SUPPLY, INSTALLATION, CONFIGURATION, TESTING AND COMMISSIONING OF A NETWORK PERIMETER SECURITY SOLUTION

Table of Contents

1.0 COMPONENTS OF THE REQUIRED SOLUTION

The proposed cybersecurity solution should cover the following;

1) Redundant Network Perimeter Security at the Head Quarters
2) Centralized Security Management (Security Management Server) for the proposed network security appliances

2.0 TECHNICAL SPECIFICATIONS

The required solution should be delivered in a unified platform with consolidated security management across the network security.

In order to ensure the unified solution mitigates attacks at each step of the cyber-kill chain, the solution must meet the general requirements below. Each response MUST reference and attach publicly available document such as datasheets. Screenshots can be included where necessary.

2.1 Technical Specifications of Network Perimeter Security Gateway

The bidder must provide evidence that the proposed Security gateway for County Headquarters Network Perimeter support all the following security features.

Technical Specifications of Security Gateway	**Compliant/ Non-Compliant**	**Bidder's Response**
The bidder MUST propose a vendor that exclusively provides cyber security solutions.		
The bidder MUST attach and reference published Gartner Magic Quadrant (MQ) reports that show the vendor's leadership positions in NGFW firewall over the last 5 years.		

The bidder MUST attach and reference NSS Labs reports that show the vendor's **Recommended** rating in Breach Detection Systems over the last 5 years.		
The bidder MUST attach and reference the 2017 NSS Labs Breach Prevention report showing the proposed solution has a **security effectiveness** of over 97%		
The security gateway must use Stateful Inspection based on granular analysis of communication and application state to track and control the network flow.		

Application Control and URL Filtering		
The Integrated Application Control must have over 6,000 web 2.0 applications		
Solution must be able to create a filtering rule with multiple categories		
URL Filtering supporting enforcement of timed access to sites and the ability to educate users.		
Solution must support access control for at least 150 predefined		

Application Control and URL Filtering		
/services/protocols		
Must provide security rule hit count statistics to the management application.		
Must allow security rules to be enforced within time intervals to be configured with an expiry date/time.		
Must support integration with multiple LDAP repositories		
Must leverage Identity Awareness for visibility into users' and group activity		
The firewall must support user, client and session authentication methods.		
The following user authentication schemes must be supported by the security gateway and VPN module: tokens (i.e. -SecureID), TACACS, RADIUS and digital certificates		
IPSec VPN with support for multiple authentication options		

Application Control and URL Filtering		
such as User Certificates, CAPI, one time tokens, software and hardware smartcards		
Mobile Access Remote VPN for at least 5 concurrent users, for SSL access to corporate web applications		
IPv6 Support		
Solution must support IPv6 traffic handling on IPS and APP module, Firewall, Identity Awareness, URL Filtering, Antivirus and Anti-Bot		
Solution must Support 6 to 4 NAT, or 6 to 4 tunnel		
Solution must support AD integration using IPv6 traffic		
Intrusion Prevention System		

IPS must leverage software based acceleration technologies to deliver security and performance.		
IPS must have mechanism of validating RFC compliance of protocols and checking anomalies		
IPS must provide geo-protections to allow the administrator to easily block inbound and/or outbound traffic based on countries.		
IPS must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection		
IPS must be able to fail open during high load.		
IPS must be integrated with firewall, application control, URL filtering, Antibot and Sandboxing features on a		

unified platform.		
The IPS vendor must supply evidence of leadership in protecting Microsoft vulnerabilities.		
IPS must support consolidated management on a single pane of glass.		
Anti-Bot and Anti-Virus		
Solution must have an integrated Anti-Bot and Anti-Virus		
Anti-Bot and Anti-Virus. Analyzing over 200 million addresses for bots and more than 250,000 websites		
Antibot must be able to detect bots and block communication to command and control sites.		
Anti-Bot and Anti-Virus policy must be administered from a central console		
Anti-virus must leverage a cloud database with over 4 million malware signatures.		
Anti-Spam and Email Security		
Anti-Spam and Email security application		

must be content and language agnostic		
Anti-Spam and Email security application must have real-time classification and protections based on		
detected spam outbreaks which are based on patterns and not content		
The Anti-Spam and Email security application must include IP reputation blocking based on an online service to avoid false positives		
Solution must include a Zero-hour protection mechanism for new viruses spread through email and spam without relying solely in heuristic or content inspection		
The Anti-Virus should support scanning for links inside emails		
The Anti-Virus should Scan files that are passing on CIFS protocol		
Email Security		

Anti-Spam and Email security application must be content/format and language agnostic.		
Antispam must include an antivirus engine that scans mail protocols such as SMTP and POP3.		
The Anti-Spam and Email security application must include IP and content reputation checks.		
Solution must include a Zero-hour protection mechanism for new viruses spread through email and spam without relying solely in heuristic or content inspection.		
Data Loss Prevention (DLP)		
The gateway must have an option to add an integrated Data Loss Prevention application on the same appliances.		
DLP application must have over 500 pre-defined data types		
DLP must have an open scripting language to create customer data types relevant to any organization		

DLP must alert the data type owner when an incident occurs		
DLP application must cover transport types SMTP, HTTP/HTTPS, and FTP TCP protocols		

2.2 Technical Specifications of the Security Management Server

The bidder must provide evidence that the proposed consolidated security management server support all the following security management features. It should consolidate management, monitoring and reporting of all the proposed security gateways.

