

REQUEST FOR PROPOSAL

for a

Firewall Security Solution

Issue Date: March 11, 2020

Bid Due On: March 27, 2020 at 12:00 pm

All Inquiries and Bid Submission should be directed to:

Bert Audette
Interim Dean of Information Technology
Eastern Maine Community College
354 Hogan Rd
Bangor, Maine 04401
Phone (207) 974-4682
E-Mail: baudette@EMCC.edu

1.0 GENERAL INFORMATION

1.1 Purpose: Eastern Maine Community College is seeking bids to purchase a firewall security solution to be used at the campus located at 354 Hogan Rd, Bangor, Maine.

This Request for Proposal (RFP) states the instructions for submitting bids, the procedure and criteria by which a vendor may be selected and the contractual terms by which the College intends to govern the relationship between it and the selected vendor.

1.2 Definition of Parties: Eastern Maine Community College (EMCC) will hereinafter be referred to as the "College". Respondents to the RFP shall be referred to as "Bidders". The Bidder to whom the contract is awarded shall be referred to as the "Contractor".

1.3 Scope: The selected Bidder will supply the proposed firewall security solution and all necessary components to EMCC as outlined in this Request for Proposal. Detailed project requirements are listed in section three.

1.4 Evaluation: Award will be made to the low Bidder(s) whose products or solutions conform best to the RFP and College requirements, provided that all other requirements are satisfactorily met. Consideration will also be given to the Bidder's qualifications, references and capabilities to provide the specified equipment and service. During the evaluation process, EMCC reserves the right where it may serve the College's best interest to request additional information or clarification from proposers, or to allow corrections of errors or omissions.

1.5 Communication with the College: It is the responsibility of the Bidder to inquire about any requirement of the RFP that is not understood. Responses to inquiries, if they change or clarify the RFP in a substantial manner, will be forwarded by addenda to all parties that have received a copy of the RFP. The College will not be bound by oral responses to inquiries or written responses other than addenda.

1.6 Award: The College reserves the right to conduct any tests it may deem advisable and to make all evaluations. The College reserves the right to reject any or all bids, in whole or in part and is not necessarily bound to accept the lowest bid if that bid is contrary to the best interest of the College. The College reserves the right to waive minor irregularities. Scholarships, donations or gifts to the College will not be considered in the evaluation of bids. A bid may be rejected if it is in any way incomplete or irregular. When there are tie bids, there shall be a preference for "in-state bidders". When the bids are either both in-state or both out-of-state, the award will be made to the bid that arrives first in Eastern Maine Community College's Information Technology Office.

1.7 Award Protest: Bidders may appeal the award decision by submitting written protest to Eastern Maine Community College's Director of Finance within five (5) business days of the award notice, with a copy to the successful bidder. The protest must contain a statement of the basis for the challenge.

1.8 Costs of Preparation: Bidder assumes all costs of preparation of the bid and any presentations necessary to the bidding process.

1.9 Debarment: Submission of a signed bid in response to this solicitation is certification that your firm (or any subcontractor) is not currently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from participation in this transaction by any State or Federal department or agency. Submission is also agreement that the College will be notified of any change in this status.

1.10 Bid Understanding: By submitting a bid, the Bidder agrees and assures that the specifications are adequate and the Bidder accept the requirements, terms and conditions herein. Any exceptions must be noted in your response.

1.11 Specification Protest Process and Remedies: If a bidder feels that the specifications are written in a way that limits competition, a specification protest may be sent to Eastern Maine Community College's Director of Finance. Protests will be responded to within five (5) business days of receipt. Determination of protest validity is at the sole discretion of the College. The due date of the bid may be changed if necessary to allow consideration of the protest and issuance of writing as soon as identified, but no less than five (5) business days prior to the bid opening date and time. No protest against the award due to

the specifications shall be considered after this deadline. Protest shall include the reason for the protest and any proposed changes to the specifications. Protest should be delivered to the Director of Finance's office in sealed envelopes, clearly marked as: "Firewall Security Solution Bid".

1.12 Bid Validity: Unless specified otherwise, all bids shall be valid for one (1) year from the due date of the bid.

1.13 Errors: Bids may be withdrawn or amended by Bidders at any time prior to the bid opening. After the bid opening, bids may not be amended. If a significant mistake has been made by an apparent low Bidder, the Bidder will be given the option of selling at the price given or withdrawing the bid. If an extension error has been made, the unit price will prevail.

