SKOKIE73.5

Elizabeth Meyer School • John Middleton Elementary School • Oliver McCracken Middle School

Request for Proposal

Firewall and Hybrid WAN Implementation

2025

RFP Issuance Date: March 17th, 2025
Deadline for Questions: April 1st, 2025
Responses to Q&A Posted: April 2nd, 2025
Proposal Submission Deadline: April 10th, 2025
Proposal Review and Shortlisting: April 11th - April 14th, 2025
Finalist Demo Scheduling: April 15th - April 17th, 2025
Vendor Finalist Demos: April 18th - April 22nd, 2025
Vendor Selection Date: May 13th, 2025
Implementation Start Date: June 2025
Project Completion Date: July 30th, 2025

Proposals must be submitted in electronic format (PDF) to it-rfp@sd735.org

Part I. General Information

1.1 Introduction

Skokie School District 73.5 is seeking proposals from qualified vendors to procure, install, and configure enterprise-grade firewalls at John Middleton Elementary School (Middleton) and Elizabeth Meyer School (Meyer). This project aims to establish independent internet connectivity at each site while maintaining secure, seamless communication between locations through an IPsec-based hybrid Wide Area Network (WAN). The district is transitioning away from its existing dark fiber infrastructure and will be establishing dedicated lit circuits at each location to enhance network resilience, reliability, and security.

The selected vendor will play a pivotal role in designing, procuring, deploying, and configuring the necessary firewall infrastructure to meet the district's evolving needs, while ensuring compatibility with the district's broader network architecture.

Current Setup:

Current Network Architecture

- **McCracken**: The current network hub connected via a single lit circuit that provides internet access for the entire district.
- **Middleton**: Currently connected to McCracken via dark fiber.
- **Meyer**: Connected to Middleton via dark fiber, with a transit layer bridging traffic to McCracken.
- **Palo Alto Firewall**: Manages internet access at McCracken but will be evaluated for replacement with a more integrated solution as part of a future upgrade.

This RFP aims to solicit proposals from vendors with expertise in network security, firewall deployment, and WAN implementation to provide a solution that ensures the district's network can scale securely and efficiently as needs evolve.

1.2 Scope of Work

The goal of this project is to enhance the district's network security infrastructure and ensure each school site can independently access the internet while remaining securely connected to the district's central resources.

Key objectives include:

- **Deployment of New Firewalls**: Procure and install enterprise-grade firewalls at Middleton and Meyer to enable independent, secure internet access.
- **Collaboration with IDOT**: Coordinate with the Illinois Department of Innovation & Technology, which will be responsible for installing the new lit circuits at Middleton and Meyer.
- **Network Reconfiguration**: Update network routing on Meraki MS425 stacks at Middleton and Meyer to direct

internet-bound traffic through their new dedicated circuits, while ensuring continued access to shared district resources at McCracken.

- **IPsec VPN Implementation**: Establish secure site-to-site IPsec VPN tunnels between Middleton, Meyer, and McCracken to ensure seamless and encrypted communication across the WAN.
- **Resiliency and Redundancy**: Ensure the solution is resilient, supporting the district's goal to minimize the impact of local power disruptions on overall network availability.

1.3 Key Features and Capabilities Sought

The proposed firewall solution must meet the following criteria to ensure the district's evolving needs are addressed with a secure, reliable, and scalable solution:

Functional Requirements

- **Firewall Procurement and Installation**: Deploy enterprise-grade firewalls at Middleton and Meyer with next-generation security capabilities, ensuring site-specific internet access while maintaining secure inter-site communication.
- **Firewall Security Configuration**:
  - Implement advanced threat prevention capabilities, including **intrusion prevention, malware detection, and real-time threat intelligence** updates.
  - Configure **web filtering (URL filtering)** to enforce safe browsing policies in accordance with district security policies and compliance requirements (CIPA, FERPA, etc.).
  - Support **sandboxing technologies (WildFire-equivalent)** to detect and analyze zero-day threats and unknown malware before they reach the network.
  - Ensure deep **SSL/TLS inspection** for encrypted traffic scanning without compromising performance.
- **VPN Implementation for Secure Remote Access**:
  - Establish **a site-to-site IPsec VPN** to ensure secure inter-site communication between Middleton, Meyer, and McCracken.
  - Deploy **a remote access VPN solution (GlobalProtect-equivalent)** to provide secure, policy-enforced connectivity for district IT staff.
  - Support **multi-factor authentication (MFA) integration** with Rapid Identity or other identity providers for enhanced security.
- **Advanced Traffic Filtering and Application Control**:
  - Provide **granular application-layer controls** to manage and secure internet usage, ensuring appropriate traffic segmentation.
  - Implement **policy-based access control** to restrict access to unauthorized applications and websites based on content categories.
- **Integration with Security Operations**:
  - Enable **centralized logging, monitoring, and alerting** to integrate with the district's SIEM (Security Information and Event Management) platform or equivalent.
  - Support **real-time threat intelligence updates** to block emerging threats proactively.

