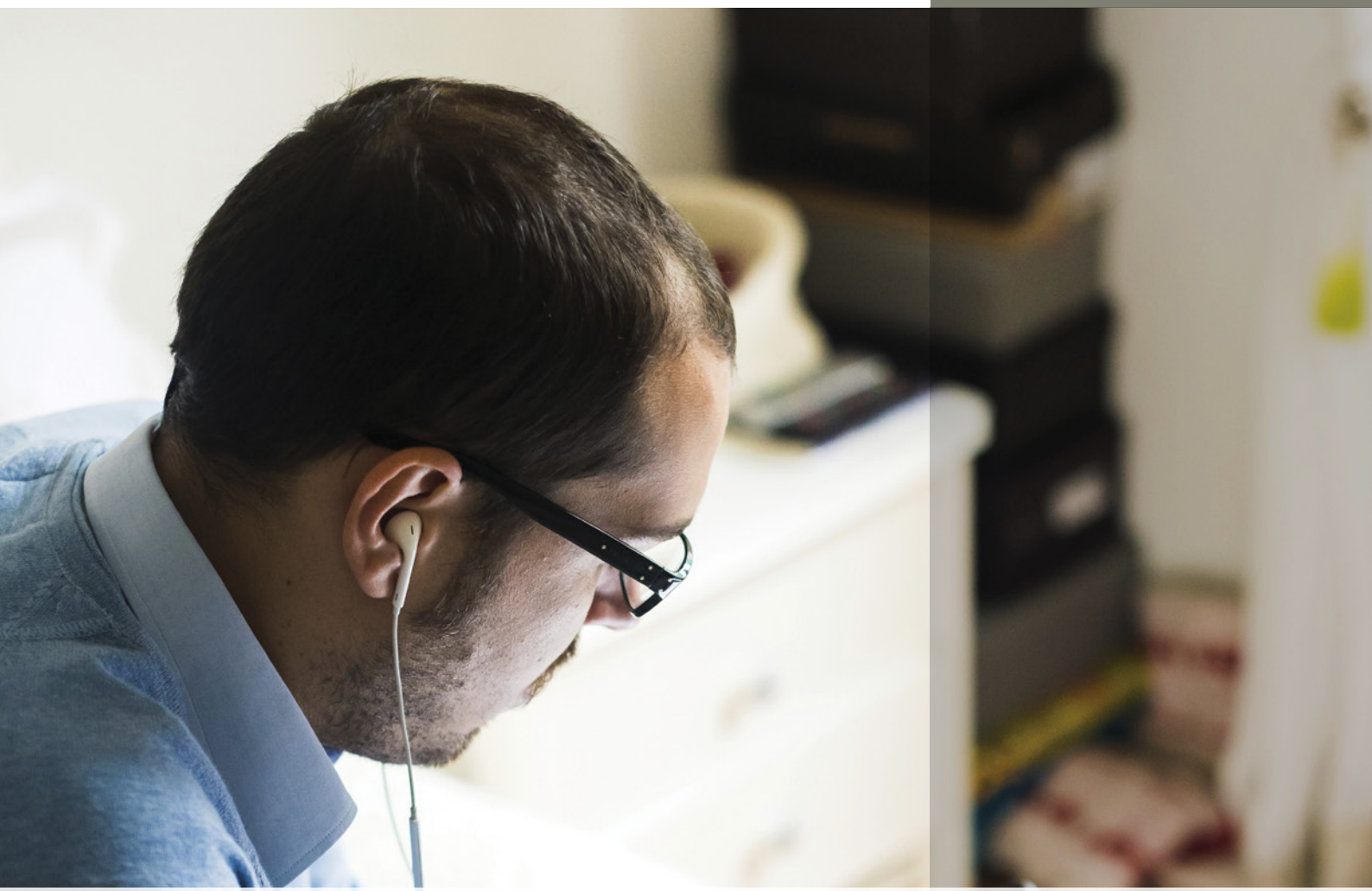
FORTINET

WHITE PAPER



The Perfect Storm

Service Provider Security In A Changing Landscape

Introduction

Profound Changes Impose New Security Model

The Telecom industry is caught in a perfect storm, driven by global technological, economic and social forces that no Communication Service Provider (CSP) can resist. The only way to survive the storm is to embrace it and adapt their business to meet these changes.

