Government of India
Department of Space
NORTH EASTERN SPACE APPLICATIONS CENTRE
Umiam-793103, Meghalaya

TENDER DETAILS

The bid is required to be submitted in **two parts**. One part is the **Techno-Commercial Un-priced Bid** and the other part is the **Price Bid**.

The Bidder shall submit the bids in two separate envelopes. One envelope shall contain Techno Commercial Un-priced bid and the other shall contain the Priced bid. The bidder shall seal the Techno Commercial Un-priced Bid and the Price Bid in two separate envelops duly marked as **"Techno-Commercial Un-priced Bid"** and **"Price Bid"** respectively. Both the envelopes shall then be sealed in one outer (main) envelope. The main envelope must be sent to **Administrative Officer, North Eastern Space Applications Centre (NESAC), Government of India, Department of Space, Umiam -793103, Meghalaya.**

The Techno-Commercial Unpriced Bid prepared by the Bidder shall include the following without indicating the price in the Bid Form.

i. Authorization Form from manufacturers (Form-i)
ii. Performance Statement Form (Form-ii)
iii. Service Support Details Form (Form-iii)
iv. Technical Specification Compliance Form (Form-iv)

PART-1

TECHNICAL BID

TERMS AND CONDITION

1. This Invitation for Bids is open to all reputed firms who fulfill the qualifying requirements specified in the NIT.

2. The Bidder should be a firm of reputation having sufficient expertise and experience in the subject area with sound warranty / service support capability and authorization from manufacturers of all major items. The firm should also have the capability & experience of installation & Commissioning of Wireless and Security Solutions. Documentary Evidence establishing the above is to be enclosed along with Technical Bid.

3. Bidder must have service facilities at Shillong and Guwahati. Details of these service support facilities must be mentioned.

4. The bidder should have executed at least two similar order valued at more than Rs. 20.00 lakhs successfully during the preceding three financial years. The details should be incorporated in the performance statement form along with documentary evidence.

5. The annual turnover of the bidder during the last three financial years should be Rs. 4.00 crores per year and above.

6. That the Bidder will assume total responsibility for the fault-free operation of system during warranty Period.

7. Bidders who do not meet the criteria given above are subject to be disqualified, if they have made untrue or false representation in the forms, statements and attachments submitted in proof of the qualification requirements or have a record of poor performance, not properly completing the contract, inordinate delays in completion or financial failure, etc.

8. Any additional bid participation criteria / eligibility conditions etc. mentioned in the Technical Specifications sheet will also form part of the qualification requirements along with those mentioned here.

9. Documentary evidence establishing that the bidder is eligible to bid and is qualified to perform the contract if its bid is accepted as per qualification requirements / criteria.

10. Upto date Sales Tax, Income Tax, Service Tax clearance Certificate to be enclosed.

11. Earnest Money Deposit (EMD) of Rs. 50,000/- (Five thousand only) should be submitted along with the bid in the FOLLOWING MANNER.

    a. Crossed demand draft drawn on any Nationalized Bank in favour of Director, NESAC, payable at Umiam (Barapani) or Shillong.

    b. EMD submitted in any form other than as specified above shall not be accepted and shall lead to rejection of the offer.

    EMD shall be forfeited in the following events:

    a. If the offer is withdrawn during the period of validity of the offer or any agreed extension.
    b. If the offer is modified/altered in a manner not accepted to NESAC.
    c. If the tenderer backs-out
    d. If the tenderer attempts to procure the contract by furnishing false/incorrect documents and by giving false declarations.

12. No interest shall be paid by NESAC on EMD. The EMD of un-successful bidders shall be returned within a reasonable time or after expiry of validity period.

13. NESAC reserves the right not to consider the offer of those bidders, whose services against any other contract have been found unsatisfactory.

14. Incomplete offers, conditional offers and offers without requisite EMD shall be rejected.

MANUFACTURERS' AUTHORIZATION FORM (Form-i)

No. _____ Dated _____

Director,
North Eastern Space Applications Centre
Government of India
Department of Space
Umiam -793103, Meghalaya

Dear Sir:

We _____ who are established and reputable manufacturers of _____having factories at (*address of factory)* do hereby authorize M/s _____ *(Name and address of Agent)* to submit a bid, negotiate and receive the order from you against your tender enquiry.

No company or firm or individual other than M/s _____ is authorized to bid, and conclude the contract in regard to this business.

We hereby extend our full guarantee and warranty as per Clause 15 of the General Conditions of Contract and Clause of the Special Conditions of Contract for the goods and services offered by the above firm.

Yours faithfully,

(Name)

(Name of manufacturers)

Note: This letter of authority should be on the **letterhead of the manufacturer** and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the Bidder in its techno-commercial un-priced bid.

BIDDER'S PERFORMANCE STATEMENT FORM (Form-ii)

(For A Period Of Last 3 Years)

Name of the Firmé é é é é é é é é é é é é ..

Order placed by (full address of purchaser)	Order No. and date	Description and quantity of ordered equipment	Price	Date of completion of delivery as per Contract/Actual	Remarks indicating reasons for late delivery, if any	Has the equipment been installed satisfactory? (Attach a certificate from the purchaser/ Consignee)	Contact Person along with Tel. NO., Fax No. & e-mail address

Signature
Rubber stamp

Place :
Date :

SERVICE SUPPORT DETAILS FORM (Form-iii)

S. N.	Nature of training imparted	List of similar type equipments serviced in the past 3 years	Address, Telephone Nos., Fax and e mail address of the firm located in nearby Shillong , Meghalaya	Value of minimum stock of consumable spares held at all times.

