REQUEST FOR PROPOSAL
#R18003

FIREWALL REPLACEMENT
April 20, 2018

JOLIET JUNIOR COLLEGE
1901

Joliet Junior College
Request for Proposal
Firewall Replacement

April 20, 2018

Background

Joliet Junior College is a comprehensive community college. The college offers pre-baccalaureate programs for students planning to transfer to a four-year university, occupational education leading directly to employment, adult education and literacy programs, work force and workplace development services, and support services to help students succeed. The College has a combined total of 14,912 full time and part time students enrolled in Spring 2018 classes and 1,950 staff on its main campus located within the city of Joliet, and its 5 extension campuses located in Romeoville, Morris, Frankfort, Weitendorf, and City Center in downtown Joliet.

Vision Statement

Joliet Junior College will be the first choice.

Mission Statement

Joliet Junior College is an innovative and accessible institution, dedicated to student learning, community prosperity, cultural enrichment, and inclusion. Joliet Junior College delivers quality lifelong learning opportunities empowering diverse students and the community through academic excellence, workforce training, and comprehensive support services.

OVERVIEW

Joliet Junior College (JJC) requests proposals for a next generation firewall solution which will provide a secure and scalable environment to support the many services provided by the College.

JJC intends to purchase a next generation firewall solution with protection from zero-day attacks for its perimeter network. A Firewall solution with built in Web Security and Web Application Firewall (WAF) services. This investment would be contracted for 3, 4, or 5 years with yearly subscription payments for software licenses. The firewall must be able to handle 20 Gbps throughput without compromising its functionalities and performance with threat prevention (application identification, IPS, antivirus, anti-spyware, malware and logging) enabled. Solution must include 3, 4, and 5-year hardware & software support options (24x7x4 hours, 8x5x4 hours, 8x5xNext Business Day (NBD)), threat intelligence subscription(s) and any other annual fee required.

The College also requires appropriate active/ standby or clustered hardware appliances that are scalable to cater for increase future needs.

The hardware must support Internet feed from multiple ISP's.

Additional scope is discussed in the **SCOPE OF WORK** section of this proposal.

I. RFP SCHEDULE

Date **(2018)**	**Event**
March 29, 2018	Vendors contacted via email / advertised
April 6, 2018 @ 2:00pm	Last date/time for submission of written questions via email to purchasing@jjc.edu
April 11, 2018	Responses to questions emailed
April 20, 2018 @ 2:00pm	Proposals must be submitted to the attention of: Janice Reedus, Director of Business & Auxiliary Service, Campus Center Building A, Room 3100, 1215 Houbolt Road, Joliet, IL 60431
April 20-26, 2018	JJC Evaluation Team reviews proposal
May 10, 2018	Notification of Award

II. INSTRUCTIONS TO VENDORS

ADVICE: The department responsible for this RFP is the Business and Auxiliary Services located at Campus Center, Building A, Room 3100, 1215 Houbolt Rd., Joliet, IL 60431-8938. The JJC contact will be Janice Reedus, Director of Business & Auxiliary Services, telephone (815) 280-6640; fax (815) 280-6631.

Questions concerning this RFP will be answered if sent to the Purchasing Department via email to purchasing@jjc.edu on or before April 6, 2018 by 2:00 pm.

All questions and answers will be published and provided to all potential suppliers by end of business day on April 11, 2018.

SUBMISSION: the submission of a response shall be prima facie evidence that the supplier has full knowledge of the scope, nature, quality of work to be performed, the detailed requirements of the project, and the conditions under which the work is to be performed.

Faxed proposals ARE NOT acceptable. All RFPs must be submitted by the date and time of

public opening (see above). RFPs must be submitted on the forms provided in a sealed envelope clearly marked (typed or blocking lettering only) with the vendor's name, return address, RFP for Firewall Replacement, the opening date and time. An original and six (6) copies of the RFP, and a complete electronic copy (DVD or flash drive) of the proposal shall be provided. Each hard copy shall be submitted in a binder. RFPs must be addressed to: Joliet Junior College, Janice Reedus, Director of Business & Auxiliary Services, Campus Center Room A3102, 1215 Houbolt Rd., Joliet, IL 60431-8938.

