ބަންޑާރަނައިބުގެ އޮފީސް
މާލެ،
ދިވެހިރާއްޖެ.

Attorney General's Office
Male',
Republic of Maldives.

މުއާމަލާތުގެ ނަންބަރު (IUL)32-A2-PR/1/2024/17 (25 އޮކްޓޯބަރު 2024) އިއުލާނާއި ގުޅިގެން ދެވޭ މަޢުލޫމާތު:

އަންދާސީ ހިސާބު ހުށަހެޅުން:

- މި މަސައްކަތަށް އަންދާސީ ހިސާބު ހުށަހަޅާނީ 07 ޑީ 2024 ވާ އަންގާރަ ދުވަހުގެ 11:00 ގައި ބަންޑާރަނައިބުގެ އޮފީސް، ވެލާނާގެ 06 ވަނަ ފަންގިފިލާ އަށެވެ.

އަންދާސީ ހިސާބުހުށަހެޅުމުގައި ސަމާލުކަންދޭންވީ ކަންކަން:

- ޝެޑިއުލް 1 ގައިވާ މަސައްކަތުގެ ތަފްސީލަށް އަންދާސީހިސާބު ހުށަހަޅަންވާނެ.

އަންދާސީ ހިސާބާއެކު ހުށަހަޅަންޖެހޭ ލިޔުންތައް:

- އަންދާސީ ހިސާބު
- އަންދާސީ ހިސާބު ހުށަހަޅާ ފަރާތުގެ ވިޔަފާރި ރަޖިސްޓްރީގެ ކޮޕީ
- ޖީ.އެސް.ޓީ އަށް ރަޖިސްޓަރީ ކުރިކަމުގެ ލިޔުން
- އެސް.އެމް.އީ ރަޖިސްޓްރީ ކުރިކަމުގެ ލިޔުން
- ޓެކްސް ކްލިއަރަންސް ރިޕޯޓް
- މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓް އެންޑް ޓްރޭޑްގެ "ބިޒްނަސް ޕްރޮފައިލް އިސްކްރީންޝޮޓް" ގެ ކޮޕީ
- މަސައްކަތުގެ ތަޖުރިބާ ބަޔާންކުރާ ރިފަރެންސް ލެޓަރ (ރިފަރެންސް ލެޓަރގައި މަސައްކަތުގެ ތަފްސީލު، ފެށުނު ތާރީޚާއި، ނިމުނު ތާރީޚާއި ހިމެނިފައި އޮންނަންވާނެ)
- މަތީގައި މި ދެންނެވުނު ލިޔުންތަކުން ނުލާ އަންދާސީ ހިސާބުތަކާ މުޢާމަލާތު ހަމަނުވާ އަންދާސީ ހިސާބުތަކެއް ކަމުގައި ބަލައި އެ އަންދާސީ ހިސާބުތައް ބާތިލުކުރެވޭނެއެވެ.

ވެލާނާގެ 6 ވަނަ ފަންގިފިލާ
އަމީރު އަޙްމަދު މަގު، 20096

info@agoffice.gov.mv
www.agoffice.gov.mv

ފޯން +960 3010100
ފެކްސް +960 3314109

2 - ގަސްތަކުގެ ތަކެއްޗާއި ގުޅުންހުރި ކަންތައްތަކުގެ ޖުމްލަ ދަށުގައި ލިބޭ ގުނަ

ގަސްތަކުގެ ތަކެއްޗާ ގުޅުންހުރި ކަންތައްތަކުގެ ޖުމްލަ (ކުރިން ގަސްތުގެ ގުނަ) ގުނަ:

ގަސްތަކުގެ ތަކެއްޗާ ގުޅުންހުރި ކަންތައްތަކުގެ ޖުމްލަ ގުނަ ކަށަވަރުކުރުމަށް ތިރީގައިވާ ގޮތަށް ގުނަ ދީފައިވާ ކަންތައްތަކުގެ ގުނަ ބަލައި ބަލަންވާނެ.

