Document for TEC-GR

GAJSHIELD
Data Security Firewall

Filtering

- The Firewall shall support Group Filtering based on L3/L7 parameters such as IP, Directory Number Identification Service (DNIS), subnet etc. is provided
- The Firewall shall support MAC Address Filtering based on source and destination address.
- The Firewall shall support Discard Unknown to drop packets that are sourced from Unknown MAC address
- The Firewall shall support Bridge protocol data unit (BPDU) filtering.
- The Firewall shall support Unicast MAC filtering.
- The Firewall shall have the capability to filter L2 traffic configurable on per Port/ PVC/ Service basis at least for the following parameters: Broadcast Traffic, Source MAC Address, Destination MAC Address, IGMP groups, Multicast Groups, TCP flags, IGMP type, ICMP type, Ether type
- Block AH traffic as per RFC 1825 & RFC 1828
- FTP as per RFC 959, RFC 2228 & RFC 2428 for IPv6
- GOPHER as per RFC 1436
- HTTP1.0 and HTTP 1.1as per RFC 1945 & RFC 2616
- ICMP_ANY as per RFC 792 for IPv4 and RFC 4443 for IPv6
- Internet-Locator-Service
- NFSv4 as per RFC 3530
- NNTP as per RFC 3977
- NTPv4 as per RFC 5905
- OSPF as per RFC 2328; OSPFv6 as per RFC 5340
- PING as per RFC 792
- TFTP, IRC
- The firewall shall support filtering for following authentication Protocols: DIAMETER
- The firewall shall support following filtering database applications: RDBMS, DB2, SQL.
- The firewall shall support for filtering multimedia applications such as VoIP, H.323, SIP, RTP, RTCP etc
- The firewall shall support for filtering HTTP traffic based on URLs based on content string matches
- The Firewall shall support transparent redirection of HTTP traffic as per RFC 3040

Security Services

- Support for ICMP filtering with configurable threshold
- Detect Ping of Death
- Detect Land attack
- Detect Win Nuke attack using IPS
- Filter IP source route option
- The Firewall shall support Flag and option checking
- The Firewall shall support TCP packet checksum verification
- The Firewall shall support privacy, identity control feature and provides transport layer security features
- The Firewall shall support Blocking of popular peer-to-peer protocols

Integrity

- Overload protection mechanism shall be available. System shall revert back to normal mode of operation when load is reduced
- On power up the firewall shall use built-in system monitoring & diagnostics before going online to detect failure of hardware
- Communication among the firewall system's components shall be secure
- The firewall shall be capable of communicating with Intrusion Detection System or in-built IPS over standard APIs or OPSec. APIs for the same shall be provided

Privacy

- Extensive debugging capabilities to assist in hardware problem resolution shall be supported
- The firewall system shall provide for a single default gateway IP address for all firewalls in a cluster
- The firewall system shall have a facility to block any unencrypted means of access to the firewall
- The firewall system shall provide a means to define and modify existing services and state engine

Logging

- The firewall shall be able to consolidate log data for –
    - Network services
    - Network resources
    - User/groups
    - Connection duration
    - Number of bytes transferred
    - Blocked connections
    - Source/Des. IP addresses
    - Failed authentication attempts
    - Date/Time
    - Firewall identity
    - Intrusion attempts
    - Alert/error conditions

- The user shall be able to specify/create modify/delete rules/policies to collect log data and consolidate based on what he requires using Firewall eMS/Manager
- The log consolidator shall be able to use firewall objects/users for use in the consolidation policy using Firewall eMS/Manager
- The firewall shall provide in-depth details on network traffic and activities
- Reporting software components shall support distributed environment/ installation.
- The firewall shall provide a means for specifying thresholds and conditions for which it would send an alert

Database

- The firewall subsystem shall allow maintenance of detailed records and audit trail information. The firewall System shall be able to provide complete real time control of the network configuration including accounting, live connections monitoring, alerting, notification to the syslog server

