

FPR9300-NGFW-K9

3RU carrier-grade modular chassis with 3 security-module bays; up to 3x SM-56 delivering 190 Gbps FW+AVC, 190 Gbps NGIPS, 110 Gbps IPsec, 60M sessions, 1100K CPS, 60K VPN peers; series EOL announced.

Cisco Firepower 9300 Series - Carrier-Grade Modular Security Platform

Note on ordering: the Cisco official ordering model for the Firepower 9300 Series is chassis + security modules (e.g., FPR-C9300-AC + FPR9K-SM-56). The FPR9300-NGFW-K9 code is a non-official shorthand used by some third-party resellers. The 9300 is a 3-RU carrier-grade modular security platform for service-provider, large data center, and campus-perimeter deployments. Up to three security modules per chassis and up to 16 chassis per cluster. The platform ships with a Cisco Firepower 9000 Supervisor providing 8x 10G Ethernet ports plus 2 network-module slots, plus 4 hot-swap fan trays. The 9300 series was announced End-of-Life on 2025-09-30; End-of-Sale 2026-03-31; support until 2031-03-31.

Specification	Value
Series / role	Cisco Firepower 9300 (carrier-grade modular)
Form factor	3 RU, 19-in square-hole rack
Security module bays	3 per chassis
Supervisor	Cisco Firepower 9000 Supervisor with 8x 10G Ethernet + 2 NM slots
Clustering	Up to 16 chassis
Per-SM-56 FW+AVC	70 Gbps (FTD) / 68 Gbps (NGIPS) / 73 Gbps (NGIPS-datasheet)
Per-SM-56 IPsec	36 Gbps (FTD)
Per-SM-56 sessions / CPS / peers	35M / 490K / 20K
3xSM-56 FW+AVC (full chassis)	190 Gbps
3xSM-56 IPsec (full chassis)	110 Gbps
3xSM-56 sessions / CPS (full chassis)	60M / 1.1M
SSL / TLS throughput	12 Gbps per SM-56; 28 Gbps for 3x SM-56
Flash / SSD	Per SM: RAID-1 NVMe (1.6 TB per SM-56; up to 4.8 TB per chassis)
Power supply	AC / DC / HVDC options; up to 2500 W per PSU; 1+1 redundant
Status	EOL announced 2025-09-30 (support through 2031-03-31)

- 3-RU carrier-grade modular security platform; 3 security module bays per chassis.
- Up to 3x FPR9K-SM-56 (or legacy SM-24/36/44) security modules per chassis.
- 3x SM-56 delivers up to 190 Gbps FW+AVC, 110 Gbps IPsec, 60M concurrent sessions.
- 8x 10G supervisor ports + 2 NM slots (8x10G / 4x40G / 2x100G options).
- Cluster up to 16 chassis; multi-instance support per module.

- End-of-Life announced 2025-09-30; support through 2031-03-31.

Performance depends on which security modules are installed. The official modules are FPR9K-SM-24/36/44 (legacy) and FPR9K-SM-40/48/56 (current). Numbers below are per-SM-56 unless noted.

Specification	FPR9300 (with 3x SM-56 / single-SM-56)
Firewall FW+AVC (per SM-56)	70 Gbps
Firewall FW+AVC (3x SM-56)	190 Gbps
NGIPS (per SM-56)	68 Gbps
NGIPS (3x SM-56)	190 Gbps
IPsec VPN (per SM-56)	36 Gbps
IPsec VPN (3x SM-56)	110 Gbps
TLS / SSL throughput (per SM-56)	12 Gbps
TLS / SSL throughput (3x SM-56)	28 Gbps
Concurrent sessions (per SM-56)	35 million
Concurrent sessions (3x SM-56)	60 million
New connections / sec (per SM-56)	490,000
New connections / sec (3x SM-56)	1,100,000
Max VPN peers (per SM-56)	20,000
Max VPN peers (3x SM-56)	60,000
Clustering	Up to 16 chassis

Component	Specification
Chassis dimensions (H x W x D)	5.25 x 17.5 x 32 in (13.3 x 44.5 x 81.3 cm)
Weight (1 SM)	105 lb (47.7 kg)
Weight (fully configured)	135 lb (61.2 kg)
Security modules per chassis	3
Network modules	8x10G SFP+; 4x40G QSFP+; 2x100G QSFP28; 6x10G SR/LR FTW; 2x40G SR FTW
Supervisor mgmt	1x 1G copper mgmt + 1x RJ-45 console + 1x USB 2.0
Power supply	AC / DC / HVDC options; up to 2500 W per PSU; 1+1 redundant
AC input	200-240 VAC (AC)
DC input	-40 to -60 VDC (DC)

Component	Specification
HVDC input	240-380 V HVDC
Fans	4 hot-swappable; 75.5 dBA at max fan speed
Storage (per SM-56)	Up to 1.6 TB RAID-1 NVMe per SM (4.8 TB per chassis max)

