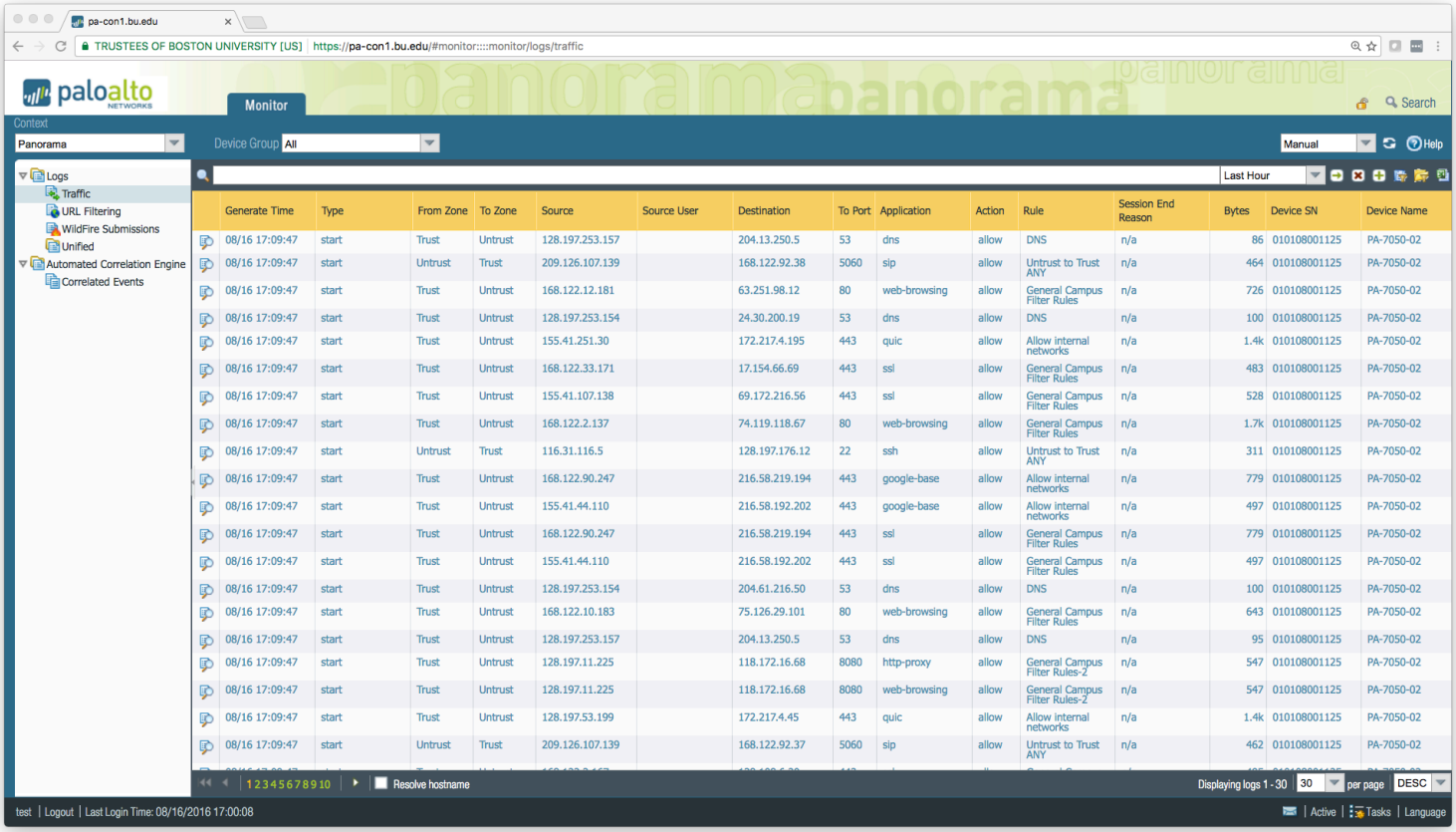
Palo Alto Front Line Support Quick Reference Guide

