



TENDER NO (77/2022)

NETWORK SECURITY UTM, EDR MANAGEMENT SOLUTION, AND VULNERABILITY TESTING TOOLS

Samra Electric Power Company



شركة السمرات لتوليد الكهرباء
Samra Electric Power Co. [SEPCO]

Date: -Dec-2022

[Handwritten signature]



Key Events & Dates

Tender Notice No	
Tender Fee (non-refundable)	
Bid Bond	
Performance Bond	10% of the Bidder Total Price
Date of Issue	
Last date for seeking clarifications, if any	
SEPCO Answer to Clarifications	
Proposals Submission Date	
Expected Award Date	
Preferred Delivery Date	
E-mail Address for all inquiries	
Validity of Proposal	(90) Ninety days from the date of Proposals Submission.


SEPCO reserves the right to reject all or any tender wholly or partly without assigning any reason whatsoever.

The vendor submitting the proposal in response to RFP, shall hereinafter be referred to as "Bidder / Vendor" interchangeably. SEPCO will not be liable for any costs incurred by the bidder in the preparation of the response to this RFP.

The preparation of bidder's proposal will be made without obligation by SEPCO to acquire any of the items included in the vendor's product, or to select any vendor's proposal, or to discuss the reasons why the bidder's proposal is accepted or rejected. All information included by the bidders in their proposal will be treated in strict confidence.

Downloading Bid document from the website:

The Bidder may download Tender Document along with terms and conditions from SEPCO website www.sepcocom.jo .


11/12/2022






Eligibility Criteria (Pre-Qualification)

SI/ No	Clause	Documents required
A	The bidder should be a registered company in Jordan for at least 5 Years	Copy of the Certificate of registration and Vocational License are required to be submitted along with the technical bid.
B	The bidder should be an authorized partner of the OEM for the product being proposed. Experience of executing similar orders is a must.	A copy of the necessary Partner Certification must be attached indicating that the local partner is authorized to perform the services assigned to it by the mother Company along with any certification, training or other certificates that supports the partner profile as an authorized partner with skilled resources. The vendor should provide evidence for the execution of similar projects (minimum 5 similar projects)
C	The Bidder to confirm that the bid is not submitted in Consortium as well as Sub-contracting	Declaration in this regard by the authorized signatory of The Responder.
D	Acceptability of all conditions contained in the Tender Document by the Bidder. No further deviations to any mentioned clause shall be sought for.	Declaration by an authorized signatory of The Responder.
E	The bidder must confirm compliance with technical specifications of the hardware proposed as per the annexure attached.	Must enclosed appropriate responses with The compliance sheet.
F	The The contractor must mention the number of the company's employees specialized in the field of security and protection, and that they are people with highly excellent technical experience and have scientific qualifications and high technical ability in the field of security and protection of networks and solving their problems, and a copy of the names of the company's experts and their CVs should be attached to the bid.	
Note:- Documentary Evidence for compliance to each of the eligibility criteria must be enclosed along with the bid together with references. Undertaking for subsequent submission of any of the require document will not be entertained under any circumstances. However, SEPCO. reserves the right to seek clarifications on the already submitted documents.		

[Signature]
11/12/2022

[Signature]



Introduction

Samra Electric Power Company (SEPCO) was established by the government of the Hashemite Kingdom of Jordan pursuant to the provisions of the Companies Act No. 22 of 1997 and in implementation of the Cabinet Resolution taken in its session held on 26/8/2003.

It is wholly owned by the government with a capital of Fifty Million Jordanian Dinars.

The Company was registered with the General Companies Controller on 20/4/2004 under number 40

Overview & Objective

SEPCO is complete upgrading of its Networking & Computing Assets. New Datacenters are built to host the new environment. Further, Cabling of SEPCO Network along with complete security solution (Network, Server & End point) are required.

SEPCO intends to select a vendor to supply, install, integrate and operationalize the needed security Hardware and software's at SEPCO HQ at Mecca St. Amman, Jordan and at Zarqa Power Station in Zarqa, Jordan.

