



Document Title:
DA High Availability Firewall

Document Type: **Specification** Engineering Type: **Equipment Specificati** Document No.: **4350.337**

Department: **Distribution** Version: **01** Effective Date: **03-18-24**

Shared document with: N/A

*Select the Departments impacted by the document

For others, specify here

Author

Jose R. Torres
Engineer, Distribution Standards & Materials

Signature and Date

Mar 18, 2024

Reviewer

Rodolfo A. Flores Ortiz, PE
General Engineer, Distribution Standards & Materials

Signature and Date

Mar 18, 2024

Approver

Ricardo Castro Gómez, PE
Manager, Distribution Standards & Materials

Signature and Date

Mar 18, 2024

Management Approval (If apply)

Approver

Name
Position

Signature and Date

N/A

Related/Referenced Documents

N/A

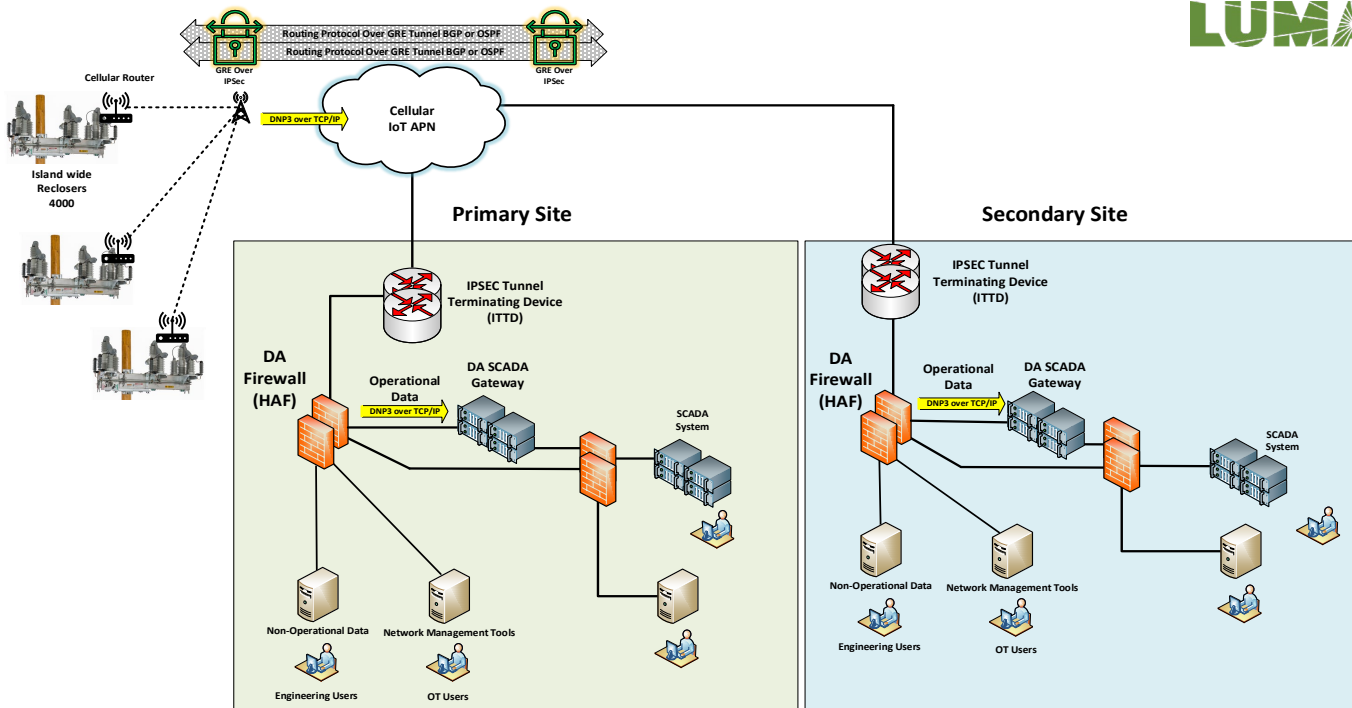
Version History

Version	Date	Revision
01	01/24/2024	Initial release



Item Version History

Warehouse Catalog #	Asset Suite	Version	Date
032-85861	85861	01	3/15/2024
032-85862	85862	01	3/15/2024
032-85863	85863	01	3/15/2024



