# Addendum 1: RFP: PGUSD Firewall 2027 470 270002780

**Correction 1:** The Manufacturer name for Basic Maintenance of Internal Connections should read “Palo Alto Networks *or equivalent.”*

## Questions and Responses

**Question 1:** Can you notify us directly of any changes or updates to the RFP or 470?
**Response:** No. In order to ensure a fair and open bidding process all changes will posted in EPC so that all bidders *known or unknown* will have access to the same information at the same time. Bidders should use the “follow” feature in EPC or monitor the 470 for changes.

**Question 2:** What is the current peak throughput and roughly how many concurrent devices pass through the firewall during the school day?
**Response:** Technically the current peak throughput should be 2Gb/s for our heavy usage days, but today our peak was 700Mb/s from our network switch to our Firewall. We have roughly 3000 devices on our network.

**Question 3.** Will the current firewall configuration (policies, NAT, objects) be shared with the awarded provider for the migration, and roughly how many rules are in place today?
**Response:** Yes, our security policies can be shared to the awarded service provider. The number of policies currently in place is not known as it is a managed service.

**Question 4:** Is the CIPA content filter running on the current firewall today, with SSL inspection, or is there a separate filtering product that will stay in place?
**Response:** The CIPA content filter is running on the current firewall without SSL Inspection and that will be required for any new solution as stated in the RFP.

**Question 5:** Will MCOE keep providing the same public IP addresses after July 1, 2027?
**Response:** We currently have 255 (/24) public IP addresses which are not transferable from MCOE. We currently use 50 different public IP addresses based on our internal VLANS.

**Question 6:** For the 15% "as a service" criterion, would a cloud-delivered firewall, with traffic sent from the data center to the provider's cloud and little or no equipment on site, fully meet the requirements?
**Response:** Yes, provided the vendor manages the firewall including hardware and software updates, troubleshooting, applying blocklist(s) similar to Palo Alto’s list and modifying the configuration based on the district's requests.

**Question 7:** For remote access VPN, what do users sign in with today (Active Directory, Entra ID, Google)?
**Response:** Currently not being used but would like the ability to set up VPN access based on Google Authentication.

**Question 8:** If equipment is placed on site, is rack space and power available at 835 Forest Ave at no cost to the provider?
**Response:** Yes, but not more than 5U and not excessive power consumption.

**Question 9:** For the 1-hour critical response, is remote response acceptable, or is onsite response expected?
**Response:** The 1-hour response time is intended for policy changes. There are technical staff onsite to perform physical work based on instructions or guidance from the vendor.

**Question 10:** What's the current firewall model?
**Response:** Palo Alto 5410.

**Question 11:** Are you seeking new firewall besides the support contract or is it only support contract for existing firewall/s?
**Response:** We are seeking a managed firewall / firewall functionality with support.

**Question 12:** How many firewalls will be supported?
**Response:** We are seeking a managed firewall / firewall functionality with support. We are not seeking support alone for an existing firewall or for a new firewall.

**Question 13:** If a new firewall is required, do you prefer specific model or should I order it (with license) for 2500 users?
**Response:** Proposals can be for any equipment that meets the specified functionality in the RFP. Palo Alto 5410 or equivalent is preferred.

**Question 14:** If a new firewall is required, how many firewalls are needed?
**Response:** Whatever Bidder feels is necessary to meet 99.9% uptime as described in the RFP.

**Question 15:** If a new firewall is required, do you want installation and configuration to it as well?
**Response:** Yes. We are looking for a turnkey managed solution as described in the RFP.

**Question 16:** What is the current peak and average Internet throughput through the firewall (in Mbps or Gbps), and what peak is expected by the end of the three optional years?
**Response:** Technically the current peak throughput should be 2Gb/s for our heavy usage days, but today our peak was 700Mb/s from our network switch to our Firewall.

**Question 17:** What are the current peak concurrent sessions and peak new connections per second?
**Response**: We have roughly 3000 devices on our network.

**Question 18:** How many users and devices (student, staff, guest, and IoT) are typically active at peak, and does this include BYOD or Chromebooks?
**Response:** We have roughly 3000 devices on our network which includes BYOD and Chromebooks.

**Question 19:** Which security features are enabled today and required going forward (application control, intrusion prevention, anti-malware or antivirus, advanced threat protection, SSL/TLS inspection, web filtering)? Throughput drops when these are enabled, so we need to size for the full feature set.
**Response:** Of these features the only ones currently enabled are application control, intrusion prevention, advanced threat protection and web filtering.

**Question 20:** What percentage of traffic is encrypted, and is SSL/TLS inspection required for all traffic, for student traffic only, or not at all?
**Response:** Most traffic should be encrypted, no inspection required.

**Question 21:** What physical interfaces are required on the firewall (for example, 1G copper, 10G SFP+ fiber), and how many are needed for the Inside, DMZ, and Outside zones?
**Response:** For on-premise hardware solutions would expect one singlemode10G SFP out to our ISP and one to our core switch.

**Question 22:** What type of handoff and optics does the MCOE connection use at the data center (for example, 10G single-mode or multi-mode fiber), and who supplies the transceivers?
**Response:** Proposals should include one 10G single mode SFP transceiver for the connection out to ISP MCOE and two 10G single-mode SFP's with transceivers for and compatible with the connection to our Meraki MS425-32.

**Question 23:** How many VLANs, subnets, and routed interfaces will the firewall terminate, and does it need to perform inter-VLAN routing or only perimeter filtering?
**Response:** Currently perimeter filtering only.

**Question 24:** Which routing protocols (static, OSPF, BGP) are in use between the firewall, MCOE, and the District core?
**Response:** Static IP addresses.

**Question 25:** How many Site-to-Site and Remote Access VPN tunnels are active today, what are the peak concurrent counts, and what client or authentication method is used (for example, IPsec, SSL VPN, SAML, MFA)?
**Response:** Currently no VPN tunnels are in place, but having the option for up to ten VPN tunnels in the future would be good.

**Question 26:** Which directory or identity source (for example, Active Directory, Entra ID, Google Workspace, LDAP) must be integrated for user-based policies and content filtering?
**Response:** No user-based policies currently in place. We are doing Mac Address filtering on our switches and firewall is perimeter filtering. Our local primary Authentication system is Google.

**Question 27:** Is high availability (active/passive or active/active) required, and is a single appliance with next-business-day replacement acceptable?
**Response:** Whatever Bidder feels is needed to achieve 99.9% uptime.

**Question 28:** What logging, reporting, and SIEM or syslog integration are required, and what log retention period applies?
**Response:** Currently no SIEM or syslog is in place or required.

**Question 29:** Does the District use IPv6, multicast, or any special protocols (for example, VoIP/SIP, video conferencing, or SCADA/building systems) that the firewall must support?
**Response:** None of these protocols will need to be supported by the firewall in the near future.

**Question 30:** Is the firewall expected to terminate the MCOE handoff directly, or is a separate router or MCOE-managed device in between? Is any NAT or public IP address space (such as a /24 block) owned by the District?
**Response:** MCOE currently owns our /24 block of public IP addresses which cannot be transferred to a different vendor. We currently use 50 of those public IP addresses based on our internal VLANS. The winning vendor will need to work with us and current ISP MCOE to design the system based on whether the selected solution is on premise equipment or offsite.