Signature and Seal of the manufacturer/Bidderé é é é é é é é é

Place:

Date:

TECHNCAL COMPLIANCE STATEMENT FORM(Form-iv)

An item-by-item commentary on the Purchaser's Technical Specifications demonstrating substantial responsiveness of the goods and services to those specifications or a statement of deviations and exceptions to the provisions of the Technical Specifications. Tender specifications and quantity required are given in the Annexure-I.

Sl. No.	Tender Specifications	Bidder's Specifications	Remarks/Deviation If any

(Technical literature/brochures/manuals should be attached along with this format)

Please note:

1. Compliance/Deviation statement comparing the specifications of the quoted model to the required specifications. This statement should also give the page number(s) of the technical literature where the relevant specification is mentioned.

2. Bids must have supporting documents (technical literature or copies of relevant pages from the service manual or factory test data) for all the points noted above, failure regarding which may result in rejection of bid.

ANNEXURE-II: TECHNICAL SPECIFICATIONS

1. WIRELESS ACCESS POINTS, QUANTITY: 43 NOS.

Sl. No.	Specifications	
1	Standards	▪ IEEE 802.11b, 802.11g Wireless LAN ▪ IEEE 802.3, 802.3u Ethernet ▪ IEEE 802.3x Flow Control ▪ IEEE 802.3af Power over Ethernet (PoE) ▪ IEEE 802.11d Regulatory Domain Selection ▪ IEEE 802.11h
2	Data Transfer Rates	▪ For 802.11g: 108, 54, 48, 36, 24, 18, 12, 9 and 6Mbps+ ▪ For 802.11b: 11, 5.5, 2 and 1Mbps
3	Wireless Frequency Range	▪ 2.4GHz to 2.4835GHz
4	RF Channels	▪ 802.11b: ▪ 11 Channels for United States ▪ 13 Channels for EU ▪ 13 Channels for Japan ▪ 802.11g: ▪ 11 Channels for United States ▪ 13 Channels for Europe Countries ▪ 13 Channels for Japan
5	Radio and Modulation Type	▪ For 802.11b (DSSS): ▪ DBPSK @ 1Mbps ▪ DQPSK @ 2Mbps ▪ CCK @ 5.5 and 11Mbps ▪ For 802.11a/g (OFDM): ▪ BPSK @ 6 and 9Mbps ▪ QPSK @ 12 and 18Mbps ▪ 16QAM @ 24 and 36Mbps ▪ 64QAM @ 48, 54 and 108Mbps ▪ For 802.11a/g (DSSS): ▪ DBPSK @ 1Mbps ▪ DQPSK @ 2Mbps ▪ CCK @ 5.5 and 11Mbps
6	Antennas	• Dual 5dBi Gain Detachable Dipole 2.4GHz Antennas With Reverse SMA Connectors
7	Transmit Output Power 2	▪ For 802.11b: ▪ 18dBm at 11, 5.5, 2 and 1Mbps ▪ For 802.11g: ▪ 18dBm at 6, 9, 12 and 18Mbps ▪ 16dBm at 24 and 36Mbps ▪ 14dBm at 48 and 54Mbps
8	EIRP	▪ Typical EIRP Using 5dBi Antennas: 63mW (18dBm)
9	Receiver Sensitivity	▪ For 802.11b:

		▪ 83dBm at 11Mbps ▪ 89dBm at 2Mbps ▪ For 802.11g: ▪ 87dBm at 6Mbps ▪ 85dBm at 12Mbps ▪ 80dBm at 24Mbps ▪ 71dBm at 48Mbps ▪ 86dBm at 9Mbps ▪ 83dBm at 18Mbps ▪ 76dBm at 36Mbps ▪ 66dBm at 54Mbps
10	Ethernet Interface	▪ 10/100BASE-TX Port With 802.3af PoE Configurable Operation Mode: ▪ Access Point Only
11	Security	▪ 64/128/152-bit WEP Data Encryption ▪ MAC Address Filtering ▪ WPA/WPA2 EAP ▪ WPA/WPA2 PSK ▪ AES ▪ 802.11i-ready ▪ 802.1Q SSID Broadcast Enable/Disable ▪ 8 SSID ▪ Isolated Security for Each SSID (Different Security Setting for Each SSID) ▪ Station Isolation ▪ IEEE 802.1X Supplicant
12	Supported Management Methods/ Protocols	▪ Uses Protocols Supported in DWS- 3024/3026 Unified Switches ▪ HTTP/HTTPS ▪ SSH ▪ Syslog ▪ Telnet
13	Diagnostic LEDs	▪ Power ▪ LAN ▪ WLAN
14	Operating Voltage	▪ 48VDC +/- 10% for PoE
15	Power Supply	▪ Through 48VDC, 0.4A External Power Adapter
16	Certification	▪ FCC Class B ▪ C-Tick ▪ TELEC ▪ Wi-Fi ▪ En60601-1-2 ▪ CE ▪ VCCI ▪ UL ▪ ICES-003

