I O N
C&IT Svcs Dte

Subject: **Technical Evaluation for Procurement of SSL-VPN Solution to Connect Remote Sites with Primary Data Center (PDC) and Secondary Data Center (SDC) Tender # NADRA-HQ-RFB-42/2026)**

Reference: NADRA-HQ-RFB-42/2026-ANDI91 dated 15 April, 2026

1. With reference to the subject noted above, it is intimated that technical evaluation report duly signed by the concerned officer is attached as Annex-A.

2. Forwarded for your information/further necessary action please.

for Misbah

Deputy Director (Admin)
(Khizer Misbah)

Director (R&S): _____

NADRA/C&IT Svcs/R&S/40 Dated 18 May 2026

To: Admin-Procurement

Procurement of SSL-VPN solution to connect Remote sites with Primary Datacenter and Secondary Data Center (SDC) with three years Support, warranty and Subscriptions (Tender # NADRA-HQ-RFB-42/2026)

S #	Firms / Vendors	M/S CNS	M/S Commtel	M/S Inara	M/S MPCL JAZZ	M/S Premier	M/S PTCL
	BOQ	FPR4225-NGFW-K9,Cisco Secure Firewall 4225 NGFW Appliance, 1U, 2xNetMod Bays, Qty 4, CON-SNC-FPR4225N SNTC-NCD Cisco Secure Firewall 4225 NGFW Applianc qty 4, FPR4K-XNM-8X10G Cisco Secure Firewall 4200 8X10G SFP+ Netmod qty4, CON-SNC-FPR4KX10 SNTC-NCD Cisco Secure Firewall 4200 8X10G SFP Ne qty 4, SFP-10G-SR-S 10GBASE-SR SFP Module, Enterprise-Class qty 8,FPR4200-PWR-AC Cisco Secure Firewall 4200 Series AC Power Supply qty 4,PWR-CAB-AC-BLK Power Cord, 20A, C20-C21, BLK qty 8, SF-F42H-TD7.4-K9 Threat Defense software v7.4 for 4200 Series appliances qty 4,SFP-10G-SR-S 10GBASE-SR SFP Module, Enterprise-Class qty 16, SFP-25G-SR-S 25GBASE-SR SFP Module qty 16, GLC-TE 1000BASE-T SFP transceiver module for Category 5 copper wire qty 8, FPR4200-SSD1800 Cisco Secure Firewall 4200 Series 1.8TB SSD qty 8, FPR4200-SLD-RAILS Cisco Secure Firewall 4200 Slide Rail Kit qty 4, CAB-CONS-RJ45-DB9 Console Cable 6ft with RJ45 and DB9F qty 4, FPR4225-BSE Cisco Secure Firewall 4225 Base License qty 4, FPR4200-PWR-AC Cisco Secure Firewall 4200 Series AC Power Supply qty 4, FPR4200-FAN Cisco Secure Firewall 4200 Series Fan qty 12, FPR4200-NM-BLANK Cisco Secure Firewall 4200 Network Module Blank Slot Cover qty 4, L-FPR4225T-TM= Cisco Secure Firewall 4225 Threat Defence and AMP Licenseqty 4, L-FPR4225T-TM-3Y Cisco Secure Firewall 4225 Threat Defence and Malware3Y Subs qty 4, SF-FMC-VMW-10-K9 Cisco Firepower anagement Center, (VMWare) for 10 devices qty 4,CON-L1SW-SFFMCK9V ENH SW Cisco Firepower Mana qty 4, ST-SEC-BUN-DISTI Cisco Secure Network Analytics Security BUN Disti+T2 Partner 1 ST-SEC-SUB Cisco Stealthwatch Enterprise XaaS ubscription qty 1, ST-FR-100-LIC Cisco Secure Network Analytics Flow Rate License - 100 Pack qty 10, SVS-ST-SEC-SUP-B Cisco Support Standard for Secure Network Analytics qty 1, L-ST-SMC-VE-K9 Cisco Secure Network Analytics Mgmt Console Virtual Edition qty 2, L-ST-FC-VE-K9 Cisco Secure Network Analytics Flow Collector Virt Edition qty 4, L-ST-DS-VE-K9 Cisco Secure Network Analytics Data Store Virtual Appliance qty 4, L-AC-PLS-LIC= Secure Client Advantage Term License, Total Unique Users qty 17000, DETAILS TECHNICAL BOQ, L-AC-PLS-3Y-S8 Cisco AnyConnect Plus License, 3YR,10K-24999 Users 17000,R-ISE-VMC-K9= Cisco ISE Virtual Machine Common PID 2 CON-L1SW-RISE9KVM ENH SW Cisco ISE Virtual Ma qty 2,ISE-SEC-SUB Cisco Identity Service Engine Subscription qty 1,ISE-E-LIC Cisco Identity Service Engine Essentials Subscription qty 17000, SVS-ISE-SUP-B Cisco Support Standard for ISE qty 1,UCS-M8-MLB UCS M8 RACK MLB qty 1,DC-MGT-SAAS Cisco Intersight SaaS qty 1,DC-MGT-IS-SAAS-ES Infrastructure Services SaaS/CVA - Essentials qty 4,UCSC-C220-M8S UCS C220 M8 Rack w/o CPU, mem, drives, 1U w SFF backplaneqty 4, CON-L1NCO-UCSCC28E CX LEVEL 1 8X7XNCDOS UCS C220 M8 Rack w/o CPU, mem, drives, 1 qty 4, IMM-MANAGED Deployment mode for UCS Fi connected Servers in IMM mode qty 4,UCSC-O-ID10GC-D Intel X710T2LOCPV3G1L 2x10GbE RJ45 OCP3.0 NIC qty 4,UCS-M2-HWRAID2 Cisco Boot optimized M.2 Raid controller for SATA drives qty 4,UCS-M2-480G-D 480GB M.2 SATA SSD qty 8,UCS-TPM-002D-D TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant qty 4, UCSC-RAIL-D Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers qty 4,UCS-CPU-I6521P Intel I6521P 2.6GHz/225W 24C/144MB DDR5 6400MT/s qty 4, UCS-MRX64G2RE5 64GB DDR5-6400 RDIMM 2Rx4 (16Gb) qty 16,UCSC-RIS1A-220M8 UCS C220 M8 Riser 1A PCIe Gen5 x16 HH qty 4, UCSC-RAID-M1L16 24G Tri-Mode M1 RAID Controller w/4GB FBWC 16 Drv 4,UCS-NVB3T8M2V 3.8TB 2.5in U.3 15mm Micron 7500 Hg Perf Med End 1X NVMe qty 16, UCSC-PSU1-1200W-D 1200w AC Titanium Power Supply for C-series Rack	Query Response:FPR4225-NGFW-K9 Cisco Secure Firewall 4225 NGFW Appliance, 1U, 2xNetMod Bays, 4, CON-SNC-FPR4225N SNTC-NCD Cisco Secure Firewall 4225 NGFW Appliance 4, FPR4K-XNM-8X10G Cisco Secure Firewall 4200 8X10G SFP+ Netmod 4, CON-SNC-FPR4KX10 SNTC-NCD Cisco Secure Firewall 4200 8X10G SFP Ne 4, SFP-10G-SR-S 10GBASE-SR SFP Module, Enterprise-Class 8 FPR4200-PWR-AC Cisco Secure Firewall 4200 Series AC Power Supply 4, PWR-CAB-AC-BLK Power Cord, 20A, C20-C21, BLK 8 SF-F42H-TD7.4-K9 Threat Defense software v7.4 for 4200 Series appliances 4 SFP-10G-SR-S 10GBASE-SR SFP Module, Enterprise-Class 16, SFP-25G-SR-S 25GBASE-SR SFP Module qty 16 GLC-TE 1000BASE-T SFP transceiver module for Category 5 copper wire 8 FPR4200-SSD1800 Cisco Secure Firewall 4200 Series 1.8TB SSD qty 8 FPR4200-SLD-RAILS Cisco Secure Firewall 4200 Slide Rail Kit 4, CAB-CONS-RJ45-DB9 Console Cable 6ft with RJ45 and DB9F 4 FPR4225-BSE Cisco Secure Firewall 4225 Base License 4, FPR4200-PWR-AC Cisco Secure Firewall 4200 Series AC Power Supply 4, FPR4200-FAN Cisco Secure Firewall 4200 Series Fan 12 FPR4200-NM-BLANK Cisco Secure Firewall 4200 Network Module Blank Slot Cover 4, L-FPR4225T-TM= Cisco Secure Firewall 4225 Threat Defense and AMP Licenseqty 4, L-FPR4225T-TM-3Y Cisco Secure Firewall 4225 Threat Defence and Malware3Y Subs qty 4, SF-FMC-VMW-10-K9 Cisco Firepower Management Center, (VMWare) for 10 devices 4, CON-L1SW-SFFMCK9V ENH SW Cisco Firepower Mana 4 ST-SEC-BUN-DISTI Cisco Secure Network Analytics Security BUN-Disti+T2 Partner 1, ST-SEC-SUB Cisco Stealthwatch Enterprise XaaS Subscription 1, ST-FR-100-LIC Cisco Secure Network Analytics Flow Rate License - 100 Pack 10, SVS-ST-SEC-SUP-B Cisco Support Standard for Secure Network Analytics 1, L-ST-SMC-VE-K9 Cisco Secure Network Analytics Mgmt Console Virtual Edition 1, L-ST-FC-VE-K9 Cisco Secure Network Analytics Flow Collector Virt Edition 4, L-ST-DS-VE-K9 Cisco Secure Network Analytics Data Store Virtual Appliance 4, L-AC-PLS-LIC= Secure Client Advantage Term License, Total Unique Users 17000, L-AC-PLS-3Y-S8 Cisco AnyConnect Plus License, 3YR,10K-24999 Users 17000,R-ISE-VMC-K9= Cisco ISE Virtual Machine Common PID 2, CON-L1SW-RISE9KVM ENH SW Cisco ISE Virtual Ma 2, ISE-SEC-SUB Cisco Identity Service Engine Subscription 1, ISE-E-LIC Cisco Identity Service Engine Essentials Subscription 17000, SVS-ISE-SUP-B Cisco Support Standard for ISE 1, UCS-M8-MLB UCS M8 RACK MLB 1, DC-MGT-SAAS Cisco Intersight SaaS 1, DC-MGT-IS-SAAS-ES Infrastructure Services SaaS/CVA - Essentials 4 SVS-DCM-SUPT-BAS Cisco Support Standard for DCM 1, DC-MGT-UCSC-1S UCS Central Per Server – 1, Server License 4 DC-MGT-ADOPT-BAS Intersight - Virtual adopt session http://cs.co/requestCSS 1 SAAS-OTHER Other Use Case 1 UCSC-C220-M8S UCS C220 M8 Rack w/o CPU, mem, drives, 1U w SFF backplane 4, CON-L1NCO-UCSCC28E CX LEVEL 1 8X7XNCDOS UCS C220 M8 Rack wo CPU, mem, drives, 1 4 IMM-MANAGED Deployment mode for UCS Fi connected Servers in IMM mode 4 UCSC-O-ID10GC-D Intel X710T2LOCPV3G1L 2x10GbE RJ45 OCP3.0 NIC 4 UCS-M2-HWRAID2 Cisco Boot optimized M.2 Raid controller for SATA drives 4 UCS-M2-480G-D 480GB M.2 SATA SSD 8 UCS-TPM-002D-D TPM 2.0 TCG FIPS140-2 CC+ Cert M7 Intel MSW2022 Compliant 4 UCSC-RAIL-D Ball Bearing Rail Kit for C220 & C240 M7/M8 rack servers 4 UCS-CPU-I6521P Intel I6521P 2.6GHz/225W 24C/144MB DDR5 6400MT/s 4 UCS-MRX64G2RE5 64GB DDR5-6400 RDIMM 2Rx4 (16Gb) 16 UCSC-RIS1A-220M8 UCS C220 M8 Riser 1A PCIe Gen5 x16 HH 4 UCSC-RAID-M1L16 24G Tri-Mode M1 RAID Controller w/4GB FBWC 16Drv 4, UCS-	(Pg-8)PDC VPN Firewall x 2: FG-2601F: 4x 100GE/40GE QSFP28 slots, 16x 25GE/10GE SFP28 slots, 16x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with 2x 960GB onboard storage qty 2,FC-10-F26F1-950-02-36,Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) qty 2,FN-TRAN-SFP28-SR: 25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots qty 8, FN-TRAN-SFP+SR: 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty 16,FG-VDOM-5-UG: Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDO qty 2, FC-10-F26F1-210-02-36, Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty 2, PDC Logging Hardware x 1: FAZ-1000G: Centralized logging & analysis appliance - 2x 2.5GbE RJ45 + 2 x 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs qty 1, FC-10-AZ1KG-247-02-36, FortiCare Premium Support qty 1,FN-TRAN-SFP+SR: 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty 2, FC-10-AZ1KG-210-02-36 qty 1,PDC FortiAuthenticator Hardware x 2: FAC-3000F: Identity and Access Management - 4 x GE RJ45 ports, 2 x 10GE SFP+, 4 TB SAS storage. Base License supports up to 40,000 users. Expand user support to 240,000 users by using FortiAuthenticator Hardware Upgrade License. qty2,FN-TRAN-SFP+SR 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty4, SDC VPN Firewall x 2,FG-2601F,4x 100GE/40GE QSFP28 slots, 16x 25GE/10GE SFP28 slots, 16x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports,SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with 2x 960GB onboard storage qty 2,FN-TRAN-SFP28-SR, 25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots qty 8, FN-TRAN-SFP+SR10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty16,PDC Logging Hardware x 1,FAZ-1000Centralized logging & analysis appliance - 2x 2.5GbE RJ45 + 2 x 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs. qty1,FN-TRAN-SFP+SR,10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty2,PDC FortiAuthenticator Hardware x 2,FAC-3000F,Identity and Access Management - 4 x GE RJ45 ports, 2 x 10GE SFP+, 4 TB SAS storage. Base License supports up to 40,000,users. Expand user support to 240,000 users by using FortiAuthenticator Hardware Upgrade License. qty2,FN-TRAN-SFP+SR 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty4, SDC VPN Firewall x 2,FG-2601F,4x 100GE/40GE QSFP28 slots, 16x 25GE/10GE SFP28 slots, 16x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports,SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with 2x 960GB onboard storage qty 2, FN-TRAN-SFP28-SR, 25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems withSFP28 slots qty 8,FN-TRAN-SFP+SR 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty 16,SDC Logging Hardware x 1, FAZ-1000Centralized logging & analysis appliance - 2x 2.5GbE RJ45 + 2 x 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs. qty1,FC-10-AC3KF-210-02-36,Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty 2, 17K Mobile Token,FTM-ELIC-2000, Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 2000 users. Electronic license certificate. License transfer between devices is not allowed. qty 1, FTM-ELIC-5000: Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5000 users. Electronic license certificate. License transfer between devices is not allowed. qty 1, FTM-ELIC-10000, Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10000 users. Electronic license certificate. License transfer between devices is not allowed qty 1,SDC VPN Firewall x 2, FG-2601F, 