

Kathmandu Upatyaka Khanepani Limited Project Management Unit Tripureshwor, Kathmandu, Nepal

ADDENDUM No. 2

Contract No. KUKL/G/03/22

IFB Published on: 10th December 2018 in Gorkhapatra daily for Supply & Installation for the Upgradation of Computerization and Automation of KUKL Billing and Accounting System (Date of Issue of Addendum No 2:9th January 2019)

Pursuant to Clause No. 8 and 24.2 of Instruction to Bidders (ITB) of bidding document, all prospective bidders are hereby informed that the deadline for submission of bid has been extended upto 12:00 noon NST of 25 January 2019.

Reference	Text in Initial Invitation for Bids	Corrected Text as Addendum No. 2*
IFB Para 5		To purchase the Bidding Document, eligible bidders should on or before 24 January 2019, 16:00 Hrs. (NST).
	On or before the deadline: 11 January 2019; 12:00 Noon (NST). Late Bids will not be accepted.	

^{*}For Details, please visit website of Kathmandu Upatyaka Khanepani Limited (KUKL)

*http://kathmanduwater.org/index.php/notice/

Kathmandu Upatyaka Khanepani Limited

Project Management Unit

Tripureshwor, Kathmandu, Nepal Contract No. KUKL/G/03/22

IFB published on:10th December 2018 in Gorkhaparta daily for

Supply & Installation for the upgradation of Computerization and Automation of KUKL Billing and Accounting System

(Date of Issue of Addendum No 2: 9th January 2019)

Reference	Text in the initial Bid document	Corrected Text as Addendum No. 2
Section 6 Part 1 3.4.2 System Architecture Figure 3: Desired Development Stack	MS-SQL .	Database
Section 6 Part 1 3.4.2 System Architecture	MS-SQL/Oracle The entire architecture relies on the centrally powered Database. Without the database, the formation of the above architecture is of no use. The Database shall comprise of enterprises license. The database server should be in high availability state.	Database The entire architecture relies on the centrally powered Database. Without the database, the formation of the above architecture is of no use. The license for database shall be of enterprise edition but can use open source database. The database server should be in high availability state.
Section 6 Part 1 1.1.4.3 Customization for Data Center Upgrade		Following points has been added as: 1. "The bidder will be responsible for supply of necessary license for database upgrade as per PART I – Supply Requirements Figure 3: Desired Development Stack and Section 3.4.2 System Architecture"



The Charles of the Ch

			"The bidder will b different database	e responsible for e is proposed."	the migration of data base if	
Section 6 Part 1 3.3 Implementatio n Plan	0		Implementation "ALL license for	n Phase	en added in Item 10) Post	
Section 6					,	
2.4.2	Title	Specification	Title		Specification	
Word Processor, Spreadsheet	Brand	Microsoft Office 365 Business or Equivalent	Preferred I	3rand	Microsoft Office 2016 or equivalent or newer	
and Presenter	License Type	Enterprise (Payable one time)	License Ty	уре	Standard or equivalent (Payable one time)	
Section 6						
Part 2 1.2.1	Title	Specifications	Title	Speci	fications	
Handheld Meter Reading Device	Operating System	PayDroid based on Android 5.1 or equivalent	Operating System	PayDroid Pow	vered by Android 7.0 or	
	Processor	Application CPU: ARM Cortex A7 1.0 GHz 4 Core Processor	Processor Application CPU: Quad-core Cort		PU: Quad-core Cortex-A53,	
		Security CPU: Cortex-M4		Security CPU	PU: 32-bit RISC Core (ARMv7-	
	Memory	1GB or more DDR3 SDRAM,		M), 1.25DMIP	S/MHz or equivalent	



