



Bangladesh Telecommunication Regulatory Commission

IEB Bhaban, Ramna, Dhaka- 1000.

Memo No.14.32.0000.400.07.024.22. **577**

Date: 03.05.2023

Addendum of the Tender Document

This is for the the information of all concerned Tenderer that the following amendments has been made for the tender doument for "Supply & Installation of Plant & Equipment of BTRC Network and Server Co-Location Center (National)" for Bangladesh Telecommunication Regularoty Commission (BTRC), Vide issue No. 14.32.0000.400.07.024.22.484, Dated: 09/04/2023.

Tender Document Reference	As in Tender Document	Amended as
ITT 14.1(b) (ii)	The Tenderer must have experience of holding at least 01 (one) Annual Maintenance Contract (AMC) of Data Center infrastructure, Active networking for at least three years in Government Organization/Telco/Bank with 24X7 support and minimum work order value of 2 (two) Crore. The tenderer must submit the contract documents.	The Tenderer must have experience of holding at least 01 (one) Annual Maintenance Contract (AMC) of Data Center infrastructure, Active networking for at least three years in Government Organization/Telco/Bank/Financial Institution with 24X7 support and minimum work order value of 2 (two) Crore. The tenderer must submit the contract documents.
ITT 14.1(b) (iii)	The bidder must have experience in Supply & Installation, testing, commissioning with at least one Tier-III/Rated-3 Data Center Development.	The bidder must have work experience in Supply & Installation, testing, commissioning with at least one Tier-III/Rated-3 Data Center.
ITT 37.1	In addition to the original of the Tender, 03 (Three) hard copies and 1 set of soft copy (In Word and Interactive PDF Format) through Pen Drive shall be submitted.	In addition to the original of the Tender, 03 (Three) hard copies and 1 set of soft copy (In Word and Interactive PDF Format) through Pen Drive shall be submitted. The tender documents must be submitted in english format including Product Brochure , Manufacturer's Authorization letter , Certification, Approvals and others.
Enclosure-2 Item No: 1	Raised Floor Works	
	Country of Origin	USA/UK/EU
	Air Grommet	To be mentioned by bidder
Feature	Reduce air loss and increase under-floor static pressure. Improve cooling efficiencies. Removable dual brush section for easy cable release. Rectangular Shape, Color black. Installation facilities at the panel edge or within the panel. Installation should be done by TIA 942 Standard.	Reduce air loss and increase under-floor static pressure. Improve cooling efficiencies. Removable dual brush section for easy cable release. Rectangular Shape, Color black. Installation facilities at the panel edge or within the panel. Installation should be done by TIA 942 or equivalent Standard.
Enclosure-2 Item No: 5	Automatic Fire Protection & Suppression System	
	Heat Detector	
	Country of Origin	USA/UK/EU
	Smoke Detector	
	Country of Origin	USA/UK/EU
	Suppression Agent	
	Brand	NOVEC
	Country of Origin	USA/UK/EU
	Suppression Module	
	Alarm Bell with strobe	
	Country of Origin	USA/UK/EU
Response Indicator		
Country of Origin	USA/UK/EU	
Very Early Smoke Detection Apparatus (VESDA)		
Country of Origin	USA/UK/EU	
Enclosure-2 Item No: 6	CAT-6 UTP CABLE 305 Meter Box	
	Jacket	LSZH jacket complying to: Fire rating IEC 60332-3-22, Acid gas IEC 60754-2, Smoke density IEC 61034-2
		LSZH jacket complying to: Fire rating IEC 60332-3-22, Acid gas IEC 60754-2, Smoke density IEC 61034-2 or equivalent

Tender Document Reference	As in Tender Document		Amended as
Enclosure-2 Item No: 7	Access Control System		
	Fingerprint, Card & Password reader		
	Country of Origin	USA/UK/EU	To be mentioned by bidder
	Controller with License Software		
Enclosure-2 Item No: 11	Country of Origin	USA/UK/EU	To be mentioned by bidder
	Phase Correction Device (PCD)		
Enclosure-2 Item No: 12	Main Distribution Board (MDB)		
	Features	Supply, Installation, testing & commissioning of following Distribution Boards of components from ABB (Swiss)/Eaton(EU)/Schneider (France) /Siemens (Germany) having ISO9001 certificate housing the following rated MCB/ MCCB & bus bars and all other accessories as per drawing, specifications and direction of the Engineer-in-charge.	Supply, Installation, testing & commissioning of following Distribution Boards of components from ABB /Eaton/Schneider /Siemens having ISO9001 certificate housing the following rated MCB/ MCCB & bus bars and all other accessories as per drawing, specifications and direction of the Engineer-in-charge.
Enclosure-2 Item No: 15	ISO Tx Output DB		
	Features	Supply, Installation, testing & commissioning of following Distribution Boards of components from ABB (Swiss)/Eaton(EU)/Schneider (France) /Siemens (Germany) having ISO9001 certificate housing the following rated MCB/ MCCB & bus bars and all other accessories as per drawing, specifications and direction of the Engineer-in-charge.	Supply, Installation, testing & commissioning of following Distribution Boards of components from ABB /Eaton/Schneider /Siemens having ISO9001 certificate housing the following rated MCB/ MCCB & bus bars and all other accessories as per drawing, specifications and direction of the Engineer-in-charge.
Enclosure-2 Item No: 23	Surge Protection Device (SPD)		
	Brand	Any International Reputed Brand like Vertiv/ Asco/ Eaton or equivalent	International Reputed Brand
	Standards Compliance	UL 1449	UL 1449 or equivalent
Enclosure-2 Item No: 24	Static Transfer Switch (STS)		
	Country of Origin	USA/UK/EU	To be mentioned by bidder
Enclosure-2 Item No: 25	Automatic Voltage Regulator		
	Country of Origin	USA/UK/EU	To be mentioned by bidder
Enclosure-2 Item No: 26	True Modular Online UPS		
	Country of Origin	USA/UK/EU	To be mentioned by bidder
	Battery Cabinet Brand	Same Brand as UPS	To be mentioned by bidder
Enclosure-2 Item No: 30	Server Rack		
	Country of Origin	USA/UK/EU	To be mentioned by bidder
	Feature & Standards	Rack should have Approvals like UL 2416 UL 60950-1, EIA-310E	Rack should have Approvals like UL 2416 UL 60950-1, EIA-310E or equivalent
Enclosure-2 Item No: 31	Network rack		
	Country of Origin	USA/UK/EU	To be mentioned by bidder
	Feature & Standards	Rack should have Approvals like UL 2416 UL 60950-1, EIA-310E	Rack should have Approvals like UL 2416 UL 60950-1, EIA-310E or equivalent
Enclosure-2 Item No: 33	Cold Aisle Containment System for 24 Racks		
	Country of Origin	USA/UK/EU	To be mentioned by bidder
	Lighting & Motion Sensor	UL Listing: Lighting system complies to UL484, CSA C22.2 No.236, EN 55022:2006, EN 55024:1998, EN 61000-3-2:2006, EN 61000-3-3:1995, EN 60950-1:2006, CFR 47 FCC Part 15:2011, ANSI C63.4-2003, ICES-003:2004, AS/NZS CISPR 22:2009.	UL Listing: Lighting system complies to UL484, CSA C22.2 No.236, EN 55022:2006, EN 55024:1998, EN 61000-3-2:2006, EN 61000-3-3:1995, EN 60950-1:2006, CFR 47 FCC Part 15:2011, ANSI C63.4-2003, ICES-003:2004, AS/NZS CISPR 22:2009 or equivalent
		Shall be provided with Modular PDU and/or Rack Mounting brackets if needed	Bidder should provide each Server and Network Rack 2x 32A Metered Rack PDU and PDU will be 36 Port.
Enclosure-2	Cat 6 UTP Patch Panel 24 Port Loaded		

