



Request for Proposal 26001
Firewall Solution
Addendum 1
October 3, 2025

<i>QUESTIONS</i>

1. Approximately how many Access rules, NAT rules, and routes are configured? In addition, please provide some context on the NGFW features in-use for these rules (IPS/IDS, L7, User-based, etc.).
Answer: Access rules 157, Nat rules 80, routes 860
2. Are we using static or dynamic routing? If so what protocols are currently in place and how extensive are they? Static and/or dynamic, how many approx. routes are there in the route table?
Answer: Dynamic and static. OSPF, static, BGP
3. Is the Fortigate firewall configured into Multiple Virtual Domains or is it functioning in a Single Domain? If so how many?
Answer: Single Domain
4. What is the transform set that is used between the 3700D Fortigate and fifteen 60 and 61 series Fortigates? Also, will the number of site-to-site VPN's increase in the future (we need a number of years to estimate)?
Answer: IPSec, Pre-shared Key, Phase 1, Diffe-Hellman Groups, Phase 2, Local address & remote address. The number could increase but we have no solid numbers
5. The firewall is listed as performing load balancing -Can you please elaborate on the specifics of the service(s) currently load-balanced, including any specific feature requirements?
Answer: Simple Static or Least Session load balancing is used for a few applications.
6. There are approximately 500 RA VPN users listed will this number increase in (we need a number of years to estimate)? How many RA VPN groups and types are there?
Answer: No
7. How is DLP configured and is TLS/SSL inspection used in the environment? If TLS/SSL inspection is enabled, then how many policies are associated with this and would we be re-using a certificate already in use in the environment?
Answer: Not using DLP. TLS/SSL, 90 policies and re-using certificate

8. How many reports are generated via Fortianalyzer and what are those reports currently sharing?

Answer: Three reports are generated and scheduled. Threat, VPN for previous six months and Web usage report from the previous week. Need to be able to generate reports as needed, bandwidth, IPS, etc....

9. What code version of Fortinet is used currently?

Answer: v7.4.8 build2795 (Mature)

10. Will the migration of the 3700D be like for like or will evaluation and re-design be requested? If evaluation and re-design are being considered what is the desired end state from what the environment is today?

Answer: Refer to Point 7 – Scope of Requirements

11. What are the specific requirements for the 15 sites with firewalls today? Are these performing NGFW features (IPS/IDS, L7 policy, SSL inspection, etc.) or are they explicitly used for the site-to-site connection? (We are trying to determine if SD-WAN could be a potential option for our proposal)

Answer: They are only used for site-to-site connectivity.

12. What is the average weekly and daily traffic flow through the existing 3700D firewalls?

Answer: Daily Peak: Inbound 7 gigs, outbound 7 gigs

13. For SSL Decryption and Inspection, how much of the total district traffic is being Decrypted on a daily basis?

Answer: We do not have that enabled.

14. What is the anticipated district throughput requirements growth over the next 3-5 years?

Answer: up to 50%

15. Please confirm if there is only a single 3700D in each Datacenter (ESC and TSC).

Answer: This is correct

16. Are there any additional advanced features configured (or required) such as IP SLA, Policy Based Routing, QOS, etc.?

Answer: Not configured but in the future maybe policy-based routing

17. For reporting, what specific reports are needed? Are there any reporting requirements we should be aware of?

Answer: Three reports are generated and scheduled. Threat, VPN for previous six months and Web usage report from the previous week. We would like to be able to generate more reports as needed.

18. Is it necessary for the firewalls in the datacenter and at the satellite offices to be managed by a common management platform?
Answer: Yes
19. Are the upgrades of the remote firewalls included with this project?
Answer: Yes, we require them to be replaced
20. What is the Total Threat Protection Throughput requirement for the datacenter and remote firewalls? Threat Protection = AV, IPS, App Control, Web Filtering.
Answer: Threat Protection: 60 + Gbps
IPS: 160 + Gbps
App Control: 130 + Gbps
Next Gen Firewall NGFW: 60 + Gbps
21. What is the Total SSL Decryption throughput required?
Answer: 60 + Gbps
22. How many devices (workstations/servers) will be subject to Full SSL Deep Packet (SSL Decryption) Inspection?
Answer: 50,000 +
23. Will SSL deep packet inspection/decryption be configured only on the datacenter firewalls?
Answer: Yes
24. Are the remote firewalls (FG-60E, 61F, etc.) requiring security services (AV, IPS, App Control, Web Filtering, etc.)? Or is all inspection taking place in the datacenter firewalls?
Answer: All Inspection is at datacenter firewalls
25. What date will TPS notify the winning bidder?
Answer: TBD
26. What date (approximate) does TPS anticipate installation beginning?
Answer: TBD
27. It is our understanding that the District is looking to replace the two Fortinet 3700D units currently deployed in their data centers. Would a hybrid on-premises next-generation firewalls with a cloud-based security service approach align with the District's expectations?
Answer: Yes
28. Do you plan to manage the firewall solution in-house, or through a managed service provider?
Answer: In house, maybe managed service later

29. If managed in-house, do you currently have 24/7 proactive monitoring and incident response capabilities?

Answer: No

30. What SIEM solution, if any, is currently in place?

Answer: No SIEM but testing with CrowdStrike Next-Gen SIEM

31. Will TPS need to support remote learning/off-school filtering to meet CIPA compliance (e.g., for student Chromebooks, faculty laptops, etc.)?