The successful vendor is expected to configure as well as test the Complete Passive Network & Data Security Environment in the HQ and the Zarqa Power Station and to perform . The selected vendor is also required to provide comprehensive On-site maintenance of the hardware supplied for a period of 3 years. The comprehensive maintenance of hardware of SEPCO includes repair/replacement of all faulty systems / parts.

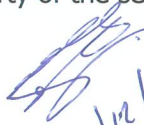
SEPCO is pleased to invite proposal from the prospective bidders having proper experience and competence in the field.

The details of the Scope of Work are mentioned in **Annex 1** .

Part(s) Replacement

All defective parts shall be replaced at no extra cost. Replacement parts shall be new or their equivalent from the same manufacturer(s).

The parts replaced will either be a new part or equivalent in performance to new parts. Whether a defective item or component is to be replaced or repaired shall be at the sole discretion of the selected firm. In the case of a part, the defective part removed from the system will become the property of the selected firm.


11/12/2022






Warranty & Support

Warranty for the Services shall be as set forth in this RFP.

After Testing of the implemented Solution /project and its acceptance by SEPCO, the Bidder has to provide regular warranty & Support for **three (3) years** as per details hereunder.

- Vendor shall provide comprehensive support for all security hardware and software listed in the document.
- The scope of the warranty/annual maintenance contract also includes, but is not limited to, provision of new system software releases, patches, software releases including firmware, test tools, and bug fixes.
- Bidders must maintain the offered Hardware+Software for at least 3 years (3 years warranty support) from the date of acceptance of SEPCO.
- The bidder shall provide free maintenance services on site during the warranty period, at the rate of a preventive maintenance visit every two months, and prompt response (within 24 hours) to the emergency maintenance request.
- The bidder must provide free maintenance services on site during the free warranty period and by conducting a technical visit every two months once, and providing us with a technical report on that (soft & hard copy).
- The bidder must clarify the prices of the annual technical support, including the renewal of all types of required licenses, after the end of the free maintenance period of the tender (3 years).


11/12/2022





Submission of RFP

Submission is required to be done as under: -

- Technical Proposal along with all required documentations and certifications as per the RFP document
- Bid Bond
- Financial Proposal with Detailed Costing per item

Technical Proposal to be submitted in **Two** Hard Copy and One Soft Copy
All Technical catalogs to be submitted in soft copy only

Proposals to be submitted to the following address:
Samra Electric Power Company
Supplies and Procurement Department
Mecca St. Amman, Jordan.

The Tender evaluation committee constituted for the said purpose, shall conduct bid evaluation. The objective of evaluation methodology is to facilitate the selection of the technically superior solution at optimal cost. The purpose of it is only to provide the Bidder an idea of the evaluation process that SEPCO may adopt.

SEPCO reserves the right to modify the evaluation process at any time during the Tender process (before submission of technical and commercial responses by the prospective bidder), without assigning any reason, whatsoever, and without any requirement of intimating the Bidders of any such change.

Technical-Commercial

1. complied bidder with lowest quote based on Total Cost of Ownership (TCO) will be considered as successful bidder.
2. The technical solution presented in the bid shall be considered as one unit and cannot be divided.

Payment Terms

- 100% After Final Acceptance by SEPCO

Project Time lines :-

The Bidder shall submit a detailed and clear work plan for the method of working with the tender documents, to be approved after the official award of the tender

The project must be completed within a maximum period of two working months from the date of the formal receipt of the referral and that From the date of agreement on the project work plan.