Driven to increase their revenue, margins, market share and overall competitiveness, modern CSPs are offering a growing number of IP-based value added services and applications, focused on any-time, any-where and to any-device connectivity. To support these business objectives, new technologies and network infrastructures must be deployed.

At the same time however, there are also a number of undesirable changes happening as well. The cyber threat facing CSPs has evolved enormously, wanting to capitalize on the same opportunities as the CSP. Squeezed between the two a CSP has to find a way to secure their infrastructure without impacting on their ability to respond to the opportunity in front of them. The cyber challenges facing the CSP include:

Increased Volume

With the increase of traffic through any-time, any-place, any-device, any-network connectivity, the volume of potential threats sources increases exponentially at the same time.

But volume is only half of the picture. With an increase in the number of devices and the applications running on those devices, the dramatic increase of the number of sessions per device will have a critical impact on the CSP's infrastructure, overwhelming traditional CPU based security appliances.

Standardized Delivery

Just as networks and applications have "standardized" on the use of IP, so have the legions of malware creators, allowing malware to be deployed faster and more efficiently. This phenomenon is made even more acute by the constant presence of the Internet in daily life.

Greater Motivation

As the use of the Internet has changed from something "not for me" to an integral component of daily life, the probability of success of a given malware has increased as well, from both an infection rate and financial reward perspectives. Increasing the size of the target and the probability of success automatically increases the number of threats introduced into the market.

Change Of Target

The network itself is no longer the target. The network is merely the way to access the applications and services that are the true objective of the cybercriminal.

Creativity And Sophistication

The Internet has evolved into a sophisticated worldwide commercial entity supporting an ever expending range of activities. Unfortunately, the threats borne by the Internet have evolved at even a faster pace. To ensure their survival against the defenses created to block them, the various forms of malware have become increasingly sophisticated and creative.

Wide-Scale Ubiquity

Gone are the days of different service providers for different kinds of networks. In most cases, the modern CSP has a single, IP infrastructure from which all services are delivered. While delivering a wide range of service and cost efficient, once a threat is able to enter the network it could potentially have unrestricted access.

Rather than turn to point solutions to address these issues individually, a CSP must create a security "DNA" into their network infrastructure. Engineering security into the fabric of the infrastructure needs to be the order of the day, not the exception.

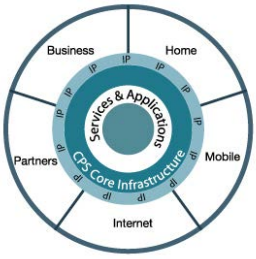
Doing so will ensure that as the network grows and evolves to meet the market and commercial changes, the underlying security grows and evolves at the same time to meet the growing cyber challenge. This paper will provide a high level presentation of the modern CSP's principle service domains, threat related "critical security spots" and the Fortinet security solution.

The Changing Landscape

Before IP became a household word, CSP networks could be considered as closed, individual islands based on proprietary technologies serving the specific needs of the network. As such, they were also relatively secure. All of that changed with the widespread adoption of IP technology as the de-facto communication standard, the wide spread availability of broadband, and the penetration of the Internet to every aspect of our economic and social life. Leveraging all of these changes has led to a staggering growth in connected mobile devices. What this all means is that while the CSP is able to take advantage of an all-IP infrastructure and offer an expanding array of services and application, it has become more and more difficult to differentiate good traffic from bad and the cybercriminal is taking full advantage of the situation.

It's An IP World

From IP Multimedia Subsystem (IMS) to Long Term Evolution (LTE), new standards and technologies have created a flat and smart IP-based infrastructure that is capable of delivering massive cost savings while delivering higher value-added services with improved Quality of Experience (QoE). However, even though the CSP has successfully transitioned from their earlier proprietary platforms to IP, the market continues to place pressure on them. IPv6 is a perfect example of this. With more and more devices accessing the Internet, regardless of how or where, the problem of supplying IP addresses to each device has returned to forefront. With the introduction of the concept of the Internet of Things (IoT), everything from televisions to refrigerators to automobiles and SCADA industrial control systems are connected to the Internet and each one of these needs its own IP address. The implementation of IPv6 will be one of the major challenges facing CSPs but cannot be allowed to affect their ability to defend themselves from malware.



