J. Sterling Morton High School District 201

Board of Education Green Sheet

Board Meeting Date:

Agenda Location: (check one)

☐Staff Travel ☐Student Travel ☐Contracts
☒Bids or Quotes ☐Bid Results ☐Donations/Grants
☐Disposal of District Property ☐Other:

Submitted by: Keith Beisman

A. EDUCATIONAL IMPACT STATEMENT

Upgrading our district firewalls is essential to maintain network security and compliance, as the current hardware will reach end-of-life in Spring 2026 and will no longer receive critical updates or vendor support needed to protect student and staff data.

B. SCHOOL IMPROVEMENT GOAL STATEMENT

N/A

C. STATUTE, BOARD POLICY OR RULE STATEMENT

N/A

D. FISCAL IMPACT STATEMENT

The IT Department recommends the replacement of the district's firewall hardware at a total cost of $382,386.25, with implementation services totaling $53,824. This recommendation reflects the most competitive pricing obtained following a thorough evaluation of multiple vendor proposals. It is further recommended that the Board authorize a contingency allowance of up $19,119.00 to cover any unforeseen expenses or adjustments necessary to ensure timely and successful project completion.

E. SUPERINTENDENT'S GOALS (check all that apply)

☐ACCOUNTABILITY
☐ENHANCED LEARNING OPPORTUNITIES
☐ENSURE PARENTS AND THE COMMUNITY ARE ACTIVE PARTNERS IN THE PROCESS
☒PROVIDE SAFE AND WELL-MAINTENAINED SCHOOLS TO ENHANCE LEARNING
☒RUN AN EFFICIENT BUSINESS OPERATION

ADMINISTRATION'S RECOMMENDATION

This administrator recommends the replacement of the district's firewall hardware, which is scheduled to reach end of support in Spring 2026, to ensure the continued protection, reliability, and stability of Morton's network infrastructure. Three firewall proposals are attached for the Board's review and consideration, with the Sentinel Technologies proposal identified as the recommended option.

The Sentinel proposal includes five years of comprehensive support and licensing, providing full coverage with no additional costs during the contract term. Sentinel Technologies, the district's current cybersecurity partner with extensive knowledge of Morton's existing firewall environment, will manage implementation. The district's current maintenance agreement will transition seamlessly to the new hardware, ensuring continuity of service and support throughout the upgrade process.

The total project cost is $382,386.25 for firewall hardware, with implementation services totaling $53,824. It is further recommended that the Board authorize a 5% contingency to cover any unforeseen costs necessary to ensure timely and successful completion of the project.

Morton Firewall Replacement Timeline

November 2025 – School Board Approval

- The Board of Education reviews and approves the purchase and implementation plan for the new firewall system.

December 2025 – Firewall Order Placement

- The IT Department will submit the purchase order and finalize the agreement with **Sentinel** for the firewall hardware, licensing, and five-year support coverage.
  - *Note: Cisco requires an estimated 6–8 week lead time to build and deliver the firewall hardware once the order is placed.*

February–March 2026 – Firewall Delivery and Programming

- Firewall hardware arrives on-site.
- Sentinel and Morton IT begin programming, configuration, and testing of the new firewall to ensure readiness for deployment.

April 2026 – Receipt and Final Configuration (Spring Break)

- Additional configuration and validation performed during Spring Break to minimize any impact on instructional time.

June 2026 – Implementation (After Graduation, Before Summer School)

- Full firewall deployment and cutover occur the first week of June 2026, ensuring a seamless transition prior to the start of summer school programs.

Data sheet
Cisco public

Cisco Secure Firewall 3100 Series

Cisco Secure Firewall

Cisco Secure IPS

Contents

Cisco Secure Firewall 3100 Series

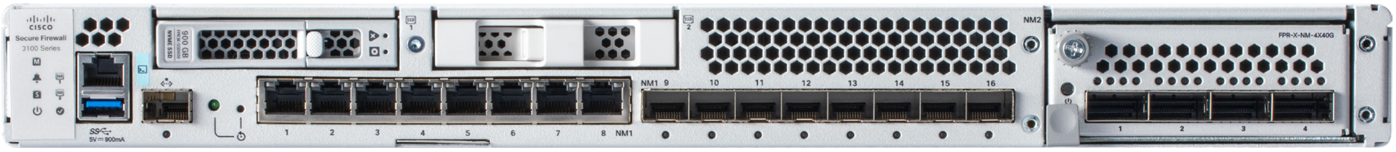
The mid-range Cisco Secure Firewall 3100 Series supports your evolving world. It makes hybrid work and zero trust practical, with the flexibility to ensure strong return on investment.

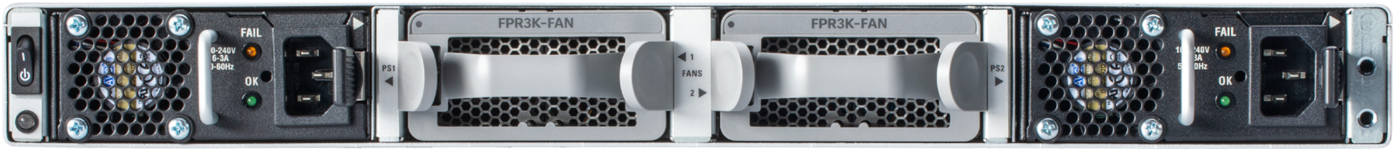
The Cisco Secure Firewall 3100 Series is a family of threat-focused security appliances that delivers business resiliency and superior threat defense. **Each model offers outstanding performance for multiple firewall use cases, even when advanced threat functions are enabled.** These performance capabilities are enabled by a modern CPU architecture coupled with purpose-built hardware that optimizes firewall, cryptographic, and threat inspection functions.

