Securing Private Mobile Networks

With an AI-Driven Network Security Fabric

The convergence of 5G, AI, and edge computing is transforming industries—powering smart factories, autonomous vehicles, enterprise IoT, and industrial OT. But this transformation brings risk. As enterprises deploy remote private mobile networks to enable real-time decision-making and automation, the attack surface expands dramatically. Legacy infrastructure, distributed edge assets, and AI-enabled devices create visibility gaps and new threat vectors.

Additionally, while private mobile networks are deployed within enterprise environments, they often extend into the public cloud for data processing and AI workloads. However, security strategies frequently overlook the AI runtime, creating a critical gap in end-to-end protection.

Private mobile networks are dedicated to the enterprise and come with built-in infrastructure security features, such as user traffic integrity protection, subscriber privacy, identity concealment, roaming interface and payload security, and mutual authentication with encryption.

However, securing the network infrastructure alone isn't sufficient. Enterprises must also protect the data that flows across the network. This requires applying enhanced security measures, including Zero Trust principles, network segmentation, application and protocol visibility, and advanced security functions such as intrusion prevention, DNS and URL filtering, and OT/IoT protection.

Comprehensive, end-to-end visibility and control are essential to ensuring mission-critical applications and assets remain secure. With increasing regulatory pressure and mission-critical operations at stake, securing the entire private 5G environment—from edge to core—is now a business imperative.

> Cyberattackers are leveraging AI to launch faster, more sophisticated attacks. Nearly **70%** of executives now see 5G-connected devices as a top OT security risk.[1]

The Solution: AI-Powered, Zero Trust Security for Private Mobile Networks

Palo Alto Networks provides unified, end-to-end visibility and protection across the private mobile network landscape. Our industry-leading 5G-Native Security protects 5G devices, networks, services, and applications everywhere, including on-premises edge, core, and cloud. It secures distributed remote private 5G networks with cellular devices and industrial equipment.

Our platform ensures that enterprise security policies and compliance are consistently enforced, whether devices are directly connected to the network or operating behind a shared SIM card. Security extends beyond the network to encompass AI workloads, protecting both the integrity of data sources and the AI application runtime, ensuring mission-critical applications remain secure at every layer.

Comprehensive, adaptive 5G security is delivered with:

- **Precision AI®:** Protect against advanced threats, including zero-day attacks.
- **Zero trust security:** Enforce user– and device–level policies from distributed remote edge locations to 5G core.
- **Prisma® SASE 5G:** Provide seamless scalability and secure connectivity across distributed locations.

1. Michael Amiri and Michela Menting, *The State of OT Security: A Comprehensive Guide to Trends, Risks, & Cyber Resilience*, Palo Alto Networks and ABI Research, April 2024.

Three-Step Framework to Secure Private 5G

Comprehensive cybersecurity across the private mobile network landscape requires a thorough three-step framework (see figure 1) that addresses access, policy segmentation, and data protection.