We're All Mobile

Mobile devices such as laptops, smartphones and tablets continue to grow. According to industry reports[1], there will be an estimated 9 billion mobile subscriptions worldwide by 2018. Mobile devices, whether through the mobile telephone network or WiFi are constantly connected and the applications and services available to them are constantly growing. The increased level of bandwidth available to these devices means that more, content rich applications and services will continue to grow, as will the resulting revenue generated from them. Protecting this revenue stream from cyber threats will be paramount to the CSP.

Data Is KING, And It's Growing Rapidly

The shift from voice to data has had significant impact on the CSP. As data rates increased with each new generation of the GSM standard, the mobile operator has had to shift their focus and their network resources to handle the ongoing demand. The use of mobile data offload, either to CSP operated WiFi networks or to small cell devices located at the user's location, have helped to manage the traffic load but have also created a potential weak link in the security chain at the same time.

Voice Is Dead...Long Live Voice Data

The introduction of Voice over IP (VoIP) signaled the beginning of the end for circuit switch voice. VoIP allows the CSP to further leverage their investment in an all-IP backbone but it also places new demands on the CSP. In light of the level of security now required in the network, the CSP must make sure that VoIP traffic has consistent and very low latency to ensure voice quality.

Threat Proliferation And Exposure

In the information age, every piece of data is valuable to someone, somewhere. Malware writers are putting substantial effort into threat research, detection evasion, and obfuscation and mitigation of security systems. Cybercriminals are increasingly threatening ecosystems with an assemblage of tools, technologies, structures, and processes previously available only to government agencies. The proliferation of mobile devices and use of social media in the workplace is also dramatically increasing the risk of threat infiltration from any number of attack vectors.

1 Ericsson's Mobility Report (Nov. 2012)

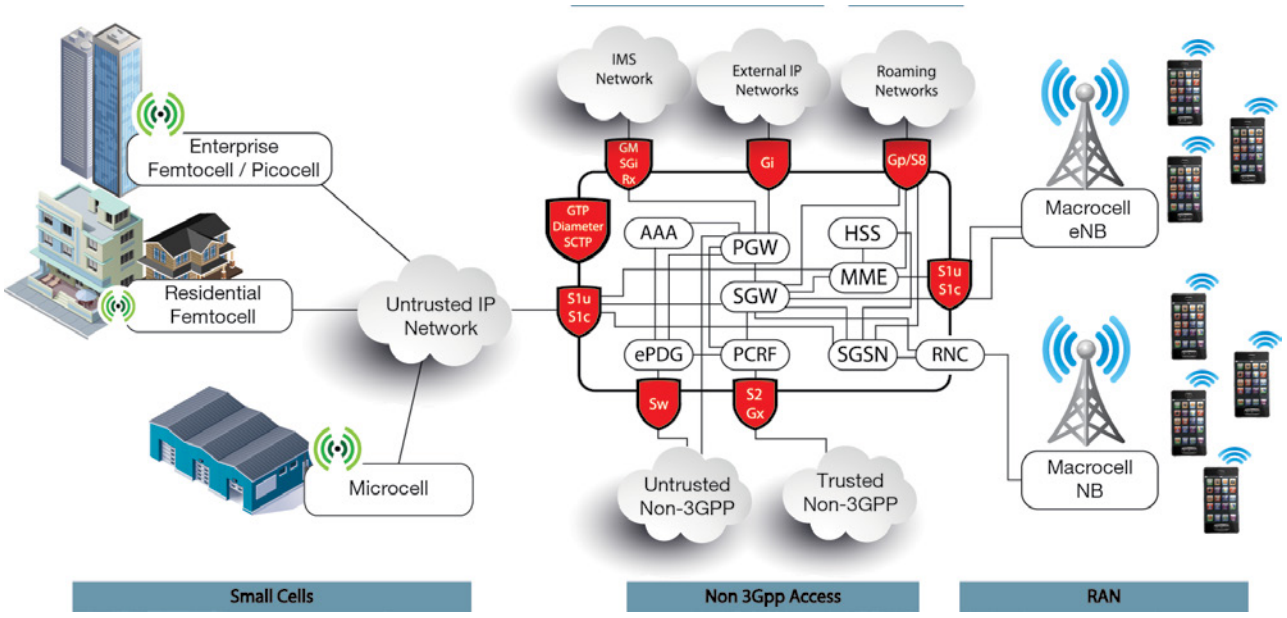
Securing the Mobile Network

LTE Backhaul, Small Cells, Non-3GPP Access And Connecting To The Outside World

The growing number of 3G/4G mobile devices and the data volume they generate, the all-IP nature of LTE and the always-connected user mentality opens the CSP's mobile network to a growing number of threats. Some of these threats will be against the network and its applications and services. However, due to the increasing popularity of 3G/4G as an Internet access method for mobile devices including laptops, the scale and power of potential botnets will increase as well. Botnets that could be used for attacking external targets or the mobile network itself.