4x 100GE/40GE QSFP28 slots, 16x 25GE/10GE SFP28 slots, 16x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with 2x 960GB onboard storage qty 2, FC-10-F26F1-950-02-36, Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) qty 2, FN-TRAN-SFP28-SR, 25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots qty 8, FN-TRAN-SFP+SR, 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty 16,FG-VDOM-5-UG , Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity qty 2, FC-10-F26F1-210-02-36, Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty 2, SDC Logging Hardware x 1, FAZ-1000G, Centralized logging & analysis appliance - 2x 2.5GbE RJ45 + 2 x 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs. qty 1. FC-10-AZ1KG-247-02-36, FortiCare Premium Support qty 1, FN-TRAN-SFP+SR, 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty 2, FC-10-AZ1KG-210-02-36, Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty 1, SDC FortiAuthenticator Hardware x 2, FAC-3000F, Identity and Access Management - 4 x GE RJ45 ports, 2 x 10GE SFP+, 4 TB SAS storage. Base License supports up to 40,000 users. Expand user support to 240,000 users by using FortiAuthenticator Hardware Upgrade License qty 2, FC-10-AC3KF-247-02-36, FortiCare Premium Support qty 2, FN-TRAN-SFP+SR, 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty 4, FC-10-AC3KF-210-02-36, Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty 2, Firewall	(Pg-57)FG-2601F,4x 100GE/40GE QSFP28 slots, 16x 25GE/10GE SFP28 slots, 16x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports,SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with 2x 960GB onboard storage qty 2.FN-TRAN-SFP28-SR,25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots qty 8, FN-TRAN-SFP+SR10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty16, FG-VDOM-5-UG, Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity qty2, FC-10-F26F1-210-02-36, FortiGate-2601F 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty2, PDC Logging Hardware x 1,FAZ-1000GFortiAnalyzer-1000G Centralized logging & analysis appliance - 2x 2.5GbE RJ45 + 2 x 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs. qty1, FC-10-AZ1KG-247-02-36FortiAnalyzer-1000G 3 Year FortiCare Premium Support,qty1, FN-TRAN-SFP+SR, 10GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty2, FC-10-AZ1KG-210-02-36 , FortiAnalyzer-1000G 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty1, PDC FortiAuthenticator Hardware x 2, FAC-3000F, FortiAuthenticator-3000F Identity and Access Management - 4 x GE RJ45 ports, 2 x 10GE SFP+, 4 TB SAS storage. Base License supports up to 40,000 users. Expand user support to 240,000 users by using FortiAuthenticator Hardware Upgrade License. qty2, FC-10-AC3KF-247-02-36 FortiAuthenticator-3000F 3 Year FortiCare Premium Suppor qty2, FN-TRAN SFP+SR 10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty4, FC-10-AC3KF-210-02-36FortiAuthenticator-3000F 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty2, 17K Mobile Token, FTM-ELIC-2000FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 2000 users. Electronic license certificate. License transfer between devices is not allowed.qty1, FTM-ELIC-5000, FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5000 users. Electronic license certificate. License transfer between devices is not allowed. qty1, FTM-ELIC-10000, FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10000 users. Electronic license certificate. License transfer between devices is not allowed. qty1, SDC VPN Firewall x 2, FG-2601F, FortiGate-2601F 4x 100GE/40GE QSFP28 slots, 16x 25GE/10GE SFP28 slots, 16x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with 2x 960GB onboard storage qty2, FC-10-F26F1-950-02-36 , FortiGate-2601F 3 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) qty2, FN-TRAN-SFP28-SR,25GE SFP28 transceiver module, short range 25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots qty 8,FN-TRAN-SFP+SR, 10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty16, FG-VDOM-5-UG, Virtual Domain License Add 5 Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity. qty2, FC-10-F26F1-210-02-36, FortiGate-2601F 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty2, PDC Logging Hardware x 1,FAZ-1000GFortiAnalyzer-1000G Centralized logging & analysis appliance - 2x 2.5GbE RJ45 + 2 x 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs. qty1, FC-10-AZ1KG-247-02-36FortiAnalyzer-1000G 3 Year FortiCare Premium Support,qty1, FN-TRAN-SFP+SR, 10GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty2, FC-10-AZ1KG-210-02-36 , FortiAnalyzer-1000G 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty1, PDC FortiAuthenticator Hardware x 2, FAC-3000F, FortiAuthenticator-3000F Identity and Access Management - 4 x GE RJ45 ports, 2 x 10GE SFP+, 4 TB SAS storage. Base License supports up to 40,000 users. Expand user support to 240,000 users by using FortiAuthenticator Hardware Upgrade License. qty2, FC-10-AC3KF-247-02-36 FortiAuthenticator-3000F 3 Year FortiCare Premium Suppor qty2, FN-TRAN SFP+SR 10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty4, FC-10-AC3KF-210-02-36 FortiAuthenticator-3000F 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty2, 17K Mobile Token, FTM-ELIC 2000 FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 2000 users. Electronic license certificate. License transfer between devices is not allowed. qty1, FTM-ELIC 5000 FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 5000 users. Electronic license certificate. License transfer between devices is not allowed qty1, FTM-ELIC 10000 FortiTokenMobile (Electronic License) Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10000 users. Electronic license certificate. License transfer between devices is not allowed. qty1, SDC VPN Firewall x 2, FG-2601F, FortiGate-2601F 4x 100GE/40GE QSFP28 slots, 16x 25GE/10GE SFP28 slots, 16x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with 2x 960GB onboard storage qty2, FC-10-F26F1-950-02-36 , FortiGate-2601F 3 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) qty2, FN-TRAN-SFP28-SR,25GE SFP28 transceiver module, short range 25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots qty8, FN-TRAN-SFP+SR, 10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty16, FG-VDOM-5-UG, Virtual Domain License Add 5 Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity. qty2, FC-10-F26F1-210-02-36,FortiGate-2601F 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty2, PDC Logging Hardware x 1, FAZ-1000G Centralized logging & analysis appliance - 2x 2.5GbE RJ45 + 2 x 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs. qty1, FC-10-AZ1KG-247-02-36 , FortiAnalyzer-1000G 3 Year FortiCare Premium Support, qty1, FN-TRAN-SFP+SR,10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty2, FC-10-AZ1KG-210-02-36 FortiAnalyzer-1000G 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty1, SDC FortiAuthenticator Hardware x 2, FAC-3000F, FortiAuthenticator-3000F Identity and Access Management - 4 x GE RJ45 ports, 2 x 10GE SFP+, 4 TB SAS storage. Base License supports up to 40,000 users. Expand user support to 240,000 users by using FortiAuthenticator Hardware Upgrade License. qty2, FC-10-AC3KF-247-02-36 , FortiAuthenticator-3000F 3 Year FortiCare Premium Support qty2, FN-TRAN-SFP+SR, 10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty4, FC-10-AC3KF-210-02-36 , FortiAuthenticator-3000F 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty2, Firewall Training, FT-ILT-D03, 3-day virtual instructor-led training. Standard NSE training content One enrollment per student in a 3-day virtual instructor-led training session or any onsite classroom session available in the public schedule.Includes standard NSE training content, instructor facilitation, course material, and lab access.Upcoming	(Pg-65)PDC VPN Firewall x 2,FG-2601F,FortiGate-2601F 4x 100GE/40GE QSFP28 slots, 16x 25GE/10GE SFP28 slots, 16x 10GE RJ45 ports, 2x 10G SFP+ HA slots, 2x 1G MGMT ports, SPU NP7 and CP9 hardware accelerated, and dual AC power supplies with 2x 960GB onboard storage qty2,FC-10-F26F1-950-02-36FortiGate-2601F 3 Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) qty 2, FN-TRAN SFP28-SR25GE SFP28 transceiver module, short range 25 GE / 10 GE SFP28 transceiver module, short range 100m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP28 slots qty 8, FN-TRAN SFP+SR10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty16, FG-VDOM 5-UGVirtual Domain License Add 5 Upgrade license for adding 5 VDOMs to FortiOS 5.4 and later, limited by platform maximum VDOM capacity. qty 2, FC-10-F26F1-210-02-36FortiGate-2601F 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty 2, PDC LoggingHardware x 1,AZ 1000GFortiAnalyzer-1000G Centralized logging & analysis appliance - 2x 2.5GbE RJ45 + 2 x 25GbE SFP28, 32TB storage, up to 660 GB/Day of Logs qty1, FC-10-AZ1KG 247-02-36FortiAnalyzer-1000G 3 Year FortiCare Premium Support qty1, FN-TRAN SFP+SR10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty2, C-10-AZ1KG 210-02-36FortiAnalyzer-1000G 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty 1, PDC FortiAuthenticatorHardware x 2, FAC 3000F FortiAuthenticator-3000F Identity and Access Management - 4 x GE RJ45 ports, 2 x 10GE SFP+, 4 TB SAS storage. Base License supports up to 40,000 users. Expand user support to 240,000 users by using FortiAuthenticator Hardware Upgrade License qty2, FC-10-AC3KF 247-02-36 FortiAuthenticator-3000F 3 Year FortiCare Premium Suppor qty2, FN-TRAN SFP+SR 10GE SFP+ transceiver module, short range 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots qty4, FC-10- AC3KF 210-02-36 FortiAuthenticator-3000F 3 Year Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite) qty2, Firewall Training, FT-ILT D03, 3-day virtual instructor-led training. Standard NSE training content One enrollment per student in a 3-day virtual instructor-led training session or any onsite classroom session available in the public schedule. Includes standard NSE training content, instructor facilitation, course material, and lab access.Upcoming
1	**Bidder must have NGFW or SSL-VPN deployment in Pakistan in years (2021-2026). Provide two P.O in any of Years (2021-2026).**	**P.Os of NADRA, LMKR, CPPA, MCB etc. are attached (pg-135)**	**P.Os of PAK SECTT (Pg-35), Dow University (Pg-94) attcehd**	**P.Os of Agha Khan Hospital, (Pg-116), Ubank (Pg-132), Parco (Pg-137) attached**	**P.Os of Allama Iqbal open Univeristy, Sindh Institute of Physical Medicine, EOBI, KPT etc. attached (Pg-82)**	**P.Os of NADRA,Askari bank, DG I&P etc. (Pg-223, 265, 334)**	**P.Os of ZTBL, PPAF, Neelam Jhelum Hydro Powe, Finja (Pg-74)**
2	**Letter of compliance with the statement "Bidder fully agreed and complied all Sections/parts/Annexures of RFP"**	**Letter provided (Pg 16)**	**Provided (Pg-97)**	**Letter provided (Pg-149)**	**Query reply Letter Provided**	**Letter provided (Pg-20)**	**Letter Provided (Pg-10)**
3	**Bidder must be OEM Authorized Partner / OEM Authorized Reseller / OEM Authorized Distributer /OEM Authorized Dealer. Bidder must submit MAL of OEM.**	**Cisco (Pg-25), OpenSpan (Query reply)**	**letters from OpenSpan,Cisco attached (Pg-98-99)**	**letter of Fortinet attached (Pg-88)**	**letter attached (Pg-55)**	**Letter provided (Pg-88)**	**Query Respose, Letter provided**
4	**Completely filled compliance sheet given in this document**	**Compliance Sheet (Pg 35)**	**attached (Pg-101)**	**Provided (Pg-69)**	**Compliance sheet Shared (Pg-10)**	**Provided (Pg-23)**	**Compliance sheet (Pg-11)**