1.14 Bid Envelope: If a special envelope is not furnished or if return in the special envelope is not possible, the signed bid can be returned in an envelope or package, sealed and identified as follows:

From	Due Date	Time
------	----------	------

1.15 Submission: A signed original plus one (1) copy of the bid may be sent to the Information Technology Office at Eastern Maine Community College, 354 Hogan Rd, Bangor, Maine 04401, in a sealed envelope by 12:00 p.m. local time by March 27th, 2020. Envelope should be marked "Firewall Security Solution RFP". Bids can also be emailed to baudette@emcc.edu with "Firewall Security Solution RFP" in the subject line. Bidders are strongly encouraged to submit bids in advance of the due date to avoid the possibility of missing the deadline due to unforeseen circumstances. Bidders assume the risk of the methods of dispatch chosen. The College assumes no responsibility for delays caused by any package or mail delivery service. A postmark on or before the due date WILL NOT substitute for receipt of bid. Bids must be dated and time stamped by the College on time to be considered. Bids received after the due date and time will not be considered. Additional time will not be granted to any single bidder, however, additional time may be granted to all vendors when the College determines that circumstances require it. **Faxed bids will not be accepted.**

1.16 Tax Exempt: The College is exempt from the payment of Federal Excise Taxes on articles not for resale and for the Federal Transportation Tax on all shipments. The Contractor and subcontractor shall quote and shall be reimbursed less these taxes. Upon application, exemption certificates will be furnished when required. The College is exempt from the payment of Maine State Sales and Uses taxes.

2.0 CONTRACT TERMS AND CONDITIONS

2.1 Contract Documents: If a separate contract is not written, the contract entered into by the parties shall consist of the Request for Bids, the signed bid submitted by the Contractor, the specifications including all modifications thereof, and a purchase order or letter of agreement requiring signatures of the College and the Contractor, all of which shall be referred to collectively as the Contract Documents.

2.2 Contract Validity: In the event one or more clauses of the contract are declared invalid, void, unenforceable or illegal, that shall not affect the validity of the remaining portions of the contract.

2.3 Contract Administration: Bert Audette, Dean of Information Technology, shall be the College's authorized representative in all matters pertaining to the administration of any contract(s) regarding the Firewall Security Solution.

2.4 Litigation: This Contract and the rights and obligations of the parties hereunder shall be governed by and construed in accordance with the laws of the State of Maine. The Contractor agrees that any litigation, action or proceeding arising out of the Contract shall be instituted in a state court located in the State of Maine.

2.5 Assignment: Neither party of the contract shall assign the contract without the prior written consent of the other, nor shall the contractor assign any money due or to become due without the prior written consent of the College.

2.6 Equal Opportunity: In the execution of the contract, the Contractor and all subcontractors agree, consistent with college policy, not to discriminate on the grounds of race, color, religion, sex, sexual orientation, transgender status or gender expression, national origin or citizenship status, age disability or veteran's status and to provide reasonable accommodations to qualified individuals with disabilities upon request. The College encourages the employment of individuals with disabilities.

2.7 Sexual Harassment: The College is committed to providing a positive environment for all students and staff. Sexual harassment, whether intentional or not undermines the quality of the educational and working climate. The College thus has a legal and ethical responsibility to ensure that all students and employees can learn and work in an environment free of sexual harassment. Consistent with the state and federal law, this right to freedom from sexual harassment was defined as College policy by the Board of Trustees. Failure to comply with this policy could result in termination of this contract without advance notice. Further information regarding this policy is available from Jody MacDonald, Human Resources Department, Eastern Maine Community College, 354 Hogan Rd, Bangor, Me 04401, (207) 974-4633.

2.8 Smoking Policy: Eastern Maine Community College must comply with the "Workplace Smoking Act of 1985" and MRSA title 22, 1541 ET seq, "Smoking Prohibited in Public Places." In compliance with this law, Eastern Maine Community College has prohibited smoking on campus. This rule must also apply to all contractors and workers that are on campus. The Contractor shall be responsible for the implementation and enforcement of this requirement.

2.9 Parking Regulations and Use of Walkways: Unregistered vehicles on the college campus are subject to a parking violation ticket and/or towing off campus. Contractors are advised that parking regulations are strictly enforced by the City of Bangor police. Towing will be at the Contractor's expense.

2.10 Payments: Payment will be upon final acceptance of product and submittal of an invoice to the College, by the Contractor on a net 30 basis unless discount terms are offered.

