JOLIET
JUNIOR COLLEGE
1901

DATE: April 11, 2018

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO: Prospective Respondents
SUBJECT: Addendum No. 1
PROJECT NAME: Firewall Replacement
JJC PROJECT NO.: R18003

This Addendum forms a part of the Bidding and Contract Documents and modifies the original bidding document as posted on the JJC website. Acknowledge receipt of this addendum as specified at the end of this addendum. FAILURE TO DO SO MAY SUBJECT BIDDER TO DISQUALIFICATION.

<u>Questions Received:</u>

1. Who is your current perimeter firewall vendor?
   Cisco

2. How long have they been deployed in your environment?
   5 years

3. Why are you looking to replace this solution?
   Hardware throughput and connection limitations

4. What email provider do you currently use (looks like O365 but just confirming)?
   Microsoft O365

5. Who do you currently use for CASB?
   Microsoft EMS

6. What is your current, maximum ISP throughput observed on your existing perimeter firewalls? **We are currently subscribed to 1.75 GB. The college has the ability to connect at 10 GB to its current ISP.**

7. You mentioned 20 Gbps throughput is the requirement. Is this maximum future growth you wish to achieve? How was this 20 Gbps throughput goal calculated?
   Yes this is the maximum future growth we wish to have available. The College is currently

supporting 7,500 wired devices and 3,500 wireless clients on a daily basis. That is 20% more devices on the JJC network since last year. The bandwidth has nearly doubled each year over the past 5 years. Increased technology requiring bandwidth, such as:

- **Unified Communications – voice/video over IP (currently 2000 devices),**
- **DR/BC with Azure Site Recovery - DPM backups),**
- **Increase in social media applications running through the network,**
- **Increase in streaming video in the classroom and from guest devices**
- **Increase frequency in updates/patching to OS and application patching on devices, and**
- **An increase in the number of devices being brought on the network by students, faculty and staff.**

To secure its critical digital assets whether they are on the college premises or hosted on third party cloud based solutions, the college is seeking to acquire very high-throughput firewalls to grow in to that offer effective intrusion detection & prevention services and micro-segmentation capabilities without affecting throughput, performance and capabilities of these firewalls.

The College is also looking for the perimeter firewall to handle SSL encryption in both directions. SSL traffic is growing and it will continue to increase in the foreseeable future due to concerns about privacy. With SSL traffic currently accounting for 77% of JJC Internet traffic, the college must factor in performance needs and future bandwidth usage.

a. Please note we often see high throughput requirements when working with universities - this target throughput is hardly ever actually observed in the environment. Higher throughput requirements may unnecessarily increase cost as larger firewalls are required to sustain the requirement.

8. What is the maximum number of nodes (active IP addresses) you see at peak times sending traffic through your current perimeter firewall?
7,500 wired devices and 3,500 wireless

9. Is remote access VPN a requirement? If so, who owns these devices? What is the maximum number of remote access clients that will be connected concurrently?
Yes it is a requirement. We currently have 22 remote VPN access clients configured for IT and other college departments. We are looking to expand and have Faculty and staff remote from off-site through VPN to increase our remote security posture (up to 1500 users).

10. 6 N. Solution must include a zero-hour protection mechanism for new viruses spread through email and spam without relying solely in heuristic or content inspection. Would a Sandbox feature fulfill these requirements?

Yes, a sandbox feature would fulfill these requirements provided that no additional hardware is needed.

11. 6. R. Block upload of data even when allowing access to the site: The application function must be able to block the upload of data to a site even if access to the site is allowed by policy. This includes input into forms as well as the upload of files. Does this include the need to decrypt SSL traffic via a reverse-proxy mechanism?
    Yes, we are trying to protect all SSL traffic (inbound and outbound).

12. 6. Y. SSL decryption at scale (decrypt enclave) - The application control feature should be able to identify the application in use within SSL traffic. Once identified, applications can be allowed, blocked and limit available bandwidth. The solution must participate in the initial SSL key exchange and then decrypt session traffic to examine the contents for attacks, including both inbound and outbound inspection based on policy, without availing of offload to alternate system. The solution must have the ability to detect malware signatures within packets encrypted within SSL, i.e. web server. Do you plan on decrypting SSL traffic both outbound and inbound on the same device (i.e. both for employees visiting external SSL sites and for customers connecting to your SSL servers?)
    Yes, we want to decrypt both inbound and outbound SSL traffic on the same device.