IP Routing Protocols

- RIPng for IPv6 as per RFC 2080
- OSPFv3 for IPv6 as per RFC 2740
- IPv6 Static Routing
- IPv6 Route Redistribution

General IPv6 support

- IPv6 Address types: Unicast (Unique Local IPv6 address as per RFC 4193), Anycast and Multicast
- ICMPv6 as per RFC 2463
- IPv6 Neighbour Discovery as per RFC 2461
- IPv6 stateless auto configuration as per RFC 4862
- IPv6 MTU path discovery as per RFC 1981
- IPv6 ping
- ICMPv6 redirect
- ICMPv6 rate limiting
- IPv6 neighbour discovery duplicate address detection
- IPv6 default router preference as per RFC 2711
- IPv6 access control
- Syslog over IPv6
- IP SLAs for IPv6
- IPv6 Specification as per RFC 2460
- IPv6 Scoped Address Architecture as per RFC 4007
- ICMPv6 for IPv6 Specification as per RFC 4443

IPv6 QoS

- Packet classification as per RFC 2474
- Traffic shaping
- Traffic policing
- Packet marking/re-marking as per RFC 2475
- IPv6 QoS queuing
- Weighted random early detection (WRED)- based drop
- Assured Forwarding PHB Group shall be as per RFC 2597
- LAN switch shall support An Expedited Forwarding PHB as per RFC 2598

IPv6 Services

- Standard access control lists for IPv6
- Secure Shell (SSH) support over IPv6
- IPv6 MIB support
- SNMP over IPv6
- IPv6 IPSec VPN
- Stateless DHCPv6
- DHCPv6 prefix delegation
- DHCP for IPv6 relay agent
- DHCPv6 prefix delegation via AAA
- DHCPv6 Server Stateless Auto Configuration
- DHCPv6 Client Information Refresh Option
- DHCPv6 relay agent notification for prefix delegation
- DHCPv6 relay- reload persistent interface ID option
- DHCP - DHCPv6 Individual Address Assignment
- Dynamic Host Configuration Protocol for IPv6 (DHCPv6) as per RFC 3315
- DNS Extensions to Support IP Version 6 as per RFC 3596
- DHCP IPv6 Prefix Delegation RFC 3633
- DNS Configuration options for DHCPv6 as per RFC 3646
- Stateless DHCP Service for IPv6 as per RFC 3736
- IP Forwarding Table MIB as per RFC 4292
- Management Information Base for the Internet Protocol as per RFC 4293
- Dynamic Host Configuration Protocol version 6 (DHCPv6) options as per RFC 3319

IPv6 Multicast

- IPv6 Multicast Listener Discovery (MLD) protocol versions 1 and 2
- IPv6 PIM sparse mode (PIM-SM)
- IPv6 PIM Source Specific Multicast (PIM-SSM)
- IPv6 multicast scope boundaries
- IPv6 multicast MLD access group
- IPv6 multicast PIM accept register
- IPv6 multicast PIM embedded RP support
- IPv6 multicast RPF flooding of bootstrap router (BSR) packets
- IPv6 multicast routable address hello option
- IPv6 multicast SSM mapping for MLDv1 SSM
- IPv6 multicast IPv6 BSR—ability to configure RP mapping
- IPv6 multicast MLD group limits
- IPv6 Multicast Address Assignments as per RFC 2375
- IPv6 Multicast Listener Discovery (MLD) protocol, versions 1 and 2 as per RFC 2710
- MLDv2 for IPv6 as per RFC 3810 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address as per RFC 3956

General Requirement

- Firewall shall support redundant fans, Disk, Control subsystem and CPU or firewall shall be deployed in high availability configuration in No single point of failure configuration (NSPOF)

User Interface

- The firewall EMS shall provide a means for exporting the firewall rules set and configuration to a text file
- The firewall shall support external user database authentication for firewall admin user