Delays in the vendor's Performance : as SEPCO Procurement Rules


11/12/2022






Delivery, Installation and Commissioning of Hardware /Software:

The Bidder will be responsible for:

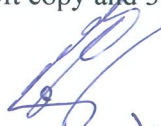
- The selected Bidder shall supply various network security system Hardware/Software components as mentioned in the **Annex-1**.
- Installation shall mean to install and configure / integrate, Hardening of every component and subsystem component, required for project security of the Data Centers.
- The bidder should provide us with all types of licenses required and specify them clearly.
- The tender includes all types of licenses that are required for equipment and software throughout the free maintenance period.
- The Bidder will promptly install the delivered goods at the designated installation sites.
- The Bidder is responsible for installation and configuration of network security system at sites including unpacking of cartons/ boxes, assembling, wiring, cabling between hardware units/Software and connecting to power supplies. The Bidder will test all hardware and accomplish all adjustments necessary for successful and continuous operation of the hardware/Software at all installation sites.
- The Bidder may commence installation of the equipment only after SEPCO has performed a successful Post Delivery Inspection of the equipment, after it has arrived at the designated sites. The Bidder or its representative may test/inspect the Hardware. During the Post Delivery Inspection, the Bidder should provide necessary support/infrastructure to facilitate Post Delivery Inspection. Hardware may be rejected by SEPCO during this inspection, which must be promptly replaced by the Bidder, in order to complete the inspection and meet the schedule.
- The Bidder must install, test and integrate network security system for hardware and software components supplied by them to ensure inter-working of hardware and software. The Bidder will also be responsible to co-operate with SEPCO and/ or its application software vendor/ any of the partners, who will install the application software and drivers on the systems, to ensure that the integrated systems are fully functional.
- All network security system Hardware/software components must be supplied along with original media and required drivers wherever applicable, the supplier must present official certificates of origin for the materials (all hardware) presented in the bid, proving that they are original and from the parent company.
- It is Bidder's responsibility to deliver all the components at the site within the time frame specified by SEPCO in the RFP and install and integrate the same within the time frame specified in the RFP.


11/12/2022





- Bidders shall, during the official bidding period, conduct a technical field visit to the Information Technology Department of SEPCO to view the components of the new data center rooms, computer servers, primary switches and local network switches for which the security system will be installed.
- The Bidder shall make its own arrangements to fulfill all delivery formalities, including payment of all taxes, duties and costs, as applicable, and SEPCO will not engage in such activities. SEPCO shall not be liable for failure by the Bidder to pay any applicable taxes and duties.
- Operation shall include completion of related activities/activities, procurement, installation, configuration, and testing of required components, site availability to SEPCO to carry out live operations and obtain SEPCO approval. Appropriate testing and commissioning must be carried out prior to commencement of operations.
- Must cover final acceptance after successful testing by SEPCO or its monitoring agency. A Final Acceptance Test (FAT) Certificate is issued by SEPCO to Vendor.
- The date on which the final FAT certificate is issued is the date the project was successfully started.
- The bidder must submit clear drawings of the network security system as it was created at the completion of the project which contains: all addresses of the security network that were created, and all the rules and policies that were applied in the network protection system with the addresses of the security devices (1 soft copy and 3 hard copies).


4/12/2021





Scope of Work -:

❖ General Scope o work points :

- Within this project, SEPCO intends to install network protection (IPS / FW) and data centers protection (UTM).
- Supply, installation, and commissioning of a complete security system as specified in the specification details attached to the tender. The bidder must verify the validity of the design and include any other materials or software that may be required and required to activate the work of the protection system.
- The bidder shall carry out a technical review of all existing policies and rules for the protection systems in the current data center of SEPCO.
- The viewer must redefine all users (clients) from the current environment and connect them to AD through the domain to comply with the rules and policies of the new security system.
- The bidder is responsible for installing and connecting all types of equipment required in the bid within the data centers and all required connections with ISP equipment.
- The Security system should cover the upgrade process (to the latest versions) and provide protection for the existing Active Directory environment with a highly available operating mode to a hyper-v cluster, including full protection of DHCP and DNS services, and protection of any required data as per the requirements of the SEPCO team.
- The bidder must test the Total security system solution in all locations after the solution is completely installed providing SEPCO with a full technical report with the results of this testing.
- Provide onsite support for a period of **3 years**, involving the implemented systems, hardware and software if any.
- The bidder must provide with bid documents (soft copy+hard copy) a comprehensive explanation of how to host and operate the protection system presented in the current environment for all servers, equipment and modern and old applications in force in SEPCO
- The bidder should carry on a live demo of the proposed security system solution in front of SEPCO bid technical studying committee.