2. WIRELESS CONTROL SWITCH, QUANTITY: 01

Sl. No.	Specifications	
1	Device Interfaces:	24 10/100/1000BASE-T Gigabit Ports With Integrated 802.3af PoE 4 Combo SFP Slots RS-232 Console Port should have minimum two Open Slots for Optional 10 Gigabit Module
2	Power over Ethernet:	Standard: 802.3af Per Port VoltageOutput: 15.4W Voltage Output: 15.4 W Total VoltageOutput: 370W Voltage Output:370 W AutoDisable If Port CurrentOver 350mA
3	Switch Capacity:	48Gbps, 35.71Mpps
4	Flow Control:	802.3x Standard in Full Duplex Mode Back Pressure in Half DuplexMode Duplex Mode
5	WLAN Management Capability:	Up to 48 AP (Directly Connected and Indirectly Connected Through LAN Switch) Up to 2,048 Wireless Users (1,024 Tunneled Users, 2,048 Non-Tunneled Users)
6	Roaming:	Fast Roaming ▪ Intra-Switch/Inter-Switch Roaming ▪ Intra-Subnet/Inter-Subnet Roaming
7	Access Control & Bandwidth Management:	Up to 16 SSID per AP (8 SSID per RF Frequency Band) ▪ AP Load Balancing
8	AP Management:	▪ AP Auto-Discovery ▪ Remote AP Reboot ▪ AP Monitoring: List Managed AP, Rogue AP, Authentication Failed AP ▪ Client Monitoring: List Clients Associated with Each Managed AP ▪ Ad-hoc Clients Monitoring ▪ AP Authentication Supporting Local Database and External RADIUS Server ▪ Centralized RF/Security Policy Management ▪ Automatic AP RF Channel Adjustment ▪ Automatic AP Transmit Output Power Adjustment.
9	WLAN Security:	MAC Address Table Size: 8K Entries ▪ IGMP Snooping: 1K Multicast Groups ▪ Spanning Tree: ▪ 8021.D Spanning Tree

		▪ 802.1w Rapid Spanning Tree ▪ 802.1s Multiple Spanning Tree ▪ 802.3ad Link Aggregation: ▪ Up to 32 Groups ▪ Up to 8 Ports per Group ▪ 802.1ab LLDP ▪ Port Mirroring: ▪ One-to-One Port Mirroring ▪ Many to One Port Mirroring ▪ Jumbo Frame Size: Up to 9Kbytes
10	VLAN:	802.1Q VLAN Tagging ▪ 802.1V ▪ MAC-based VLAN ▪ Double VLAN ▪ VLAN Groups: Up to 3965 ▪ Subnet-based VLAN ▪ GVRP
11	L3 Features:	▪ IPv4 Static Route ▪ Floating Static Route ▪ Proxy ARP ▪ Routing Table Size: Up to 128 Static Routes ▪ VRRP
12	Quality of Service:	802.1p Priority Queues (Up to 8 Queues per Port) ▪ CoS Based on: Switch Port, VLAN, DSCP, TCP/UDP Port, TOS, Destination/Source ▪ MAC Address, Destination/Source IP Address ▪ Minimum Bandwidth Guarantee per Queue ▪ Traffic Shaping per Port
13	ACL (Access Control List):	ACL Based on: Switch Port, MAC Address, 802.1p Priority Queues, VLAN, Ethertype, DSCP, IP Address, Protocol Type, TCP/UDP Port
14	LAN Security:	▪ RADIUS Authentication for Management Access ▪ TACACS+ Authentication for Management Access ▪ SSH v1, v2 ▪ SSL v3 , TLS v1 ▪ Port Security: ▪ 20 MAC Addresses per Port ▪ Trap Violation Notification ▪ MAC Filtering ▪ 802.1x Port-Based Access Control ▪ Denial of Service Protection ▪ Broadcast Storm Control in Granularity of 1% of Link Speed ▪ Protected Port ▪ DHCP Filtering
15	Management Methods:	Web-Based GUI ▪ Telnet Server: Up to 5 Sessions ▪ TFTP Client ▪ Multiple Configuration Files

		▪ BOOTP/DHCP Client ▪ SNTP ▪ Dual Images ▪ CLI ▪ Telnet Client ▪ SNMP v1, v2c, v3 ▪ RMON v1: 4 Groups (Statistics, History, Alarms, Events) ▪ DHCP Server SYSLOG
16	EMI/EMC Certification	FCC Class A ▪ VCCI ▪ C-Tick ▪ ICES-003 ▪ CE
17	Safety Certification:	▪ UL/cUL ▪ CB
18	Power	AC Input Power: 100 to240 VAC, 50/60 Hz Internal Universal Power Supply

3. GIGBIT ACCESS SWITCH QUANTITY: 4 NOS

Sl. No.	**Specifications**	
1	Ports	24 * 10/100/1000 BASE-T Ports with 4 Combo SFP Slots
2	Switch Capacity	▪ 68Gbps
3	Power Over Ethernet	802.3af PoE Support per 10/100/1000BASE-T Port Auto Power/Device Discovery Over-Current Protection
4	L2 Features	+ IGMP snooping v1, v2 - Up to 256 IGMP snooping groups - Up to 64 static multicast address - IGMP Per VLAN - IGMP snooping fast leave + MLD snooping1 + Spanning Tree - 802.1D STP - 802.1w RSTP - 802.1s MSTP + STP Loopback Detection + BPDU filtering + 802.3ad Link Aggregation: max. 32 groups per device, 8 ports per group + Mirroring - One-to-one mode - Many-to-one mode
5	VLAN	+ 802.1v protocol VLAN1 + VLAN Groups: total 256 VLAN groups, max. 256 static VLAN groups, max. 256 dynamic VLAN groups + GVRP