The five models in the 3100 Series deliver a range of performance levels to address use cases from the Internet edge to the data center and private cloud. The 3100 Series supports also clustering to deliver increased performance that can scale to meet your needs as your organization grows.

Each model in the series can run either ASA or Firewall Threat Defense (FTD) software and the platform can be deployed in both firewall and dedicated IPS modes. For inline sets and passive interfaces, the 3100 series supports Q-in-Q (stacked VLAN) with up to two 802.1Q headers in a packet.

Model overview





Cisco Secure Firewall 3100 series summary

Table 1. Cisco Secure Firewall 3100 Series performance and specification highlights

Secure Firewall Models	Firewall	FW+AVC+IPS	IPS Throughput	Interfaces	Optional interfaces
3105	10G	10G	10G	8 x RJ45, 8 x 1/10G SFP+	10G SFP+
3110	18G	17G	17G	8 x RJ45, 8 x 1/10G SFP+	10G SFP+
3120	22G	21G	21G	8 x RJ45, 8 x 1/10G SFP+	10G SFP+
3130	42G	38G	38G	8 x RJ45, 8 x 1/10/25G SFP+	10G/25G/40G SFP+, 4X40G NM
3140	49G	45G	45G	8 x RJ45, 8 x 1/10/25G SFP+	10G/25G/40G SFP+, 4x40G NM

Performance specifications and feature details

Table 2. Cisco Secure Firewall 3100 Series performance and capabilities, running on Firewall Threat Defense (FTD) software

Features	3105	3110	3120	3130	3140
Throughput: FW + AVC (1024B)	10 Gbps	17.0 Gbps	21.0 Gbps	38.0 Gbps	45.0 Gbps
Throughput: FW + AVC + IPS (1024B)	10 Gbps	17.0 Gbps	21.0 Gbps	38.0 Gbps	45.0 Gbps
Maximum concurrent sessions, with AVC	1.5 million	2 million	4 million	6 million	10 million
Maximum new connections per second, with AVC	90,000	130,000	170,000	240,000	300,000
TLS[1]	3.2 Gbps	4.8 Gbps	6.7 Gbps	9.1 Gbps	11.5 Gbps
Throughput: NGIPS (1024B)	10.0 Gbps	17.0 Gbps	21.0 Gbps	38.0 Gbps	45.0 Gbps
IPSec VPN Throughput (1024B TCP w/Fastpath)	5.5 Gbps	8 Gbps	10 Gbps	17.8 Gbps	22.4 Gbps
Projected IPSec VPN Throughput (1024B TCP w/Fastpath) with VPN Offload (FTD 7.2)	NA	11.0 Gbps	13.5 Gbps	33.0 Gbps	39.4 Gbps
Maximum VPN Peers	2,000	3,000	7,000	15,000	20,000
Local On-device Management	Yes	Yes	Yes	Yes	Yes
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by the Firewall Management Center or alternatively in the cloud with Cisco Defense Orchestrator				
Application Visibility and Control (AVC)	Standard, supporting more than 4000 applications, as well as geolocations, users, and websites				
AVC: OpenAppID support for custom, open source, application detectors	Standard				
Cisco Security Intelligence	Standard, with IP, URL, and DNS threat intelligence				
Cisco Secure IPS	Available; can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence				

Features	3105	3110	3120	3130	3140
Cisco Malware Defense	Available; enables detection, blocking, tracking, analysis, and containment of targeted and persistent malware, addressing the attack continuum both during and after attacks. Integrated threat correlation with Cisco Secure Endpoint is also optionally available				
Cisco Secure Malware Analytics	Available				
URL Filtering: number of categories	More than 80				
URL Filtering: number of URLs categorized	More than 280 million				
Automated threat feed and IPS signature updates	Yes: class-leading Collective Security Intelligence (CSI) from the Cisco Talos Group (https://www.cisco.com/c/en/us/products/security/talos.html)				
Third-party and open-source ecosystem	Open API for integrations with third-party products; Snort® and OpenAppID community resources for new and specific threats				
High availability and clustering	Active/active, Active/standby. Cisco Secure Firewall 3100 Series allows clustering of up to 8 chassis (no clustering on 3105)				
Cisco Trust Anchor Technologies	Secure Firewall 3100 Series platforms include Trust Anchor Technologies for supply chain and software image assurance. Please see the section below for additional details				

[1] Throughput measured with 50% TLS 1.2 traffic with AES256-SHA with RSA 2048B keys.

Note: Performance will vary depending on features activated, and network traffic protocol mix, and packet size characteristics. Performance is subject to change with new software releases. Consult your Cisco representative for detailed sizing guidance.

Table 3. ASA Performance and capabilities on Secure Firewall 3100 appliances

Features	3105	3110	3120	3130	3140
Stateful inspection firewall throughput[1]	10.0 Gbps	18.0 Gbps	22.0 Gbps	42.0 Gbps	49.0 Gbps
Stateful inspection firewall throughput (multiprotocol)[2]	9.0 Gbps	15.0 Gbps	17.0 Gbps	39.0 Gbps	43.0 Gbps
Concurrent firewall connections	1.5 million	2 million	4 million	6 million	10 million
New connections per second	150,000	300,000	500,000	875,000	1,100,000
IPsec VPN throughput (450B UDP L2L test)	5.5 Gbps	8 Gbps	10 Gbps	14 Gbps	17 Gbps
Projected IPsec VPN throughput (450B UDP L2L test) with VPN Offload (ASA 9.18)	7.0 Gbps	12.0 Gbps	15.4 Gbps	28.0 Gbps	33.0 Gbps

Features	3105	3110	3120	3130	3140
Maximum VPN Peers	2,000	3,000	7,000	15,000	20,000
Security contexts (included; maximum)	2; 100	2; 100	2; 100	2; 100	2; 100
High availability	Active/active and active/ standby	Active/active and active/ standby	Active/active and active/ standby	Active/active and active/ standby	Active/active and active/ standby
Clustering	N/A	8	8	8	8
Scalability	VPN Load Balancing				
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by Cisco Security Manager or alternatively in the cloud with Cisco Defense Orchestrator				
Adaptive Security Device Manager	Web-based, local management for small-scale deployments				

[1] Throughput measured with 1500B User Datagram Protocol (UDP) traffic measured under ideal test conditions.