Tender Document Reference	As in Tender Document		Amended as
Item No: 35	Approvals	UL listed and IEC 60603-7 compliant	UL listed and IEC 60603-7 compliant or equivalent
Enclosure-2	Face Plate Dual		
Item No: 36	Country of Origin	USA/UK/EU	To be mentioned by bidder
Enclosure-2	Cat 6 UTP Patch Cord 1 Meter		
Item No: 38	Approval	Intertek – ETL 4 connector channel compliant.	Intertek – ETL 4 connector channel compliant or equivalent
Enclosure-2	Pre-terminated 24F SM Fan out Cable, LC – LC 5 Meter		
Item No: 43	Cable Qualification Standards	ANSI/ICEA S-83-596, ANSI/TIA 568-C.3 and Telcordia GR-409	ANSI/ICEA S-83-596, ANSI/TIA 568-C.3 and Telcordia GR-409 or equivalent
Enclosure-2	Pre-terminated 24F MM Fan out Cable, LC – LC- 5 Meter		
Item No: 46	Cable Qualification Standards	ANSI/ICEA S-83-596, ANSI/TIA 568-C.3 and Telcordia GR-409	ANSI/ICEA S-83-596, ANSI/TIA 568-C.3 and Telcordia GR-409 or equivalent
Enclosure-2	Environment Monitoring System		
Item No: 47	Brand	Same as DCIM	To be mentioned by bidder
	Country of Origin	USA/UK/EU	To be mentioned by bidder
Enclosure-2	Data Center Monitoring System (DCIM) with Server		
Item No: 48	Country of Origin	USA/UK/EU	To be mentioned by bidder
Enclosure-2	Next-Generation Firewall		
Item No: 53	Country of Origin	USA/UK/EU	To be mentioned by bidder
	Certifications (Safety, EMC, Quality)	CB, CE, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, Checkmark, ICSA Labs, EAL4+, ISO 9000.	CB, CE, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, Checkmark, ICSA Labs, EAL4+, ISO 9000.
	Environmental	Operating Temperature: 0°C to 40°C	Operating Temperature: 0°C to 40°C
		Storage Temperature: -20°C to 70°C	Storage Temperature: -20°C to 70°C
		Humidity (non-condensing): 10% to 90%	Humidity (non-condensing): 10% to 90%
	Part No	Bidder should submit BOQ of proposed device including the detailed part numbers.	Bidder should submit BOQ of proposed device including the detailed part numbers.
	Form Factor	1U Rack Mountable with sliding rails (incl.)	1U Rack Mountable with sliding rails (incl.)
	Hardware Architecture	Should have 64-bit Dual Processors based multicore architecture and should not be any proprietary ASIC-based in nature	Should have 64-bit Dual Processors based multicore architecture and should not be any proprietary ASIC-based in nature
		Minimum 64GB system memory	Minimum 64GB system memory
		Minimum 480GB SATA-III SSD from day 1	Minimum 480GB SATA-III SSD from day 1
		Should have multi-function LCD display with navigation	Should have multi-function LCD display with navigation
		Should have Dual Internal redundant auto-ranging AC-DC 100-240VAC, 3.7-7.4A@50-60Hz power supply from day 1.	Should have Dual Internal redundant auto-ranging AC-DC 100-240VAC, 3.7-7.4A@50-60Hz power supply from day 1.
	Interface requirement (minimum)	Should have the following fixed ethernet ports from day 1: 8 x GbE copper, 8 x SFP+ 10 GbE fiber	Should have the following fixed ethernet ports from day 1: 8 x GbE copper, 8 x SFP+ 10 GbE fiber
		Should have 2 + 1 for high-density module fixed bypass ports pair.	Should have 2 + 1 for high-density module fixed bypass ports pair.
		SFP/SFP+ transceivers should be included from the same OEM from day 1.	SFP/SFP+ transceivers should be included from the same OEM from day 1.
		All interfaces should be freely configurable as LAN, WAN & DMZ ports without any limitation.	All interfaces should be freely configurable as LAN, WAN & DMZ ports without any limitation.
		Should not be any fixed WAN ports so that any port can be configured as WAN for multiple WAN load balancing.	Should not be any fixed WAN ports so that any port can be configured as WAN for multiple WAN load balancing.
		Should have 2x Flexi Port bays for future extension of Copper/SFP/SFP+.	Should have 2x Flexi Port bays for future extension of Copper/SFP/SFP+.
		Max total port density (incl. optional modules): 48 nos.	Max total port density (incl. optional modules): 48 nos.
		Max PoE using Flexi Port Module: 2x Module, 4 Ports, 60W Max Each.	Max PoE using Flexi Port Module: 2x Module, 4 Ports, 60W Max Each.