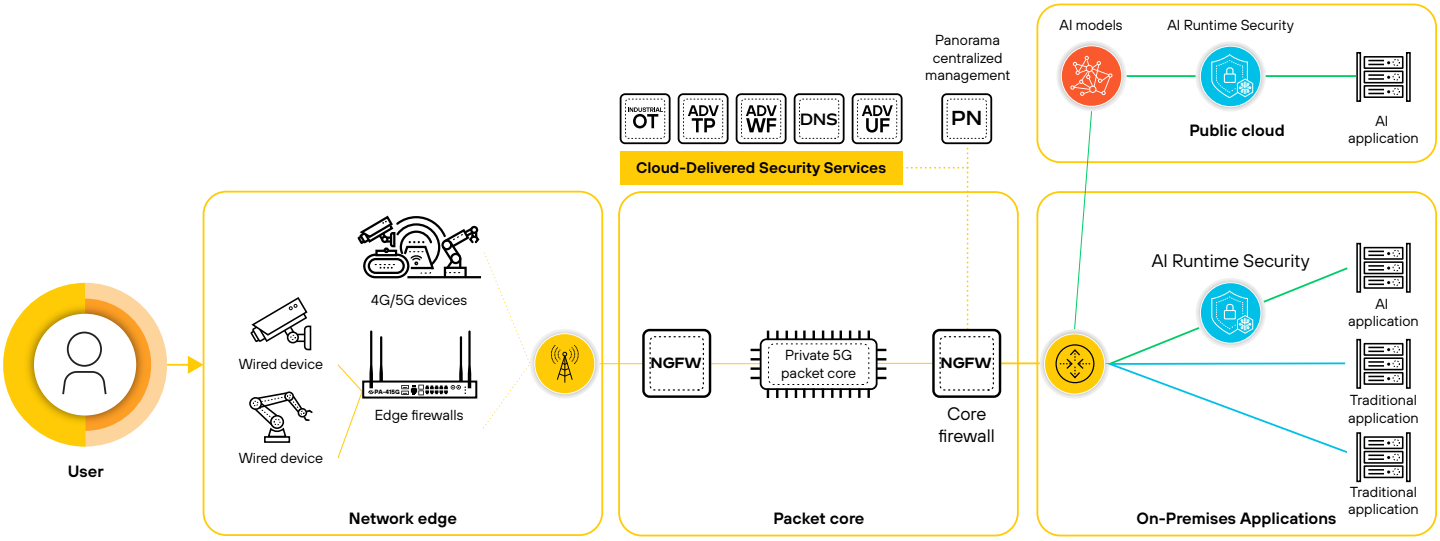


Figure 1. Three-step framework to secure private 5G

1. Secure the Private Mobile Network Core

The majority of OT breaches start with an IT breach, as the attacker moves laterally into the OT environment. Organizations must gain intelligent visibility into core traffic and apply zero trust policies to reduce the attack surface and prevent lateral threat movement.

Our private 5G security starts at the core by isolating private 4G/5G networks from IT, cloud, and internet networks, and then establishing clear segmentation between edge, core, and broader enterprise environments. It helps organizations ensure secure communications, minimize vulnerabilities, and run resilient, regulation-ready operations by leveraging our:

- **App-ID™ and advanced security subscriptions:** Monitor, classify, and control traffic based on applications, users, and devices, as well as enforce device and service-level policies to secure OT and IT systems.
- **AI/ML-powered Threat Prevention:** Profile assets, detect anomalies, and stop unauthorized access in real time with deep packet inspection and advanced policy enforcement.

2. Secure the Private Mobile Network Edge

In many industrial and enterprise deployments, IoT and OT devices are unable to connect directly to mobile networks. Additionally, organizations often leverage a single SIM or shared cellular connection to support multiple endpoints. These architectures typically rely on cellular routers, which provide connectivity but also introduce challenges in extending security controls from the network core to the edge. As a result, enforcing consistent enterprise security policies across all connected devices becomes complex, increasing the risk of visibility gaps and policy drift.

Our edge firewalls with integrated cellular capabilities enable seamless extension of core security policies to the network edge. The built-in redundant cellular connectivity capability:

- Simplifies network deployment and operations.
- Supports segmentation of devices behind a single device.
- Reduces the attack surface by associating device identity with application and protocol visibility.

The PA-400-5G series is available in multiple models—both ruggedized and nonruggedized—to support a wide range of industrial and enterprise use cases. These devices are centrally managed through Panorama® or Strata™ Cloud Manager, alongside core and other firewalls within the private mobile network, ensuring consistent policy enforcement from core to edge. Additionally, Zero Touch Provisioning (ZTP) significantly reduces deployment time, cost, and operational complexity. Figure 2 illustrates how ZTP simplifies branch onboarding.