		+ Asymmetric VLAN
6	QoS (Quality of Service)	+ Priority queues number: 4 queues + 802.1p standard + Queue handling: WRR/Strict/ST+WRR modes + Bandwidth Control: - Port and Flow based bandwidth control - Granularity: down to 64Kbps + Class of Service based on: - 802.1p priority - VLAN MAC address - Ether type - IP address - DSCP - Protocol type - TCP/UDP port number
7	EMI/EMC	FCC Class A, ICES-003 Class A, CE, C-Tick, VCCI Class A

4. LAYER 3 SWITCH FOR INTERVLAN ROUTING, QUANTITY: 01 NO

Sl. No.	**Specifications**	
1	Interface	10/100/1000BASE-T Ports: 24 ▪ Combo SFP slots: 4 ▪ Open Slot for 10-Gigabit Uplink Modules:3 ▪ RS-232 Console Port: 1
2	Performance	Switch Fabric: 108Gbps ▪ Packet Forwarding Rate: 80.36Mpps ▪ Packet Buffer: 2MB ▪ MAC Address Table: 16K Entries ▪ IP v4/v6 Routing Table: 12K Entries ▪ IP v6 Routing Table: 6K Entries ▪ IP v4 Host Table: 8K Entries ▪ IP v6 Host Table: 4K Entries ▪ Jumbo Frame Size: 9,216 Bytes
3	L2 Features	IGMP snooping v1, v2, v3 1K IGMP snooping groups 64 static multicast address ▪ MLD snooping 1K MLD snooping groups64 static multicast addresses ▪ Spanning Tree ▪ 802.1D STP ▪ 802.1w RSTP ▪ 802.1s MSTP ▪ STP Loopback detection ▪ BPDU filtering per port and per device ▪ 802.3ad Link Aggregation ▪ Up to 32 groups per device ▪ Up to 8 Gigabit ports or 2 10-Gigabit ports per group ▪ Port mirroring ▪ One-to-One mode

		▪ Many to One mode ▪ ACL mode ▪ Trunking across stack
4	VLAN	802.1Q ▪ 802.1v ▪ Total 4K VLAN groups ▪ Max 4K static VLAN groups ▪ Max 255 dynamic VLAN groups ▪ Configurable VLAN ID from 1 to 4094 ▪ GVRP
5	L3 Features	L3 routing ▪ Up to 12K entries (all route entries combined) ▪ Up to 256 IPv4 static route entries ▪ Up to 128 IPv6 static route entries ▪ Up to 12K IPv4 dynamic route entries ▪ Up to 6K IPv6 dynamic route entries ▪ L3 forwarding ▪ Up to 8K entries (all L3 hardware forwarding entries combined) ▪ Up to 8K Ipv4 forwarding entries ▪ Up to 4K Ipv6 forwarding entries ▪ Floating Static Route ▪ IPv4 Floating Static Route ▪ IPv6 Floating Static Route ▪ Policy Based Route ▪ RIP v1, v2 ▪ RIPng (Ipv6)* ▪ OSPF v2 ▪ OSPF Passive Interface ▪ OSPF NSSA (Not So Stubby Area) ▪ OSPF Equal Cost Route* ▪ Up to 64 IP Interfaces ▪ Multiple IP interfaces per VLAN (up to 5) Multi Path Routing supporting Equal ▪ Cost (EC) and Weighted Cost (WC)* ▪ VRRP ▪ IP v6 Ready Phase 1* ▪ Multicast ▪ Up to 1K multicast groups (static and dynamic multicast groups combined) ▪ Up to 64 static multicast groups ▪ Up to 1K dynamic multicast groups ▪ IGMP v1, v2, v3 ▪ DVMRP v3 ▪ PIM DM for Ipv4 ▪ PIM SM for IPv4 * ▪ Multicast duplication (up to 32 VLAN per port)

		▪ Per port limit IP multicast address range for control packet
	QoS (Quality of Service)	Per port bandwidth control (granularity of 64Kbits per second) ▪ Per flow bandwidth control (granularity of 64Kbits per second) ▪ 802.1p Priority Queues (8 queues) ▪ Queue handling mode support: WRR and Strict modes ▪ CoS based on: ▪ Switch port ▪ VLAN ID ▪ 802.1p Priority Queues ▪ MAC address ▪ IPv4/v6 address ▪ DSCP ▪ Protocol type ▪ IPv6 traffic class ▪ IPv6 flow label ▪ TCP/UDP port ▪ User-defined packet content
6	Access Control List	Up to 8 profiles ▪ Up to 1792 global rules, each rule can set its own port range ▪ ACL based on: ▪ Switch port ▪ VLAN ID ▪ 802.1p Priority Queues ▪ MAC address ▪ IPv4/v6 address ▪ DSCP ▪ Protocol type ▪ IPv6 traffic class ▪ IPv6 flow label ▪ TCP/UDP port ▪ User-defined packet content ▪ Time (time-based ACL) ▪ CPU interface filtering
7	Security	RADIUS authentication for management access (RFC 2138, 2139) ▪ TACACS+ authentication for management access (RFC 1492) ▪ SSH v2 ▪ SSL v3 ▪ Port security (up to 16 MAC addresses per port) ▪ 802.1x port-based/MAC-based access control ▪ Web-based Access Control* ▪ MAC-based Access Control* ▪ Broadcast/Multicast Storm Control (minimum

