भारत सरकार
वित्त मंत्रालय
क्षेत्रीय प्रत्यक्ष कर
प्रशिक्षण संस्थान

GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DIRECT TAXES REGIONAL
TRAINING INSTITUTE

No.17, Near HMT Watch Factory, Jalahalli, Bengaluru-560013
Telephone: 080-23452841/23082001/23452565, Fax: 080-23082026, E-Mail: dtrti.bang@gmail.com

F.No.118/Networking/2016-17/DTRTI

Date: 14-02-2017

TENDER NOTIFICATION

Direct Taxes Regional Training Institute (DTRTI), Bangalore, invites sealed bids for providing **Firewall security with inbuilt wireless for the internet, Eighteen Access Points compatible to the firewall switch/wireless controller and two POE access switches, installation & redressing of 9U rack** in DTRTI, Bengaluru Campus.

The bidder has to give **proper buy back value** of the all related scraps came out of DTRTI. All the **legal norms have to be taken care to discard/dispose the scrap material. DTRTI, Bengaluru shall not be responsible for the violation of any norms any manner done by the bidder.**

2. The period of service/warranty for the software/hardware from the service provider/contractor shall be for 3 years irrespective of whether or not the manufacturer provides/does not provide the AMC.

3. Sealed quotations should be submitted addressed to the Additional Director General (Trg.), No.17, Near HMT Watch Factory, Jalahalli, Bengaluru-560013, by **20-02-2017 by 12.00hrs.** The tenders will be **opened on 20-02-2017 at 14.30hrs.** by the limited tender evaluation committee.

4. (A). Specifications of the Gateway Firewall are as under:

A. Gateway Firewall Specifications:

1) Firewall should support for Multi-core technology to provide excellent throughput for all key processes.
2) Supplied Firewall should have minimum 6 GE port with an expansion slot (SFP and SFP+ supported modules) for future extension purpose, along with USB ports to support WWAN interface.
3) Gateway level Firewall License should not be per user or IP based, it should be Firewall Appliance based.
4) The proposed solution must provide flexible, granular role-based GUI administration for local & remote firewall administrators.

5) Should have Management access through console, SSH, HTTPS using browser based GUI for securely managing the firewall.
6) The firewall throughput performance should be at up to 14 Gbps
7) Firewall Internet MIX (IMIX=with UTM features enabled) throughput upto 4.9 Gbps
8) Firewall VPN throughput should up to 1 Gbps
9) Firewall IPS throughput should up to 2 Gbps
10) NGFW (IPS + App Ctrl + Web Filter) throughput up to: 1 Gbps
11) Firewall Antivirus throughput up to: 2 Gbps
12) NGFW (IPS + App Ctrl + Web Filter) throughput up to: 1 Gbps
13) Firewall Antivirus throughput up to: 2 Gbps
14) Firewall appliance Concurrent connections up to: 8000000
15) Firewall appliance new connections/sec: 130,000
16) Firewall should have local storage for logging, reporting and email quarantine purpose up to 120 GB.
17) Physical specifications: 1U rack mountable
18) Should support for Power supply with DC:12V, 100-240 VAC at 50-60 Hz.
19) Product should be certified like CB, CE, FCC Class B, IC, VCCI, MIC, RCM, UL, CCC.
20) Supplied appliance power consumption specifications: 19W, 65 BTU/hr (for idle) & 29W, 99 BTU/hr (on full load). Auto-ranging 100-240VAC, 50-60 Hz
21) Firewall operating temperature should meet specs: 0-40°C (operating) -20 to +80°C (storage)
22) Should support transparent mode/Bridge mode for Seamless deployment into existing network adding all security functionality without changing IP configurations in the network.
23) Should have minimum Solid-State Storage capabilty of 120 GB with minimum of 8 GB RAM
24) Firewall should automatically download Gateway Anti-virus signatures, Gateway IPS updates on the scheduled intervals.
25) Dashboard monitoring should give us details of resource utilization like CPU, Memory interface utilization for live and historical upto a year's period.
26) Proposed solution should have a monitoring widget to identify total number of firewall rules, active/inactive rules, newly modified rules kind of features.
27) Firewall should have rule templates for common business applications like Microsoft Exchange, SharePoint, Lync, and much more defined in XML enabling customization and sharing.
28) Granular traffic shaping features should be available for Web, App, Firewall rule and User based.

