12:00 AM	Sep 04, 12:00 AM		Sep 11, 12:00 A		18, 12:00 AM	
anet (cations (AVC) all less Cennet ellaneous Reports	30 Mbps 20 Mbps 10 Mbps 0 bps	Aug 28, 12:09 AM	5ep 04, 12:00 AM		Sep 11, 12.00 A Date		18, 12:00 AM	
anet cations (AVC) wall less Connect ellaneous Reports et for Ken	30 Mbps 20 Mbps 10 Mbps 0 bps	Aug 28, 12 00 AM	5«p 04, 12:00 AM		Sep 11, 12.00 A Date	M Sep	18, 12:00 AM	<u> II i</u>
anet anet sall less cennect itaneous Reports et fur Van	30 Mbps 20 Mbps 10 Mbps 0 bps	Aug 28, 12:00 AM	Sep 04, 12:00 AM		5ep 11, 12:00 A Date	M Sep	18, 12:00 AM	
anet cafoos (AVC) eall less cennet Hisneous Reports a four Ken ctions	30 Mbps 20 Mbps 10 Mbps 0 bps Ø Show Total BR Rate Rumber of datasets: 306	Aug 25, 12:09 AM	Sep 04, 12:00 AM		5ep 11, 12:00 A Date		18, 12:00 AM	
anet cabos (AVC) all Itess Connect Itlaneous Reports at for Yan	30 Mbps 20 Mbps 10 Mbps 0 bps 9 Shar Tela (bt Rate Rumber of datasets 306 Application	Aug 28, 12:00 AM	Sep D4, 12.00 AM Total Packets	E [Averag	Sep 11, 12.00 A Date Aver	op Packet Rate	Q. Peak	Packet Rate
anet cadoos (AVC) vali less connect likaneous Reports et for Ken ctions	30 Mbps 20 Mbps 10 Mbps 0 bps ? Show Total Bt Rate Rumber ef datasets: 306 Application 20 etc. howsing	Aug 26, 12 09 AM Total Rives Total Bytes 966,723	Sep 04, 12:00 AM Total Packets 87 G8	97.076.733	Sep 11, 12 00 A Date	op Pocket Rate 27.45 pps	18, 12:00 AM	Packet Rats
net adons (AVC) all ess annett illaneous Reports for stan	30 Mbps 20 Mbps 10 Mbps 0 bps	Aug 28, 12 00 AM Total Ross Total Bytes 956,7213 4,624,540	Sep D4, 12:00 AM Total Packets 87 G8 83 G8	Averag 97.076.733 121.150.125	5ep 11, 12:00 A Date Aver 267.00 Kbpt 277.39 Kbpt	And Base Press Dir Rate 12/45 pps 42/45 pps	18, 12:00 AM	Packet Rats
net: all all ess fornet: Illaneous Reports # for Kan tions	30 Mbps 20 Mbps 10 Mbps 0 bps 500 Tols Bt Rate Norther of datasets: 306 Application C set set	Aug 26, 12 09 AM Total Flore Total Bytes 4,624,540 2,249,810	Sep 04, 12:00 AM Total Pastets 87 08 83 08 84 08 84 08	Averag 97.076.733 121.150.15 45.845.873	5ep 11, 12:00 A Date 267.00 Kbpi 257.39 Kbpi 166.30 Kbpi	A Sep Proceed Rate To a Proceed Rate 12-65 pps 46.74 pps 46.74 pps 76.35 pps	Reak 18, 12:00 AM 66,10 Mbps 13,22 Mbps 73,82 Mbps 73,85 Mbps	Packet Rate 12333 5411 2958 551