RFPs not submitted in the format as instructed by this RFP will not be accepted. Addendums to this RFP, once filed, may be submitted in a sealed envelope only, properly identified, prior to the opening hour.

Receipt of RFP / Late RFP: Sealed RFPs shall be received at the place and until the time indicated in this RFP. It is the sole responsibility of the vendors to ensure timely delivery of the RFP. JJC will not be responsible for failure of service on the part of the U.S. Postal Service, courier companies, or any other form of delivery service chosen by the vendor.

RFPs received after the date and time specified shall be considered LATE, and shall not be opened.

Accuracy of Proposals / Withdrawal of Proposals prior to RFP Opening: Proposals will represent a true and correct statement and shall contain no cause for claim of omission or error. Proposals maybe withdrawn in writing or by facsimile (provided that the facsimile is signed and dated by vendor's authorized representative) at any time prior to the opening hour. However, no proposal may be withdrawn for a period of one hundred twenty (120) days subsequent to the opening of the RFP without the prior written approval of the Director of Business and Auxiliary Services or Joliet Junior College.

ADDENDA: The only method by which any requirement of this solicitation may be modified is by written addendum.

PROPOSAL DUE DATE: The proposal must be received on or before April 20, 2018 by 2:00pm at the Business and Auxiliary Services Department, Campus Center, Room A3100, 1215 Houbolt Rd., Joliet, IL 60431-8938

INSURANCE:

The supplier performing services for JJC shall:

Maintain worker's compensation insurance as required by Illinois statutes, for all employees engaged in the work.

Maintain commercial liability, bodily injury and property damage insurance against any claim(s), which might occur in carrying out the services, referenced in this RFP. Minimum coverage will be TWO MILLION DOLLARS ($2,000,000) liability for bodily injury and property damage including product liability and completed operations.

Provide motor vehicle insurance for all owned, non-owned and hired vehicles that are used in carrying out the services described in this RFP. Minimum coverage shall be TWO MILLION DOLLARS ($2,000,000) per occurrence combined single limit for automobile liability and property damage.

TAXES:

JJC is exempt from all federal excise, state and local taxes unless otherwise stated in this document. In the event taxes are imposed on the services purchased, JJC will not be responsible for payment of the taxes. The supplier shall absorb the taxes entirely. Upon request, JJC's Tax Exemption Certificate will be furnished.

INDEMNIFICATION:

The supplier shall protect, indemnify and hold JJC harmless against any liability claims and costs of whatsoever kind and nature for injury to or death of any person or persons and for loss or damage to any property occurring in connection with or in any incident to or arising out of occupancy, use, service, operations or performance of work in connection with the contract, resulting in whole or in part from the negligent acts or omissions of the supplier.

DISCLOSURE:

Vendor shall note any and all relationships that might be a conflict of interest and include such information with the bid.

TERM OF CONTRACT:

Any contract, which results from this RFP may be for a period of three (3), four (4) or five (5) year(s) from the date of the contract award. **Respondents to this proposal must provide pricing for all three (3) contract timeframes.**

BLACKOUT PERIOD:

After the College has advertised for proposals, no pre-proposal vendor shall contact any College officer(s) or employee(s) involved in the solicitation process, except for interpretation of specifications, clarification of bid submission requirements or any information pertaining to prebid conferences. Such vendors making such request shall email Janice Reedus, Director of Business & Auxiliary Services, at purchasing@jjc.edu No vendor shall visit or contact any College officers or an employee until after the proposal is awarded, except in those instances when site inspection is a prerequisite for the submission of a proposal. During the black-out period, any such visitation, solicitation or sales call by any representative of a prospective vendor in violation of this provision may cause the disqualification of such bidder's response

III. GENERAL TERMS AND CONDITIONS

Applicability: These general terms and conditions will be observed in preparing the proposal to be submitted.

Purchase: After execution of the contract, purchases will be put into effect by means of purchase orders or suitable contract documents executed by the Director of Business and Auxiliary Services.