29) Firewall should have option to be managed from Centralized Console with graphical interface.
30) Proposed solution should support High Availability functionality both in Active-Active and Active-Passive.
31) Firewall should support SNMP and Netflow protocols for monitoring the health of appliance.
32) Firewall network usage reports and alerts have to be sent over email along with configuration backup.

B. Firewall, Networking & Routing

1) Firewall should support Stateful deep packet inspection.
2) Multi-Core Architecture with Fast Path Packet Optimization.
3) Firewall rules should support Zone based comprising User based, Network (IP/MAC based), or business application based on access time duration.
4) Should support Flood protection like DoS attack, DDoS attack and port scan blocking.
5) Firewall rule should support Country blocking by geo-IP with country and continent selections.
6) Supports routing: static, multicast (PIM-SM) and dynamic (RIP, BGP, OSPF)
7) Per-rule and policy based routing by source, destination, user/group or layer-4 service*
8) Should Support Upstream proxy support for future requirements.
9) Protocol independent multicast routing with IGMP snooping
10) Bridging with STP support and ARP broadcast forwarding
11) Should support multiple WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rules
12) Should support full configuration of DNS, DHCP, NTP and Dynamic DNS
13) Should support IPv6 support with tunneling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec for future requirements.
14) Should support user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical.

C. Secure Wireless

1) Should have Simple plug-and-play deployment of Vendor specific wireless access points (APs) after authorization of deployed APs.
2) Firewall should act like central monitor and manage all Vendor specific APs and wireless clients through the built-in wireless controller functionality.

3) Firewall should supply Hotspot (custom) vouchers, password of the day and T&C acceptance for guest users.

D. Authentication

1) Should support Transparent (Single Sign in), proxy authentication (NTLM) or client authentication.
2) Firewall should support Authentication via remote authentication servers like Active Directory, e-Directory, RADIUS, LDAP and TACACS+. Should also include options for Client authentication agents for Windows, Mac OS X, Linux 32/64. Authentication certificates for iOS and Android.
3) Two factor authentication (one-time password support) for IPSec and SSL VPN, user portal, and Web admin.
4) User should have privilege to change the predefined password set by the security admin, and also should have authorization to check his/her personal internet usage.

E. VPN Options

1) Should support Site-to-site VPN through SSL, IPSec, using pre-shared key & Certificate based. L2TP VPN, PPTP VPN, Remote access VPN Client software through SSL, IPsec on multiple operating system platforms.
2) Should support encryption algorithms like AES (128/192/256), DES, 3DES, Blowfish, Twofish, Serpent, RSA (up to 2048 Bit), DH groups 1/2/5/14, Authentication algorithms like MD5 and SHA-1/256.
3) Should support split-tunneling for optimum traffic routing for remote access VPN users.
4) Should support HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet and VNC for Clientless VPN users.

F. Network Protection

1) Gateway level Intrusion Prevention (IPS) should have high-performance with IPS deep packet inspection engine with selective IPS patterns for maximum performance and protection
2) Gateway level Intrusion Prevention (IPS) should have 7000+ signatures and also provision to create custom IPS signatures.
3) Firewall should have Advanced Threat Protection that is Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall technology.

4) Firewall's Secure Web access feature should have enterprise-grade Secure Web Gateway web policy engine with top-down execution and inheritance with flexible user/group policy definitions, customizable activities, block/warn/allow actions.
5) Firewall's Secure Web access feature should have URL Filter database with millions of sites across 90+ categories and file type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)
6) Should have provision to limit on surfing quota time policies per user/group
7) Should have Malware scanning techniques to block all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email. Should enforce Safe Search on the search engine portals and have creative commons image search enforcement to block illicit images.
8) Real-time or batch mode scanning and should support protection through Pharming.
9) Proposed firewall should include Application control based on category, characteristics, technology and risk level along with traffic shaping based on individual applications.
10) Firewall's Anti-Spam engine should support Per-domain mail routing.
11) Should support E-mail scanning with SMTP, POP3, and IMAP.
12) Should support email reputation service with spam outbreak monitoring based on Recurrent-Pattern-Detection technology.
13) Should block spam and malware during the SMTP transaction and File-Type detection/blocking/scanning of attachments. Accept/reject/drop over-sized email messages and also detects phishing URLs within e-mails.
14) TLS Encryption support for SMTP, POP and IMAP.
15) Should include Email archive functionality.
16) Quarantined emails should have self-serve user portal for viewing and releasing quarantined messages with reason to release and delete messages.
17) Firewall should support Web Application Firewall to protect hosted web servers.