2

Tender Document Reference	As in Tender Document	Amended as
	Management I/O Ports	1 x RJ45 MGMT, 1 x COM RJ45, 1 x COM Micro-USB (w/cable), 2 x USB 3.0 (front), 1x USB 2.0 (rear).
		Optional Flexi Ports required for future expansion: 8 port GE copper, 8 port GE SFP Fiber, 4 port 10GE SFP+ Fiber, 4 port GE copper bypass (2 pairs), 4 port GE copper PoE + 4 port GE copper, 4 port 2.5 GE copper PoE, SFP DSL Module (VDSL2)
Security Performance (minimum)	Firewall throughput – Minimum 100 Gbps	Firewall throughput – Minimum 100 Gbps
	Firewall IMIX throughput –50 Gbps	Firewall IMIX throughput –50 Gbps
	NGFW throughput –Minimum 38 Gbps	NGFW throughput –Minimum 38 Gbps
	Firewall Latency (64 byte UDP): 5µs	Firewall Latency (64 byte UDP): 5µs
	IPS throughput – 40 Gbps	IPS throughput – 40 Gbps
	Threat Protection (combined FW, IPS, App Ctrl, & malware prevention enabled using HTTP 200 KB packet size) throughput – 14 Gbps	Threat Protection (combined FW, IPS, App Ctrl, & malware prevention enabled using HTTP 200 KB packet size) throughput – 14 Gbps
	IPsec VPN throughput – 90 Gbps	IPsec VPN throughput – 90 Gbps
	Xstream SSL/TLS Inspection throughput – 13 Gbps	SSL/TLS Inspection throughput – 13 Gbps
	Xstream SSL/TLS concurrent connections – 512k	SSL/TLS concurrent connections – 512k
	Concurrent connections – 32 mil	Concurrent connections – 32 mil
	New connections/sec – 460k	New connections/sec – 460k
	Wireless Access Point Supported - 180	Wireless Access Point Supported - 180
	Maximum licensed users – unrestricted/unlimited	Maximum licensed users – unrestricted/unlimited
	General Management	Purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators
Two-factor authentication (One-time-password) support for administrator access, user portal, IPsec and SSL VPN		Two-factor authentication (One-time-password) support for administrator access, user portal, IPsec and SSL VPN
Advanced troubleshooting tools in GUI (e.g., Packet Capture)		Advanced troubleshooting tools in GUI (e.g., Packet Capture)
High Availability (HA) support clustering two devices in active-active or active-passive mode with plug-and-play Quick HA setup		High Availability (HA) support clustering two devices in active-active or active-passive mode with plug-and-play Quick HA setup
Full command line interface (CLI) accessible from GUI		Full command line interface (CLI) accessible from GUI
Role-based administration		Role-based administration
Automated firmware update notification with easy automated update process and roll-back features		Automated firmware update notification with easy automated update process and roll-back features
Reusable system object definitions for networks, services, hosts, time periods, users		Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients, and servers
Self-service user portal		Self-service user portal
Configuration change tracking		Configuration change tracking
Flexible device access control for services by zones		Flexible device access control for services by zones
Email or SNMP trap notification options		Email or SNMP trap notification options
SNMP v3 and NetFlow support		SNMP v3 and NetFlow support
Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly		Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
API for third-party integration	API for third-party integration	
Interface renaming	Interface renaming	

2

Tender Document Reference	As in Tender Document		Amended as	
		Remote access option for OEM Support		Remote access option for OEM Support
		Cloud-based license management via portal		Cloud-based license management via portal
	Central Management	Central cloud-based management and reporting for multiple firewalls provides group policy management and a single console		Central cloud-based management and reporting for multiple firewalls provides group policy management and a single console
		Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group		Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group
		Task Manager provides a full historical audit trail and status monitoring of group policy changes		Task Manager provides a full historical audit trail and status monitoring of group policy changes
		Backup firmware management in web-based Central Console stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access		Backup firmware management in web-based Central Console stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access
		Firmware updates from web-based Central console offer one-click firmware updates to be applied to any device		Firmware updates from web-based Central console offer one-click firmware updates to be applied to any device
		Zero-touch deployment enables the initial configuration to be performed in web-based Central Console and then exported for loading onto the device from a flash drive at startup automatically connecting the device back to Central Console		Zero-touch deployment enables the initial configuration to be performed in web-based Central Console and then exported for loading onto the device from a flash drive at startup, automatically connecting the device back to Central Console
	Firewall, Networking, and Routing	Stateful deep packet inspection firewall		Stateful deep packet inspection firewall
		Xstream Architecture to provide extreme levels of visibility, protection, and performance		Architecture to provide extreme levels of visibility, protection, and performance through stream-based
		Xstream TLS inspection with high performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade policies, unique dashboard visibility, and compatibility troubleshooting		TLS inspection with high performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade policies, unique dashboard visibility, and compatibility troubleshooting
		Xstream DPI Engine to provide stream scanning protection for IPS, AV, Web, App Control, and TLS Inspection in a single-high performance engine		DPI Engine to provide stream scanning protection for IPS, AV, Web, App Control, and TLS Inspection in a single-high performance engine
		XStream Network Flow FastPath to deliver policy-driven and intelligent acceleration of trusted traffic automatically		Network Flow FastPath to deliver policy-driven and intelligent acceleration of trusted traffic automatically
		User, group, time, or network-based policies, Access time policies per user/group		User, group, time, or network-based policies, Access time policies per user/group
		Enforce policy across zones, networks, or by service type		Enforce policy across zones, networks, or by service type
		Zone isolation and zone-based policy support		Zone isolation and zone-based policy support
		Default zones for LAN, WAN, DMZ, LOCAL, VPN, and WiFi. Custom zones on LAN or DMZ		Default zones for LAN, WAN, DMZ, LOCAL, VPN, and WiFi. Custom zones on LAN or DMZ