nnet all ess anneet faneeus faneeus teor sen to sen	30 Mbps 20 Mbps 10 Mbps 0 bps Show Total Bt Rate Number of disasts: 306 Applexiston C two-browning C two-browning C two-browning C two-browning	Aug 28, 12.00 AM Total Flows Total Bytes 966,723 4,624,540 2,249,510 2,219,510 2,219,	Sep 04, 12:00 AM Tots/Packets 87:06 83:06 54:08 51:06 51:06	Averag 97.076.733 121.150.175 60.460.6607 45.845.873 49.764.107	5ep 11, 12:00 A Date 267.00 Xbps 265.30 Xbps 166.30 Xbps 156.48 Xbps	And September 27.45 pps 47.45 pps 47.45 pps 47.45 pps 10.01 pps	Q- 18, 12:00 AM 66,10 Mbps 42,28 Mbps 21,79 Mbps 73,85 Mbps 84,76 Mbps	Packet Rate 12333 5411 2915 8117 10994
net all ess fornet litanesus Reports # for Kan	30 Mbps 20 Mbps 10 Mbps 0 bps 0 bps 0 movement 0 movement 0 states 0 states 0 states 0 states 0 states 0 states 0 states 0 states 0 movement 0 states 0 states 0 movement 0 states 0 states 0 movement 0 movemo	Aug 26, 12:00 AM Total Free (Total System) 4,624,540 2,249,810 13:240 13:240 13:240 13:240 13:240 13:240 14:250 14:	Sep 04, 12:00 AM Total Packets 87 GG 84 GB 51 GB 51 GB 52 GS	4verag 97.076.733 121.150.175 60.460.607 49.264.107 75.461.207	5ep 11, 12:00 A Date 4 267.00 Kbps 257.39 Kbps 166.30 Kbps 154.84 Kbps 144.02 Kbps	An Sep Packet Rate 24.54 pps 12.65 pps 12.65 pps 12.61 pps 1	21.7 Mbps 21.7 Mbps 21.7 Mbps 21.7 Mbps 21.7 Mbps 23.85 Mbps 34.7 6 Mbps	Packet Rate 12333 295411 2958 117 10494 3976
net all ess ess innet i innet innet innet i innet i i i i i i i i i i i i i i	30 Mbps 20 Mbps 10 Mbps 0 bps 31 Mbps 0 bps 32 Mbp Telai Bt Rate Thruber of dataset: 306 Applecies 10 mbps 10 mbp	Aug 28, 12 09 AM Total Fone Total Bytes 966,723 4,624,540 2,249,810 3,242 1,242 3,242 3,242 2,243,311	Sep 04, 12:00 AM Total Packets 87 C6 83 C6 54 C8 54 C8 55 56 C8 56	4 versa 97.076.733 121.150.175 60.460.607 43.845.873 49.264.107 75.461.207 139.072.065	Sep 11, 12:00 A Date 267.00 Kbpi 257.30 Kbpi 156.30 Kbpi 156.00 Kbpi 154.02 Kbpi 144.02 Kbpi 81.42 Kbpi	Arr 32 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 -	18, 12:00 AM	Packet Bate 12333 5411 2958 8117 10494 3976 1776
radi di di d	30 Mbps 20 Mbps 10 Mbps 0 bps 0	Aug 28, 12 09 AM Total Ross Total Bytes 6545/23 4,524540 2,249,810 2,120,311 3,187,481	Total Packets 87 G4 81 G4 51 G5 51 G5 51 G5 51 G5 52 G5 26 G5 26 G5 26 G5 26 G5 26 G5	Averag 97.076.733 121.150.175 45.465.873 49.264.107 75.461.207 13.072.065	54.9 X Rate 54.9 X Rate 267.00 Xbpi 267.30 Xbpi 166.30 Xbpi 154.06 Xbpi 154.0	Ar Sep Ar Sep	111, 12:00 AM	Packet Rate 12333 111 2958 117 10494 13976 1776 220