 11/12/2022





❖ This project includes the following requirements:

1. Perimeter Next Generation Firewall (IPS/FW) Intrusion Prevention System

Vulnerabilities can adversely affect an organization beyond its bottom line. They can also risk the privacy of personally identifiable information (PII) that, when compromised, can have real-life consequences. They undermine not only a company's reputation — they also undermine the integrity of the infrastructures that store and manage this sensitive data.

The requested Intrusion Prevention System (IPS) needed to stop threats & attacks that originate from Internet. The desired solution should include complete hardware delivery, installation and a clear design of the overall solution that must agree to.

The proposed solution should include Virtual patching — or vulnerability shielding — to act as a safety measure against threats that exploit known and unknown vulnerabilities. Virtual patching should work by implementing layers of security policies and rules that prevent and intercept an exploit from taking network paths to and from a vulnerability.

The proposed solution should include the capabilities that inspect and block malicious activity from business-critical traffic; detect and prevent intrusions; thwart attacks on web-facing applications; and adaptably deploy on physical, virtual, or cloud environments.

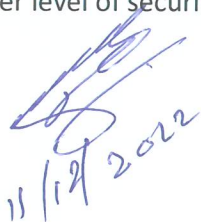
To prevent evasive users and applications from bypassing security functions, all product functions for Intrusion Prevention System (IPS), Threat Prevention, and Anti-Virus, shall not require specific software port and protocol combinations for detection, mitigation, or enforcement.

2. Advanced Endpoint Detection and Response (EDR)/ Advance Endpoint Protection (Application Whitelisting)

Advanced EDR helps to Shrink the footprint of your EDR agent to minimize impact on your server's disk performance and utilization. Moreover, . It Keeps your memory resources available for those applications that matter most to your business. When Advanced EDR installed, all applications on your servers will continue to run fast. The IT department should have peace of mind that there is no hit on server performance and that their systems are being fully protected by Malwarebytes.

3. Unified Threat Management New Generation Firewall for Data Center. (UTM NGFW)

NGFW (Next Generation Firewalls) and UTM appliances the first choice when networks need to be segmented and communication protected from attacks. A NGFW enables internal IT systems to be divided up into security classes and services to be separated from one another by a strategic network segmentation – so that internal attacks are blocked, and network anomalies are prevented from spreading. If necessary additional functions can be added to the platforms to achieve a greater level of security.


11/11/2022





4. Vulnerability Assessment tools:

To provide tools that can identify, rank, and report vulnerabilities, may result in an intentional or unintentional compromise of a system through a variety of automated tools combined with manual verification of identified issues. Vulnerability assessment Provided Tool should be comprehensive but not limited to following features: -

1- Network Scanning /Surveying: Vendor shall identify active hosts on a network, for the purpose of simulating attack and for network security assessment with the help of suitable procedure/tools including but not limited to: -

- a. Examine Name server responses
- b. Review the outer wall of the network
- c. Review tracks from the target organization
- d. Review Information Leaks

2- Port Scanning: To find the active ports on server port addresses on a host vendor shall perform the following but not limited to: -

- a. Error Checking
- b. Enumerate Systems
- c. Enumerating Ports
- d. Verification of Various Protocol Response
- e. Verification of Packet Level Response

3- Port sweep: To scan multiple hosts for a specific listening port for potential vulnerabilities.

4- System & OS Fingerprinting: To guess the system information i.e., type and version of OS etc.

5- System Identification & Trusted System Scanning: Vendor shall perform the scanning which would include but not limited to the following: -

1. Match each open port to a service and protocol.
2. Identify server uptime to latest patch releases.
3. Identify the application behind the service and the patch level using banners or fingerprinting.
4. Verify the application to the system and the version.
5. Locate and identify service remapping or system redirects.
6. Identify the components of the listening service.
7. Use UDP-based service and Trojan requests to all the systems in the network.

