**Network Security Appliances**

1. **Overview:**

The Requesting Unit (RU)is looking to enhance its Cybersecurity defense by implementing multiple layers of security from the best security vendors. The Solution is composed of two Cisco Next Generation Firewalls for Data Center with one Firepower Management Center (FMC) virtual machine, two Palo Alto firewalls for internet perimeter and WAF from Barracuda. Moreover the RU is looking to replace its current core switches with new high performance redundant Cisco 9606 switches. The existing core switches will be moved to a new location where they will be implemented and configured.

1. **Project Management Plan:**

The bidders shall assign a dedicated project manager who serves as focal point of contact for project status reporting, follow up and escalation.

The bidders shall manage the whole project including supply, installation, configuration, testing, commissioning and integration with the existing LAN, WLAN, WAN, Internet, and existing monitoring applications.

The bidder should be a Cisco, Barracuda and PaloAlto Gold partner or above in Lebanon and shall assign an engineer certified (PNCSE and CCNP Security), specialized and experienced in Network Security for more than 5 years, and 3 years in Vendor’s P/Ns, who shall be responsible for designing, leading, supervising the daily implementation tasks and commissioning of the complete solution.

The bidders are required to provide an implementation plan illustrating all testing, staging, and deployment activities. In addition, bidders are required to specify and describe their deliverables in each phase of the project including but not limited to the following:

* **Initiation phase:**
	+ Kickoff meeting to set project milestones
	+ Communication Management Plan
	+ Escalation Process
* **Planning and design phase:**
	+ Assess the existing network design and configuration, gather all information required to start the project.
	+ Clean unused configuration
	+ Suggest enhancements in terms of design and configuration
	+ Deliverables:
		- Detailed project plan
		- High level design
		- Low level design
		- Network implementation plan
		- User Acceptance Test (UAT) including but not limited to:
			* High availability testing
			* Routing
			* Applications
			* Services
			* Malware simulation
			* Performance under full load conditions
			* Vendor configuration assessment tool
		- Detailed migration methodology (Noting that migration will be scheduled after working hours, weekends or public holidays)
		- Risk Assessment and Down Time estimation.
		- Rollback procedure
	+ Discuss and approve documents by customer and by vendor when required
* **Execution phase**
	+ Validate that all devices are properly functioning and replace any malfunctioning or “Dead on Arrival” devices
	+ Unmount existing devices
	+ Mount all devices in their corresponding racks
	+ Connect, organize and label required power and data (including copper and fiber) cables
	+ Configure initial setup of all devices
	+ Install licenses
	+ Upgrade to latest recommended release
	+ Configure High Availability
	+ Deploy configuration on firewalls and switches based on planning documents
	+ Go through all Testing scenarios using the previously prepared User Acceptance Test document
	+ Rollback if necessary and document the issues that caused the rollback
* **Closure** **phase**
	+ As built documentation
	+ Knowledge transfer

**The Scope will include the below phases but GSF has the right to request any additional work without any charges from the supplier.**

1. **Scope of Work:**
* **Cisco Data Center Firewalls**

Configurationof Cisco Data Center Firewalls need to contain (but not limited to) the following list:

* + Deploy FMC Virtual Machine on existing servers that will manage firewalls (including hypervisor installation)
	+ Connect Cisco firewalls to FMC
	+ Configure High Availability
	+ Upgrade all devices to latest and recommended release
	+ IP Addressing on interfaces/zones
	+ MTU change
	+ L2 interfaces when required
	+ Routing (destination-based routing, source-based routing, tracking of destinations and dynamic routing)
	+ NAT
	+ Link Aggregation
	+ Logging
	+ Customized Security Policies (IPS, Anti Malware, Days Zero Attacks, file control and blocking…)
	+ Optimize security policies based on customer needs and eliminate false positives
	+ DNS Security and Sinkhole
	+ URL Filtering using categories, custom URLs, geolocation, regex…
	+ Application visibility and control
	+ SSL Decryption
	+ Handle Encrypted Traffic
	+ Integration with third party devices/appliances such as AAA, SNMP, Netflow, syslog, LDAP, email server…
	+ Integration with threat intelligence list
	+ Custom Applications to identify all internal applications
	+ Advanced Network Analysis and Preprocessing
	+ Correlation Rules and Responses Group
	+ Customized Reports and Dashboards
	+ Network Discovery and Identity
	+ Configure Service Policies to protect TCP applications
	+ Custom HTTP Response Page and Interactive Blocking
	+ 5 years 24x7 onsite SLA
* **Palo Alto Internet Firewalls**