13. 8. F. Solution must support the VPN configuration with a GUI using drag-and-drop object addition to VPN communities. Please explain this requirement in more detail, include an example screen-shot if at all possible.
    We are looking for a more user-friendly interface for setting up configurations.

14. 20Gbps throughput requirement with Next Gen features enabled in real world traffic. Can you elaborate on the nature of your 'real world' traffic? What percentage of this traffic is SSL? How many new sessions per second are you seeing at peak? Do you have any data on how the required 20 Gb/s breaks out between client and server requests?
    Currently, 77% of our traffic is SSL. We have determined we have reached our maximum firewall connections per second (50,000) during peak time. On our current network we have peaked at 1.75 GB/s. We wish to achieve 20Gbps maximum future growth and the ability for the firewall to apply all Threat Prevention features enabled with that throughput (measured with application identification, IPS, antivirus, anti-spyware, URL filtering and logging enabled).

15. Solution must be Tufin compliant - for continuous compliance and audit readiness. By 'compliant' do you mean able to send real-time data to Tufin in a format it understands or something more involved?
    Yes, the ability to send to Tufin in a format it understands.

16. How many connections does JJC have?
    We have determined we have reached our maximum connections per second (50,000) during peak time.

17. How many VLAN's? Does JJC have a DMZ, and if so how many devices are sitting in there (approximate is okay)?
    Approximately 200 VLANS
    Yes, JJC does utilize a DMZ. Devices equivalent up to a Class-C network.

18. Will this be High Availability?
    Yes.

19. How many FW rules does JJC have?
    425 rules (50 of which are NAT)

20. Does JJC have any VPN? Site to site or clients?
    Yes, utilizing both site to site for Azure connection and clients for remote access VPN. We have a site-to-site VPN to Microsoft for our Azure environment. We have the need for additional site-to-site VPN connections for short-term engagements with third-party vendors.

21. What features of the firewall do you plan to use? Will we be setting those up? Do you have policies on those from your current FW? (Web Filtering, IPS, Malware, Sandboxing, etc)
    We currently do not have any of these additional features on our current firewall, but we would like for these to be implemented in the install.

22. If using Web Filter, do you have different URL Filtering profiles for different groups?
    Currently, we are using Web Reputation and white-listing on a separate Cisco WSA web filter. We would like to switch this feature over to the firewall.

23. For the 4 quarterly health checks, will these be performed onsite or remotely. We would recommend remotely but can do both. If done remotely, we will need remote access (VPN, RDP, etc)
    Provide cost for both options. VPN access will be granted after signing our third party connection agreement.

24. If we do not have independently audited statements, what alternative document will be accepted?
    The requested documentation is required.

25. What are the current devices in place in your environment and how many are being replaced?
    Two Cisco ASA 5585-X, high availability, active/standby

26. Can you provide a current network inventory and include the current firewalls?
    7,500 wired devices and 3,500 wireless

27. In planning for the future (over next 5 years), Is there a plan in place to expand hardware and users that needs to be considered when responding to the RFP?
    User base may increase by 2 to 3 percent per year (current head counts: 2,000 faculty/staff and 15,000 students). Bandwidth and connection count growth will need to be considered. In addition to this hardware based firewall solution, the college is also seeking to implement a limited set of software based firewalls in the future to protect its most critical Microsoft Hyper-V based virtual machines in the cloud (future capability).

28. How many policies and rules currently exist that will be evaluated and potentially brought forward to the new firewall?
    425 rules (50 of which are NAT)

29. Will the firewall replacement occur during the day or will it need to happen "off hours" in the evening or on a weekend day?
    During a change control window which tends to be Friday night in to the weekend.

30. Do you expect the quarterly review of the installed firewall to be done via remote access or through an on-site visit? (mentioned in the scope of work)
    See question 23 above.