S#	Feature	Requirement	Compliance (Fully-Comply/Not-Comply)	Remarks	Compliance (Fully-Comply/Not-Comply)	Remarks	Compliance (Fully-Comply/Not-Comply)	Remarks	Compliance (Fully-Comply/Not-Comply)	Remarks	Compliance (Fully-Comply/Not-Comply)	Remarks	Compliance (Fully-Comply/Not-Comply)	Remarks
Connectivity Scenario														
Connectivity Requirements														
1	Primary Data Center (PDC) and Secondary Data Center (SDC) must be equipped with redundant Perimeter firewalls installed for protection from the internet threats with all the features mentioned in this document.	Redundant Perimeter firewall at PDC and SDC	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query response, Fully-Comply	Fully-Comply	offered 2 x FG-2601F in HA at PDC and SDC with UTP protection	Fully- Comply	offered 2 x FG-2601F in HA at PDC and SDC with UTP protection	Fully-Comply	offered 2 x FG-2601F in HA at PDC and SDC with UTP protection	Fully-Comply	offered 2 x FG-2601F in HA at PDC and SDC with UTP protection
2	PDC and SDC must be equipped with redundant SSL-VPN central site solution with all the features mentioned in this document.	Redundant SSL-VPN Solution at PDC and SDC	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	the VPN solution is built-in on the offered firewall	Fully- Comply	the VPN solution is built-in on the offered firewall.	Fully-Comply	the VPN solution is built-in on the offered firewall	Fully-Comply	the VPN solution is built-in on the offered firewall.
3	All configuration/data sync between PDC and SDC	Replication	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	As per the clarification received, the purpose/objective of this clause is to have remote user connectivity to PDC and SDC should be automatic/manual, in case of issue at PDC	Fully- Comply	As per the clarification received, the purpose/objective of this clause is to have remote user connectivity to PDC and SDC should be automatic/manual, in case of issue at PDC	Fully-Comply	As per the clarification received, the purpose/objective of this clause is to have remote user connectivity to PDC and SDC should be automatic/manual, in case of issue at PDC	Fully-Comply	As per the clarification received, the purpose/objective of this clause is to have remote user connectivity to PDC and SDC should be automatic/manual, in case of issue at PDC