Quality Requirements

- The supplier / manufacturer shall manufacture with international quality standards ISO 9002 for which the manufacturer shall be duly accredited. The quality plan describing the quality assurance system followed by the manufacturer shall be required to be submitted
- The equipment locally manufactured in India shall be as per guidelines vide Documents No. QM 118, QM 205, QM 206, QM 210 and QM 301
- The equipment shall meet the environmental requirements as per category A of QM-333/Issue-1/Sept 1990
- All components used shall be as per approval procedures prescribed by BSNL in document QA QM – 324
- Marking and identification of the equipment, sub-assemblies, PCBs etc. shall be as per guidelines given in Para 5.1.7 Quality Assurance Telecom Document QM 351/Issue 2 /Jan.'95
- The MTBF (Mean Time Between Failure) and MTTR (Mean Time to Repair) predicted and the manufacturer shall furnish observed values along with calculations

EMI/EMC Requirements

- **General Electromagnetic Compatibility (EMC) Requirements:**
  - The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished from a test agency
- **Conducted and radiated emission (applicable to telecom equipment):**
  - **Name of EMC Standard:** "CISPR 22 (2005) with amendment 1 (2005) & amendment 2 (2006) - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment"
  - **Limits: -**

    i) To comply with Class A or B (to be mentioned in the GR / IR as per the specific requirement) of CISPR 22 (2005) with amendment 1 (2005) & amendment 2 (2006).

    ii) The values of limits shall be as per TEC Standard No. TEC/EMI/TEL-001/01/FEB09
- **Immunity to Electrostatic discharge:**
  - **Name of EMC Standard:** IEC 61000-4-2 {2001) "Testing and measurement techniques of Electrostatic discharge immunity test"
  - **Limits: -**

    i) Contact discharge level 2 {± 4 kV} or higher voltage;
    ii) Air discharge level 3 {± 8 kV} or higher voltage;

- **Immunity to radiated RF:**
    - **Name of EMC Standard**: IEC 61000-4-3 (2006) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test"
    - **Limits**: - For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)
      i) Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and
      ii) Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.
      For Telecom Terminal Equipment without Voice interface (s) Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz

- **Immunity to fast transients (burst):**
    - **Name of EMC Standard:** IEC 61000- 4- 4 {2004) "Testing and measurement techniques of electrical fast transients/burst immunity test"
    - **Limits: -**
      Test Level 2 i.e. (a) 1 kV for AC/DC power lines; (b) 0. 5 kV for signal / control / data / telecom lines

- **Immunity to surges:**
    - **Name of EMC Standard**: IEC 61000-4-5 (2005) "Testing & Measurement techniques for Surge immunity test"
    - **Limits: -**

      i) For mains power input ports: (a)1.0 kV peak open circuit voltage for line to ground coupling (b) 0.5 kV peak open circuit voltage for line-to-line coupling

      ii) For telecom ports: (a) 0.5 kV peak open circuit voltage for line to ground (b) 0.5 KV peak open circuit voltage for line-to-line coupling

- **Immunity to conducted disturbance induced by Radio frequency fields:**
    - **Name of EMC Standard:** IEC 61000-4-6 (2003) with amendment 1 (2004) & amd. 2 (2006) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields"
    - **Limits: -**
      Under the test level 2 {3 V r.m.s.} in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines

- **Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):**
    - **Name of EMC Standard:** IEC 61000-4-11 (2004) "Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests"
    - **Limits: -**

      i) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e., 70 % supply voltage for 500 ms)

