

LA Mission College Firewall Summary

LA Mission perimeter network secured with dual Palo Alto Network's, PA-4020 series firewall, configured in active/passive failover to insure protection of network. The college subscribes to Palo Alto's WildFire cloud based malware analysis for advanced threat detection and prevention. Dynamic analysis of suspicious content in a cloud-based virtual environment to discover unknown threats. More details: <https://www.paloaltonetworks.com/products/technologies/wildfire.html>

The screenshot displays the Palo Alto Networks management console for a device named 'mission-fw1'. The interface is organized into several panels:

- General Information:** Lists device details such as MGT IP Address (172.20.1.201), MGT Netmask (255.255.255.0), MGT Default Gateway (172.20.1.254), MGT IPv6 Address (unknown), MGT IPv6 Link Local Address (fe80::230:48ff:febc:2b38/64), MGT IPv6 Default Gateway, MGT MAC Address (00:30:48:fc:2b:38), Model (PA-4020), Serial # (0002C101099), Software Version (6.0.5-h3), GlobalProtect Agent (0.0.0), Application version (544-3039 (12/08/15)), Threat Version (518-2835 (12/08/15)), Antivirus Version (1611-2088 (07/31/15)), URL Filtering version (4589), Time (Wed Jan 6 15:05:28 2016), and Uptime (68 days, 2:11:10).
- System Resources:** Shows Management CPU at 15%, Data Plane CPU at 9%, and Session Count at 5908 / 524286.
- Logged In Admins:** A table listing active administrators:

Admin	From	Client	Session Start	Idle For
panorama	172.25.43.50	Panorama	10/30 14:04:19	00:00:12s
sadovsg	172.20.100.23	Web	01/06 15:02:19	00:00:00s
- Data Logs:** No data available.
- System Logs:** A list of system events with descriptions and timestamps, including DHCP lease started, user logins, authentication failures, and IPsec key management events.
- Config Logs:** No data available.
- Locks:** No locks found.
- ACC Risk Factor:** A risk factor indicator showing a score of 3.1 on a scale of 1 to 5, with a color-coded bar below it.

sadovsg | Logout

Active Tasks Language

110%

Firewalls provide detailed information about applications, users and content traversing network to determine risks and respond accordingly. Dedicated, function-specific process is used for networking, security, content inspection and management to deliver predictable firewall performance.

The screenshot displays the Palo Alto Networks firewall logs interface. The main content is a table of log entries. The table has the following columns: Receive Time, Type, Name, From Zone, To Zone, Attacker, Attacker Name, Victim, To Port, Application, Action, and Severity. The log entries show various threats, including spyware and vulnerability alerts, with actions such as 'drop-all-packets' and 'alert'.

Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
01/06 15:03:58	vulnerability	HTTP Non RFC-Compliant Response Found	External	Internal	54.152.126.174		10.10.60.17	51343	unknown-tcp	alert	informat...
01/06 15:03:57	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	212.92.241.105		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:56	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	97.80.128.153		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:55	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	186.55.116.89		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:54	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	201.210.254.182		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:53	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	27.3.108.29		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:52	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	105.227.159.69		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:51	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	86.97.21.183		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:51	vulnerability	HTTP Non RFC-Compliant Response Found	External	Internal	54.152.126.174		10.10.60.17	51321	unknown-tcp	alert	informat...
01/06 15:03:50	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	82.199.195.153		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:49	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	41.70.170.57		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:48	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	190.120.151.107		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:47	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	80.109.220.63		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:46	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	124.187.138.124		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:45	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	91.135.248.2		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:44	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	188.124.204.246		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:43	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	113.11.27.244		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:43	vulnerability	HTTP Non RFC-Compliant Response Found	External	Internal	54.152.126.174		10.10.60.17	51308	unknown-tcp	alert	informat...
01/06 15:03:42	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	85.26.122.215		172.20.102.155	1066	unknown-udp	drop-all-packets	critical
01/06 15:03:41	spyware	ZeroAccess.Gen Command and Control Traffic	External	Internal	37.143.208.112		172.20.102.155	1066	unknown-udp	drop-all-packets	critical

At the bottom of the interface, there is a navigation bar with the text "sadvsg | Logout" and "Active" status. The page is displayed at 110% zoom.



4401 Great America Parkway
Santa Clara CA 95054
USA

PH NO: 408-753-4000
FAX NO: 408-753-4001

Renewal Order 40123709

Customer Number 223557
Customer Name LA Community College Dist
Order Number 40123709
Customer Order Number 103301295137

Thank you for renewing the services on your Palo Alto Networks device(s). The services listed below have been extended on the Palo Alto Networks serial numbers noted.

To enable the service extensions to your Palo Alto Networks devices, please follow the instructions detailed below. **Please contact your sales representative if you have any questions.**

Auth Code	Part Number	Description	Apply To
40017314	PAN-SVC-PREM-4020-R	Premium support renewal, PA-4020 Period Covered: 08/04/2015 - 08/04/2016	0002C101099
65877859	PAN-PA-4020-URL4-HA2-R	PANDB URL filtering subscription for device in an HA pair renewal, PA-4020 Period Covered: 12/11/2015 - 08/04/2016	0002C101099
93889765	PAN-PA-4020-TP-HA2-R	Threat prevention subscription for device in an HA pair renewal, PA-4020 Period Covered: 12/11/2015 - 08/04/2016	0002C101099
28360672	PAN-SVC-PREM-4020-R	Premium support renewal, PA-4020 Period Covered: 08/04/2015 - 08/04/2016	0002C101087
48035424	PAN-PA-4020-URL4-HA2-R	PANDB URL filtering subscription for device in an HA pair renewal, PA-4020 Period Covered: 12/11/2015 - 08/04/2016	0002C101087
62797515	PAN-PA-4020-TP-HA2-R	Threat prevention subscription for device in an HA pair renewal, PA-4020 Period Covered: 12/11/2015 - 08/04/2016	0002C101087

Instructions:

1. Log in to the device's web interface.
2. Click on the 'device' tab on the web interface, then click the 'Licenses' link on the left column.
3. Click 'Retrieve license keys from license server'. The device will then show the new expiration dates.

Note: If your device doesn't have access to the Internet, you may activate your subscription by manually uploading a license key to the device. For further details, please refer to your Palo Alto Networks Administrator's Guide.

If you have any questions, please contact Palo Alto Networks Technical Support at +1.866.898.9087 (United States) or +1.408.738.7799 (outside the United States).