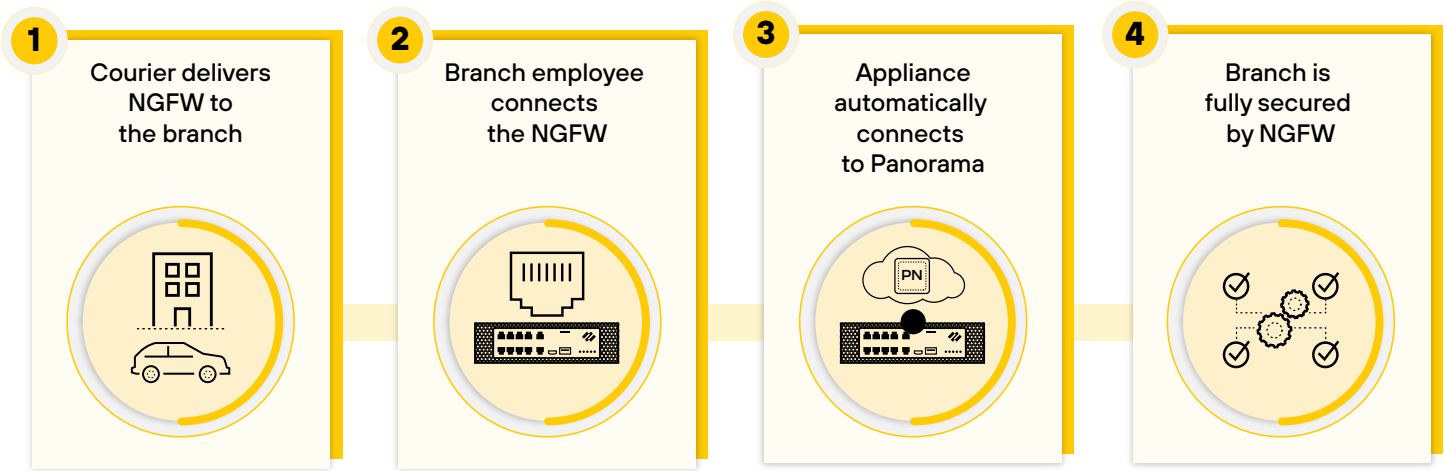
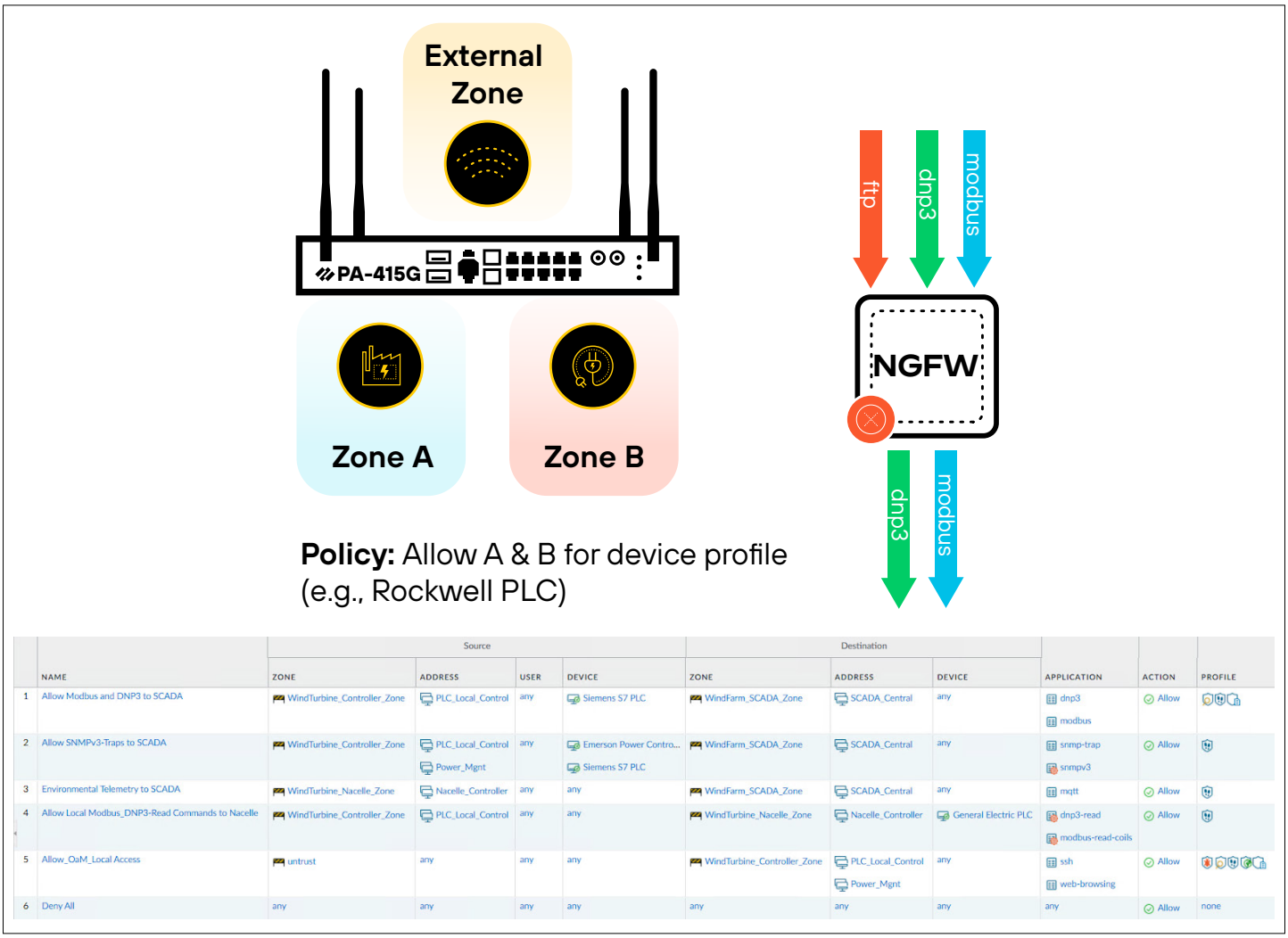