data data kisi Jannet J	30 Mbps 20 Mbps 10 Mbps 0 bps 30 Shue Tela Bit Rate Number of datasets: 306 Application 101 ms-period 101 ms-peri	Aug 28, 12 09 AM Total Flores Total Bytes 966,723 4,624,540 2,249,810 3,240 1,240 2,240,810 3,240 2,120,331 3,387,481 3,445	Top 04, 12:00 AM Top Packets 87 CE 83 CE 54 CE 54 CE 54 CE 54 CE 24 CE 26 CE 24 CE 26 CE 20 CE	4xrrag 97.076.733 121.150.175 60.460.607 43.264.107 75.461.207 75.461.207 39.072.065 41.734.222 29.897.227	se bl. Rate Aver. 267.00 Kbps 257.10 Kbps 154.04 Kbps 154.64 Kbps	A Sep A	18, 12:00 AM 66-10 Mips 42:28 Mips 42:28 Mips 73:45 Mips 31:86 Mips 14:65 Mips 13:86 Mips	Packet Rate 12333 5411 2915 8117 10494 3976 220 151
dati dagon (AVC) all variante de la constante	30 Mbps 20 Mbps 20 Mbps 0 bps 0 bps 0 bps 0 bps 0 bps 0 cmost of 88 Rate Retro for an 4 cmost 0 cmost of 10 c	Total flows Tetal Bytes 656223 7,512 7,524 7,523 7,132 8,523 7,132 8,235 7,132 8,235 7,132 8,235 8,230,331 3,387,441 36,445 2,059,620	Total Packets 87 Cel 51 Cel 51 Cel 51 Cel 51 Cel 51 Cel 52 Cel 24 Cel 25 Cel 26 Cel 26 Cel 26 Cel 27 Cel 28 Cel 29 Cel 20	Averag 97.076.733 121.150.175 45.845.873 49.264.107 75.461.207 13.072.065 41.734.222 29.897.227 14.454.603	Sep 11, 12 00 A Date Arer 257,59 Kbp 165,30 Kbp 154,68 Kbp 154,68 Kbp 154,68 Kbp 154,68 Kbp 154,68 Kbp 154,68 Kbp 154,68 Kbp	Ar Sep Ar Sep	116, 12:00 AM 66:10 Mbps 41:28 Mbps 41:28 Mbps 41:28 Mbps 13:65 Mbps 14:65 Mbps 13:66 Mbps 13:66 Mbps 13:66 Mbps 13:66 Mbps 13:64 Mbps 13:65 Mbps 13:	Packet Bate 12333 5413 5413 1452 1452
cellons (AVC) and the sta connect interesus Reports refor tan refor tan refor tan connect interesus CENY	30 Mbps 20 Mbps 10 Mbps 0 bps 0	Aug 26, 12 09 AM Total Flows Total Syste 966,723 4,624,540 2,73,810 7,152 8,162,660 2,100,314 1,56,455 2,059,620 964	Sep 04, 12 00 AM T60/ Puters 87 Cd 81 Cd 91 Cd 91 Cd 92 Cd 94 Cd 9	4xerag 97.076.733 122.1350.175 66.460.607 47.461.207 19.072.065 41.734.222 29.897.227 11.4454.605 10.9454.6627	98 El Rate Aver. 267-00 Xbps 257-39 Xbps 154-36 Xbps 154-36 Xbps 154-36 Xbps 154-36 Xbps 154-36 Xbps 154-36 Xbps 134-36 Xbps 144-36 Xbps 1	A Sep A S	14, 12 00 AM 66.10 Mbps 43.28 Mbps 21.79 Mbps 73.85 Mbps 14.65 Mbps 14.65 Mbps 14.65 Mbps 1.36 Mbps 9.42 Mbps 9.42 Mbps	Packet Rate 23333 5411 2958 8117 10494 3976 220 2151 1452
