ML-Powered NGFWs for 5G

Powered by PAN-OS®, ML-Powered Next-Generation Firewalls for 5G offer the most granular visibility and control for your emerging 5G cybersecurity challenges. ML-Powered 5G security comprises all PA-5200 Series and PA-7000 Series[1] hardware firewalls, as well as VM-Series virtual and CN-Series container firewalls.

Organizations need 5G security powered by machine learning (ML) to maintain the speed of business. 5G promises transformative mobility through enhanced mobile broadband experiences and industrial digitalization through customer value creation. 5G networks enable new enterprise use cases not previously possible, such as industrial-scale Internet of Things (IoT) networks with ultra-low latency, mission-critical reliability, and a high degree of mobility. Yet cyberattacks can take advantage of the speed and volume of 5G traffic, which creates new challenges for security teams.

Designed to handle growing throughput needs due to increasing amounts of application-, user-, and device-generated data, our ML-Powered NGFWs offer high performance and threat prevention capabilities to stop advanced cyberattacks and ensure business continuity.

[1] Requires a 100 Gbps Network Processing Card (NPC) as well as the second-generation Switch Management Card (SMC) and Log Forwarding Card introduced with PAN-OS 9.0 software.

Key Security Features

Granular Visibility and Control

- Complete visibility across all layers, including signaling, data, and control plane, with application-layer visibility in a mobile network.
- 5G network slice security that helps unlock new revenue streams for service providers to offer secure network as a service (NaaS) to enterprise 5G customers.
- Automated threat correlation and security enforcement based on subscriber, equipment, and network slice levels to help isolate and quarantine the infected subscriber/user in 5G networks and accelerate security event investigation.
- Comprehensive visibility into and granular control of cellular IoT traffic.

Automated Security

- Automated cloud-delivered threat intelligence powered by ML to help teams defend against adversaries operating at 5G speeds—and prevent known and unknown threats in real time across 5G networks on a global scale.
- Unknown malware identification and analysis based on hundreds of malicious behaviors, with delivery of automated protections.
- Data-driven threat prevention that provides contextual security outcomes to prevent multi-stage attacks and anomalies.

Cloud Native Agility

- Simple and tightly integrated 5G security platform leveraging automation, Kubernetes® native orchestration, and integration with open APIs for operational simplicity.
- Cloud native platform with the same features across physical, virtualized, and cloud native deployments to ensure consistent security enforcement everywhere.
- Enhanced agility and deployment flexibility to meet scaling across VNF/CNFs.

Understanding Common 5G Challenges

The massive increase in network connectivity, move to software-driven networks, and emergence of new types of applications pose expanded security risks for both service providers and their enterprise customers. Threats are amplified in 5G, where attacks leverage 5G speeds and new points of attack as IoT devices proliferate. The severity and frequency of attacks associated with IoT in 5G networks continues to evolve at an alarming rate.

Carrier Challenges

With 5G networks, there is a greater reliance on cloud and edge compute, which creates a highly distributed environment spanning multi-vendor and multi-cloud infrastructures. Mobile network operators face new malware-based incidents that threaten network availability and subscriber confidentiality. These expanding threats and vulnerabilities—previously focused on the internet peering interfaces—can now exploit the application layer in other mobile network interfaces, degrade the customer experience, create network performance challenges, and affect operator revenues.

In addition, service providers are witnessing significant changes in traffic characteristics with the exponential growth of roaming and signaling traffic. These trends constitute new threat vectors that increase the risk of service disruption by both malicious actors and unintentional events that can overload the signaling infrastructure.