Configurationof Palo Alto Internet Firewalls need to contain (but not limited to) the following list:

* + Upgrade all devices to latest and recommended release
	+ IP Addressing on interfaces/zones
	+ MTU change
	+ Routing (destination-based routing, source-based routing, tracking of destinations and dynamic routing)
	+ NAT
	+ Link Aggregation
	+ Configure High Availability
	+ Logging
	+ Customized Security Policies (IPS, Anti Malware, Days Zero Attacks, file control and blocking…)
	+ Optimize security policies based on customer needs and eliminate false positives
	+ Botnet/CnC connections blocking
	+ DNS Security and Sinkhole
	+ URL Filtering using categories, custom URLs, geolocation, regex…
	+ Application visibility and control
	+ SSL Decryption
	+ Handle Encrypted Traffic
	+ Integration with third party devices/appliances such as AAA, SNMP, Netflow, syslog, LDAP, email server…
	+ Custom Applications to identify all internal applications
	+ Customized Reports and Dashboards
	+ Antivirus, Anti-Spyware, Vulnerability Protection
	+ Data Filtering and File Blocking Protection
	+ Denial of Service Protection Profiles
	+ DNS Security and Sinkhole
	+ Flood Protection
	+ Reconnaissance Protection (TCP Port scan, Host Swap, UDP Port Scan)
	+ Packet Based attack Protection
	+ Integration with External monitoring tools
	+ Configure Layer 7 based rules
	+ Integration with External Dynamic Lists
	+ Configure RBAC
	+ Apply configuration Best Practices
	+ 5 years 24x7 onsite SLA
	+ Migrate the VPN client (with all its security features) from Cisco ASA to Palo Alto FW and integrate it with VIP OTP (Symantec) for remote users.
* **Cisco Core Switches**

Implementation and Configurationof 2 Cisco 9606 Core Switches needs to include (but not limited to) the following:

* + Remove 2 existing Cisco 6807 core switches (overnight), then install and configure them in another site that will be specified in a later stage.
	+ Upgrade switches to latest recommended release
	+ High availability
	+ Interface MTU
	+ VLANs
	+ VTP
	+ Trunks
	+ Spanning-tree protocol
	+ Link Aggregation
	+ HSRP
	+ Security features such as:
		- Layer 2 security
		- Root guard
		- BPDU Guard
		- DHCP Snooping
		- IP Source guard
		- Private VLANs
		- Protected ports
		- Dynamic ARP Inspection
		- Port-level traffic controls
		- Disable unused services
		- Management security (ACL, SSH, HTTPS…)
	+ Access Control Lists (IP, MAC, VLAN…)
	+ Integration with third party devices/appliances such as AAA, SNMP, Netflow, syslog, LDAP, email server…
	+ 5 years 24x7 onsite SLA
* **Barracuda Web Application Firewalls**

Implementation and Configurationof 2 Barracuda WAF 862 needs to include (but not limited to) the following:

* + Remove 2 existing Barracuda WAF 660, then install and configure them in another site.
	+ Upgrade WAFs to latest recommended release
	+ High availability
	+ Networking and Routing
	+ Logging, Monitoring and Reporting
	+ Migration of application from 660 to 862
	+ Adding 10 additional web applications
	+ Security Policies
	+ Bot Mitigation Policies
	+ Application Delivery
	+ Access Control
	+ SSL/TLS
	+ 5 years 24x7 onsite SLA

Implementation and Configurationof 2 Barracuda WAF 660 needs to include (but not limited to) the following:

* + Upgrade WAFs to latest recommended release
	+ High availability
	+ Networking and Routing
	+ Logging, Monitoring and Reporting
	+ Adding 10 web applications
	+ Security Policies
	+ Application Delivery
	+ Access Control
	+ SSL/TLS
	+ 5 years 24x7 onsite SLA
* **Data Center organization**

Each bidder is requested to do a site survey to the main datacenter of GSF to assess the needed requirement for a proper re-arrangement and re-organization of the cabinets. The bidder will be responsible to execute the job and supply the needed accessories. All related work will be done during weekend/outside working hours.