Right to Cancel: JJC may cancel contracts resulting from this RFP at any time for a breach of any contractual obligation by providing the contractor with thirty-calendar days written notice of such cancellation. Should JJC exercise its right to cancel, such cancellation shall become effective on the date as specified in the notice to cancel.

Governing Law and Venue: This contract shall be construed in and governed under and by the laws of the State of Illinois. Any actions or remedies pursued by either party shall be pursued in the State and Federal Courts of Will County, Illinois, only after Alternate Dispute resolution (ADR) has been exhausted.

Dispute Resolution: JJC and the contractor shall attempt to resolve any controversy or claim arising from any contractual matter by mediation. The parties will agree on a mediator and shall share in the mediation costs equally.

Costs: All costs directly or indirectly related to preparation of a response or oral presentation, if any, required to supplement and/or clarify a proposal shall be the sole responsibility of and shall be borne by the vendor.

Proprietary Information: Vendor should be aware that the contents of all submitted proposals are subject to public review and will be subject to the Illinois Freedom of Information Act. All information submitted with your proposal will be considered public information unless vendor identifies all proprietary information in the proposal by clearly marking on the top of each page so considered, "Proprietary Information." The Illinois Attorney General shall make a final determination of what constitutes proprietary information or trade secrets. While JJC will endeavor to maintain all submitted information deemed proprietary within JJC, JJC will not be

liable for the release of such information.

Business Enterprise Program (BEP):
Minorities, Females, and Persons with Disabilities Participation and Utilization Plan:
Joliet Junior College will make every effort to use local business firms and contract with small, minority-owned, and/or women-owned businesses in the procurement process. This solicitation contains a goal to include businesses owned and controlled by minorities, females, and persons with disabilities in the College's procurement and contracting processes in accordance with the State of Illinois' Business Enterprise for Minorities, Females, and Persons with Disabilities Act (30 ILCS 575). Because these goals vary by business ownership status and category of procurement, we urge interested businesses to visit the Department of Central Management Services (CMS), Business Enterprise Program (BEP) web site to obtain additional details. To qualify, prime vendors or subcontractors must be certified by the CMS as BEP vendors prior to contract award. Go to (http://www2.illinois.gov/cms/business/sell2/bep/Pages/default.aspx) for complete requirements for BEP certification. For applicable projects, vendors may be asked to submit a utilization plan and letter of intent that meets or exceeds the identified goal. If a vendor cannot meet the goal, documentation and explanation of good faith efforts to meet the specified goal may be required within the utilization plan.

Negotiation: JJC reserves the right to negotiate all elements, which comprise the vendor's proposal to ensure the best possible consideration, be afforded to all concerned. JJC further reserves the right to waive any and all minor irregularities in the proposal, waive any defect, and/or reject any and all proposals, and to seek new proposals when such an action would be deemed in the best interest of JJC.

Award: The successful vendor, as determined by JJC, shall be required to execute a contract for the furnishing of all services and other deliverables required for successful completion of the proposed project. The supplier may not assign, sell, or otherwise transfer its interest in the contract award or any part thereof without written permission from JJC.

Retention of Documentation: All proposal materials and supporting documentation that is submitted in response to this proposal becomes the permanent property of JJC.

Opening of Proposals: Proposals will be opened in a manner that avoids disclosure of the contents to competing vendors. Contents for proposals will remain confidential during the negotiations period. Only the proposal number and the identity of the vendor submitting the proposal response will be made available to the public.

IV. FORMAT FOR RESPONSE

To achieve a uniform review process and obtain the maximum degree of comparability, it is required that the proposal be organized in the format specified.

An original and six (6) copies of the RFP and a complete electronic copy (DVD or flash drive) of the proposal shall be provided. Each hard copy shall be submitted in a binder. The original copy should be so noted and signed.

1. **Title Page**

   Show the RFP subject, the name of the vendor's firm, address, telephone number, name of contact person, and date.

2. **Table of Contents**

   Clearly identify the materials by sections and page number(s).

3. **Letter of Transmittal**

   Limit to one or two pages.

   a. Briefly state the vendor's understanding of the scope of services to be provided and make a commitment to provide the services within the time period.
   b. List the names of the persons who will be authorized to make representations for the vendor, their titles, address, and telephone numbers.