6- Vulnerability Scanning: Tool should cover all SEPCO assets.

7- Application Security Testing & Code Review: In case of some application whose code review is allowed to be done for the purpose of VAPT, the tool shall conduct the same.

 11/12/2022





8- Service Fingerprinting: The vendor shall do the following: -

1. Examine system responses to determine operating system type and patch level.
2. Examine application responses to determine operating system type and patch level.
3. Verify the TCP sequence number prediction for each live host on the network.
4. Search job postings for server and application information from the target.
5. Search tech bulletin boards and newsgroups for server and application information from the target.

9- Authorization Testing: Tool shall do the authorization & authentication testing for the present AD system.

10- Lockout Testing: To mitigate the brute force attack etc., lockout testing must be carried out.

11- Password Cracking: To mitigate the brute force attack, cryptographic attack etc., Password cracking testing must be carried out.

12- Cookie Security: Tool shall review the cookie settings and recommend the best practise for making the environment secure.

13- Cookie & Web Bug Analysis: Tool shall review the cookie for bugs and recommend the best practise for making the environment secure .

14- Functional validations: Any or all application when offered for functional validation, vendor shall perform the same.

15- Server Assessment (OS Security Configuration): Tool shall review the present configuration of critical servers and recommend for the improvement if any.

16- Security Device Assessment: Tool shall review the present security devices and recommend for the improvement if any.

17- Network Device Assessment: Tool shall review the present network devices and recommend for the improvement if any.


11/12/2022





5. Training:

- The Bidder shall provide full and comprehensive training to SEPCO System Administrators (minimum =3) on all aspects of the applicable solution with complete evidence (hard copies and soft copies)

in the following areas -:

1. Explanation and clarification of the technical solution presented in the bid.
2. Local training courses in the field of protecting operating systems, networks, and cybersecurity
3. Submission of the necessary training material hard and soft copies.

Deliverables:

1. Local training certificates for the technical courses offered to each trainee.
2. Technical training manuals (soft copy and hard copy) for the technical courses offered to each trainee
3. Technical manuals with all schemes of the built protection system, including all rules and policies


11/12/2022



Annex 1

Detailed Technical Specifications


11/2/2022



Detailed Technical Specifications

1	No	Internet Perimeter Next Generation Firewall (NGFW) (Qty 2) in Amman HQ	Comply/Not Comply	Remarks
	1.1	Full on-box management for local configuration without any external software		
	1.2	Hardware from the same vendor		
	1.3	Must be able to deploy a single device in multiple network deployment modes simultaneously including Layer 1, Layer 2, Layer 3 and passive transparent.		
	1.4	Both transparent and routed in same time.		
	1.5	Must be able to perform SSL decryption inbound and outbound for threat inspection without additional device.		
	1.6	The NGFW appliance should integrate with Active Directory and Wireless RADIUS server for Single Sign-on user identification.		
	1.7	Provide Zero-day protection (sandbox) .		
	1.8	The device should support an IPS throughput of 5 Gbps or more		
	1.9	The device should also support Threat Protection Throughput 1 Gbps or more		
	1.10	NGFW throughput 4 Gbps or more		
	1.11	Provide High Availability Cluster Centralized Management.		
	1.12	The NGFW appliance should also support scanning of SMTP, POP3, IMAP, MAPI, FTP and their equivalent SSL encrypted version.		
	1.13	The NGFW appliance should be able to scan HTTP traffic and intercept HTTPS/SSL web traffic without requiring additional appliance and analyse the traffic for threats.		
	1.14	Provide IPSec VPN + SSL VPN		
	1.15	Provide Intrusion Prevention System		
	1.16	Provide Application Control		
	1.17	One power supply –		
	1.18			

[Signature]
11/12/2022

[Signature]



		Option : Dual power supply .	
1.19		High Availability active/passive	
1.20		High availability (active/active optional)	
1.21		Interfaces requirements 10/100/1000, SFP+s	
1.22		Minimum (6 Interfaces + 2 SFP+)	
1.23		Provide reporting for (3) months.	
1.24		The firewalls must be equipped with all needed cables and transceivers for full connectivity.	