		granularity of 1 packet per second) ▪ Traffic segmentation ▪ IP-MAC binding (up to 500 entries per device) ▪ IP-MAC-Port binding (up to 500 entries per device) supporting ARP and ACL modes
8	Management	Single IP Management v1.6 ▪ Web-based GUI ▪ CLI ▪ Web GUI traffic monitoring ▪ Web MAC address browsing ▪ Telnet server ▪ Telnet client* ▪ TFTP client ▪ SNMP v1, v2c, v3 ▪ SNMP trap on MAC notification ▪ RMON v1, v2 ▪ Sflow* ▪ BootP/DHCP client ▪ DHCP auto-configuration ▪ DHCP relay option 82 ▪ System log ▪ Trap/Alarm/Log Severity Control ▪ Dual Image ▪ Dual Configuration ▪ Flash file system ▪ Port description ▪ Editable login banner ▪ Editable system prompt ▪ CPU monitoring via web, CLI,SNMP

5. PCI WIRELESS ADAPTOR, QUANTITY: 50 NOS

Sl. No.	**Specifications**	
1	Standards	802.11g wireless LAN ▪ PCI 2.2
2	Media Access Control Protocol	CSMA/CA with ACK
3	Network Transfer Rate/Modulation Technique	802.11b:11Mbps, 5.5Mbps: CCK 2Mbps: DQPSK 1Mbps: DBPSK ▪ 802.11g:54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps, 6Mbps OFDM (Orthogonal Frequency Division Multiplexing)
4	Data Encryption	64/128-bit WEP (Wired Equivalent Privacy)
5	Frequency Range	2.4 - 2.4835 GHz
6	Antenna	External dipole antenna with detachable reverse SMA connector

7	OS Support	Windows 98SE, ME, 2000, XP, Vista

6. UTM (UNIFIED THREAT MANAGEMENT APPLIANCE), QUANTITY: 04 NOS

Sl. No.	**Unified Tread Management Appliance Specification**
	Appliance Requirements
	Product or OEM should be ISO 9001-2000 Certified
	Firewall should be ICSA Labs Certified and UTM Modules should be West Coast Labs Checkmark UTM Level 5 Certified
	OEM should have regional presence for sales & support
	Inbuilt Hard Drive for storage of detailed graphical Logs & Reports
	No additional appliance or software is acceptable for Logs and Reports
	Should comply FCC and CE norms
	Proposed Appliance should support Hindi GUI facility
	UTM Throughput and User Support
	The proposed system should provide minimum 130Mbps UTM Throughput
	The proposed system should provide minimum 500Mbps Firewall Throughput
	The proposed system should support 1000 users
	the proposed system should have 2 ports of GBE & 2 Ports of 10/100
	Administration, Authentication & Configuration
	The proposed system should be able to export and import User Data & Policies in CSV Format
	The proposed system should support Windows NTLM Database, LDAP, RADIUS & Active Directory and in built database of the appliance for User Authentication
	Solution should have Automatic Single-Sign-On (ASSO) Support for Authentication
	The proposed system should be able to support user mapping with single IP address/MAC address or group of IP address/MAC address for authentication.
	The proposed system should provide dynamic DNS support with NATted IP detection facility
	The proposed system must have facility to generate daily, weekly, monthly, and yearly Bandwidth Utilization Graphs (like MRTG) for all the defined ISP Links
	The proposed System should do Real time monitoring of data transfer done by user/IP/application
	The proposed system should allow Network admin to view bandwidth consumed by each individual user in the network in real time basis
	The proposed system must be able generate real time traffic reports Application wise & user wise
	The proposed solution must be able to detect real time bandwidth utilization by Application, User or IP.
	The proposed system should provide facility for Web-based & Secure console based remote administration
	The proposed system must support Parent Proxy with IP and FQDN support.

	The proposed system should able to function as SNMP agent and should be SNMP v1, v2c and v3 compliant
	The proposed system must provide session timeout on per-group basis to forcefully logout user after login session gets timed out.
	Identity based Policy Controls *a) Surfing Quota Policy:* The proposed system should support creation of Daily/Weekly/Monthly Cyclic policy for internet access on Individual User/group basis. *b) Access Time Policy:* The proposed system should support creation of policy to control Internet access time for individual users and group. It should support creation of policy to control Internet access time based on time and days of the week for individual user and group *c) Data Transfer Policy:* • The proposed system should provide facility to allocate Data transfer Quota (1 GB, 2 GB, 100 MB etc) to individual user policies or group policies based on User Identity • The proposed system should support creation of Daily/Weekly/Monthly Cyclic policy for data transfer policy on Individual User/group basis. • The proposed system should provide facility to allocate Data transfer Quota on shared basis between group users
	Firewall Requirements: • The firewall should be dedicated standalone appliance • The proposed system should be ICSA certified. • The proposed system must be Westcoast labs Checkmark Enterprise Firewall certified. • The proposed system must able to create firewall rules with username as matching criteria along with host/host group/Subnet • The proposed system should have firewall with stateful packet filtering technology & must support one-to-one and dynamic user based NAT with a facility to create rules based on usernames, Source & Destination IP address, Hosts, network, IP Range. • The firewall of the proposed system should be based on a hardened OS, should be capable of delivering network protection services at all layers along with options of network gateway level anti virus, anti spam, intrusion detection and prevention, content filtering, multiple ISP load balancing and failover solutions. • The firewall of the proposed system should be able support transparent mode/Bridge mode for Seamless deployment into an existing network without changing IP configurations in the network. • The proposed system must be able to create firewall rules along with unified threat controls like IDP policy, IAP policy, bandwidth policy, Route through specific gateway • The firewall of the proposed system should provide multi-zone security architecture as follows: • User assignable zones on different physical interfaces • Different IDP policies between different zones • Multiple IDP policies for each zone • Anti Virus, Anti Spam, IDP, Web filter between different zones. • The firewall of the proposed system should provide Pre-defined services

