SECURITY SOLUTION FOR MOBILE CARRIERS

EXPLOSIVE GROWTH OF MOBILE SERVICES

Mobile communication has been embraced globally at a record pace and now has become the preferred form of communication. Personal communication is just the start. The next inflection point of mobile growth towards IoT promises to be more exciting; however, more challenges await. Service providers need to scale the networks and implement security more effectively.

Some mobile carriers have over hundreds of millions of subscribers. The scale of mobile carrier networks is unprecedented; as much as 8 to 10 times greater when compared to fixed-line networks.

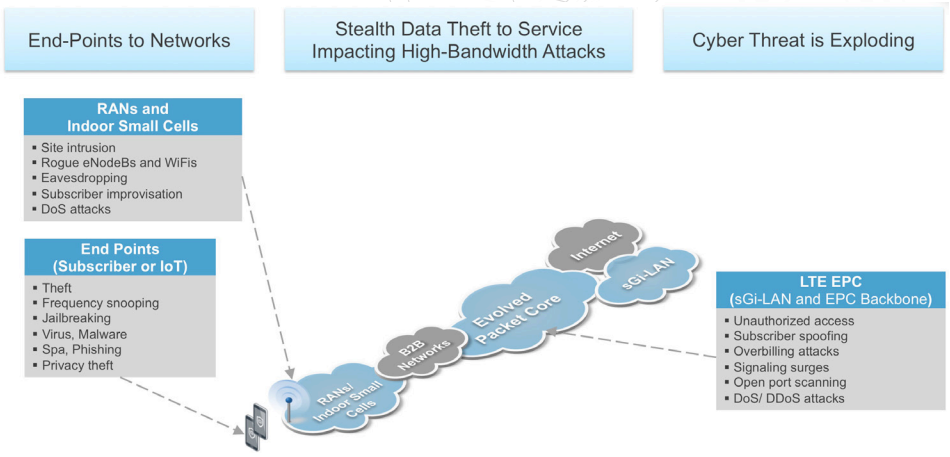

FIGURE 1. DIVERSITY OF ATTACKS IN MOBILE NETWORKS

THE ALL-CONNECTED WORLD—THE ERA OF IoT

By 2020, it is forecasted that the growth of Internet of Things (IoT) will far eclipse that of personal mobile devices. Many industry analysts predict that about 30 billion IoT devices will come on line. For scale, that is about five times the size of personal mobile devices.

Unlike the distributed fixed networks, mobile networks are built on a centralized architecture with the head-end intelligence concentrated in certain locations and can be easily become the targets for attacks. Furthermore, since most IoT devices are headless units, in the future, the vulnerability will be amplified even further.

DIVERSITY OF SECURITY ATTACKS

Security attacks on the mobile network can come from any part of the network, from the subscriber endpoints, intercepted transmission line from radio tower backhauls, or from the out-of-region roaming partner towers (Gp/S8) and more commonly, from the Internet interface (Gi/sGi).

As the figure 1 shows, the attack takes the form of a multitude of vectors, from stealthy subscriber data theft to a hard-hitting attack that can cripple the service to tens of thousands of subscribers. This often results in brand damage and costly subscriber churns, in addition to the heavy financial penalty. By some estimates, the total of the three can be as high as $184 million to $332 million (Ponemon Institute).

To overcome the serious challenges of protecting these new networks, mobile carriers need to improve their security posture and future-proof their investments.

FORTINET ADVANTAGES

HIGH-PERFORMANCE SECURITY PROCESSOR ENGINES AT MOBILE SCALE

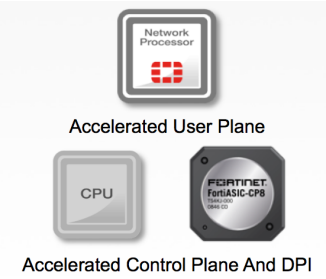

FIGURE 2 - FORTINET SECURITY PROCESSOR UNITS

Each release of a new, powerful mobile operating system enables a device to run more concurrent connections and execute higher rates of connection setup and teardown requests, which ultimately puts a tremendous demand on the control plane, data plane, and deep content processing of the mobile head-end networks.

Building high-performance security platforms is Fortinet's specialty. By investing heavily in the development of security processor units (SPUs) to accelerate the user plane, control plane, and more importantly, deep content processing, high performance is standard in all Fortinet architectures, from the UTM to the high-end, carrier-grade firewall that scales up to 1 Tbps.

To meet the massive mobile scale requirement, Fortinet has built a custom operating system to run on carrier-grade platforms and calls the purpose-built software platform, FortiOS-Carrier.

The FortiOS-Carrier scales magnitudes higher than the standard enterprise-grade platforms. The combination of high performance and high scalability makes Fortinet security platforms unique in the industry and well-suited for the security challenges of mobile network growth.

HIGH-EFFICACY SECURITY OS AND FORTIGUARD TO COUNTER RISING THREATS

FIGURE 3 - FORTINET SECURITY OPERATING SYSTEMS

To effectively secure the mobile evolved packet core (EPC) and Gi/sGi-LAN (aka packet backbone), three interfaces need to be protected. First and foremost is to put a high-performance firewall at the Gi/sGi interface facing the Internet.

