



**MCWA Firewall Refresh & Installation RFP/Q
Questions and Answers
2/15/2023**

For the Business Network Firewall (RFP/Q Section 2.2.2A)

1. As you noted the "Network modules 8 x 1/10/25G, 4 x 40G Options" are options now which one you want to do?

Answer: Please provide separate line item pricing for 8 x 1/10/25 modules and 4 x40G.

2. The firewall will support site to site VPN out of the box but for a Client to site VPN (25 users) you'll need an anyconnect for it. If you want to do it, then we need to know if you need anyconnect VPN only, anyconnect plus or anyconnect apex license?

Answer: AnyConnect plus or equivalent licensing for 25 users for both firewalls; one for each business internet egress.

3. How many years do they want to subscription?

Answer: One year.

4. The firewall itself cannot be integrated with SIEM but it can with the help of Firepower management center. If you want to do it then how many firewalls are you trying to manage and what are those specific firewalls? Are you trying to deploy it through VMware or KVM?

Answer: All three firewalls noted in section 2.2.2 need to be managed. VMware for deployment is preferred.

5. The firewall was just released so there's no end of life announcement yet for it, meaning it's still going to be supported in the next 5yrs.

Answer: N/A

6. You need to add Advanced Malware Protection (AMP) they want to have "Provide protection from zero day attacks and unknown threats"

Answer: *Yes or like product – Need to accept free and paid Security Feeds.*

For the Industrial Control Network (RFP/Q Section 2.2.2B)

7. As you noted "Network modules 8 x 1/10G" is an optional item, do you want to add it?

Answer: *Yes. Please provide pricing on 8 x 1/10/25 modules as line item options.*

8. The firewall itself cannot be integrated with SIEM but it can with the help of Firepower management center If you want to do it then how many firewalls are you trying to manage and what are those specific firewalls?

Answer: *Three.*

9. Are you trying to deploy it through VMware or KVM?

Answer: *VMware.*

10. The firewall was just release so there's no end of life announcement yet for it, meaning it's still going to be supported in the next 5yrs.

Answer: *N/A.*

11. You need to add Advanced Malware Protection (AMP) they want to have "Provide protection from zero day attacks and unknown threats"

Answer: *Yes or like product – Need to accept free and paid Security Feeds.*

Miscellaneous Questions

1. Are the current firewalls running ASA or Firepower Threat Defense code? Can you please confirm the software version?

Answer: *ASA with Firepower.*

2. Are the current firewalls configured with any advanced firewalling capabilities (IPS, URL filtering, anti-malware) or just stateful packet inspection?

Answer: *Yes, all advanced firewalling capabilities.*

3. How are these firewalls currently being centrally managed?

Answer: *Through the product / software toolset provided by the current manufacturer.*

4. Would you require any on-going management and support of the firewall solution? If so, would a physical or virtual server solution be preferred?

Answer: *Optional pricing for these services is allowed. Virtual server preferred.*

5. Can you please confirm the SIEM in place?

Answer: *There is a SIEM in place but cannot confirm manufacturer / product due to security concerns.*

6. Is SIEM integration required?

Answer: *Yes*

7. Can you please provide any current or desired integrations with additional security tools besides SIEM?

Answer: *Integration with Protective DNS in the cloud desired.*

8. How many access control lists are currently deployed on each set of firewalls?

Answer: *Approximately 20 on each of the two Firewalls– Needs 3rd party review and recommendation.*

9. The RFP states the solution will require IPS capabilities. Are there any additional advanced firewalling capabilities required? (URL filtering, anti-malware, etc.)

Answer: *Yes IPS, IDS, AMP or like product. (inter segmentation control - Need to bring multiple segment to FW so control lateral traffic (east-west) in addition to north south. Initial configuration needed with rules/control to be added over time per corporate direction. Ability to ingest security feeds as well.*

10. Is BGP currently configured in the environment for requested failover?

Answer: *No.*

11. Can you please confirm all current carrier information? (vendor, speeds, etc.)

Answer: *ISP1 1G, IPS 2 1G, but looking for increased bandwidth in the future. Business Firewalls should be capable of higher speeds, as noted in the requirements of the RFP.*

12. Do you currently own BGP AS numbers and IP address space? Any detail would be helpful.

Answer: *No*

13. How many site-to-site VPN tunnels are in place today? Any additional tunnels planned for new solution?

Answer: Five IPsec PTP, with approximately 5 to 10 client based at one time. Also one IPsec tunnel with a cloud provider for setup. Need BGP implemented for redundancy on all of these connections.

14. Is remote VPN currently configured today? Anyconnect clients can connect to each egress

Answer: Yes.

15. Is there any additional SFP modules or cabling required?

Answer: Please provide line item pricing. Optional pricing is encouraged for all available modules / cables that are needed.

16. Can you confirm the connectivity between data centers? (Layer 2 or Layer 3, bandwidth, where the connections terminate etc.)

Answer: Both Layer 2 and 3 with fiber links that terminate in each Data Center.

17. Is any high availability in place today between data centers? If so, is that regularly tested?

Answer: Some, but looking for best option available between the two Data Centers with the new Firewalls. BGP implementation as required by the RFP for ISP redundancy as well.

18. Would you like to see optional pricing on multiyear support warranties and feature licenses?

Answer: Yes.

19. Do you have any specific security regulatory compliance requirements we should adhere to? (DFARS, GDPR, HIPAA, PCI-DSS etc)

Answer: N/A.

20. Is local support and implementation preferred?

Answer: Preferred but not required. Remote access can be set up as you will be working closely with a few of our team members on install/config and training where applicable. We need to know how the set up was configured and implemented so we can maintain it in the long run, including documentation.