	based on port numbers and Layer 7 application signatures and ability to create user-definable services which can be used to define firewall rules. • The proposed system must provide inbuilt PPPoE client and should be capable to automatically update all required configuration (NAT Policies, VPN Configuration, Firewall Rules) whenever PPPoE IP get changed. • The proposed system should provide alerting system on dashboard to alert whenever default passwords are not changed, non-secure access is configured and module subscription is expiring. • The proposed system must provide Personalized Dashboard to allow repositioning of the sections that requires special attention on the top and the information less used, moved to the bottom. Option should be flexible to define multiple layouts of Dashboard view of multiple administrators. • The firewall of the proposed system should support 802.1q based VLAN tagging to segregate devices logically. • The proposed system must provide support for dynamic routing protocol like RIPv1, RIPv2, OSPF, BGP v4. • The proposed system should provide Cisco Compliance Command Line Interface (CLI) for static / dynamic routing management.
	Bandwidth Management: • The proposed system must have integrated Bandwidth Management • The proposed system must be able to set guaranteed and burstable bandwidth per User/IP on individual or shared basis. • The proposed system must be able to create Bandwidth Policies for assigning QoS based on applications and not on IP or Ports • The proposed system should provide user based and layer 7 based visibility and bandwidth utilization for every connection established through that system
	Intrusion Detection and Prevention (IDP): • The proposed system should have signature and anomaly base intrusion detection and prevention system • The proposed system must support the creation of custom IDP signatures • The proposed system must be able to provide multiple IDP policies and allow attaching an IDP policy to a firewall rule. This should help the administrator in defining customized IDP policies as per his requirements of security and alerts • The proposed system must report internal alerts based on username and not on hostnames or IP addresses. • The proposed system should automatically update the attack signatures database from a central database server • The proposed system should be able to detect and block HTTP proxy traffic both from Content filtering solution & also from IDP • The proposed system should be able to detect and block P2P based Instant Messaging applications like Skype. • The proposed system should be able to detect and block Instant Messaging applications like Windows Live Messenger, Rediff bol etc and other port independent applications using IDP signatures. • The proposed solution must have 3500+ signatures for IDP

Gateway Anti-Virus:

- The proposed system must be westcoast labs Checkmark Anti-Virus Gateway certified.
- The proposed system should be westcoast labs Checkmark Anti-Spyware Gateway certified.
- The proposed system should use asynchronous non-blocking I/O model for Antivirus Engine to reduce the load on the appliance.
- The proposed system should have an integrated Anti-Virus solution and should be able to provide real-time detection of viruses and malicious code at the gateway for HTTP, SMTP, POP3, IMAP and FTP over HTTP Internet traffic
- The Basic Virus Signature Database of the proposed system should comprise of the complete Wild List Signatures and variants as well as malware like phishing mails and spyware. The antivirus system should not be share-ware, free-ware
- The proposed system should have facility to add signature / Disclaimer in emails
- The proposed system should have facility to send notification of virus information to admin email id
- The proposed system must support Quarantined functionality on appliance
- The proposed system should have configurable policy options to block different file types such as Executables, Dynamic files
- The proposed system should have configurable policy options to block customized file type attachments like .doc, .xls, .ppt etc
- In SMTP Antivirus scanning subsystem, if email message is either infected, suspicious or protected attachment, then following options should be there to either deliver original email, Do not deliver or remove attachment and deliver. Similarly notification to administrator on either of the above options should be available
- The proposed system should act SMTP proxy not as MTA or Relay server
- In SMTP system, it should support facility to create customized scanning rules
- Customized scanning rules should allow policies to be applicable on sender/recipient email addresses or address groups for notification settings, quarantine settings and file extension blocking
- The proposed system should be able to update signature database automatically at a preconfigured interval with the frequency of less than 1 hour and through manual update action also
- For POP3 & IMAP system, the proposed system should be able to strip the virus infected attachment from the message if virus is detected in the email and should replace the message body with a notification message.
- The HTTP Anti Virus gateway should be able to scan sites based on source, destination and URL regular expressions
- The HTTP Anti Virus system should be able to bypass source & destination Hosts
- The HTTP Anti Virus should have scanning options of real mode and batch mode with option to restrict file size for scanning
- Support Personalized Individual User Quarantine support.
- The proposed system should be able to provide alerts and reports based on username, protocol, IP address, sender, recipient, subject and virus-names
- The proposed system should have virus detection rates of 98% or more