NOTICE TO VENDORS AND BIDDERS:

STANDARD TERMS AND CONDITIONS APPLICABLE TO ALL MCCS CONTRACTS

The following standard contracting terms and conditions are incorporated and shall become a part of any final contract that will be awarded by any college or other operating unit of the Maine Community College System (collectively "MCCS"). These terms and conditions derive from the public nature and limited resources of the MCCS. MCCS DOES NOT AGREE TO:

1. Provide any defense, hold harmless or indemnity;
2. Waive any statutory or constitutional immunity;
3. Apply the law of a state other than Maine;
4. Procure types or amounts of insurance beyond those MCCS already maintains or waive any rights of subrogation;
5. Add any entity as an additional insured to MCCS policies of insurance;
6. Pay attorneys' fees, costs, expenses or liquidated damages;
7. Promise confidentiality in a manner contrary to Maine's Freedom of Access Act;
8. Permit an entity to change unilaterally any term or condition once the contract is signed; and
9. Automatic renewals for term(s) greater than month-to-month.

By submitting a response to a Request for Proposal, bid or other offer to do business with MCCS, YOUR ENTITY UNDERSTANDS AND AGREES THAT:

1. The above standard terms and conditions are thereby incorporated into any agreement entered into between MCCS and your entity; that such terms and condition shall control in the event of any conflict with such agreement; and that your entity will not propose or demand any contrary terms;
2. The above standard terms and conditions will govern the interpretation of such agreement notwithstanding the expression of any other term and/or condition to the contrary;
3. Your entity will not propose to any college or other operating unit of the MCCS any contractual documents of any kind that are not in at least 11-point font and completely contained in one Word or PDF document, and that any references to terms and conditions, privacy policies or any other conditions referenced outside of the contract will not apply; and
4. Your entity will identify at the time of submission which, if any, portion or your submitted materials are entitled to "trade secret" exemption from disclosure under Maine's Freedom of Access Act; that failure to so identify will authorize MCCS to conclude that no portions are so exempt; and that your entity will defend, indemnify and hold harmless MCCS in any and all legal actions that seek to compel MCCS to disclose under Maine's Freedom of Access Act some or all of your submitted materials and/or contract, if any, executed between MCCS and your entity.

3.0 SCOPE OF WORK

3.1 Background: The current firewall solution at EMCC is end of life and does not meet current and anticipated demand. Cloud based applications (Office 365, etc.), modern technologies (web video streaming, video meetings, etc.), and ever-increasing security challenges are straining the capabilities of our current solution. EMCC has outdated firewall appliances as well as newer firewall appliances that are not meeting growth / demand (speed) requirements. EMCC is looking for a solution that will address these and future challenges.

The current firewall security infrastructure at EMCC consists of a variety of an active-active pair of FortiGate 800C hardware appliances, combined with a FortiAnalyzer 300D. These devices are located at the main campus in Bangor, Maine. This current solution provides perimeter security, primarily, and includes the following services through April 30, 2020: hardware maintenance / replacement, firmware and general updates, enhanced support, advanced malware protection, next generation firewall, web filtering, and anti-spam. The current firewall security infrastructure at EMCC also includes a single FortiGate 100D appliance and a single FortiGate 60E appliance, each located at two different external properties in the state (Dover, Maine and Millinocket, Maine.) Each of these smaller appliances has the same set of services as those listed above for the main site. The remote sites are currently stand-alone with connections to the Internet through different Internet service providers, but are not currently connected to the main site in any way. Client VPN services are also not currently implemented.

3.2 Scope: EMCC is looking to replace the current perimeter security solution at the main campus with a new solution that is capable of providing perimeter security and also securing additionally defined internal zones with traffic crossing between a variety of internal networks, existing and planned. The solution should allow for additional security zones (or similar functionality) to be added at a later time. It is expected that the solution will provide common next generation firewall security features such as application awareness, advanced malware protection, URL filtering, security intelligence, intrusion detection, and intrusion prevention. The solution must have high availability and fault tolerance. EMCC is also interested in upgrading the two remote properties to a more capable solution. EMCC prefers a single firewall vendor security solution for the main campus and the remote properties. The solution for the remote properties must be capable of establishing site to site VPN connectivity with the main campus solution. The main campus solution must be capable of providing client VPN connectivity. EMCC wishes to receive bids that provide the following elements:

- 1) Hardware, software and services which meets the stated requirements to replace the current firewall appliance and logging/reporting hardware at the main campus solution.
- 2) Hardware, software and services which meets the stated requirements to replace the current firewall appliances at the two remote properties.