Technical Requirements

Next-Generation Firewall (NGFW) Capabilities

- Support intrusion prevention system (IPS) and intrusion detection system (IDS) to detect and mitigate threats at the network perimeter.
- Implement AI-driven or cloud-based threat analysis (such as WildFire or an equivalent solution) to analyze unknown files for malware.
- Provide zero-trust network security features, ensuring strict access control based on identity and least-privilege principles.

Seamless VPN Integration

- Provide secure, always-on VPN access for district IT staff with policy-driven access controls.
- Ensure role-based VPN access with split tunneling support for optimized performance.
- Offer remote troubleshooting and management capabilities for IT staff to securely access network resources.

High Availability (HA) and Reliability

- Firewalls must support active/passive and active/active HA configurations to ensure uninterrupted service.
- Include automated failover mechanisms for redundancy.

Network Visibility and Logging

- Support deep packet inspection (DPI) and full layer 7 traffic analysis to identify potential threats.
- Ensure compatibility with cloud-based log aggregation and monitoring tools.

Integration and Compatibility

Cloud-Managed Security Policies

- Ensure centralized, cloud-based administration to streamline policy deployment and configuration updates.
- Support automatic security policy synchronization across multiple sites.

Identity and Access Management Integration

- The firewall solution must integrate with Rapid Identity or other existing authentication solutions for single sign-on (SSO) and role-based access control.

Training & Support Requirements

Comprehensive Training for IT Staff:

- Provide training on firewall management, VPN administration, policy enforcement, and incident response.
- Offer hands-on lab sessions or simulated attack scenarios to prepare IT staff for real-world security incidents.

Ongoing Technical Support and Software Updates:

- Include 24/7 vendor support options, with response time guarantees for critical issues.
- Ensure continuous security updates, including threat intelligence feeds, firmware upgrades, and vulnerability patches.

Licensing Requirements

Comprehensive Subscription Model

- Licensing must cover:
    - Next-Generation Threat Prevention (IPS, malware scanning, sandboxing)
    - Advanced URL Filtering
    - Cloud-based threat intelligence updates
    - Remote Access VPN licenses for IT staff
- The vendor must provide flexible licensing options to accommodate future scalability and growth.

1.4 RFP Participation Requirements

Right of Selection/Rejection of Proposals

Skokie School District 73.5 reserves the right to select or reject any proposal for any reason. The district may negotiate terms with vendors, select the most favorable financial terms, and waive any informalities or deviations from the RFP.

Incorporation of RFP in the Final Agreement

This RFP and the successful vendor's response will be incorporated into the final contract with the vendor.

Errors in Proposals

Skokie School District 73.5 may waive deviations or errors in a proposal but reserves the right to reject proposals if discrepancies are found. Any errors or omissions in a proposal will not diminish the vendor's obligations.

Cost of Development of RFP Proposals

All expenses incurred by vendors in the development of proposals will be borne by the vendor, and no reimbursement will be provided.

Non-Collusion

Vendors must certify that they have not engaged in price-fixing or other anti-competitive practices.

Proposal Disposition

All materials submitted will remain the property of Skokie School District 73.5.

1.5 Evaluation Criteria

Proposals will be evaluated based on the following criteria:

- **Technical Fit**: Alignment with technical, functional, and security requirements.
- **Cost**: Total cost of ownership, including setup, licensing, and support fees.
- **Experience & References**: Vendor experience with K-12 schools or similar environments.
- **Implementation Approach**: Timeline, risk mitigation, and project management methodology.
- **Support & Training**: Quality and availability of ongoing support and training.
- **Scalability & Future-readiness**: Adaptability to future technology changes.