	(provide supporting document to claim the same)
	Gateway Anti-Spam: • The proposed system must have an integrated Anti-Spam solution in the Appliance • The proposed system must have ability to filter SMTP, POP3 and IMAP traffic • The proposed system should have configurable policy options to select what traffic to scan for spam • The proposed system should have facility to mark a copy of all incoming and outgoing emails to administrator defined email address • The proposed system should have an option of having a configurable spam policy per email address or address group • The proposed solution should be able to tag email subject based on the spam filter matching criteria • The proposed system must not use RBL database to check spam mails. • The proposed system should be able to provide alerts and reports based on username, mail protocol IP address, sender, recipient, subject and spam-categories • The proposed system should provide language independent spam detection functionality • The proposed system should provide option to enable/disable antispam functionality for SMTP authenticated traffic. • The proposed system must have facility of real time spam detection. • The proposed system should have ability to filter Image based spam i.e. email message with the text embedded in an image file. • Should support spam detection using Recurrent Pattern Detection (RPD) to identify spam out breaks • The proposed system should provide Proactive Virus Detection Technology which detects and blocks the new outbreaks immediately and accurately. (Virus Outbreak Detection Technology) • The proposed system should store spam emails in Quarantined section in the appliance itself. • Support Personalized Individual User Quarantine support.
	Web Filtering and Application control: • The proposed system must be Westcoast labs Checkmark URL Filtering certified. • The proposed system should use asynchronous non-blocking I/O model for Web Filtering and Application Control to reduce the load on the appliance. • The proposed system should have integrated Web Filtering solution in the appliance • Websites & its category information should be locally stored inside the Appliance & it should not query third party or Remotely Hosted Servers on Data centres • The proposed solution must have provision to block all HTTP upload traffic through content filtering categories. • The web content filtering solution should also be able to work as an independent HTTP proxy server The proposed system should provide web content filtering features as follows:

	• URL database should have at least 20 million sites and 68+ default categories. • Must block / filter HTTPS traffic based on domain names using site Certificates. • Should block URLS based on regular expressions • Should have support for URL exclusion list based on regular expressions • Should be able identify & block Google cached links based on its categories • Should be able to block websites which are hosted on akamai • Should be able to identify requests behind a proxy server and block requests by IP addresses and username which are even behind a proxy server • Should be able to identify URL Translation Web server and block requests to such servers The proposed system should provide application control features as follows: • Should be able to block famous chat and instant messaging communication like yahoo, jabber, msn, AOL messenger etc and other applications based on signatures and independent of ports. • Should be able to block file upload through IM, FTP protocols. • Should be able to block users from accessing public HTTP proxies running on port 80 as well as any other port • The proposed system should have support for user authentication from Windows PDC, Windows AD, LDAP, RADIUS server and Internal Database • The proposed system should be able to customize block message for each categories • The proposed system should be able to log and report usernames, request IP address, domain name, URL, website category and category type • The proposed system should be able to identify traffic based on productive, neutral & unproductive websites as specified by admin • The proposed system should provide default Internet Access policy for unauthenticated HTTP Proxy users. • The proposed system should be CIPA compliant and should provide preconfigured CIPA based Internet Access policy The proposed solution must act as HTTP proxy server
	Multiple ISP Load Balancing and Failover • The proposed system should have integrated multiple ISP load balancing and failover for outbound traffic • The proposed system should support load balancing and failover for more than 2 ISP links • The proposed system should be able to do weighted round robin based load balancing of traffic over multiple links based on the weight assigned to each link • The proposed system should be able to detect link failure based on user configurable set of rules based on ICMP, TCP and UDP
	High Availability • The proposed system should have hardware failover protection in terms of Active-Passive support

	• The proposed system should have automatic as well as manual synchronization facility • The proposed system should be able send alerts on change of appliance status
	Logging and Reporting solution • The proposed system should have integrated on appliance reporting solution. The reports should be accessible through HTTP or HTTPS • The proposed system should provide individual users download & Upload traffic reports • The proposed system should provide user based, group based and IP address based reports for traffic discovery, Gateway level Anti Virus & Anti Spam, Intrusion detection and prevention and Web Content Filter • The proposed system should provide reports in HTML, Graphical and CSV format • The proposed system should have configurable options to send the reports on mail to designated email addresses • The proposed system should have options to create users with different access rights (E.g. users who can only view reports and not manage the system) • The proposed system should be able to provide connection wise reports for user, application, source and destination IP address and source and destination port and protocol • The reporting solution of the proposed system should be able to provide detailed reports about the mail activity passing through the system • The reporting solution of the proposed system should be able to provide detailed Audit log for auditing and tracking system • The proposed system should provide approximate 45 regulatory compliance reports for SOX, HIPPA, PCI, FISMA and GLBA compliance. • The proposed system should support multiple syslog servers (at least 5) for remote logging. • The proposed system should support logging of Antivirus / Antispam / Content Filtering / Traffic Discovery / IDP / Firewall activities on syslog servers. • The proposed solution must support minimum 5 syslog server for logging information
	Virtual Private Network (VPN) • The proposed system should be westcoast labs Checkmark VPN certified. • The proposed system should be VPNC Basic Interop Certified. • The proposed system should be VPNC AES Interop Certified. • The proposed system should allow to create and establish IPSec (Net-to-Net, Host-to-Host and Road warrior connection), L2TP and PPTP VPN connection • The proposed system should allow Preshared key and Digital Certificate based Authentication. • The proposed system should support Connection fail over for Net-to-Net, Host-to-Host and Road warrior connection. • The proposed system should support following Encryption algorithm: 3DES, DES, AES, Twofish, Blowfish, Serpent • The proposed system should support external Certificate Authorities