and and adors (AVC) address (AVC) and the second address of the se	30 Mbps 20 Mbps 10 Mbps 0 bps	Aug 28, 12:00 AM Total Ryses 265(272) 4,55(28) 4,55(28) 2,249,510 2,445,500 2,475,5000 2,47	Total Packets 87 C6 87 C6 81 C6 81 C6 81 C6 81 C6 81 C6 81 C6 82 C	27.076.72 121.150.175 60.460.667 45.845.873 49.264.107 75.461.207 13.473.4222 29.897.227 10.360.3137 10.360.3137 12.278.333	Sep 11, 12 00 A Date Aver. 265.00 May 155.00 Kap 156.00 Kap	Ar The second se	18, 12 CO AM 18, 12 CO AM 42.28 Mbps 21.79 Mbps 31.86 Mbps 31.86 Mbps 31.86 Mbps 31.86 Mbps 31.86 Mbps 	Packet Bate 12333 5413 5413 1452 153 1452
cov Cov	30 Mbps 20 Mbps 10 Mbps 0 bps 0 bps 0 bps 0 bps	Aug 25, 12:00 AM Total Flores Total Syles 4,624,540 2,249,510 2,249,510 2,249,510 2,10,311 3,37,445 2,059,620 4,02,56 4,02,56 4,02,	5ep 04, 12 00 AM [160] Pacists 87 Cd 83 05 54 05 55 05 56 0	97.076.733 122.1350.175 66.460.607 49.264.1017 49.264.1017 39.072.065 41.734.222 29.897.227 14.454.606 10.360.312 22.278.333 8.394.139	5 Fe p 1 1 20 0 A 5 Fe p 1 1 12 00 A Date 257.39 Kips 267.39 Kips 166.30 Kips 164.30 Kips 164.45 Kips 144.64 Kips 14.64 Kips 13.84 Kips 13.84 Kips 13.84 Kips 13.84 Kips	A 540 pps 150 pps 1	14, 12 00 AM	Packet Bate 12333 25411 25411 25413 10545 10545 2056 2056 2056 2053 1452
ctiv	30 Mbps 20 Mbps 10 Mbps 0 bps 0 bps ∞ bps w	Aug 28, 12:00 AM Total Ryss 966,723 4,524,540 2,324,660 2,120,311 3,36,445 2,120,311 3,36,445 2,059,620 40,279,66 42,786 4	Total Packets 87 G8 87 G8 87 G8 95 G8 9	Averag 12.1156.1257 12.1156.1257 45.845.873 45.845.873 45.845.873 45.845.873 19.072.662 42.9897.227 10.360.332 5.8476.673 11.4754.666 10.360.332 5.8476.473 11.4754.5755 11.4754.5755 11.47555 11.47555 11.47555 11.475555	sep 11, 12 50 A Sep 11, 12 50 A 257.00 Kbpi 257.10 Kbpi 154.00 Kbpi 154.84 Kbpi 154.84 Kbpi 154.84 Kbpi 154.84 Kbpi 14.62 Kbpi 14.62 Kbpi 14.62 Kbpi 14.63 Kbpi 25.64 Kbpi 25.64 Kbpi	Arr	18, 12 00 AM 66,10 Mbps 41,28 Mbps 21,38 Mbps 31,88 Mbps 14,65 Mbps 1,36 Mbps 9,42 Mbps 9,42 Mbps 	Packet Rate 12333 54154 541555 541555 5415555 54155555 541555555 5415555555555

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.

