

**Technical Specification for Next Generation Firewalls (NGFW)**

1. NGFW shall have following features including but not limited to:  
Encryption through IPSec VPN (Virtual Private Network), Deep Packet Inspection (DPI), Denial of service (DoS) & Distributed Denial of Service (DDoS) prevention, Port Block/ Allow, rules/policies for block/allow, IP (Internet Protocol) & Media Access Control (MAC) spoofing protection, threat detection, Intrusion Prevention System (IPS), Anti-Virus, Anti-Spyware, Man In The Middle (MITM) attack prevention.
2. The proposed firewall shall be able to handle (alert, block or allow) unknown /unidentified applications e.g. unknown TCP & UDP packets. It shall have the provision to define application control list based on application group and/or list.
3. Firewall shall have feature and also have capability to update the definition/ Signatures of Anti-Virus online as well as offline. Firewall shall also be compatible to update the definitions/signatures through CMC. There shall be a defined process for security patching and firmware up-gradation. There shall be a feature to field validate firmware checksum. The same shall also be validated before using the OEM provided file/binary in the process of firmware up-gradation and security patching
4. Firewall shall have Management Console port to configure remotely.
5. Firewall shall be EMI/EMC compliant in Substation environment as per IEC 61850-3.
6. Firewall shall be rack mounted in existing standard equipment cabinets.
7. Firewall shall have support of SCADA applications (IEC-60870-5-104), ICCP, PMU (IEEE C37.118), Sub-Station Automation System (IEC 61850), Ethernet and other substation environment protocols.
8. Client based Encryption/ VPN must support different Operating System platforms e.g. Windows, Linux & Mac.
9. The solution must have content and comprehensive file detection policies, blocking the files as function of their types, protocols and directions.
10. Firewall shall have logging facility as per standard logs/events format. Firewall shall have features to export the generated/stored logs/events in csv (Comma Separated Value) and also any other standard formats for offline usage, analysis and compliance. Firewall shall have suitable memory architecture and solution to store and be able to export all logs/events for a period of last 90 days at any given time.
11. Firewall shall have features and be compatible with local as well as central authentication system (RADIUS, LDAP, or TACACS+) for user account and access right management. It shall also have Role Based User management feature.

12. Firewall shall have the capability to configure sufficient number of VLANs.
13. Firewall shall have the capability to support sufficient number of sessions.
14. Firewall shall have provision to configure multiple IP Sec VPNs, at least 100 nos., (one-to-many or many-to-one). Shall support redundant operation with a similar router after creation of all the IP Sec VPN. IPsec VPN shall be with encryption protocols as AES128, AES256 and hashing algorithms as MD5 and SHA1. IPsec VPN throughput shall be at least 300 Mbps.
15. Firewall shall be capable of SNMP v3 for monitoring from Network Management system. It shall also have SNMPv3 encrypted authentication and access security.
16. Firewall shall operate in Active/Passive or Active-Active mode with High Availability features like load balancing, failover for firewall and IPsec VPN without losing the session connectivity.
17. Firewall should have integrated traffic shaping (bandwidth, allocation, prioritisation, etc.) functionality.
18. Shall support simultaneous operation with both IPv4 and IPv6 traffic.
19. Firewall shall be compatible with SNTP/NTP or any other standards for clock synchronization.
20. Firewall shall have the features of port as well as MAC based security.
21. Firewall shall support exporting of logs to a centralized log management system (e.g. syslog) for security event and information management.
22. Firewall time shall be kept synchronised to official Indian Timekeeping agency, time.nplindia.org.
23. Firewall product shall be provided with all applicable updates at least until 36 months since the applicable date of product shipping to the concerned utility.

**Figure-1**

