

Invitation for Bids: Firewall Purchase and Implementation

Date of Issuance: September 3, 2015

Issued by: Department of Innovation and Technology, City of Burlington

Due Date for Questions: September 14, 2015 by 5PM
Reponses will be available September 18 by 5PM

Due Date for Bids: September 25, 2015 by 5PM

Contact: Beth Anderson
Chief Innovation Officer
City of Burlington
(802) 865-5357
banderson@burlingtonvt.gov

Overview

The City of Burlington is accepting bids for supply, installation and configuration of a firewall. The solution should be a next generation security device that will sit at the edge of the City's network.

Current Environment

Network: Connectivity provided by Burlington Telecom (1Gb), 1 Firewall, Barracuda web filter (would consider replacing). Connectivity is centrally served to 17+ locations across Burlington from a private router behind the firewall.

Servers & Applications: VMWare virtualization platform: ~25 virtual machines. Barracuda backup appliance. Most applications are maintained in house. Email moved to the cloud in 2015. Financial management system moving to a hosted environment.

End Users: Approximately 550 staff computers are supported.

Specifications

Vendors are asked to provide a bid that includes purchase of a firewall as well as installation and configuration of the firewall, including migrating policies from the existing firewall.

The City is interested in receiving bids that consider different types of firewalls, including stateful inspection firewalls and application firewalls. Vendors are welcome to submit more than one proposal if interested in proposing more than one firewall type.

Device specifications are:

#	Specification	Required?
1	The solution must be a Next Generation Firewall hardware appliance.	Yes
2	The solution must perform packet filtering and network address translation (NAT).	Yes
3	The solution must provide multi-layered threat protection.	Yes
4	The solution must provide full stack visibility and application identification, with the ability to identify, allow, block or limit usage of applications beyond ports and protocols.	Yes
5	The solution must be capable of identifying and controlling both UDP and TCP based applications.	Yes
6	The solution must provide at minimum:	Yes
6a	<ul style="list-style-type: none"> 4GBPS firewall throughput 	Yes
6b	<ul style="list-style-type: none"> 2 Gbps integrated threat prevention throughput with no latency or performance impact with all protection capabilities enabled 	Yes
6c	<ul style="list-style-type: none"> 500,000 concurrent connections 	Yes
6d	<ul style="list-style-type: none"> 40,000 new sessions / second 	Yes
6e	<ul style="list-style-type: none"> 2,000 policies 	Yes
6f	<ul style="list-style-type: none"> 8 10/100/1000 Mbps copper interfaces 	Yes
7	The solution must provide integrated Intrusion Prevention System (IPS) capabilities.	Yes
8	The solution must provide protection from known and advanced threats.	Yes
9	The solution must provide protection from targeted and persistent malware attacks.	Yes
10	The solution must allow administrators to create Firewall/IPS policy by application, active directory users/groups and content.	Yes
11	The solution must provide antivirus protection. Scanning should be performed in a way to minimize performance impacts.	Yes
12	The solution must be able to perform regular, automated updates of signature, content matching and/or classification data (i.e. IPS, URL Filtering, AV signatures, etc.), through a subscription based or similar service.	Yes
13	The solution should include zero day threat prevention that validates executable files and provides threat analysis of unknown executables and signature creation for those determined to be dangerous.	No
14	The solution must provide granular access controls within web applications to control access within the application where possible.	Yes
15	The solution must be able to apply QOS/bandwidth management/traffic shaping at the application level.	Yes
16	The solution should provide URL Filtering Capabilities	Yes
17	The solution should support policy- and category-based web filtering.	Yes
18	The solution should allow for white- and black-listing of IPs and URLs.	Yes
19	The solution should perform all of the scanning and identification processes in a single pass.	Yes

20	The solution must have the ability to integrate with LDAP and Active Directory for user-based authentication and policy enforcement. Must support multiple AD domains.	Yes
21	The solution must have integrated troubleshooting tools and utilities. (i.e. packet capture, traceroute, ping, etc.)	Yes
22	The solution must provide IPv4 and IPv6 support.	Yes
23	The solution should offer VPN functionality (SSL and IPSec) for at least 500 users	No
24	The solution should include mobile device management and protection capabilities.	No
25	The solution must support custom threat prevention and application signatures.	Yes
A1	The solution should contain role/discretionary based administration functions to provide for separation of duties for administrative access and control.	Yes
A2	The solution should offer a centralized management module capable of managing multiple sites if required in the future.	No
A3	The solution should provide a configuration audit capability.	No
R1	The solution must provide basic statistics about firewall health, traffic and performance.	Yes
R2	The solution must provide a graphical user interface that provides a dynamic overview of network activity (e.g. applications, threats, URLs and users), including current activity as well as trends over time.	Yes
R3	The solution must provide the ability to map traffic to users.	Yes
R4	The solution must be able to generate automatic mail alerts, to multiple recipients.	Yes
R5	The solution must include logging capabilities, including off the box monitoring and logging.	Yes
R6	The solution should provide compliance reporting (e.g. PCI).	No
S1	The solution proposed must include 7X24X365 technical support from the device provider.	Yes
S2	The solution must provide software upgrades with no downtime.	Yes
S3	The solution must allow for upgrades to include future new information and functionality to address new threats and capabilities.	Yes
S4	The solution must provide SSL or PKI encrypted communication between firewall components.	Yes
S5	The solution must provide a minimum three year warranty.	Yes
S6	The solution must include next-day delivery of a replacement firewall in the event of a failure.	Yes

These specifications are included in the attached spreadsheet. Each vendor must complete the spreadsheet and identify their ability to meet each specification, and provide their responses as part of their bid. Exceptions to requirements should be clearly identified and explained.