[2] "Multiprotocol" refers to a traffic profile consisting primarily of TCP-based protocols and applications like HTTP, SMTP, FTP, IMAPv4, BitTorrent, and DNS.

Hardware specifications

Table 4. Cisco Secure Firewall 3100 Series hardware specifications

Features	Cisco Secure Firewall Model				
	3105	3110	3120	3130	3140
Dimensions (H x W x D)	1.75 x 17 x 20 in. (4.4 x 43.3 x 50.8 cm)	1.75 x 17 x 20 in. (4.4 x 43.3 x 50.8 cm)	1.75 x 17 x 20 in. (4.4 x 43.3 x 50.8 cm)	1.75 x 17 x 20 in. (4.4 x 43.3 x 50.8 cm)	1.75 x 17 x 20 in. (4.4 x 43.3 x 50.8 cm)
Form factor (rack units)	1RU	1RU	1RU	1RU	1RU
Integrated I/O	8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45), 8 x 1/10 Gigabit (SFP) Ethernet interfaces	8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45), 8 x 1/10 Gigabit (SFP) Ethernet interfaces	8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45), 8 x 1/10 Gigabit (SFP) Ethernet interfaces	8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45), 8 x 1/10/25 Gigabit (SFP) Ethernet interfaces	8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ- 45), 8 x 1/10/25 Gigabit (SFP) Ethernet interfaces
Network modules	8 x 1/10G Options	8 x 1/10G Options	8 x 1/10G Options	8 x 1/10/25G, 4 x 40G Options,	8 x 1/10/25G, 4 x 40G Options
Maximum number of interfaces	Up to 24 total Ethernet ports, (8x1G RJ-45, 8x1/10G SFP, and network module)	Up to 24 total Ethernet ports, (8x1G RJ-45, 8x1/10G SFP, and network module)	Up to 24 total Ethernet ports, (8x1G RJ-45, 8x1/10G SFP, and network module)	Up to 24 total Ethernet ports (8x1G RJ-45, 8x1/10/25G SFP,	Up to 24 total Ethernet ports (8x1G RJ-45, 8x1/10/25G SFP,

Features	Cisco Secure Firewall Model				
	3105	3110	3120	3130	3140
				and network module)	and network module)
Integrated network management ports	1 x 1/10G SFP	1 x 1/10G SFP	1 x 1/10G SFP	1 x 1/10G SFP	1 x 1/10G SFP
Serial port	1 x RJ-45 console	1 x RJ-45 console	1 x RJ-45 console	1 x RJ-45 console	1 x RJ-45 console
USB	1 x USB 3.0 Type-A (900mA)	1 x USB 3.0 Type-A (900mA)	1 x USB 3.0 Type-A (900mA)	1 x USB 3.0 Type-A (900mA)	1 x USB 3.0 Type-A (900mA)
Storage	1x 900 GB, 1x spare slot	1x 900 GB, 1x spare slot	1x 900 GB, 1x spare slot	1x 900 GB, 1x spare slot	1x 900 GB, 1x spare slot
Power supply configuration	Single 400W AC, Dual 400W AC optional. Single/Dual 400W DC optional[1]	Single 400W AC, Dual 400W AC optional. Single/Dual 400W DC optional[1]	Single 400W AC, Dual 400W AC optional. Single/Dual 400W DC optional[1]	Dual 400W AC. Single/dual 400W DC optional[1]	Dual 400W AC. Single/dual 400W DC optional[1]
AC input voltage	100 to 240V AC	100 to 240V AC	100 to 240V AC	100 to 240V AC	100 to 240V AC
AC maximum input current	< 6A at 100V	< 6A at 100V	< 6A at 100V	< 6A at 100V	< 6A at 100V
AC maximum output power	400W	400W	400W	400W	400W
AC frequency	50 to 60 Hz	50 to 60 Hz	50 to 60 Hz	50 to 60 Hz	50 to 60 Hz
AC efficiency	>89% at 50% load	>89% at 50% load	>89% at 50% load	>89% at 50% load	>89% at 50% load
DC input voltage	-48V to -60VDC	-48V to -60VDC	-48V to -60VDC	-48V to -60VDC	-48V to -60VDC
DC maximum input current	< 12.5A at -48V	< 12.5A at -48V	< 12.5A at -48V	< 12.5A at -48V	< 12.5A at -48V
DC maximum output power	400W	400W	400W	400W	400W
DC efficiency	>88% at 50% load	>88% at 50% load	>88% at 50% load	>88% at 50% load	>88% at 50% load
Redundancy	1+1 AC or DC with dualsupplies	1+1 AC or DC with dualsupplies	1+1 AC or DC with dualsupplies	1+1 AC or DC with dualsupplies	1+1 AC or DC with dualsupplies
Fans	2 hot-swappable fan modules (with 2 fans each)[2]	2 hot-swappable fan modules (with 2 fans each)[2]	2 hot-swappable fan modules (with 2 fans each)[2]	2 hot-swappable fan modules (with 2 fans each)[2]	2 hot-swappable fan modules (with 2 fans each)[2]
Noise	65 dBA@ 25C	65 dBA@ 25C	65 dBA@ 25C	65 dBA@ 25C	65 dBA@ 25C