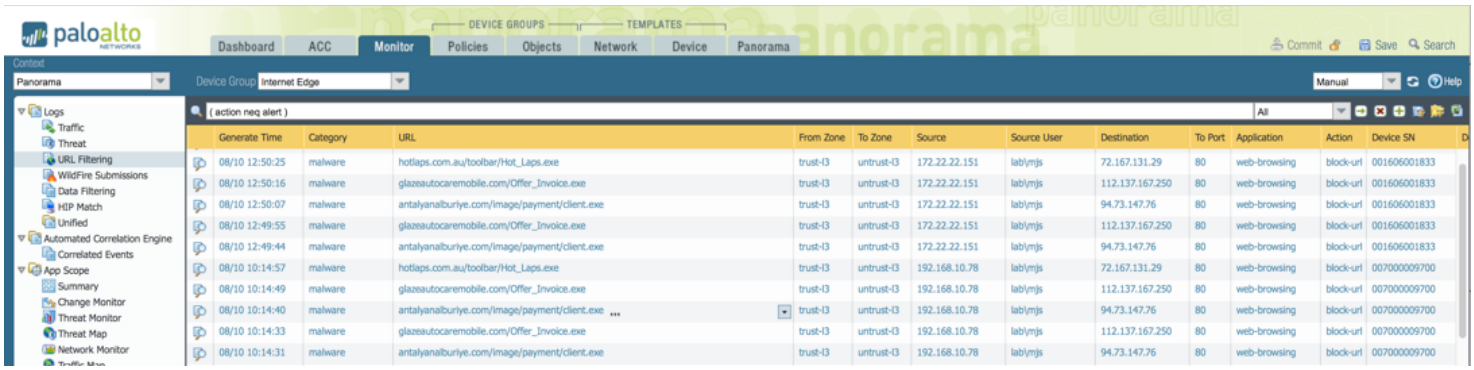
s traffic being blocked? Click on theTraffic Log on the left, enter search filter (see example filters), and select for last 15 minutes or last hour from the drop down menu.



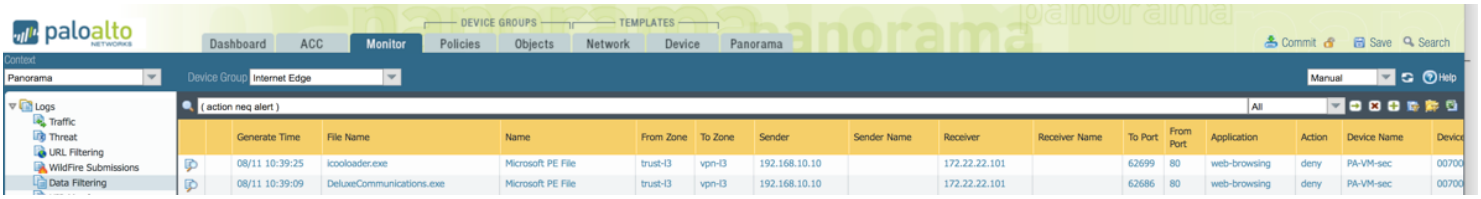
Example Filters:
Displays only blocked traffic for a specific IP address
(action neq allow) and (addr.src in 128.197.11.225)

Web 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).



s a file/executable being blocked? Click Data Filtering log to confirm/deny a file was blocked or ıot. (Note action=deny)



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

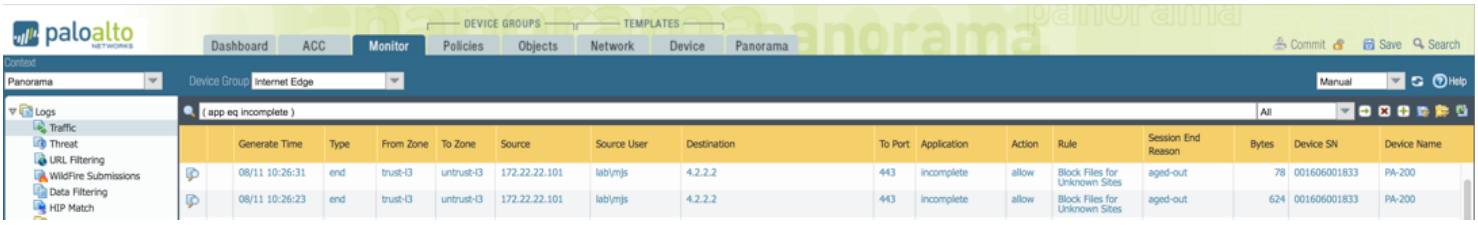
Does the client need an exemption? Direct client to the online form: ıttp://www.bu.edu/tech/services/security/network/firewall/campus/exempt/

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

Escalation information

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

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



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

For more detailed information, see:

Monitor Log Data:
https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/reports-and-logging/monitor-log-data.html