4. **Profile of the Vendor**

   Indicate the number of people in the organization and their level of experience and qualification and the percentage of their time that will be dedicated to this process.

   a. Provide a list of the vendor's top five current and prior two-year clients indicating the type of services the organization has performed for each client.
   b. Submit independently audited financial statements (one copy only). Such information will be considered in strict confidence.
   c. Indicate any third-party firms involved with your program and state their role(s).
   d. Provide contact information (name, phone number, and email address of at least three (3) references for projects of similar size and scope.

5. **Scope Section**

   Clearly describe the scope of services to be provided based upon the information in the scope section. Respond to each item listed.

6. **Responses to Addendum**

7. **Prices Responses**

8. **Invoicing Procedure**

   a. Describe the firm's invoicing procedures.
   b. Include documentation identifying all of the vendor's fees.

9. **Proposed Contract**
   Please submit a draft contract for the services being offered.

10. **Bidder's Certification Statement**

V. EVALUATION

In evaluating the proposals submitted, JJC will apply the "Best Value" standard in selecting the supplier to be awarded a contract for this project. Purchase price is not the only criteria that will be used in the evaluation process. Any award resulting from this RFP will be made to that vendor whose offer conforms to the RFP and it is determined to be the most advantageous, of "best value" to JJC, in the sole judgment of JJC. The selection process will include, but not be limited to, the following considerations:

1. The provider's ability to assist JJC in meeting the overall goals of this RFP.
2. The quality and range of services the firm proposes to provide
3. The extent to which the goods or services meet JJC needs
4. The firm's overall experience, reputation, expertise, stability and financial responsibility
5. The vendor's past relationship with JJC, if any
6. The experience and qualifications of the staff that will be assigned to service JJC's account
7. The ability to provide service in an expedient and efficient manner
8. The quality and range of management reports
9. Vendor's financial terms offered to JJC
10. The training options available
11. Quality of the implementation plan
12. Feedback from references
13. The total long-term cost to JJC to acquire the vendor's goods and services

SCOPE OF WORK

The Scope of Work involves:

- Supplying and installing hardware
- Information gathering and scoping the engagement to create an implementation plan
- Identifying the relationship and configuration of existing hardware to be replaced by the bidder's solution as well as full migration of settings, VPN's, rules, and policies from existing firewall to new solution
- Conducting a firewall rules and objects review to ensure best practices are being followed and increase firewall performance and security
- Onsite implementation (single location in JJC Main Campus) and knowledge transfer based on the implementation plan generated in the information gathering engagement
- Executing four (4) post- implementation Health Checks on a quarterly basis to ensure that the solution is configured and performing optimally
- Ensuring compliance to requirements of the College
- Ensuring no proxy bypass software or techniques should be usable to bypass the firewall

Please refer to Attachment "A" for Firewall Security Requirements.

QUANTITY

There is no guaranteed amount of services intended either expressly or implied, to be purchased or, contracted for by JJC. However the supplier awarded the contract shall furnish all required services to JJC at the stated price, when and if required.

PROPOSED PRICING

The vendor should provide pricing options for a three (3), four (4), or five (5) year contract for all services and materials to be used during the term of the contract. The list of proposed prices should be structured to allow for the calculation of unit cost analyses. The prices included herein are to be firm through each contract term, unless noted otherwise by the vendor.

JOLIET JUNIOR COLLEGE
1901

CERTIFICATION OF CONTRACT/BIDDER

The below signed contractor/bidder hereby certifies that it is not barred from bidding on this or any other contract due to any violation of either Section 33E-3 or 33E-4 of Article 33E, Public Contracts, of the Illinois Criminal Code of 1961, as amended. This certification is required by Public Act 85-1295. This Act relates to interference with public contracting, bid rigging and rotating, kickbacks and bribery.