2

Tender Document Reference	As in Tender Document	Amended as
	<p>Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule with a convenient NAT rule wizard to quickly and easily create complex NAT rules in just a few clicks</p> <p>Upstream proxy support</p> <p>Protocol-independent multicast routing with IGMP snooping</p> <p>Bridging with STP support and ARP broadcast forwarding</p> <p>VLAN DHCP support and tagging,</p> <p>VLAN bridge support, Jumbo frame support</p> <p>WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules</p> <p>Wireless WAN support</p> <p>802.3ad interface link aggregation</p> <p>Full configuration of DNS, DHCP, and NTP</p> <p>Dynamic DNS (DDNS)</p> <p>IPv6 Ready Logo Program Approval Certification</p> <p>IPv6 tunneling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPsec</p>	<p>Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule with a convenient NAT rule wizard to quickly and easily create complex NAT rules in just a few clicks</p> <p>Upstream proxy support</p> <p>Protocol-independent multicast routing with IGMP snooping</p> <p>Bridging with STP support and ARP broadcast forwarding</p> <p>VLAN DHCP support and tagging,</p> <p>VLAN bridge support, Jumbo frame support</p> <p>WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules</p> <p>Wireless WAN support</p> <p>802.3ad interface link aggregation</p> <p>Full configuration of DNS, DHCP, and NTP</p> <p>Dynamic DNS (DDNS)</p> <p>IPv6 Ready Logo Program Approval Certification</p> <p>IPv6 tunneling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPsec</p>
	<p>SD-WAN</p> <p>Support for multiple WAN link options including VDSL, DSL, cable, and 3G/4G/LTE cellular with essential monitoring, balancing, and failover</p> <p>Application path selection and routing, used to ensure quality and minimize latency for mission-critical applications such as VoIP</p> <p>Synchronized SD-WAN Security feature to leverage the added clarity and reliability of application identification that comes with the sharing of synchronized app control information between managed endpoints and firewall</p> <p>Application routing over preferred links via firewall rules or policy-based routing</p> <p>Affordable, flexible, and zero-touch or low-touch</p> <p>Robust VPN support including IPsec and SSL VPN</p> <p>Encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC</p> <p>Centralized VPN orchestration</p> <p>Unique RED Layer 2 tunnel with routing</p>	<p>Support for multiple WAN link options including VDSL, DSL, cable, and 3G/4G/LTE cellular with essential monitoring, balancing, and failover</p> <p>Application path selection and routing, used to ensure quality and minimize latency for mission-critical applications such as VoIP</p> <p>Synchronized SD-WAN Security feature to leverage the added clarity and reliability of application identification that comes with the sharing of synchronized app control information between managed endpoints and firewall</p> <p>Application routing over preferred links via firewall rules or policy-based routing</p> <p>Affordable, flexible, and zero-touch or low-touch</p> <p>Robust VPN support including IPsec and SSL VPN</p> <p>Encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC</p> <p>Centralized VPN orchestration</p> <p>Unique RED Layer 2 tunnel with routing</p>
<p>Base Traffic Shaping and Quotas</p>	<p>Flexible network or user-based traffic shaping (QoS)</p> <p>Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical</p> <p>Real-time VoIP optimization</p> <p>DSCP marking</p>	<p>Flexible network or user-based traffic shaping (QoS)</p> <p>Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical</p> <p>Real-time VoIP optimization</p> <p>DSCP marking</p>

2

Tender Document Reference	As in Tender Document	Amended as
Secure Wireless	Central monitoring and management of APs and wireless clients through the built-in wireless controller	Central monitoring and management of APs and wireless clients through the built-in wireless controller
	Bridge APs to LAN, VLAN, or a separate zone with client isolation options	Bridge APs to LAN, VLAN, or a separate zone with client isolation options
	Multiple SSID support per radio including hidden SSIDs	Multiple SSID support per radio including hidden SSIDs
	Support for diverse security and encryption standards including WPA2 Personal and Enterprise	Support for diverse security and encryption standards including WPA2 Personal and Enterprise
	Channel width selection option	Channel width selection option
	Support for HTTPS login	Support for HTTPS login
	Support for 802.11r (fast transition)	Support for 802.11r (fast transition)
	Hotspot support for (custom) vouchers, password of the day, or T&C acceptance	Hotspot support for (custom) vouchers, password of the day, or T&C acceptance
	Wireless guest Internet access with walled garden options	Wireless guest Internet access with walled garden options
	Wireless repeating and bridging meshed network mode with supported APs	Wireless repeating and bridging meshed network mode with supported APs
	Support for the latest security and encryption standards including WPA2 Personal and Enterprise	Support for the latest security and encryption standards including WPA2 Personal and Enterprise
	Time-based wireless network access	Time-based wireless network access
	Support for IEEE 802.1X (RADIUS authentication) with primary and secondary server support	Support for IEEE 802.1X (RADIUS authentication) with primary and secondary server support
	Authentication	Synchronized User ID utilizes Synchronized Security to share currently logged in Active Directory user ID between endpoints and the firewall without an agent on the AD server or client
Single sign-on: Active directory, eDirectory, RADIUS Accounting		Single sign-on: Active directory, eDirectory, RADIUS Accounting
Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+		Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
Server authentication agents for Active Directory SSO, STAS, SATC		Server authentication agents for Active Directory SSO, STAS, SATC
Client authentication agents for Windows, Mac OS X, Linux 32/64		Client authentication agents for Windows, Mac OS X, Linux 32/64
Authentication certificates for iOS and Android		Authentication certificates for iOS and Android
Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos		Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos
Authentication services for IPsec, SSL, L2TP, PPTP		Authentication services for IPsec, SSL, L2TP, PPTP
Google Chromebook authentication support for environments with Active Directory and Google G Suite		Google Chromebook authentication support for environments with Active Directory and Google G Suite
API-based authentication		API-based authentication
Browser Captive Portal		Browser Captive Portal
User Self-Service Portal	Download the Authentication Client	Download the Authentication Client
	Hotspot access information	Hotspot access information
	Change username and password	Change username and password
	View personal Internet usage	View personal Internet usage
	Access quarantined messages and manage user-based block/allow sender lists	Access quarantined messages and manage user-based block/allow sender lists
	Download SSL remote access client (Windows) and configuration files (other OS)	Download SSL remote access client (Windows) and configuration files (other OS)