Features	Cisco Secure Firewall Model				
	3105	3110	3120	3130	3140
	74 dBA maximum	74 dBA maximum	74 dBA maximum	74 dBA maximum	74 dBA maximum
Rack mountable	Yes. Fixed mount brackets optional. (2- post). Mount railsincluded (4-post EIA-310-D rack)	Yes. Fixed mount brackets optional. (2- post). Mount railsincluded (4-post EIA-310-D rack)	Yes. Fixed mount brackets optional. (2- post). Mount railsincluded (4-post EIA-310-D rack)	Yes. Fixed mount brackets optional. (2- post). Mount railsincluded (4-post EIA-310-D rack)	Yes. Fixed mount brackets optional. (2- post). Mount railsincluded (4-post EIA-310-D rack)
Weight	23 lb (10.5 kg) 1 x power supplies, 1 x NM, fan module, 1x SSD	23 lb (10.5 kg) 1 x power supplies, 1 x NM, fan module, 1x SSD	23 lb (10.5 kg) 1 x power supplies, 1 x NM, fan module, 1x SSD	25 lb (11.4 kg) 2 x power supplies, 1 x NM, fan module, 1x SSD	25 lb (11.4 kg) 2 x power supplies, 1 x NM, fan module, 1x SSD
Temperature: operating	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C) or NEBS operation (see below)[3]	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)
Temperature: nonoperating	-4 to 149°F (-20 to 65°C)	-4 to 149°F (-20 to 65°C)	-4 to 149°F (-20 to 65°C)	-4 to 149°F (-20 to 65°C)	-4 to 149°F (-20 to 65°C)
Humidity: operating	10 to 85% noncondensing	10 to 85% noncondensing	10 to 85% noncondensing	10 to 85% noncondensing	10 to 85% noncondensing
Humidity: nonoperating	5 to 95% noncondensing	5 to 95% noncondensing	5 to 95% noncondensing	5 to 95% noncondensing	5 to 95% noncondensing
Altitude: operating	10,000 ft (max)	10,000 ft (max)	10,000 ft (max) or NEBS operation (see below)[3]	10,000 ft (max)	10,000 ft (max)
Altitude: nonoperating	40,000 ft (max)	40,000 ft (max)	40,000 ft (max)	40,000 ft (max)	40,000 ft (max)
NEBS operation (FPR- 3120 Only)[3]			Operating altitude: 0 to 13,000 ft (3962 m) Operating temperature: Long term: 0 to 45°C, up to 6,000 ft (1829 m) Long term: 0 to 35°C, 6,000 to 13,000 ft (1829 to 3964 m) Short term: -5 to 55°C, up to 6,000 ft (1829 m)		

[1] Dual power supplies are hot-swappable.

[2] Fans operate in a 3+1 redundant configuration where the system will continue to function with only 3 operational fans. The 3 remaining fans will run at full speed.

[3] FPR-3120 platform is designed to be NEBS ready. The availability of NEBS certification is pending.

Table 5. Cisco Secure Firewall 3100 Series NEBS, Regulatory, Safety, and EMC Compliance

Specification	Description
Regulatory compliance	• Products comply with CE markings per directives 2004/108/EC and 2006/108/EC
Safety	• UL 62368-1 • CAN/CSA-C22.2 No. 62368-1 • EN 62368-1 • IEC 62368-1 • IEC 60950-1 • AS/NZS 62368-1 • GB4943
EMC: emissions	• FCC 47CFR15 Class A • AS/NZS CISPR 32 Class A • EN55032/CISPR 32 Class A • ICES-003 Class A • VCCI Class A • KS C 9832 Class A • CNS-13438 Class A • EN61000-3-2 Power Line Harmonics • EN61000-3-3 Voltage Changes, Fluctuations, and Flicker
EMC: Immunity	• IEC/EN61000-4-2 Electrostatic Discharge Immunity • IEC/EN61000-4-3 Radiated Immunity • IEC/EN61000-4-4 EFT-B Immunity • IEC/EN61000-4-5 Surge • IEC/EN61000-4-6 Immunity to Conducted Disturbances • IEC/EN61000-4-11 Voltage Dips, Short Interruptions, and Voltage Variations • KS C 9835
EMC: ETSI/EN	• EN 300 386 Telecommunications Network Equipment (EMC) • EN55032/CISPR 35 Multimedia Equipment (Emissions) • EN55024/CISPR 24 Information Technology Equipment (Immunity) • EN55035/CISPR 35 Multimedia Equipment (Immunity) • EN61000-6-1 Generic Immunity Standard

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

Document history

New or Revised Topic	Described In	Date
3105 model added	Tables 1, 2, 3, 4	March xx, 2023

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA

C78-745072-05 09/24

New Cisco Firewall

Budgetary Proposal # 022848

Prepared for:

J Sterling Morton High School District 201

Artur Wilczynski
awilczynski@jsmorton.org

Prepared by:

Sentinel Technologies, Inc

Kyle Donnelly
kdonnelly@sentinel.com

Cisco Secure Firewall 3120

Product Description	Qty	Price	Ext. Price
Solution Subscriptions - *Unless explicitly indicated otherwise within this contract, the below term for these subscription services will automatically renew, absent at least ninety (90) days' notice of cancelation by Customer before the start of the renewal term. For subscription services that do not automatically renew, Customer must provide Sentinel with at least ninety (90) days' notice of its intention to renew the services and shall hold Sentinel harmless from any service interruption to result from the cessation of services due to Customer's failure to provide timely notice as stated herein.*			
Cisco Secure Firewall 3120 NGFW Appliance, 1U	4	$22,189.00	$88,756.00
Cisco Secure Firewall 3K Series 400W AC Power Supply	4	$1,005.00	$4,020.00
Cisco Secure Firewall 3K Series 400W AC Power Supply	4	$0.00	$0.00
AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	8	$0.00	$0.00
Threat Defense software v7.4 for 3100 Series appliances	4	$0.00	$0.00
Cisco Secure Firewall 3K Series 900GB	4	$0.00	$0.00
Cisco Secure Firewall 3100 Slide Rail Kit	4	$0.00	$0.00
Cisco Secure Firewall 3120 Base Lic	4	$0.00	$0.00
CISCO SECURE FIREWALL 3K SERIES FAN TRAY	8	$0.00	$0.00
CISCO SECURE FIREWALL 3100 SERIES SSD BLANK SLOT COVER	4	$0.00	$0.00
Cisco Secure Firewall 3100 Network Module Blank Slot Cover	4	$0.00	$0.00
Console Cable 6ft with RJ45 and DB9F	4	$0.00	$0.00
ACTS Maintenance - 60 Months			
ACTS Gold SNTC-8X5XNBD Cisco Secure Firewall 3120 - 60 Months	4	$26,000.00	$104,000.00
Subscriptions - 60 Months			
Initial Term: 60 Months | Requested Start Date: Upon Order | Billing Model: Prepaid | Renewal Term: Requote			
Cisco Secure Firewall 3120 TD, Malware and URL License	4	$0.00	$0.00
CISCO SECURE FIREWALL 3120 TD, AMP & URL FILTERING 5Y SUBS	4	$43,776.00	$175,104.00
ACTS Platinum CISCO SECURE FIREWALL 3120 TD, AMP & URL FILTERING 5Y SUBS	4	$2,626.56	$10,506.24

Subtotal:	**$382,386.24**

Professional Services

Product Description	Ext Price
Professional Services - Fixed Price	$53,824.00
Subtotal:	**$53,824.00**

Statement of Work

Statement of Work

Executive Summary

J Sterling Morton High School District 201 (client) is replacing end of life Cisco FTD firewalls with newer Cisco FTD firewalls. Sentinel Technologies has been engaged to provide a recommended solution and remote configuration and migration assistance of the new firewalls.

It is the intent of this engagement that Sentinel will architect, design, and implement the project according to Sentinel established best practices and, in a manner, ready for production computing. During this project, knowledge transfer of general administration tasks, points of scale, and the environment will be provided to prepare the customer staff moving forward after the engagement.

Solution Description

The proposed solution includes basic firewall configurations for up to two (2) pairs Cisco FTD firewalls configured for active/standby high availability (HA) at two (2) sites.
Sentinel assumes the firewalls in this proposal will be managed by one (1) existing on premise Cisco virtual FMC (vFMC) server.

Project Methodology

Project Initiation

Sentinel Project Management will coordinate a kick-off meeting to review and approve the Scope of Work provided to the Customer. Customer and Sentinel provided resources will be introduced and their relevant roles for the project discussed. Sentinel Project Management will then coordinate a design meeting between Sentinel Engineers and Customer in order to draft a blueprint of all proposed work which will be provided to the Customer. High level timelines for project milestones will also be identified and discussed.

Design

Sentinel engineers will perform a high-level audit of the Customer's relevant infrastructure. The data collected from this audit will be used to generate a design for the implementation of the solution. Sentinel engineers will inform the Customer of any design requirements that will need to be completed by the Customer's IT staff prior to the start of the next phase (such as provisioning of storage space, acquisitions of licenses, and other essential design components not covered within this document). Upon acceptance of the work as detailed within the blueprint by the Customer, Sentinel engineers and project managers will then coordinate specific dates and times appropriate for accommodating the nature of the work involved (i.e. work which will require outages will be scheduled during appropriate maintenance windows).

Implementation

During the Implementation phase, equipment will be unboxed, burned-in, configured and tested. Unless explicitly stated in this Scope of Work, the staging of equipment will occur at Customer's location. This ensures maximum efficiency and quality while minimizing the disruptions and impacts to the Customer’s environment. After the equipment has been staged Sentinel engineers will proceed with the implementation of all items specified within this Scope of Work and further detailed in the Customer approved Design Document.

Cutover and Post Support

Cutovers will be scheduled per the details in the scope below. Sentinel engineers will be dedicated to being available for the resolution of any problems or issues that arise during the post support portion of the project.

Project Completion

Upon conclusion of all other phases of work Sentinel’s engineers will provide the Customer with updated design documents for the project. Sentinel’s project management team will then arrange for a meeting with the Customer to review the status of all project items. If no project items remain open Sentinel’s project managers will request that the Customer sign off on the project, thus closing the project at that time.

Project Management

Sentinel will provide a project manager committed to the success of the project. The project manager will be responsible for:

- Complete success of the project.
- Optimal coordination of all resources.
- Guiding the Customer on aspects of the project they are required to perform.
- Tracking and reporting of progress.
- Management of agreed to budget issues.
- Management of expected timelines for implementation.
- Changes to the project and communications of changes in writing using a Project Change Form.
- Post installation document gathering, assembly and presentation.
- Post installation project completion agreement and signature.

Project management will ensure complete project success. Communication is the cornerstone of project management and the project manager will be the central communication mechanism for all parties. This will assure all relevant parties are informed about decisions that may affect the success of their component of the solution.