31. The scope of work mentioned Compliance to the college requirement, which specific guidelines should we refer to and can those be provided?
    Compared to NIST 800-53

32. For the proxy bypass - is there some specific items you have in mind that would define our test level to ensure no proxy bypass? What is currently blocked and would matching the current restrictions be adequate in the next solution?
    We want the new solution to have this capability. Looking for recommendations from your solution on how to test.

33. Question 16 of the Security Requirements states "capable of being implemented in multiple virtual environments as well as cloud" does this mean the request is for both a physical firewall and a virtual firewall to be provided?
    This request is for a physical firewall replacement, but want to have a solution that has a software version for future implementation in the cloud (i.e. Azure).

34. Current Firewall:
    a. Is current firewall an HA Pair?
       HA Pair
    b. Is it Active/Active or Active/Passive?
       Active/Passive
    c. Total number of interfaces currently used on primary Firewall? ***Six (6)***
    d. Number of outside interfaces (ISP connectivity) on primary Firewall? ***Two (2)***
    e. Current Bandwidth to the ISP(s)? ***1.75 GB***

f. Average bandwidth utilization to each ISP? ***400 MB Avg., 1.75 GB Peak***

g. Number of security policies (number lines of security filters)?

  i. For policy? ***375 rules***

  ii. For NAT? ***50 rules***

h. Number of objects on the current firewalls?

530 Object groups
1240 Network Objects
135 Service Objects

35. What services are currently used on your firewall:

  a. IPS/IDS? ***NO***

  b. Encrypt/Decrypt of packet streams? ***NO***

  c. Application Visibility and Control (AVC)? ***NO***

  d. IPSEC VPN ***YES***

    i. How many site-to-site VPN tunnels are used?
    We have a site-to-site VPN to Microsoft for our Azure environment. We have the need for additional site-to-site VPN connections for short-term engagements with third-party vendors.

  e. Client VPN

    i. On average, number of VPN clients connected at one time ***22***

    ii. Maximum number of VPN Clients allowed***. 5000***

  f. URL filtering? ***NO.***

  g. Malware protection? ***NO***

  h. Threat Protection? ***NO***

  i. Data Loss Prevention? ***NO***

  j. Sandboxing? ***NO***

36. Current Performance of Firewall

  a. Throughput of current firewall ***2 GB***

  b. Average number of concurrent connections through firewall
  Avg at 30,000, Peaking at 50,000

  c. High water mark of number of concurrent connections ***Peaking at 50,000***

37. Expected performance of new Firewall system

  a. Are you looking to increase bandwidth to ISP(s)? ***Yes. Incrementally as needed.***

    i. If so, what will be the likely bandwidth increase? ***Incrementally as needed and as budget allows.***

  b. Encrypt/Decrypt

    i. Are you planning to exempt traffic like Healthcare (HIPAA) from Encrypt/Decrypt?
    We need to have the ability to choose decryption exceptions to exclude applications that do not function properly when the firewall decrypts them, URL categories (financial or health-related), services (port or protocol), and targeted server (certificate) traffic from decryption.

c. Desired maximum number of concurrent sessions
We are currently maxing out at 50,000 connections. Looking for the ability to grow and the solution to last up to 5 years (Est. between 250,000 to 350,000 connections)

38. Are you looking for a Build of Materials for this RFP? ***YES.***

a. If so, what are the number of public and private cloud environments which will be needed to be secured? ***This request is for a physical firewall replacement, but want to have a solution that has a software version for future implementation in the cloud (i.e. Azure).***

End of Addendum #1

JOLIET JUNIOR COLLEGE
1901

DATE: April 11, 2018

Joliet Junior College
1215 Houbolt Road
Joliet, IL 60431

TO:	Prospective Respondents
SUBJECT:	Addendum No. 1
PROJECT NAME:	Firewall Replacement
JJC PROJECT NO.:	R18003

Please acknowledge receipt of these addenda by including this page with your proposal. Include your company name, printed name, title, and signature in your acknowledgement below. Failure to do so could result in disqualification of your bid.

Issued by:

Janice Reedus
Director of Business & Auxiliary Services
Joliet Junior College
815.280.6643

I acknowledge receipt of Addendum #1.

____
Company Name

____
Printed Name

____
Title

____
Signature