Answer: No

32. The RFP provides different numbers of firewalls to be replaced: Section 2.c references replacement of eight end-of-life Fortigate 60E models; Section 7 states that TPS expects to replace about 17 firewall devices; and Exhibit II states that only two Fortinet 3700D firewalls are being replaced. Can TPS please clarify the exact number and types of firewall devices that are expected to be replaced under this solicitation? (Ref: Section 2.c, Section 7, Exhibit II).

Answer: Replace all 17

33. The RFP provides different numbers of firewalls to be replaced: Section 2.c references replacement of eight end-of-life Fortigate 60E models; Section 7 states that TPS expects to replace about 17 firewall devices; and Exhibit II states that only two Fortinet 3700D firewalls are being replaced. If the scope of work involves replacing fewer than the full complement of TPS's firewall environment, will TPS require the proposed solution to interoperate with any remaining Fortinet firewalls or other devices that remain in service? If so, can TPS provide additional detail on interoperability expectations (e.g., management, policy synchronization, VPN compatibility, etc.)? (Ref: Section 2.c, Section 7, Exhibit II)

Answer: Replace all 17

34. The RFP provides different numbers of firewalls to be replaced: Section 2.c references replacement of eight end-of-life Fortigate 60E models; Section 7 states that TPS expects to replace about 17 firewall devices; and Exhibit II states that only two Fortinet 3700D firewalls are being replaced. If some or all of the Fortinet 60/61 firewalls are to be replaced, can TPS provide use cases and functional requirements for these remote firewalls, along with any throughput, feature, or user-capacity requirements needed to size and price replacements appropriately?

Answer: Replace all 17.

35. The RFP specifies Fortinet devices in the current environment but does not indicate whether TPS has a preferred vendor platform for the replacement firewalls. Because centralized management, reporting, and licensing models vary significantly across vendors, can TPS state its preferred vendor platform, if any? (Ref: Section 2, Exhibit II)

Answer: No preferred vendor

36. The RFP establishes a base year with four one-year option renewals. Can TPS clarify its expectations for the vendor's responsibilities during these periods after go-live — specifically, whether ongoing obligations are limited to manufacturer support contracts (warranty, licensing, updates) plus the 80 hours referenced in section 8.2.e or if additional vendor-provided professional services are anticipated? How should vendors indicate their price for additional services, including option year services? (Ref: Section 3, Section 8.2.e)

Answer: limited to manufacturer support contracts (warranty, licensing, updates) plus the 80 hours referenced in section 8.2.e

37. The list of pricing metrics does not include equipment procurement. Is the vendor responsible for procuring the firewall devices? If so, how should vendors indicate their prices? (Ref: Section 8.2)

Answer: Yes, pricing should include hardware costs plus any shipping or delivery fees

38. What restrictions on downtime should vendors expect that might impact installation and cutover (after-hours, only during instructional breaks, etc.)? (Ref: N/A)

Answer: Will have to be on a scheduled outage, From Friday night to Sunday afternoon

39. Can TPS clarify the scope of VPN migration? Specifically, will the vendor be expected to reconfigure all 15 site-to-site VPN connections and ~500 remote-access users on the new platform, including client software distribution and cutover testing? (Ref: Section 2.c-d, Section 7.viii)

Answer: Yes, turnkey solution, as of now we have 50 vpn clients

40. The RFP states that the current firewalls are configured in proxy mode and non-HA, but mandates high availability and failover between data centers. Can TPS clarify whether this means maintaining the current two-firewall footprint with HA configured between the two sites, or if TPS prefers HA pairs at each site for enhanced resilience? (Ref: Section 2.e, Exhibit II)

Answer: We want high availability and failover

41. The RFP notes that the current ESC firewall is being used as a load balancer for the Student Information System. Can TPS clarify whether the replacement firewalls are required to provide equivalent load balancing functionality? If the firewall devices do not provide this capability, should vendors propose alternative solutions? (Ref: Section 2.f, Exhibit II)

Answer: Yes, load balancing is required or an alternative provided.

42. The description of Attachment A ("Pricing") does not match the provided Attachment A, and attachment A is not included in the list of attachments to be completed. Please clarify. (Ref: Section 5, Section 8.3, Attachments)

Answer: That should be Attachment C. Attachments A-G are required.

Vendor Signature

Date:

Maranda Jessie

Purchasing Manager

Proposal responses must include a copy of this page, signed by the vendor, confirming receipt of same. We hope this information is helpful in developing your response and we appreciate your participation.