ii) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) and

iii) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s

- **Note 1:** Classification of the equipment:
- **Class B:** Class B is a category of apparatus which satisfies the class B disturbance limits. Class B is intended primarily for use in the domestic environment and may include:
  *Equipment with no fixed place of use; for example, portable equipment powered by built in batteries;
  * Telecommunication terminal equipment powered by the telecommunication networks
  * Personal computers and auxiliary connected equipment. Please note that the domestic environment is an environment where the use of broadcast radio and television receivers may be expected within a distance of 10 m of the apparatus connected
- **Note 2:** The test agency for EMC tests shall be an accredited agency and details of accreditation shall be submitted. Alternatively, EMC test report from a non-accredited test lab, which is audited by an accredited lab / accrediting authority for the availability of all the essential facilities (test equipment, test chamber, calibrations in order, test instructions, skilled personnel etc.), required for performing the tests according to the EMC test methods audited, may be acceptable. However, such accredited lab / accrediting authority should take responsibility of the test results of the "non accredited lab" along with indication of period of such delegation and the submitted test report should be of such valid period of delegation. The audit report, mentioning above facts, should be provided along with EMC test report
- **Note 3**:- For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. TEC/EMI/TEL-001/01/FEB-09 and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (g) and TEC Standard No. TEC/EMI/TEL-001/01/FEB-09

Safety Requirements

- The equipment shall conform to IS 13252 part 1: 2010 "Information Technology Equipment - Safety- Part 1 General Requirements" [equivalent to IEC 60950-1 {2005} "Information Technology Equipment -Safety- Part 1 General Requirements" and IS 10437 {1986} "Safety requirements for radio transmitting equipment's" [equivalent to IEC 60215]

Management & Reporting

- The firewall System functionality shall be carried out with the help of a completely independent operating system, which shall be written/ hardened with Information security as the objective
- The firewall subsystem shall allow data communication only by authenticated network resources
- The firewall System shall support Telnet client functionality. It shall be possible to deactivate Telnet session. It shall support egress and ingress filtering so that only authorized IP address is able to enter into the firewall system. Number of permitted telnet session shall be configurable
- The firewall System shall support Remote login as per the latest guidelines issued by DoT
- The Firewall shall meet the security certification requirements mandated by DoT from time to time

Engineering Requirements

- The equipment shall adopt state of the art technology
- The manufacturer shall furnish the actual dimensions and weight of the equipment
- All connectors shall be reliable, low loss and standard type so as to ensure failure free operations over long operations
- All LAN cabling shall be of Gigabit Ethernet ready
- The equipment shall have adequate cooling arrangements
- The equipment shall be designed for continuous operation
- The equipment shall be able to perform satisfactorily without any degradation at an altitude up to 3000 meters above mean sea level
- The design of the equipment shall not allow plugging of a module in the wrong slot or upside down
- The removal or addition of any cards shall not disrupt traffic on other cards
- The removal or addition of any cards shall not disrupt traffic on other cards
- In the event of a full system failure, a crash dump shall be supported for analysis and problem resolution
- A power down condition shall not cause loss of connection configuration data storage in high availability mode
- Live Insertion and hot swap of modules shall be possible for chassis-based firewalls to ensure maximum network availability and easy maintainability
- The system hardware and software shall not pose any problem, due to changes in date and time caused by events such as changeover of millennium / century, leap year etc., in the normal functioning of the system
- Wherever, the standardized documents like ITU-T, IETF, QA and TEC documents are referred, the latest issue and number with the amendments shall be applicable
- Power Supply: The equipment power supply requirements are given for each of the Category. In addition, it shall meet the following requirements:
    - The equipment shall be able to function over the range specified in the respective chapters, without any degradation in performance

  - The equipment shall be protected in case of voltage variation beyond the range specified and against input reverse polarity
  - The derived DC voltages shall have protection against short circuit and overload
- The equipment shall have:
  - Proper earthing arrangement
  - Protection against short circuit / open circuit
  - Protection against accidental operations for all switches / controls provided in the front panel
  - Protection against entry of dust, insects, and lizards

General

- HTTP security services:
  - The Firewall shall support RFC compliance
  - The Firewall shall support protocol state tracking
  - The Firewall shall support Uniform Resource Identifier (URI) length enforcement.
- FTP security services:
  - The Firewall shall support Protocol state tracking
  - The Firewall shall support Dynamic Port opening & closing
  - The Firewall shall have the capability to enforce what operations users and groups can perform within FTP sessions