The growing importance, usage and threat associated with the CSP mobile network, as shown in Figure 1 demands an uncompromising security solution to protect the network and its interfaces to other networks and domains.

FIGURE 1: THE MOBILE NETWORK



Radio Access Network (RAN) To Evolved Packet Core (EPC) Interface Security

Unlike 3G networks, where the traffic is encrypted from the mobile device all the way to the Radio Network Controller (RNC), in LTE networks the encryption from the User Equipment (UE) stops at the eNodeB (eNB) leaving a clear IP traffic path to the EPC. There are two interfaces between the eNB and the EPC which use the SCTP and the GTP protocols.

3GPP recommends the deployment of a Secure Gateway (SeGW) to provide IPsec tunneling on the interfaces between the eNB and the EPC to protect against threats, such as eavesdropping. However, IPsec alone is not enough to provide the required level of security. "Bad" traffic, which may originate, for example, from the UE or physical tempering with the eNB, will still be tunneled and arrive at the EPC.

The SeGW must be able to support a large number of IPsec tunnels and SCTP and GTPv2 firewalling. The functions of the SeGW should be hardware based to support the throughput and latency needed to maintain service levels. The SeGW must also support both Public Key Infrastructure (PKI) and Pre-Shared Key (PSK) encryption methodologies.

Small Cells: Mobile Core Interface Security

The growth in mobile data volumes and the need for mobile data offloading has boosted small cells deployments, which have an unsecured access to the mobile core. Positioned closer to the consumers, these deployments are difficult to physically hide and protect, thus representing a security vulnerability.

Small cells technologies, such as Femtocells, Picocells and Microcells (NHB as defined by 3GPP), provide the same functionalities as NodeB (NB) and eNB and use the same interfaces to access the Mobile Core. To secure such a deployment scenario, with large scale IPsec tunnels and PKI and PSK encryption requirements, connections from small cells should be terminated in a SeGW with the same qualities as that used for terminating the connection from an eNB.

Roaming To Mobile Network Interface Security

Roaming requires that home and visited networks are interconnected and share sensitive information such as user information stored in the Home Subscriber Server (HSS). The rise of VoIP and data roaming results in the intervention of multiple service providers, which include Over The Top (OTT) players, VoIP providers, and Mobile Virtual Network Operators (MVNO). Consequently, security weaknesses on the roaming networks connected directly, or via a GPRS Roaming eXchange (GRX) / IP Packet eXchange (IPX) service provider, may expose the CSP to additional threats.

With roaming, security threats typically focus on affecting service availability and quality through DDoS attacks such as SYN flooding, data flooding and spoofing. However, the interfaces used between a mobile operator and its roaming partners are also susceptible to data thefts, SQL injections and overbilling attacks.

To enforce the appropriate protection while providing visiting customers with a continuous and high quality service, the CSP must deploy a carrier-grade, hardware-based firewall with native IPv4/IPv6 and GTP/GTPv2 support, Diameter and SCTP firewalling, deep-packet content scanning and rate limiting. All protocol inspection must be performed in hardware so that the scalability requirements are met with zero performance degradation.

Untrusted Non 3GPP Access to Mobile Network Interface Security

In LTE, Trusted and Untrusted Non-3GPP Access Networks use access technologies whose specifications are outside of the scope of 3GPP. Public WiFi is an example of an untrusted, non-3GPP access. According to the 3GPP definitions, Trusted Non-3GPP accesses can connect directly with the EPC, while Untrusted Non-3GPP accesses must connect with the EPC via the Evolved Packet Data Gateway (ePDG) which acts as the termination point of IPsec tunnels established with the UE.

As with any untrusted IP network access, IPsec tunneling by itself does not provide the level of security control needed to protect the CSP mobile network from data theft, malware, and other malicious attacks. In addition to high IPsec tunnel concentration, a combination of hardware-based Deep Packet Inspection (DPI) with contextual analysis of the data must be deployed in order to provide the most fine-grained security enforcement.

