Request for Quotation

For the Supply, Installation, and Configuration of Firewall Upgrade Project

PASEGURUHAN NG MGA NAGLILINGKOD SA PAMAHALAAN
(GOVERNMENT SERVICE INSURANCE SYSTEM)
Financial Center, Pasay City

GSIS

A. Confidentiality Statement

This document, and any attachments thereto, regardless of form or medium, is intended only for use by the addressee(s) and may contain legally privileged and/or confidential, copyrighted, trademarked, patented or otherwise restricted information viewable by the intended recipient only. If you are not the intended recipient of this document (or the person responsible for delivering this document to the intended recipient), you are hereby notified that any dissemination, distribution, printing or copying of this document, and any attachment thereto, is strictly prohibited and violation of this condition may infringe upon copyright, trademark, patent, or other laws protecting proprietary and, or, intellectual property. In no event shall this document be delivered to anyone other than the intended recipient or original sender and violation may be considered a breach of law fully punishable by various domestic and international courts. If you have received this document in error, please respond to the originator of this message or email him/her at the address below and permanently delete and/or shred the original and any copies and any electronic form this document, and any attachments thereto and do not disseminate further.

B. Submission Details

Submission Deadlines

All submissions for responding to this request must be submitted on paper and delivered to our office, as stated below, no later than:

Friday, July 3, 2015
No later than 5:00pm EDT

Submission Delivery Address

The delivery address to be used for all submissions is:

ALEXANDER A.S EA
Information Security Office
6F GSIS Head Office
Financial Center, Pasay City
1308
Voice: (632)-859-0311
Email: aasea@gsis.gov.ph

Submission Questions and Clarifications

You may contact the following person if you have any questions or require clarification on any topics covered in this Request For Proposal:

ALEXANDER A.S EA
Information Security Office
6F GSIS Head Office
Financial Center, Pasay City
1308
Voice: (632)-859-0311
Email: aasea@gsis.gov.ph

Electronic Submissions

Electronic submissions in response to this Request for Proposal will be accepted as long as they meet the following criteria:

Sent via email to: aasea@gsis.gov.ph

Document standards:
Must be in PDF format
Containing the company seal or the proponent

C. Terms of Reference

1. Project Scope

The winning bidder is responsible for the following:

1. Supply, installation and configuration of network firewall systems
2. Software and hardware warranty and maintenance from the date of acceptance.
3. Capability building/training
4. Project documentation
5. Technical Support off-site and on-site.

2. Minimum Technical Requirements

2.1. Lot 1 – Enterprise Network Firewall

2.1.1. General Requirements

2.1.1.1. High availability – must support active-active and active-standby

2.1.1.2. Must support an optical and copper port

2.1.1.3. Must have central management console

2.1.1.4. Highly reliable platform with hot-swappable redundant power supply, hard disk drives and fans.

2.1.1.5. Able to remotely diagnose, start, stop and manage the appliance and capable of remotely installing an OS image from an ISO file via web interface

2.1.1.6. The appliance must be managed locally with its integrated security management of via unified central management

2.1.1.7. Must be similar to our existing production network firewall and existing warranties must be applied to the proposed solution.

2.1.1.8. Multi-Core appliance-based real-time and embedded based firewall system.

2.1.1.9. Bidder must be certified and trained to offer front line technical support directly to end-users and must maintain a back line direct support relationship with manufacturer.

2.1.1.10. The prospective bidder should be able to escalate reported problems directly to manufacturer and should be certified and trained to offer front line technical support directly to end-users. Maintains a back line direct support relationship with manufacturer

2.1.1.11. The prospective bidder must be an Appliance Certified Expert support provider and is trained to offer and deliver on-site replacement service for the proposed product

2.1.1.12. The prospective bidder should be an Authorized Partner of the proposed product. Bidder must submit a current and valid certification from the manufacturer.

2.1.1.13. Must be in leader quadrant of Gartner Magic Quadrant for Enterprise Network Firewall

2.1.1.14. Management **Software Specification:**

2.1.1.14.1. Must have a dedicated application client console for security policy configurations of Firewall, application controls, IPS, IPSec VPN, etc. in order to prevent Cross Site Request Forgery (CSRF) attacks

2.1.1.14.2. Must have dedicated application client console for reviewing traffic and audit logs. Logs searching must be intuitive or Google-like

2.1.1.14.3. Must have dedicated security policy tabs for Firewall, application control, IPS, etc. for flexible definitions and focused creation of rules.