4	SSL-VPN client software will be installed at remote users. This can be web based but must comply all requirements of this RFP.	SSL-VPN Client	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query response, Fully-Comply	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download supports both SSL and IPSec VPN	Fully- Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download supports both SSL and IPSec VPN from	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download supports both SSL and IPSec VPN from	Fully-Comply	FortiClient software would be installed on remote users. Free VPN only standalone FortiClient version is available to download supports both SSL and IPSec VPN
5	Monitoring from central dashboard at PDC	Central Dashboard	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	The proposed solution provides centralized monitoring from the PDC via FortiAnalyzerdeployed at PDC. All firewall clusters and FortiAuthenticator deployed at both PDC and SDC forward logs and security events to the FortiAnalyzer at PDC.	Fully- Comply	The proposed solution provides centralized monitoring from the PDC via FortiAnalyzer deployed at PDC. All firewall clusters and FortiAuthenticator deployed at both PDC and SDC forward logs and security events to the FortiAnalyzer at PDC	Fully-Comply	The proposed solution provides centralized monitoring from the PDC via FortiAnalyzer deployed at PDC. All firewall clusters and FortiAuthenticator deployed at both PDC and SDC forward logs and security events to the FortiAnalyzer at PDC.	Fully-Comply	The proposed solution provides centralized monitoring from the PDC via FortiAnalyzer deployed at PDC. All firewall clusters and FortiAuthenticator deployed at both PDC and SDC forward logs and security events to the FortiAnalyzer at PDC
6	In case any issue at PDC, remote user will automatically connect with SDC as per configured policy (This process must allow both options i.e. Automatically and manually). This switching must be transparent for remote user	PDC to SDC Switching	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query response, Fully-Comply	Fully-Comply	Automatic and manual VPN failover from PDC to SDC is supported via common FQDN and secondary gateway configuration, with FortiAuthenticator for remote user authentication.	Fully- Comply	Automatic and manual VPN failover from PDC to SDC is supported via common FQDN and secondary gateway configuration, with FortiAuthenticator for remote user authentication.	Fully-Comply	Query Resposne: Automatic and manual VPN failover from PDC to SDC is supported via common FQDN and secondary gateway configuration, with FortiAuthenticator for remote user authentication	Fully-Comply	Automatic and manual VPN failover from PDC to SDC is supported via common FQDN and secondary gateway configuration, with FortiAuthenticator for remote user authentication
7	Monitoring from central dashboard at SDC	Central Dashboard	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	The proposed solution provides centralized monitoring from the SDC via FortiAnalyzer deployed at SDC. All firewall clusters and FortiAuthenticator deployed at both PDC and SDC forward logs and security events to the FortiAnalyzer at SDC	Fully- Comply	The proposed solution provides centralized monitoring from the SDC via FortiAnalyzer deployed at SDC. All firewall clusters and FortiAuthenticator deployed at both PDC and SDC forward logs and security events to the FortiAnalyzer at SDC.	Fully-Comply	The proposed solution provides centralized monitoring from the SDC via FortiAnalyzer deployed at SDC. All firewall clusters and FortiAuthenticator deployed at both PDC and SDC forward logs and security events to the FortiAnalyzer at SDC	Fully-Comply	The proposed solution provides centralized monitoring from the SDC via FortiAnalyzer deployed at SDC. All firewall clusters and FortiAuthenticator deployed at both PDC and SDC forward logs and security events to the FortiAnalyzer at SDC.
8	In case issue resolved at PDC, remote user will automatically switch back to PDC as per configured policy (This process must allow both options i.e. Automatically and manually). This switching will be transparent for remote user	SDC to PDC Switching	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query response, Fully-Comply	Fully-Comply	When PDC service is restored, new connections are automatically directed to PDC via DNS resolution. The existing users connected to SDC reconnect to the PDC gateway upon session reauthentication, timeout, or administrator-triggered reconnection	Fully- Comply	When PDC service is restored, new connections are automatically directed to PDC via DNS resolution. The existing users connected to SDC reconnect to the PDC gateway upon session reauthentication, timeout, or administrator-triggered reconnection	Fully-Comply	When PDC service is restored, new connections are automatically directed to PDC via DNS resolution. The existing users connected to SDC reconnect to the PDC gateway upon session reauthentication, timeout, or administrator-triggered reconnection.	Fully-Comply	When PDC service is restored, new connections are automatically directed to PDC via DNS resolution. The existing users connected to SDC reconnect to the PDC gateway upon session reauthentication, timeout, or administrator-triggered reconnection.
Hardware Based Next Generation Firewall (Perimeter Firewall)															
Perimeter Firewalls															
1	Next Generation Firewall Throughput	20Gbps	Fully-Comply	80 Gbps	Fully-Comply	80 Gbps	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
2	IPS Throughput	20Gbps	Fully-Comply	80 Gbps	Fully-Comply	80 Gbps	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
3	Concurrent sessions	12 Million	Fully-Comply	30 Million	Fully-Comply	30 Million	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
4	Connections Per Seconds	500,000	Fully-Comply	600k	Fully-Comply	600k	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
5	Policies	100,000	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
6	Storage Support (Usable)	1TB	Fully-Comply	1.8 TB x 2	Fully-Comply	1.8 TB x 2	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
7	Threat protection throughput	20Gbps	Fully-Comply	80 Gbps	Fully-Comply	80 Gbps	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
8	SSL/TLS Inspection throughput	15Gbps	Fully-Comply	30 Gbps	Fully-Comply	30 Gbps	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
9	SSL VPN Throughput	15Gbps	Fully-Comply	30 Gbps	Fully-Comply	30 Gbps	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
Interfaces															
1	25 GE SFP28 interfaces with matched transceivers	4	Fully-Comply	8x 1/10/25 Gigabit Ethernet ports (SFP28	Fully-Comply	8x 1/10/25 Gigabit Ethernet ports (SFP28	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
2	10 GE SFP+ interfaces with matched transceivers	8	Fully-Comply	8 x 1/10 Gigabit Ethernet Small Form-Factor Pluggable (SFP+) network modules	Fully-Comply	8 x 1/10 Gigabit Ethernet Small Form Factor Pluggable (SFP+) network modules	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
3	1/10 GE RJ45	2	Fully-Comply	2 x 1/10/25 Gigabit Ethernet ports (SFP28	Fully-Comply	2 x 1/10/25 Gigabit Ethernet ports (SFP28	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
4	All interfaces must be fully populated with matched transceivers and ready to use	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
5	HA Port	Yes	Fully-Comply	HA will be established via fixed ports	Fully-Comply	HA will be established via fixed ports	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
6	Console Port	Yes	Fully-Comply	1 x RJ-45 console	Fully-Comply	1 x RJ-45 console	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
7	Management Port RJ-45	Yes	Fully-Comply	2 x 1/10/25 Gigabit Ethernet ports (SFP28)	Fully-Comply	2 x 1/10/25 Gigabit Ethernet ports (SFP28)	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
Features															
1	High Availability	Active/Active, Active/Passive, Clustering	Fully-Comply	Active/active and active/ standby, 16	Fully-Comply	Active/active and active/ standby, 16	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
2	Virtual Domains (Each virtual domain will act as a separate virtual firewall in same quoted hardware firewall)	15	Fully-Comply	15 as per compliance sheet	Fully-Comply	Query Response : 15	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
				Query Reply: It is not just round robin.Load will be distributed evenly in the cluster. ,VPN load balancing in FTD allows you group two or more devices logically and distribute remote access VPN sessions among the devices equally. VPN load balancing shares		Query Reply: It is not just round robin. Load will be distributed evenly in the cluster,VPN load balancing in FTD allows you group two or more devices logically and distribute remote access VPN sessions among the devices equally. VPN load balancing shares AnyConnect VPN sessions among the devices in a load balancing group.VPN load balancing is based on simple distribution of traffic without taking into account throughput or other factors. A							

3	Load Balancing (HTTP/HTTPs/TCP/UDP/IP) with multiple methods like Round Robin/Weighted/Least Session	Yes	Fully-Comply	AnyConnect VPN sessions among the devices in a load balancing group. VPN load balancing is based on simple distribution of traffic without taking into account throughput or other factors. A VPN load-balancing group consists of two or more FTD devices. One device acts as the director, and the other devices are member devices. Devices in a group do not need to be of the exact same type, or have identical software versions or configurations. Any FTD device that supports remote access VPN can participate in a load balancing group.All active devices in a VPN load-balancing group carry session loads. VPN load balancing directs traffic to the least-loaded device in the group, distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability	Fully-Comply	VPN load-balancing group consists of two or more FTD devices. One device acts as the director, and the other devices are member devices. Devices in a group do not need to be of the exact same type, or have identical software versions or configurations. Any FTD device that supports remote access VPN can participate in a load balancing group. All active devices in a VPN load-balancing group carry session loads. VPN load balancing directs traffic to the least-loaded device in the group, distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability.	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
4	Zero trust policies	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
5	Malware Protection	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
6	BOTNET protection	Yes	Fully-Comply	Integrated with Cisco AMP	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
7	Support static, dynamic and policy-based routing	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
8	Dynamic Routing Protocols RIPv1/v2, OSPF, BGP	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
9	Multiple virtual routers	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
10	Source Based Routing	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
11	Policy Based Routing	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
12	VLANs	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
13	IPSEC Support, site to site IPSEC VPN	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
14	Aggregations Interfaces / Port-Channel	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
15	Inter-VLAN routing support while applying access rules policies	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
16	NAT Support	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
17	Stateful firewall inspection	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
18	All features must be accessible via web and cli over https, ssh and console	Yes	Fully-Comply	Via FMC	Fully-Comply	Via FMC	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
19	SNMP to poll in NMS and syslog to send logs to syslog server	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query response, Fully-Comply	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
20	Zone Based firewalling	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
21	Multicast Support	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
22	Virtual Routers	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
23	Traffic shaping	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
24	Time based access policies	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
25	SSL Inspection	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
26	SSL/TLS Inspection: Full decryption and inspection of encrypted traffic.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query response, Fully-Comply	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
27	Threat Protection: Must include IPS, antivirus, anti-malware, and sandboxing capabilities.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
28	IPS must have packet logging option	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
29	The IPS must have an option to exempt any IP addresses from specific signatures	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query response, Fully-Comply	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
30	IP Reputation	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
31	Integration with Third party SOAR	Yes	Fully-Comply	Cisco Security and IBM SOAR - Cisco	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
32	Integration with third party SIEM	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
33	All hardware equipment must be Rack Mounted	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
34	All hardware equipment must be Dual Power Supply	yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
35	integration of solution with already deployed external on-prem sandboxing solution	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
36	DNS filtering	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
37	Insider Threat Detection: Ability to detect and respond to suspicious internal activities.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
38	Malware C2 Communication Detection: Detect and block command-and-control (C2) traffic from compromised devices.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Query response Fully Comply	Fully-Comply	Query Response fully comply	Fully-Comply	Complied as per Compliance sheet
39	Deep inspection	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet

40	True least-privileged access so that it Identify applications based on Apps identification at Layer 7. This is to enable precise access control at the app and sub-app levels, independent of network constructs like IP and port numbers.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query response, Fully-Comply	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Query response Fully Comply	Fully-Comply	Query Response fully comply	Fully-Comply	Complied as per Compliance sheet		
41	Full traffic inspection	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet		
Rating																
1	OEM of quoted firewalls must be listed in Gartner MQ for Quoted Firewalls in Leaders/Challengers in any of last two Reports for NGFW/Network-Firewall.	Yes	Fully-Comply	Cisco was challanger in the last Gartner magic quadrant for NGFW of 2022	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	(Pg-89) attached	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	provided (Pg-36)	Fully-Comply	(Pg-89) attached		
SSL VPN Users (17,000 SSL-VPNs)																
Deployment and Hardware																
1	All solution and its components must be deployed on-prem.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Fortigate Firewalls FG-2601F as VPN gateway, FAZ-1000G as hardware logging solution, FAC-3000F as authentication and MFA solution		
2	Solution must be delivered as turnkey solution, if any software required then bidder will be responsible for provision of hardware/server, licensed virtualization, licensed db etc with same warranty and support requirements mentioned in this document.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	all offered solution is OEM hardware based	Fully- Comply	Query response Fully Comply	Fully-Comply	all offered solution is OEM hardware based	Fully-Comply	all offered solution is OEM hardware base		
3	Solution and its components must not be open source	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	onents offered are based on OEM's harden	Fully- Comply		Fully-Comply	The components offered are based on OEM's hardend solution	Fully-Comply	The components offered are based on OEM's hardend solution		
4	Licensing must cover all features required in this RFP.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	l, all licencing offered covers the requried fe	Fully- Comply	refer to the BOM, all licencing offered covers the requried fearture in the RFP	Fully-Comply	refer to the BOM, all licencing offered covers the requried fearture in the RFP	Fully-Comply	refer to the BOM, all licencing offered covers the requried fearture in the RFP		
5	All proposed hardware must have minimum 4 x 10/25 fiber and 4 x 10G fiber ready to use interfaces	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	based on the clarification received, the firewall offered with the required number of interfaces outlined in the RFP. The hardware based logging and authentication solution offered with 2 x 10G	Fully- Comply	based on the clarification received, the firewall offered with the required number of interfaces outlined in the RFP. The hardware based logging and authentication solution offered with 2 x 10G.	Fully-Comply	Query resposne based on the clarification received, the firewall offered with the required number of interfaces outlined in the RFP. The hardware based logging and authentication solution offered with 2 x 10G.	Fully-Comply	based on the clarification received, the firewall offered with the required number of interfaces outlined in the RFP. The hardware based logging and authentication solution offered with 2 x 10G.		
6	If servers are required then solution requirements must be fulfilled by using maximum 4 x Servers at PDC and 4 x Servers at SDC	Yes	Fully-Comply	N/A – Not applicable for dedicated firewall appliances	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	ed solution is based on OEM's provided hard	Fully- Comply	Query Reply: Offered solution is based on OEM's provided hardware	Fully-Comply	Offered solution is based on OEM's provided hardware	Fully-Comply	Offered solution is based on OEM's provided hardware		
7	Bidder can propose ssl-vpn users requirements using same hardware (Firewalls) but must comply for RFP requirements.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Offered solution is based on VPN feature on the fortigate firewall. Fortigate support SSL VPN with FortiOS 7.4 and IPSec VPNs with FortiOS 7.6.3 for secure remote connectivity	Fully- Comply	Offered solution is based on VPN feature on the fortigate firewall. Fortigate support SSL VPN with FortiOS 7.4 and IPSec VPNs with FortiOS 7.6.3 for secure remote connectivity	Fully-Comply	Offered solution is based on VPN feature on the fortigate firewall. Fortigate support SSL VPN with FortiOS 7.4 and IPSec VPNs with FortiOS 7.6.3 for secure remote connectivity	Fully-Comply	Offered solution is based on VPN feature on the fortigate firewall. Fortigate support SSL VPN with FortiOS 7.4 and IPSec VPNs with FortiOS 7.6.3 for secure remote connectivity.		
Scalability																
1	Fully licensed SSL-VPN concurrent users	17,000	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	The solution offered is for concurrent 17K VPN users	Fully- Comply	The solution offered is for concurrent 17K VPN users	Fully-Comply	The solution offered is for concurrent 17K VPN users	Fully-Comply	The solution offered is for concurrent 17K VPN users		
2	Hardware must be scalable to handle 47,000 concurrent SSL VPN users.	Yes	Fully-Comply	via Increasing Firewall	Fully-Comply	Via Increasing firewall	Fully-Comply	As per the clarification received the solution is scaleable to support 47K concurrent VPN users.FG-2601F Concurrent SSL VPN Users 30K (FortiOS 7.4), The solution supports scalability by adding more FortiGate appliances. FG-2601 Max Client to G/W IPSEC Tunnels 100K (FortiOS 7.6+)	Fully- Comply	As per the clarification received the solution is scaleable to support 47K concurrent VPN users. FG-2601F Concurrent SSL VPN Users 30K (FortiOS 7.4), The solution supports scalability by adding more FortiGate appliances. FG-2601 Max Client to G/W IPSEC Tunnels 100K (FortiOS 7.6+)	Fully-Comply	As per the clarification received the solution is scaleable to support 47K concurrent VPN users. FG-2601F Concurrent SSL VPN Users 30K (FortiOS 7.4), The solution supports scalability by adding more FortiGate appliances. FG-2601 Max Client to G/W IPSEC Tunnels 100K (FortiOS 7.6+)	Fully-Comply	As per the clarification received the solution is scaleable to support 47K concurrent VPN users. FG-2601F Concurrent SSL VPN Users 30K (FortiOS 7.4), The solution supports scalability by adding more FortiGate appliances. FG-2601 Max Client to G/W IPSEC Tunnels 100K (FortiOS 7.6+) https://docs.fortinet.com/document/fortigate/7.6.3/fortios-release notes/173430 Also additional user licenses on offered FortiAuthenticator and mobile tokens can		
Total Sites																
1	Primary Data Center (PDC)	1	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Acknowledged	Fully- Comply	Acknowledged	Fully-Comply	Acknowledged	Fully-Comply	Acknowledged		
2	Secondary Data Center (SDC)	1	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Acknowledged	Fully- Comply	Acknowledged	Fully-Comply	Acknowledged	Fully-Comply	Acknowledged		
3	Remote Sites must be able to connect simultaneously	17,000	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	17,000 Remote users at remotes sites will be able to connect simultaneously	Fully- Comply	17,000 Remote users at remotes sites will be able to connect simultaneously	Fully-Comply	17,000 Remote users at remotes sites will be able to connect simultaneously	Fully-Comply	17,000 Remote users at remotes sites will be able to connect simultaneously		
SSL-VPN Security & Access Control																
1	Multi-Factor Authentication (MFA): Bidder must deliver complete MFA mobile app based with the solution for all quoted users.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator FAC-1000F - 40K user licenses offered, scaleable.Mobile Tokens - 17K offered, scaleable	Fully- Comply	FortiAuthenticator FAC-1000F - 40K user licenses offered, scaleable https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAuthenticator.pdf Mobile Tokens - 17K offered, scaleable https://www.fortinet.com/products/identity-access-management/fortitoken	Fully-Comply	FortiAuthenticator FAC-1000F - 40K user licenses offered, scaleable,Mobile Tokens - 17K offered, scaleable	Fully-Comply	FortiAuthenticator FAC-1000F - 40K user licenses offered, scaleable, Mobile Tokens - 17K offered, scaleable		

Pg-4

2	Solution must bind the SSL-VPN user with end device so that same user cannot be used on any other device. Host binding.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator supports device-based host binding for SSL-VPN users through client certificate authentication. FortiAuthenticator acts as a Certificate Authority (CA), issuing unique client certificates per user-device pair. The SSL-VPNon FortiGate is configured to require this client certificate alongside user credentials, ensuring a specific user can only authenticate from the enrolled device	Fully- Comply	FortiAuthenticator supports device-based host binding for SSL-VPN users through client certificate authentication. FortiAuthenticator acts as a Certificate Authority (CA), issuing unique client certificates per user-device pair. The SSL-VPN on FortiGate is configured to require this client certificate alongside user credentials, ensuring a specific user can only authenticate from the enrolled device	Fully-Comply	FortiAuthenticator supports device-based host binding for SSL-VPN users through client certificate authentication. FortiAuthenticator acts as a Certificate Authority (CA), issuing unique client certificates per user-device pair. The SSL-VPN on FortiGate is configured to require this client certificate alongside user credentials, ensuring a specific user can only authenticate from the enrolled device	Fully-Comply	FortiAuthenticator supports device-based host binding for SSL VPN users through client certificate authentication. FortiAuthenticator acts as a Certificate Authority (CA), issuing unique client certificates per user-device pair. The SSL-VPN on FortiGate is configured to require this client certificate alongside user credentials, ensuring a specific user can only authenticate from the enrolled device
3	Identity Integration: Support for integration with AD/LDAP, SAML, OAuth etc.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	via FortiAuthenticator	Fully- Comply	via FortiAuthenticator	Fully-Comply	via FortiAuthenticator	Fully-Comply	via FortiAuthenticator
4	Secure Communication: All communications must be encrypted	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply		Fully- Comply		Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
5	Cross-region Access Management: Manage user access policies across PDC and SDC. The solution at PDC and SDC must be synced at real time so that if user disconnect from PDC and connect at SDC then user will be able to connect using same username, password and 2FA.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	using FortiAuthenticator HA where where both PDC and SDC FACs synchronized users and tokens.	Fully- Comply	using FortiAuthenticator HA where where both PDC and SDC FACs synchronized users and tokens.	Fully-Comply	Query response: using FortiAuthenticator HA where where both PDC and SDC FACs synchronized users and tokens.	Fully-Comply	using FortiAuthenticator HA where where both PDC and SDC FACs synchronized users and tokens
6	Geographic control per user	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups based on policy. FortiGate calls these RADIUS groups in SSL-VPN firewall policies, where Geo-IP based source address restrictions are applied per group, effectively enforcing geographic access control at the per-user level	Fully- Comply	FortiAuthenticator assigns users to RADIUS user groups based on policy. FortiGate calls these RADIUS groups in SSL-VPN firewall policies, where Geo-IP based source address restrictions are applied per group, effectively enforcing geographic access control at the per-user level	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups based on policy. FortiGate calls these RADIUS groups in SSL VPN firewall policies, where Geo-IP based source address restrictions are applied per group, effectively enforcing geographic access control at the per-user level	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups based on policy. FortiGate calls these RADIUS groups in SSL-VPN firewall policies, where Geo-IP based source address restrictions are applied per group, effectively enforcing geographic access control at the per-user level
7	Limit network access only for necessary resources	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	using firewall policies on fortigate	Fully- Comply	using firewall policies on fortigate	Fully-Comply	using firewall policies on fortigate	Fully-Comply	using firewall policies on fortigat
8	Access control on time and date per user or user group. Access policies can be configured time based and date based.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	using schedule feature available on firewall policies	Fully- Comply	using schedule feature available on firewall policies	Fully-Comply	using schedule feature available on firewall policies	Fully-Comply	using schedule feature available on firewall policies,
9	Role based user checks	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups based on their role, synced from AD/LDAP group membership. These groups are returned to FortiGate via RADIUS attributes upon authentication, where role-specific SSL-VPN firewall policies grant or restrict access to resources based on the user's assigned role	Fully- Comply	FortiAuthenticator assigns users to RADIUS user groups based on their role, synced from AD/LDAP group membership. These groups are returned to FortiGate via RADIUS attributes upon authentication, where role-specific SSL-VPN firewall policies grant or restrict access to resources based on the user's assigned role	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups based on their role, synced from AD/LDAP group membership. These groups are returned to FortiGate via RADIUS attributes upon authentication, where role-specific SSL-VPN firewall policies grant or restrict access to resources based on the user's assigned role	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups based on their role, synced from AD/LDAP group membership. These groups are returned to FortiGate via RADIUS attributes upon authentication, where role-specific SSL-VPN firewall policies grant or restrict access to resources based on the user's assigned role
10	Solution must allow to restrict the user with its source IP	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query Response Fully Comply	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups which are returned to FortiGate upon successful authentication. On FortiGate, per-group VPN firewall policies are configured with specific destination IP addresses and ports permitted for each group
11	Allow to restrict access of user groups to their required destinations IP/Ports only. One user group must not able to access the destination IP/Ports of other user groups	Yes	Fully-Comply	Query response: Fully Complied	Fully-Comply	Query Response Fully Comply	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups which are returned to FortiGate upon successful authentication. On FortiGate, per-group VPN firewall policies are configured with specific destination IP addresses and ports permitted for each group	Fully- Comply	FortiAuthenticator assigns users to RADIUS user groups which are returned to FortiGate upon successful authentication. On FortiGate, per group VPN firewall policies are configured with specific destination IP addresses and ports permitted for each group	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups which are returned to FortiGate upon successful authentication. On FortiGate, per-group VPN firewall policies are configured with specific destination IP addresses and ports permitted for each group	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups which are returned to FortiGate upon successful authentication. On FortiGate, per-group VPN firewall policies are configured with specific destination IP addresses and ports permitted for each group
12	Solution must allow option to allow or block split tunneling both on IPV4 and IPV6.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply		Fully- Comply		Fully-Comply		Fully-Comply	
13	Must provide restrictions on per user, user group or all users for destination IP, port	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups which are returned to FortiGate upon successful authentication. On FortiGate, per-group VPN firewall policies are configured with specific destination IP addressesand ports permitted for each group	Fully- Comply	FortiAuthenticator assigns users to RADIUS user groups which are returned to FortiGate upon successful authentication. On FortiGate, per group VPN firewall policies are configured with specific destination IP addresses and ports permitted for each group	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups which are returned to FortiGate upon successful authentication. On FortiGate, per-group VPN firewall policies are configured with specific destination IP addresses and ports permitted for each group	Fully-Comply	FortiAuthenticator assigns users to RADIUS user groups which are returned to FortiGate upon successful authentication. On FortiGate, per-group VPN firewall policies are configured with specific destination IP addresses and ports permitted for each group
14	Prevent one SSL-VPN users to access other SSL-VPN users as well	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply		Fully-Comply		Fully-Comply	Complied as per Compliance sheet