Figure 2. Palo Alto Networks ZTP is designed to simplify and speed up branch onboarding

Implementing layered security across branches is facilitated with network microsegmentation, application-aware security zones, and NGFW policies powered by App-ID, Device-ID, and User-ID™.



	NAME	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	ACTION	PROFILE
1	Allow Modbus and DNP3 to SCADA	WindTurbine_Controller_Zone	PLC_Local_Control	any	Siemens S7 PLC	WindFarm_SCADA_Zone	SCADA_Central	any	dnp3 modbus	Allow	
2	Allow SNMPv3-Traps to SCADA	WindTurbine_Controller_Zone	PLC_Local_Control Power_Mgnt	any	Emerson Power Contro... Siemens S7 PLC	WindFarm_SCADA_Zone	SCADA_Central	any	snmp-trap snmpv3	Allow	
3	Environmental Telemetry to SCADA	WindTurbine_Nacelle_Zone	Nacelle_Controller	any	any	WindFarm_SCADA_Zone	SCADA_Central	any	mqtt	Allow	
4	Allow Local Modbus_DNP3-Read Commands to Nacelle	WindTurbine_Controller_Zone	PLC_Local_Control	any	any	WindTurbine_Nacelle_Zone	Nacelle_Controller	General Electric PLC	dnp3-read modbus-read-coils	Allow	
5	Allow_OaM_Local Access	untrust	any	any	any	WindTurbine_Controller_Zone	PLC_Local_Control Power_Mgnt	any	ssh web-browsing	Allow	
6	Deny All	any	any	any	any	any	any	any	any	Allow	none

Figure 3. PA-400-5G series NGFWs support secure communication between SCADA devices

Use Case: Communication Between Devices on the Same Site (PA-400)

In a smart manufacturing plant, industrial IoT devices, such as sensors, actuators, and controllers, are connected to a single PA-400. The firewall policies enforce strict security rules, ensuring all data transmitted between devices within the same network segment is encrypted, authenticated, and monitored for threats. For instance, sensor data transmitted from machines to the central system is protected against tampering or interception, ensuring secure communication within the factory.

Use Case: Communication Between Devices Across Different Sites (PA-400s)

A global energy company deploys PA-400s at remote oil rigs, connected to a central data center. Communication between the PA-400 firewalls at the remote locations and the core data center is secured using VPN or IPsec tunnels. This ensures sensitive data, such as operational metrics and real-time sensor information from the rigs, is encrypted during transit, protecting it from cyberthreats as it moves between distant sites and the central network.

The company augments defenses with advanced threat prevention tailored for 5G-OT environments, stopping zero-day threats and securing mission-critical operations at the edge.

3. Secure AI Applications

AI-enabled devices are revolutionizing industries, such as healthcare, manufacturing, and logistics, with private 4G/5G networks serving as the backbone for these transformations. As AI workloads—like generative AI, computer vision, AR/VR/XR, and IoT—become more compute-intensive, private 5G offers the secure, low-latency connectivity required to support these applications at the edge. It's imperative to protect the applications that devices communicate and share data with.

Deploying AI applications on private 5G enables enterprises to harness the full power of AI while ensuring that sensitive data remains protected. With AI-powered security and zero trust policies, organizations can safeguard high-performance AI workloads from edge to core, prevent unauthorized access, and mitigate evolving cyberthreats. Whether AI processing is offloaded to public clouds or runs locally on the edge, AI Runtime Security™ protects AI apps, models, and data against runtime threats. This creates a secure environment where innovation and efficiency can thrive, empowering industries to drive real-time decision-making and operational excellence.

Secure Private 5G with Confidence

Trusted by global leaders to secure mission-critical OT and 5G infrastructures, we enable organizations to move fast, stay secure, and maintain compliance in their journey toward fully connected, intelligent operations. By securing private 5G networks from the core to the edge with zero trust principles, organizations can maximize uptime, reduce risk, and confidently embrace innovation.

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

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

strata_sb_securing-private-mobile-networks_070125