EXTENDED APPLICATION-LAYER VISIBILITY ACROSS MULTIPLE MOBILE NETWORK PEERING POINTS

Palo Alto Networks Security Operating Platform comprises numerous critical security controls, including:

- **Next-Generation Firewall**, which identifies and controls traffic flowing across physical and virtual mobile network elements; inspects the application layer for known or unknown malware, packet anomalies or overload conditions; and ties applications to user identities.
- **WildFire® malware prevention service**, which provides centralized intelligence capabilities, security for SaaS applications and automated delivery of preventive measures that can eliminate new threats within five minutes from attacks on networks, clouds and endpoints.
- **Application-layer visibility** for all network interfaces, including internet (SGi), RAN/Core (S1/S11) and roaming (S8/Gp).

Near-perfect network availability is one of the most important strategic objectives for mobile network operators, or MNOs, who have supported it with billions in network investment. Historically, with malicious attacks coming primarily through the internet (Gi/SGi), operators' security strategies have focused on protecting known vulnerabilities of specific network elements, interfaces and protocols, but the environment has significantly changed. MNOs now face new malware-based incidents that threaten network availability and subscriber confidentiality. Cybercriminals have become highly sophisticated and can quickly change their malware tools to avoid detection. Attacks are now as likely to come from infected mobile or IoT devices in the radio access network or roaming partners as from the internet.

In addition, operators have witnessed significant changes in traffic, with exponential growth in roaming and signaling. These are new threat vectors with risk of service disruption from malicious actors as well as unintentional events that can overload signaling infrastructure.

Palo Alto Networks® Security Operating Platform includes a comprehensive set of software features that significantly enhance application-layer protection and visibility across all network peering points – at the internet-facing SGi interface, S1 RAN interface and S5/S8 roaming network interface points of presence.

Mobile Operator Challenges

The overall attack surface on mobile operator networks has expanded with increased IoT device connections; small-cell deployments; converged access (i.e., fixed, mobile, Wi-Fi); public and hybrid cloud; shared mobile infrastructure; and the growth of interconnected networks to support roaming (see Figure 1). The evolution from 4G to 5G and virtual networks (NFV/SDN) will continue to shift the distribution of traffic across multiple network environments, resulting in multiple threat vectors emerging that create new opportunities for hackers to exploit.

Sophisticated bad actors can inject malware into an ever-growing volume of traffic distribution points, where they can develop new exploitation techniques, leveraging data and signaling channels to attack subscribers, as well as multiple elements and networks, before they spread and morph to avoid control or detection.

