

1. Can JCPS please provide estimated network throughput between the sites and your central datacenters?
  - a. 1Gb x 150
2. Can JCPS please confirm if all remote locations connected in the same manner, fiber, MPLS, etc..
  - a. All Fiber
3. For VPN services, will these be utilized by external users connecting into the environment, or will they be used to connect to remote locations?
  - a. User connections 1500 users / 1000 Concurrent
4. 4.Can JCPS please confirm if all applications and services are hosted in the central data center, or will certain services be hosted remotely at different locations?
  - a. All in the datacenter currently but could be distributed in a couple of locations in the future. Ensure proposal includes equipment that can be HA with nodes being separated physically.
5. Regarding the Certificate of Insurance – Line 4C lists Commercial Bus Insurance. Would JCPS consider removing this requirement for this RFP?
  - a. This section of the COI is not applicable to this bid.
6. Is JCPS looking for a managed firewall solution by where the vendor owns and manages the firewalls or is JCPS looking to own and manage the firewall solution?
  - a. Prefer owning and this is an Internal Firewall as our External Firewall is managed by the Kentucky Department of Education. (KDE)
7. What is the expected network throughput?
  - a. Up to 400Gb
8. What is the network architecture?
  - a. Will be discussed at a later date
9. Are the firewalls to be deployed as HA?
  - a. Yes
10. How many ports are required by segment? i.e. WAN, LAN, DMZ
  - a. 4

11. What types of ports are required? i.e. Ethernet (RJ45), fiber (SFP/SFP+), or other  
a. QSFP28 or above

12. What are the port speed requirements? i.e., 1 Gbps, 10 Gbps, 40 Gbps  
a. 100Gb

13. What is the Internet routing to the firewall? i.e. static, BGP, etc..  
a. Static

14. The specifications note “multiple 100G connections.” How many 100G will the firewalls need to support? What is the minimum port density needed (ie, how many of each port type)?  
a. 4

15. Aside from the current 100G port connections, how many are anticipated to be added in the next 36 months?  
a. No additional 100G required for this timeline.

16. Will these firewalls be acting as internal firewalls for the customer? Will they be interfacing with additional networks, or segmenting external networks across shared fiber? For example, in the case where JCPS owns a portion of fiber and leases that to an external entity.  
a. Yes, internal firewall, not interfacing with other/external networks

17. Are there topology maps available showing all connections to the datacenter firewalls?  
a. Information to be shared with the winning bidder.

18. What is the estimated IMIX utilization?

- a. Our environment reflects a typical enterprise/school district traffic mix with:
  - i. File repository (SMB, CIFS, SFTP, NFS)
  - ii. Streaming security video (Cameras)
  - iii. Internal web application traffic (e.g., MUNIS, other internal apps)
  - iv. Remote Management (RDP, BeyondTrust, SSH) for select personnel
  - v. Alarm system traffic (fire/burglar central station)

**Typical packet size distribution** (approximate):

- vi. 20% small packets (~64–128 bytes, e.g., ACKs, DNS, core network service)
- vii. 30% medium packets (~512 bytes, e.g., general web, high connection count)
- viii. 50% large packets (~1,200–1,500 bytes, e.g., video, file transfer)

Firewall should sustain **full throughput with NGFW services enabled** (e.g., IPS, application control) under this realistic IMIX load, **not just large-packet “ideal” lab tests.**

19. What is the estimated IPS/IDS utilization?

- a. 400Gb

20. Is the support and ticketing system with SLA request for during installation time frame or does JCPS require support and response after the installation/testing and handover as well? Is this outside of manufacturer hardware/software support? if so, for how long?

- a. We need bidders to include their ticketing, support, SLA information in their proposal for both implementation/initial setup phase and the ongoing support phase. Whether or not that is bidder provided or augmented by manufacturer support is up to the bidder.

21. For ongoing maintenance and escalation support, is this outside of manufacturer hardware/software support? If so, for how long?

- a. Support requested for minimum of 5-year cycle, but realistically up to around 7 (+ or -) within the useful life of the hardware. We need the solution supported by the manufacturer throughout the term of the contract, including potential extensions. We’re requesting a line item for hardware refresh as well at the end of the initial hardware lifecycle at the end of year 5.

22. Does JCPS have guidance for what is considered acceptable SLA's?

**a. Acceptable Firewall SLA example:**

**Uptime Guarantee:**

- i. 99.99% monthly uptime (excluding scheduled maintenance – coordinated with the school district (14 days – 30 days' notice typical))

**Support Availability:**

- ii. 24x7x365 for critical (Severity 1 and 2) issues
- iii. Business hours (e.g., 6:30 AM – 5 PM Eastern, Mon–Fri) for lower-priority issues

**Response & Resolution Targets:**

- iv. Severity 1 (Critical): Respond within 30 min, resolve within 4 hours
- v. Severity 2 (High): Respond within 1 hour, resolve within 8 hours
- vi. Severity 3 (Medium): Respond within 4 hours, resolve within 1–2 business days
- vii. Severity 4 (Low): Respond within 1 business day, resolve within 3–5 business days

**Performance Metrics (if applicable):**

- viii. At least 90% of rated throughput under normal load
- ix. <5 ms latency for inline services (IPS/IDS, etc.)

**Change Management:**

- x. Emergency changes: within 2 hours of approval
- xi. Scheduled changes: within scheduled window (typical 14-30 days minimum notice)

23. What are expected average and maximum concurrent firewall session quantities?

**a. 3-5**

24. What total firewall throughput is required with threat prevention security services enabled?

**a. 80-100gps**

25. What security inspection and enforcement services (subscriptions) are required such as threat prevention, URL filtering, malware prevention, DNS security, IOT device detection, and/or data loss prevention?

**a. Threat Prevention, Malware Prevention**

26. What are network interface requirements such as quantity of network interfaces, type of network interfaces (i.e., copper, optical, virtual subinterfaces such as VLAN subinterfaces), link speeds, and data throughput?

**a. Optical 100G x 4**

27. What are network traffic decryption requirements such as type or percentage of traffic to decrypt for increased threat inspection and detection capabilities?

- a. Decrypt 60% – 80%, Web Browsing (HTTPS/443), Email over HTTPS (webmail), File Transfer (Dropbox, Google Drive, OneDrive), Social Media & Messaging Apps, Custom Applications Over TLS