	• The proposed system should provide a facility to export the Road Warrior connection configuration for use by the VPN client • The proposed should support most commonly available VPN IPSec Clients. • The proposed system should provide local Certificate Authority and should provide facility to create/renew/delete self-signed certificates. The proposed system should have preloaded 3rd party Certificate Authority including VeriSign/Entrust.Net/Microsft and provide facility to upload any 3rd party Certificate Authority

7. OTHER NETWORK COMPONENTS:

a) **CAT 6 cable (**305 Mtrs of Cat 6 Cable for connecting the APôs to switches**) QUANTITY: 2 BOXES OF 305 MTRS**

b) **RJ 45 CONNECTORS, QUANTITY: 100 NOS.**

c) **CABLE LYING WITH CASING AND CAPPING, QUANTITY: 2 BOXES OF 305 MTRS**

d) **6U RACK (**6U wall Mount Rack with accessories**), QUANTITY: 04 NOS.**

e) **RACK 42U (**42U Floor Mount Rack with accessories**), QUANTITY: 01 NO**

8. SERVICES

Installation Rack , Laying of UTP Cable using proper conduit, Installation of Wireless Access Points , Switches etc.
Network Integration/Network Management/Consultancy
Configuration of UTM Appliance as per NESAC Requirement and Regulations

9. *DEDICATED ENGINEER FOR MAINTENANCE OF WIRELESS LAN, QUANTITY: 01 NO*

Terms & Conditions:

a) One dedicated Engineer with good working experiences in installation & configuration of Wireless Local Area Network (LAN), Wide Area Network (WAN), Virtual LAN (VLAN), Linux, Security solution etc. to be posted at NESAC during the warranty period (One year).

b) Vendor must furnish the name, address and qualification of the Engineer along with relevant proof of qualifications and experience documents.

c) The vendor must furnish the C & A (character & antecedents) report of all the DEOs from the concerned authority within one month from the date of agreement.

d) The vendor and his Engineer should abide by all the safety and security regulations of NESAC. He is not permitted to do any work other than the work being assigned by NESAC and also they are not permitted to take out any material, printout, drawings and documents etc. belonging to NESAC. The vendor shall be responsible and liable for any such action of their Engineer employed by him.

BILL OF MATERIAL FOR WIRELESS NETWORK

Sl No	Item Description	Qty
01	Wireless Access Point	43
02	Wireless Control Switch	01
03	Gigabit Access Switch	04
04	Layer 3 switch for Inter VLAN routing	01
05	PCI Wireless Adapters for Desktops	50
06	Unified Threat Management (UTM) Device	04
07	Cat 6 UTP Cable	2 Boxes of 305 Mtrs
08	RJ 45 Connector	100
09	Cable Lying with casing and capping	2 Boxes of 305 Mtrs
10	Pre-Installation site survey ,installation and configuration of Wireless Devices and Switches	
11	Installation and Configuration of UTM Device as per the requirement of NESAC	
12	Installation and configuration Linux for Wireless security	
13	Dedicated Engineer for maintenance of Wireless LAN	01

PART-II

PRICE BID

Terms & conditions:

- The Price Bid shall comprise the Techno Commercial Bid with price indicated in the bid form.
- The Bidder shall indicate the unit prices with item wise price break-up and total bid prices of the goods it proposes to supply under the order and enclose it with the priced bid.
- Prices shall be quoted in Indian Rupees.
- Purchaser will award the contract to the successful Bidder whose bid has been determined to be substantially responsive and as per the requirement of NESAC
- NESAC reserves the right to award the order to a technically qualified party only based on Price bid evaluation on total amount only. Since it is a single package of requirement, hence, in any case, order will not be divided to more than one vendor.
- The Purchaser reserves the right at the time of contract award to increase or decrease the quantity of goods and services originally specified in the schedule of requirements without any change in unit price or other terms and conditions.
- Suppliers shall be entirely responsible for all taxes, duties, license fees, octroi, road permits, etc., incurred until delivery of the contracted Goods to the Purchaser. However, VAT in respect of the transaction between the Purchaser and the Supplier shall be payable extra, if so stipulated in the order.

PERFORMA FOR SUBMISSION OF QUOTATIONS

Sl No	Item Description	Qty	Unit price (Rs)	Total Price (Rs)
01	Wireless Access Point	43		
02	Wireless Control Switch	01		
03	Gigabit Access Switch	04		
04	Layer 3 switch for Inter VLAN routing	01		
05	PCI Wireless Adapters for Desktops	50		
06	Unified Threat Management (UTM) Device	04		
07	Cat 6 UTP Cable	2 Boxes of 305 Mtrs		
08	RJ 45 Connector	100		
09	Cable Lying with casing and capping (one time)	2 Boxes of 305 Mtrs		

10	Pre-Installation site survey ,installation and configuration of Wireless Devices and Switches (one time)			
11	Installation and Configuration of UTM Device as per the requirement of NESAC (one time)			
12	Installation and configuration Linux for Wireless security (one time)			
13	Dedicated Engineer for maintenance of Wireless LAN (one year)	01		