2

Tender Document Reference	As in Tender Document	Amended as
Base VPN options	Site-to-site VPN: SSL, IPsec, 256-bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key	Site-to-site VPN: SSL, IPsec, 256-bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
	Robust and lightweight RED site-to-site VPN tunnel	Robust and lightweight RED site-to-site VPN tunnel
	L2TP and PPTP	L2TP and PPTP
	Route-based VPN	Route-based VPN
	Remote access: SSL, IPsec, iPhone/iPad/Cisco /Android VPN client support	Remote access: SSL, IPsec, iPhone/iPad/Cisco /Android VPN client support
	IKEv2 Support	IKEv2 Support
	SSL client for Windows and configuration download via user portal	SSL client for Windows and configuration download via user portal
VPN Client	Authentication: Pre-Shared Key (PSK),	Authentication: Pre-Shared Key (PSK),
	PKI (X.509), Token and XAUTH	PKI (X.509), Token and XAUTH
	Intelligent split-tunneling for optimum traffic routing	Intelligent split-tunneling for optimum traffic routing
	NAT-traversal support	NAT-traversal support
	Client-monitor for graphical overview of connection status	Client-monitor for graphical overview of connection status
	Mac and Windows Support	Mac and Windows Support
	Enables Synchronized Security and Security Heartbeat for remote connected users	Enables Synchronized Security and Security Heartbeat for remote connected users
SD-RED VPN Device Management	Central management of all SD-RED (Remote Ethernet) VPN Device Management	Central management of all SD-RED (Remote Ethernet) VPN Device Management
	No configuration: Automatically connects through a cloud-based provisioning service	No configuration: Automatically connects through a cloud-based provisioning service
	Secure encrypted tunnel using digital X.509 certificates and AES 256-bit encryption	Secure encrypted tunnel using digital X.509 certificates and AES 256-bit encryption
	Virtual Ethernet for reliable transfer of all traffic between locations	Virtual Ethernet for reliable transfer of all traffic between locations
	IP address management with centrally defined DHCP and DNS Server configuration	IP address management with centrally defined DHCP and DNS Server configuration
	Remotely de-authorize SD-RED devices after a select period of inactivity	Remotely de-authorize SD-RED devices after a select period of inactivity
	Compression of tunnel traffic	Compression of tunnel traffic
Clientless VPN	Encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC	Encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC
ATP and Security Heartbeat	Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)	Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
	Security Heartbeat instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise	Security Heartbeat instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise
	Security Heartbeat policies can limit access to network resources or completely isolate compromised systems until they are cleaned	Security Heartbeat policies can limit access to network resources or completely isolate compromised systems until they are cleaned
	Lateral Movement Protection further isolates compromised systems by having healthy managed endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain	Lateral Movement Protection further isolates compromised systems by having healthy managed endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain

Tender Document Reference	As in Tender Document	Amended as
Intrusion Prevention (IPS)	High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection	High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection
	Top rated by NSS Labs	Top rated by NSS Labs
	Support for custom IPS signatures	Support for custom IPS signatures
	IPS Policy Smart Filters enable dynamic policies that automatically update as new	IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added
	Granular category selection	Granular category selection
	Thousands of signatures	Thousands of signatures
Web Protection and Control	Fully transparent proxy for anti-malware and web filtering	Fully transparent proxy for anti-malware and web filtering
	Enhanced Advanced Threat Protection	Enhanced Advanced Threat Protection
	URL Filter database with millions of sites across 92 web categories, backed by OEM Labs	URL Filter database with millions of sites across 92 web categories, backed by OEM Labs
	Surfing quota time policies per user/group	Surfing quota time policies per user/group
	Access time polices per user/group	Access time polices per user/group
	Malware scanning: block all forms of viruses, web malware, trojans, and spyware on HTTP/S, FTP and web-based email	Malware scanning: block all forms of viruses, web malware, trojans, and spyware on HTTP/S, FTP and web-based email
	Advanced web malware protection with JavaScript emulation	Advanced web malware protection with JavaScript emulation
	Live Protection real-time, in-the-cloud lookups for the latest threat intelligence	Live Protection real-time, in-the-cloud lookups for the latest threat intelligence
	Dual malware detection engine for dual scanning (At least one AV vendor should be Gartner Leader)	Dual malware detection engine for dual scanning (At least one AV vendor should be Gartner Leader)
	Real-time or batch mode scanning	Real-time or batch mode scanning
	Pharming protection	Pharming protection
	HTTP and HTTPS scanning and enforcement on any network and user policy with fully customizable rules and exceptions	HTTP and HTTPS scanning and enforcement on any network and user policy with fully customizable rules and exceptions
	SSL protocol tunneling detection and enforcement	SSL protocol tunneling detection and enforcement
	Certificate validation	Certificate validation
	High performance web content caching	High performance web content caching
	Forced caching for Endpoint updates	Forced caching for Endpoint updates
	File type filtering by mime-type, extension, and active content types (e.g. ActiveX, applets, cookies, etc.)	File type filtering by mime-type, extension, and active content types (e.g. ActiveX, applets, cookies, etc.)
	YouTube for Schools enforcement per policy (user/group)	YouTube for Schools enforcement per policy (user/group)
	SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)	SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)
	Web keyword monitoring and enforcement to log, report, or block web content matching keyword lists with the option to upload customs lists	Web keyword monitoring and enforcement to log, report, or block web content matching keyword lists with the option to upload customs lists
	Block Potentially Unwanted Applications (PUAs)	Block Potentially Unwanted Applications (PUAs)
	Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users	Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users

