5197-0500

BOUNDARY EOL REPLACEMENT (MATERIAL ORDERING REQUEST #488)

1. CMDNet Boundary - 2x NG-1402 (13 copper 10/100/1000 (4x integrated & 8x expansion module), additional 4x SFP+)
    a. 40Gb throughput with minimum of 4.5GB throughput with full packet inspection.
    b. These will be used to replace the existing [redacted] that are currently providing for the boundary defenses. The existing devices have 9 copper 10/100/1000 interfaces, all of which are used or accounted for. These new devices need to allow for the current interfaces plus an additional 3x copper and 4x SFP+ interfaces. The planned port distribution and utilization is as follows:
        i. 1x Copper, trunked
            1. 2x Zones
        ii. 1x Copper, Trunked
            1. 2x Zones
        iii. 1x Copper, Trunked
            1. 5x Zones
        iv. 1x Copper, Trunked
            1. 2x Zones
        v. 1x Copper
            1. 1x Zone
        vi. 1x Copper
            1. 1x Zone
        vii. 1x Copper
            1. 1x Zone – heartbeat
        viii. 1x Copper
            1. 1x Zone
        ix. 1x Copper
            1. 1x Zone
        x. 1x Copper
            1. 1x Zone
        xi. 1x Copper
            1. 2x Zones
        xii. 1x Copper
            1. 3x Zones
2. Yoko Internal Boundary - 2x NG-1402 (4 copper 10/100/1000 (4x integrated & 4 or 8x expansion module))
    a. 40Gb throughput with minimum of 4.5GB throughput with full packet inspection.
    b. These devices will be a new addition to Yoko to support the separation of traffic and allow for configuration of zone to support internal and external traffic. The planned port distribution and utilization is as follows:
        i. 1x Copper
            1. 1x Zone

Attachment #2

ii. 1x Copper
    1. 1x Zone
iii. 1x Copper
    1. 1x Zone – heartbeat
iv. 1x Copper
    1. 3-4x Zones
v. 4x Copper Additional Interfaces
    1. Multi-zones as needed for final design.

3. Internal/PIT- 2x NG-1402 (4 copper 10/100/1000 (4x integrated))
    a. 40Gb throughput with minimum of 4.5GB throughput with full packet inspection.
    b. These devices where originally planned to support the separation of traffic and allow for configuration of zone to support internal and external traffic. The planned port distribution and utilization is as follows. The planned port distribution and utilization is as follows:
        i. 1x Copper
            1. Zone
        ii. 1x Copper
            1. Zone
        iii. 1x Copper
            1. Zone – heartbeat
                a. IP's TBD
        iv. 1x Copper
            1. Zone
        v. 4x Copper Additional Interfaces
            1. Multi-zones as needed for final design.

System Level Requirements

1. The next generation firewall must support application identification and options for intrusion detection scanning (IDS), intrusion prevention scanning (IPS), and URL filtering all on a single platform with a single browser based GUI for configuration management.

2. The firewall must be manageable via a central management console. The firewall and management console must support a local configuration (for on-site operators) and central configuration (for operators at a centralized headquarters) simultaneously.

3. The next generation firewall management interface must also support multiple roles for different types of operators. As an example a role for network operations, a role for security policy, and a role for IA auditing.

4. Hardware based firewalls must separate the management plane from the data forwarding plane. Management plane must have its own dedicated CPU, memory, and storage for managing the device and generating reports. The dataplane must have its own dedicated CPUs and memory for inspecting traffic and forwarding packets.

5. The firewall must classify all applications on all ports all the time. All traffic must be classified regardless of IP port, encryption (SSL or SSH), or evasive techniques employed. Unidentified applications – typically a small percentage of traffic, yet high in potential risk – must be automatically categorized for systematic management. The firewall must use applications and users as the basis of security policy – all access control decisions will be based on that information.

6. The Firewall OS must have a protection profile by the NIAP Evaluation and Validation Program. Protection Profiles must be listed at the NIAP website or documentation provided to verify there is a protection profile in place for the firewall being used on the network that has been evaluated at one of the accredited NIAP locations.

7. Must support SNMP ver. 3 Security Model with FIPS 140-2 validated cryptography for any SNMP agent configured on the device.

8. The network device must drop half-open TCP connections through filtering thresholds or timeout periods.

9. Device must support the use of authentication, authorization and accounting servers for access to the device for management i.e. RADIUS/TACACS+

10. Must support administrative access using SSH version 2

11. Alerts automatically generated to notify administrator when log storage reaches seventy-five percent or more of its maximum capacity.