Q+ Type here to filter reports.	Application	X Top Analysis X	Top Analysis	×								
Reports Interface Bandwidth Top Analysis	Тор	Analysis	5							15m 1h 6h	1d 1w 30d Cu	ustom
IPs and Ports IPs and Application	0	9/23/16, 09:32::	34 AM to 0	19/23/16, 03:32:34 PM					Execute Repo	1		
 Applications Protocol 	Source	PA-PANFirewall			Al Interfaces 0				Number of flor	vs: 5,000+	CSV File	e Results
Pretocel Port Application Group Application	Search fle	ow.app=facebook-	base								x •	7
Application Flow Duration Top Wan Applications	-									0,-	4	
Top Wan Application Topolog	Protocol	Src P Addr 10.1.6.603	Sec Port	Dist IP Addr Dist Port exage-star-m., 993	User-ID (PAN) Inveacoon.com/cesume	Application App-ID (PAN) racebook-base racebook-base	Bit Rate Fa	cket Rate Src Country 3-37 pps -	Dist Country In Bytes	In Packets	Src DSCP 94 U IDE/	TC
Kaw Appressen Topology	TCP	edge-star-m	. 443	12.33.223.132 42,315	liveaction.com\testme	facebook-base facebook-base	36.70 Kbps	4.07 pps MUS/United		124 KB	110 0 (BE)	
Raw Application Path	TCP	10.1.2.205	49,465	xx-fbcdn-sh 443	liveaction.com\testme	facebook-base facebook-base	4.54 Kbps	4.20 pps -	E IE/Ireland	3 KB	210 (BE)	
Application Projection	TCP	xx-fbcdn-sh.	. 443	12.33.223.132 50,215	liveaction.com\testme	facebook-base facebook-base	107.59 Kbps	10.00 pps I IE/Ireland	US/United	67 KB	50.0 (BE)	
Site to Site Application	TCP	10.1.2.205	49,534	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	22.74 Kbps	8.00 pps -	US/United	3 KB	8 0 (BE)	
DSCP vs Application	TCP	edge-star-m	. 443	12.33.223.132 52,704	liveaction.com\testme	facebook-base facebook-base	25.54 Kbps	7.00 pps MUS/United	. M US/United	3 KB	7 0 (BE)	
Business Relevance	TCP	10.1.1.52	59,197	edge-star-m 443	-	facebook-base facebook-base	308.16 bps	0.21 pps -	E IE/Ireland	3 KB	15 0 (BE)	
Traffic Class	TCP	edge-star-m	. 443	12.33.223.132 54,489	-	facebook-base facebook-base	275.40 bps	0.23 pps IIE/Ireland	MUS/United	3 KB	17 0 (BE)	
them, coss	TCP	10.1.1.86	58,474	edge-star-m 443		facebook-base facebook-base	21.69 bps	0.03 pps -	E BIE/Ireland	160 B	2 0 (BE)	
▶ Qos	TCP	edge-star-m	. 443	12.33.223.132 61,140		facebook-base facebook-base	13.56 bps	0.02 pps IIE/Ireland	M US/United	100 B	10 (BE)	
Network	TCP	10.1.1.86	58,475	xx-fbcdn-sh 443	-	facebook-base facebook-base	21.69 bps	0.03 pps -	E IE/Ireland	160 B	2 0 (BE)	
Medianet	TCP	xx-fbcdn-sh.	. 443	12.33.223.132 47,391	-	facebook-base facebook-base	21.69 bps	0.03 pps IIE/Ireland	MUS/United	160 B	2 0 (BE)	
Applications (AVC)	TCP	10.1.2.205	49,545	xx-fbcdn-sh 443	liveaction.com\testme	facebook-base facebook-base	6.62 Kbps	10.00 pps -	E ItE/Ireland	2 KB	30 0 (BE)	
Frewall	TCP	xx-fbcdn-sh.	. 443	12.33.223.132 11,374	liveaction.com\testme	facebook-base facebook-base	224.70 Kbps	20.00 pps 1 1E/Ireland	US/United	112 KB	80 0 (BE)	
A 100	TCP	10.1.2.205	49,547	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	2.78 Kbps	0.62 pps -	US/United	8 KB	15 0 (BE)	
