²alo Alto Front Line Support Quick Reference Guide

s traffic being blocked? Click on the Traffic Log on the left, enter search filter (see example filters), and select for last 15 minutes or last hour from the drop down menu.

🔍 🔍 🖉 pa-con1.bu.edu		×														
	TON I	UNIVERSITY [US]	https://pa-con1.bu	.edu/#monito	r::::monitor/l	ogs/traffic										Q 🛧 🚺 🔜 🗄
an paloalto																
Contaxt		Monitor		U AC												😚 🔍 Search
Panorama		Device Group All		-											Manual	💌 😋 🔞 Help
														Last Hou		× 🕂 🐃 🎼 💁
Traffic													Session End			
URL Filtering		Generate Time	Туре	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Reason	Bytes	Device SN	Device Name
C Unified	Þ	08/16 17:09:47	start	Trust	Untrust	128.197.253.157		204.13.250.5	53	dns	allow	DNS	n/a	86	010108001125	PA-7050-02
Automated Correlation Engine	Þ	08/16 17:09:47	start	Untrust	Trust	209.126.107.139		168.122.92.38	5060	sip	allow	Untrust to Trust ANY	n/a	464	010108001125	PA-7050-02
Contelated Events	Þ	08/16 17:09:47	start	Trust	Untrust	168.122.12.181		63.251.98.12	80	web-browsing	allow	General Campus Filter Rules	n/a	726	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	128.197.253.154		24.30.200.19	53	dns	allow	DNS	n/a	100	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	155.41.251.30		172.217.4.195	443	quic	allow	Allow internal networks	n/a	1.4k	010108001125	PA-7050-02
	\mathbb{P}	08/16 17:09:47	start	Trust	Untrust	168.122.33.171		17.154.66.69	443	ssl	allow	General Campus Filter Rules	n/a	483	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	155.41.107.138		69.172.216.56	443	ssl	allow	General Campus	n/a	528	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	168.122.2.137		74.119.118.67	80	web-browsing	allow	General Campus	n/a	1.7k	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Untrust	Trust	116.31.116.5		128.197.176.12	22	ssh	allow	Untrust to Trust	n/a	311	010108001125	PA-7050-02
		08/16 17:09:47	start	Trust	Untrust	168.122.90.247		216.58.219.194	443	google-base	allow	Allow internal	n/a	779	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	155.41.44.110		216.58.192.202	443	google-base	allow	Allow internal	n/a	497	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	168.122.90.247		216.58.219.194	443	ssl	allow	General Campus	n/a	779	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	155.41.44.110		216.58.192.202	443	ssl	allow	General Campus	n/a	497	010108001125	PA-7050-02
		08/16 17:09:47	start	Trust	Untrust	128.197.253.154		204.61.216.50	53	dns	allow	DNS	n/a	100	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	168.122.10.183		75.126.29.101	80	web-browsing	allow	General Campus	n/a	643	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	128.197.253.157		204.13.250.5	53	dns	allow	DNS	n/a	95	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	128.197.11.225		118.172.16.68	8080	http-proxy	allow	General Campus Filter Rules-2	n/a	547	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	128.197.11.225		118.172.16.68	8080	web-browsing	allow	General Campus Filter Rules-2	n/a	547	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Trust	Untrust	128.197.53.199		172.217.4.45	443	quic	allow	Allow internal	n/a	1.4k	010108001125	PA-7050-02
	Þ	08/16 17:09:47	start	Untrust	Trust	209.126.107.139		168.122.92.37	5060	sip	allow	Untrust to Trust ANY	n/a	462	010108001125	PA-7050-02
	144	12345678	9 10 🕨 🗖 Re:	solve hostname		460 400 0 467		400 400 6 00					Di	splaying logs 1	-30 <mark>30 💌 p</mark>	er page DESC 💌
test Logout Last Login Time: 08/16/2	016 1	7:00:08													📼 Active	👼 Tasks Language

Example Filters:

Displays only blocked traffic for a specific IP address (action neq allow) and (addr.src in 128.197.11.225)

Neb site blocked? Click URL the Filtering log instead of the Traffic log to confirm/deny a site was blocked by the Palo Alto firewall or not.

note: The Action field will equal block-url if the site was blocked and that you can use a filter to narrow the scope to a single host as in this example (addr.src in 128.197.11.225).