8GB or more EMMC Expandable to 41 GB or more via Micro SD

5.0 Inch or higher 720 x 1280 Pixel Capacitive Touch Screen

Slot

Display



Memory

Card Readers



1 x Micro SD Card Slot, Expandable up to

Magnetic Card Reader , Smart Card

2GB DDR + 16GB eMMC

128GB

	White LED Backlight
Physical Keys	1 x ON/OFF Key 2 x Shortcut
Printer	High-Speed Thermal Printer Paper Roll Width / Diameter: 2.25" / 1.57"
Communications	4G LTE I Bluetooth 4.0 Wi-Fi: 802.11 b/g/n, 2.4 GHz
Camera	5 Megapixel or higher Auto Zoom Camera 0.3 Megapixel Fixed Front Camera
Card Readers	Magnetic Card Reader, Smart Card Reader, Contactless Card Reader
Battery	Long Lasting Li-Ion Battery, 5∠50 mAH or higher, 3.7
Audio	Speaker Functionality, Microphone & Sound, Wave Payment Supported
Physical	L x W x H (mm): 175.7 x 78 x 57 Weight (g): 458 g or less (Including Battery)
Location	Must Support GPS
Peripheral Ports	At least 1 Micro-USB (OTG) 1 SIM Card Slot 2 PSAM Card Slot
	1 Micro SD Card Slot, Supports Up To 32 GB

	Reader , Contactless Card Reader
Camera	5 Megapixel or higher Auto Zoom Camera 0.3 Megapixel Fixed Front Camera Rear Camera with LED Flashlight
Display	5.5-inch or higher Capacitive Touchscreen
Audio	1 x Speaker Volume up to 85dB 1 x Microphone
Physical Button	1 x ON/OFF Button 2 x Volume +/- Button
Communications	WiFi 2.4G 4G (FDD-LTE / TDD-LTE) + 3G (WCDMA / CDMA2000) + 2G (GSM / CDMA / GPRS) I Bluetooth 4.0
Card Slots	1 x SIM + 2 x SAM or 2 x SIM + 1 x SAM
Peripheral Ports	1 x Micro USB Supports charging and USB 2.0, OTG 6 x POGO pin or equivalent
Printer	2-inch Thermal Printer Print Speed: 80mm/s Paper Width: 58mm Diameter: 40mm
Battery	2600 mAH or higher Rechargeable Li-ion Battery
Adapter	Input: 100 - 240V AC, 50Hz / 60Hz Output: 5.0V DC, 2.0A





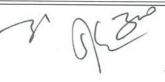
	Env	vironmental	0°C ~ 50°C (32°F ~ 122°F) or better Operating Temperature
			5% ~ 95% or better Relative Humidity, Non-Condensing
			-20°C ~ 70°C (-4°F ~ 158°F) or better Storage Temperature
	Vol	tage	Input: 100 - 240V AC, 50Hz / 60Hz Output: 5.0V DC, 2.0
	Acc	cessories	Multi-Functional Base, Charging base and
			1.0 m Micro-USB Charging Cable
	Warranty & Support Installation and Commissioning		PCI PTS 5 x EMV L1 & L2 or equivalent, MasterCard Contactless, Visa payWave, MasterCard TQM
			Minimum 2 (two) years full warranty (without cost) including parts replacements, software, labor
			Vendor shall take full responsibility of installation and commissioning part with necessary accessories
Section 6 Part 2	Features Description		
2.1.1			
Network Switch	Interface	Minimum 24 x 10/100/1000 Base-T ports with 4x10G SFP+ Uplink ports	

Sensor	Light sensor G-Sensor (optional)
Location	Must Support standard GPS
Accessories	Charging Base Wireless Base Multifunctional Base Charging Cable
Indicators	4 x Contactless Transaction Lights Charging Indicator Smart Card Reader Indicator
Certifications	PCI PTS 5.x, SRED, EMV L1 & L2 I EMV Contactless L1, MasterCard TQM, Visa payWave, MasterCard Contactless, ABECS Discover D-PAS, Interac_Flash L2, APCA, CE, Anatel RoHs or equivalent
Warranty & Support	Minimum 2 years full warranty (without cost) including parts replacements, software and labor
Installation and Commissioning	Vendor shall take full responsibility of installation and commissioning part with necessary accessories

Features	Description
Interface	Minimum 24 x 10/100/1000 Base-T ports with 4x1G SFP+ Uplink ports