External IP Networks Interface Security

A mobile network's interworking with external IP networks may represent a significant risk as most of these networks are considered untrusted and are out of the CSP's control. Some of them, like the Internet, represent the most common entry point for malicious attacks.

The mobile network connects with external IP networks via the Packet Data Network Gateway (PGW). The PGW terminates the SGi/Gi interface towards the external network and is responsible to act as an "anchor" of mobility between 3GPP and non-3GPP technologies. These interfaces use the IP based protocols GTP/GTPv2 and Diameter.

The SGi/Gi interface must be fortified to protect against a wide range of threats including DDoS, data theft, Botnets, and overbilling. Due to the enormous quantity of traffic transiting through this interface and the high number of sessions, hardware-based DPI for protocol and application inspection and very low latency are essential to any security implementation around this interface.

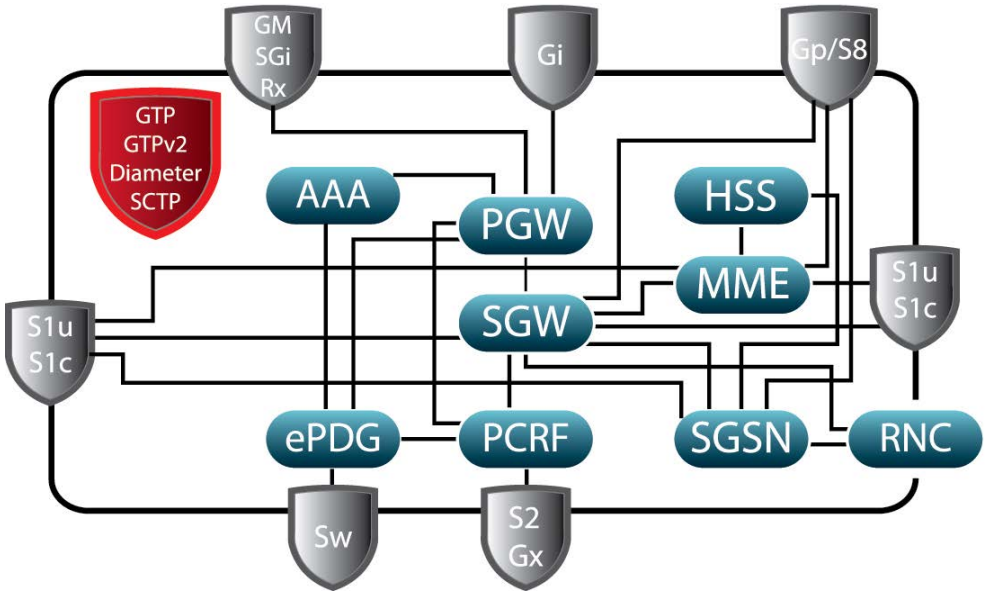
Inward Mobile Core Security

With the introduction of 4G Evolved Packet System, EPC components have been added to the "traditional" 3G core components of the CSP mobile network, as seen in Figure 2. As discussed earlier in this document, an important step in protecting the mobile network is to fortify each access point and interface that acts as a gateway into the mobile network. This is, however, not enough. Internal factors have the potential to pose real threats to the integrity, availability and QoS of the services offered by the CSP. These internal factors may include configuration mistakes, application misbehavior, mobile device originated malware and botnets, internal malicious attacks and data thefts.

It is evident that similar security mechanisms to the ones that must be deployed on the mobile network's external borders are required within the mobile network itself.

The best solution, from CAPEX, OPEX and operational perspectives is to deploy a security platform that is powerful enough in terms of performance, low latency, and depth and breadth of capabilities, to provide end-to-end protection. By securing both the network's external interfaces and the internal network itself, the deployed platform represents a coherent, cost-effective and easy-to-manage solution.

