5G Security with Palo Alto Networks ML-Powered NGFW and MantisNet Containerized Visibility Fabric

Visibility into Subscriber ID and Other 5G Identifiers for N6 NGFW Deployments

Benefits of the Integration

- NGFWs on the N6 interface can enforce policies based on SUPI today, and other identifiers such as PEI, Slice ID, etc., in the future.
- The NGFW will show the SUPI (and possibly other identifiers) in all logs, including Traffic, Threat, URL, and WildFire logs.
- The SOC will now receive subscriber information, not just the IP. The SOC will now instantly know the affected user/device.
- Enterprises can enact security policies based on the SUPI today. Other identifiers could also be used but have not been tested.
- If certain users are allowed to access a resource, but others are not, policies can target SUPIs to enforce this posture.
- IP addresses of the device can change, but the SUPI-based policies will remain effective.

The Challenge

When it comes to securing a mobile network (e.g., 4G or 5G), the firewall is often placed on the perimeter of the network. In a 5G network, this location or interface has a name, and is called the N6 interface. When a Palo Alto Networks Next-Generation Firewall (NGFW) is located on N6, it is challenging for it to know the "who" of each flow, which is needed for an effective Zero Trust security posture. In an enterprise deployment the "who" is answered by User-ID, which is populated by information from Active Directory (AD) and LDAP, but in a mobile network, we often don't have AD or LDAP. In a mobile network there are other identifiers, which can be used to identify the "who" of each flow. In a 5G network, one of the primary identifiers is the Subscriber Permanent Identity (SUPI).

When the NGFW is located on other interfaces other than N6, such as the N3 and N4 interfaces, it has visibility into the SUPI (and other identifiers). On N6, however, it does not, which is where additional information from the 5G Core control plane signaling is needed.

The Solution

5G identifiers are found within the control plane messaging of a 5G core—examples of important identifiers are the 5G SUPI, Permanent Equipment Identity (PEI), and Slice ID. However, when an NGFW is sitting on the N6 interface, it can't access the messaging to correlate network activity to specific 5G entities. To apply policies that are application-, user-, or slice-specific, more information is needed. One strategy to get this information is to have probes/sensors deployed in the core send the 5G identifiers to the NGFW via API. These sensors extract key identifiers like the SUPI and PEI from the core and push this metadata to the NGFW via APIs, allowing the NGFW to start making more granular policy decisioning.

MantisNet Containerized Visibility Fabric

The CVF is an extended Berkeley Packet Filter (eBPF)-based solution built for introspecting containerized environments and tailored specifically for 5G SA (stand-alone) networks. Consisting of agents deployed via DaemonSet, the CVF scales alongside production nodes while introspecting all messaging within the 5G core. These sensors extract a variety of datasets from the 5G control plane to pass along to analytics/security tools via the message bus datasets include Topology, Cloud-Native Flow, Protocol Metadata, Encrypted Session Data (plaintext payload), and Packet Capture. The MantisNet CVF can operate not only in environments running in the clear, but also within networks that are running with TLS encryption—the data is extracted the same way in both scenarios, and no decrypt engines are needed. Another value of using the CVF is that it is completely vendor-agnostic. It doesn't matter which network function vendors are present within the environment, the CVF can introspect all activity across all vendors without any code changes needed.

Palo Alto Networks Next-Generation Firewalls

Palo Alto Networks NGFWs offer a prevention-focused architecture that's easy to deploy and operate. The machine learning (ML)-powered NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. Automation reduces manual effort, so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters most, and enforce consistent protection everywhere. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies and write rules that are easy to understand and maintain.

Palo Alto Networks and MantisNet: 5G Security on the N6 Interface

This joint solution allows customers to establish granular NGFW policies based on the SUPI when the Palo Alto Networks NGFW VM-Series and hardware are deployed as a perimeter firewall on the N6 interface. Customers can now make policy decisions based on the SUPI when they previously have only been able to apply policy by IP address—which can be challenging when securing 5G environments, which are cloud-native by design and have IP addresses changing frequently. Zero Trust architectures can be enforced by Palo Alto Networks NGFWs sitting on the perimeter of 5G networks, as this solution fully addresses the question of "Who?" Additionally, this solution addresses the challenge of gaining visibility into TLS-encrypted traffic, which is the standard within 5G cores, and it also can be deployed regardless of the vendors present within the environment.

Use Case: 5G Security on the N6 Interface

Challenge

Visibility into Subscriber IDs (SUPIs in 5G) and the ability to apply granular policies to establish Zero Trust security within 5G networks is challenging when the NGFW is sitting on a perimeter (N6) interface and not the core. The main challenge is that the NGFW doesn't have visibility into the core control plane messaging, which includes 5G identifiers that help correlate activity on the network and "who" is responsible for said activity (SUPI, IMEI, Slice ID, etc.). Further challenges are presented considering that any probe/sensor conveying this information to the NGFW has to deal with TLS-encrypted traffic, as well as an ever-increasing number of vendors present in 5G SA environments.

Solution

In this joint solution, MantisNet's CVF acts as the probe/sensor layer within the 5G core and extracts 5G identifiers

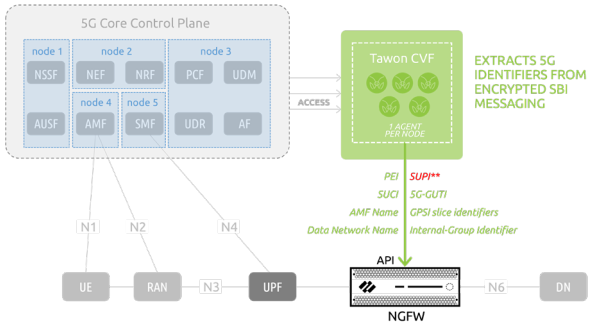

Figure 1: MantisNet CVF extracting 5G identifiers to provide to the Palo Alto Networks NGFW

from the messaging between network functions. The CVF agents send these identifiers to the Palo Alto Networks NGFW via the User-ID API. The MantisNet CVF observes the UE attach signaling and at that time uses a Python script to make an API call to the Palo Alto Networks NGFW located on the N6 interface. Upon UE detach from the network, the SUPI to IP address mapping is removed via the User-ID XML API. This provides visibility into the SUPI for all log types. It also allows customers to create differentiated policies using User-ID, where the User-ID values are the SUPIs of the mobile devices.

About MantisNet

MantisNet is a leader in observability and cloud-native technology. The MantisNet observability platform—the Containerized Visibility Fabric (CVF)—provides access and visibility into the inner workings of cloud-native, micro-services based, environments—from the core to the edge. The MantisNet CVF platform is both vendor and cloud agnostic; it combines the power of deep kernel-level instrumentation, a composable event-driven architecture, and in-node processing to deliver continuous, real-time visibility. As a result, the MantisNet CVF provides significant cost, operational and security benefits. For more information, visit www.mantisnet.com and follow MantisNet on LinkedIn at linkedin.com/company/mantis-networks.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS | MantisNet

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