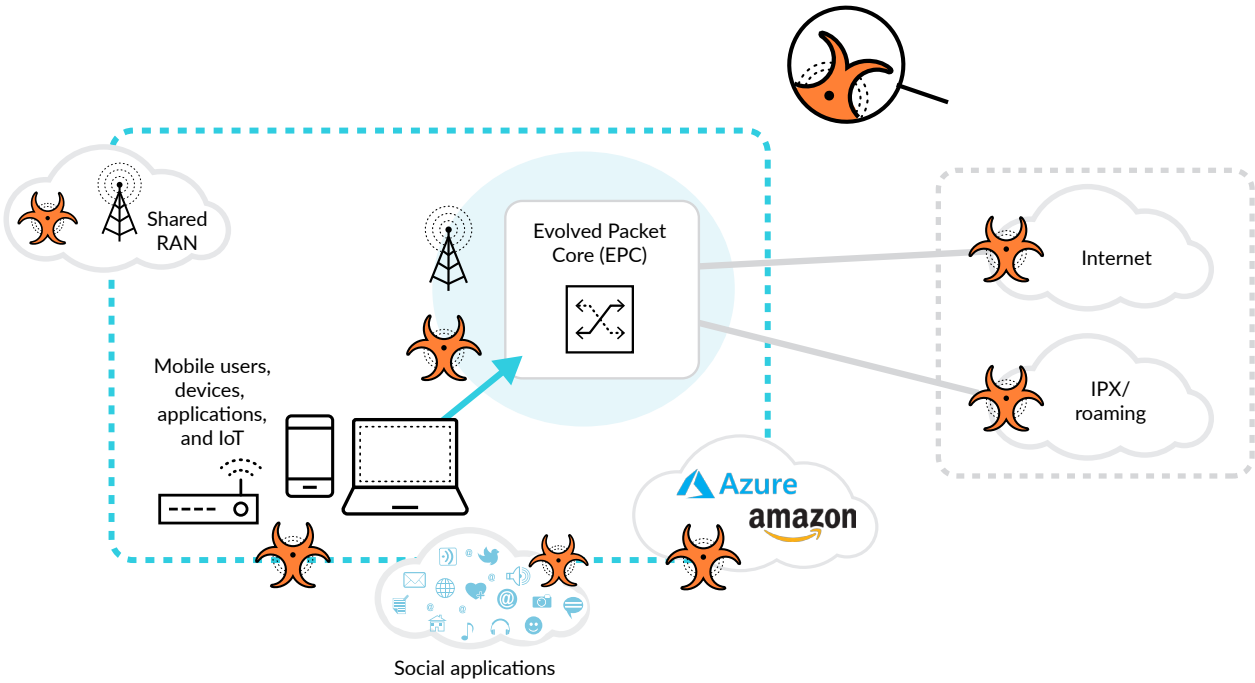

Figure 1: Rapidly expanding attack surface requires full visibility across all mobile network peering points

New Threats Through the RAN, Roaming, IoT and Botnets

As a result, these expanding threats, previously focused on the SGi interface, can now exploit the application layer at other mobile network interfaces, degrading the customer experience and leading to network performance challenges and revenue impact for MNOs. This requires a more comprehensive and prevention-oriented security posture that leverages application-layer visibility.

Cyberthreats have become increasingly sophisticated over time, with attackers perfecting their techniques to attract victims and using multiple application types to maximize their financial gains or harm network availability. Malware is the preferred tool for cybercriminals and thus, together with credential theft, is part of the event chain in virtually every cybersecurity incident.

Attackers can rapidly infect large numbers of lightly protected smart, mobile and IoT devices to leverage them as elements of a botnet, threatening the mobile infrastructure as well as subscribers. Attackers target devices that are largely unprotected, powerful enough, well-connected and generally ignored. IoT devices and smartphones are perfect candidates.

MNOs have traditionally maintained a security posture focused on protecting network elements and defined network perimeters with Layer 3/Layer 4 network security approaches, putting little or no emphasis on preventing application-layer threats or protecting subscribers' endpoint devices.

Known Threats and Vulnerabilities

The known architectural vulnerabilities of 3G and 4G networks have been identified and analyzed by multiple standards groups and infrastructure vendors:

- **GTP-based attacks:** GTP-based attacks include abnormal GTP packets, out-of-state GTP messages, spoofing and scanning. Packet abnormalities can be created due to poorly configured or faulty network elements, or roaming partners with incompatible network elements.
- **Infected subscribers:** Network outages/service disruption can stem from denial-of-service attacks initiated by infected subscriber devices.
- **Non-malicious signaling flood:** Network element failure, unusual events and poorly designed mobile devices and applications can overwhelm signaling infrastructure with high volumes of simultaneous requests for network connection.
- **Malicious DDoS:** Infected mobile and IoT devices can form botnets and launch attacks against network infrastructure.
- **Protocol abnormalities:** Malformed packets or packets not complying with protocol standards and other anomalies can crash network signaling infrastructure.
- **DoS attack using signaling messages:** Attackers can use compromised or impersonated network elements to send various signaling messages to launch a DoS attack on a network.
- **Service bypass:** Network vulnerabilities have also been manipulated to allow unbilled and unauthorized services and for data exfiltration from subscriber devices, often using infected devices as unwitting accomplices.

Offering Description

Palo Alto Networks provides a complete security platform with the deepest prevention for all network interfaces, with consistent management and application visibility across the broadest scalability range in a variety of physical and virtual form factors. The platform also includes protections for both control plane and data plane traffic.