Tender Document Reference	As in Tender Document		Amended as
		User/Group policy enforcement on Google Chromebooks	User/Group policy enforcement on Google Chromebooks
	Cloud Application Visibility	Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated	Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
		Discover Shadow IT at a glance	Discover Shadow IT at a glance
		Drill down to obtain details on users, traffic, and data	Drill down to obtain details on users, traffic, and data
		One-click access to traffic shaping policies	One-click access to traffic shaping policies
		Filter cloud application usage by category or volume	Filter cloud application usage by category or volume
		Detailed customizable cloud application usage report for full historical reporting	Detailed customizable cloud application usage report for full historical reporting
	Application Protection and Control	Synchronized App Control to automatically, identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between managed endpoints and the firewall.	Synchronized App Control to automatically, identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between managed endpoints and the firewall.
		Signature-based application control with patterns for thousands of applications	Signature-based application control with patterns for thousands of applications
		Cloud Application Visibility and Control to discover Shadow IT	Cloud Application Visibility and Control to discover Shadow IT
		App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added	App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added
		Micro app discovery and control	Micro app discovery and control
		Application control based on category, characteristics (e.g., bandwidth and	Application control based on category, characteristics (e.g., bandwidth and productivity consuming),
		Per-user or network rule application control policy enforcement	Per-user or network rule application control policy enforcement
	Web and App Traffic Shaping	Enhanced traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared.	Enhanced traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared.
	Zero-day Protection (Dynamic Sandbox Analysis)	Full integration into the security solution dashboard	Full integration into the security solution dashboard
		Inspects executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)	Inspects executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
		Aggressive behavioral, network, and memory analysis	Aggressive behavioral, network, and memory analysis
		Detects sandbox evasion behavior	Detects sandbox evasion behavior
		Machine Learning technology with Deep Learning scans all dropped executable files	Machine Learning technology with Deep Learning scans all dropped executable files
		In-depth malicious file reports with screen shots and dashboard file release capability	In-depth malicious file reports with screen shots and dashboard file release capability
		Includes exploit prevention and Cryptoguard Protection technology	Includes exploit prevention and Cryptoguard Protection technology
		Optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis	Optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis
		Supports one-time download links	Supports one-time download links

2

Tender Document Reference	As in Tender Document	Amended as
Zero-day Protection (Static Threat Intelligence Analysis)	All files containing active code downloaded via the web or coming into the firewall as email attachments such as executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) are automatically sent for Threat Intelligence Analysis	All files containing active code downloaded via the web or coming into the firewall as email attachments such as executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) are automatically sent for Threat Intelligence Analysis
	Files are checked against OEM Labs' massive threat intelligence database and subjected to multiple machine learning models to identify new and unknown malware	Files are checked against OEM Labs' massive threat intelligence database and subjected to multiple machine learning models to identify new and unknown malware
	Extensive reporting includes a dashboard widget for analyzed files, a detailed list of the files that have been analyzed and the analysis results, and a detailed report outlining the outcome of each machine learning model.	Extensive reporting includes a dashboard widget for analyzed files, a detailed list of the files that have been analyzed and the analysis results, and a detailed report outlining the outcome of each machine learning model.
SD-WAN Orchestration	SD-WAN and VPN orchestration with easy and automated wizard-based creation of site-to-site VPN tunnels between network locations using an optimal architecture (hub-and-spoke, full mesh, or some combination).	SD-WAN and VPN orchestration with easy and automated wizard-based creation of site-to-site VPN tunnels between network locations using an optimal architecture (hub-and-spoke, full mesh, or some combination).
	Supports IPsec, SSL or RED VPN tunnels.	Supports IPsec, SSL or RED VPN tunnels.
	Integrates seamlessly with SD-WAN features for application prioritization, routing optimization, and leveraging multiple WAN links for resiliency and performance.	Integrates seamlessly with SD-WAN features for application prioritization, routing optimization, and leveraging multiple WAN links for resiliency and performance.
Advanced Firewall Reporting Storage	30-days of cloud data storage for historical firewall reporting with advanced features to save, schedule and export custom reports.	30-days of cloud data storage for historical firewall reporting with advanced features to save, schedule and export custom reports.
XDR & MTR Connector	Ready to integrate with Extended Threat Detection and Response (XDR) for cross-product threat hunting and analysis	Ready to integrate with Extended Threat Detection and Response (XDR) for cross-product threat hunting and analysis
	Support for 24/7 Managed Threat Response (MTR) service	Support for 24/7 Managed Threat Response (MTR) service
Reporting (Central cloud)	Central cloud-based Firewall Reporting should be included at no additional cost	Central cloud-based Firewall Reporting should be included at no additional cost
	Reporting features should be accessed from anywhere by Admin without direct access to the device	Reporting features should be accessed from anywhere by Admin without direct access to the device
	Administrators should drill down into the syslog data for a granular view that is	Administrators should drill down into the syslog data for a granular view that is presented in a visual format for
	Pre-defined reports with flexible customization options	Pre-defined reports with flexible customization options