Scope of Work

Design

Firewall Design

- Qty (2) - Firewall Base Design
    - Review and discovery of current firewall environment with the goal of creating a design blueprint containing the following:

  - 3 Firewall Zones.
  - 30 Firewall rules.
  - 10 Static NATs or port translations.
  - 1 Remote access VPN profile/policy.
  - Up to 2 LAN to LAN IPSec tunnels
  - 2 WANs with static routing and failover.
  - 2 Local user accounts.
  - Written Design Document
- Qty (2) - NGFW Design
  - Consisting of:
  - 1 Malware policies
  - 1 Basic IPS policies
  - 1 Web filtering policies
- Qty (2) - Additional NAT Design, per up to 10 additional NATs
  - Each quantity provides 10 additional NAT rules
- Qty (2) - Additional Security design, per 1 additional zone and up to 20 additional rules
  - Additional security rules for access control
  - Additional zone as specified for customer need DMZ, guest.
- Qty (2) - Additional Site To Site Tunnel/VPN
  - Business to Business IPSEC tunnels
- Qty (2) - Additional New Custom IPS Policy
  - Custom IPS policy development (per policy)
- Qty (2) - Design Additional Remote Access Policy
  - Client VPN remote access configuration - IP Pool - Policy
- Qty (2) - Design Advanced remote access VPN authentication with SAML or Single Sign-On (SSO)
  - Define groups
  - Define requirements
  - Define platform, protocol, and process
- Qty (2) - Design Advanced LAN routing (OSPF, EIGRP) Per Device/HA
  - Design interior routing protocol to establish dynamic route exchange with internal layer 3 devices
- Qty (2) - Design High-availability (Active/Standby)
  - Define required design elements for active/standby HA group
- Qty (2) - Design CISCO - FXOS chassis
  - define FXOS requirements
- Design User identity integration for filtering, per realm/Domain
  - Identify servers for connector service
  - Identify groups for inclusion/exclusion
  - Define directory type

- Document requirements and limitations
- Select mapping approach

Implement

Firewall Implementation

- Qty (2) - Firewall Base Configuration
    - Configuration of base design:
    - 3 zones
    - 30 security rules
    - 10 NAT rules
    - RA VPN
    - Base system config
- Qty (2) - Advanced remote access VPN authentication with SAML or Single Sign-On (SSO)
    - SAML integration for client VPN authentication.
- Qty (2) - Advanced LAN routing (OSPF, EIGRP) Per Device/HA
    - Configuration and implementation of standard LAN routing protocols, such as OSPF or EIGRP
- Qty (2) - High-availability (Active/Standby)
    - Configuration and implementation of Active/Passive firewall design
- Qty (2) - Additional Malware Services (Per Firewall/Pair)
    - Each Quantity represents 1 Malware & File policy.
    - Includes file types, threat level, archive scanning based on platform features and client requirements.
- Qty (2) - Additional URL Filtering (Per Firewall/Pair)
    - Each quantity represents 1 URL Filtering Policies based off of built in policy
    - (1) Custom Permit List
    - (1) Custom Deny List
- Qty (2) - CISCO - FXOS Chassis Configuration
    - Configure FXOS for Secure Firewall Platforms which require FXOS
    - Update FXOS Firmware
- Qty (2) - Additional Security rules configuration, configure up to 1 additional zone and 20 additional rules, according to design
    - Additional security rules for access control
    - Additional zone as specified for customer need e.g. DMZ, guest.
- Qty (2) - Additional NAT rule configuration, configure up to 10 additional NAT rules, according to design
    - Each quantity provides 10 additional NAT rules
- User identity integration for filtering, per realm or domain, up to 8 Domain Controllers or directory servers
    - Service to provide username to IP address mappings.
    - Includes deployment of agents, security accounts, groups, any GPO, or any additional logging configuration needed to provide user ID functionality.
- Qty (2) - IPS Tuning

  - Monitor and review IPS logs
  - Assist with the identification of false positives
  - Provide recommendations for IPS contents
  - Configure exclusions and exemptions as needed for proper business operation and security

Cutover and Post Support

Firewall Cutover and Post Support

- Qty (2) - Base Cutover and Post Support, single site
  - Cutover from existing firewall to new firewall
  - Includes cutover window as well as dedicated post support
- Administrative knowledge transfer, per 2 hour session
  - Sentinel will provide administrative knowledge transfer on the platform(s) as requested, including points of scale, common administrative tasks, and troubleshooting.

Out of Scope

Sentinel is responsible to perform only the Services described in this Statement of Work Agreement. Any additional services discussed or implied that are not defined explicitly by this SOW will be considered out of scope. All services requested outside of this SOW as detailed above will require a "Change Order" before any services are performed. "Change Order" must be agreed upon by all parties and signed. Specific examples from this project may be listed below.

- Resolution of current known issues has not been included in the scope of this proposal.
- Upgrades or downgrades of existing firewalls and FMC management server operating systems to different major versions has not been included in the scope of this proposal.
- Additional platforms or services that are not native to the firewall platform operating system
- User account creation
- Security group creation
- Directory maintenance
- Feature enhancements or software licenses for third party products (i.e. ISE, Anyconnect).
- Implementation or configuration of any local or external authentication system that is not otherwise specified in this scope of work.
- Routing configuration excludes, and at Sentinel's sole discretion, any significant or unrelated changes not directly related to this scope of work or for which Sentinel lacks access, visibility, or is owned by an entity not party to this agreement.
- Additional platforms or services that are not native to the firewall platform
- Remediation of malicious behavior identified on the network
- Identification and location of hosts that are indicated in security logs

Customer Responsibilities

To ensure the successful execution of this project, both Sentinel and the customer, acknowledge and agree to the following responsibilities. This section outlines the specific obligations and expectations that the Customer must fulfill throughout the duration of the project or engagement. It is imperative that the Customer's active participation, timely cooperation, and adherence to these responsibilities are vital to achieving the project's objectives and meeting mutually agreed-upon timelines.