Link Aggregation Requirements

- The firewall shall support IEEE 802.3ad link aggregation control protocol (LACP)

Intrusion Detection & Prevention (IDP) Requirements

Architecture IDP

- IDP shall allow working in failover mode
- IDP shall provide multi segment protection with provision to have different security policies for different IP addresses/ subnets, port, VLANs & also provision for different action per segment/policy
- Attack Isolation at multi-gigabit speeds, ensures the availability of mission critical traffic even while under attack
- IDP devices shall block only the attack session without effecting service to legitimate clients
- For each attack the system shall send a complete capture of the filtered packet along with the attack event report to management station that can be used as proof of attack
- IDP system shall have Centralized configuration, management & Reporting station with provision for secure communication & authentication between IDP & management station.
- The IDP shall be able to get synchronized to a network time source through Network Time Protocol or simple Network Time Protocol

- The IDP shall be scalable and re-configurable, and its licensing shall be such so as not to affect network expansion
- IDP system if installed in bridge mode shall be transparent and invisible to network (Applicable only if Bridge mode deployment available)

Filtering in IDP

- NetMeeting
- PC-Anywhere
- SIP-Messenger
- SAMBA
- SKYPE, HANGOUT, GOOGLE-TALK etc
- Lotus Notes based on SMTP
- Microsoft Exchange based on SMTP

Incident Monitoring and Detection

- IDP shall be able to monitor the network traffic on all the LAN segment for signs of attack, unauthorized access attempts and misuse and shall be able to detect them
- Protocol analysis (for protocol like FTP, HTTP, SMTP, POP3, IMAP, TELNET etc.) and pattern matching shall be supported by IDP. iii. IDP shall support pattern-based signatures having a strong sense of context, so that false alarms/incident detections are minimized
- IDP shall be able to detect incidents that originate from inside the network perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies
- IDP shall be able to detect and shall be able to stop Denial of Service attacks like Smurf attack, Teardrop attack, UDP Flooding, Land attack, Win Nuke attack, TFN2K, SYN attack, Stream – like DoS attack, IP/MAC spoofing etc
- IDP shall support blocking of anonymous open HTTP Proxy running on 80 port or any other port & also shall support client based open proxy like Ultra surf
- IDP shall be able to detect & block known P2P based instant messaging application like skype & known chat application like WLM, Rediff Bol etc
- IDP shall be able to detect VoIP (like SIP) data and shall be able to block the same
- IDP shall be able to detect and shall be able to stop Pre-Attack Probes like various types of TCP/UDP scanners, Vertical Scanning Detection, etc
- IDP shall be able to detect and shall be able to stop any Suspicious Activity
- Creation of User-specified signatures shall be possible based upon contents i.e., string matching etc
- IDP shall be able to modify the application filtering logic such that it detects incidents related to a subset of the network traffic (specific IP addresses, for example)
- IDP shall support signatures tuning to match the operational requirements of the customer network so that false policies are minimized
- IDP shall support help system that describes the incidents in adequate detail, providing sufficient information about:
    - The incident
    - The potential damage
    - Possible false positives