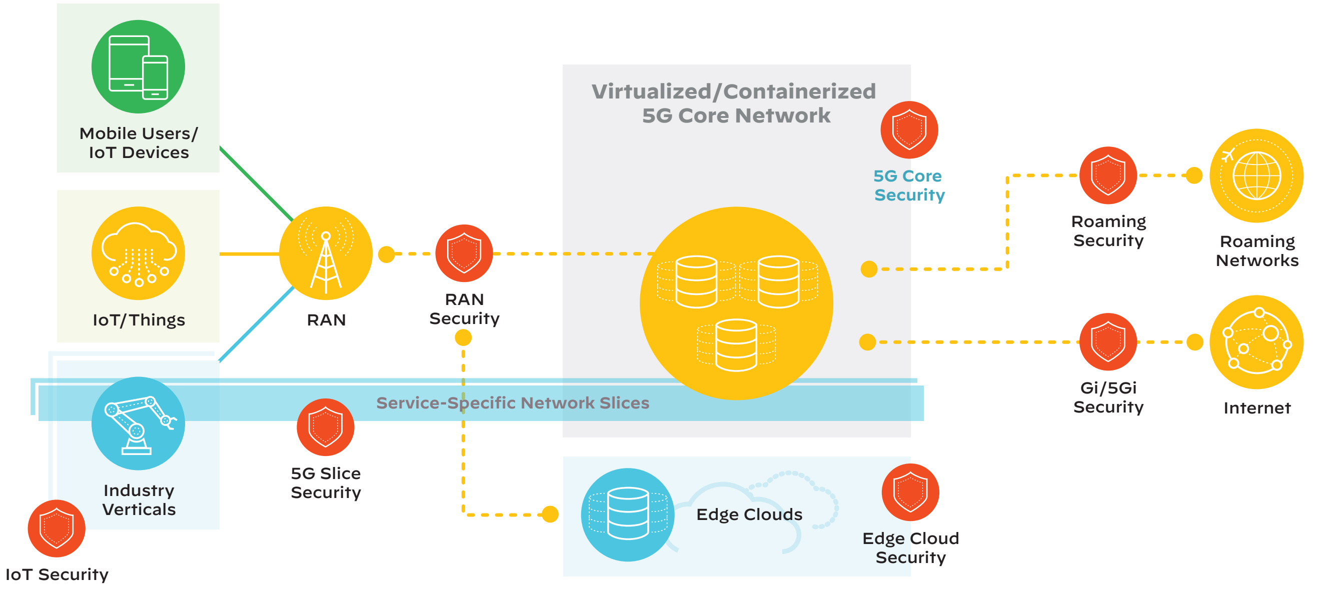

Figure 1: Reference architecture depicting security positioning over service provider 5G networks

Enterprise Challenges

Many enterprises are investing in 5G networks to deliver enterprise connectivity, improved productivity and increased operational efficiencies—all of which are made possible through more digitization, accelerated IoT adoption, and the harnessing of innovative techniques.

The modern mobile IoT environment presents substantial security risks, however. More devices and data mean more targets for cyberattacks. While attack targets and techniques are constantly evolving, the most common threats enterprises with business-critical services face are acts of cyberespionage. These intrusions are designed to gain access to control systems, and nation-states run spear phishing meant to gain key business intelligence, set up cryptomining operations, and launch ransomware.

New enterprise 5G trends also demand a new approach to security. Establishing a strong security posture with granular visibility in 5G traffic, along with automated security enforcement at 5G subscriber and device levels in real time, can stop cyberattackers from infiltrating networks, disrupting critical services, destroying industrial assets, and threatening the safety of the environment.

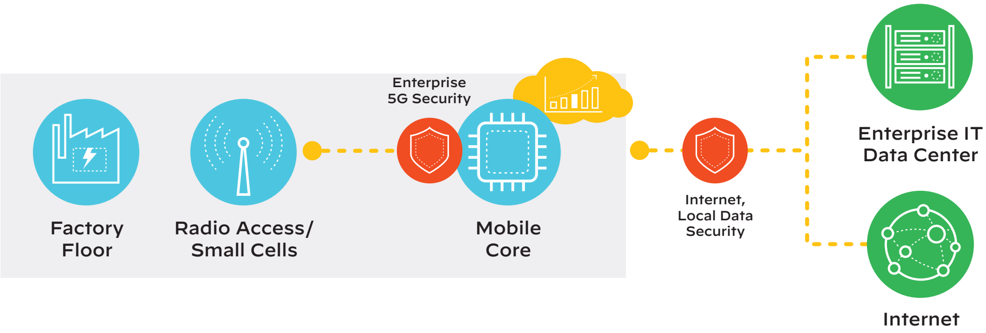
Enterprise 5G Security
Factory Floor
Radio Access/ Small Cells
Mobile Core
Internet, Local Data Security
Enterprise IT Data Center
Internet

Figure 2: Reference architecture depicting security positioning over enterprise 5G networks

Introducing ML-Powered NGFWs for 5G

Palo Alto Networks ML-Powered NGFWs for 5G address these significant security challenges with a robust, prevention-oriented security posture that takes advantage of application-layer visibility, across all layers, including user, control, and management planes, encompassing the 4G/5G network:

- Cellular IoT
- Radio access network (RAN)
- Roaming
- 5G network slice
- 5G next-generation core networks (5G NGCN)
- Multi-access edge computing (MEC)
- Edge and telco clouds; interfaces to other networks

Deployment Flexibility

ML-Powered Next-Generation Firewalls for 5G can be configured to meet varied security and throughput requirements for securing existing 4G networks as well as ongoing 5G deployments.