2.1.1.14.4. Must have policy based NAT rules for granular creation of source, destination and port translations

2.1.1.14.5. Must have profile based IPS policy assignments. IPS Signatures must have a rating for severity, confidence level and performance impact and auto/scheduled update feature

2.1.1.14.6. Must be able to set application control policy actions accept, block, bandwidth limit and time based

2.1.1.14.7. Must have user awareness interactions (ask and inform) integrated on application control policy to educate them on security risks and company policies

2.1.1.14.8. Must have a multi logical management capability

2.1.1.14.9. Must be able to create Global policy and share it across multiple logical management

2.1.1.14.10. Must have a dedicated dashboard and logging database for each logical management

2.1.1.14.11. Must have granular administrative controls and role assignments

2.1.1.14.12. Must allow multiple administrators to work on different logical management simultaneously

2.1.2. Internal Firewall

2.1.2.1. Hardware Specification

2.1.2.1.1. Firewall throughput minimum of 70Gbps, 1518 byte UDP

2.1.2.1.2. Intrusion Prevention System (IPS) throughput minimum of 7 Gbps, running on “Recommended” policy, IMIX traffic

2.1.2.1.3. Concurrent connections minimum of 20 million

2.1.2.1.4. Connections per second minimum of 170,000, 64 byte HTTP response

2.1.2.1.5. Interface ports, RJ45, minimum of 6 x 1000Base-T

2.1.2.1.6. Interface ports, minimum of 6 x 10Gb SFP+ with SR transceivers (LC connector)

2.1.2.1.7. RAM minimum of 64GB

2.1.2.1.8. Dual power supply, hot swappable

2.1.2.1.9. Dual hot swappable Hard disk drive (HDD) minimum size of 500GB, RAID 1

2.1.2.1.10. Lights out management (LOM) card

2.1.2.1.11. Operating system must be vendor proprietary, running on 64bit

2.1.2.1.12. Must have multicore performance acceleration technologies

2.1.2.2. Software

2.1.2.2.1. Security Technologies

2.1.2.2.1.1. Must have stateful packet inspection

2.1.2.2.1.2. Must have address spoofing protection

2.1.2.2.1.3. Must support Network Address Translation (NAT) - one-to-one, many-to-one and policy based NAT

2.1.2.2.1.4. Must have granular policy definitions per user, group and machine identity

2.1.2.2.1.5. Configurable user role identity with combination of either user, group or machine

2.1.2.2.1.6. Must have seamless and agent less integration with active directory

2.1.2.2.1.7. Must have multiple identification methods but not limited to ff. – browser-based authentication w/ captive portal & transparent Kerberos authentication support, AD query and identity client-side app

2.1.2.2.1.8. Must have a built-in Intrusion Prevention System (IPS) to prevent application layer attacks, vulnerabilities and exploits

2.1.2.2.1.9. Must be Application aware. Current application identification must be minimum of 4,000+ and classify minimum of 300,000+ Web 2.0 widgets inside social networking, instant messaging, VOIP, etc.

2.1.2.2.2. Virtual Firewall Technology (Internal Firewall)

2.1.2.2.2.1. Must have a license of at least 10 Virtual Firewalls

2.1.2.2.2.2. Must be able to support VLANs

2.1.2.2.2.3. Must be able to allocate customized policy per Virtual Firewalls

2.1.2.2.2.4. Must have creation templates of Virtual Firewalls

2.1.2.2.2.5. Must have Virtual Routers and Virtual Switches

2.1.2.2.2.6. Must have per Virtual Firewall resource usage monitoring (CPU, memory, concurrent connections, etc.)

2.1.2.2.2.7. Must able to support per Virtual Firewall resource allocation

2.1.3. External (Perimeter) Firewall

2.1.3.1. Hardware Specs

2.1.3.1.1. Firewall throughput minimum of 10Gbps, 1518 byte UDP

2.1.3.1.2. VPN throughput minimum of 2Gbps, AES 128

2.1.3.1.3. IPSec VPN tunnels minimum of 30,000

2.1.3.1.4. IPS throughput minimum of 1Gbps, running on “Recommended” policy, IMIX traffic

2.1.3.1.5. Interface port: at least 10 copper ports

2.1.3.1.6. Concurrent connections minimum of 3 million

2.1.3.1.7. Connections per second minimum of 70,000, 64 byte HTTP response

2.1.3.1.8. RAM minimum of 8GB

2.1.3.1.9. Single power supply, capable of dual hot swappable

2.1.3.1.10. HDD minimum size of 250GB

2.1.3.1.11. LOM card

2.1.3.1.12. Operating system must be vendor proprietary, running on 64bit

2.1.3.1.13. Must have multicore performance acceleration technologies

2.1.3.2. Software Specs

2.1.3.2.1. Security Technologies

2.1.3.2.1.1. Must have stateful packet inspection

2.1.3.2.1.2. Must have address spoofing protection

2.1.3.2.1.3. Must support Network Address Translation (NAT) - one-to-one, many-to-one and policy based NAT

2.1.3.2.1.4. Must have granular policy definitions per user, group and machine identity

2.1.3.2.1.5. Configurable user role identity with combination of either user, group or machine

2.1.3.2.1.6. Must have seamless and agent less integration with active directory

2.1.3.2.1.7. Must have multiple identification methods but not limited to ff. – browser-based authentication w/ captive portal & transparent Kerberos authentication support, AD query and identity client-side app

2.1.3.2.1.8. Must have built-in Intrusion Prevention System (IPS) to prevent application layer attacks, vulnerabilities and exploits

2.1.3.2.1.9. Must be Application aware. Current application identification must be minimum of 4,000+ and classify minimum of 300,000+ Web 2.0 widgets inside social networking, instant messaging, VOIP, etc.