11/12/2022





2	No	Unified Threat (UTM) Management(Data Center) Qty 2-in Amman HQ data center	Comply/N ot Comply	Remarks
		<p>The contractor should Designing, Supply, Implementing, Integrate and Support Haigh availability Unified Threat Management Solution with web application security Technology to be implemented at SEPCO main Data Center. The Solution should be including the following features and components: -</p>		
	2.1	Full on-box management for local configuration without any external software		
	2.2	<p>Must be able to deploy a single device in multiple network deployment modes simultaneously including Layer 1, Layer 2, Layer 3 and passive transparent. Both transparent and routed in same time.</p>		
	2.3	<p>Must be able to perform SSL decryption inbound and outbound for threat inspection without additional device.</p>		
	2.4	<p>Enhanced Web filtering, including extensive category options and a real-time scorecard delivered in partnership with leading Web security provider</p>		
	2.5	<p>Effective inbound and outbound content filtering based on MIME type, file extension, and protocol commands</p>		
	2.6	<p>Provide High Availability Cluster Centralized Management.</p>		
	2.7	<p>Multilayered spam protection, up-to-date phishing URL detection, standards-based S/MIME, Open PGP and TLS encryption</p>		
	2.8	<p>Analyzes application data and classifies it based on risk level, zones, source and destination addresses.</p>		
	2.9	<p>Provide IPSec VPN+ SSL VPN</p>		
	2.10	<p>Provide Intrusion Prevention System</p>		
	2.11	<p>Provide Application Control</p>		
	2.12	<p>Provide URL Filtering</p>		
	2.13	<p>Provide Antivirus</p>		
	2.14	<p>Provide Anti-spyware</p>		
	2.15	<p>Provide web application Firewall</p>		
	2.16	<p>Provide Advanced Network Threat Prevention</p>		

Handwritten signature and date: 11/12/2022

Handwritten signature



- | | |
|------|--|
| 2.17 | Protocol anomaly detection and same day coverage for newly found vulnerabilities are provided. |
| 2.18 | Provide Threat Intelligence |
| 2.19 | The device should support an IPS throughput of 6 Gbps or more |
| 2.20 | The device should also support Threat Protection Throughput 1 Gbps or more |
| 2.21 | NGFW Throughput 5 Gbps or more |
| 2.22 | one power supply. |
| 2.23 | Option: Dual power supply . |
| 2.24 | Interface Modes L2, L3, tap. |
| 2.25 | High Availability active/passive (active/active optional) |
| 2.26 | Minimum 6 Interfaces + 2 SFP+s |
| 2.27 | Interfaces requirements 10/100/1000, SFP+ |
| 2.28 | Appliance reporting |
| 2.29 | Provide IPS |
| 2.30 | Provide reporting for (3) months. |
| 2.31 | The firewalls must be equipped with all needed cables and transceivers for full connectivity. |



3	Endpoint Detection and Response (EDR)/Advance endpoint protection	Comply/N ot Comply	Remarks
	<p>The contractor should Designing, Supply, Implementing, Integrate and Support endpoint detection and response and advance endpoint protection to be installed in all windows and Linux workstations and servers. Critical components need protection from unauthorized applications or malware that may compromise availability, integrity, confidentiality, and control. The solution should be integrated with other solutions SEPCO solutions and provide following features</p> <p>for 250 End points (including 15 servers)</p> <p>3.1 - Delivering complete endpoint visibility across organization.</p> <p>3.2 - Automatically detect attacker activities.</p> <p>3.3 - Identify indicators of attack (IOAs) to automatically identify attacker behaviour.</p> <p>3.4 - Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework.</p> <p>3.5 - Act against adversaries in real time to stop attacks before they become breaches.</p> <p>3.6 - Capture critical details for threat hunting and forensic investigations.</p> <p>3.7 - Should aggregate data on endpoints including process execution, endpoint communication, and user logins; analyse data to discover anomalies and malicious activity; and record data about malicious activity, enabling security teams to investigate and respond to incidents. In addition, should enable automated and manual actions to contain threats on the endpoint, such as isolating it from the network or wiping and reimaging the device.</p> <p>Advanced features:</p> <p>3.8 Best Windows server product</p> <p>3.9 management console</p> <p>3.10 Includes next-gen antivirus software</p> <p>3.11 Real-time protection against malware and other threats</p> <p>3.12 Ransomware, zero-day exploits, phishing protection</p> <p>3.13 Best-in-class threat remediation.</p>		

