TERMS OF REFERENCE
FOR THE PROCUREMENT OF FIREWALL (3 years license) FOR THE DEPARTMENT OF JUSTICE MAIN and NATIONAL PROSECUTION SERVICE OFFICES

A. BACKGROUND

The DOJ NPS-NCR offices is subscribing internet connectivity to be used for email, research and in preparation for the implementation of Prosecution Case Management System (PCMS) which connects the NPS NCR offices through Virtual Private Network (VPN) to the main server in DOJ Main. PCMS is scheduled to be deployed on the 3rd quarter of 2017. Each NCR office will be provided with a firewall to provide perimeter/network security especially coming from the internet.

B. PROJECT DESCRIPTION

This project involves supply, delivery, installation, configuration, and testing of 20 units firewall and 1 unit management appliance to be deployed in DOJ Main and NPS Offices.

C. APPROVED BUDGET FOR THE CONTRACT

The Approved Budget for the Contract (ABC) is Php10,007.055.00 inclusive of all taxes and charges.

D. QUALIFICATIONS OF BIDDER

1. Prospective bidder/s should be duly authorized by the manufacturer/distributor to provide, sell, configure and support the firewall and management appliance.

   The certification from the manufacturer/distributor authorizing the prospective bidder to provide such product should be submitted together with the bid proposal. Bid proposals that do not include the Certification shall not be accepted/considered for award.

2. Prospective bidder/s should have at least two (2) certified security professionals. Training certificates of the certified security professionals should be attached to the bid proposal.

3. Bidder must have the capacity to escalate product technical issues directly to the manufacturer.

4. Any and all costs necessary for the bidder to fulfill its obligations in the supply, delivery, installation and commissioning of the firewall shall be deemed included in the financial proposal. Any cost incurred in the fulfillment of the obligations but were not included in the financial proposal shall be shouldered by the bidder with the lowest complying quotation

E. PROJECT DELIVERABLES

1. Documentation – Provide users guide and technical manuals.

2. Training - Provide a comprehensive certification training relative to all firewall and management appliance proposed for at least five (5) MISD personnel.

F. DELIVERY PERIOD AND PLACE OF DELIVERY

The winning bidder shall supply and deliver the set of equipment sixty (60 c.d.) calendar days from receipt of the Purchase Order (PO) at the DOJ Central Office located at Ermita Manila.

G. TECHNICAL SPECIFICATIONS

Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specifications and compliance issued by the manufacturer, samples, independent test data etc., as appropriate.

A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or suppler liable for prosecution.

Item I. Firewall/UTM Appliance for Head Office (Minimum Specifications)				
Item No.	Particulars	Description	Comply Yes/No	Bidder's Offer
1.1	Form Factor	• Rack Mountable 2RU		
1.2	Certification	ICSA Labs: Firewall, IPSecs, IPS, Antivirus, SSL VPN or its equivalent		
1.3	Compliance	• Safety Certifications: FCC Part 15 Class A, C – Tick, VCCI, CE, UL/cUL, CB		
1.4	Features	• Comprehensive threat protection that delivers the following. ✓ Firewall ✓ IPS ✓ VPN (IPsec and SSL) ✓ Web Filtering ✓ Anti-Virus ✓ APT (Advance Persistent Threat) ✓ Anti-Spam ✓ DLP (Data Loss Prevention)		

		✓ Botnet/IP Domain ✓ Mobile Security Services • Wireless Intrusion Detection System (WIDS) with built-in wifi or its equivalent • Virtual WAN (able to detect link quality on jitter or Latency) • ASIC or Intel based standalone appliance • Comprehensive protection against network, content and application-level threats without degrading network availability and affecting application performance. • Real-time content scanning to block threats, control web surfing and control data/file transfers • Securely enable applications on networks based on users and groups and IP addresses • Application control, data loss prevention, dynamic routing (IPv4 & IPv6), endpoint NAC, SSL-encrypted traffic inspection, and WAN Optimization • Internet connection load balancing and failover capabilities		
1.5	Hardware Specifications	• 8 x 10-GbE SFP+ Interfaces • 16 x 10/100/1000 Interfaces (RJ-45) • 16 x Accelerated GbE SFP • 10/100/1000 Bypass Interfaces • 2 x 10/100/1000 Management Interface • 1 Console RJ-45 Port • 1 USB Ports • 2 x 240 Gbps Internal storage • Redundant power supply		
1.6	Performance	• Minimum of 80/80/55 Gbps Firewall throughput (IPv4 and IPv6) • Minimum of 82.5 Mpps Firewall Throughput (Packet per Second) • Minimum of 50 Gbps IPsec VPN throughput • Minimum of 4 Gbps SSL VPN throughput • Supports 20,000 Gateway to Gateway IPSec VPN Tunnels • Supports 50,000 Client to Gateway IPSec VPN Tunnels • Must have 11 Gbps IPS throughput		