Property	Value
Form factor	3 RU rack-mount (19-in square-hole)
Operating temperature (SM-40/SM-48)	0 to 40 C up to 10,000 ft
Operating temperature (SM-56)	0 to 35 C at sea level (-1 C per 1000 ft)
Storage temperature	-40 to 65 C
Storage altitude	Up to 40,000 ft
Operating humidity	5 to 95% non-condensing
NEBS	NEBS-compliant with SM-40 and SM-48 modules
MTBF	Not published in official datasheet

The platform runs Cisco Secure Firewall Threat Defense (FTD) image by default with Snort 3 detection engine. The capabilities below are supported through the FTD software.

Capability	Description
Stateful firewall	Layer 3/4 stateful inspection with zones, interfaces, and ACLs
NGFW / Application visibility	Application Visibility and Control (AVC) with NBAR2/L7 inspection
Intrusion prevention (IPS)	Cisco Talos-backed signatures; Snort 3 with custom rule sets
URL filtering	Categorical and reputation-based URL filtering (Cisco Talos cloud)
Advanced Malware Protection	Cisco AMP / AMP Threat Grid sandbox integration
TLS / SSL inspection	Inline decryption for threat inspection (where licensed)
Cisco Umbrella integration	DNS-layer security via Cisco Umbrella SIG (where licensed)
DNS layer security	DNS-layer policy and threat enforcement
VPN (site-to-site, RA)	IPsec / IKEv2 / DTLS; hub-spoke and remote-access VPN
High availability	Active/active and active/standby failover pairs (where supported)
Clustering	Multi-chassis clustering for carrier-class scale (where supported)
Management planes	FMC (central), CDO (cloud), local management (platform capable)

The platform runs Cisco Secure Firewall Threat Defense (FTD) software. Key software capabilities and their operational role are summarized below.

Feature	Role
Snort 3 engine	Multi-threaded next-gen IPS with Talos signature feed
Application Visibility (AVC)	L7 application recognition and policy enforcement
URL filtering	Category / reputation based URL control
Advanced Malware Protection (AMP)	File / malware inspection and threat grid sandboxing
TLS / SSL inspection	Inline decryption for encrypted-threat visibility
Stateful firewall	Zone-based stateful inspection and NAT
DNS security (Umbrella)	DNS-layer policy via Cisco Umbrella integration
Multi-instance (VDC)	Virtual firewall instances on one chassis (where supported)
Management	FMC central, CDO cloud, REST API / NETCONF-YANG
Reporting	FMC dashboards, syslog / CEF to SIEM
Auto-update	Talos signature and rule auto-update
Policy automation	REST API and templates for orchestration

Cisco Secure Firewall (FTD) platforms support several deployment modes to fit the network topology. The mode is chosen at initial configuration and managed centrally via FMC or CDO.

Mode / Configuration	Description
Routed firewall	Layer-3 routed interfaces with zones and inter-zone policies
Transparent (bump-in-the-wire)	Layer-2 bridge groups for inline insertion without renumbering
Inline IPS / IDS	Inline pair or passive IDS using the IPS interfaces (Snort 3)
Multi-instance	Virtual firewalls on one appliance (FTD multi-instance, where supported)
High availability	Active/standby or active/active stateful failover pairs
Clustering	Multi-chassis clustering up to 16 chassis (where supported)
Zero-touch deployment	PnP / ZTP enrollment via Cisco Defense Orchestrator
VPN	Site-to-site, remote-access (RA) VPN, hub-spoke topologies
Interface redundancy	Redundant / EtherChannel interface groups
Fail-to-wire	Inline security modules with fail-open bypass (where supported)
AVC / NBAR	Application-aware policies and per-application visibility
TLS decryption	Inline SSL/TLS inspection policies (where licensed)

Cisco Secure Firewall platforms support a rich set of operational and high-availability features to keep threat defense active and policy-driven in production deployments.

Capability	Description
Active/standby failover	Stateful failover with configuration and session sync

Capability	Description
Active/active failover	Active/active failover for data center deployments (where supported)
Multi-chassis clustering	Up to 16 chassis cluster for carrier-class scale (where supported)
Zero-touch provisioning	PnP and ZTP through the Cisco Defense Orchestrator
Smart licensing	Cisco Smart Licensing with PnP enrollment and offline reservation
REST API	Full REST API for automation and policy orchestration
NETCONF/YANG	NETCONF / YANG models for FTD configuration and telemetry
Syslog / SIEM	Syslog export and CEF-format delivery to SIEM collectors
Threat intelligence	Cisco Talos automatic signature feed; Snort 3 rule updates
Sandboxing	Cisco AMP Threat Grid sandbox integration
Encrypted traffic analytics	ETA on supported platforms (where licensed)
Backup / restore	FMC-managed configuration and policy backup / restore

The chassis supports a range of fixed and modular network interfaces through the available network-module bays for FPR9300-NGFW-K9.