Networking Features

ML-Powered Next-Generation Firewalls for 5G support a wide range of networking features and are designed for easy integration into your 5G network. They can be deployed on all network interfaces to achieve scalable, complete protection with consistent management and application visibility.

VM-Series for Virtual Environments

Virtual Next-Generation Firewalls support all use cases, including RAN, roaming, 5G NGCN, MEC, data network/ internet, and non-3rd Generation Partnership Project (3GPP) access protection. The VM-Series can:

- Interoperate with most orchestrators and virtual network function managers (VNFMs).
- Interplay with software-defined network scaling and service chaining scenarios.
- Meet the stated VNF requirements of the Open Networking Automation Platform (ONAP).
- Expose REST APIs, which can be used easily under ETSI MANO as well as ONAP architectures.

- Automate VM-Series bootstrapping via Panorama™ network security management (day-N configuration, license and subscriptions, and registration).
- Offer extensibility with automation tools, such as Ansible®, Terraform®, and many more.

NFV, Cloud, and Virtualization Environments

VM-Series firewalls can be deployed in a variety of NFV, cloud, and virtualization environments, including VMware NSX®, VMware ESXi™, VMware vCloud® Air™, Linux KVM, OpenStack®, Cisco ACI®, and Arista.

VM-Series on OpenStack

The VM-Series on OpenStack enables automated firewall service insertion by way of Heat templates in basic L2/L3 mode as well as with prominent SDN controller vendors. The Heat templates can also be extended to provide networking service, monitoring, and OpenStack telemetry to facilitate auto scale security.

CN-Series for Container Environments

Our cloud native CN-Series Container Next-Generation Firewalls support all use cases, including RAN, roaming, 5G NGCN, MEC, data network/internet, and non-3GPP access protection. The CN-Series can be deployed in:

- On-premises Kubernetes environments, including native Kubernetes, Red Hat OpenShift®, and VMware Tanzu™ Kubernetes Grid
- Public cloud Kubernetes environments, including AWS EKS, Microsoft Azure AKS, and GKE

5G Cloud Native Network Functions on Kubernetes

5G cloud native network functions (CNF) require specific infrastructure support for Kubernetes in terms of networking and network acceleration. CN-Series firewalls can:

- Inspect 5G CNF interfaces with Multus CNI
- Interoperate with network acceleration that is often used with 5G CNF deployments
- Support Helm Chart-based orchestration and automation

Table 1: 5G Security Deployment Scenarios

Network Slice Security	Dynamically enforce granular security per 5G network slice ID, 5G equipment ID or group of equipment, and 5G subscriber ID or a group of subscribers, to offer personalized, scalable, and differentiated security policies per enterprise customer.
RAN Security	**4G:** Gain full content inspection of subscriber traffic inside GTP tunnels across all layers. Control, signaling, and data planes with application visibility help prevent suspicious signaling events on the access network. **5G:** Benefit from visibility and prevention capabilities into the transport layer with SCTP stateful inspection and application layer with NGAP.
Roaming Security	**4G:** Protect the mobile network from signaling storms, including various tunneling and application-layer attacks coming through the GRX/IPX networks on S8, S6a/S6d, and Gp interfaces. **5G:** Protect the mobile network from application-layer and data tunneling attacks coming through the IPX networks over N9 interfaces.
Enterprise 5G Security	Extend enterprise-grade security to your new 5G network and accelerate your 5G digital transformation with confidence. Enable faster security event investigations by dynamically correlating infected devices and subscribers to threats in real time.
Cellular IoT Security	Secure the mobile network from weaponized IoT device-initiated attacks. Leverage deep visibility and granular control over cellular IoT traffic (including NB-IoT) to discover and prevent attacks from known and unknown threats, command-and-control communications, denial-of-service attacks, and more.
Internet Security	Achieve a comprehensive, prevention-oriented security posture that takes advantage of application-layer visibility on Gi/SGi and N6 interfaces to secure your network infrastructure against multi-stage attacks from the internet.
Signaling Security	Benefit from visibility and prevention capabilities at multiple layers in signaling traffic, including SCTP, PFCP, SIGTRAN, Diameter, and SS7.
Telco Cloud Security	Enforce cloud-agnostic security at scale across cloud native architectures and embed security in every stage of the DevOps workflow for proactive defense. Gain full lifecycle security and full stack protection for your 5G core telco cloud environments and protect your mission-critical workloads.
Edge Cloud Security	Secure applications and data across MEC deployments in distributed 5G multi-cloud and hybrid environments.