- Procuring the necessary virtual resources for solution.
- Procuring any hardware required for the solution, unless otherwise stated.
- ISE-PIC licensing would be required
- Client to provide directory structure or backend database
- Customer is responsible for any acquisition and/or costs related to the purchasing of public IP space, BGP Autonmous System Numbers (ASN), third-party SSL certificates, domain names.
- Customer is responsible for any public DNS related tasks.
- Customer to provide directory structure or backend database compatible with the system being configured under this SOW.
- Remediation of malicious and/or false positive alerts

Key Assumptions

The successful execution of this project is contingent upon a set of key assumptions. These assumptions serve as reference points for the project's planning and execution. It is imperative that these assumptions are understood, acknowledged, and monitored throughout the project to ensure that the project proceeds as intended. Deviations from these assumptions may have an impact on project timelines, costs, and outcomes. The Key Assumptions are as follows:

- All work performed by Sentinel engineers and project managers will be performed remotely.
- User based identification or classification will integrate with an existing directory structure
- The customer provided directory is functional and is free of critical errors that would prevent successful user ID mapping
- Sentinel assumes that, and prior to project kickoff, customer already has a working external authentication system compatible with both the hardware being implemented and SAML/SSO, unless otherwise specified in this scope of work.
- Customer network is assumed to have a stable, error free routing protocol setup. Issues resulting from, or work required to remediate or troubleshoot, routing instabilities may require a change order.
- Systems under this SOW assume integration with an existing directory service.
- Directory is functional and free of critical errors that prevent successful user ID mapping
- IPS will begin in a monitor state and all findings will be resolved before moving to a blocking state.

Documentation and Knowledge Transfer

Sentinel will include:

- Documentation of the setup including a revised Sentinel design doc as well as any available vendor-created administrative and/or best practices guides.
- Knowledge transfer including basic functional overviews of products implemented, demonstrating the normal operations as installed in the Customer’s environment.
    - Note that knowledge transfer and functional overviews are not a substitute for formal vendor product Customer Education courses available. Sentinel strongly encourages attendance at Customer

Education classes to gain further insight into the product architecture and its integration.

Sentinel welcomes Customer to be involved in all aspects of the project life cycle to achieve the highest level of knowledge transfer during the project. While there is no way to guarantee the level of knowledge transfer that will occur, additional time can be added to the staging, installation or testing portions of the project to try and accomplish this need. This request should be scheduled with the Project Manager. If additional time is added for this request, it will be handled through Sentinel's Change Order process.

Customer's that seek to get the most out of the knowledge transfer have had a higher degree of success by combining the specific deployment knowledge transfer with formal course training. When the course work is done prior to the project knowledge transfer Sentinel has seen the highest degree of self support post installation. That knowledge transfer and functional overviews are not a substitute for formal vendor product Customer Education courses available. Sentinel strongly encourages attendance at Customer Education classes to gain further insight into the product architecture and its integration.

General Assumptions

The following is a list of responsibilities and/or tasks that Sentinel assumes have been completed or reviewed by Customer to the execution of the above-mentioned project. If additional responsibilities are uncovered during the project, Sentinel will make sure that Customer is made aware of any issues promptly to determine resolution.

Product Lead Times

Depending on the technologies quoted, orders may be direct or through distribution. Lead times should be expected to be 8 weeks but can exceed 8 weeks. Should expedited equipment requirements arise, there could be an additional charge to source through a warehousing distribution partner.

Remote Access

Sentinel's service estimate assumes remote access through IP VPN or IP PPP connection. Without this access, additional service charges may be incurred for optimization and tuning required pre and post installation.

Travel Requirements and Cost

Unless specified within the proposal, all travel expenses and time are not included. Travel time shall be invoiced at pre-negotiated rates and expenses plus per diem at actual costs.

3rd Party Integration

Unless noted otherwise, Sentinel assumes no reliance on 3rd Party applications, connections or plug-ins to software deployments and updates as specified in this scope. If during Analysis and Planning any required 3rd Party integration is uncovered, additional hours may be incurred.

Labor Union Requirements

Sentinel has NOT included any parameters for Union workers. Any requirement would require a subcontract arrangement to be determined up front and would increase the cost of deployment.

Managed Services

The applicable devices outlined within the Pricing Summary of this document will be added to the existing NOC Monitoring and Managed Services contract upon the conclusion of the project.

Statement of Work

Appendix A

-

This Appendix A is governed by the Master Services Agreement by and between Sentinel Technologies, Inc., (Contractor) with principal offices at 2550 Warrenville Road, Downers Grove, Illinois 60515, and J Sterling Morton High School District 201 with principal offices at 5801 W Cermak Rd Cicero, IL 60804-2102.

New Cisco Firewall

Prepared by:

Sentinel Technologies, Inc

Kyle Donnelly
kdonnelly@sentinel.com

Prepared for:

J Sterling Morton High School District 201

5801 W Cermak Rd
Cicero, IL 60804-2102
Artur Wilczynski
+17087802126
awilczynski@jsmorton.org

Contract Information:

Budgetary Proposal # 022848

Version: 8
Delivery Date: 09/30/2025
Expiration Date: 08/02/2025

Quote Summary

Description	Amount
Cisco Secure Firewall 3120	$382,386.24
Professional Services	$53,824.00
Contingency Recommendation	$19,119.00
Total:	**$455,329.24**

Taxes, shipping, handling and other fees may apply. We reserve the right to cancel orders arising from pricing or other errors.

Terms and Conditions

By signing below, Customer agrees that the products and services being purchased through this contract are subject to the Sentinel Technologies Terms and Conditions, as applicable, located at https://sentinel.com/Terms-and-Conditions unless expressly provided herein or otherwise addressed in a separate Agreement between the parties.