- 3) Professional services required to manage the project and complete the basic installation and configuration of the solution at all three properties, as well as provide basic training for EMCC IT staff and access to OEM vendor training materials.

3.3 Bidder Minimum Qualifications: Bidder and all key personnel assigned to the project shall be regularly and continuously engaged in the business of providing next generation firewall and security design, implementation, and support for at least three years. Bidder shall be authorized to sell and support the products and related services. Bidder must provide proof of certification that the bidder is authorized to supply product and perform services as specified under this RFP. Bidder must have architects and engineers certified at the highest level for the products proposed.

3.4 Requirements:

3.4.1 General Requirements:

1. Bidder's solution shall include product selection, design, implementation and migration to a new firewall security solution.
2. The solution will include five (5) year maintenance, including 24x7 support and service licensing for all components of the solution. Maintenance and support should provide for next business day parts replacement.
3. Bidder shall provide industry best practices for installation and management of production services and any specifics related to their proposed solution.
4. The solution architecture shall be designed to accommodate future growth without requiring investment in expensive network architecture redesign.

3.4.2 Solution Requirements:

1. Bidder's solution for all hardware firewall appliances at all locations will provide at least eight (8) 1G ethernet interfaces on each appliance. In addition, the solution for the main campus firewall appliance will also provide at least eight (8) 10G SFP+ interfaces with four (4) 10G LR optical transceivers provided per appliance.
2. Bidder's solution shall offer minimum 10G bi-directional throughput with all security features enabled for the main campus site and minimum 1G bi-directional throughput with all security features enabled for the two remote sites.
3. Security features such as SSL decryption, application awareness, application visibility, advance malware protection, URL filtering, security intelligence, intrusion detection, intrusion prevention, quality of service, data loss prevention, address translation, and centralized administration will be fully implemented.

4. The solution shall allow for additional security zones and or instance capability.
5. The solution shall support multiple active directory domains as well as RADIUS and user aware authentication.
6. The solution shall be compatible with other security solutions or security monitoring solutions using common / industry standard protocols.
7. The solution shall have active / passive high availability and fault tolerance for the main campus site, including redundant hot-swappable power supplies. The solution does not require high availability for the remote sites, but should include redundant power supplies.
8. The solution shall have capability to store at least 90 days of logs, either natively or via remote logging. Ideal solutions will integrate well with a SIEM infrastructure.
9. Preference will be provided to physical appliance-based solutions. Any virtual server-based software solutions must be compatible with the Microsoft Hyper-V hypervisor.

3.4.3 Product Requirements:

1. All products shall be new products and shall be general release products.
2. All required performance specifications shall be from published public sources from production environments with all required features and applications simultaneously active.
3. To reduce administrative costs, overhead, and human error, the solution shall simplify management by having a single interface for configuring policy for all running features, including application, user, and content ID's. Additionally, software interfaces will be functionally similar across all hardware products at each physical location.
4. Product must be able to correctly classify all traffic through to application identification, determine source/destination and affect change to that traffic, as necessary. Product must also be able to handle unknown traffic by policy
5. In addition to being an edge security device, product must function as a next generation firewall by providing the following services and capabilities: Intrusion Prevention / Detection, URL filtering, malware / file integrity scanning, sandboxing, and threat intelligence feeds.
6. Product shall support Authentication, Authorization, and Accounting (AAA) protocols and support certificate-based authentication as well as integrate with Microsoft Active Directory/ Lightweight Directory Access Protocol (AD/LDAP) and Remote Authentication Dial-In User Service (RADIUS) to associate traffic to users for multiple domains, authenticate VPN client users, etc.
7. Product must have the ability to insure optimal performance for delay and jitter-sensitive applications, such as VOIP, high definition video, and real-time sensitive applications by minimizing delay and jitter in its design and utilizing quality of service (QoS) traffic identification techniques.