Module / Accessory	Description
Network modules (1G/10G/25G)	NM with 8x1/10/25G SFP+ ports (platform dependent)
Network modules (40G/100G)	NM with 4x40G QSFP+ or 2x100G QSFP28 ports (platform dependent)
Fail-to-wire (FTW) modules	FTW 8x1G copper or 6x10G/25G SR/LR fiber network modules
SFP / SFP+ optics	GLC-T (1G copper), GLC-SX-MMD / -LX-SMD (1G SX/LX); SFP-10G-SR/LR
SFP28 25G optics	SFP-25G-SR-S, SFP-25G-LR-S (where 25G ports available)
QSFP / QSFP28 optics	QSFP-40G-SR4/LR4; QSFP-100G-SR4-S / -LR4-S (where 100G available)
Power supply	AC 400W / 1900W PSU (platform dependent); DC options where available
Spare fan tray	Hot-swappable fan module (FRU) for field replacement
Console / management	RJ-45 console cable included for local management
Rack-mount kit	Standard 19-in four-post EIA-310-D rack-mount brackets included
Cisco Defense Orchestrator	Cloud-based management subscription for centralized policy
FMC license	Firewall Management Center feature license tier (per-platform)

The platform complies with the following interoperability, safety and environmental standards. Compliance is verified by independent testing laboratories.

Category	Standard
IPsec / VPN	RFC 4303 ESP, RFC 7296 IKEv2, RFC 5246 TLS 1.2, RFC 8446 TLS 1.3, AES-GCM

Category	Standard
IP routing	RFC 1812 IPv4, RFC 4291 IPv6; OSPFv2/v3, IS-IS, BGP-4, MP-BGP, static
High availability	Active/active and active/standby failover; multi-chassis clustering
Threat intelligence	Cisco Talos signature feeds and sandbox integration
DNS / URL filtering	Cisco Umbrella DNS-layer; URL reputation feed (Talos)
Management	REST API, NETCONF/YANG (FTD), SNMPv2c/v3, FMC/CDO central management
Quality of Service	802.1p, DSCP (RFC 2474), RFC 2597/2598 PHB
Safety	UL/CSA/IEC/EN 62368-1, IEC 60950-1, AS/NZS 62368-1, GB4943
EMC / EMI	FCC 47 CFR Part 15 Class A, EN 55032/CISPR 32, EN 55024/55035, EN 300 386
Environmental	RoHS 2011/65/EU, WEEE 2012/19/EU; NEBS Level-3 where indicated

The platform runs Cisco Secure Firewall Threat Defense (FTD) image by default with Snort 3 detection engine. The capabilities below are supported through the FTD software.

Capability	Description
Stateful firewall	Layer 3/4 stateful inspection with zones, interfaces, and ACLs
NGFW / Application visibility	Application Visibility and Control (AVC) with NBAR2/L7 inspection
Intrusion prevention (IPS)	Cisco Talos-backed signatures; Snort 3 with custom rule sets
URL filtering	Categorical and reputation-based URL filtering (Cisco Talos cloud)
Advanced Malware Protection	Cisco AMP / AMP Threat Grid sandbox integration
TLS / SSL inspection	Inline decryption for threat inspection (where licensed)
Cisco Umbrella integration	DNS-layer security via Cisco Umbrella SIG (where licensed)
DNS layer security	DNS-layer policy and threat enforcement
VPN (site-to-site, RA)	IPsec / IKEv2 / DTLS; hub-spoke and remote-access VPN
High availability	Active/active and active/standby failover pairs (where supported)
Clustering	Multi-chassis clustering for carrier-class scale (where supported)
Management planes	FMC (central), CDO (cloud), local management (platform capable)

The platform runs Cisco Secure Firewall Threat Defense (FTD) software. Key software capabilities and their operational role are summarized below.

Feature	Role
Snort 3 engine	Multi-threaded next-gen IPS with Talos signature feed
Application Visibility (AVC)	L7 application recognition and policy enforcement
URL filtering	Category / reputation based URL control

Feature	Role
Advanced Malware Protection (AMP)	File / malware inspection and threat grid sandboxing
TLS / SSL inspection	Inline decryption for encrypted-threat visibility
Stateful firewall	Zone-based stateful inspection and NAT
DNS security (Umbrella)	DNS-layer policy via Cisco Umbrella integration
Multi-instance (VDC)	Virtual firewall instances on one chassis (where supported)
Management	FMC central, CDO cloud, REST API / NETCONF-YANG
Reporting	FMC dashboards, syslog / CEF to SIEM
Auto-update	Talos signature and rule auto-update
Policy automation	REST API and templates for orchestration

Cisco Secure Firewall (FTD) platforms support several deployment modes to fit the network topology. The mode is chosen at initial configuration and managed centrally via FMC or CDO.