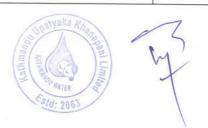








	Switching Capacity	160 Gbps or higher	Switching Capacity	40 Gbps or higher
	Forwarding Rate	90 Mpps or higher	Forwarding Rate	20 Mpps or higher
	MAC Adddress	16K or higher	MAC Adddress	16K or higher
	Security Features	Packet filtering based on MAC addresses, MAC address authentication, Port-based 802.1x authentication, RADIUS authentication, Portal authentication,Port isolation,Storm suppression, DHCP snooping,ACL	Security Features	Packet filtering based on MAC addresses, MAC address authentication, Port-based 802.1x authentication, RADIUS authentication, Portal authentication, Port isolation, Storm suppression, DHCP snooping
	VLANs	4K VLANs, Access port, Trunk port, Hybrid port, Management VLAN, Voice VLAN	VLANs	4K VLANs, Access port, Trunk port, Hybrid port, Management VLAN, Voice VLAN
	Spanning Tree Protocol (STP)	STP, RSTP, MSTP	Spanning Tree Protocol (STP)	STP, RSTP, MSTP
	Routing Protocol	IPv4 and IPv6 Static Routing	Routing Protocol	IPv4 and IPv6 Static Routing
	Warranty	One year of product replacement warranty	Preferred Brand	Cisco, Juniper or Equivalent
			Warranty	Minimum 2 years full warranty (without cost) including parts replacements, software and labor
Section 6				





2.1.2 Integrated Service Router	Features	Description
	Hardware and Interfaces	The proposed solution must be in the 'Leaders/Challengers/Visionaries' Quadrant of Gartner's Magic Quadrant for Enterprise Firewall published in any last three years or in the 'Leaders/Challengers/Visionaries' Quadrant of Gartner's Magic Quadrant for Wired/Wireless LAN Access infrastructure in any last three years Minimum 10 x 10/100/1000 Base-T port
	VPN Performance	2 Gbps or higher
	Concurrent Session	1 Millions or higher
	IPSec Tunnel	175 or higher
	SSL Users	100 or higher
	Layer 2 switching	Should support 802.1Q and 802.3ad/LACP
	Routing	Should support Static routes, OSPF, BGP
	Virtual Router/ Firewall	10 or higher
	Security	Should support Zone based firewall/ Policy based firewall Stateful firewall, ACL filters
	User Authentication	Should support third-party user authentication RADIUS, LDAP, Active directory

Features	Description
Hardware and Interfaces	The proposed solution must be in the 'Leaders/Challengers/Visionaries' Quadrant of Gartner's Magic Quadrant for Enterprise Firewall published in any last three years or in the 'Leaders/Challengers/Visionaries' Quadrant of Gartner's Magic Quadrant for Wired/Wireless LAN Access infrastructure in any last three years Minimum 8 x 10/100/1000 Base-T port and with 2x10G SFP
Ram	1GB or Higher
Flash Memory	512 MB or Higher
IPSec Tunnel	175 or higher
SSL Users	50 or higher
Layer 2 switching	Should support 802.1Q and 802.3ad/LACP
Protocols	Networking Protocol: Gigabit Ethernet, IEEE 802.1ag, IEEE 802.1ah, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1x, OSPF, RADIUS, RIP, SSH, TACACS+ Remote Management Protocol: CLI, HTTP, SNMP 3, Telnet Transport Protocol: IPSec, L2TP



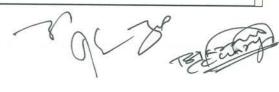




High availability	Should provide active/active, active/passive deployment
System management	Should support CLI, HTTPS, SSH
Warranty	One year of product replacement warranty

Routing	Should support Static routes, OSPF, BGP
Security	Should support • Zone based firewall/ Policy based firewall • Stateful firewall, ACL filters
User Authentication	Should support third-party user authentication RADIUS, LDAP, Active directory
High availability	Should provide active/active, active/passive deployment
Features	Features Access Control List (ACL) support, Class of Service (CoS), Intrusion Prevention System (IPS), Link Fragmentation and Interleaving (LFI), Low-latency queuing (LLQ), MAC address filtering, NAT support, Quality of Service (QoS), RADIUS support, Spanning Tree Protocol (STP) support, VLAN support, VPN support, Class-Based Weighted Fair Queuing (CBWFQ), Virtual Routing and Forwarding (VRF), Weighted Fair Queuing (WFQ), DHCP client, DHCP relay, DHCP server, DNS proxy, DiffServ support, IGMP snooping, IPv6 support
System management	Should support CLI, HTTPS, SSH
Preferred Brand	Cisco, Juniper or Equivalent
Others	Shall be rack mountable
Warranty	Minimum 2 years full warranty (without cost) including parts replacements, software and labor