End points														
1	End points can have all available versions of following OS, so solution must support all end points: a. Windows b. Linux c. MAC d. Android	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download	Fully- Comply	Query response Fully Comply	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download
User Management and Onboarding														
1	Self-onboarding portal so that users can onboarded with some verification checks	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
2	Approval portal so that users can be approved by administrators once user onboarded	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
3	Configure users in multiple groups based on certain parameters to apply group-based policies	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator supports assigning users to multiple user groups based on parameters such as AD/LDAP group membership, user attributes, authentication type, or manual assignment. These groups are returned t	Fully-Comply	FortiAuthenticator supports assigning users to multiple user groups based on parameters such as AD/LDAP group membership, user attributes, authentication type, or manual assignment. These groups are returned to FortiGate via RADIUS attributes upon authentication, where group-specific VPN firewall policies enforce access control
4	All users must be centrally managed via single console	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator supports assigning users to multiple user groups based on parameters such as AD/LDAP group membership, user attributes, authentication type, or manual assignment. These groups are returned to FortiGate via RADIUS attributes upon authentication, where group-specific VPN firewall policies enforce access control	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply		Fully-Comply	Complied as per Compliance sheet
5	Push polices centrally for one user, user group or all users	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator allows RADIUS policies to be configured and pushed centrally for an individual user, a specific user group, or all users from a single console. Each RADIUS policy defines authentication method, 2FA requirements, and access criteria	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator allows RADIUS policies to be configured and pushed centrally for an individual user, a specific user group, or all users from a single console. Each RADIUS policy defines authentication method, 2FA requirements, and access criteria	Fully-Comply	FortiAuthenticator allows RADIUS policies to be configured and pushed centrally for an individual user, a specific user group, or all users from a single console. Each RADIUS policy defines authentication method, 2FA requirements, and access criteria
6	Simple and user-friendly UI	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
7	Solution must allow to create all users in the quoted solution.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
8	Solution also allow integration with Radius, LDAP integration	Yes	Fully-Comply	Query response: Fully Complied	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
9	Send passwords and 2FA (QR Code to enable 2FA on end user mobile) directly to end user. The administrator must not have the password and 2FA information of end user.	Yes	Fully-Comply	Query response: Fully Complied	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Query response Fully Comply	Fully-Comply	Query Resposne fully comply	Fully-Comply	Complied as per Compliance sheet
10	Allow users to download SSL-VPN client from provided link	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download	Fully- Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download
11	Real-time dashboard	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	real-time dashboards of Fortigate, FortiAnalyzer and FortiAuthenticator
12	Automatic email alerts	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	
13	Supports custom groups	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator supports creation of custom local user groups with administrator-defined names, membership criteria, and attributes. Custom groups can be manually populated or dynamically mapped from AD/LDAP attributes	Fully- Comply	FortiAuthenticator supports creation of custom local user groups with administrator-defined names, membership criteria, and attributes. Custom groups can be manually populated or dynamically mapped from AD/LDAP attributes	Fully-Comply	FortiAuthenticator supports creation of custom local user groups with administrator-defined names, membership criteria, and attributes. Custom groups can be manually populated or dynamically mapped from AD/LDAP attributes	Fully-Comply	FortiAuthenticator supports creation of custom local user groups with administrator-defined names, membership criteria, and attributes. Custom groups can be manually populated or dynamically mapped from AD/LDAP attributes
14	Update SSL-VPN client software centrally	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download,	Fully-Comply	FortiClient software would be installed on remote users. Free VPN-only standalone FortiClient version is available to download
15	Centralized SSL-VPN client deployment and provisioning	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	https://www.fortinet.com/support/product-downloads From the above centralized link, client can be downloaded/upgraded or an updated version of Forticlient can be placed on a central repository for the end-users to download	Fully- Comply	From the above centralized link, client can be downloaded/upgraded or an updated version of Forticlient can be placed on a central repository for the end-users to download	Fully-Comply	https://www.fortinet.com/support/product-downloads From the above centralized link, client can be downloaded/upgraded or an updated version of Forticlient can be placed on a central repository for the end-users to download	Fully-Comply	Complied as per Compliance sheet
16	Single-pane-of-glass visibility and management, consistent policy, and shared data for all users	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator provides GUI management access for user policies, management and provisioning	Fully- Comply	FortiAuthenticator provides GUI management access for user policies, management and provisioning	Fully-Comply	FortiAuthenticator provides GUI management access for user policies, management and provisioning	Fully-Comply	FortiAuthenticator provides GUI management access for user policies, management and provisioning

17	Each user must be assigned with a sperate static IP which will be used to access the internal applications. This IP must be routable internally.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
18	Solution must allow to create local users, integration with RADIUS, integration with LDAP	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Query response Fully Comply	Fully-Comply	Query Resposne fully comply	Fully-Comply	Complied as per Compliance sheet
User authentication														
1	User must be authenticated using username, password and 2FA using mobile based application second factor.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	When 2FA is enabled for the user, user will need to give username, password and 2FA code in order to authenticate	Fully-Comply	When 2FA is enabled for the user, user will need to give username, password and 2FA code in order to authenticate	Fully-Comply	When 2FA is enabled for the user, user will need to give username, password and 2FA code in order to authenticate
2	2FA must be part of solution for required number of users. Strong MFA	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	fortiMobile Token will be part of 2FA solution.	Fully-Comply	FortiMobile Token will be part of 2FA solution	Fully-Comply	Complied as per Compliance sheet
3	User profile must contain the mobile number and email address so that if required, second factor can be shared via sms or email	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Via SMS gateway integration	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
4	Identify and Authenticate device	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
5	Authorized device	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
6	Approved for access or revoked	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
7	User identity should be verified	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	fied using passwords, and well as binded so	Fully- Comply	user identity will be verified using passwords, and well as binded source IP and 2FA method	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	User identity will be verified using passwords, and well as binded source IP and 2FA method
8	Role-based access controls	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator then sends these groups to Fortigate, where these group roles based access is granted to certain resources	Fully- Comply	fortiAuthenticator then sends these groups to Fortigate, where these group roles based access is granted to certain resources	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
9	Solution must bind an IP address with user after successful authentication to access the internal services	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Using Framed-IP address as the RADIUS attribute in user settings, this IP address will be forwarded to FortiGate to use for VPN	Fully- Comply	using Framed-IP address as the RADIUS attribute in user settings, this IP address will be forwarded to FortiGate to use for VPN	Fully-Comply	Using Framed-IP address as the RADIUS attribute in user settings, this IP address will be forwarded to FortiGate to use for VPN	Fully-Comply	Complied as per Compliance sheet
10	Window Active Directory integration	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply		Fully-Comply		Fully-Comply	Complied as per Compliance sheet
11	Solution must provide centralized identities of users and devices for centralized authentication.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	FortiAuthenticator can be integrated with other IdPs like LDAP, RADIUS, SAML, OAuth, TACACS+, and import user identities and local users can also be create, thus providing centralized idenitites of users and their devices	Fully-Comply	FortiAuthenticator can be integrated with other IdPs like LDAP, RADIUS, SAML, OAuth, TACACS+, and import user identities and local users can also be create, thus providing centralized idenitites of users and their devices	Fully-Comply	FortiAuthenticator can be integrated with other IdPs like LDAP, RADIUS, SAML, OAuth, TACACS+, and import user identities and local users can also be create, thus providing centralized idenitites of users and their devices
12	Solution must allow to configure DNS settings for SSL-VPN users so that URLs get resolved at user end.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiClient accept putting FQDNs as VPN gateway	Fully- Comply	Query response Fully Comply, FortiClient accept putting FQDNs as VPN gateway	Fully-Comply	FortiClient accept putting FQDNs as VPN gateway	Fully-Comply	FortiClient accept putting FQDNs as VPN gateway
Communication														
1	End-to-end encryption	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	FortiGate VPN either use SSLVPN or IPSec VPN for secure tunnel establishment. The new OS recommends to use IPSec VPN as most secure method as compared to SSL. Further, FortiAuthenticator uses HTTPS/TLS for management and LDAPS/RADIUS-TLS for backend communications	Fully-Comply	FortiGate VPN either use SSLVPN or IPSec VPN for secure tunnel establishment. The new OS recommends to use IPSec VPN as most secure method as compared to SSL. Further, FortiAuthenticator uses HTTPS/TLS for management and LDAPS/RADIUS-TLS for backend communications	Fully-Comply	FortiGate VPN either use SSLVPN or IPSec VPN for secure tunnel establishment. The new OS recommends to use IPSec VPN as most secure method as compared to SSL. Further, FortiAuthenticator uses HTTPS/TLS for 30 management and LDAPS/RADIUS-TLS for backend communications
2	All communication must be logged	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	FortiAuthenticator logs all authentication events including login attempts, token validations, RADIUS requests, and admin actions locally and forwards them to syslog/FortiAnalyzer. FortiGate logs all SSL-VPN session events including connect, disconnect, traffic, and policy violations, forwarding them to syslog in CEF/JSON format for SIEM integration	Fully-Comply	FortiAuthenticator logs all authentication events including login attempts, token validations, RADIUS requests, and admin actions locally and forwards them to syslog/FortiAnalyzer. FortiGate logs all SSL-VPN session events including connect, disconnect, traffic, and policy violations, forwarding them to syslog in CEF/JSON format for SIEM integration	Fully-Comply	FortiGate VPN either use SSLVPN or IPSec VPN for secure tunnel establishment. The new OS recommends to use IPSec VPN as most secure method as compared to SSL. Further, FortiAuthenticator uses HTTPS/TLS for 30 management and LDAPS/RADIUS-TLS for backend communications
Compliance														
1	Solution must be highly ranked by international or national level organization. Proof of OEM solution must be provided in certification body reports/certificate.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Fortinet has been recognized as a Leader in the inaugural 2025 Gartner® Magic Quadrant™ for Hybrid Mesh Firewall, with the highest placement for Ability to Execute	Fully- Comply	Fortinet has been recognized as a Leader in the inaugural 2025 Gartner® Magic Quadrant™ for Hybrid Mesh Firewall, with the highest placement for Ability to Execute.	Fully-Comply	Fortinet has been recognized as a Leader in the inaugural 2025 Gartner® Magic Quadrant™ for Hybrid Mesh Firewall, with the highest placement for Ability to Execute.	Fully-Comply	Fortinet has been recognized as a Leader in the inaugural 2025 Gartner® Magic Quadrant™ for Hybrid Mesh Firewall, with the highest placement for Ability to Execute.
2	The proposed solution must be inline with the Information Security Requirements outlined in the Pakistan Security Standards (PSS) for Cryptographic and IT Security Devices, where and when applicable. Bidder must submit compliance letter for the same with the proposal.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Fortinet solution is compliance with Pakistan Security Standards (PSS) for Cryptographic and IT Security Devices.	Fully- Comply	Query reply Fully Comply, Fortinet solution is compliance with Pakistan Security Standards (PSS) for Cryptographic and IT Security Devices	Fully-Comply	Fortinet solution is compliance with Pakistan Security Standards (PSS) for Cryptographic and IT Security Devices.	Fully-Comply	Fortinet solution is compliance with Pakistan Security Standards (PSS) for Cryptographic and IT Security Devices.
3	Quoted solution must be of same quoted firewall OEM.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	All offered components are from same OEM	Fully- Comply	All offered components are from same OEM	Fully-Comply	All offered components are from same OEM	Fully-Comply	All offered components are from same OEM
Siem, Soar Integration														