**NB: GSF has the right to request any additional work related to this project without any charges from the supplier.**

**Required Cisco, Palo Alto and Barracuda BOQ:**

**Cisco Firewalls**

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| FPR4112-BUN | Cisco Firepower 4112 Master Bundle | 1 |
| FPR4112-NGFW-K9 | Cisco Firepower 4112 NGFW Appliance, 1U, 2 x NetMod Bays | 2 |
| FPR4K-PWR-AC-1100 | Firepower 4000 Series 1100W AC Power Supply | 2 |
| SF-F4K-TD6.6-K9 | Cisco Firepower Threat Defense software v6.6 for FPR4100 | 2 |
| SF-F4KFXOS2.8.1-K9 | Cisco Firepower Extensible Operating System v2.8.1 - FPR4100 | 2 |
| CAB-AC-EUR | Power Cord - Europe, 16/10A,250V, 2500mm, -40C to +85C | 4 |
| FPR4K-NM-BLANK | Firepower 4000 Series Network Module Blank Slot Cover | 2 |
| FPR4K-PWR-AC-1100 | Firepower 4000 Series 1100W AC Power Supply | 2 |
| FPR4K-S-FAN- | Firepower 4000 Series Fan - Siingle | 12 |
| FPR4K-RACK-MNT | Firepower 4000 Series Rack Mount Kit | 2 |
| FPR4K-ACC-KIT2 | FPR4K Hardware Accessory Kit | 2 |
| GLC-TE | 1000BASE-T SFP transceiver module for Category 5 copper wire | 2 |
| SFP-H10GB-ACU7M | Active Twinax cable assembly, 7m | 8 |
| FPR4K-SSD400- | Firepower 4000 Series 400GB SSD for FPR-4125 | 2 |
| FPR4K-SSD-BBLKD | Firepower 4000 Series SSD Slot Carrier | 2 |
| CON-SNT-FPR41FWK | 5 years SNTC-8X5XNBD Cisco Firepower 4112 NGFW Appliance, 1U, | 2 |
| L-FPR4112T-TM= | Cisco FPR4112 Threat Defense Threat and Malware License | 2 |
| L-FPR4112T-T-5Y | Cisco FPR4112 Threat Defense Threat and malware for 5YEARS Subs | 2 |
| SF-FMC-VMW-2-K9 | Cisco Firepower Management Center, (VMWare) for 2 devices | 1 |
| CON-ECMU-SFMMCVWK | 5 years SWSS UPGRADES Cisco Firepower Management Center, (VMWare) for 2 devices | 1 |
| SFP-10G-SR-S | 10GBASE-SR SFP Module, Enterprise-Class | 8 |
| FPR4K-NM-8X1G-F | Cisco FirePower 8 port 1G Copper FTW Network Module | 8 |

**Training**

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| **Cisco Firepower** | Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System (SSFIPS) | 2 persons |
| Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW) v1.0 | 2 persons |

**Cisco Core Switch**

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| **C9606R** | Cisco Catalyst 9600 Series 6 Slot Chassis | 2 |
| CON-SNT-C9606R | 5 years SNTC-8X5XNBD Cisco Catalyst 9600 | 2 |
| C9600-NW-A | Cisco Catalyst 9600 Network Advantage License | 2 |
| S9600UK9-173 | Cisco Catalyst 9600 XE 17.3 UNIVERSAL | 2 |
| C9600-CAMPUS-CORE | Catalyst 9600 Campus Core Deployment; For Tracking Only | 2 |
| C9606-FAN | Cisco Catalyst 9600 Series C9606 Chassis Fan Tray | 2 |
| CAB-CONSOLE-USB | Console Cable 6ft with USB Type A and mini-B | 2 |
| C9606-SLOT-BLANK | Cisco Catalyst 9600 Series Blank for Chassis Module Slot | 2 |
| C9600-DNA-A | Cisco Catalyst 9600 DNA Advantage Term License | 2 |
| C9600-DNA-A-3Y | Cisco Catalyst 9600 DNA Advantage 3 Year License | 2 |
| PI-LFAS-T | Prime Infrastructure Lifecycle & Assurance Term - Smart Lic | 6 |
| PI-LFAS-AP-T-3Y | PI Dev Lic for Lifecycle & Assurance Term 3Y | 6 |
| C9600-SUP-1 | Cisco Catalyst 9600 Series Supervisor 1 Module | 2 |
| C9K-F2-SSD-960GB | Cisco Catalyst 9600 Series 960GB SSD Storage | 2 |
| C9600-LC-24C | Cisco Catalyst 9600 Series 24-Port 40GE/12-Port 100GE | 2 |
| QSFP-40G-SR-BD | QSFP40G BiDi Short-reach Transceiver | 24 |
| C9600-LC-48YL | Cisco Catalyst 9600 Series 48-Port 25GE/10GE/1GE | 2 |
| SFP-10G-SR-S | 10GBASE-SR SFP Module, Enterprise-Class | 48 |
| C9600-LC-48TX | Cisco Catalyst 9600 Series 48-Port Copper | 2 |
| C9600-LC-48YL | Cisco Catalyst 9600 Series 48-Port 25GE/10GE/1GE | 2 |
| C9600-PWR-2KWAC | Cisco Catalyst 9600 Series 2000W AC Power Supply | 8 |
| CAB-TA-EU | Europe AC Type A Power Cable | 8 |
| NETWORK-PNP-LIC | Network Plug-n-Play Connect for zero-touch device deployment | 2 |
| CON-SNT-6807S2TB | 5 years SNTC-8X5XNBD Chassis+Fan Tray+ Su | 2 |