Handwritten signature and date: 11/12/2022

Handwritten signature

- | | |
|------|-------------------------------------|
| 3.14 | Single, lightweight agent |
| 3.15 | Automated, on-demand reports |
| 3.16 | Threat hunting, isolation, recovery |
| 3.17 | Windows ransomware rollback |


11/12/2022





4	Next Generation Firewall Solution for DR (QTY=1)-Samra Station	Comply/Not Comply	Remarks
	<p>The contractor should Designing, Supply, Implementing, Integrate and Support Next Generation Firewall Solution to be implemented at the SEPCO DR. The Solution should be including the following features and components :-</p> <p>4.1 Full on-box management for local configuration without any external software</p> <p>4.2 Hardware from the same vendor</p> <p>4.3 Must be able to deploy a single device in multiple network deployment modes simultaneously including Layer 1, Layer 2, Layer 3 and passive transparent. Both transparent and routed in same time</p> <p>4.4 Must be able to perform SSL decryption inbound and outbound for threat inspection without additional device.</p> <p>4.5 The Control plane and Data plane should be separated.</p> <p>4.6 Provide High Availability Cluster Centralized Management.</p> <p>4.7 Provide Identity Awareness</p> <p>4.8 Provide IPSec VPN + SSL VPN .</p> <p>4.9 Provide Intrusion Prevention System</p> <p>4.10 Provide Application Control</p> <p>4.11 Provide Antivirus</p> <p>4.12 Provide Anti-spyware</p> <p>4.13 Provide Advanced Network Threat Prevention</p> <p>4.14 Provide Zero-day protection</p> <p>4.15 Provide Threat Intelligence Technical Specification</p>		

Signature
11/12/2022

Signature



4.16	The device should support an IPS throughput of 5 Gbps or more	
4.17	The device should also support Threat Protection Throughput 1 Gbps or more	
4.18	NGFW Throughput 4 Gbps or more	
4.19	One power supply	
4.20	Option : Dual power supply .	
4.21	Minimum 6 Interfaces + 2 SFP+	
4.22	Interfaces requirements 10/100/1000, SFP+	
4.23	Provide UPL Filtering	
4.24	Provide reporting for (3) months.	
4.25	The firewalls must be equipped with all needed cables and transceivers for full connectivity.	


12/12/2022





5

Vulnerability Assessment testing tools**Comply/No
t Comply****Remarks**

The Solution Should include Tool and service to perform following: Vulnerability Management tool to cover all assets (500) with on-premise licensed tool with deployment ,configuration and training should be capable of following :-

5.1.1 - Identifying Vulnerabilities

5.1.2 - Evaluating Vulnerabilities

5.1.3 - Treating Vulnerabilities

5.1.4 - Reporting vulnerabilities and Remediation plan

5.2 The VA activities shall be comprehensive. It shall include (but not limited to) the following activities:

5.2.1 - Network scanning, port scanning, system scanning, vulnerability scanning, malware scanning, application security testing, access control testing, OS security testing, DB security testing.

5.3 Also, Bidder should offer following:

- Hardening service done quarterly during the free warranty period
- Overall Architecture and design review and assess.
- Vulnerability scanners.


11/14/2022