G. On appliance Logging and Reporting

1) Firewall should support on-box reports with custom report options: Dashboards (Traffic, Security, and User behavior analysis report), Applications (App Risk, Blocked Apps, Search Engines, Web Servers, FTP), Network & Threats (IPS, ATP, Wireless), VPN, Email, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA). Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks

2) Should have provision for report scheduling to multiple recipients by report group with flexible frequency options. Reports have to sent in HTML, PDF, Excel (XLS) formats.
3) Should have option for customized log retention by log categories.

H. Support

1) Onsite support 24 X 7 from the Bidder as well as manufacturer
2) Onsite installation & commissioning

(B). Specifications of the Access Points are as under:

1) Mounting : Ceiling/wall
2) Physical security: Kensington lock
3) Enclosure Bottom: metal; top cover: plastic; white; plenum-rated according to UL2043 CPU QCA9558 (2.4GHz), QCA9880 (5GHz)
4) Memory 128 MB DDR2
5) Flash 16 MB
6) Maximum Throughput 867 Mbps (5GHz / 802.11ac) + 300 Mbps (2.4GHz / 802.11n)
7) Multiple SSIDs 8 per radio, 16 in total
8) Number of radios 2
9) MIMO capabilities 2x2:2
10) MTBF 26280 hours
11) LAN Interfaces 1 x 10/100/1000 Base-TX
12) Antennas 4 x internal antenna /2 external antenna
13) Antenna gain 2.4G: 4.36 / 5.77 dBi 5G: 6.13 / 6.27 dBi
14) Supported WLAN standard 802.11a/b/g/n/ac
15) Certifications : CB, CE, FCC, UL (plenum-rated)
16) Transmit power and receive sensitivity
17) 802.11 a

Data Rate	TX power	RX sensitivity
6 Mbps	22 dBm	-90 dBm
24 Mbps	22 dBM	-81dBm
54 Mbps	18 dBm	-74 dBm

18) 802.11 b

Data Rate	TX power	RX sensitivity
1 Mbps	23 dBm	-93 dBm
5.5 Mbps	23 dBM	-89 dBm
11 Mbps	23 dBm	-85 dBm

19) 802.11 g

Data Rate	TX power	RX sensitivity
6 Mbps	23 dBm	-86 dBm
18 Mbps	23 dBM	-84 dBm
54 Mbps	19 dBm	-72 dBm

20) 802.11 n (2.4G)

Data Rate	TX power	RX sensitivity
MCS0	23 dBm	-83 dBm
MCS4	21 dBM	-75 dBm
MCS6	19 dBm	-69 dBm
MCS7	18 dBm	-68 dBm

21) 802.11 ac

Data Rate	TX power	RX sensitivity
MCS0	23 dBm	-84 dBm
MCS4	21 dBM	-69 dBm
MCS6	19 dBm	-66 dBm
MCS9	15 dBm	-58 dBm

22) Modulation

23) 802.11a - OFDM with BPSK, QPSK, 16QAM, 64QAM

24) 802.11b -BPSK, QPSK, CCK

25) 802.11g -OFDM with BPSK, QPSK, 16QAM, 64QAM
26) 802.11n -OFDM with BPSK, QPSK, 16QAM, 64QAM
27) 802.11ac -OFDM with BPSK, QPSK, 16QAM, 64QAM, 128 QAM, 256QAM
28) Center frequencies / channels

ETSI	
2.412-2.472GHz (channels 1-13)	RLAN sub-band 1: RLAN sub-band 2: 5.180-5.320GHz (channels 36-64) 5.500-5.580GHz (channels 100-116) 5.660-5.700GHz (channels 132-140)
FCC	
2.412-2.462GHz (channels 1-11)	U-NII-1: U-NII-2: U-NII-2e: U-NII-3: 5.180-5.240GHz (channels 36-48) 5.260-5.320GHz (channels 52-64) 5.500-5.580GHz (channels 100-116) 5.660-5.700GHz (channels 132-140) 5.745-5.825GHz (channels 149-165)