- ތަކެއްޗާ ގުޅުންހުރި ކަންތައްތަކުގެ ގުނަ (ކުރިން ގަސްތުގެ ގުނަ / ކުރަންޖެހޭ ގަސްތުގެ ގުނަ × 65)

ދުވަސްތަކުގެ 30 (ތިރީސް) ގުނަ:

- ގަސްތަކުގެ ދުވަސްތަކުގެ ތެރެއިން 30 (ތިރީސް) ގުނަ ލިބޭ **ގަސްތަކުގެ ސިނާގަތުގެ ދުވަސްތަކުގެ ވަކިވަކި ގުނަ** ކަށަވަރުކުރަންވާނެ. ގުނަ ދީފައިވާ ގޮތަށް ކަންތައްތަކުގެ ގުނަ ބަލައި ކަންތައްތަކުގެ ގުނަ ތަކެއްޗާ ގުޅުންހުރި ގުނަ ތަކާ ބަލަންވާނެ.
  - ގަސްތަކުގެ ދުވަސްތަކުގެ (ކުރިން ގަސްތުގެ ދުވަސްތަކުގެ ކުރަންޖެހޭ ގަސްތުގެ / ކުރަންޖެހޭ ގަސްތުގެ ދުވަސްތަކުގެ × 30)

ތަފާތުތައް 5 (ފަސް) ގުނަ:

ތަފާތުތަކުގެ ގުނަ ކަށަވަރުކުރުމަށް ތިރީގައިވާ ގޮތަށް ގަސްތަކުގެ ކުރިން ގަސްތުގެ ތަކެއްޗާ ގުޅުންހުރި ތަފާތުތަކުގެ ތެރެއިން ބޮޑެތި ތަފާތު ތަކެއް ތަފާތުތަކުގެ ގުނަ ބަލަންވާނެ.
(ގުނަ ދީފައިވާ ގޮތަށް ގުނަ ދީފައިވާ 10 ތަފާތުތަކުގެ)

- (ކުރަންޖެހޭ ގަސްތުގެ ތެރެއިން ގަސްތަކުގެ ތަކެއްޗާ ގުޅުންހުރި ތަފާތުތަކުގެ ތެރެ ގަސްތަކުގެ ތަކެއްޗާ ގުޅުންހުރި ތަފާތުތަކުގެ / ގަސްތަކުގެ ތަކެއްޗާ ގުޅުންހުރި ތަފާތުތަކުގެ ގުނަ × 5)

އެނެކްސް

އެނެކްސް 1

Terms of Reference for Firewall Replacement for Attorney General's Office

Project Overview

The Attorney General's Office is looking to replace the existing firewall due to the product's end of life. The requirements for the project include the Design, supply, and Commissioning of a new Firewall with the Software Licensing Bundle. The supplier shall comply with the additional requirements for installation, Testing and Commissioning, Knowledge Transfer, Warranty, and Support.

1. Requirements

Physical specifications	
Mounting	1U rackmount (2 rackmount ears included)
Environment	
Power supply	Internal auto-ranging AC-DC 100-240VAC, 3-6A@50-60 Hz External Redundant PSU Option
Performance	
Firewall throughput	30,000 Mbps
Firewall IMIX	16,500 Mbps
Firewall Latency (64 byte UDP)	6 µs
IPS throughput	6,000 Mbps
Threat Protection throughput	1,250 Mbps
NGFW	5,200 Mbps
Concurrent connections	6,500,000
New connections/sec	134,700
IPsec VPN throughput	17,000 Mbps
IPsec VPN concurrent tunnels	5,000
SSL VPN concurrent tunnels	2,500
SSL/TLS Inspection	1,100 Mbps
SSL/TLS Concurrent connections	18,432
Physical Interfaces	
Storage (local quarantine/logs)	Integrated min. 120 GB SATA-III SSD
Ethernet interfaces	Minimum 6 GbE copper and 2 SFP fiber ports
Management ports	1 x RJ45 MGMT 1 x COM RJ45 1 x Micro-USB (cable incl.)
Other I/O ports	2 x USB 3.0 (front) 1 x USB 2.0 (rear)
Number of Flexi Port slots	1

ފޯން +960 3010100
ފެކްސް +960 3314109
info@agoffice.gov.mv
www.agoffice.gov.mv
ވެލާނާގެ 6 ވަނަ ފަންގިފިލާ
އަމީނީ މަގު، މާލެ، 20096

Display	Multi-function LCD module
Network size	150 users
License	1-year subscription

Throughput: The firewall should support high throughput to handle network traffic efficiently without causing bottlenecks. It should provide adequate performance for both inbound and outbound traffic.