Security Management Server (Quantity 1)	**Compliant /Non-Compliant**	**Bidder's Response**
Security management application must be able to co-exist on the security gateway as an option.		
Security management must support unified management of both perimeter networks and mobile security		
Security management must support unified management of cloud and endpoint security for scalability		
Security management must support		

Security Management Server (Quantity 1)	Compliant /Non-Compliant	Bidder's Response
concurrent administration.		
Security management must support integration with LDAP-based information stores to centralize user management.		

Security management must provide browser-based access to administrators and auditors to view policies, gateway status and user administration.		
Security Management must provide APIs to enable self-service and automated workflows.		
Security management must support central management of policy change management with review and audit capabilities of policy changes.		
Security management must enable administrators to action on identified events such as by locking it immediately.		
Security management must support management of endpoint security.		

Logs and Event management		
The service must incorporate with a firewall specific graphical log and event management		
The proposed centralized log management system must scale in minimum 50 simultaneous management sessions via graphical UI.		
The log and event management system must fulfil the same role-based access and authentication requirements that are applied to the centralized management system.		
The Log analyzing must support creationof custom log queries.		
The log entries must be possible to search and sort by:		
• Firewall		
• Rule Id		
• Any firewall object		
• User identity		
• Time stamp		
• Most hitted firewall rules		

• Least hitted firewall rules		
The detected firewall specific session alerts must be logged and the log data must show the top5 source and destination talkers during the threshold exceeding		
The customer specific log data must be available for the customer for three Months		
The data of top5 sources of blocked traffic must be available		
The log data must be possible to be archived to another external repository for longer storage time.		
Rule based analysis sorting the rules based on the hits and revealing if some rules are not used at all.		
Best Practice Governance Risk and Compliance (GRC)		
Vendor must have an option to provide a fully integrated Governance Risk and Compliance application		
Vendor must have an option for Real Time Compliance Monitoring across all security services in the product		

Vendor must have an option to Deliver real-time assessment of compliance with major regulations (ISO, PCI-DSS, SOX...)		
Vendor must have an option for Instant notification on policy changes impacting compliance		
Vendor must have an option to Provide actionable recommendations to improve compliance		
Vendor must have an option to recommend configuration of device based on OEM Security Best Practices		

3.0 PERFORMANCE REQUIREMENTS

3.1 Security Gateway for the Head Quarters Network Perimeter

The bidder MUST attach and reference public datasheet(s) as evidence that the proposed Network perimeter Security Gateway meets all the performance and hardware requirements in the table below.

Network Perimeter Security Gateway (1 required)	**Minimum Specification**	**Compliant/Non-Compliant**	**Bidder's Response**
1 GbE Copper ports	8		
Supports up to 1 GbE Fiber ports	Supported		
RAM	16 GB		
Lights Out Management port	Included		
Firewall throughput	14 Gbps		
IPS throughput	2 Gbps		
VPN Throughput	1 Gbps		
Threat Prevention throughput	1 Gbps		
NGFW throughput	2 Gbps		
Concurrent connections with 64byte response	3 Million		
Connections per second with 64byte response	100,000		
Storage	500 GB		
Expansion slot	1		
Direct Support and warranty with vendor	1 year		

3.2 Central Security Manager Requirements

The bidder MUST attach and reference public datasheet(s) as evidence that the proposed Consolidated Security Management appliance meets all the performance and hardware requirements in the table below.

Security Management Servers (1 required)	**Minimum Specification**	**Compliant/Non-Compliant**	**Bidder's Response**
Managed security gateways	20		
Logs per Second	50,000		
Indexed Logs Per Second	12,000		
Storage(HDD)	2 x 4TB		
RAM	32 GB		
Copper GbE Interfaces	4		
Dual-Host swappable PSU	required		
Console Port DB9	1		
USB Ports	4		
Management of Network Policies	Included		
Management of policies for the Remote Access users	included		
GRC Compliance reporting and monitoring	Included		
Direct Support and warranty with vendor	1 year		

4.0 PRICE SCHEDULE

The bid prices shall be given in the form given below or any equivalent for the following components of the tender.

Implementation Services Post warranty OEM Support and Maintenance – Bidders to include two years proactive direct support, services and warranty

#	Part No.	Description	QTY	Unit cost	Total cost
1.		Security Gateways for the HQ perimeter security	1		
2.		Centralized Security Management Server	1		
3.		Implementation services For the entire solution (including training)			
4.		Direct premium OEM support and warranty	1 year		
		TOTAL			

Bidders MUST include and justify any additional items required for full implementation of the proposed security solution.

NOTE:

1. Prices should be inclusive of all applicable taxes.
2. In case of discrepancy between unit price and total, the unit price shall prevail.
3. Prices should include one year of software subscriptions and support.