1.6 Timeline

- **RFP Issuance Date:** March 17th, 2025
- **Deadline for Questions:** April 1st, 2025
- **Responses to Q&A Posted:** April 2nd, 2025
- **Proposal Submission Deadline:** April 10th, 2025

- **Proposal Review and Shortlisting:** April 11th - April 14th, 2025
- **Finalist Demo Scheduling:** April 15th - April 17th, 2025
- **Vendor Finalist Demos:** April 18th - April 22nd, 2025
- **Vendor Selection Date:** May 13th, 2025
- **Implementation Start Date:** June 2025
- **Project Completion Date**: July 30th, 2025

Part II. Instructions for Submitting Proposals

2.1 Proposal Format

Vendors must structure their proposals using the following format:

1. **Cover Letter**: Introduction and statement of interest.
2. **Company Overview**: History, experience with K-12 or similar institutions, and relevant certifications.
3. **Project Approach**: Description of how the vendor will meet the district's requirements.
4. **Technical Solution**: Detailed technical specifications, features, and system architecture.
5. **Implementation Plan**: Timeline, milestones, and resource requirements.
6. **Training and Support Plan**: Training schedule, support response times, and escalation procedures.
7. **Cost Proposal**: Detailed breakdown of setup, subscription, licensing, maintenance, and support fees.
8. **References**: At least three (3) references from K-12 or public sector clients.

Part III. Vendor Finalists Demo Guidelines

3.1 Finalist Selection

After reviewing the proposals, Skokie School District 73.5 will select a shortlist of finalists based on the evaluation criteria outlined in Section II. Shortlisted vendors will be invited to participate in a live demo as part of the final selection process.
3.2 Demo Format
The vendor demo should include the following components:

- System Overview: A high-level overview of the proposed solution, including its key features and benefits.
- System Architecture & Integration: Detailed explanation of the architecture and how the firewall solution integrates with existing systems (e.g., Cisco Meraki, Palo Alto firewall, internal network resources).
- Firewall Configuration & Management: Demonstrate firewall rule configuration, VPN setup, and integration with current district network infrastructure.
- Training and Support: Demonstration of the training resources available for district IT staff, including configuration management, firewall rule adjustments, and troubleshooting.

- Security Features: Highlight security features such as deep packet inspection, threat prevention, and IPsec VPN capabilities. Demonstrate compliance with industry standards and FERPA.
- Scalability: Showcase how the solution can scale for future district needs, particularly in regard to additional sites or traffic demands.
- Logging and Monitoring: Demonstration of logging, alerting, and monitoring capabilities as part of the ongoing firewall management.

3.3 Technical Setup

Vendors should ensure that the system is set up and configured for the demonstration to showcase the most relevant features of the proposed firewall solution.
All devices required for the demo (e.g., firewalls, routers, VPN clients, monitoring dashboards) should be pre-configured and available for demonstration purposes.

3.4 Duration and Format

Each vendor will have 60 minutes for their demo:

- 45 minutes for the presentation and walkthrough.
- 15 minutes for Q&A with the selection committee.
  Demos will be conducted virtually (via Zoom or similar video conferencing platform) unless otherwise specified.

3.5 Evaluation Criteria for Demo

The demos will be assessed based on the following criteria:

- Relevance to Needs: How well the solution addresses the district's specific firewall and network security requirements, including IPsec VPN and routing configuration.
- Ease of Use: User-friendliness and intuitiveness of the firewall configuration interface, including the ability to set up and manage security policies and VPN tunnels.
- Integration Feasibility: How easily the solution integrates with existing systems, including Cisco Meraki and the district's Palo Alto firewall infrastructure.
- Scalability: The solution's ability to scale to accommodate future network growth, additional sites, and more complex security needs.
- Security and Compliance: Adequacy of security features, including FERPA compliance, encryption, and the firewall's capacity to meet district security policies.
- Support and Training: Quality and depth of training materials and ongoing support provided to district IT staff post-implementation.

3.6 Scheduling of Demos

- All demos will be scheduled following the proposal submission deadline. Vendors will be contacted by the district to arrange a convenient time.
- Vendors should be prepared to accommodate demo scheduling within a reasonable window (7-10 business days after the proposal deadline).

Part IV: Q&A Access

4.1 Question Submission

All interested vendors may submit questions regarding the RFP by the deadline outlined in section 1.6. These should be directed to it-rfp@sd735.org.

4.2 Responses to Questions

All answers to submitted questions will be shared with all potential vendors by the date outlined in section 1.6. A Q&A document will be posted publicly on the RFP portal and/or emailed to all participants to ensure equal access.