

**TECHNICAL SPECIFICATIONS**

**Project Title: Supply and Installation of One (1) Lot Web Security Gateway Appliance Solution.**

**PROJECT DESCRIPTION:**

Supply, installation, configuration and testing of One Unit multi-layered Web security appliance that would protect the Bureau of the Treasury from spywares and a wide variety of Web-based threats. A license renewal for the systems that will help fulfill the purpose of this security project are also included.

**PROJECT DURATION: 60 CALENDAR DAYS**

**APPROVED BUDGET FOR THE CONTRACT (ABC): P4,000,000.00**

The minimum requirement specified in this Technical Specifications shall be complied with. Non-compliance with these requirements is a ground for disqualification.

<b>PURCHASER’S SPECIFICATIONS</b>	<b>SUPPLIER’S SPECIFICATION</b>
<p style="text-align: center;"><b>PART I. ONE (1) UNIT WEB SECURITY GATEWAY APPLIANCE SOLUTION</b></p> <p><b>A. GENERAL REQUIREMENTS.</b></p> <ol style="list-style-type: none"><li>1. Appliance based Solution to be provided with Proprietary OS – Please mention the OS.</li><li>2. Minimum of 250 users.</li><li>3. Must have at least minimum 1x2 (1 Dual Core) Pentium processor.</li><li>4. Solution support must have at least two Gigabit Ethernet Cards.</li><li>5. Should have RAID 1 configuration; Dual channel hardware with battery-backed.</li></ol>	

6. Access Log should be scalable. The retention period should be customizable.
7. Rack Mounted 1U Size
8. Support from parent company should be available. Should Provide Toll Free Support, Email Support and should also provide Support Portal access
9. Email/Remote support using secure methods
10. Onsite support to be made available within one day (24 hours) of reporting the complaint.

**B. SYSTEM FUNCTIONALITY.**

1. Web based Administration via HTTP or HTTPS.
2. Appliance Should have a inbuilt AntiVirus Engine. Please mention the Antivirus Engine.
3. Appliance should have a inbuilt AntiMalware / Antispyware Engine. Please mention the AntiSpyware / AntiMalware Engine.
4. Appliance should provide built-in Web Based Reputation Services and scoring options.
5. Appliance should have customizable setting in the Web Based Reputation Services, like Allow, Scan and Block based on the scoring settings by the Administrator.
6. Solution should scan for Incoming traffic.
7. Appliance should support L4 traffic monitoring.
8. Appliance should support L4 traffic monitoring for antipsyware and block Phone home attempts.

9. L4 traffic should detect and block Spyware/ Malware in all the 65535 ports and details reporting should be provided on a per user basis.
10. Appliance should have an inbuilt URL filtering functionality with categories.
11. Appliance should support Pre-defined categories and custom categories.

**C. NETWORK SCALABILITY.**

1. Should Support Forward Proxy
2. Should Support Transparent Proxy via WCCP.

**D. PROXY FUNCTIONALITY.**

1. Should be Fast Web Proxy
2. Should provide URL Filtering Categories
3. Should provide easy and Automatic Updating of the URL Category
4. Should provide Custom Categories to bypass certain sites/urls in the URL categories
5. Should provide a window for submitting sites/urls to Specify Category
6. Should have Reputation Filters or equivalent technology
7. URL category should support Multilingual Site
8. Should be capable of responding to new website and new threats. Vendor/Principal solution provider to have a dedicated 24x7 lab operations to detect and update signatures.
9. Online auto updates of antivirus, anti-malware signatures (should not require the services to be stopped while update process).

10. Supports Whitelist and Blacklist of sites as defined by the administrator

11. Provides the flexibility of keeping the logs for no of days

**E. GUI AND REPORTS.**

1. Web-based/role based reports. A provision for report only user to be present.

2. Web-based access to be only through SSL. http access to web based interface should NOT be allowed.

3. Should have Informative and exhaustive set of reports on User Activity and URL filtering activities (GUI to report past activity, top usage users and top malware threat).

4. maintains detailed access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it.

5. Detailed report on a per user basis should be provided on the L4 traffic monitoring.

**F. DIRECTORY SERVICES.**

1. Seamlessly Integrate with Active Directory / LDAP directory

2. Capable of Defining policies based on User Groups and User Accounts

**G. CONSOLE ACCESS.**

1. Console Access, if any, to be provided as secure shel (life ssh). Telnet access should not be allowed.

**H. PRIVACY.**

1. Should not run any other services except those required for the Proxy product to be successfully run. Vendor to demonstrate

and certify the same.

