Secure Firewall

(formerly Firepower)

Cisco Partner
https://cs.co/1page

Cisco **Secure Firewall** prevents breaches and can quickly detect and mitigate stealthy attacks using deep visibility and the most advanced security capabilities of any firewall available today – all while maintaining optimal network performance and uptime.

Discovery Questions:

- What is your current firewall strategy: internet edge, remote locations, cloud, data center?
- Are you facing performance issues with your current firewall appliances when using multiple security features, inspecting encrypted traffic, IPS or logging and NAT are enabled?
- Do your existing security products work together to share threat intelligence?
- Are your existing NGFW solutions and other security products tightly integrated with your routers, switches, and other network devices?

Key Features:

License:

Standard Firewall Features: Include traditional firewall functions such as stateful port & protocol inspection, Network Address Translation (NAT), and Virtual Private Network (VPN). — ESS

Application Visibility & Control (AVC): Thousands of applications supported, control custom apps with *OpenAppID*, Geolocations, users, and websites. — ESS

GeoLocation: Control traffic based on its source or destination country or continent. — ESS

Next-Generation Intrusion Prevention System (NGIPS): Snort 3 IPS can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC). — IPS

Security Intelligence: Early opportunity to drop unwanted traffic based on IP or destination URL (e.g. *Botnet*, *CnC*, *Exploit Kits*, *Spam, Phishing* etc.) as defined and updated by ***Talos***. — IPS

Impact Flags: For each intrusion event, the system adds an impact level to correlation between intrusion data, network discovery data, and vulnerability information. Impact flags score the relevance of an attack based on the vulnerability of the device. — IPS

Recommended Rules: Automated recommendations within Secure Firewall - Intrusion Prevention that can enable/disable rules based on OS, applications & protocols observed passively. This greatly reduces false positive and false negative events. — IPS

Encrypted Visibility Engine (EVE): Detect OS, applications and threats within encrypted packet without decryption. Can be used to apply to policies based on detection. — IPS

Malware Defense for Networks: Detection, blocking, tracking, analysis, & remediation to protect the enterprise against targeted persistent malware attacks. — MAL

Reputation and category-based URL filtering: Alerting and control over suspect web traffic. Enforces policies on hundreds of millions of URLs in more than 80 categories. — URL

Multi-Threaded Architecture: More capable of handling high-throughput single-flow traffic. — IPS

Licenses:

NOTE: Essentials = Base | IPS = Threat

- ESS **Essentials:** Switch/Route (DHCP, NAT), HA, Clustering, User/App control, GeoDB, TLS decrypt
- IPS **IPS:** Intrusion Detection/Prevention, File control, Security Intelligence, EVE, TLS 1.3 decrypt
- MAL **Malware Defense:** Malware Defense, Malware Analytics, File Storage
- URL **URL:** Category & Reputation-based URL filtering

Secure Firewall Series:

Virtual (NGFWv) - Public & Private cloud:

- Optimized for cloud and data center environments
- AWS, Azure, and Azure government cloud
- 1.2 Gbps throughput firewall + AVC, 1.1 Gbps throughput AVC + IPS

Secure Firewall Cloud Native:

- Kubernetes-based for scalable and resilient cloud-native security
- Multi-tenant remote access with massive throughput potential

1000 Series: (890 Mbps – 5.3 Gbps) [1]

1200 Series: (1.7 Gbps – 6.5 Gbps) [1] Coming soon!

- Desktop (1210 & 1220)
- Rack Mount (1230, 1240, 1250 & 1260)
- Fully integrated System-on-a-Chip (SOC)

2100 Series: (2.6 Gbps – 10.4 Gbps) [1]

- For Internet edge to DC environments

3100 Series: (10 Gbps – 45 Gbps) [1]

- For Internet edge to DC environments
- VPN crypto h/w accelerators

4100 Series: (16.5 Gbps – 153 Gbps) [1]

- Internet edge, DC & high-performance
- DDoS mitigation capabilities

4200 Series: (50 Gbps – 200 Gbps) [1]

- Internet edge, DC & high-performance
- VPN crypto h/w accelerators

9300 Series: (55 Gbps – 190 Gbps) [1]

- For service provider, data center
- DDoS mitigation capabilities
- 1.2 Tbps clustered throughput

[1] Throughput based on Threat Defense software

Management Options:

Firewall Management Center (FMC): Hardware or Virtual appliance for visibility and management for Cisco Secure Firewall and NGIPS.

Firewall Device Manager (FDM): A web-based local on-box manager to provide firewall management.

Cisco Defense Orchestrator (CDO): Cloud-based management solution to manage security policies and configurations for multiple platforms including Secure Firewall, ASA, Meraki MX and more. (SKU: **CDO-SEC-SUB**)

Cloud Delivered Firewall Management Center (cdFMC): SaaS Mgmt. built within CDO which includes feature parity across Cloud, On-Prem and Hybrid deployments.

Resources:

SalesConnect
Ordering Guide
Configuration Guides
At-a-Glance
Feature Matrix
Firewall Essentials
FW Performance Estimator
Log Estimator Tool
Security Analytics & Logging
Firewall Migration Tool
Cisco Defense Orchestrator
FMC New Features
YouTube Channel
Secure Firewall FAQ
Firestarter
AppID Portal
Public page

Example SKU: ***FPR9K-FTD-BUN***