Mode / Configuration	Description
Routed firewall	Layer-3 routed interfaces with zones and inter-zone policies
Transparent (bump-in-the-wire)	Layer-2 bridge groups for inline insertion without renumbering
Inline IPS / IDS	Inline pair or passive IDS using the IPS interfaces (Snort 3)
Multi-instance	Virtual firewalls on one appliance (FTD multi-instance, where supported)
High availability	Active/standby or active/active stateful failover pairs
Clustering	Multi-chassis clustering up to 16 chassis (where supported)
Zero-touch deployment	PnP / ZTP enrollment via Cisco Defense Orchestrator
VPN	Site-to-site, remote-access (RA) VPN, hub-spoke topologies
Interface redundancy	Redundant / EtherChannel interface groups
Fail-to-wire	Inline security modules with fail-open bypass (where supported)
AVC / NBAR	Application-aware policies and per-application visibility
TLS decryption	Inline SSL/TLS inspection policies (where licensed)

Cisco Secure Firewall platforms support a rich set of operational and high-availability features to keep threat defense active and policy-driven in production deployments.

Capability	Description
Active/standby failover	Stateful failover with configuration and session sync
Active/active failover	Active/active failover for data center deployments (where supported)
Multi-chassis clustering	Up to 16 chassis cluster for carrier-class scale (where supported)
Zero-touch provisioning	PnP and ZTP through the Cisco Defense Orchestrator

Capability	Description
Smart licensing	Cisco Smart Licensing with PnP enrollment and offline reservation
REST API	Full REST API for automation and policy orchestration
NETCONF/YANG	NETCONF / YANG models for FTD configuration and telemetry
Syslog / SIEM	Syslog export and CEF-format delivery to SIEM collectors
Threat intelligence	Cisco Talos automatic signature feed; Snort 3 rule updates
Sandboxing	Cisco AMP Threat Grid sandbox integration
Encrypted traffic analytics	ETA on supported platforms (where licensed)
Backup / restore	FMC-managed configuration and policy backup / restore

The chassis supports a range of fixed and modular network interfaces through the available network-module bays for FPR9300-NGFW-K9.

Module / Accessory	Description
Network modules (1G/10G/25G)	NM with 8x1/10/25G SFP+ ports (platform dependent)
Network modules (40G/100G)	NM with 4x40G QSFP+ or 2x100G QSFP28 ports (platform dependent)
Fail-to-wire (FTW) modules	FTW 8x1G copper or 6x10G/25G SR/LR fiber network modules
SFP / SFP+ optics	GLC-T (1G copper), GLC-SX-MMD / -LX-SMD (1G SX/LX); SFP-10G-SR/LR
SFP28 25G optics	SFP-25G-SR-S, SFP-25G-LR-S (where 25G ports available)
QSFP / QSFP28 optics	QSFP-40G-SR4/LR4; QSFP-100G-SR4-S / -LR4-S (where 100G available)
Power supply	AC 400W / 1900W PSU (platform dependent); DC options where available
Spare fan tray	Hot-swappable fan module (FRU) for field replacement
Console / management	RJ-45 console cable included for local management
Rack-mount kit	Standard 19-in four-post EIA-310-D rack-mount brackets included
Cisco Defense Orchestrator	Cloud-based management subscription for centralized policy
FMC license	Firewall Management Center feature license tier (per-platform)

The platform complies with the following interoperability, safety and environmental standards. Compliance is verified by independent testing laboratories.

Category	Standard
IPsec / VPN	RFC 4303 ESP, RFC 7296 IKEv2, RFC 5246 TLS 1.2, RFC 8446 TLS 1.3, AES-GCM
IP routing	RFC 1812 IPv4, RFC 4291 IPv6; OSPFv2/v3, IS-IS, BGP-4, MP-BGP, static
High availability	Active/active and active/standby failover; multi-chassis clustering
Threat intelligence	Cisco Talos signature feeds and sandbox integration

Category	Standard
DNS / URL filtering	Cisco Umbrella DNS-layer; URL reputation feed (Talos)
Management	REST API, NETCONF/YANG (FTD), SNMPv2c/v3, FMC/CDO central management
Quality of Service	802.1p, DSCP (RFC 2474), RFC 2597/2598 PHB
Safety	UL/CSA/IEC/EN 62368-1, IEC 60950-1, AS/NZS 62368-1, GB4943
EMC / EMI	FCC 47 CFR Part 15 Class A, EN 55032/CISPR 32, EN 55024/55035, EN 300 386
Environmental	RoHS 2011/65/EU, WEEE 2012/19/EU; NEBS Level-3 where indicated