	TCP	edge-star-m	. 443	12.33.223.132 23,459	liveaction.com\testme	facebook-base facebook-base	3.18 Kbps	0.67 pps MUS/United_	US/United	10 KB	16 0 (BE)	
 Wireless 	TCP	10.1.2.205	49,526	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	670.24 bps	0.12 pps -	US/United	5 KB	7 0 (BE)	
AnyConnect	TCP	edge-star-m	. 443	12.33.223.132 13,896	liveaction.com\testme	facebook-base facebook-base	273.49 bps	0.14 pps MUS/United_	. US/United	2 KB	8 0 (BE)	
► Miscellaneous	TCP	10.1.2.205	49,456	xx-fbcdn-sh 443	liveaction.com\testme	facebook-base facebook-base	30.77 bps	0.04 pps -	I IE/Ireland	300 B	3 0 (BE)	
Y Custom Reports	TCP	xx-fbcdn-sh.	. 443	12.33.223.132 29,825	liveaction.com\testme	facebook-base facebook-base	369.54 bps	0.08 pps 1 E/Ireland	US/United	4 K8	6 0 (BE)	
report for Ken	TCP	10.1.2.205	49,401	xx-fbcdn-sh 443	liveaction.com\testme	facebook-base facebook-base	284.57 bps	0.20 pps -	E E/Ireland	3 KB	17 0 (BE)	
and the second	TCP	xx-fbcdn-sh.	. 443	12.33.223.132 2,275	liveaction.com\testme	facebook-base facebook-base	3.93 Kbps	0.46 pps 1 1E/Ireland	US/United	41 KB	39.0 (BE)	
	TCP	10.1.2.205	49,402	xx-fbcdn-sh 443	liveaction.com\testme	facebook-base facebook-base	303.43 bps	0.26 pps -	I IE/Ireland	3 KB	22.0 (BE)	
Report Actions	TCP	xx-fbcdn-sh.	. 443	12.33.223.132 56,737	liveaction.com\testme	facebook-base facebook-base	7.65 Kbps	0.73 pps I IE/Ireland	US/United	80 KB	610 (BE)	
IN SCHLAPPINGELS	TCP	10.1.2.205	49,466	xx-fbcdn-sh 443	liveaction.com\testme	facebook-base facebook-base	31.17 bps	0.04 pps -	E IE/Ireland	300 B	3 0 (BE)	
Save	TCP	xx-fbcdn-sh.	. 443	12.33.223.132 61,138	liveaction.com\testme	facebook-base facebook-base	374.44 bps	0.08 pps 1 1E/Ireland	US/United	4 KB	6 0 (BE)	
Save As	TCP	10.1.1.211	65,038	xx=fbcdn=sh 443	1.0	facebook-base facebook-base	13.26 Kbps	0.00 pps -	I IE/Ireland	2 KB	18 0 (BE)	
3976 /6	TCP	xx-fbcdn-sh.	. 443	12.33.223.132 31,042	-	facebook-base facebook-base	498.39 Kbps	0.00 pps 1 E/Ireland	US/United	62 KB	480 (BE)	
Create	TCP	10.1.2.205	49,483	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	1.22 Kbps	0.53 pps -	US/United	2 KB	8 0 (BE)	
	TCP	edge-star-m	. 443	12.33.223.132 60,171	liveaction.com\testme	facebook-base facebook-base	8.33 Kbps	1.13 pps MUS/United_	US/United	16 KB	17 0 (BE)	
	TCP	10.1.1.211	65,046	edge-star-m, 443		facebook-base facebook-base	17.87 Kbps	12.00 pps -	US/United	2 KB	12 0 (BE)	
	TCP	edge-star-m	. 443	12.33.223.132 46,238		facebook-base facebook-base	23.82 Kbps	14.00 pps MUS/United_	. MUS/United	3 KB	14 0 (BE)	
	TCP	10.1.1.136	48,468	edge-mott-s 443		facebook-base facebook-base	3.91 bps	0.01 pps -	I IE/Ireland	425 8	5 0 (BE)	
Schedule	TCP	edge-mqtt-s_	. 443	12.33.223.132 59,142		facebook-base facebook-base	4.89 bps	0.00 pps 1 IE/Ireland	US/United	531 B	4 0 (BE)	
0.0-1	TCP	10.1.2.205	49,546	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	2.69 Kbps	0.62 pps -	US/United	8 KB	15 0 (BE)	