_____
SIGNATURE OF CONTRACTOR/BIDDER

_____
TITLE

_____
DATE

THIS FORM **MUST** BE RETURNED WITH YOUR BID TO:

Joliet Junior College District #525
Director of Business & Auxiliary Services, A-3100
1215 Houbolt Road
Joliet IL 60431

FireWall Security Requirements

	REQUIREMENTS - Vendors are required to completely fill and Submit this page onwards	Vendor Response Yes or No	Feature is included in base price (Y or N). Indicate if requires extra license and cost	cost ($)
1	Stateful firewalls are required with a 'default deny' policy, with capability to tell if a packet is part of an existing connection. Stateful-inspection traffic classification is performed separately, prior to application identification.			
	Detailed Response from Vendor with any caveats documented:			
2	Identify applications within the HTTP/HTTPS protocol (browserbased applications): The solution must provide an application control feature that must be able to identify the application in use within the HTTP/HTTPS protocol, as well as Mobile Applications, for any TCP Port used. Once identified, applications can be allowed, blocked and limit available bandwidth.			
	Detailed Response from Vendor with any caveats documented:			
3	Identify applications outside of HTTP/HTTPS traffic (desktop applications): The solution must provide an application control feature that must be able to identify the application in use when the traffic is not sent via HTTP or HTTP Secure (HTTPS). Once identified, applications can be allowed, blocked and limit available bandwidth.			
	Detailed Response from Vendor with any caveats documented:			
4	Windows Active Directory Integration: The solution must provide an interface to Active Directory (AD) to pull user IDs and groups that can then be used in firewall rules. Must support multiple independent AD/LDAP domains.			
	Detailed Response from Vendor with any caveats documented:			
5	Integrated Windows Authentication - For all domain based devices, the solution must be able to seamlessly authenticate using Integrated Windows Authentication. Along with the capability to use an authentication service that uses a two-factor authentication scheme.			
	Detailed Response from Vendor with any caveats documented:			
6	Firewall must meet all threat management, policy, and computing functionality listed:			
A.	Ability to safely enable applications, users, and content by classifying all traffic and assigning policies to allow and protect access to relevant applications, including software-as-a-service (SaaS) applications.			
B.	Ability to secure public and private cloud computing environments with increased visibility and control; deploy, enforce and maintain security policies.			
C.	Ability to integrate with a cloud access security broker (CASB) to provide data protection, regardless of location (on-premise, virtualized, private or public cloud (IaaS/PaaS/SaaS) such as Azure or AWS).			
D.	Solution must embrace safe mobile computing by extending the security platform to users and devices no matter where they are located. Deploys consistent policies to local and remote users running on Windows; Apple Mac OS X, macOS and iOS; Linux; and Android platforms.			
E.	Easily integrates firewall policies with 802.1X wireless, proxies, NAC solutions, and any other source of user identity information.			
F.	Application identification and Control - Support for application information feed - The solution must provide an application control function and must allow for the importation and use of information about applications. The feed should include information about how applications are used and provide recommendations to the College regarding actions to take if the application is discovered in use.			
G.	User-developed application signatures: The solution must provide the necessary interface for the College to create, edit and deploy custom application signatures.			
H.	User Identification and Control - Enforce policy on individual users and user groups: The solution must provide a policy to allow, deny and limit available bandwidth. Traffic must be enforceable on individual users or user groups.			
I.	Content Inspection and Control (Data Loss Prevention) - Limits the unauthorized transfer of files and sensitive data, and safely enables non-work-related web surfing. Includes outbound data theft protection: • Credit card numbers • SSN • Custom pattern matching (regex)			