(C) Specification of POE switches are as under:

1) POE +Switch 24 Port with 1 G Module
2) I/O ports and slots 24 RJ-45 auto-negotiating 10/100/1000 PoE+ ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3af PoE, IEEE 802.3at) 4 SFP 100/1000 Mbps slots (IEEE 802.3u Type 100BASE-FX, IEEE 802.3z Type 1000BASE-X Supports a maximum of 24 autosensing 10/100/1000 ports plus 4 SFP 100/1000 slots
3) Additional ports and slots 1 RJ-45 console port to access limited CLI port
4) Memory and processor MIPS @ 500 MHz, 32 MB flash, 128 MB SDRAM; packet buffer size: 512 KB
5) Mounting and enclosure Mounts in an EIA standard 19-inch telco rack or equipment cabinet (hardware included)
6) Performance 100 Mb Latency
7) 100 Mb Latency < 5 µs
8) 1000 Mb Latency < 5 µs
9) Throughput up to 41.7 Mpps (64-byte packets
10) Routing/Switching capacity 56 Gbps

11) Routing table size 32 entries (IPv4)
12) MAC address table size 32 entries (IPv6) 8192 entries
13) Reliability
14) MTBF (years) 65.78
15) Frequency 50/60 Hz
16) AC voltage 100 - 240 VAC
17) PoE power 370 W PoE+
18) Safety UL 60950; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No.60950-1-03
19) Emissions FCC part 15 Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; EN 61000-3-2 2000, 61000-3-3; ICES-003 Class
20) Management IMC—Intelligent Management Center; limited command-line interface; Web browser; SNMP Manager; IEEE 802.3 Ethernet MIB
21) Notes SFP ports and copper ports can work simultaneously, independent of each other, to provide a total of 28 Gigabit switching ports
22) General protocols IEEE 802.1D MAC Bridges IEEE 802.1p Priority IEEE 802.1Q VLANs IEEE 802.1s (MSTP)
23) MIBs RFC 1213 MIB II RFC 1493 Bridge MIB RFC 2021 RMONv2 MIB RFC 2233 Interface MIB RFC 2233 Interfaces MIB RFC 2571 SNMP Framework MIB RFC 2572 SNMP-MPD MIB
24) Network management IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
25) QoS/CoS IEEE 802.1P (CoS)

5. Eligibility Criteria:

The bidders fulfilling all the following criteria shall be considered as qualified for opening of financial bids:

1) The bidders should possess the experience of having successfully completed/running similar works during the last 3 years. Similar works means "supply of firewall, providing software security and it's maintenance".
2) The bidders should not have been blacklisted or debarred from bidding or declared as a non-performer by any Govt./Semi Govt./Autonomous body. The bidders shall submit an affidavit duly attested by Notary that they have not been blacklisted or debarred from biding or declare as a non-performer by any Govt./Semi Govt./Autonomous body.
3) The bidders should have the following registrations/documents:
    i. Labour License
    ii. Service Tax Registration
    iii. Valid PAN in the same name of the bidder.

6. Instructions to the Bidders:

1. The "bidder" as used in this document shall mean the one who has signed the tender document forms. He may be either the Principal Officer or the duty

authorized representative in which case, the bidder shall submit a certificate of authority. All certificates and documents (Including any clarifications sought and any subsequent correspondence). Shall, be furnished san signed by such representative or the Principal Officer.