paloalto		Dashboard	ACC No	DEVICE GROUPS TEMPLATES TEMPLATES	an	or	am	nisq	IIGNOI	Ng	a Commi	8 6	Save 🔍 Search
Context Panorama		vice Group Internet E	īdge								Ľ	Manual	🔽 🖸 🕢 Help
V 🚺 Logs	٩,	(action neg alert)									Al	-	🛚 🖶 📭 🎥 🗳
Traffic Threat		Generate Time	Category	URL.	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Device SN D
Q URL Filtering	D	08/10 12:50:25	malware	hotlaps.com.au/toolbar/Hot_Laps.exe	trust-I3	untrust-I3	172.22.22.151	lab\mjs	72.167.131.29	80	web-browsing	block-url	001606001833
WildFire Submissions	D	08/10 12:50:16	malware	glazeautocaremobile.com/Offer_Invoice.exe	trust-I3	untrust-I3	172.22.22.151	lab\/mjs	112.137.167.250	80	web-browsing	block-url	001606001833
HIP Match	D	08/10 12:50:07	malware	antalyanalburiye.com/image/payment/client.exe	trust-13	untrust-I3	172.22.22.151	lab\mjs	94.73.147.76	80	web-browsing	block-url	001606001833
Chified Unified	B	08/10 12:49:55	malware	glazeautocaremobile.com/Offer_Invoice.exe	trust-I3	untrust-I3	172.22.22.151	lab\/mjs	112.137.167.250	80	web-browsing	block-url	001606001833
Automated Correlation Engine Correlated Events	D	08/10 12:49:44	malware	antalyanalburiye.com/image/payment/client.exe	trust-I3	untrust-I3	172.22.22.151	lab\/mjs	94.73.147.76	80	web-browsing	block-url	001606001833
T App Scope	D	08/10 10:14:57	malware	hotlaps.com.au/toolbar/Hot_Laps.exe	trust-I3	untrust-I3	192.168.10.78	lab\/mjs	72.167.131.29	80	web-browsing	block-url	00700009700
Summary Summary	D	08/10 10:14:49	malware	glazeautocaremobile.com/Offer_Invoice.exe	trust-I3	untrust-I3	192.168.10.78	lab\/mjs	112.137.167.250	80	web-browsing	block-url	00700009700
Change Monitor	D	08/10 10:14:40	malware	antalyanalburiye.com/image/payment/client.exe	trust-I3	untrust-I3	192.168.10.78	lab\mjs	94.73.147.76	80	web-browsing	block-url	007000009700
Threat Map	P	08/10 10:14:33	malware	glazeautocaremobile.com/Offer_Invoice.exe	trust-I3	untrust-I3	192.168.10.78	lab\mjs	112.137.167.250	80	web-browsing	block-url	00700009700
Network Monitor	D	08/10 10:14:31	malware	antalyanalburiye.com/image/payment/client.exe	trust-I3	untrust-I3	192.168.10.78	lab\/mjs	94.73.147.76	80	web-browsing	block-url	007000009700

s a file/executable being blocked? Click Data Filtering log to confirm/deny a file was blocked or not. (Note action=deny)

m naloalto			DEVICE	GROUPS TE	MPLATES -	10										
patoarco	Das	shboard AC	C Monitor Policies	Objects Network	Devic	e Pan	orama						📥 Co	mmit 💣	🗟 Save 🔍 Se	arch
Context																
Panorama 👻		roup Internet Edge	*											Manua	🗾 🖂 🤇	Help
V Calego	🔍 (actio	n neq alert)											All	Y	🗢 🗷 🖶 📭 🇯	9 9
Traffic III Threat		Generate Time	File Name	Name	From Zone	To Zone	Sender	Sender Name	Receiver	Receiver Name	To Port	From Port	Application	Action	Device Name	Device
WildFire Submissions	Þ	08/11 10:39:25	icooloader.exe	Microsoft PE File	trust-13	vpn-I3	192.168.10.10		172.22.22.101		62699	80	web-browsing	deny	PA-VM-sec	00700
Data Filtering	ø	08/11 10:39:09	DeluxeCommunications.exe	Microsoft PE File	trust-I3	vpn-I3	192.168.10.10		172.22.22.101		62686	80	web-browsing	deny	PA-VM-sec	00700

Are the Firewall(s) up? Review the Traffic log and note most recent log entry; it should be current.