	J.	Ability to turn on audit logging - All network components must provide syslogs to the Security logging solution. Logging must provide sufficient detail to indicate any configuration changes made, when they were made, and who made them.			
	K.	Signature-based IPS: The solution must have a signature-based IPS function where the signatures are created by the manufacturer and automatically applied once they are published. IPS must be able to detect and block network and application layer attacks, protecting at least the following: email services, VoIP protocols, DNS, FTP, Windows services (Microsoft Networking), SNMP, vulnerabilities, protocol misuse, malware communications, tunneling attempts, and covert channel communications.			
	L.	Any IDP solution must be compatible with JJC's Security Incident and Event Management (SIEM) solution (LogRhythm).			
	M.	The solution must provide Advanced Persistent Threat (APT) protection functionality, including features such as network traffic and user behavioral analysis and anomaly detection. Prevent threats by eliminating unwanted applications to reduce your threat footprint and apply targeted security polices to block known vulnerability exploits, viruses, spyware, botnets and unknown malware (APTs).			
	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.			
	O.	Malware detection/protection - Integrated malware protection: The solution must have the ability to detect malware signatures and behaviors running on the network, particularly polymorphic and metamorphic threats.			
	P.	Categorize and Filter URLs: The solution must be able to block, allow and limit available bandwidth specific URL categories and/or reputation of the URL.			
	Q.	Block specific browsers: The application control function must be able to block the use of specific browsers and applications (i.e. Java version).			
	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.			
	S.	Block unauthorized browser plugins: The application control function must be able to block the use of specific browser plugins that are visible in network traffic.			
	T.	Detect Evasive Techniques (e.g. IP packet fragmentation, payload encoding, URL obfuscation, FTP evasion, etc.)			
	U.	DoS protection: The solution must include the mechanism to protect itself from basic Denial of Service (DoS) attacks, such as flooding and resource consumption attacks, and application layer DoS for Web applications including XML DoS protection.			
	V.	Protection against common attacks (Not limited to): • SQL injection • Cross-site scripting • Cookie or forms tampering • JSON payload inspection			
	W.	The solution must have the ability to view current network packet data, and provide accurate reporting on threats within the enterprise. Also has the ability to retain pcap data for historical correlation.			
	X.	Ability to use QoS to prioritize traffic			
	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 off-load to alternate system. The solution must have the ability to detect malware signatures within packets encrypted within SSL, i.e. web server.			
		Detailed Response from Vendor with any caveats documented:			
7		Firewall/Proxy must have ability to perform URL Filtering:			
	A.	Must be able to block URLs based on URL grouped Categories. The blocking must not be in the 'background' i.e. traffic to/from the URL must not be allowed while the lookup is taking place. No traffic to/from the URL must be allowed until the category lookup has been completed and a Permit/Block decision can be made. The URL filtering must work for both HTTPS and HTTP traffic.			
	B.	Must be able to log all the URLs that are passing through the URL filter, both blocked and permitted. The use-case here is User Internet Reports that HR may request. Must be able to provide all the URLs a user has accessed (whether blocked or allowed) over a certain period of time.			
	C.	Must allow the categorization of a URL to be overridden (whitelisted or blacklisted) easily. Must be able to either want to block a URL that is categorized as safe or allow a URL that is incorrectly categorized as unsafe.			

	D.	Must allow URL Categorization bypass for specific Categories (i.e. Cloud Storage) based on Active Directory Groups consisting of User IDs. The default action for URLs categorized as Cloud Storage must be to block, but specific users may have an exception that allows them access to URLs in that category for business purposes.			
	Detailed Response from Vendor with any caveats documented:				
8	VPN: Internal CA and external third party CA must be supported. The solution must act as VPN				
	A.	Site-to-site IPsec VPN: must support remote site recognition that is based on certificates or pre-shared key.			
	B.	SSLVPN: VPNs must support 2 factor authentication and certificates.			
	C.	Solution must support 3DES and AES-256 cryptographic for IKE Phase I and II IKEv2 plus "Suite-B-GCM-128" and "Suite-B-GCM-256" for phase II.			
	D.	Solution must support at least the following Diffie-Hellman Groups: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20.			
	E.	Solution must support data integrity with MD5, SHA1, SHA-256, SHA-384 and AES-XCBC.			
	F.	Solution must support the VPN configuration with a GUI using drag-and-drop object addition to VPN communities.			
	G.	Solution must support L2TP VPNs, including support for iPhone or Android L2TP client.			
	Detailed Response from Vendor with any caveats documented:				
9	Sandboxing				
	A.	The solution must provide the ability to protect against zero-day & unknown malware attacks before static signature protections have been created.			
	B.	Deployment topologies:			
		1) The solution should be part of a complete multi-layered threat prevention architecture.			
		2) The solution should support network-based sandboxing.			
		3) The solution should support host-based sandboxing.			
	Detailed Response from Vendor with any caveats documented:				
10	Administrator logon to network packet capturing equipment should be logged to the SIEM solution. Sufficient detail should be logged to specify the network connections that were viewed, including Source/Destination address pair, capture and view filters, and time of capture.				
	Detailed Response from Vendor with any caveats documented:				
11	Link Aggregation Control Protocol (LACP) and multichassis EtherChannel (MCEC) support of aggregate groups.				
	Detailed Response from Vendor with any caveats documented:				
12	Jumbo Frames support				
	Detailed Response from Vendor with any caveats documented:				
13	Management must utilize a separate routing instance along with memory and CPU.				
	Detailed Response from Vendor with any caveats documented:				
14	20Gbps throughput requirement with Next Gen features enabled in real world traffic.				
	Detailed Response from Vendor with any caveats documented:				
15	Orchestration within Software Defined Networking (SDN) environments for North/South - East/West traffic firewalls. (Integrate with various security tools) Integration with Hyper-V preferred.				
	Detailed Response from Vendor with any caveats documented:				
16	Must be capable of being implemented in multiple virtual environments as well as cloud environments. Azure preferred.				