HI

1	Must Provide integration with NADRA SIEM and SOAR.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator can send syslog to SIEM. FortiGate can be integrated with SOAR via RESTApi to apply blocking rouge source IPs for SSL VPN.	Fully- Comply	FortiAuthenticator can send syslog to SIEM. FortiGate can be integrated with SOAR via RESTApi to apply blocking rouge source IPs for SSL VPN.	Fully-Comply	FortiAuthenticator can send syslog to SIEM. FortiGate can be integrated with SOAR via RESTApi to apply blocking rouge source IPs for SSL VPN.	Fully-Comply	FortiAuthenticator can send syslog to SIEM. FortiGate can be integrated with SOAR via RESTApi to apply blocking rouge source IPs for SSL VPN.
Scalability													
1	Solution must be scalable upto 47,000 SSL-VPN Concurrent Users	Yes	Fully-Comply	By adding more devices and using VPN Load Balancing feature	Fully-Comply	Via Increasing firewall	Fully-Comply	FG-2601F Concurrent SSL VPN Users 30K (FortiOS 7.4), The solution supports scalability by adding more FortiGate appliances. FG-2601 Max Client to G/W IPSEC Tunnels 100K (FortiOS 7.6+)https://docs.fortinet.com/document/fortigate/7.6.3/fortios-release-notes/173430 Also additional user licenses on offered FortiAuthenticator and mobile tokens can be added to scale.	Fully- Comply	Also additional user licenses on offered FortiAuthenticator and mobile tokens can be added to scale	Fully-Comply	FG-2601F Concurrent SSL VPN Users 30K (FortiOS 7.4), The solution supports scalability by adding more FortiGate appliances. FG-2601 Max Client to G/W IPSEC Tunnels 100K (FortiOS 7.6+) https://docs.fortinet.com/document/fortigate/7.6.3/fortios-release-notes/173430 Also additional user licenses on offered FortiAuthenticator and mobile tokens can be added to scale.	Fully-Comply	FG-2601F Concurrent SSL VPN Users 30K (FortiOS 7.4), The solution supports scalability by adding more FortiGate appliances. FG-2601 Max Client to G/W IPSEC Tunnels 100K (FortiOS 7.6+) https://docs.fortinet.com/document/fortigate/7.6.3/fortios-release notes/173430 Also additional user licenses on offered FortiAuthenticator and mobile tokens can be added to scale.
2	SSL-VPN user means all features of SSL-VPN user mentioned in this document.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	offered solution compliance with RFP requirements	Fully- Comply	ffered solution compliance with RFP requirements	Fully-Comply	offered solution compliance with RFP requirement	Fully-Comply	offered solution compliance with RFP requirements
Hardware													
1	All components must be deployed in HA (High Availability) mode.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	All components offered as below 2xFG-2601F at PDC and 2xFG-2601F at SDC 1xFAZ-1000G at PDC and 1xFAZ-1000G at SDC (offered as per RFP compliance of single hardware machine)2xFAC-3000F at PDC and 2xFAC-3000F at SDC	Fully- Comply	All components offered as below 2xFG-2601F at PDC and 2xFG-2601F at SDC 1xFAZ-1000G at PDC and 1xFAZ-1000G at SDC (offered as per RFP compliance of single hardware machine) 2xFAC-3000F at PDC and 2xFAC-3000F at SDC	Fully-Comply	All components offered as below 2xFG-2601F at PDC and 2xFG-2601F at SDC 1xFAZ-1000G at PDC and 1xFAZ-1000G at SDC (offered as per RFP compliance of single hardware machine) 2xFAC-3000F at PDC and 2xFAC-3000F at SDC	Fully-Comply	All components offered as below 2xFG-2601F at PDC and 2xFG-2601F at SDC 1xFAZ-1000G at PDC and 1xFAZ-1000G at SDC (offered as per RFP compliance of single hardware machine) 2xFAC-3000F at PDC and 2xFAC-3000F at SD
2	Redundant power, NICs	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	All offered components having dual power supplies	Fully- Comply	all offered components having dual power supplies	Fully-Comply	all offered components having dual power supplies	Fully-Comply	all offered components having dual power supplies
Integration													
1	PKI Integration	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator acts as a full PKI Certificate Authority, issuing and managing X.509 certificates for users, devices, and services. It supports SCEP, CSR signing, CRL, and certificate lifecycle management	Fully- Comply	FortiAuthenticator acts as a full PKI Certificate Authority, issuing and managing X.509 certificates for users, devices, and services. It supports SCEP, CSR signing, CRL, and certificate lifecycle management	Fully-Comply	FortiAuthenticator acts as a full PKI Certificate Authority, issuing and managing X.509 certificates for users, devices, and services. It supports SCEP, CSR signing, CRL, and certificate lifecycle management	Fully-Comply	FortiAuthenticator acts as a full PKI Certificate Authority, issuing and managing X.509 certificates for users, devices, and services. It supports SCEP, CSR signing, CRL, and certificate lifecycle management
Connectivity & Remote Site Integration													
1	Remote Connectivity: Remote sites must connect securely over the internet.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	using FortiClient a user establish secure channel VPN over Internet with offered Fortigates at PDC and SDC.	Fully- Comply	using FortiClient a user establish secure channel VPN over Internet with offered Fortigates at PDC and SDC.	Fully-Comply	suing FortiClient a user establish secure channel VPN over Internet with offered Fortigates at PDC and SDC.	Fully-Comply	using FortiClient a user establish secure channel VPN over Internet with offered Fortigates at PDC and SDC.
2	Secure Tunnel: Must use secure tunneling protocols	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Fortigate support SSL VPN with FortiOS 7.4 and IPSec VPNs with FortiOS 7.6+ for secure remote connectivity.	Fully- Comply	Fortigate support SSL VPN with FortiOS 7.4 and IPSec VPNs with FortiOS 7.6+ for secure remote connectivity.	Fully-Comply	Fortigate support SSL VPN with FortiOS 7.4 and IPSec VPNs with FortiOS 7.6+ for secure remote connectivity	Fully-Comply	Fortigate support SSL VPN with FortiOS 7.4 and IPSec VPNs with FortiOS 7.6+ for secure remote connectivity.
Management & Monitoring													
1	Centralized Management: Unified dashboard for monitoring, configuration, and reporting.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator provides a unified web-based dashboard for user, policy, and authentication management. FortiAnalyzer offer centralized log management, log monitoring and reporting	Fully- Comply	FortiAuthenticator provides a unified web-based dashboard for user, policy, and authentication management. FortiAnalyzer offer centralized log management, log monitoring and reporting	Fully-Comply	FortiAuthenticator provides a unified web-based dashboard for user, policy, and authentication management. FortiAnalyzer offer centralized log management, log monitoring and reporting	Fully-Comply	FortiAuthenticator provides a unified web-based dashboard for user, policy, and authentication management. FortiAnalyzer offer centralized log management, log monitoring and reporting
2	Role-Based Access Control: Different administrative roles with granularity.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply		Fully- Comply		Fully-Comply	reporting via FortiAnalyzer logging and reporting solution	Fully-Comply	
3	Reporting: Real-time and scheduled reports for user access, health, threats, etc.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	reporting via FortiAnalyzer logging and reporting solution	Fully- Comply	reporting via FortiAnalyzer logging and reporting solution	Fully-Comply	reporting via FortiAnalyzer logging and reporting solution	Fully-Comply	reporting via FortiAnalyzer logging and reporting solution
4	Alerting: Configurable alerts via email, SNMP, syslog, etc.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator supports SNMP traps and syslog forwarding for authentication and system events. Email notifications are supported for user-facing events such as OTP delivery and account activation or password expiry notification	Fully- Comply	FortiAuthenticator supports SNMP traps and syslog forwarding for authentication and system events. Email notifications are supported for user-facing events such as OTP delivery and account activation or password expiry notification	Fully-Comply	FortiAuthenticator supports SNMP traps and syslog forwarding for authentication and system events. Email notifications are supported for user-facing events such as OTP delivery and account activation or password expiry notification	Fully-Comply	FortiAuthenticator supports SNMP traps and syslog forwarding for authentication and system events. Email notifications are supported for user-facing events such as OTP delivery and account activation or password expiry notification
5	Policy Enforcement: Policy updates across all sites and users.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	RADIUS policies on FortiAuthenticator are applied centrally and synced for all users across all FAC instances	Fully- Comply	RADIUS policies on FortiAuthenticator are applied centrally and synced for all users across all FAC instances	Fully-Comply	RADIUS policies on FortiAuthenticator are applied centrally and synced for all users across all FAC instances	Fully-Comply	RADIUS policies on FortiAuthenticator are applied centrally and synced for all users across all FAC instances
6	Orchestration: Easy rollout, update, and configuration propagation across all sites.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	FortiAuthenticator HA ensures configuration synchronization across PDC and SDC nodes.	Fully- Comply	FortiAuthenticator HA ensures configuration synchronization across PDC and SDC nodes.	Fully-Comply	FortiAuthenticator HA ensures configuration synchronization across PDC and SDC nodes.	Fully-Comply	FortiAuthenticator HA ensures configuration synchronization across PDC and SDC nodes
Hardware Based Logging Solution (1 at PDC, 1 at SDC)													
1	Reporting	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	via offered FAZ-1000G	Fully- Comply	via offered FAZ-1000G	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
2	Ability to visualize and drill-down into key elements traffic logs, top destinations, top sources etc	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query Resposne Full comply		Query Reply fully comply		Query Resposne fully comply	Fully-Comply	Complied as per Compliance sheet
3	Logging	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	via offered FAZ-1000G	Fully- Comply	via offered FAZ-1000G	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet

4	Must provide all Reports, Analytics, logs and view of at least last six months of all quoted equipment. Must support 100GB Per day Or 10,000EPS, bidder must calculate disk space and quote the solution accordingly.	100GB Logs Per day Or 10,000 EPS	Fully-Comply	BOM	Fully-Comply	Query response : fully comply	Fully-Comply	via offered FAZ-1000G	Fully- Comply	via offered FAZ-1000G	Fully-Comply	Via offered FAZ-1000G	Fully-Comply	via offered FAZ-1000G
5	Export of logs and reports	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply		Fully- Comply		Fully-Comply		Fully-Comply	
6	Quoted solution must be of same quoted firewall/SSL-VPN OEM	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Fortigates and FortiAnalyzer are of same OEM	Fully- Comply	Fortigates and FortiAnalyzer are of same OEM	Fully-Comply	Fortigates and FortiAnalyzer are of same OEM	Fully-Comply	Fortigates and FortiAnalyzer are of same OEM
7	Centralized logging	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	via offered FAZ-1000G	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	via offered FAZ-1000G
8	SIEM Integration: Solution must integrate with standard SIEM platforms (QRadar, Elastic etc)	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
9	Real-time Audit Trails: Instant access logs, administrative actions, and policy changes.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
10	Must provide all type of logs including but not limited to firewall logs, traffic logs, attack, authentication, SSL-VPN, 2FA, event, debug and audit logs using single interface at PDC and SDC.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	via offered FAZ-1000G	Fully- Comply	via offered FAZ-1000G	Fully-Comply	Via offered FAZ-1000G	Fully-Comply	Complied as per Compliance sheet
11	Provide log analytics	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	via offered FAZ-1000G	Fully- Comply	via offered FAZ-1000G	Fully-Comply	Via offered FAZ-1000G	Fully-Comply	via offered FAZ-1000G
12	Provide built-in and custom reporting	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
13	Must Provide integration with NADRA SIEM and SOAR.	Yes	Fully-Comply	As per Query Resposne	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
14	Logging must be for all solution components mentioned in BOQ of this document and proposed by bidder	Yes	Fully-Comply	query response: Fully Complied	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	offered FortiClient free/standalone version activity logs to FortiAnalyzer via FortiGate	Fully-Comply	offered FortiClient free/standalone version activity logs to FortiAnalyzer via FortiGate
Support, Warranty, Subscription and Training for all quoted equipment (Hardware, Software, Licenses, Subscriptions)														
1	Three Year 24x7 Support, subscription and updates direct from principal for all quoted solution components (Hardware, Software, Licenses, Subscrptions, features).	3x Years	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	offered with 3 years support and services	Fully- Comply	offered with 3 years support and services	Fully-Comply	offered with 3 years support and services	Fully-Comply	offered with 3 years support and services
2	• TAC Access over TAC Portal Account, TAC Login, email and phone call. • NADRA must get support direct From Principal via TAC Portal Login, email address and Phone • On-Site Partner support • SLA and NDA with successful bidder	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	offered with 3 years support and services	Fully- Comply	offered with 3 years support and services	Fully-Comply	offered with 3 years support and services	Fully-Comply	offered with 3 years support and services
3	Next calendar day delivery warranty for all quoted hardware	3x Years	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	refer to the BOM, FortiCare Preimum and Elite support both quoted with 3 years support and services	Fully- Comply	refer to the BOM, FortiCare Preimum and Elite support both quoted with 3 years support and services	Fully-Comply	eimum and Elite support both quoted wil	Fully-Comply	reimum and Elite support both quoted with
4	Bidder shall provide 3-year subscriptions for all quoted subscription-based features	3x Years	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	offered with 3 years support and services	Fully- Comply	offered with 3 years support and services	Fully-Comply	offered with 3 years support and services	Fully-Comply	offered with 3 years support and services
5	Must provide auto real-time updates and manual update option	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	both options available. Auto connect to FortiGuard Services manually download updates from support portal and upload	Fully- Comply	both options available. Auto connect to FortiGuard Services manually download updates from support portal and upload	Fully-Comply	both options available. Auto connect to FortiGuard Services manually download updates from support portal and upload	Fully-Comply	both options available. Auto connect to FortiGuard Services manually download updates from support portal and upload
6	All Licenses on Name of NADRA	Yes	Fully-Comply		Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	All licenses will be in the name of NADRA	Fully- Comply	offered to NADRA	Fully-Comply	offered to NADRA	Fully-Comply	offered to NADRA
7	The proposed solution must not be announced End of Life (EOL), End of Sale, End of Support by the principal for next 5 years	Yes	Fully-Comply	As per Query Resposne	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied in Compliance Sheet	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance sheet
8	All hardware must come with manufacturer warranty for a minimum of 3 years	3 Years	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Query Resposne : fully comply	Fully-Comply	offered with 3 years support and services	Fully- Comply	offered with 3 years support and services	Fully-Comply	offered with 3 years support and services	Fully-Comply	offered with 3 years support and services
9	Online, certified, instructor LED OEM training must cover following topics as per quoted products official trainings of OEM. Bidder must provide certificates for the same direct from OEM. If multiple trainings cover the topic then bidder must ensure the delivery: - a. Operator training b. Design training c. Expert level training d. Zero Trust Access e. Firewall administration and security f. Second Factor authentication g. SSL-VPN client end h. SSL-VPN central site solution with HA and DR Bidder shall arrange training Venue	5 Resources (Each resource must get all trainings)	Fully-Comply	As per Query Resposne	Fully-Comply	Query Resposne : fully comply	Fully-Comply	offered 5xFortigate, 5xFortiAnalyzer and 5xFortiAuthenticator OEM led online trainings. These trainings cover all components of the solution being offered	Fully- Comply	offered 5xFortigate, 5xFortiAnalyzer and 5xFortiAuthenticator OEM led online trainings	Fully-Comply	offered 5xFortigate, 5xFortiAnalyzer and 5xFortiAuthenticator OEM led online trainings	Fully-Comply	offered 5xFortigate, 5xFortiAnalyzer and 5xFortiAuthenticator OEM led online trainings

8-9

	for dedicated training session. Training certificate of principal is required for all training participants. All expenses of training will be the responsibility of Bidder.												
Misc Requirements													
1	Bidder must be OEM Authorized Partner / OEM Authorized Reseller / OEM Authorized Distributer /OEM Authorized Dealer. Bidder must submit MAL of OEM.	Yes	Fully-Comply	Cisco MAL provided. MFA One Span MAF is attached	Fully-Comply	letters from OpenSpan,Cisco attached (Pg-98-99)	Fully-Comply	Query Response, Letter of Fortinet attached (Pg-88)	Fully- Comply	letter attached (Pg-55)	Fully-Comply	**Letter provided (Pg-88)**	Fully-Comply	**Query Respsnse, letter provided**
2	Bidder shall submit Letter of compliance with the statement "Bidder fully agreed and complied all Sections/parts/Annexures of RFP"	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Provided (Pg-97)	Fully-Comply	Query Response, Letter provided (Pg 149)	Fully- Comply	Query Reply , letter provided	Fully-Comply	**Letter provided (Pg-20)**	Fully-Comply	**Letter Provided (Pg-10)**
3	OEM/Principal must ensure in compliance and also mention via letter that quoted solution have no backdoors.	Yes	Fully-Comply	Letter provided Pg 26,	Fully-Comply	letter Provided (Pg-184), Query Reply	Fully-Comply	Query response, letter from OEM and bidder attached (Pg-159-160)	Fully- Comply	letter attached (Pg-56)	Fully-Comply	**Letter provided (Pg-21)**	Fully-Comply	Letter Provided (Pg-91)
4	Complete solution, its components and sub-components must be deployed on-premises. All processing must be done on-premises. On-Premises solution so that no client data leaves the network.	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	only on-prem solution components have been offered	Fully- Comply	all offered components are on-prem	Fully-Comply	all offered components are on-prem	Fully-Comply	all offered components are on -prem
5	All equipment must be dual power supply	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	all offered components have dual-power	Fully- Comply	all offered components have dual-power	Fully-Comply	all offered components have dual-power	Fully-Comply	all offered components have dual -power
6	All equipment must be rack mounted to mount in data center racks	Yes	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	Complied as per Compliance Sheet	Fully-Comply	all offered components have rack mount	Fully- Comply	Complied as per Compliance Sheet	Fully-Comply	all offered components have rack mount	Fully-Comply	all offered components have rack mount
7	OEM of Quoted equipment must have deployment of SSL-VPN solution 2,000+ SSL-VPN users within Pakistan or internationally. Evidence must be submitted for the same in form of Contract/PO/email-from-client.	Yes	Fully-Comply	Pg 154, Zong P.O Cisco AnyConnect Apex License, 1YR, 2500-4999 Users	Fully-Comply	Email from client provided (Pg-181), Query reply	Fully-Comply	Query Response, Evidence email of PLRA is attached	Fully- Comply	Query Reply evidence Provided	Fully-Comply	Query Reply: Evidence Provided	Fully-Comply	Query response, Email of NBP Provided

Recommendation (Tender # NADRA-HQ-RFB-42/2026)	**M/S CNS: Recommended**	**M/S Commtel: Recommended**	**M/S Inara: Recommended**	**M/S MPCL JAZZ: Recommended**	**M/S Premier: Recommended**	**M/S PTCL: Recommended**

Recommendations have been made as per technical criteria only, However Procurement Dept kindly verify remaining all clauses for selection of bidder as per NADRA Procurement rules for all bidders.

President: _____

Name: Mr. Rehman Gul

Director (C&IT Svcs)

Member 1: _____ 13/5/26

Name: Mr. M. Junaid Zafar

Dupety Director (C&IT SVCS)

Member 2: _____

Name: Mr. Syed Mutahir Hussain

Dupety Director (NDW)

Member 3: _____

Name: Mr. Haroon Hafeez Ahamd

Dupety Director (TND)

Pg-10