1. Introduction

This specification is for redundant high availability firewalls (HAF) that will be installed in diverse LUMA OT sites as depicted in figure 1. The HAF will provide a secure, reliable, and resilient gateway between the LUMA OT environment and Distribution Automation (DA) IOT devices. The IOT devices include reclosers, fault sensors and other future IOT devices. The DA IOT devices communicate via cellular networks to the OT environment. Each DA IOT device will be configured with two IPSEC tunnels to provide operational and non-operational data. Operational data is used by the LUMA SCADA to securely control the IOT devices. Non-Operational data is used for fleet management and maintenance of the IOT devices. The data usage for the IOT devices can be as much as 1GB per device per month.

LUMA expects to connect 20,000 IOT devices to the LUMA OT environment.

2. Special Requirements

Samples shall be furnished requested by LUMA Energy. The equipment/material will be received at the LUMA’s general warehouse (011) at Palo Seco, Puerto Rico. Shipping will include transportation and unloading at the indicated warehouse.

Figure 1

3. Literature

Descriptive and technical literature must be supplied by the vendor at time of bidding. This literature may include, but is not limited to details of material, drawings, documented testing, and instructions for use and installation. Failure to submit documents on time will cause bidder disqualification.

4. Markings

- 4.1. Containers shall be marked outside with LUMA Energy's purchase order, item number, name and size, net and gross weight, manufacturer's name, and lot number.
- 4.2. Packaging labels and tags shall be waterproof.

5. Packaging

All equipment/material shall be packaged and marked in such a way as to facilitate handling and protection from damage and that the receiving warehouse can readily identify it and send it, in one complete unit, to a field location without opening crates or boxes to sort items and/or parts.

6. Number Per Package (Logistics)

Supplier shall indicate the logistics at opening bid or as required by LUMA Energy.

7. Acceptance Criteria

- 7.1. Certified by external laboratories.
- 7.2. Latest applicable codes, standards, and other regulations.
 - a. Safety: UL 60950-1
 - a. EMC
 1. Emissions: 47CFR Part 15 (CFR 47) Class A (FCC Class A)
 2. Immunity: EN55024
- 7.3. Compliance to technical specification requirements
- 7.4. Compliance with relevant industry standards and regulations for OT cybersecurity

8. Technical Specification

- 8.1. The high availability firewalls Requirement and a hardware component.
- 8.2. Firewall Requirements
 - a. Minimum Security Features
 1. Firewall
 2. VPN (IPsec)
 3. Identity Awareness

4. Application Control
 5. Content Awareness
 6. IPS
 7. URL Filtering
 8. Anti-Bot
 9. Anti-Virus
 10. Anti-Spam
 11. DNS Security
 12. High Availability
- b. Minimum Requirement Functions and Performance
1. Throughput:
 - a. Firewall: 9Gbps
 - b. NGFW: 3Gbps
 - c. VPN-(AES-128): 2Gbps
 - d. TLS: 760 Mbps
 - e. IPS (1024B): 5Gbps
 - f. IPsec VPN: 2 Gbps
 2. IPsec VPN: 2 Gbps
 3. Connections /sec: 65,000
 4. Concurrent connections: 1 million
 5. Maximum VPN Peers: 10,000
 6. Local device management
 7. Centralized device management
 8. Application Support: 3,800 applications
 9. Open-Source Application Detectors AVC
 10. Number of URL Filtering custom categories: more than 70
 11. High Availability:
 - a. Active/Standby, Active/Active L
 - b. Ensure the firewall remains operational even in case of hardware or software failures.

- c. Provide failover mechanisms to maintain network connectivity and prevent disruptions to OT operations.
12. VPN Load Balancing
13. Policies / Rules:
- a. Security Rules
 - b. Security Rule Schedules
 - c. NAT Rules
 - d. Decryption Rules
 - e. App Override Rules
 - f. Tunnel Content inspection rules
 - g. SD-WAN rules
 - h. Policy based forwarding rules.
 - i. Captive Portal Rules
 - j. DoS protection Rules
14. Security profiles: 100
15. App-ID:
- a. Custom Signatures
 - b. Shared custom App-IDs
16. User ID:
- a. IP User Mappings
 - b. Active groups
 - c. User-ID agents
 - d. Terminal server agents
 - e. Tags per user
17. SSL Decryption:
- a. SSL inbound certificates
 - b. SSL certificate cache
 - c. 100,000 Concurred decryption sessions
 - d. SSL Port Mirror
18. Virtual Routers
19. Routing:

- a. IPv4, IPv6
 - b. Static and Multicast Routes
 - c. Policy Based Routing
20. L2 Forwarding: ARP, IPv6, MAC`
21. NAT Rule Capacity: 3,000
22. Address Assignments:
- a. 3 DHCP Servers
 - b. 50,000 assigned addresses
23. QoS Policies: 800
24. User Based Policy: Microsoft AD, LDAP, RADIUS, Cisco pxGrid.
25. Deep Packet Inspection:
- a. Analyze data packets beyond headers, identifying specific protocols and applications used in OT environments.
 - b. Detect anomalous traffic patterns and malicious payloads targeted at OT devices.
26. Stateful Inspections:
- a. Track the state of network connections, allowing only authorized traffic to flow through.
 - b. Prevent unauthorized access and potential manipulation of OT devices.
27. Application Control:
- a. Whitelist specific applications and protocols allowed to communicate between the OT and IT networks.
 - b. Block unauthorized applications and prevent the spread of malware within the OT environment.
28. Zone-Based Security:
- a. Divide the network into different security zones based on trust levels and function.
 - b. Restrict communication between zones to authorized traffic flows, minimizing the attack surface.
29. Intrusion Detection and Prevention (IDS/IPS):
- a. Monitor network traffic for known attack signatures and suspicious activity.
 - b. Detect and automatically block intrusion attempts, minimizing potential damage to OT operations.

30. Vulnerability Management

- a. Scan OT devices and systems for known vulnerabilities that can be exploited by attackers.
- b. Prioritize and patch vulnerabilities to mitigate risks and prevent successful attacks.

31. Device Authentication and Authorization

- a. Implement strong authentication protocols for OT devices to prevent unauthorized access.
- b. Provide granular access control based on user roles and responsibilities.

32. Secure Logging and Auditing

- a. Log all network activity and security events for forensic analysis and incident response.
- b. Provide audit trails to identify potential security breaches and improve defenses.

33. OT-Specific Protocols Support

- a. Support deep packet inspection and filtering capabilities for commonly used OT protocols like Modbus, DNP3, and IEC 61850.
- b. Provide visibility and control over OT network traffic without impacting system performance.

34. Integration with SIEM

- a. Security Information and Event Management systems for centralized monitoring and threat detection.

35. Support for secure remote access solutions for maintenance and troubleshooting.

8.3. Hardware Characteristics:

- a. Form Factor: 1 Rack Unit
- b. Integrated I/O:
 1. 8 x 10M/100M/
 2. 1 GBASE-T Ethernet interfaces (RJ- 45), 4 x 10 Gigabit (SFP+) Ethernet interfaces
- c. Network Modules: 10G SFP+, 1/10G FTW
- d. Maximum number of interfaces: Up to 24 total Ethernet ports (12x1G RJ-45, 4x10G SFP+, and network module
- e. Storage: 1x 200 GB, 1x spare slot (for MSP)
- f. AC Power Supply: 2



- g. DC Power Supply: 1
- h. AC Voltage: 110 V AC
- i. DC Voltage: 48 V DC
- j. Power Supply Redundancy: AC/DC
- k. Hot Swappable Fans
- l. Operating Humidity: 10 to 85% Noncondensing

8.4. Conformance and Compliance Standards

- a. Safety: UL 60950-1
- b. EMC
 - 1. Emissions: 47CFR Part 15 (CFR 47) Class A (FCC Class A)
 - 2. Immunity: EN55024

9. Licensing and Subscriptions

- a. Vendor will provide detail what firewall feature need to be license.
- b. Vendor will provide firewall subscription bundle detail and subscription pricing validity.

10. Inspection

The acceptance of any material or equipment/material shall in no way relieve the vendor from his responsibility to meet all the requirements of this specification, and it would not prevent subsequent rejection if such equipment/materials were found later to be defective.