2

Tender Document Reference	As in Tender Document	Amended as
	Ability to configure flexible reports with a high degree of customization - each report table, containing dozens of column choices, allows administrators to add or remove columns of data, to make report more granular, compressed, or enriched as desired	Ability to configure flexible reports with a high degree of customization - each report table, containing dozens of column choices, allows administrators to add or remove columns of data, to make report more granular, compressed, or enriched as desired
	Application bandwidth report that shows bandwidth usage by application and risk. The application and risk columns can be removed and replaced with source IP to provide a bandwidth usage report broken out by IP address	Application bandwidth report that shows bandwidth usage by application and risk. The application and risk columns can be removed and replaced with source IP to provide a bandwidth usage report broken out by IP address
	Reporting for NG Firewalls - hardware, software, virtual, and cloud	Reporting for NG Firewalls - hardware, software, virtual, and cloud
	Intuitive user interface provides graphical representation of data	Intuitive user interface provides graphical representation of data
	Report dashboard provides an at-a-glance view of events over the past 24 hours	Report dashboard provides an at-a-glance view of events over the past 24 hours
	Customizable chart options - can select between a bar, pie, stacked area, and line chart for any report	Customizable chart options - can select between a bar, pie, stacked area, and line chart for any report
	Easily identify network activities, trends, and potential attacks	Easily identify network activities, trends, and potential attacks
	Deep insight into user activity, application usage, and security threats on the network	Deep insight into user activity, application usage, and security threats on the network
	Easy backup of logs with quick retrieval for audit needs	Easy backup of logs with quick retrieval for audit needs
	Simplified deployment without the need for technical expertise	Simplified deployment without the need for technical expertise
	Managed Threat Response (MTR) Connector enables analysts to receive alerts from Firewall	Managed Threat Response (MTR) Connector enables analysts to receive alerts from Firewall
	Reporting (On-appliance)	
	Firewall reporting should be included at no extra cost (on-box reports) with custom report options	Firewall reporting should be included at no extra cost (on-box reports) with custom report options
	Dashboards (Traffic, Security, and User Threat Quotient)	Dashboards (Traffic, Security, and User Threat Quotient)
	Applications reports (App Risk, Blocked Apps, Synchronized Apps, Search Engines, Web Servers, Web Keyword Match, FTP)	Applications reports (App Risk, Blocked Apps, Synchronized Apps, Search Engines, Web Servers, Web Keyword Match, FTP)
	Network and Threats reports (IPS, ATP, Wireless, Security Heartbeat, Sandstorm)	Network and Threats reports (IPS, ATP, Wireless, Security Heartbeat, Sandstorm)
	User Threat Quotient (UTQ) reports to identify risky users based on recent browsing behavior and ATP triggers	User Threat Quotient (UTQ) reports to identify risky users based on recent browsing behavior and ATP triggers
	VPN reports	VPN reports
	Email reports	Email reports
	Compliance reports (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)	Compliance reports (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
	Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks	Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks
	Report anonymization	Report anonymization
	Report scheduling to multiple recipients by report group with flexible frequency options	Report scheduling to multiple recipients by report group with flexible frequency options
	Export reports as HTML, PDF, Excel (XLS)	Export reports as HTML, PDF, Excel (XLS)
	Report bookmarks	Report bookmarks

Tender Document Reference	As in Tender Document	Amended as
Next-Gen Xstream Protection from day 1	Log retention customization by category	Log retention customization by category
	Full-featured log viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization	Full-featured log viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization
	Base Firewall Protection includes:	Base Firewall Protection includes:
	Networking and SD-WAN: Wireless, SD-WAN, Application Aware Routing, Traffic Shaping.	Networking and SD-WAN: Wireless, SD-WAN, Application Aware Routing, Traffic Shaping.
	Protection and Performance: Xstream Architecture with Network Flow FastPath, TLS 1.3 Inspection, Deep-Packet Inspection.	Protection and Performance: Architecture with Network Flow FastPath, TLS 1.3 Inspection, Deep-Packet Inspection.
	VPN: IPsec/SSL Site-to-Site and Remote Access VPN (unlimited), SD-RED Site-to-Site VPN.	VPN: IPsec/SSL Site-to-Site and Remote Access VPN (unlimited), SD-RED Site-to-Site VPN.
	Central Management: Group firewall management, backup management, firmware update scheduling.	Central Management: Group firewall management, backup management, firmware update scheduling.
	Reporting: Historical on-box logging and reporting.	Reporting: Historical on-box logging and reporting.
	Central Firewall Reporting: Prepackaged and custom report tools with seven days cloud storage for no extra charge.	Central Firewall Reporting: Prepackaged and custom report tools with seven days cloud storage for no extra charge.
	Network Protection includes:	Network Protection includes:
	Xstream TLS Inspection: TLS 1.3 inspection with pre-packaged exceptions.	TLS Inspection: TLS 1.3 inspection with pre-packaged exceptions.
	Xstream DPI engine: streaming deep-packet inspection.	DPI engine: streaming deep-packet inspection.
	IPS: Next-gen Intrusion Prevention.	IPS: Next-gen Intrusion Prevention.
	ATP: Advanced Threat Protection.	ATP: Advanced Threat Protection.
	Synchronized Security Heartbeat: Integration with Endpoints to identify and isolate threats.	Synchronized Security Heartbeat: Integration with Endpoints to identify and isolate threats.
	Clientless VPN: HTML5.	Clientless VPN: HTML5.
	SD-RED VPN: Manage SD-RED devices.	SD-RED VPN: Manage SD-RED devices.
	Reporting: Extensive network and threat reporting.	Reporting: Extensive network and threat reporting.
	Web Protection includes:	Web Protection includes:
	Xstream TLS Inspection: TLS 1.3 inspection with pre-packaged exceptions.	TLS Inspection: TLS 1.3 inspection with pre-packaged exceptions.
	Xstream DPI engine: Streaming deep-packet inspection.	DPI engine: Streaming deep-packet inspection.
	Web Control: By user, group, category, URL, keyword.	Web Control: By user, group, category, URL, keyword.
	Web Threat Protection: Malware, PUA, malicious JavaScript, Pharming.	Web Threat Protection: Malware, PUA, malicious JavaScript, Pharming.
	App Control: By user, group, category, risk, and more.	App Control: By user, group, category, risk, and more.
	Synchronized App Control: Integration with endpoints to identify unknown apps.	Synchronized App Control: Integration with endpoints to identify unknown apps.
	Synchronized SD-WAN: Utilizing Synchronized App Control to route unknown apps.	Synchronized SD-WAN: Utilizing Synchronized App Control to route unknown apps.
	Reporting: Extensive web and app reporting.	Reporting: Extensive web and app reporting.
Zero-day Protection includes:	Zero-day, Protection includes:	
Xstream TLS Inspection: TLS 1.3 inspection with pre-packaged exceptions.	TLS Inspection: TLS 1.3 inspection with pre-packaged exceptions.	
Xstream DPI engine: Streaming deep-packet inspection.	DPI engine: Streaming deep-packet inspection.	