	TCP	edge-star-m	. 443	12.33.223.132 23,998	liveaction.com\testme	facebook-base facebook-base	3.64 Kbps	0.46 pps 🔜 US/United	US/United	11 KB	110 (BE)	
	TCP	10.1.2.205	49,377	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	270.46 bps	0.08 pps -	US/United	4 KB	8 0 (BE)	
	TCP	edge-star-m	. 443	12.33.223.132 22,972	liveaction.com\testme	facebook-base facebook-base	657.85 bps	0.14 pps 🔜 US/United	. MUS/United	9 KB	15 0 (BE)	
Help	TCP	10.1.2.205	49,514	edge-star-m 443	liveaction.com\testme	facebook-base facebook-base	401.66 bps	0.13 pps -	US/United	4 KB	110 (BE)	
	TCP	edge-star-m	. 443	12.33.223.132 55,979	liveaction.com\testme	facebook-base facebook-base	1.41 Kbps	0.24 pps SUS/United_	US/United	14 KB	200 (BE)	
	TCP	10 1 2 205	40 544	vv-flords-sh 442	Economican completeness	Freehool, here freehool, here	3 CC Mars	167 ppr -	H B IF Handamad	060.0	E.O. (00)	
	1540	10.1.1.1.0.0		AA TOLDT THE THE	inveacuon.com/cescine	Lacebook - pase lacebook - pase	2.50 KDps	1.01 pps -	I I IE/Inciano	300 B	3 U (DE)	

22 | Palo Alto Networks Integration with LiveNX

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.

REPORTS View Reports									View Schedule Creat	e Advanced Report
All Devices	Application Ad Hoc	0	Cloud	Annlica	tions from	LiveAction	HO			rs
nterfaces			ciouu	Applied	lions nom	LITCHCLIOI	i iliq		Q By Report Name	
All Interfaces	2 10			4 .					Name	Last updated
DVANCED -	A see Do		1	À	A					
ne Zone		-			1				Application Ad Hoc	09/17 10-
GMT-08:00) America/Los Angeles 🔹				LA L			EN A	12.1	Application Ad Hoc	09/17 10_ 0
🔁 Daylight Savings Time			0	AV		A 5 4	- GA		Application Ad Hoc	09/16 19: 0
splay Filter	16:15 36:20	16:25	16:30 16	135 16:40	56:45 56:50	16:55 17:0	0 17:09	17:30	Application Ad Hoc	09/16 t8 0
No Display Filtering			14 4 24	ge 2 /12)	н	Q, Search		=	Application Ad Hoc	09/16 18.
rection									(2) Application Ad Hoc	09/16 17:-
Dutbound	APPLICATION	FLOWS	BYTES	TOTAL PACKETS	AVERAGE BIT RATE	AVERAGE PACKET RATE	PEAK BIT RATE	PEAK PACKET RATE	Application Ad Nor	00/16.16-
n Duration	salesfores.bars	2142	22 MB	44708	40.58 Khos	12.44 pps	4		(e) Application Ho Hoc	
Auto .			13.140	76014	30.03 vber	21.12.000			(g) Site Traffic Ad Hoc	09/16 12
ow Type	ricp		13 MB	/0034	29.93 Kops	21.12 pps	59 59	2	A Destination Site Traff	L. 09/16 12 0
irewall .	sharepoint-online	456	TUMB	9843	23.21 Kops	2.73 pps	•.			
ecution Type	quic	1673	9 MB	13391	20.65 Kbps	3.72 pps	\$2. 	3		
Time Series *	ms-lync-online	1277	6 MB	9355	12.43 Kbps	2.60 pps	÷	3		
rt By	Laboraffic	157	5 MB	1	12.22 Kbps	0.00 pps	<u>.</u>	3 C		
Sit Rate -	drs	55416	5 MB	15688	10.91 Kbps	4.36 pps	8	8		
ix Search	dropcarn	56	4 M8	59483	8.75 Kbps	16.52 pps	2	8		
tag-internet-edge	icloud-base	407	3 MB	5060	7.12 Klops	1.41 pps	<			

23 | Palo Alto Networks Integration with LiveNX

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.

24 | Palo Alto Networks Integration with LiveNX

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.

25 | Palo Alto Networks Integration with LiveNX