11. Proposal Information

11.1. Submitted proposals must include:

- a. Technical information
- b. Tables of Compliance completed by the bidder with reference (see Appendix)

Warehouse Number	Asset Suite	Item Type
032-85861	85861	DA Firewall device
032-85862	85862	DA Firewall management software
032-85863	85863	DA Firewall subscription





Appendix



Table of Compliance

Line	Criteria	Description	Pass/Fail (P / F)	Comments	
1	Acceptance Criteria	Certified by external laboratories.			
2		Latest applicable codes, standards, and other regulations.			
3					
4		a. Safety: UL 60950-1			
5		a. EMC			
6		1. Emissions: 47CFR Part 15 (CFR 47) Class A (FCC Class A) 2. Immunity: EN55024			
7		Compliance to technical specification requirements			
8		Compliance with relevant industry standards and regulations for OT cybersecurity			
9	Technical Specification	high availability firewalls Requirement and a hardware component			
10		a. Minimum Security Features			
11			1. Firewall		
12			2. VPN (IPsec)		
13			3. Identity Awareness		
14			4. Application Control		
15			5. Content Awareness		
16			6. IPS		
17			7. URL Filtering		
18			8. Anti-Bot		
19			9. Anti-Virus		
20			10. Anti-Spam		
21			11. DNS Security		
22		12. High Availability			
23		b. Minimum Requirement Functions and Performance			
24			1. Throughput:		
25			a. Firewall: 9Gbps		
26			b. NGFW: 3Gbps		
27			c. VPN-(AES-128): 2Gbps		
28			d. TLS: 760 Mbps		
29			e. IPS (1024B): 5Gbps		
30			f. IPSec VPN: 2 Gbps		
31			IPsec VPN: 2 Gbps		
32			Connections /sec: 65,000		
	Concurrent connections: 1 million				



33	Maximum VPN Peers: 10,000		
34	Local device management		
35	Centralized device management		
36	Application Support: 3,800 applications		
37	Open-Source Application Detectors AVC		
38	Number of URL Filtering custom categories: more than 70		
39	11. High Availability:		
40	a. Active/Standby, Active/Active L		
41	b. Ensure the firewall remains operational even in case of hardware or software failures.		
42	c. Provide failover mechanisms to maintain network connectivity and prevent disruptions to OT operations.		
43	VPN Load Balancing		
44			
45	Policies / Rules:		
46	a. Security Rules		
47	b. Security Rule Schedules		
48	c. NAT Rules		
49	d. Decryption Rules		
50	e. App Override Rules		
51	f. Tunnel Content inspection rules		
52	g. SD-WAN rules		
53	h. Policy based forwarding rules.		
54	i. Captive Portal Rules		
55	j. DoS protection Rules		
56	Security profiles: 100		
57	App-ID:		
58	a. Custom Signatures		
59	b. Shared custom App-IDs		
60	User ID:		
61	a. IP User Mappings		
62	b. Active groups		
63	c. User-ID agents		
64	d. Terminal server agents		
65	e. Tags per user		
66	Decryption:		
67	a. SSL inbound certificates		
68	b. SSL certificate cache		
69	c. 100,000 Concurred decryption sessions		
70	d. SSL Port Mirror		
71	Virtual Routers		



72	Routing:		
73	a. IPv4, IPv6		
74	b. Static and Multicast Routes		
	c. Policy Based Routing		
75	L2 Forwarding: ARP, IPv6, MAC`		
76	NAT Rule Capacity: 3,000		
77	Address Assignments:		
78	a. 3 DHCP Servers		
79	b. 50,000 assigned addresses		
80	QoS Policies: 800		
81	User Based Policy: Microsoft AD, LDAP, RADIUS, Cisco pxGrid.		
82	Deep Packet Inspection:		
83	a. Analyze data packets beyond headers,		
84	identifying specific protocols and applications		
85	used in OT environments.		
86	b. Detect anomalous traffic patterns and		
87	malicious payloads targeted at OT devices.		
88	Stateful Inspections:		
89	a. Track the state of network connections,		
	allowing only authorized traffic to flow through.		
90	b. Prevent unauthorized access and potential		
	manipulation of OT devices.		
91	Application Control:		
92	a. Whitelist specific applications and protocols		
	allowed to communicate between the OT and IT		
	networks.		
93	b. Block unauthorized applications and prevent		
	the spread of malware within the OT		
	environment.		
94	Zone-Based Security:		
95	a. Divide the network into different security		
	zones based on trust levels and function.		
96	b. Restrict communication between zones to		
	authorized traffic flows, minimizing the attack		
	surface.		
97	Intrusion Detection and Prevention (IDS/IPS):		
98	a. Monitor network traffic for known attack		
	signatures and suspicious activity.		
99	b. Detect and automatically block intrusion		
	attempts, minimizing potential damage to OT		
	operations.		
100	Vulnerability Management		
101	a. Scan OT devices and systems for known		
	vulnerabilities that can be exploited by		