Tender Document Reference	As in Tender Document	Amended as
	<p>Zero-Day Threat Protection: Analyze all unknown files using AI, ML, and sandboxing.</p> <p>Threat Labs Intelix: Cloud-based intelligence and analysis.</p> <p>Machine Learning: Using multiple deep learning models.</p> <p>Cloud Sandboxing: Dynamic run-time analysis of unknown files.</p> <p>Reporting: Extensive threat intelligence analysis reporting.</p> <p>Central Management includes:</p> <p>Group Firewall Management: Synchronized policy across firewall groups.</p> <p>Backup and firmware updates: Storage and scheduling.</p> <p>Zero-touch deployment: For new firewalls from the cloud.</p> <p>Central Orchestration includes:</p> <p>SD-WAN Orchestration: Point and click Site-to-Site VPN Orchestration.</p> <p>Cloud Firewall Reporting: Multi-firewall reporting with save, schedule and export reports (30-day data retention).</p> <p>XDR and MDR Connector: Support for XDR and MTR services</p> <p>Enhanced Plus Support includes:</p> <p>24x7x365 technical support including statutory, public and bank holidays.</p> <p>Advance RMA replacement hardware warranty.</p> <p>Direct OEM technical support via portal/telephone/remote access.</p> <p>Online Support case management and reporting portal.</p> <p>Free security updates and patches.</p> <p>Free software download, updates, upgrades & maintenance.</p> <p>VIP access to Senior Technical Resource Team (priority queues for support cases, routed to senior level engineers, etc.).</p> <p>Remote consulting engagement for 4 hours per year (proactive health check, basic troubleshooting, demonstration on best practices for configuring, performance and feature optimization etc)</p> <p>Malware sample handling for priority malware analysis.</p>	<p>Zero-Day Threat Protection: Analyze all unknown files using AI, ML, and sandboxing.</p> <p>Threat Labs Intelix: Cloud-based intelligence and analysis.</p> <p>Machine Learning: Using multiple deep learning models.</p> <p>Cloud Sandboxing: Dynamic run-time analysis of unknown files.</p> <p>Reporting: Extensive threat intelligence analysis reporting.</p> <p>Central Management includes:</p> <p>Group Firewall Management: Synchronized policy across firewall groups.</p> <p>Backup and firmware updates: Storage and scheduling.</p> <p>Zero-touch deployment: For new firewalls from the cloud.</p> <p>Central Orchestration includes:</p> <p>SD-WAN Orchestration: Point and click Site-to-Site VPN Orchestration.</p> <p>Cloud Firewall Reporting: Multi-firewall reporting with save, schedule and export reports (30-day data retention).</p> <p>XDR and MDR Connector: Support for XDR and MTR services</p> <p>Enhanced Plus Support includes:</p> <p>24x7x365 technical support including statutory, public and bank holidays.</p> <p>Advance RMA replacement hardware warranty.</p> <p>Direct OEM technical support via portal/telephone/remote access.</p> <p>Online Support case management and reporting portal.</p> <p>Free security updates and patches.</p> <p>Free software download, updates, upgrades & maintenance.</p> <p>VIP access to Senior Technical Resource Team (priority queues for support cases, routed to senior level engineers, etc.).</p> <p>Remote consulting engagement for 4 hours per year (proactive health check, basic troubleshooting, demonstration on best practices for configuring, performance and feature optimization, etc.).</p> <p>Malware sample handling for priority malware analysis.</p>
Warranty	36 months from the date of activation of the subscriptions/device registration	36 months from the date of activation of the subscriptions/device registration
Installation	Product should be installed and commissioned by the bidder.	Product should be installed and commissioned by the bidder.
Configuration Assurance Check	Configuration Assurance Check report directly from OEM should be provided after successful installation.	Configuration Assurance Check report directly from OEM should be provided after successful installation.
Professional Services	Professional Services directly from OEM should be included for minimum of 16 hours. OEM part numbers of such services should be submitted.	Professional Services directly from OEM should be included for minimum of 16 hours. OEM part numbers of such services should be submitted.

2

Tender Document Reference	As in Tender Document		Amended as
	Technical Training	OEM Certification Training with online exam voucher should be included for minimum of 03 (three) persons. Course name, curriculum with OEM part numbers should be submitted.	OEM Certification Training with online exam voucher should be included for minimum of 03 (three) persons. Course name, curriculum with OEM part numbers should be submitted.

Note:

1. This Amendment shall be an integral part of the Tender Document.
2. All other terms & conditions of the Invitation for the Supply & Installation of Plant & Equipment of BTRC Network and Server Co-Location Center (National) published earlier shall remain unchanged.


 (Abdullah Al Mamun) 3/5/2023
 Director General
 Administration Division, BTRC.