**Training**

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| **Cisco Core Switch** | Advanced routing and switching | 2 persons |

**Accessories:**

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| SFP-H10GB-CU5M= | 10GBASE-CU SFP+ Cable 5 Meter | 16 |
| QSFP-H40G-CU5M= | 40GBASE-CR4 Passive Copper Cable, 5m | 16 |
| SFP  | Single Mode, 1Gb | 14 |
| Services | Installation and configuration | LS |
| Patch Cords | American or European Patch cords, LC-LC, OM3, 50um, 5 meters | 40 |
| Patch Cords | American or European Patch cords, LC-LC, OM3, 50um, 10 meters | 60 |
| Patch Cords | American or European Single mode, UPC SC to LC , 3 meters | 4 |
| Patch Cords | American or European Single mode, UPC SC to LC , 10 meters | 8 |
| LEVITON Opt-X 500i 1RU Flush Mount Fiber Distribution and Splice Enclosure, accepts up to 3 Adapter Plates or MTP Modules/cassettes, Empty | 2 |
| LEVITON SM, FO cable 24 cores, outdoor anti rodent | 2000 |
| LEVITON FIBER PIGTAIL LC 9/125 SM | 48 |
| LEVITON FIBER ADAPTER 24F | 2 |
| LEVITON SPLICE TRAY 24F | 2 |
| LEVITON LC-LC Patch Cord duplex SM 9/125 (OS2) 2m | 12 |

**Cisco Edge Switches**

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| C1000-8P-2G-L | Cisco Catalyst 1000 8port GE, POE, 2x1G SFP | 50 |
| CAB-ACE | AC Power Cord (Europe), C13, CEE 7, 1.5M | 50 |

**HP Servers DL380 (Qty:/2/)**

|  |  |  |
| --- | --- | --- |
| **Item** | **Description** | **Qty** |
| **HPE ProLiant DL380 Gen10 8SFF / 2P Intel Xeon-Gold 5218 2.3GHz, 16-core / 256GB RAM / 6x 900GB SAS 15K HDD / Smart Array P408i-a, 2GB cache + Smart Storage battery / Embedded 4-port 1GbE / Ethernet 10Gb 2-port SFP+ / 2x 10Gb SFP+ SR Transceiver / 2x 800W RPS Qty: /2/** |
| P20249-B21 | HPE ProLiant DL380 Gen10 8SFF | 2 |
| 1P Intel Xeon-Gold 5218 (2.3GHz/16-core/125W) FIO Processor Kit |
| P408i-a/2GB with Smart Storage Battery |
| 32 GB RDIMM 2R 2933 MT/s |
| Ethernet 1Gb 4-port |
| 1x 800W Power Supply |
| 2U Rack |
| 3 years warranty |
| P02498-B21 | Intel Xeon-Gold 5218 (2.3GHz/16-core/125W) | 2 |
| P00924-B21 | HPE 32GB 2Rx4 PC4-2933Y-R Smart Kit | 14 |
| 865414-B21 | HPE 800W Flex Slot Platinum Hot Plug Low Halogen Power Supply Kit | 2 |
| 455883-B21 | HPE BladeSystem c-Class 10Gb SFP+ SR Transceiver | 4 |
| 652503-B21 | HPE Ethernet 10Gb 2-port SFP+ 57810S Adapter | 2 |
| 870759-B21 | HPE 900GB SAS 12G Enterprise 15K SFF (2.5in) SC 3yr Wty Digitally Signed Firmware HDD | 12 |