	Detailed Response from Vendor with any caveats documented:			
17	IP addresses should have geo-location information included in the logs. The firewall should easily allow permit/deny rules based on geo-location of source or destination IPs.			
	Detailed Response from Vendor with any caveats documented:			
18	Should have the ability to dynamically block source or destination IPs based on a Threat Intel feed (e.g. via API calls or some form of importing threat feeds).			
	Detailed Response from Vendor with any caveats documented:			
19	Firewall Role Based Access Control (RBAC) should provide granular access control for Security team to implement a block URL or blacklist an IP address in real time. This capability should be without the need for a policy push as Indicators of Compromise (IOCs) are discovered during an Incident. And, without the Security team needing to have global Admin access to the firewall.			
	Detailed Response from Vendor with any caveats documented:			
20	FQDN based rules.			
	Detailed Response from Vendor with any caveats documented:			
21	Centralized Management: The solution must be manageable via a 'single pane of glass' management console for all features included in the solution. It is preferred that the solution has a single point of administration and notification for:			
	A. Threat prevention.			
	B. Secure site connections.			
	C. Network segmentation.			
	D. User and application awareness.			
	E. End-point security.			
	F. Sandbox applications/isolate malicious behavior.			
	G. Application Control			
	H. URL filtering			
	Detailed Response from Vendor with any caveats documented:			
22	The communication between the management servers and the security appliances must be encrypted and authenticated with PKI Certificates.			
	Detailed Response from Vendor with any caveats documented:			
23	Solution must be Tufin compliant - for continuous compliance and audit readiness.			
	Detailed Response from Vendor with any caveats documented:			
24	SNMP traps/SNMP standard - Management Information Base (MIB) preferred.			
	Detailed Response from Vendor with any caveats documented:			
25	Ability to schedule remote backups with version control and compare: The solution must provide version control (backup) for all modifications made to the system to facilitate compare, rollback.			
	Detailed Response from Vendor with any caveats documented:			
26	Rule verification mechanism: The solution must provide a notification to the administrator when a new rule either masks another rule, duplicates, and overlaps or interferes with an existing rule.			
	Detailed Response from Vendor with any caveats documented:			
27	System availability (active/standby): The solution must provide two Firewalls and allow failover to support 99.999% availability in active/passive or active/standby mode.			

