1. Hardware Acceleration (NP7Lite + CP10)

It is necessary to have separate high speed hardware chips that provide accelerated network packets and security content processing. It can be equivalent but should be identified and mentioned. Besides the performance throughput numbers must be achieved as minimum.

2. Equivalence Clause

Hardware architecture should be equivalent along side with performance numbers. For example, multi hardware accelerator chips should exist to provide network and content processing.

3. Port Configuration

Minimum number of ports and types should be achieved as per the tender technical specifications considering types and speeds.

4. Security Subscriptions

As long as all the security engines/features are covered: IPS, malware protection, web control, application control, vpn, dns security, mail filtering, video filter; then it is accepted.

5. Performance Values

IPS: throughput measured with ips enabled plus logging

NGFW: throughput measured with ips, app control, plus logging

Threat protection: same as NGFW plus malware scanning

Packet sizes and types (tcp/udp) is considered mixed traffic for the above

IPsec throughput: encryption considered aes256-sha256 with 512byte packet size

Data sheets showing test conditions/environment should be provided to check.

1. Deployment Model for Security Logging: The security logging solution can be deployed on a virtual machine (VM). Cloud deployment is not considered.

2. Log Retention: The expected log volume is approximately 5 GB per day.

3. Firewall Deployment: The two firewalls are intended to be deployed as a High Availability (HA) pair.