



ERate Category 2 Internal Connections

REQUEST FOR PROPOSAL (RFP)

Enterprise Next-Generation Firewall (NGFW) Solution

Target Implementation Date: July 1, 2027

Closing Date and Time: November 18, 2026, at 4:00pm

Single Point of Contact (SPC): Glenn Whitcomb, Director of Information Technology

Address	6972 Keene Road
City, State, Zip	West Richland, WA 99353
E-mail	glenn.whitcomb@rsd.edu

Electronic Submission Portal

<https://erate.imesd.k12.or.us/submission/33734b37d0e82513dbeb>

Richland School District No. 400 promotes equal opportunity for all individuals without regard to age, color, creed, disability, marital status, national origin, race, religion, sex, gender identity or expression, sexual orientation, veteran or military status, or the presence of any sensory, mental, or physical disability.

1. Executive Overview & Contract Scope

Richland School District (RSD) is soliciting competitive, vendor-neutral proposals for a pair of high-availability Enterprise Next-Generation Firewalls (NGFW) to secure core enterprise network boundaries, data center environments, and internet edge connectivity. The solution must deliver real-time deep packet inspection, encrypted traffic analysis, advanced threat prevention, and centralized management without performance degradation under high operational loads.

1.1 Contract Term & Renewal Options

- Primary Base Term: Initial contract term of three (3) years [or optional five (5) years], commencing upon formal execution and delivery.
- Optional Extensions: RSD reserves the sole right to execute up to two (2) additional one-year contract extensions (Year 4 & Year 5, or Year 6 & Year 7).
- Extension Pricing Terms: Extension options must be guaranteed at annual rates equivalent to or lower than the amortized annual cost of the primary base term. Fixed pricing caps for optional extensions must be explicitly guaranteed within the vendor response.

2. Technical & Performance Specifications

Respondents must explicitly certify compliance based on real-world production traffic mix (HTTP/AppMix with 64KB average payload) rather than laboratory UDP burst figures.

2.1 Throughput & Architecture Standards

- Baseline Firewall Throughput: Minimum 40 Gbps raw stateful packet inspection.
- Inspected Threat Prevention Throughput: Minimum 20 Gbps active inspected throughput with Application Control, Intrusion Prevention System (IPS), Anti-Malware, and Logging simultaneously enabled.
- Encrypted Traffic Inspection (SSL/TLS): Minimum 10 Gbps throughput under active TLS 1.3/1.2 hardware-accelerated decryption and re-encryption.
- Concurrent TCP Sessions: Minimum 5,000,000 concurrent sessions.
- New Connections Per Second (CPS): Minimum 250,000 CPS measured via Layer 7 application transactions.
- Physical Form Factor: Maximum 2U physical rack unit footprint with redundant, hot-swappable AC/DC power supplies (1+1) and field-replaceable fan modules.

2.2 Interface & Network Density

- 25GbE Support: Minimum 4 x 25GbE (SFP28) native or modular interfaces.
- 10GbE / 1GbE Support: Minimum 12 x 10GbE (SFP+) interfaces.
- High-Speed Uplinks: Minimum 2 x 100GbE (QSFP28) or 4 x 40GbE (QSFP+) core switch interconnects.
- Out-of-Band & HA Ports: Dedicated 1G/10G management ports and high-speed HA synchronization interfaces (minimum 10G/40G) fully isolated from user dataplanes.

3. Core Security & Networking Capabilities

- Layer 7 Application Control: Identify, inspect, and enforce policies across 3,000+ enterprise applications regardless of port, protocol, or evasive technique.
- User & Identity Mapping: Native integration with Microsoft Active Directory, LDAP, Entra ID, SAML 2.0, and Okta for user-centric policy enforcement.
- Advanced Threat Prevention: Inline IPS with dynamic CVE signature updates, cloud/on-premise zero-day sandboxing, and automated C2/DNS security filtering.
- Resiliency & High Availability: Stateful Active/Passive and Active/Active HA with sub-second session, tunnel, and routing failover.
- Routing Protocols: Complete IPv4/IPv6 dual-stack support for OSPFv2/v3, BGP4, RIP, static routing, and Policy-Based Routing (PBR).

4. Lifecycle & Product Availability Guarantees

- Current Hardware Availability: All proposed hardware platforms must be generally available (GA) and actively manufactured. End-of-Life (EoL), End-of-Sale (EoS), or gray-market equipment is strictly unacceptable.
- Guaranteed Support Horizon: Hardware platforms must feature a guaranteed vendor support lifecycle of at least seven (7) years post-award (minimum through July 2034).
- Long-Term Software Maintenance: Operating system software must be designated Long-Term Support (LTS) with guaranteed security patches throughout the contract term.