    - The systems affected
    - How to respond immediately upon detection of the incident
    - How to remove the vulnerability associated with the incident
- IDP shall be configured to focus on the incidents that pose the greatest risk to the network.
- IDP shall detect the malicious activity event in fragmented and de-fragmented packets
- IDP shall provide Stateful Operation
    - TCP Reassembly
    - IP De-fragmentation
    - Bi-directional Inspection
    - Forensic Data Collection
    - Access Lists
- The IDP shall provide the capability to annotate incidents recorded in the database.
- IDP shall provide Intrusion Detection & Prevention for at least following Applications:
    - Web Protection: IIS and Apache vulnerabilities, protection for web applications such as CGI, Cold Fusion, FrontPage, SQL Injection and cross-site scripting
    - Remote access protection: Telnet vulnerabilities and FTP server protection
    - SNMP Vulnerability
    - SQL server protection: prevention of the exploitation of vulnerabilities found in SQL implementation from miscellaneous vendors
    - DNS protection: prevents the exploitation of vulnerabilities found in DNS implementation of various vendors
    - Backdoor & Trojans prevents the backdoor outbound and inbound communications, and prevent the network from being controlled remotely
- IDP Shall Protect against various DOS & DDOS attacks as follows:
    - One Packet Attack Protection
    - Protection against TCP, UDP & ICMP Flood
    - Layer 2 attacks such as DHCP Flooding prevention

Incident Response

- IDP shall be able to show alarms on the management console, upon detection of an incident
- Shall detect attack due to URL decoding vulnerabilities
- IDP shall be capable of:
    - IDP shall be capable of Attack Isolation:
    - Access Control of traffic per application ports and networks allows a predefined set of applications only and denies all other types of traffic
    - Attack isolation and protection against unknown flooding attacks

Configuration IDP

- IDP shall provide creation of multiple IDP policy for different zone instead of blanket policy at interface level
- IDP shall support help system providing a detailed description of the attack signature that is selected
- The administrator, from the management console, shall be able to specify the response to each pre-defined event

- IDP shall be able to tune the pre-defined signatures in such a way that the false alarms/incident detections are minimized. Shall provide capability to filter out false positives once they have been identified as such
- IDP shall be able to be configured such that attack signature and traffic analysis focus only on specified hosts, specified protocols, or specified services
- It shall be possible to specify New Services (as defined by TCP/IP port number) by the administrator. New attack signatures shall then be based upon that new, user-defined Service
- IDP shall be capable of attack policy customization.
- IDP shall have provision to analyse and identify the ingress point of attack

IDP User Interface

- IDP user interface
- IDP user interface shall support following for access:
    - HTTPS
    - SSH
- IDP user interface shall provide Graphical User Interface (GUI) as follows:
    - IDP shall be able to graphically depict both suspicious activity and normal network activity
    - The graphical interface shall be easy to use for by operators and shall require no special technical knowledge
    - The graphical interface shall use an iconic display to alert operators to important occurrences
    - The graphical interface shall be able to display summary information sorted by source address (initiator), destination address (target), or event type
    - The graphical interface shall support a "drill down" mechanism so that the operator may obtain additional information about an event. This information includes action(s) that were taken by IDP in response to the event
    - The graphical interface shall be able to consolidate multiple event occurrences into a single alarm

Data Management IDP

- IDP shall support data management capabilities provide critical information required for risk assessment and decision-making
- IDP shall be capable of prioritization of security event data for quick and easy threat assessment

IDP Reports

- IDP shall have customized report generation capability e.g., excel, text, HTML, etc., as per SP’s requirement which shall be specified at the time of tendering
- It shall be possible to generate templates for the pre-defined reports, so that custom reports can be generated using the standards reports as a starting point
- It shall be possible to generate multiple forms of reporting suitable for all technical levels.

- IDP shall support reports that may be exported to different formats, such as excel, HTML or a Word document etc
- Provision for structured reporting to reduce security events messages floods when the device is under attack. Instead of sending an event per each security event, the device shall send an event within a pre-defined reporting period
- IDP shall provide drill down reports based on Real Time attack statistics for following:
    - Security event risk level
    - Date/time
    - Subnets (Networks/ IP Address)
    - Event name
    - Source IP
    - Destination IP
    - User Identity
    - Response taken
    - Severity
    - Top attack types
    - Attack groups
    - Top-10 Source of Attacks
    - Top-10 Destination of attacks
- Management station shall be able to show Graph with number of attacks coming from different networks
- Provision to automatically generate & email reports daily, weekly or monthly to predefined email addresses. (optional)
- Provide reports in different formats like excel sheet, Word, HTML etc
- IDP shall provide alerts/notify

