

Technical Specifications

Lot: 1

Item #	QTY	Details
1	1	Clustering Firewall

#	Item / Minimum Requirement	Qty	Technical Compliance including manufacturer part number
1	<p>Clustering Firewall</p> <p>General Features:</p> <ul style="list-style-type: none"> • Shall be based on proven security (AV, IPS, DNS, web/content filtering) built around business intent (users, devices and applications) natively integrated • Automated threat intelligence in minutes • Shall support centralized cloud-management • The appliance architecture shall have dedicated CPU for security processing apart from the main central processing units (CPUs). • The appliance shall identify thousands of applications inside network traffic for deep inspection and granular policy enforcement • The appliance shall protect against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic • The appliance shall prevent and detect against known and unknown attacks using continuous threat intelligence backed by dedicated global security services • Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location • The appliance shall support automatically blocking threats on decrypted traffic using the Industry's standard SSL inspection • The appliance shall support blocking and controlling web access based on user or user groups across URL's and domains • The appliance shall support Block DNS requests against malicious domains 	1	

<ul style="list-style-type: none">• The appliance shall support Multi-layered advanced protection against zero-day malware threats delivered over the web• The appliance shall support consistent business application performance with accurate detection, dynamic WAN path steering on any best-performing WAN transport• Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility• The appliance shall support extended security fabric integrating security and management across network switches, wireless access points and end point security• The security appliance should shall provide converged networking and security into a secure, simple to manage architecture with a single focal point for management and configuration for LAN devices such as Network Switches and Wireless Access Points.• The security appliance shall be fully compatible for management with existing centralized security management platform• The security appliance shall be fully compatible with existing firewall for high availability configuration <p>System Performance:</p> <ul style="list-style-type: none">• Firewall throughput: 25 Gbps• IPS throughput: 5 Gbps• NGFW throughput: 3.5 Gbps• Threat Protection throughput: 3 Gbps• Concurrent Sessions: 3 Million• SSL Inspection Throughput: 4 Gbps• Supported High availability Configuration: Active-Passive, Active-Active, Cluster <p>Ports:</p> <ul style="list-style-type: none">• 16 x Gigabit Ethernet RJ45• 08 x Gigabit Ethernet SFP Port• 04 x 10 Gigabit Ethernet SFP+• Dedicated management and console ports <p>Compliance and Certification</p>		
--	--	--

<ul style="list-style-type: none"> • Independently tested and validated best security effectiveness and performance • Should have received third-party certifications from NSS Labs • Should be and enterprise grade firewall from a manufacturer listed as Leader in the 2020 or 2021 Gartner Magic Quadrant for Network Firewalls • Should submit relevant Gartner’s magic quadrant report. <p>Required Security and Service Subscriptions</p> <ul style="list-style-type: none"> • 1 Year Security Subscription - Web Filtering, Malware Protection, IPS, Antispam, Antivirus, Botnet, Virus Outbreak Protection, Application Control, Sandbox • 1-Year Support Subscription: 24x7 Support, Hardware Replacement, Firmware Upgrades • 1-Year Technical Support: Local technical support <p>2 Installation and Configuration</p> <ul style="list-style-type: none"> • Hardware installation • Shall design appropriate LAN, WAN, and DMZ security policies. • Shall configure application control policies • Shall configure AV and Web filtering policies • Shall configure antispam filtering • Shall configure IPS policies • Shall configure traffic shaping and ISP WAN load balancing • Shall configure network segmentation and configure appropriate security policy per segment • Shall Configure remote access connectivity policies • Shall Configure management • Shall Configure centralized log analytics and standard security reporting • Shall provide on the job training on basic management, operation and maintenance. • Shall do comprehensive testing and a detailed documentation on the configuration and settings of the delivered solution should be provided. 	<p>1</p>	
---	-----------------	--