 **Barracuda New Appliances 862**

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| BWFi862C | Barracuda Web Application Firewall 862 w/ Fiber NIC & Bypass | 2 |
| BWFi862a-e | Barracuda Web Application Firewall Appliance 862 Energize Updates Subscription 60 Months | 2 |
| BWFi862a-h | Barracuda Web Application Firewall Appliance 862 Instant Replacement Subscription 60 Months | 2 |

**Barracuda support renewal for existent appliances**

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| BWFi660a-e | Barracuda Web Application Firewall Appliance 660 Energize Updates Subscription **(to be co-term with the new appliances, same expiry date)** | 1 |
| **Training** |  |  |
| **P/N** | **Description** | **Qty** |
| **Barracuda** | Barracuda Web Application Firewall – Foundation WAF01 (2Days) – Online Distance Learning Conducted by an Authorized Training Center | 2 persons |
| Barracuda Web Application Firewall - Advanced Features WAF0201 (1Day) – Online Distance Learning Conducted by an Authorized Training Center | 2 persons |

**PaloAlto 3410 BOQ**

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| PAN-PA-3410 | Palo Alto Networks PA-3410 with redundant AC power supplies | 2 |
| PAN-PA-3410-TP-5YR-HA2 | Threat prevention subscription 5 years prepaid for device in an HA pair, PA-3410 | 2 |
| PAN-PA-3410-ADVURL-5YR-HA2 | Advanced URL filtering subscription 5 years prepaid for device in an HA pair, PA-3410 | 2 |
| PAN-PA3410-DNS-5YR-HA2 | DNS Security subscription 5 years prepaid for device in an HA pair, PA-3410 | 2 |
| PAN-PA-3410-GP-5YR-HA2 | GlobalProtect subscription 5 years prepaid for device in an HA pair, PA-3410 | 2 |
| PAN-SVC-BKLN-3410-5YR | Partner enabled premium support 5-years prepaid, PA-3410 | 2 |

**Training**

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| EDU-210 | PaloAlto official training firewall 10.0 essentials; configuration and management | 2 persons |

1. **Support**

Bidder shall consider in his offer an onsite SLA for a period of 5 years which is capable of supporting the implemented solution based on the following conditions:

* + 24x7 ON-SITE
	+ 2 hours maximum response time
	+ Replacement of failed hardware within 24hrs/Next business day from the time call is logged
	+ Warranty includes all software subscriptions (critical hot fixes, service packs, and major upgrades) for a period of 5 years
	+ Software updates, upgrades and patching during period of warranty at no additional cost.
	+ Perform preventive maintenance every /3/ months for all network security appliances.
	+ The SLA will start after project completion and sign off.
1. **Documentation:**
* The supplier must submit complete implementation and operations documentation that shall reflect all the set up and configuration of the implementation performed in GSF.
* The project should be fully documented (Soft and hard copies). The soft copy must be in “.docx” format and contains all the configuration files and Visio drawings in “.vsd” format.
1. **Staffing & Team Experience:**
* Provider is requested to provide details on the implementation and support team:
	+ Number and details of the team Certifications.
	+ Level of expertise.
1. **Training**
* The bidders shall provide onsite hand-over and training session about how to install, operate, support, and manage the new implemented solutions

(Cisco Core Switches, Cisco Firepower, Barracuda Firewalls, PaloAlto Firewalls)

* The training must cover all levels from fundamental up to Advanced. The bidder shall also provide a customized training to be able to migrate to the new firewall platform.
* Moreover, trainings led by a certified training center are required as per the below table.

|  |  |  |
| --- | --- | --- |
| **P/N** | **Description** | **Qty** |
| **Cisco Core Switch** | Advanced routing and switching | 2 persons |
| **Cisco Firepower** | Securing Networks with Cisco Firepower Next-Generation Intrusion Prevention System (SSFIPS) | 2 persons |
| Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW) v1.0 | 2 persons |
| **PaloAlto**  | PaloAlto official training firewall 10.0 essentials; configuration and management | 2 persons |
| **Barracuda** | Barracuda Web Application Firewall – Foundation WAF01 (2 Days) – Online Distance Learning Conducted by an Authorized Training Center | 2 persons |
| Barracuda Web Application Firewall - Advanced Features WAF0201 (1 Day) – Online Distance Learning Conducted by an Authorized Training Center | 2 persons |