			License	Vendor shall provide two-year VPN license (without cost)
			Installation and Commissioning	Vendor should take full responsibility of installation and commissioning part with necessary accessories.
Section 6 Part 2	Title	Specification	Title	Specification
2.1.6 Router for Data Center	Hardware and Interfaces	The proposed solution must be in the 'Leaders/Challengers/Visionaries' Quadrant of Gartner's Magic Quadrant for Enterprise Firewall published in any last three years or in the 'Leaders/Challengers/Visionaries' Quadrant of Gartner's Magic Quadrant for Wired/Wireless LAN Access infrastructure in any last three years Minimum 16 x 10/100/1000 Base-T port and 4 x 1 Gigabit SFP	Hardware and Interfaces	The proposed solution must be in the 'Leaders/Challengers/Visionaries' Quadrant of Gartner's Magic Quadrant for Enterprise Firewall published in any last three years of in the 'Leaders/Challengers/Visionaries' Quadrant of Gartner's Magic Quadrant for Wired/Wireless LAN Access infrastructure in any last three years Minimum 8 x 1G SFP/Base-T port & 2 x 10G ports with media convertor and required fiber should support interfaces supported by
	Storage Capacity	Storage: 400GB or higher for log retention		router like Channelized E1/T1, V.35, G.703, LTE, Gigabit and 10G Ethernet
	VPN Performance	9 Gbps or higher		modules to accommodate field upgrades without rebooting the router.
	Firewall Throughput	18 Gbps or higher		should have 2 empty slot for future use



Processor

Memory

Power supply

2 Millions or higher

Should support 802.1Q and 802.3ad/LACP

2000 or higher

300 or higher



Redundant Hot swappable power supply

minimum 16GB RAM & 16 GB FLASH.

multi-core Processor

Concurrent Session

Layer 2 switching

IPSec Tunnel

SSL Users

Routing	Should support Static routes, OSPF, BGP
Traffic management	Application prioritization based on source, destination, user, service, service group,
Virtual Router/ Firewall	10 or higher
Security	Should support
	Zone based firewall/ Policy based firewall Stateful firewall, ACL filters
	Should Integrate with Active Directory for user and group based firewall policies
User Authentication	Should support third-party user authentication RADIUS, LDAP, Active directory
High availability	Should provide active/active, active/passive deployment
System management	Should support CLI, HTTPS, SSH
Warranty	One year of product replacement warranty

VPN Performance
IPSec Tunnel
SSL Users
Layer 2 switching
Routing
Traffic management
Latyer-3 Features and Security





				external appliance for the same functionality can be provided. Shall have 802.1p class of service and marking, classification, policing and shaping. Should support SSHv2, SNMPv2c, SNMPv3 and NTP Should support AAA using RADIUS and TACACS+
			User Authentication	Should support third-party user authentication RADIUS, LDAP, Active directory
			High availability	Should provide active/active, active/passive deployment
			System management	Should support CLI, HTTPS, SSH
			Preferred Brand	Cisco, Juniper or Equivalent
			License	Vendor shall provide two-year at least 20 VPN license (without cost)
			Warranty	Minimum 2 years full warranty (without cost) including parts replacements, software and labor
	Title	Specification	Title	Specification
			Throughput: FW + AV	/C 4.0 Gbps or higher
			Throughput: AVC + IF	PS 4.0 Gbps or higher
Section 6 Part 2				7







