

## FPR3105-NGFW-K9

1RU entry-level Secure Firewall 3105; 8x 1GE RJ45 + 8x 1/10G SFP+ + 1 NM bay; 10 Gbps FW+AVC, Snort 3, FTD software.

Cisco Secure Firewall 3105 Appliance - Threat Defense

The Cisco Secure Firewall 3105 is the entry-level model of the Secure Firewall 3100 Series, providing up to 10 Gbps of firewall + AVC throughput and up to 10 Gbps of NGIPS throughput. It ships with 8 fixed 10/100/1000 RJ-45 ports plus 8 fixed 1/10G SFP+ ports, plus a single network module (NM) bay for additional 1/10G modules. The platform runs Cisco Secure Firewall Threat Defense (FTD) or ASA software and is managed via Firewall Management Center (FMC), Cisco Defense Orchestrator (CDO), or on-device management. The 3105 does not support clustering.

| Specification                       | Value                                                              |
|-------------------------------------|--------------------------------------------------------------------|
| Series / role                       | Cisco Secure Firewall 3105 (entry 1RU)                             |
| Fixed network ports                 | 8x 10/100/1000Base-T RJ-45 + 8x 1/10G SFP+                         |
| Network module bay                  | 1 (8x1/10G SFP+ / 8x1G FTW / 6x1G FTW / 6x10G FTW options)         |
| Management ports                    | 1x 1/10G SFP + 1x RJ-45 console + 1x USB 3.1                       |
| Firewall throughput (FW+AVC, 1024B) | 10 Gbps                                                            |
| NGIPS throughput                    | 10 Gbps                                                            |
| IPsec VPN (1024B TCP Fastpath)      | 5.5 Gbps                                                           |
| New connections / sec (FTD)         | 90,000                                                             |
| Concurrent sessions                 | 1.5 million (with AVC)                                             |
| Max VPN peers                       | 2,000                                                              |
| TLS throughput                      | 3.2 Gbps                                                           |
| DRAM / SSD                          | 64 GB / 1x 900 GB NVMe (slot1; optional RAID1)                     |
| Power supply                        | 1x 400W AC ship (1+1 with second 400W AC/DC PSU)                   |
| Warranty                            | Standard Cisco hardware warranty (extendable via service contract) |

- Entry-level 1RU Secure Firewall with 10 Gbps FW+AVC throughput.
- 8 fixed 1G RJ-45 + 8 fixed 1/10G SFP+ ports plus a single NM bay for 1/10G modules.
- Runs Cisco FTD (Snort 3) or ASA software - managed via FMC, CDO, or on-device.
- Up to 1.5 million concurrent sessions and 90,000 new connections/sec.
- Single 400W AC PSU ships by default; second PSU optional for redundancy.

| Specification                   | FPR3105-NGFW-K9 |
|---------------------------------|-----------------|
| Firewall (FW+AVC, 1024B)        | 10 Gbps         |
| NGIPS / IPS (FW+AVC+IPS, 1024B) | 10 Gbps         |
| IPsec VPN (1024B TCP Fastpath)  | 5.5 Gbps        |
| New connections / sec (FTD)     | 90,000          |
| Concurrent sessions (with AVC)  | 1.5 million     |
| Max VPN peers                   | 2,000           |
| TLS throughput                  | 3.2 Gbps        |
| Clustering                      | Not supported   |

| Component              | Specification                                                 |
|------------------------|---------------------------------------------------------------|
| Fixed network ports    | 8x 1G RJ-45 + 8x 1/10G SFP+                                   |
| Network module bay     | 1                                                             |
| Network module options | 8x1/10G SFP+ (FPR3K-XNM-8X10G); 8x1G FTW; 6x1G FTW; 6x10G FTW |
| Management port        | 1x 1/10G SFP                                                  |
| Console port           | 1x RJ-45                                                      |
| USB                    | 1x USB 3.1 Type-A                                             |
| CPU / DRAM             | Not published / 64 GB                                         |
| Flash / SSD            | 2x NVMe slots; ships with 1x 900 GB SSD (slot 1)              |
| Power supply           | 1x 400W AC ships; second 400W AC or DC optional               |
| AC input               | 100-240 VAC                                                   |
| Weight                 | 23 lb (10.5 kg)                                               |

| Property               | Value                                                                   |
|------------------------|-------------------------------------------------------------------------|
| Form factor            | 1 RU rack-mount (optional 2-post brackets/slide rails; desktop capable) |
| Operating temperature  | 0 to 40 C (32 to 104 F)                                                 |
| Storage temperature    | -20 to 65 C                                                             |
| Operating humidity     | 10 to 85% non-condensing                                                |
| Storage humidity       | 5 to 95% non-condensing                                                 |
| Dimensions (H x W x D) | 1.75 x 17 x 20 in (4.4 x 43.3 x 50.8 cm)                                |
| 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                |
| 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 FPR3105-NGFW-K9.

| Module / Accessory           | Description                                        |
|------------------------------|----------------------------------------------------|
| Network modules (1G/10G/25G) | NM with 8x1/10/25G SFP+ ports (platform dependent) |

| Module / Accessory         | Description                                                          |
|----------------------------|----------------------------------------------------------------------|
| 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                       |
| 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      |

| Capability                  | Description                                                        |
|-----------------------------|--------------------------------------------------------------------|
| 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) |

| Mode / Configuration  | Description                                                     |
|-----------------------|-----------------------------------------------------------------|
| 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                   |
| 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 FPR3105-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)            |

| Module / Accessory         | Description                                                          |
|----------------------------|----------------------------------------------------------------------|
| 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                       |
| 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            |