To complement the Gi/sGi firewall, Fortinet recomends the FortiGuard service for an up-to-date threat intelligence information collected from the most advanced security fabric available with a global footprint. As shown figure 4, Fortinet Security Fabric receives a massive amount of security data and feeds the distilled information to the endpoints, making the FortiGuard service powerful and fully automated.

The other two interfaces to protect are the RAN backhauls (S1) and the roaming interface (Gp/S8) by installing a security gateway (SeGw) based on the same firewall platform. With the addition of FortiOS-Carrier, the SeGw can aggregate IPsec tunnels and provide firewall protection against attacks hidden in the GTP, SCTP, and MMS traffics.

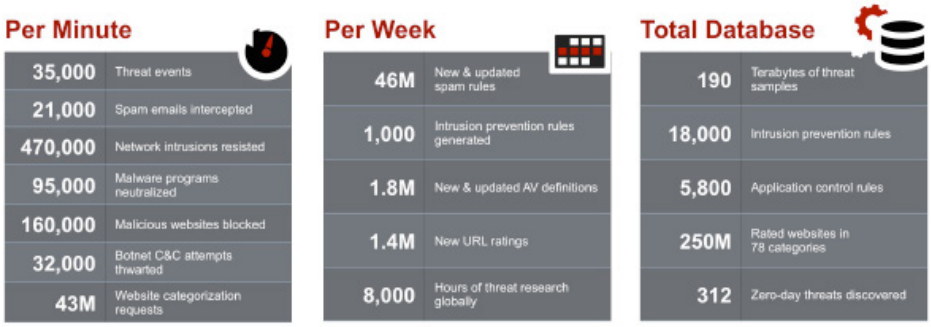

FIGURE 4 - VOLUME OF SECURITY ATTACKS (FORTINET DATA)

INCREASE OPERATIONAL EFFICIENCY AND AUTOMATION

In light of the massive scale and complexity, automation is the most effective path to increase operational efficiency. The deployment of FortiGuard is just one example. For mobile carriers with modernization projects that include virtualization, Fortinet offers an extensive, high-performance virtual platforms.

This includes FortiGate-VM08 all the way to VM32 and VMUL (unlimited cores), all of which have been certified to support the FortiOS-Carrier for mobile network deployment that requires GTP, SCTP, and MMS firewall capability.

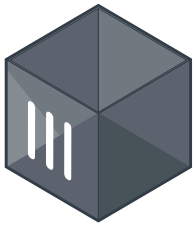

FIGURE 5 - FORTIGATE-VM08/ 16/ 32/ UL

KEY FUNCTIONALITY AT A GLANCE

GI/SGI FIREWALL

Gi/sGi firewall is a standard functionality in the high-end FortiGate platforms designed to provide protection for both subscribers and packet core critical components from cyberthreats targeted at the Gi/sGi
Internet interface.

For large evolved packet core (EPC), Fortinet recommends the flagship chassis, FortiGate 5000C, for improved extensibility and resilience, or the high-capacity FortiGate 3000 series.

MOBILE SECURITY GATEWAY (SEGW) AND ACCELERATED GTP INSPECTION (FGT-3700DX ONLY)

SeGw functionality provides protection against diverse threats coming from the access and backhaul networks, such as intercepted transmission lines from the radio tower backhauls (S1 interface) or from the out-of-region roaming partner towers (Gp/ S8 interface).

SeGw is not a standard functionality and is available only through the support of FortiOS-Carrier. FortiOS-Carrier is an extended feature set that is integrated into the FortiOS and can be activated with the purchase of a separate license.

FIGURE 6 - FORTIGATE 5000C AND FORTIGATE 3700DX

FortiOS-Carrier is supported in all high-end FortiGate platforms, including the virtualized versions, from the FortiGate-VM08 to FortiGate-VM32 (32 cores) and FortiGate-VMUL (unlimited cores). This combination and breadth of performance options provide a flexible choice for mobile carriers who want to virtualize their packet core networks.

All high-end FortiGates to support multiple domains in order to protect different areas of the packet core. The FortiGate 3700DX is unique because it comes with a customized security processor (SPU TP1) to accelerate GTP inspection, making it one of the highest-performance mobile SeGw platform in the industry.

CGN (CARRIER-GRADE NAT AND IPV6 MIGRATION TECHNOLOGIES)

At the Gi/sGi interface, another important function to add is CGN. CGN is a revenue-generating functionality because it can scale out the subscriber base to hundreds of thousands more without disrupting the legacy IPv4 infrastructure. CGN also enables a migration to IPv6.

The three benefits that CGN brings are summarized below:

1. Enables IP address expansion by relying on the CG-NAT to overcome the IPv4 address exhaustion. The support of NAT64/ DNS64 and NAT46 seamlessly connects IPv4/v6 clients to the IPv4/v6 Internet with.
2. Enhances threat prevention by hiding subscribers' and infrastructures' IP addresses from the Internet
3. Expands the number of subscribers and devices by as much as five times when compared to the FortiGate 5000C's CG-NAT scale and substantially increases revenue.