Table 2: ML-Powered NGFWs for 5G Networking Features
5G Security
3GPP standards references: • 23.502 up to 15.5.0 • 29.502 up to 15.4.0 • 29.244 up to 16.4.0
5G Network Slice Security—visibility and policy control per 5G Network Slice ID
5G Equipment ID Security—visibility and policy control per 5G Equipment ID, incl. PEI/IMEI
5G Subscriber ID Security—visibility and policy control per 5G Subscriber ID ID, incl. SUPI/IMSI
PFCP stateful inspection
PFCP inspection on N4 to extract context
HTTP/2 inspection in SBA on N11 to extract context
Filtering per APN/ DNN, RAT, per-IMSI, and IMSI-prefix
GTP-in-GTP
GTP-U content inspection
GTP-U TEID validation over N3
GTP Security
3GPP standards references: • GTPv2-C TS 29.274 up to release 15.2 • GTPv1-C TS 29.060 up to release 15.1 • GTP-U TS 29.281 up to release 15.0
4G Subscriber ID Security—policy control per 4G Subscriber ID, incl. IMSI
4G Equipment ID Security—policy control per 4G Subscriber ID, incl. IMEI
GTPv2 and GTPv1 message filtering per message type
GTPv2-C, GTPv1-C, and GTP-U stateful inspection and protocol validation
GTP-U content inspection
IMSI and IMEI correlation to subscriber IP traffic, threat, and content
GTP-in-GTP check
GTPv2 and GTPv1 flood protection per message type
Filtering per IMSI, IMSI-prefix, APN, RAT
Overbilling protection
Narrowband IoT security

Table 2: ML-Powered NGFWs for 5G Networking Features (continued)
SCTP Security
SCTP stateful inspection and protocol validation
SCTP multihoming support
SCTP multi-chunk inspection
Signaling filtering, including: • SCTP payload protocols filtering per PPID for M3UA, M2PA, S1AP, X2-AP, and more • Diameter message filtering per App-ID, Command Code, and AVP for applications 3GPP-S6a/S6d, S9, and more • SS7 message filtering per SSN, Calling Party GT, and opcode for protocols including MAP, CAP, and SCCP
Signaling flood protection, including: • SCTP INIT flood protection • Diameter message flood protection per App-ID, Command Code, and AVP • S1AP message flood protection
High Availability
Failure detection: path monitoring, interface monitoring
Interface Modes
L2, L3, tap, virtual wire (transparent mode)
Network Acceleration
OvS, DPDK, SR-IOV, PCI Passthrough
Routing
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing
Policy-based forwarding
Point-to-Point Protocol over Ethernet (PPPoE) and DHCP
Supported for dynamic address assignment
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
Bidirectional Forwarding Detection (BFD)

Table 2: ML-Powered NGFWs for 5G Networking Features (continued)
IPv6
L2, L3, tap, virtual wire (transparent mode)
Features: App-ID, User-ID, Content-ID, WildFire, and SSL decryption
SLAAC
IPsec VPN
Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)
Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
GlobalProtect Large Scale VPN (LSVPN) for simplified configuration and management

Table 2: ML-Powered NGFWs for 5G Networking Features (continued)
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP
Network Address Translation
NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation)
NAT64, NPTv6
Additional NAT features: dynamic IP reservation, tunable dynamic IP and port oversubscription

To learn more about the security features and associated capacities of ML-Powered NGFWs for 5G, please visit paloaltonetworks.com/network-security/next-generation-firewall.

paloalto
NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com