2.1.7 Firewall for Data Center	Hardware and Interfaces	The proposed solution must be in the 'Leaders/Challengers/Visionaries' Quadrant of Gartner's Magic Quadrant for Enterprise Firewall published in any last three years or in the 'Leaders/Challengers/Visionaries' Quadrant of Gartner's Magic Quadrant for Wired/Wireless LAN Access infrastructure in any last three years Minimum 16 x 10/100/1000 Base-T port and 4 x 1 Gigabit SFP
	Storage Capacity	Storage: 400GB or higher for log retention
	VPN Performance	9 Gbps or higher
	Firewall Throughput	18 Gbps or higher
	Concurrent Session	2 Millions or higher
	IPSec Tunnel	2000 or higher
	SSL Users	300 or higher
	Layer 2 switching	Should support 802.1Q and 802.3ad/LACP
	Routing	Should support Static routes, OSPF, BGP
	Traffic management	Application prioritization based on source, destination, user, service, service group,
	Virtual Router/ Firewall	10 or higher

Maximum concurrent sessions, with AVC	2 million or more
Maximum new connections per second, with AVC	24K or more
IPSec VPN Throughput (1024B TCP w/Fastpath)	1.5 Gbps or higher
Maximum VPN Peers	7500 or more
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by the Management Center or alternatively in the cloud with Cisco Defense Orchestrator or equivalent
Application Visibility and Control (AVC)	Standard, supporting more than 4000 applications, as well as geolocations, users, and websites
AVC: OpenAppID support for custom, open source, application detectors	Standard
Security Intelligence	Standard, with IP, URL, and DNS threat intelligence
NGIPS	Available; can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence
URL Filtering: number of categories	More than 80







Security	Should support Zone based firewall/ Policy based firewall Stateful firewall, ACL filters Should Integrate with Active Directory for user and group based firewall policies
User Authentication	Should support third-party user authentication RADIUS, LDAP, Active directory
High availability	Should provide active/active, active/passive deployment
System management	Should support CLI, HTTPS, SSH
Warranty	One year of product replacement warranty

URL Filtering: number of URLs categorized	More than 280 million
Automated threat feed and IPS signature updates	Yes
VLANs maximum	1024 or higher
Stateful inspection firewall throughput	10 Gbps or higher
Stateful inspection firewall throughput (multiprotocol)	5 Gbps or higher
Concurrent firewall connections	2 million or more
New connections per second	40000 or more
IPsec VPN throughput (450B UDP L2L test)	1 Gbps or higher
IPsec/Cisco AnyConnect/Apex site-to- site VPN peers	7500 or more
Maximum number of VLANs	750 or more
High availability	Active/active and active/standby
Scalability	VPN Load Balancing



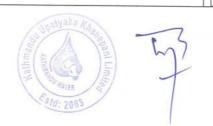


Centralized management	Shall be possible to perform centralized configuration, logging, monitoring and reporting
Adaptive Security Device Manager	Web-based, local management for small-scale deployments
Hardwa	are Specifications
Form factor (rack units)	1RU
Integrated I/O	At least 12 x 10M/100M/1GBASE-T Ethernet interfaces (RJ-45), 4 x 10 Gigabit (SFP) Ethernet interfaces
Maximum number of interfaces	Up to 16 total Ethernet ports (12x1G RJ-45, 4x1G SFP)
Integrated network management ports	1 x 10M/100M/1GBASE-T Ethernet port (RJ-45)
Serial port	1 x RJ-45 console
USB	1 x USB 2.0 Type-A (500mA)
Memory	Minimum 16GB
Storage	At least 1x 200 GB, 1x spare slot (for MSP)
Warranty & Support	Minimum 2 (two) years full warranty (without cost) including parts replacements, software, labor