		• Supports 12Gbps Application Control throughput • Supports 7Gbps NGFW throughput • Supports 5Gbps Threat Protection throughput • Supports 12 Million concurrent sessions • Supports 300,000 new session per second • Up to 100,000 Firewall Policies • Up to 10,000 Concurrent SSL-VPN Users • Must support local virtualization with 10 Default Virtual Domains • Supports up to 1024 tunnels and 4,096 bridge number of APs • Supports two factor authentication • Supports up to 8,000 Maximum number of registered clients • High availability configurations: Active/Active, Active/Passive, Clustering • Unlimited user licenses		
1.7	Management	• Easy to manage via web (http and https) and CLI (ssh and telnet) • Granular policy enforcement • Must have the capability to generate report		
1.8	Support	• Three (3) Years (8x5) enhanced support including all necessary security subscription services and firmware upgrades • Three (3) Years software warranty against media defect • Original media kits and manuals • Unlimited phone and email support		
1.9	Warranty	• Three (3) Years on all parts and service • Three (3) Years email, call and remote services • In case of equipment failure, a service unit equal to or with higher specifications than the existing equipment shall be provided pending the replacement of said unit.		

Item III. 8 units of Firewall/UTM Appliance for Remote Sites (Minimum Specifications)				
Item No.	Particulars	Description	Comply Yes/No	Bidder's Offer

1.1	Form Factor	• Rackmount 1RU		
1.2	Certification	ICSA Labs: Firewall, IPSecs, IPS, Antivirus, SSL VPN or its equivalent		
1.3	Compliance	• Safety Certifications: FCC Part 15 Class A, C – Tick, VCCI, CE, UL/cUL, CB		
1.4	Features	• Comprehensive threat protection that delivers the following. ✓ Firewall ✓ IPS ✓ VPN (IPsec and SSL) ✓ Web Filtering ✓ Anti-Virus ✓ APT (Advance Persistent Threat) ✓ Anti-Spam ✓ DLP (Data Loss Prevention) ✓ Botnet/IP Domain • Wireless Intrusion Detection System (WIDS) with built-in wifi or its equivalent • Virtual WAN (able to detect link quality on jitter or Latency) • ASIC or Intel based standalone appliance • Comprehensive protection against network, content and application-level threats without degrading network availability and affecting application performance. • Real-time content scanning to block threats, control web surfing and control data/file transfers • Securely enable applications on networks based on users and groups and IP addresses • Application control, data loss prevention, dynamic routing (IPv4 & IPv6), endpoint NAC, SSL-encrypted traffic inspection, and WAN Optimization • Internet connection load balancing and failover capabilities		
1.5	Hardware Specifications	• 40 x GE RJ 45 Ports • 2 x GE SFP Ports • 1 Console RJ-45 Port • 1 USB Ports • 32GB internal Storage		

1.6	Performance	• Minimum of 2.5Gbps Firewall throughput • Minimum of 300 Kpps Firewall Throughput (Packet per Second) • Minimum of 450 Mbps IPsec VPN throughput (512 byte packets) • Minimum of 300 Mbps SSL VPN throughput • Supports 2000 Gateway to Gateway IPSec VPN Tunnels • Supports 5000 Client to Gateway IPSec VPN Tunnels • Must have 950/310 Mbps IPS throughput (HTTP/Enterprise Mix) • Supports 2 Million concurrent sessions • Supports 22,000 new session per second • Up to 10,000 Firewall Policies • Up to 300 Concurrent SSL VPN Users • Must support local virtualization with 10 Default Virtual Domains • Supports up to 32 tunnel mode number of APs • Supports up to 1000 Maximum number of Tokens • Supports unlimited number of registered clients • High availability configurations: Active/Active, Active/Passive, Clustering • Unlimited user licenses		
1.7	Management	• Easy to manage via web (http and https) and CLI (ssh and telnet) • Granular policy enforcement • Must have the capability to generate report		
1.8	Support	• Three (3) Years (8x5) enhanced support including all necessary security subscription services and firmware upgrades • Three (3) Years software warranty against media defect • Original media kits and manuals • Unlimited phone and email support		
1.9	Warranty	• Three (3) Years on all parts and service • Three (3) Years email, call and remote services • In case of equipment failure, a service unit equal to or with higher specifications than the		

		existing equipment shall be provided pending the replacement of said unit.		