12. Device will be able to disable or uninstall unused services.

13. Granular IPv6 control.

14. Administration through non graphical means i.e. Command Line Interface (CLI) is a requirement.

15. Call home service or feature disable ability.

16. Independent Signature Server capability.

17. Traffic prioritization and bandwidth reservation.

18. Granular ICMP control.

19. Full support of VMWare NSX. To support interoperability and reduce operational cost, vendor product line should also have a virtual server software platform meeting the same requirements, with the exception of throughput and physical connections. Supported platforms must include ESXi. The firewall and management console must support integration with software defined network (SDN) orchestrations systems. - Vmware NSX and OpenStack must be supported at a minimum.

20. The selected firewall should have predefined applications written to work with the corporate log review solution SPLUNK.

21. The device hardware and software must not have a projected End-of-Support date closer than 60 months from delivery date.

22. Must be configurable as a High Availability pair in an "Active-Standby" configuration.

User ID/Authorization Requirements

23. The firewall must have the ability to map IP addresses to users and support security policy definition based upon users and groups

24. The firewall must be able to map users to IP addresses with both a software agent or directly from the firewall.

25. The firewall must be able to map users to IP addresses by Captive Portal, Active Directory/LDAP, Microsoft Exchange and Syslog information stores.

26. Firewall must be able to support DoD CAC authentication for account access for each role.

27. Must support a minimum of 8 each, 10 GB (line rate) connections in a single chassis.

Content Inspection Requirements

28. All firewalls must perform L7 application identification at 90%+ of firewall rated performance under documented real-world (i.e. not UDP-only) traffic loads. The firewall must deny unknown traffic.

29. Firewall documentation must detail how the operator can create custom application signatures without having to load new software or databases

30. Verifiable throughput of mixed traffic type with all Firewall features turned on of a minimum of 60GB in a single chassis.

31. The firewall must perform threat inspection of known signatures at 50% of the firewall's rated throughput, while simultaneously maintaining 90%+ L7 performance

32. The firewall must be able to select files for forwarding, with negligible (<1%) performance impact), to a local appliance for unknown malware detection. It must also accept local signature insertion from that appliance into its threat database with turnaround time within 15 minutes.

33. The firewall must support URL filtering capability which adds a categorical URL database functionality to the device for use as a URL and Web Content filter. URL categories must be able to be used to define security policy, complementing the application level control as well as to define SSL decryption exceptions, to determine quality-of-service policy and more.

Management Requirements

34. The firewall must have on-box reporting and logging; additionally both global and local rules should be enabled for central and remote operators from the same UI with role-based privileges. Last, the firewall must continue to log all events during configuration, operational, and service maintenance windows

35. The management system must be able to set bandwidth-shaping policies based on user, time-of-day, and application--or a combination of any of these variables

36. Firewall must be configurable via a REST API or equivalent.

37. Reports on the firewall must be available via REST API or equivalent

38. The firewall must be able to identify unused rules.

39. Operators must have the ability to intermix port/protocol rules with app-based rules.

40. Dashboard traffic reports. System must have both standardized and customizable reports.

41. Must be able to display DoD approved warning banner prior to system administrator logging in.

42. Device must log administrator logons, changes to administrator group and account lockouts.

43. The device console port must be able to time out after 10 minutes or less.

44. Management connections to the device must be established using secure protocols with FIPS 140-2 validated cryptographic modules.

45. Management connections for administrative access must be configurable to time out after 10 minutes or less of inactivity.

46. Device must be configurable to timeout after 60 seconds or less for incomplete or broken SSH sessions.

47. Device must be configurable to reset interface after 3 unsuccessful SSH login attempts.

48. Must not allow SSH ver. 1 for administrative access.

49. Must support 802.1Q tags.

50. Must be configurable for NTP authentication.

51. Auxiliary port must be able to be disabled.

52. Admin configurable End-User notification for policy violations or filtering events.

Preferred options, but not required

53. The firewall must be able to selectively identify which SSL traffic is decrypted to address privacy concerns. (ex. not decrypt PII or HIPPA data)
    a. PII and HIPPA data must be protected at significantly higher standard than most of our other traffic. We need a way to ensure that this traffic is not decrypted when it is moving from the system to system, i.e. web client sending traffic to database.
54. The firewall must be capable of providing SSL/TLS decryption to allow inspection of SSL/TLS encrypted traffic. The firewall must also be capable of providing a copy of the unencrypted traffic to other security devices for inspection.

a. In order to provide content inspection analysis of all packets even those being transmitted via SSL/TLS must be reviewed. Not performing packet analysis of this traffic allows for attack over those protocols.

55. The firewall and unknown malware detection appliance combination must be able to analyze JAR, SWF, APK, EXE, PDF, DLL and standard office document files for zero-day threats

a. This is a defense-n-depth request. The ability to block the propagation of these files types from system to system over production would allow for the increased control and limitation of malware.