Security Features: The firewall should offer a comprehensive set of security features, including Stateful Packet Inspection (SPI), Intrusion Detection and Prevention System (IDPS), Deep Packet Inspection (DPI), application control, antivirus/anti-malware, and content filtering capabilities.

Scalability: The firewall should be scalable to accommodate the organization's growth. It should support the addition of new users, devices, and applications without compromising performance or security.

Redundancy: Redundant hardware components, such as power supplies and network interfaces, should be available to minimize single points of failure and enhance reliability.

VPN Support: The firewall should provide robust VPN (Virtual Private Network) support for secure remote access and inter-site connectivity. It should support various VPN protocols, including IPsec, SSL VPN, and L2TP/IPsec.

Traffic Management: Advanced traffic management features, such as Quality of Service (QoS), bandwidth management, and traffic shaping, should be available to prioritize critical applications and ensure optimal network performance.

Centralized Management: The firewall should offer centralized management capabilities for easy configuration, monitoring, and maintenance of multiple devices from a single interface. It should support role-based access control (RBAC) and integration with management platforms.

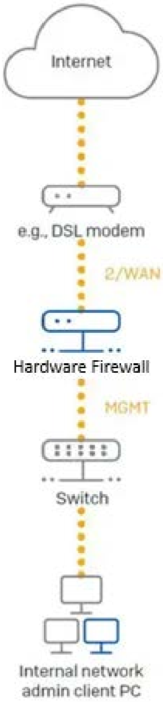
Logging and Reporting: Comprehensive logging and reporting capabilities should be included to monitor network activity, analyze security events, and generate compliance reports. The firewall should support logging to external SIEM (Security Information and Event Management) systems.

Compliance: The firewall should comply with industry regulations and standards, such as GDPR, PCI DSS, HIPAA, and SOX. It should support features and configurations necessary for achieving and maintaining regulatory compliance.

Integration: Integration with other security solutions, such as endpoint protection, threat intelligence platforms, and security analytics tools, should be supported to enhance overall security posture and threat visibility.

+960 3010100 ފޯނު
+960 3314109 ފެކްސް
info@agoffice.gov.mv
www.agoffice.gov.mv
ވެލާނާގެ 6 ވަނަ ފަންގިފިލާ
އަމީރު އަޙްމަދު މަގު، 20096

2. Network layout



3. Needs Analysis and Proposal:

The vendor shall analyze the Attorney General's Office network and firewall requirements. Based on the findings, the vendor shall propose a suitable product that aligns with the organizational network needs. The proposal should include detailed cost breakdowns for the supply and installation setup of the approved firewall solution.

4. Supply and Delivery:

Upon agreement signing, the vendor shall supply the firewall to the Attorney General's Office. The delivered firewall must include all necessary licenses and subscriptions to ensure immediate functionality upon installation.

5. Installation and Configuration:

The vendor shall complete the firewall's setup and configuration within 7 (seven) days of its delivery. The installation must be done by an OEM-certified architect or engineer. This setup must adhere to the specific network requirements of the Attorney General's Office.

6. Installation and Firmware Updates:

The firewall shall be securely installed in the server room using rack-mounting hardware. The vendor shall ensure the firewall's firmware is up-to-date by applying any available updates.

7. Configuration Migration:

The vendor shall transfer the configuration settings from the backup file to the new firewall if they are compatible with the previous firewall. Alternatively, the vendor shall recreate network configurations and routing rules as necessary to maintain the operational continuity of the Attorney General's Office network.

8. Testing and Verification:

Following configuration setup, the vendor shall verify that all settings have been accurately implemented on the new firewall. The Attorney General's Office will conduct comprehensive testing to confirm network connectivity and functionality, including WAN and firewall rules. If any issue is identified, the vendor shall immediately rectify the problem.

9. Training and Support:

The vendor shall provide training sessions for network administrators and staff members on the usage of the new firewall interface and its features. Additionally, training shall be provided on setting up monitoring tools for performance and security.

10. Warranty and Support:

The vendor shall provide a one-year manufacturer warranty and support service for the firewall solution. This warranty shall cover any defects or malfunctions encountered during normal usage. The servicing, whenever required, must be provided by a certified Architect or Engineer.