Item IV. 12 units Firewall/UTM for Branches (The proposed firewall should have built in Wi-Fi capability)				
Item No.	Particulars	Description	Comply Yes/No	Bidder's Offer
2.1	Form Factor	• Desktop		
2.2	Certification	ICSA Labs: Firewall, IPSecs, IPS, Antivirus, SSL VPN or its equivalent		
2.3	Compliance	• Safety Certifications: FCC Part 15 Class A, C – Tick, VCCI, CE, UL/cUL, CB		
2.4	Features	• Comprehensive threat protection that delivers the following. ✓ Firewall ✓ IPS ✓ VPN (IPsec and SSL) ✓ Web Filtering ✓ Anti-Virus ✓ APT (Advance Persistent Threat) ✓ Anti-Spam ✓ DLP (Data Loss Prevention) ✓ Botnet/IP Domain • Wireless Controller with built-in dual-band, dual-stream access point with internal antennas, 802.11n coverage on both 2.4 GHz and 5 GHz bands. • ASIC or Intel based standalone appliance • Comprehensive protection against network, content and application-level threats without degrading network availability and affecting application performance. • Real-time content scanning to block threats, control web surfing and control data/file transfers • Securely enable applications on networks based on users and groups and IP addresses • Application control, data loss prevention, dynamic routing (IPv4 & IPv6), endpoint NAC, SSL-encrypted traffic inspection, and WAN Optimization • Internet connection load balancing and failover capabilities		
2.5	Hardware Specifications	• Must have 2 GbE RJ45 Wan Port • Minimum of 14 GbE RJ45 Switch Ports		

		• Must have Wireless Interface 802.11a/b/g/n • Must have 2 USB Ports		
2.6	Performance	• Supports 3.5 Gbps Firewall throughput • Supports 5.3 Mpps Firewall Throughput (Packets per Second) • Supports 1Gbps IPsec VPN throughput • Supports 35 Mbps SSL VPN throughput • Supports up to 200 Gateway to Gateway IPSec VPN Tunnels • Supports up to 1000 Client to Gateway IPSec VPN Tunnels • Supports 275/41 Mbps IPS throughput (HTTP/Enterprise Mix) • Supports 22.5mbps Threat Protection throughput • Supports 25Mbps NGFW throughput • Supports up to 2,000,000 concurrent sessions • Supports up to 4,000 new session per second • Up to 5,000 Firewall Policies • Up to 200 Concurrent SSL VPN Users • Up to 100 Maximum number of Tokens • Up to 200 Maximum number of registered clients • High availability configurations: Active/Active, Active/Passive, Clustering • Unlimited user licenses		
2.7	Management	• Easy to manage via web (http and https) and CLI (ssh and telnet) • Granular policy enforcement • Must have the capability to generate report		
2.8	Support	• Three (3) years (8x5) enhanced support including all necessary security subscription services and firmware upgrades • Three (3) years software warranty against media defect • Original media kits and manuals • Unlimited phone and email support		
2.9	Warranty	• Three (3) years on all parts and service • Three (3) years email, call and remote services • In case of equipment failure, a service unit equal to or with higher specifications than the existing		

		equipment shall be provided pending the replacement of said unit.		

Item V. Management Appliance (This will be used to centrally manage all Firewall devices deployed in the remote and branch offices)				
Item No.	Particulars	Description	Comply Yes/No	Bidder's Offer
3.1	Form Factor	• Rack Mountable 2U		
3.2	Compliance	• FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE • Appliance must be Japan, U.S. or Europe brand.		
3.3	Features	• Centralized configuration, policy-based provisioning, update management and end to end monitoring for FW • Manage VPN policy and configuration • Multi frame display for single view of policies and objects • Appliance state		
3.4	Hardware Specifications	• 2 x GE Total Interface • Console Port DB9 • Storage Capacity 24TB (8x 3 TB) • RAID Levels Supported RAID 0/1/5/6/10/50/60 • High Availability Support • Redundant Hot Swap Power Supplies		
3.5	Performance	• Drag and drop between frames • In-View policy object editing • Up to 1000 Devices and Virtual Domains • Up to 2 Gigabyte of logs per day		
3.6	Support	• Three (3) years (8x5) enhanced support including all necessary security subscription services and firmware upgrades • Three (3) years software warranty against media defect • Original media kits and manuals • Unlimited phone and email support		
3.7	Warranty	• Three (3) years on all parts and service • Three (3) years email, call and remote services • In case of equipment failure, a service unit equal to or with		

		higher specifications than the existing equipment shall be provided pending the replacement of said unit.		

Additional requirements for all firewalls;

1. Shall have built-in reporting
2. Must provide after warranty/subscription license within six (6) months upon expiration of warranty/subscription.
3. Proposed Firewall/UTM Appliance for Head Office (Minimum Specifications) must be different from the existing Firewall.
4. The proposed firewall basic functionalities must still be operational after the expiration of firewall license.

The Department of Justice has the right to test, evaluate and accept the software and hardware equipment before acceptance. Prospected bidder must be Certified Distributor and have authority to sell, deploy, manage and provide support services for firewall issued by the product owner/manufacturer and must have certified product engineers.

I hereby certify to comply and deliver all the above requirements.

_____ _____ _____

Name of Company/Bidder Signature Over Printed Name Date