Load Balancer and Web Application Firewall Solution’s Technical Requirements

L4 – L7 Load Balancing Standard Features

- The solution should support Layer4 and Layer7 Server Load Balancing for TCP and UDP Protocols;
- The solution should support TLS/SSL Offload and Re-encryption support;
- The solution should support Layer 7 Content Switching and Header Modification for HTTPS (Offloaded) and HTTP protocols;
- The solution should support Transparent caching for HTTP/HTTPS protocols;
- The solution should support compression of Static and dynamic HTTP/HTTPS content;
- The solution shall support up to 1000 Virtual Services and up to 1000 Real Servers
- The solution should support NAT-based Forwarding and Direct Server return and Server-NAT (S-NAT) configurations;
- The solution shall support VLAN Trunking (802.1Q);
- The solution shall support Link interface bonding (802.3ad);
- The solution should support IPv6 for addressing and features and have IPv6 to IPv4 bidirectional conversion;
- The solution should support persistence for various methods including: Layer 4 Source IP, TLS (SSL Session ID) Layer 4, HTTP/HTTPS Browser Session (L7), HTTP/HTTPS WebClient-session (L7), RDP Login ID (L7), Port Following for mixed HTTP/HTTPS sessions, Session Reconnection for Microsoft RDS;
- The solution should support the following scheduling and balancing methods for load distribution: Round Robin, Weighted Round Robin, Least Connection, Weighted Least Connection, Agent based Adaptive, Chained failover (Fixed Weighting), Source-IP Hash, Layer 7 Content Switching, Geo Load Balancing, Location Based, Regional, Custom, AD steering, SDN Adaptive.

Health Checking

- The solution should support aggregated health checks;
- The solution should support Layer 3, 4 and 7 health checks for ICMP, TCP, UDP and specific L7 applications for health checking. There should be a capability to specify the URL’s needed to validate application health for HTTP/HTTPS based applications too. Custom health checks for binary checks may also be required;
- The solution should support the ability to specify dependencies relating to the real server pool – ensuring a minimum number of real servers are available to service the requests.
- The solution should support advanced health checks for HTTP 1.1, HTTP Method and Custom Headers and Status Codes. SNI Support is also required for health checking.
- The solution should support configurable intervals for health checking. Please define minimum thresholds.

SSL/TLS Features

- The solution should support SSL (2.0 and 3.0) and TLS 1.0, 1.1 and 1.2. and include support for STARTTLS mail protocols for POP3, SMTP and IMAP.
- The solution should support EV (Extended Validation) Certificates;
- The solution should provide OCSP Configuration, Certificate Validation and Stapling;
- The solution should support Server Name Indication (SNI);
- The solution should support up to 1000 TLS (SSL) Certificates at 2048k key size. There should also be an automated TLS (SSL) Certificate chaining capability;
- The solution should provide Certificate Signing Request (CSR) generation.

Administration

- The solution should support a Context based Web User Interface (WUI), SSH Interface and Console Option. Diagnostics access via shell or equivalent is also required;
- The solution should support a change audit log and have support for syslog and SNMP reporting. There should also be a comprehensive support for logging and reporting to be sent to third party tools for monitoring of the solution;
- The solution should support RESTful and PowerShell API's as well as possessing other capability to be configured by applications such as VMWare vRealize Orchestrator, Puppet, Chef and Ansible for automation;
- The solution should support a Real Time display of performance and availability of services published;
- The solution should support application templates for best practice and simple configuration. These templates should be included as standard and downloadable from the vendor website;
- The solution should support an automated backup option and selective restore for disaster recovery and reinstatement of services;
- The solution should support connection draining to real servers which will enable administrators to remove servers for maintenance with minimal interruption to service;
- The solution should offer a comprehensive application to manage multiple load balancers from a single interface. This application should provide monitoring, visibility and reporting, as well as configuration and backup options for an estate of load balancers. This should be included as part of the overall package and not sold as a separate add-on to the solution;
- The solution should support a proactive monitoring and management service for monitoring and remediation of applications. This service should be included as standard; and should provide an intuitive solution which gives insight into the health of associated services and applications; and provide proactive support for such;

Security

- The solution should support Access Control Lists for Permit/Deny Access Lists for applications. There should also be support for IP Address filtering
- The solution should support IPSec tunneling for VPN to public clouds and on premise data centers;
- The solution should provide DDoS mitigation, including protection against L7 rate-based attacks as standard;

- The solution should support Authenticated NTP configuration;
- The solution should offer Two Factor Authentication support for RSA, LinOTP, Swivel Secure and Okta. There should also be support for X509 client certificates;
- The solution should support Pre-Authentication, Multi-Domain Authentication with SSO and Custom Login Forms with the ability to create and upload bespoke forms. Forms to Forms authentication should also be a feature;
- The solution should support an Intrusion Prevention Service with the ability to use SNORT Compatible rulesets;
- The solution should support Automated IP Reputation updates for Global Server Load Balancing features;

Web Application Firewall Functionality

- The solution should support Web Application Firewall (WAF) Features to provide and include:
    - Real-time application threat mitigation for cookie tampering;
    - Cross-Site Request Forgery;
    - Cross-Site Scripting;
    - Data Loss Prevention;
    - SQL Injection and others to help satisfy a PCI-DSS 6.6 compliance posture;
    - A daily rule update service is expected to be part of the solution.

Geo Server Load Balancing

- The solution should support Web Application Firewall (WAF) Features to provide and include real-time application threat mitigation for cookie tampering, Cross-Site Request Forgery, Cross-Site Scripting, Data Loss Prevention, SQL Injection and others to help satisfy a PCI-DSS 6.6 compliance posture. A daily rule update service is expected to be part of the solution;
- The solution should provide the capability to configure local subnets to be defined as custom locations, with specified geographical co-ordinates. These custom locations should be able to be allocated to these to specific or custom locations for enhanced load distribution options;
- The solution should support configurable health checks to provide monitoring of services and applications. This is required to ensure seamless failover between sites and services in the event of site or application failure.

Kubernetes Infrastructure

- Automated mapping of Kubernetes service object configuration to Load Balancer;
- Support for reading Kubernetes annotations to ingest metadata information about objects;
- Capabilities for communication with a Kubernetes API server;
- Solution should route traffic directly to the Kubernetes Pods and allows microservices to be managed alongside traditional monolithic applications while utilizing advanced enterprise services, such as Web Application Firewall, Access Management, and L7 Service traffic management;

- Solution should be able to act as Ingress Controller for Kubernetes infrastructure;

Product Requirements

- The solution required needs to be based upon a specific platform: VMware vSphere;
- The solution should support up to 4,000 SSL TPS (Transactions per second, with support for up to 1000 Virtual Services and 1000 Real Servers. The solution should be a available Virtual offering capable of delivering upto 3 Gb/Sec of Throughput, L4 connections per second of 3,000,000;

Product Support Requirements

- Customer support should be made available in various methods – such as telephone, online and via email. Support should be depicted in the subscription tiers.
- The customer may be required to provide remote access to the solution to assist with any troubleshooting. It is expected that the vendor will engage with the customer and provide a suitable mechanism to aid troubleshooting – such as webex type tools or other remote control functionality;
- Product support duration should be 3 year;