Consistent Security Posture

Palo Alto Networks Security Operating Platform includes a comprehensive set of software features that work together to prevent successful security breaches and enhance application-layer visibility in mobile networks. All features are deployable across the entire portfolio, including high-performance

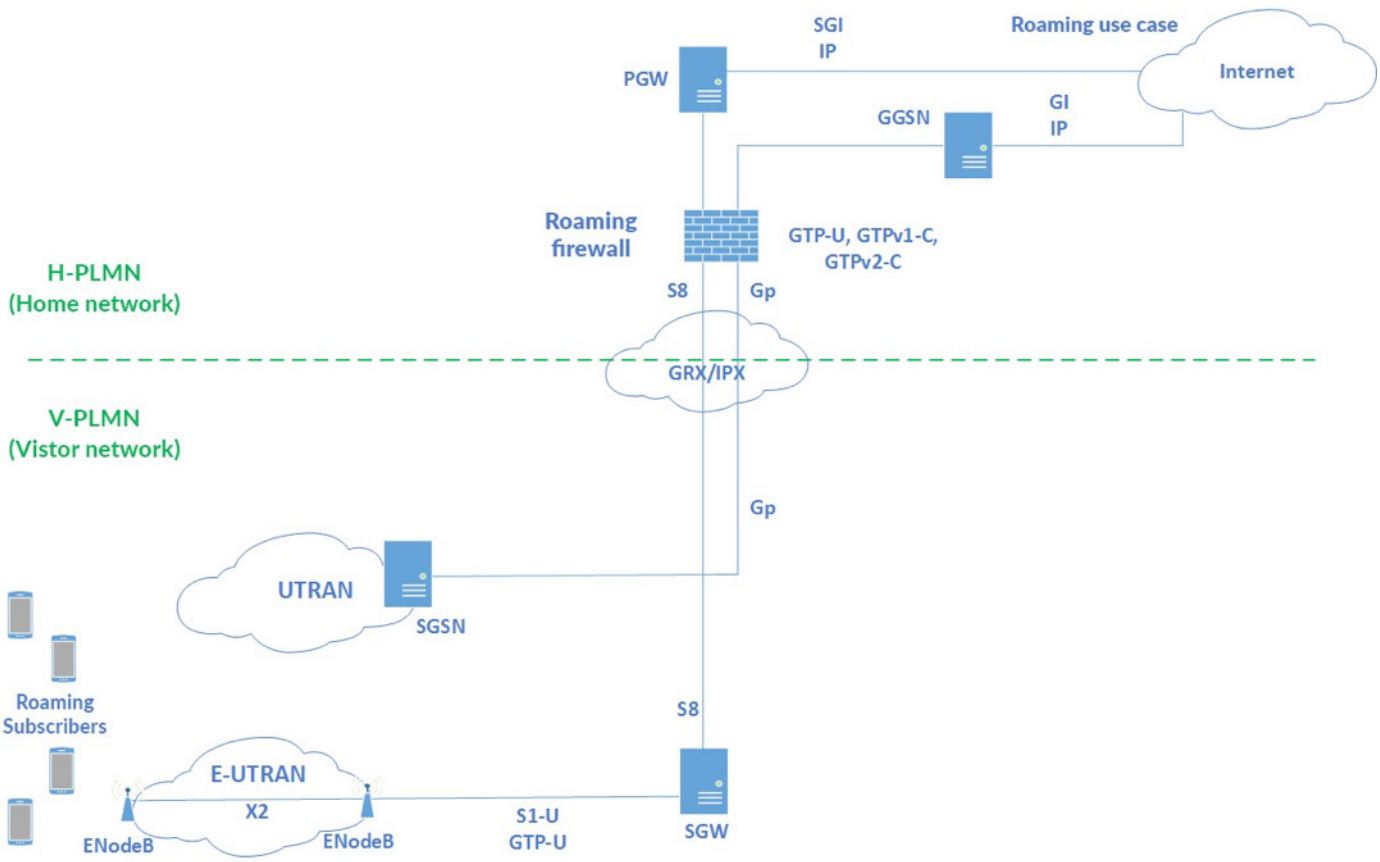

Figure 2: Palo Alto Networks roaming security in 3G and 4G mixed networks

physical appliances and VM-Series virtual deployments. This enables a consistent security posture across all network points, for all users, applications and locations.