In addition, bids must include:

- Cost for complete procurement, installation and configuration of the firewall. It is expected that the vendor will maintain necessary resources onsite during critical stages of the project.
 - Configuration should include working with the City IT team to understand policies and requirements to be implemented.
 - The firewall should be delivered, installed, tested and in production within 45 days of signing of the contract. The City will have the right to deduct 1% per day from the total project cost for failure to complete, up to 15% of total project cost.
- The option to purchase a second device to be kept for active standby in case of failure of the primary firewall. Depending on overall costs, the City may decide to not purchase a second device.
- The provision of appropriate training for two (2) City staff members. Training should include proper configuration, operation and maintenance of the equipment. The proposal should include an estimate of the training time that will be required.
- The option for ongoing support by the vendor, and a proposed cost for that support. Support should be available within a four hour time frame.
 - The City intends to move to a managed services model, which may ultimately include management of the firewall. However, the City requires that the vendor be available to provide on-going support as needed.
 - If a vendor is capable of providing ongoing managed security services, through it or a partner, information about that service may be provided as the City is interested to explore service options. Security services will not be awarded as part of this contract.

Submission Requirements

Responses should be submitted in hard copy (1 copy) or by email in PDF format. The selected vendor will be required to have a signed nondisclosure agreement in place prior to beginning any work.

Responses should be submitted by 5PM EDT on Friday September 25, 2015. Responses should include:

- An executive summary explaining the recommended solution;
- A detailed description of the proposed firewall, and any other hardware recommended, including any data sheets provided by the manufacturer;
- A completed specifications spreadsheet, explaining the proposed firewall's compliance with the required specifications;
- A detailed description of the work that will be performed to implement the firewall;
- A detailed work plan with deliverables and deadlines;
- A cost proposal detailing the cost for each hardware component, the individual services to be provided, ongoing licensing or support costs, and any travel costs. Costs should be provided for 1, 3 and 5 year licensing and support options;
- An overview of the vendor's organization and its qualifications;
- The name of the individual(s) who would be responsible for implementation, if chosen, and a summary of their experience;
- An explanation of any partnering arrangements that have been made to respond to this request;
- 3 references for similar projects.

The proposer must have been in business for at least five years performing work related to the provisioning, installation and configuration of firewalls and IT equipment. In addition, the proposer should have at least five full time IT professionals.

Bidders must comply with all provisions of state law, and the accepted bidder will have to comply with the city's livable wage and union deterrence ordinances, copies of which are available on the city's website (or may be supplied on request).

The City of Burlington does not tolerate unlawful harassment or discrimination on the basis of political or religious affiliation, race, color, national origin, place of birth, ancestry, age, sex, sexual orientation, gender identity, marital status, veteran status, disability, HIV positive status or genetic information.

The City is also committed to providing proper access to services, facilities, and employment opportunities.

Bids should be sent in a sealed envelope to the contact listed above.

Questions

Questions may be submitted by email by the deadline identified above. Vendors will be required to sign and return a non-disclosure agreement prior to receiving additional information from the City. Any revisions, addendums and answers to questions that are not deemed to be a security risk for the City if made public and that are received by the due date for questions will be sent to all vendors who directly received this proposal via email. Similarly, where appropriate revisions will be posted on the City's RFP web page <http://burlingtonvt.gov/RFP/>.

Bid Evaluation

Responses will be reviewed by department staff based upon the information provided in the proposal. Additional information and/or a product demo may be requested prior to final selection. The city intends to accept the bid it determines to be in the best interests of the city, based on the overall proposal, not exclusively on cost or any other specific factor. The city reserves the right to amend, modify, reject, negotiate, or accept any bid in whole or in part at its sole discretion. It is anticipated that a decision will be made within 45 days of the due date.

Indemnification

The Vendor will act in an independent capacity and not as officers or employees of the Municipality. The Vendor shall indemnify, defend and hold harmless the Municipality and its officers and employees from liability and any claims, suits, expenses, losses, judgments, and damages arising as a result of the Vendor's acts and/or omissions in the performance of this contract.

The Municipality is responsible for its own actions. The Vendor is not obligated to indemnify the Municipality or its officers, agents and employees for any liability of the Municipality, its officers, agents and employees attributable to its, or their own, negligent acts, errors or omissions.

Limitations of Liability

The City of Burlington assumes no responsibility and liability for costs incurred by parties responding to this invitation to bid or responding to any further requests for interviews, additional data, etc, prior to the issuance of the contract.

Rejection of Proposals

The City of Burlington reserves the right to reject any or all responses, to negotiate with one or more parties, or to award the contract in the City's best interests. The City reserves the right to re-advertise for additional responses and to extend the deadline for submission of responses.

Ownership of Documents

Proposals, plans, specifications, basis of designs, electronic data and reports prepared under any agreement with the selected contractor and the City shall become the property of the City. Records shall be furnished to the City by the contractor upon request at any time, however contractor may retain copies of the original documents.