Installation and Commissioning	Vendor shall take full responsibility of installation and commissioning part with necessary accessories
Preferred Brand	Cisco, Palo Alto, Juniper or Equivalent
Power Supplies	Redundant Hot swappable power supply
License	Defense Threat, Next Generation IPS License, Malware Protection License, URL Filtering License shal be available for at least 2 Years
Othe	r Firewall Specifications
D 15 " "	
shall be open architect scale against dynamic	I not be proprietary ASIC based in nature & ure based on multi-core CPU's to protect & latest security threats.
shall be open architect scale against dynamic Firewall shall provide a	ure based on multi-core CPU's to protect &
shall be open architect scale against dynamic Firewall shall provide a SMTP, ESMTP, LDAP TFTP, H.323, SNMP	ure based on multi-core CPU's to protect & latest security threats. pplication detection for DNS, FTP, HTTP, MGCP, RTSP, SIP, SCCP, SQLNET, reating access-rules with IPv4 & IPv6
shall be open architect scale against dynamic Firewall shall provide a SMTP, ESMTP, LDAP TFTP, H.323, SNMP Firewall shall support objects simultaneously	ure based on multi-core CPU's to protect & latest security threats. pplication detection for DNS, FTP, HTTP, MGCP, RTSP, SIP, SCCP, SQLNET, reating access-rules with IPv4 & IPv6
shall be open architect scale against dynamic Firewall shall provide a SMTP, ESMTP, LDAP TFTP, H.323, SNMP Firewall shall support objects simultaneously Firewall shall support of the state of the stat	ure based on multi-core CPU's to protect & latest security threats. pplication detection for DNS, FTP, HTTP, MGCP, RTSP, SIP, SCCP, SQLNET, reating access-rules with IPv4 & IPv6
shall be open architect scale against dynamic Firewall shall provide a SMTP, ESMTP, LDAP TFTP, H.323, SNMP Firewall shall support objects simultaneously Firewall shall support of Shall support Static, RI	pplication detection for DNS, FTP, HTTP, MGCP, RTSP, SIP, SCCP, SQLNET, reating access-rules with IPv4 & IPv6 perating in routed & transparent mode P, OSPF, OSPFv3 and BGP manual NAT and Auto-NAT, static NAT,





Firewall shall support Multicast protocols like IGMP and PIM

Shall support security policies based on security group names in source or destination fields or both

Shall support capability to limit bandwidth on basis of apps / groups, Networks / Geo and Ports

Firewall shall support Active/Standby failover

Firewall shall support redundant interfaces to provide interface level redundancy before device failover

Firewall shall support 802.3ad

Ether channel functionality to increase the bandwidth for a segment.

Shall have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.

The device shall allow administrators to create Custom IPS signatures

Shall be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies and updating policies) with minimal human intervention.

Shall be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.



The state of the s

Shall be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.

Shall be capable of detecting and blocking IPv4/ IPv6 attacks.

Shall support the capability to quarantine end point

Solution shall support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.

The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor

Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.

Solution must support URL and DNS threat intelligence feeds to protect against threats

Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.

Shall support more than 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.

The appliance OEM must have its own threat intelligence analysis center and shall use the global footprint of security deployments for more comprehensive network protection.





The detection engine shall support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows and P2P attacks).

Shall be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location.

The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.

The management platform must be accessible via a web-based interface and ideally with no need for additional client software.

The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.

The management platform must include a scheduling subsystem to facilitate automation of routine tasks, such as backups, upgrades, report creation, and policy application.

Centralized management can do contextual threat intelligence service accelerates analysis, correlation of events. This can be on appliance or can be cloud services

The management platform must be capable of automatically receiving rule updates published by the vendor and automatically distributing and applying those rule updates to sensors.



The Centralized management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. Report can be consolidated or can be generate individual NGFW

Logging of Administrative Changes that provides an audit trail for administrative activities.

The management platform must provide a highly customizable dashboard.

The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows

The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.

Shall support REST API for monitoring and config programmability

The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.

The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).

The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.





Section 6 Part 2 2.1.13 Internet Service Firewall for Data Center	Warranty	One year of product replacement warranty	Warranty	Minimum 2 years full warranty (without cost) including parts replacements, software and labor
Section 6 Part 2 2.1.10 Gigabit Switch for Data Center	Warranty	One year of product replacement warranty	Warranty	Minimum 2 years full warranty (without cost) including parts replacements, software and labor
Section 6 Part 2 2.1.9 Link Switch for Data Center	Warranty	One year of product replacement warranty	Warranty	Minimum 2 years full warranty (without cost) including parts replacements, software and labor
Section 6 Part 2 2.1.8 Core Switch for Data Center	Warranty	One year of product replacement warranty	Warranty	Minimum 2 years full warranty (without cost) including parts replacements, software and labor