102		attackers. b. Prioritize and patch vulnerabilities to mitigate risks and prevent successful attacks.		
103		Device Authentication and Authorization a. Implement strong authentication protocols for OT devices to prevent unauthorized access. b. Provide granular access control based on user roles and responsibilities.		
104				
105				
106		Secure Logging and Auditing a. Log all network activity and security events for forensic analysis and incident response. b. Provide audit trails to identify potential security breaches and improve defenses.		
107				
108				
109		OT-Specific Protocols Support a. Support deep packet inspection and filtering capabilities for commonly used OT protocols like Modbus, DNP3, and IEC 61850. b. Provide visibility and control over OT network traffic without impacting system performance.		
110				
111				
112		Integration with SIEM a. Security Information and Event Management systems for centralized monitoring and threat detection.		
113				
114		Support for secure remote access solutions for maintenance and troubleshooting.		
115	Hardware Characteristics	Form Factor: 1 Rack Unit		
116		Integrated I/O: 1. 8 x 10M/100M/ 2. 1 GBASE-T Ethernet interfaces (RJ- 45), 4 x 10 Gigabit (SFP+) Ethernet interfaces		
117				
118				
119		Network Modules: 10G SFP+, 1/10G FTW		
120		Maximum number of interfaces: Up to 24 total Ethernet ports (12x1G RJ-45, 4x10G SFP+, and network module		
121		Storage: 1x 200 GB, 1x spare slot (for MSP)		
122		AC Power Supply: 2		
123		DC Power Supply: 1		
124		AC Voltage: 110 V AC		
125		DC Voltage: 48 V DC		
126		Power Supply Redundancy: AC/DC		
127		Hot Swappable Fans		
128	Operating Humidity: 10 to 85% Noncondensing			



129	Licensing and Subscriptions	Vendor will provide detail what firewall feature need to be license.		
130		Vendor will provide firewall subscription bundle detail and subscription pricing validity.		











4350.337 DA Firewall Specification 3-13-24

Final Audit Report

2024-03-18

Created:	2024-03-18
By:	jose torres (JoseR.Torreslrizarr@Lumapr.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA7rHBU9oXxbY6-tkBCvy0T9cO1si_pdq_

"4350.337 DA Firewall Specification 3-13-24" History

-  Document created by jose torres (JoseR.Torreslrizarr@Lumapr.com)
2024-03-18 - 12:51:16 PM GMT
-  Document emailed to jose torres (JoseR.Torreslrizarr@Lumapr.com) for signature
2024-03-18 - 12:51:41 PM GMT
-  Document e-signed by jose torres (JoseR.Torreslrizarr@Lumapr.com)
E-signature obtained using URL retrieved through the Adobe Acrobat Sign API
Signature Date: 2024-03-18 - 12:52:33 PM GMT - Time Source: server
-  Document emailed to Rodolfo Flores (rodolfo.floresortiz@lumapr.com) for signature
2024-03-18 - 12:52:35 PM GMT
-  Email viewed by Rodolfo Flores (rodolfo.floresortiz@lumapr.com)
2024-03-18 - 1:42:54 PM GMT
-  Document e-signed by Rodolfo Flores (rodolfo.floresortiz@lumapr.com)
Signature Date: 2024-03-18 - 1:43:49 PM GMT - Time Source: server
-  Document emailed to Ricardo Castro (ricardo.castro@lumapr.com) for signature
2024-03-18 - 1:43:54 PM GMT
-  Email viewed by Ricardo Castro (ricardo.castro@lumapr.com)
2024-03-18 - 2:33:49 PM GMT
-  Signer Ricardo Castro (ricardo.castro@lumapr.com) entered name at signing as Ricardo Castro Gómez
2024-03-18 - 2:35:11 PM GMT
-  Document e-signed by Ricardo Castro Gómez (ricardo.castro@lumapr.com)
Signature Date: 2024-03-18 - 2:35:13 PM GMT - Time Source: server

✔ Agreement completed.

2024-03-18 - 2:35:13 PM GMT