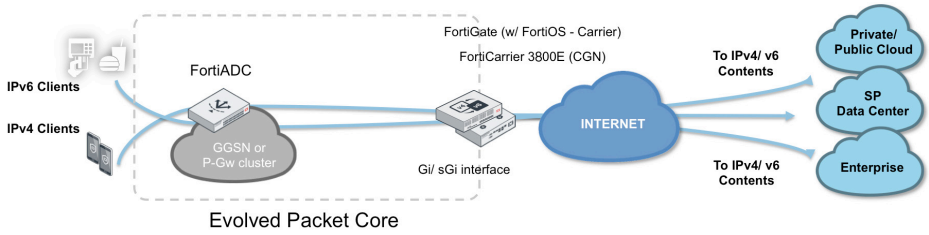

FIGURE 7 - FORTICARRIER 3000E CGN IN MOBILE CORE DEPLOYMENT

Fortinet offers the FortiCarrier 3600E (with 10 GE support) and the FortiCarrier 3800E (with 100 GE support), both are designed to be placed at the aggregation and core networks. Both platforms are based on the proven FortiGate D-series and support a customized security processor (SPU XP2). Similar to the SPU TP1 that accelerates the GTP inspection, the SPU XP2 accelerates IPv4 CG-NAT traffic processing and enables high-speed logging to meet a common government security mandate worldwide.

The main point of difference of the FortiCarrier 3600E/ 3800E CGN is the concurrent connection scalability (CCS) that is at least two times larger than the closest competitor's platform. The unmatched scalability results in the total cost of ownership that is 56% lower and places the FortiCarrier 3600E/ 3800E in the industry leading category.

APPLICATION DELIVERY CONTROLLER (ADC)

ADC is another functionality that can be deployed at the DNS controller to optimize IP packet gateway (3G GGSN and LTE P-Gw) utilization and accelerate Internet service delivery. While ADC is not a critical function in the packet core, it delivers a clear benefit in load balancing the DNS controller for the cluster of LTE packet gateways and 3G GGSNs.

It can also be deployed in the sGi-LAN or packet backbone area to assist the DNS controller in accelerating the performance of the back-end application servers such as video caching, policy controller, and IMS gateways.

DEPLOYMENT SCENARIO

CLEAN PIPE SECURITY FOR MOBILE EPC

The figure 8 shows the complete three-interface security protection. Starting on the right with, the Gi/sGi firewall, and FortiGuard to effectively scan for known cyberthreats.

The same FortiGate 5000C can be partitioned into multiple domains for maximum flexibility. With the addition of FortiOS-Carrier, the same platform can also serve as a high-performance SeGw to prevent transmission intercept and at the same time remove hidden threats coming in from local or out-of-region roaming RANs.

Combined into a solution, all the above mentioned platforms provide a complete protection for the mobile packet core.

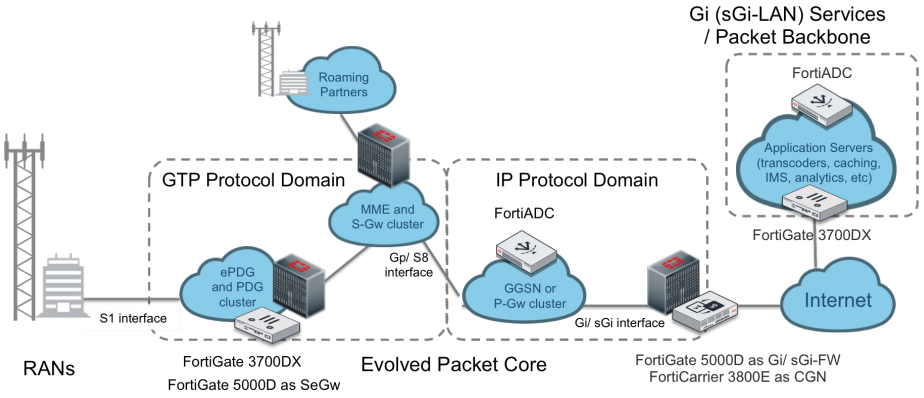

FIGURE 8 - FORTINET CLEAN PIPE SOLUTION FOR MOBILE EPC

SUMMARY

The explosive growth of mobility and anticipated migration to the cloud have posed a massive challenge to the mobile carriers globally as they struggle to cope with the imminent and constantly evolving security threats, coming from multiple vectors. To compound the issue, the unprecedented scale of the mobile networks strains many IP infrastructures.

Fortinet offers the mobile carrier a strategic security solution that is based on the reliable performance of FortiCarrier and FortiGate platforms. These platforms are purpose-built to address the new challenges of today's large mobile networks and the complex IoT networks of tomorrow. The solution provides the scale and performance to meet the most stringent security requirements and offers the following benefits:

- Flexible choice of form factors from the flexible virtual platforms to high-performance appliances and modular chassis.
- Powered by Fortinet's high-performance and high-scale security processors.
- Highly-effective and extensible security operating systems.
- Built for operational efficiency and automation to reduce the network TCO.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

59452-A-0-EN **March 17, 2017**