Does the client need an exemption? Direct client to the online form: http://www.bu.edu/tech/services/security/network/firewall/campus/exempt/

Please do not simply re-assign the ticket to IRT, there is important information at the above link that the client needs to know before requesting an exemption.

Escalation information

Malicious = yes in Verdict Column Escalate to Desktop Support for remediation of nanaged devices, Service Desk for all others.

maloalto					- DEVICE	GROUPS -	TEMP										
POLO NETWORKS		Dashboard	ACC Mon	itor Po	olicies	Objects	Network	Device	Panorama						🏯 Cor	nmit 💣 🛗 Sav	e 🔍 Search
Context				_													_
Panorama 👻		ice Group All		۳.												Manual	🖌 🖸 😧 Help
V 🔂 Logs	٩.														All	∀ → X	🖶 📭 🍺 🔁
R III Ellering		Generate Time	File Name	So Zo	ource	Destination Zone	Attacker	Attacker Name	Victim	Victim Name	Desti Port	Application	Rule	Verdict	Sender Address	Recipient Address	File Type
WildFire Submissions	Þ	08/11 11:42:45	client.exe	un	ntrust-I3	trust-I3	94.73.147.76		172.22.22.101	lab\mjs	63128	web-browsing	MJS Outbound Trust	malicious			pe
Ling Data Filtering	Þ	08/11 11:42:45	client.exe	un	ntrust-I3	trust-I3	94.73.147.76		172.22.22.101	lab\mjs	63273	web-browsing	MJS Outbound Trust	malicious			pe
Configuration	Þ	08/11 11:42:09	client.exe	un	ntrust-I3	trust-I3	94.73.147.76		192.168.10.78	lab\mjs	51416	web-browsing	MJS Outbound Trust	malicious			pe
Unified	Þ	08/11 11:42:09	client.exe	un	ntrust-I3	trust-I3	94.73.147.76		192.168.10.78	lab\mjs	52314	web-browsing	MJS Outbound Trust	malicious			pe

Application = Incomplete Remote site is not allowing the information. Direct the client to contact the support organization for the remote host(s)/service.

M paloalto				12	DEVIC	E GROUPS	TEMPLATE										
	D	ashboard AC	C 1	Monitor	Policies	Objects	Network D	evice Panorama							2	Commit 💰 🔂	Save 🥵 Search
Context Panorama		Group Internet Edge		×												Manual	💌 😒 🕑 Help
V 🔂 Logs	🔍 (ap	p eq incomplete)													Al	¥ 🗈	🗙 🖶 📚 🍃 🖄
Threat		Generate Time	Туре	From Zone	To Zone	Source	Source User	Destination	To I	Port	Application	Action	Rule	Session End Reason	Bytes	Device SN	Device Name
WildFire Submissions	Þ	08/11 10:26:31	end	trust-I3	untrust-13	172.22.22.101	lab\mjs	4.2.2.2	443	3	incomplete	allow	Block Files for Unknown Sites	aged-out	78	001606001833	PA-200
Ling Data Filtering	P	08/11 10:26:23	end	trust-I3	untrust-I3	172.22.22.101	lab\mjs	4.2.2.2	443	3	incomplete	allow	Block Files for Unknown Sites	aged-out	624	001606001833	PA-200

Session End Reason = Threat Escalate to InfoSec Investigations (IRT)

JP paloalto	Das	hboard ACC		fonitor	Policies	Objects	TEMPLATES Network D	evice Panorama							۵	Commit 🔗 🔂	Save 🗣 Search
Context Panorama 👻	Device Gr	roup All		*												10 Seconds	💌 😋 🔞 Help
V 🔂 1005	(addr.	min 172 05 05 4) a	ad (adds do	lin 72 167 12	20.)												
	(abdi)	src in 172.25.25.4) a	na (addr.ds	11172.107.13	.29)										Al	· · · ·	× 🛛 🖻 🛤 🗖
Traffic		Generate Time	Type	From Zone	To Zone	Source	Source User	Destination	То	Port	Application	Action	Rule	Session End Reason	Bytes	Device SN	Device Name

⁻or more detailed information, see:

Monitor Log Data:

<u>https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/reports-and-ogging/monitor-log-data.html</u>