Invoice Terms

Hardware: Upon Shipment (50% down if over $100K)

Subscription/License: At the beginning of the contract - In Full

Paragon Micro

PO Box 775695
Chicago IL 60677-5695

PARAGON MICRO
EXPERIENCE THAT KEEPS IT EASY.

Quote Q5232277

Date:	Expires:
9/29/2025	10/29/2025

Sales Rep

Marty, Mangan
847 719 7199
mmangan@paragonmicro.com

DUNS: 800436714
TIN: 20-0144408
CAGE CODE: 4ZHT8

Customer Contact

Contact: Beisman, Keith
Account: 98602143
PO#:
Phone: 7087802800
Email: kbeisman@jsmorton.org

Bill To:

J. Sterling Morton
Keith Beisman
5801 W. Cermak Rd
Cicero IL 60804

Ship To:

J. Sterling Morton
Keith Beisman
5801 W. Cermak Rd
Cicero IL 60804

Quote Name	Terms	Cost Center
Cisco 3120		

External Notes

Qty	MPN	Description	Notes	Unit Price	Total
4	FPR3120-NGFW-K9	Cisco FirePOWER 3120 Next-Generation Firewall - Firewall - 10GbE - front to back airflow - 1U - rack-mountable		27,288.60	109,154.40
4	CON-SNT-FPR3120N	Cisco Smart Net Total Care - Extended service agreement - replacement - 8x5 - response time: NBD - for P/N: FPR3120-NGFW-K9		15,272.82	61,091.28
4	L-FPR3120T-TMC-5Y	Cisco Threat Defense Threat, Malware and URL - Subscription license (5 years) - 1 appliance - ESD		78,065.47	312,261.88
4	FPR3K-PWR-AC-400	Cisco - Power supply (plug-in module) - AC - 400 Watt - for P/N: FPR3105-ASA-K9, FPR3105-NGFW-K9, FPR3120-ASA-K9, FPR3130-NGFW-K9, FPR3140-ASA-K9		1,791.23	7,164.92

Subtotal	489,672.48
Shipping Cost (FedEx Ground® (2-5 Business Days))	0.00
Tax Total	34,286.50
Total	$523,958.98

We value your business and will continue to provide you with excellent service in addition to our comprehensive product line.

SALES TAXES ARE ESTIMATED and may change depending on the rates levied by the destination's tax jurisdiction at the time of invoicing. Finalized invoice will be sent by Paragon Micro's Accounting Department.

PRICING AND INFORMATION DISCLAIMER: All pricing is subject to change without notice. For all prices, products and offers, Paragon Micro, Inc. reserves the right to make adjustments due to changing market conditions, product discontinuation, manufacturer price changes, errors in advertisements and other extenuating circumstances. While Paragon Micro, Inc. uses reasonable efforts to include accurate and up-to-date information on the Site, Paragon Micro, Inc. makes no warranties or representations as to the Site's accuracy. Paragon Micro, Inc. assumes no liability or responsibility for any errors or omissions in the content on the Site.

Accepted By: Printed Name

Purchase Order #

Authorized Signature

Date

DATA CENTER WAREHOUSE

[illegible] Avenida De La Carlota, Suite [illegible]
Laguna Hills, CA 92653
Phone: (732) 491-8997

Number: **Q-138665**

Date: **09/24/2025**

Bill To:
Keith Beisman
J Sterling Morton High School District 201
2400 Home Ave
Berwyn, IL 60402
Phone: (708)780-2800
Email: kbeisman@jsmorton.org

Ship To:
Keith Beisman
J Sterling Morton High School District 201
2400 Home Ave
Berwyn, IL 60402
Phone: (708)780-2800
Email: kbeisman@jsmorton.org

Item #	Mfr. Part	Description	Price	Qty.	Extended
*1	FPR3120-NGFW-K9	Cisco 3120 Network Security/Firewall Appliance - 16 Port - 10/100/1000Base-T, 1000Base-T - 10 Gigabit Ethernet - 21 Gbit/s Firewall Throughput - 6000 VPN - 8 x RJ-45 - 8 Total Expansion Slots - 50 Hz, 60 Hz - 1U - Rack-mountable **Mfr: CISCO SYSTEMS, INC**	$ 27,265.00	4	**$ 109,060.00**
*2	CON-SNT-FPR3120N	Cisco Smart Net Total Care - Extended Service - Service - 8 x 5 x Next Business Day - Exchange - Parts **Mfr: CISCO SYSTEMS, INC**	$ 19,019.00	4	**$ 76,076.00**
*3	L-FPR3120T-TMC-5Y	Cisco Threat Defense Threat, Malware and URL - Subscription License - 1 Appliance - 5 Year - Available via Electronic **Mfr: CISCO SYSTEMS, INC**	$ 77,995.00	4	**$ 311,980.00**
*4	FPR3K-PWR-AC-400	Cisco 400W Power Supply **Mfr: CISCO SYSTEMS, INC**	$ 1,789.00	4	**$ 7,156.00**
		4 item(s)		**Sub-Total**	**$ 504,272.00**
				Freight	**$ 0.00**
				Tax	**$ 0.00**
				Total	**$ 504,272.00**

(*) Tax exempted Part(s)

Quote Valid Until: 10/24/2025

Payment Details

Credit Card [VISA # Expires On:]

Shipping and Delivery Details

Shipping via: FEDEX Ground

Terms and Conditions

This quote is based on current duty and tax rates. Any increases in duties, tariffs, or related government-imposed fees after this quote but before the order date shall be the sole responsibility of customer.

Please visit http://datacenterwarehouse.com/terms-and-conditions/ for terms and conditions.

Prepared by: **Steve Squires** Email: **Steve.Squires@4dcw.com** Phone: **(732) 491-8997**