	Detailed Response from Vendor with any caveats documented:			
28	Redundancy in physical appliances: The solution must support redundant hot-swappable power supplies.			
	Detailed Response from Vendor with any caveats documented:			
29	The solution must integrate with SMTP mail services (Microsoft O365). Email Alerts, based on policy or thresholds for: • Hardware • High Availability • Networking • Resources • Log Server Connectivity • Firewall rule triggered • User defined			
	Detailed Response from Vendor with any caveats documented:			
30	Administrator audit: The solution must ensure that all administrative actions be logged to include the action taken, a time stamp, and the source IP address of the endpoint used to make the change and the admin user ID.			
	Detailed Response from Vendor with any caveats documented:			
31	The solution must include, at a minimum, four (4) 10 Gbps fiber (SFP/SFP+) links and eight (8) 1 Gbps Copper interfaces plus any additional interface requirements for the HA cluster.			
	Detailed Response from Vendor with any caveats documented:			
32	IPv6 Support: The solution must be IPv6 ready and the ability for 6-to-4 NAT or 6-to-4 tunnel migration. Solution must support the following IPv6 RFCs: - RFC 1981 Path Maximum Transmission Unit Discovery for IPv6. - RFC 2460 IPv6 Basic specification. - RFC 2464 Transmission of IPv6 Packets over Ethernet Networks. - RFC 3596 DNS Extensions to support IPv6. - RFC 4007 IPv6 Scoped Address Architecture. - RFC 4193 Unique Local IPv6 Unicast Addresses. - RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported. - RFC 4291 IPv6 Addressing Architecture (which replaced RFC1884). - RFC 4443 ICMPv6. - RFC 4861 Neighbor Discovery. - RFC 4862 IPv6 Stateless Address Auto-configuration.			
	Detailed Response from Vendor with any caveats documented:			
33	WIFI Controller based Authentication: The bidders must provide list of all wireless controllers supported to pass authentication information transparently.			
	Detailed Response from Vendor with any caveats documented:			
34	Quality of Service: The solution must shape and prioritize traffic based on rules defined for Quality of Service.			
	Detailed Response from Vendor with any caveats documented:			
35	Centralized advanced Reporting console: The solution must provide Analytics reporting engine that allows the customer to create custom and reports linked to specific queries must be provided. Reports must include and correlate logs from all functions (firewall, IPS, application control, etc.) without requiring for customization or scripting. Sample reports are provided with the bid. The solution must be able to provide:			
	A. summary reports based on application and URL category usage.			
	B. summary reports based on top policies by bandwidth			
	C. summary reports based on top users by browse time by social media.			
	D. summary reports based on top sites visited.			
	E. summary reports based on top blocked sites by request			
	F. summary reports based on top sites by browse time			
	G. summary reports based on top users by bandwidth			
	H. summary reports based on top sites by bandwidth			
	I. summary reports based on top users by browse tim			
	J. summary reports based on Blocked Files by Security Threat			

	K.	ability to perform investigative report for minimum of three months of usage.			
	L.	ability to schedule reports on groups of users and auto send to the specified email addresses.			
	M.	ability to schedule reports on overall user activity, performance, and security threats			
	N.	alerts on custom defined user activities.			
	Detailed Response from Vendor with any caveats documented:				
36	Solution must have the capability to provide incident handling.				
	Detailed Response from Vendor with any caveats documented:				
37	TECHNICAL SPECIFICATIONS of recommended solution- Specify answers to the right.				
	A.	Number of 10-Gb fiber SFP/SFP+ Interfaces			
	B.	Number of 10/100/1000 Interfaces (RJ-45)			
	C.	Number of GbE SFP or 10/100/1000 Interfaces			
	D.	Number of Management Interfaces			
	E.	Size of Internal Storage (GB)			
	F.	Size of Built-in cache (GB)			
	G.	Number of USB Ports			
	H.	Maximum Firewall Throughput (Gbps)			
	I.	Threat Prevention Throughput (GBps)			
	J.	Firewall Throughput (Packets Per Second)			
	K.	Maximum IPS Throughput (Gbps)			
	L.	Maximum Firewall Latency (µs)			
	M.	Maximum Sessions			
	N.	Number of New Sessions per Second			
	O.	Concurrent TCP Sessions			
	P.	Max ARP/MAC entries per broadcast domain			
	Q.	Number of NAT rules capacity			
	R.	Maximum Number of Firewall Policies			
	S.	Number of Virtual Firewalls/Routers			
	T.	Number of IPSec VPN site to site/Max IKE peers			
	U.	Number of QoS policies			
	V.	Physical interfaces supporting QoS			
	W.	Number of User License (Limited to or Unlimited)			
	X.	Number of Power Supply (1 or 1+1)			
	Y.	Lifecycle of Hardware\Software			
	Z.	Hardware/software support Internet feed from multiple ISP's.			
	Detailed Response from Vendor with any caveats documented:				