Security IDP

- The IDP shall be able to protect itself against attacks and shall not use any service/functionality/feature on the host that might make it vulnerable to attack
- The IDP shall monitor its internal application modules and notify the management station when a module goes offline unexpectedly
- The IDP and management console shall be protected against intentional or accidental abuse, unauthorized access and loss of communication

Performance IDP

- IDP shall process network traffic at a rate that does not add delay, or becomes a congestion point while attack signatures active
- IDP shall support performance that scales well with the number of attack signatures and filters active

IDP Updates

- Update attack signatures, rule bases and service releases via the Internet or with Version Upgrades

- It shall be possible to download and update new attack signatures and major software releases from the Web in addition to local update from the management console
- It shall be possible to update IDP remotely and securely with new signature (Pattern of DoS Attack, pattern for hacking attempts using a particular hacking software etc.) updates or full IDP software update

Antivirus

- The Firewall shall perform both inbound and outbound inspection
- The Firewall shall have 2.5+ million virus signatures for comprehensive coverage
- The Firewall shall perform email attachment inspection including compressed files in multiple layers (e.g., where a compressed attachment has another compressed file), email messages and FTP downloads/uploads, or embedded scripts
- The Firewall shall be able to scan all traffic or specific extensions as defined by the administrator
- The Firewall shall support an Allow and Deny list of valid IP to allow/deny relaying for
- The Firewall shall be able to block attachment by file name and extension
- The Firewall shall support Recursive Analysis on messages and Compressed files
- The Firewall shall have separate inbound and outbound virus and content. Scanning policies
- The Firewall shall provide option to bypass scanning for specific HTTP traffic
- The Firewall shall scan http traffic based on username, source/destination IP address or URL based regular expression

Documentation

- System description documents
- Installation, Operation and Maintenance documents
- Training documents
- Repair manual
- System description documents: The following system description documents shall be supplied along with the system
    - Over-all system specification and description of hardware and software
    - Equipment layout drawings
    - Cabling and wiring diagrams
    - Detailed specification and description of all Input / Output devices
    - Adjustment procedures if there are any field adjustable units
    - Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification
- System operation documents: The following system operation documents shall be available
    - Installation manuals and testing procedures
    - Precautions for installation, operations, and maintenance
    - Operating and Maintenance manual of the system
    - Safety measures to be observed in handling the equipment
    - Man-machine language (command set) manual
    - Fault location and troubleshooting instructions including fault dictionary
    - Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance and unit / card / subassembly replacement.

    - Emergency action procedures and alarm dictionary

- **Training Documents**
    - Training manuals and documents necessary for organizing training in installation, operation and maintenance and repair of the system shall be made available
    - Any provisional document, if supplied, shall be clearly indicated. The updates of all provisional documents shall be provided immediately following the issue of such updates
    - The structure and scope of each document shall be clearly described
    - The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information
    - All diagrams, illustrations and tables shall be consistent with the relevant text

Installation

- All necessary interfaces, connectors, connecting cables and accessories required for satisfactory installation and convenient operations shall be supplied. Type of connectors, adopters to be used shall be in conformity with the interfaces defined in this GR
- It shall be ensured that all testers, tools, and support required for carrying out the stage by stage testing of the equipment before final commissioning of the network shall be supplied along with the equipment
- All installation materials, consumables, and spare parts to be supplied
- All literature and instructions required for installation of the equipment, testing, and bringing it to service shall be made available in English language
- For the installations to be carried out by the supplier, the time frames shall be furnished by the supplier including the important milestones of the installation process well before commencing the installations
- In the event of a bug found in the software, the manufacturer shall provide patches and firmware replacement if involved, free of cost. Compatibility of the existing hardware shall be maintained with future software/firmware
- Special tools required for wiring shall be provided along with the equipment