Technical Specifications

Perimeter Defence

1. Purpose:

The purpose of this tender is to acquire a network security appliance capable of providing robust perimeter defence and comprehensive security services. The appliance should support failover functionality to ensure continuous and reliable network protection and connectivity.

2. General Requirements:

1. **Network Security Appliance:**
   - The appliance must be capable of deep packet inspection and provide high throughput for network traffic, both encrypted and unencrypted.
   - It should support at least five (5) Gigabit Ethernet interfaces.
   - The appliance must support advanced routing capabilities, including static routing, dynamic routing (such as OSPF and BGP), and policy-based routing.
2. **Failover Capability:**
   - The appliance should include built-in failover features to ensure continuous connectivity in case of hardware failure or link downtime.
   - It must support automatic WAN failover between multiple ISP links.
   - The failover functionality should include link aggregation for load balancing and high availability.
3. **Security Features:**
   - The appliance must support stateful packet inspection and intrusion prevention.
   - It should provide advanced threat protection capabilities, including anti-virus, anti-spyware, anti-malware, and content filtering.
   - The device should include application intelligence and control to manage and monitor network applications.

4. **Virtual Private Network (VPN) Support:**
    - It must support secure remote access through SSL VPN and IPSec VPN for mobile users and branch offices.
    - The appliance should have the capacity to support a minimum of 50 concurrent VPN connections.
5. **Management and Monitoring:**
    - The appliance must include an intuitive web-based management interface for configuration and monitoring.
    - It should support centralized management for multiple devices and real-time analytics and reporting.
    - The device should have logging and alerting capabilities, including the generation of reports on network and security events.
6. **Performance:**
    - The appliance must support a minimum throughput of 1 Gbps for threat prevention services.
    - It should handle a minimum of 100,000 concurrent sessions and 10,000 new connections per second.

3. Security Services:

The appliance should offer a range of security services, including but not limited to:

1. **Gateway Anti-Malware and Anti-Virus Protection:**
    - Real-time scanning and prevention of viruses, malware, and spyware at the network gateway.
    - Cloud-based threat intelligence for proactive identification and blocking of zero-day threats.
2. **Intrusion Prevention System (IPS):**
    - Detection and prevention of network intrusions with automated signature updates.

    - Protection against denial-of-service attacks, exploitation of vulnerabilities, and evasion techniques.

3. **Content Filtering:**
    - Filtering and blocking of undesirable or dangerous web content.
    - Enforced policy-based access control for users and groups.
4. **Application Control and Intelligence:**
    - Identification and management of network applications, including web applications and social media.
    - Granular control over application usage and bandwidth prioritization.
5. **Comprehensive Logging and Reporting:**
    - Detailed logging of security events and network traffic.
    - Regular reports on network health, security incidents, and user activity.

4. Technical Support and Warranty:

- The appliance must come with a minimum of one (1) year warranty and technical support for hardware replacement and software updates.
- Technical support should be available 24x7 via phone and email with a response time of no more than 4 hours for critical issues.

5. Installation and Configuration:

- The supplier must provide installation and initial configuration services for the appliance.
- The installation should include setting up failover, security policies, and VPN connections as per the network requirements.