2. The Bidder shall bear all costs associated with the preparation and submission of its bid. The Direct Taxes Regional Training Institute, Bangalore, hereinafter referred to as **"DTRTI"**, will in no case be responsible or liable for these costs, regardless of the conduct or outcome or the bidding process.
3. At any time prior to the deadline for submission of bids, the DTRTI may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the bidding document by a written amendment. All prospective bidders who have given their e-mailing address will be notified of the amendment by email, which will be binding.
4. In order to allow prospective bidders reasonable time within which to take the amendment into account in preparing their bids, the DTRTI, at its discretion, may extend the deadline for the submission of bids.
5. The bid prepared by the Bidder, as well as all correspondence and documents shall be written in **English** language.
6. The price must be both in words and figures. If there is a discrepancy between the price quoted in words and figure, the amount in words shall prevail and in case of further doubt, the discretion of the DTRTI will prevail.
7. The price once accepted by the DTRTI shall remain valid for year i.e. it will start from the date of entering into the agreement and will run for 1 year. In the event there is a reduction in Government levy/duties during the period of execution of the order, the rates shall be suitably adjusted with effect from the date notifying the said reduction in the Government levy/ excise duty, if applicable.
8. Prices shall be quoted in Indian rupees only.
9. **Bidder should Submit Authorization letter from OEM referring to this tender**
10. **A tender Compliance certificate has be submitted.**

7. Terms and Conditions

i. The successful bidder shall provide software updates with no Updation/installation charges excluding software upgrade subscription, if any.

ii. The successful bidder shall provide Escalation Matrix containing all the relevant contact no./emails/landline nos. of the persons concerned at each level.

iii. The bidders having experience of having done similar work in a Govt. Organization /Public Sector Industry shall be given preference.

iv. The firewall security has to be provided 24x7 without any interruption.

v. The Service provider shall arrange to tender efficient service as required. However, in case the Contractor fails to maintain the service to the entire satisfaction of the Officer-in-charge, the department shall make alternate arrangement, the expenditure thus incurred will be recovered from the performance guarantee submitted by the contractor. The decision of the ADG in this regard shall be final.

vi. Only bona fide contractor's persons shall be allowed in the premises for carrying out any related work.

vii. The service provider shall be responsible for any accident, hospitalization of their Staff etc., occurring during maintenance work.

viii. The service provider shall be responsible for any damage caused to the equipment/building during the execution of the maintenance work.

ix. During the period of maintenance of contract, the Service provider shall provide the following services:

a. Break Down Calls	:	As required or requisitioned from time to time.
b. Reach time	:	Every effort shall be made to attend to any complaint within 4 hours.
c. Major Breakdown: repairs		May take up to 24 hours from the date and time of complaints consultation of Officer-in-charge.

x. In case any major defects found in the system during checking, it should be informed to the Officer-in-charge and defects should be rectified immediately. Payment for rectification of defects, if any, will be as per agreement conditions.

xi. Any abnormality in electrical installation or major fault should be brought into the notice of Officer-in-charge immediately.

xii. The work includes installation of POE switches and redressing of 9 U rack.

xiii. The bidder should provide quality personnel for looking after the AMC works to the satisfaction of DTRTI.

xiv. No Tools & Parts will be issued to the contractor by the department.

xv. It will be the sole responsibility of the bidder alone to execute the entire contract on its award to the satisfaction of the DTRTI.

xvi. The service provider should maintain the confidentiality of the work carried out by them.

xvii. In case of failure of the device, the service provider should immediately provide a replacement device till the existing device is repaired and installed successfully. Failure to comply this suitable penalty will be levied as per the relevant para.

xviii. The DTRTI does not bind itself to accept the lowest tender and reserves to itself the right to reject any or all tenders without assigning any reason, whatsoever.

xix. The DTRTI will award the contract to the Bidder whose bid has been determined to be the most responsive to the Bidding Document and who has offered the best evaluated bid.

xx. The DTRTI reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time, without thereby incurring any liability to the affected Bidder or Bidders or any obligations to inform the affected Bidder or bidders or the grounds for the DTRTI's action.

xxi. In case of any dispute, if any, the decision of the ADG, DTRTI, Bengaluru shall be final.

8. Payment Schedule:

i. No advance payment will be made to the Contractor.

ii. The DTRTI shall take all necessary steps to make the contract payment within 30 days of receipt of the bill. In any case, the DTRTI shall not be responsible for delays if any for reasons beyond its control.

iii. A certificate of completion of installation of Firewall duly signed by competent officer of DTRTI, Bengaluru has to be produced alongwith the bill.

9. Action for non-compliance:

In case, there is no compliance from the contractor/service provider/manufacturer to sort out the complaint, the DTRTI reserves the right to blacklist any/all of the contractor, service provider and manufacturer.

(S. RADHAKRISHNA)
Additional Director General(Trg.)
DTRTI, Bengaluru.