**J. HIGH AVAILABILITY.**

1. Provision of High Availability to be made.
2. Load Balancing and Clustering

**PART II. SUPPORT MAINTENANCE  
RENEWAL FOR THE  
FOLLOWING ITEMS:**

1. JUNIPER IC 4000 and JUNIPER SSG550  
FW:
  - a. For 3 years.
  - b. Return-to-factory Hardware  
Repair.
  - c. Next Day Replacement.
  - d. Access to all new Software  
Releases applicable to the two  
products.
  - e. Unlimited access to Juniper  
Technical Assistance Centre  
(JTAC) by phone and online,  
24x7x365.
  - f. Access to Juniper Customer  
Support Center (CSC).
  - g. Unlimited access to Reseller  
Helpdesk by phone/email,8x5.  
Technical engineers must be a  
certified Juniper Engineers, could  
provide immediate technical  
assistance, must guarantee a 4-hr  
response time.
2. IPSCAN PROBE 600F:
  - a. For 3 years.

- b. Return to factory for hardware repair or replacement.
- c. Access to all new software releases applicable.
- d. Unlimited access to IPScan Technical Assistance Centre by phone and online, 24x7x365.
- e. Access to IPScan Customer Support Center .
- f. Unlimited access to Reseller Helpdesk by phone/email,8x5. Must provide immediate technical assistance, must guarantee a 4-hr response time.

**PART III. OTHER REQUIREMENTS.**

**1. WARRANTIES FOR THE EQUIPMENTS.**

- o 3 Yrs. On Hardware
- o 3 Yrs. Maintenance and Support

**2. TRAINING.**

- o Must be conducted by a Certified Engineer, after the implementation.

**3. TECHNICAL SUPPORT SERVICES (for a period of 3yrs.).**

- o Provide 8 x 5 email and phone support.

**4. KEY PERSONNEL QUALIFICATION FOR THE IMPLEMENTATION OF THE PROJECT AS BIDDERS COMPETENCY REQUIREMENT.**

Minimum required experience of key personnel under regular employ of the Bidder. *(Submit copy of curriculum vitae, company ID and training certificates).*

At least Two (2) Systems Administrator certified in the following:

- Juniper Networks Certified Internet Associate in Firewall/VPN
- Has a minimum of 6 months of experience supporting the Web Security product that will be proposed.

**5. CLIENTELE.**

- List of Client Attached.
- The Bidder must submit at least five (5) Certificates of Satisfactory Performance/Completion from previous clients.

**6. STATEMENT UNDER OATH OF BIDDER'S BUSINESS EXISTENCE AND EXPERTISE**

- The Bidder must be an ICT company with expertise and/or experience in different fields of ICT, Network Management, Security Management Solution Software, and Network Design
- The Bidder must be operating in the Philippines for the past fifteen (15) years.
- The Bidder must have completed projects that are similar to the project to be bid in an amount equivalent to 50% of the ABC. (submit proof)  
*Note: Similar projects are those related to Network Security projects.*
- The Bidder must have completed consultancy project involving network assessment and design enhancement, network asset inventory, network health and performance, network monitoring and management of end-to-end LAN and WAN status for the past 5 years. (submit proof).

**7. BIDDER'S CERTIFICATION REQUIREMENTS.**

- Certificate from the manufacturer that the product and model to be bid is being manufactured by the concern manufacturer.
- Certification issued by the Manufacturer of the proposed Web Security Appliance that the bidder is the authorized reseller and support provider in the Philippines.
- Certification from the Distributor of the proposed Web Security Appliance that the Distributor is willing to extend its support to the Bureau of the Treasury for the product being offered by the bidder.

**8. OTHER VALUE ADDED SERVICES.**

- Please Specify.

**9. DOCUMENTATION.**

- Installation Procedure (Customized for BTr).
- Administration Procedure (Customized for BTr).

**10. MODE OF PAYMENT**

- Within 30 days from complete delivery or issuance of certificate of acceptance by BTR through the Systems Administration Divisions.
- One-time payment of the contract shall be made upon completion of supply, delivery, installation of hardware and software components and upon issuance of certificate of acceptance by the end-user.
- Training component shall not form part of the requirements for the payment of the contract, but must be completed by the bidder after all configuration and/or installation, based

<p>on the schedule to be determined by the end-user.</p> <p>○ For failure to completely deliver any portion of the goods, a penalty equivalent to one-tenth of one percent (0.1%) of the total cost of the unperformed portion of services shall be imposed for everyday of delay.</p>	
--	--

Prepared by:

Approved:

Wilfredo L. Yatco  
OIC-SAD

Regilito L. Tamayo  
OIC-MISS