5. Project Implementation Schedule & Rollback Plan

The implementation schedule assumes project initiation on or before July 1, 2027, aligned with E-Rate Funding Year guidelines.

5.1 Estimated Implementation Phasing (Starting July 1, 2027)

Phase / Dates	Key Milestones & Operational Activities
Phase 1 July 1 - July 2, 2027	Project Kickoff & Design: Review legacy policies, NAT, VPNs, and VLANs. Finalize High-Level (HLD) & Low-Level Design (LLD).
Phase 2 July 6 - July 9, 2027	Staging & Testing: Appliance delivery, patch to LTS firmware, policy conversion import, lab failover validation. Parallel Installation: Out-of-path rack installation, OOB management setup, identity mapping & routing validation. Cutover Execution: Scheduled maintenance window cutover, physical cable swing, core switch path updates, app verification
Phase 3 July 12 – Aug 31, 2027	Hypercare & Optimization: 45-day intensive monitoring, SSL decryption tuning, hand-off documentation and training

5.2 Contingency Rollback Strategy

1. Go/No-Go Decision Point: A strict decision deadline is established 2 hours prior to the conclusion of the maintenance window.
2. Rollback Triggers: Unresolvable loss of core connectivity (>30 mins), dynamic routing failure (BGP/OSPF), HA synchronization failure, or critical application outages.
3. Execution Procedure: Revert core switch routing paths/physical patches back to legacy firewalls, re-establish dynamic routing adjacencies, and verify service restoration.
4. Post-Mortem Analysis: Conduct Root Cause Analysis (RCA) within 48 hours and resolve identified anomalies in lab prior to rescheduling.

6. Technical Training & Knowledge Transfer (up to 40 Hours)

The proposal must include up to 40 hours of dedicated technical training and knowledge transfer specifically tailored to the RSD Network Team to ensure operational self-sufficiency.

- System Architecture & Centralized Management: Platform overview, HA failover testing, centralized manager setup, backup/restore.
- L7 Application & Identity Policy: User-to-IP mapping (Entra ID/AD/Okta), app-control policy creation, custom app signatures, NAT.
- Advanced Threat & Sandbox: IPS configuration, zero-day sandbox profile setup, URL/content filtering, DNS security policies.
- SSL Decryption & Routing: Inbound/Outbound TLS decryption profiles, bypass lists, PKI cert management, BGP/OSPF/PBR.
- Ops & Diagnostics: Live traffic monitoring, CLI packet captures, session diagnostics, OS upgrades, TAC escalation.

7. E-Rate Compliance & Cost Allocation Schedule

Respondents must provide a valid SPIN number and categorize all proposed costs according to USAC E-Rate Category Two (Internal Connections & BMIC) eligibility rules.

Item Category	Item Description	E-Rate Status	Base Term Cost	Optional Renewal (+1 Yr)
Hardware	NGFW Primary & Secondary Appliances (HA Pair)	Fully Eligible (100%)	\$	\$
Hardware	Network Interface Modules & Transceivers (25G/100G)	Fully Eligible (100%)	\$	\$
Software / OS	Base Firewall Operating System & License	Fully Eligible (100%)	\$	\$
Security Sub	Intrusion Prevention System (IPS / IDS)	Fully Eligible (100%)	\$	\$
Security Sub	Advanced Malware / Cloud Sandbox Engine	Non-Eligible (0%)	\$	\$
Security Sub	URL / Web Content Filtering License	Non-Eligible (0%)	\$	\$

Support	Basic Hardware Maintenance & OS Updates (BMIC)	Fully Eligible (100%)	\$	\$
Services	Migration, Staging & Implementation Services	Partially Eligible	\$	\$
Training	RSD Network Team Technical Training (up to 40 Hours)	Partially Eligible	\$	\$

8. Vendor Equivalent Benchmark Reference

The following industry benchmark models represent acceptable technical capacity standards for evaluation:

Manufacturer	Equivalent Platform Family	Architectural Benchmark Focus
Palo Alto Networks	PA-5420 Platform	Single-Pass Architecture & Integrated ML
Fortinet	FortiGate 1800F / 2600F	NP7/CP9 ASIC Hardware Acceleration
Cisco	Secure Firewall 4225 / 4245	Snort 3 Inspection Engine & ISE Integration
Juniper Networks	SRX4300 / SRX4600	Junos Routing Engine & Mist Telemetry
Check Point	Quantum 16200 / 28000	SandBlast Threat Emulation & Unified Management