MNOs can leverage application-layer visibility across data and signaling traffic at all network peering points, including:

- **Internet/EPC security (SGi):** You can prevent advanced attacks between the internet and the EPC emanating directly from malicious hosts or from command-and-control communication between a host and an infected device. You can also prevent malware and other attacks that may be targeting end-user mobile devices.
- **RAN/EPC security (S1/S11):** The platform helps prevent advanced attacks between the RAN and mobile core – the EPC – emanating from infected or malicious mobile end-point devices, as well as mitigate potential mobile network resource congestion and degradation of service.
- **Roaming security (S8/Gp):** You can prevent advanced attacks emanating from roaming networks and mitigate potential mobile network resource congestion and degradation of service.
- **IoT security:** You're able to establish a mobile network protection framework for "things" connected through 4G or 5G mobile networks and prevent hackers from infecting IoT devices that could then cause anomalies or launch attacks on mobile network infrastructure.
- **Signaling security:** The platform provides protection for multiple network elements and protocols that are vulnerable to signaling attacks and storms, including:
  - Mobility Management Entity, or MME
  - Serving gateway, or SGW
  - Packet gateway, or PGW
  - IP Multimedia Subsystem, or IMS
  - Other core elements using protocols like GPRS Tunneling Protocol, Stream Control Transmission Protocol, Diameter and Signaling System No. 7.

GTP and SCTP Security

Palo Alto Networks provides comprehensive, consistent protection, including GTP and SCTP security functions. The Security Operating Platform provides deep application-layer visibility, consistent policy enforcement and identification of already-infected devices. The platform's multilayered approach allows:

- Stateful inspection of SCTP and GTP protocols
- Validation of SCTP and GTP protocols in compliance with standards
- Advanced filtering capabilities for SCTP payload protocols, GTP, Diameter and SS7 protocols
- Flood protection for protocols like GTPv2-C, GTPv1-C, SCTP, S1AP, Diameter

GTP stateful inspection also provides visibility into international mobile subscriber identity and international mobile equipment identity – IMSI and IMEI, respectively – which allows data sessions to be correlated to the device/subscriber. This can enable the MNO to identify infected devices engaging in attacks, notify subscribers of infection, and prevent sessions from being hijacked for malicious purposes.

GTP-U decapsulation and content inspection provides the capability to scan the content of mobile subscriber traffic carried in GTP-U tunnels.

These security measures can mitigate numerous malicious events and prevent attackers from causing network congestion, or outages that disrupt data and voice services, for subscribers and devices connected to these networks.

Comprehensive Application-Layer Visibility

MNOs will gain expanded visibility across all potential mobile network attack surfaces that impact their networks and subscribers, enabling them to prevent a greater number of potential attacks and extending their ability to respond immediately and automatically as new threats emerge.

Roaming Security Summary

- **Data charging bypass:** Protection against unbilled and unauthorized services, such as DNS tunneling.
- **Network service disruption:** Protection against unauthorized access or network outages/service disruption due to DoS initiated by infected roaming subscriber devices.
- **Mitigation of GTP attacks/vulnerabilities:** Protection against GTP-based attacks from roaming partners caused by abnormal GTP packets, out-of-state messages, spoofing and scanning. GTP message floods caused due to unintentional actions and natural disasters or other local outages.
- **Subscriber data protection:** Prevention of sensitive subscriber data/information theft. Protects subscribers from over-billing attacks and session hijacking through GTP.

Prevent Successful Breaches

Operators need to shift their security priorities to prevention, rather than mitigation. Successful breaches or attacks and other non-malicious events that would impair network or service availability can be prevented. This requires constant, application-level vigilance across the entire network and automated, near-real-time response to unknown threats.

Malware is part of the event chain in virtually every security incident. By stopping malware installation on mobile devices or disrupting its execution if already installed, MNOs can prevent threats to their subscribers and networks.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform safeguards your digital transformation with continuous innovation that combines the latest breakthroughs in security, automation, and analytics.

Palo Alto Networks Security Operating Platform is a comprehensive, cost-effective offering that helps mobile network operators get ahead of the tremendous leaps in cybercriminal capability to relieve multiple urgent mobile operator pain points.

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

extended-application-layer-visibility-across-multiple-mobile-network-peering-points-b-100218