8. The product shall be able to use all identification methods in a single policy, to accept or deny traffic, packet shape, apply QoS, and policy route traffic.
9. The product shall provide support for standard Voice over IP technologies, including Session Border Controllers, H.323 and H.225 compliance, etc.
10. To maximize the granularity of security policies, the product shall allow policy creation and enforcement based on any combination of time-of-day, security zone, ingress and egress hardware port, ingress and egress software port, application identification, device identification, user identification, and content identification.
11. To prevent evasive users and applications from bypassing security functions, the product shall be port agnostic and analyze all data on all ports all the time for application identification. All product functions for Intrusion Prevention System (IPS), Threat Prevention, and Anti-Virus, shall not require specific software port and protocol combinations for detection, mitigation, or enforcement.
12. The product should include a zero-day threat prevention system that validates executable files passing through the firewall, and provides automatic cloud-based behavioral threat analysis of unknown executables, and automatic signature creation to block delivery for executable files that are deemed dangerous by the analysis system. The product must also recognize and prevent SQL injection and denial of service attacks.
13. The product shall decrypt outbound and inbound SSL and TLS traffic for inspection (and also identify and allow high security (ie., banking) solutions that do not work with SSL/TLS decryption to pass without decryption.)
14. Have the ability to handle at least 10 simultaneous site-to-site VPN and 50 simultaneous client-to-site VPN sessions. Site-to-site VPN technologies supported should include IPSec, L2TP and SSL/TLS. VPN capability must support site-to-site VPN tunnels with remote hardware from other manufacturers and support virtual firewalls in major cloud service providers such as Microsoft Azure and Amazon AWS.
15. The product must be both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (Ipv6) compliant.
16. The product shall provide edge security to separate Local Area Networks from public Internet, provide complete network address translation (NAT) functionality, and handle multicast traffic by rule.
17. The product shall be able to send alerts for correlation to alerting and logging servers using industry standard protocols (SNMP, syslog, etc.)

3.4.4 Professional Services Requirements:

1. All implementation work at the main campus shall be completed as soon as possible proposed target install date is prior to April 30, 2020. Bidder should identify whether this target date is possible.

2. Bidder and EMCC IT staff shall hold meetings weekly and daily as necessary to complete the project on time.
3. Bidder shall provide pre-identified project resources (experts) for migration.
4. Bidder shall provide basic project management services for the implementation. Project managers shall have experience with firewall and security solution implementations.
5. Bidder shall seek to minimize impact to EMCC normal business operations. If network downtime is inevitable to deliver the proposed solution, a mutually agreeable time will be determined with at least 3 business days prior notice required by EMCC.
6. It is the Bidder's responsibility to install, configure and integrate the complete solution as per EMCC's business schedule.
7. All costs related to the installation of the equipment (including all necessary materials, labor, etc.) will be the responsibility of the Bidder.
8. Bidder shall provide onsite installation and configuration support.
9. Bidder shall work closely with EMCC IT staff regarding the configuration to ensure EMCC business needs are met and will make changes at times determined by EMCC IT staff.
10. Bidder shall provide EMCC IT staff with the following support and training information:
 - a. Registration with OEM for support using EMCC IT provided contact information.
 - b. Detailed contact information for OEM support resources, including telephone numbers, web sites, support login information, etc.
 - c. Training for EMCC IT staff in the proper use, operation, maintenance and administration of the solution, including firmware / software upgrade procedures.

4.0 VENDOR BACKGROUND

1. List your company's legal name, address and telephone number.
2. How long has your company been in business?
3. Indicate whether your company is the manufacturer or the distributor of the proposed equipment. If you are a distributor, describe the terms of your agreement with the manufacturer and the manufacturer's level of support.
4. Provide contact information for three references where your company has provided similarly sized and scoped systems and services to. Provide detail regarding the size and scope of the system or services provided. It is preferred that bidders notify their references that Eastern Maine Community College may be verifying references immediately following closing of this bid.

5.0 RFP SCHEDULE

RFP Schedule	Date
RFP issued	3/11/2020
Deadline for Questions	3/20/2020 by 12:00pm
Response to Questions	3/23/2020 by 4:00pm
RFP due	3/27/2020 by 12:00 pm
Winner selected and notified	4/1/2020

5.1 Questions will not be accepted by telephone. Questions should be submitted by email to baudette@EMCC.edu. EMCC will make every effort to answer questions submitted by bidders to the best of our ability by the due date. We strongly encourage bidders to submit questions as early in the RFP process as possible.

5.2 Bidders may wish to provide product presentations prior to RFP submission. This is encouraged.

5.3 Depending on the responses to the RFP, EMCC will make every effort to select and notify the winning bidder by the end of business April 1, 2020. The college reserves the right to change the RFP schedule allowing the time necessary to make the most appropriate selection for the college.