2.1.3.2.1.10. Must have Anti Bot that has detection methods at least but not limited to Reputation (IPs, URLs, DNS), traffic patterns and bot types. Database must be cloud and dynamically updated in real time

2.1.3.2.1.11. Must able to support IPSec Virtual Private Networking (VPN) - Site-to-Site VPN and Remote Access.

2.1.3.2.1.12. Must have a Secure Socket Layer (SSL) VPN for secured remote access of corporate resources. Connectivity must either via Web Based and VPN Client with support for SmartPhones minimum of IOS and Android, license is at least 200 users (concurrent based)

2.1.3.2.1.13. Must be able to support SSL inspection with option for SSL low level inspection

2.1.3.3. High Availability (HA) and Networking Technologies

2.1.3.3.1. Must be able to perform Active-Active or active-standby device high-availability (HA) with session/state synchronization and automatic load distribution. Active-Active setup must only require one Virtual IP-address (VIP) which is shared among HA members for ease of configuration for adjacent hosts and devices.

2.1.3.3.2. Must able to detect device failure when configured as HA

2.1.3.3.3. Must able to detect link failure when configured as HA

2.1.3.3.4. Must able to support both IPv4 and IPv6

2.1.3.3.5. Must able to support 802.3ad link aggregation

2.1.3.3.6. Must have bandwidth controls or Quality-of-Service (QoS) to prioritize and limit network applications and hosts.

2.1.3.3.7. Must have Server Load Balancing to distribute load to multiple servers serving identical services

2.1.3.3.8. Must have ISP-Redundancy and support for minimum of two ISP

2.1.3.3.9. Must have policy-based routing support

2.2. Lot 2 – Web Application Firewall (WAF) for Disaster Recovery Site

2.2.1. Technical Requirements

2.2.1.1. Delivery, installation and configuration to GSIS DR site inclusive of implementation team accommodation and travel expenses

2.2.1.2. Able to prevent but not limited to OWASP Top 10 web application attacks, SQL injection, cross site scripting or cross site request forgery

2.2.1.3. web service security including but not limited to XML/SOAP, XML protocol performance, web services signature

2.2.1.4. Fraud and malware detection

2.2.1.5. Content modification includes but not limited to URL rewriting, custom error message, cookie signing, cookie encryption, or error code handling

2.2.1.6. System should be scalable, able to support multiple network

2.2.1.7. The proposed solution must have perpetual license(s)

2.2.1.8. Must have a DDOS prevention capability

2.2.1.9. Must have web application acceleration

2.2.1.10. Must be able to update signature/policy

2.2.1.11. Authentication: supports LDAP (Active Directory)

2.2.1.12. Automated tracking of web application users

2.2.1.13. Deployment mode: supports transparent bridge (layer 2), reverse proxy and transparent proxy (layer 7) and non-inline sniffer

2.2.1.14. Management: must have a web user interface (http/https) and command line (SSH/console)

2.2.1.15. Stateful firewall

2.2.1.16. Supports data leak prevention for credit card number, PII (personally identifiable information), or pattern matching

2.2.1.17. Integrated graphical reporting

2.2.1.18. Supports SNMP

2.2.1.19. Supports IPV4 and IPV6

2.2.1.20. Must be in the leader or challenger quadrant of June 2014 Gartner Magic quadrant for web application firewall.

2.2.1.21. ICSA Labs Certified Web Application Firewall

3. Warranty and Maintenance from the date of acceptance.

3.1. Lot 1 – Enterprise Network Firewall

3.1.1. Software and hardware warranty and maintenance for one(1) year including free subscription of software upgrade and updates

3.2. Lot 2 - Web Application Firewall for Disaster Recovery Site

3.2.1. Software and hardware warranty and maintenance for three(3) year including free subscription of software upgrade and updates

4. Capability Building

4.1. The vendor shall provide classroom type administrator's training to a minimum of three (3) participants including training hand-outs with hands-on.

5. Technical Support

5.1. Lot 1- Enterprise Network Firewall

5.1.1. One (1) year technical support period from the date of acceptance and completion

5.1.2. Technical support response time must be at most one (1) hour for phone support and at most two (2) hours for onsite support

5.1.3. Off-site support should be available via email and internet

5.2. Lot 2 - Web Application Firewall for Disaster Recovery Site

5.2.1. Three (3) years technical support period from the date of acceptance and completion

5.2.2. Technical support response time must be at most one (1) hour for phone support and at most two (2) hours for onsite support

6. Project Documentation

The vendor shall provide project documentation such as but not limited to:

- Project Plan
- Systems configuration
- System procedure and maintenance including shutdown and power up procedure.