FIGURE 2: THE 4G EVOLVED PACKET CORE



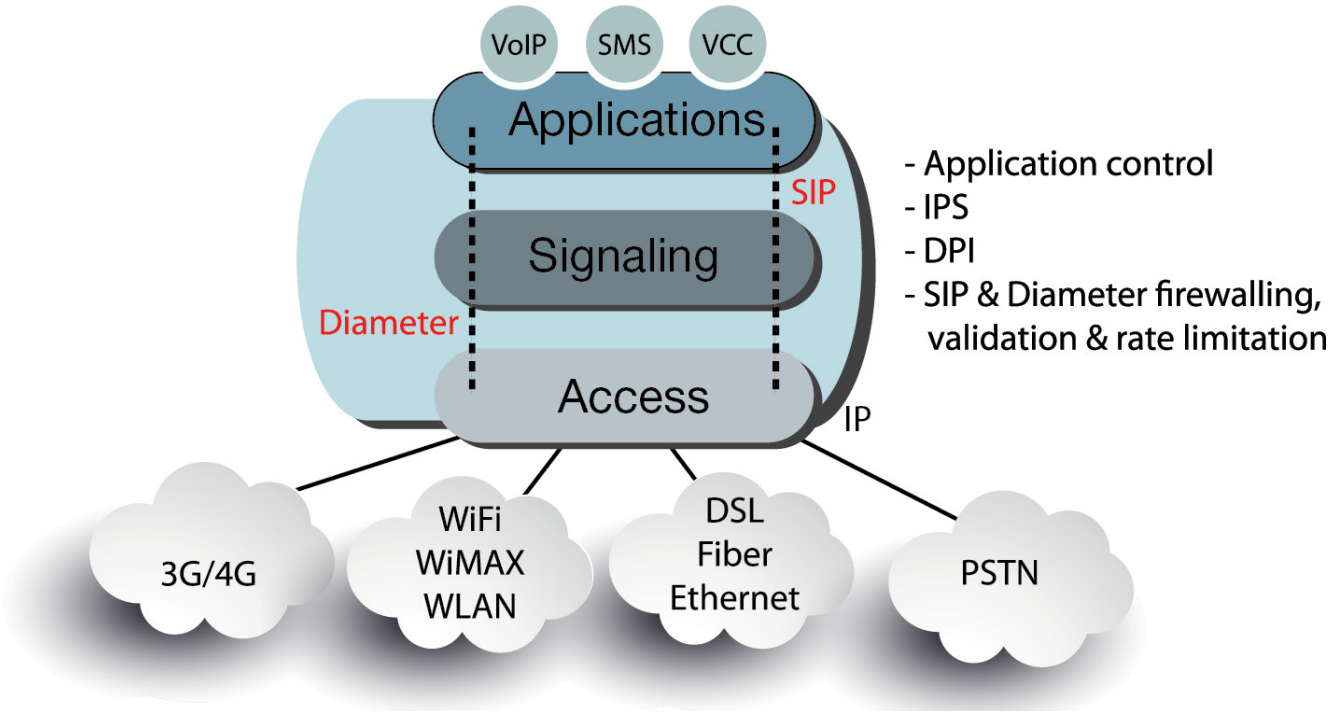
Securing the Mobile Network

The Growing Importance of IMS Demands Growing Security

As 4G becomes widely available, IMS will play an ever bigger and more important role in enabling both basic (such as VoLTE and SMS) and advanced services. In the long term, new standards and technologies, such as the Rich Communication Services (RCS) initiative, will continue to mandate the use of IMS to provide the infrastructure for delivering multimedia services.

Given its increasing strategic role in enabling value added services/applications and QoE, all representing the key revenue engines for the CSP, the IMS represents a growing target for malicious attacks. The complexity of the IMS and its growing importance for IP-based services require strong security at the interfaces with external networks to protect the IMS from threats and vulnerabilities propagated intentionally or by misconfiguration/misbehaviour.

FIGURE 3: IMS



Securing the Cloud And The Datacenter Hiding Behind It

Hybrid Security For A Hybrid Environment

Clouds are dynamic and automated environments where pools of computing resources are available to support any device or application access, anytime, anywhere. The move to virtualized datacenters and the cloud has changed the way data and services are delivered and consumed. Public and hybrid clouds use multitenant architecture to maximize ROI and reduce OPEX. Large quantity of sessions and transactions can now be treated more cost effectively.

These Internet-connected, highly dynamic and transaction-rich environments require high performance and flexible security both at the physical infrastructure and the virtual planes. Visibility into virtual machine traffic and the ability to tie security policies to virtual machines is a mandatory requirement. A viable and cost-effective security policy for the cloud must be based on the following foundations:

Securing Both The Physical & Virtual Layers

Physical firewalling is required to control and secure data at the physical layers, such as the traffic between physical servers, traffic between virtual machines and data storage, Internet traffic, etc. Virtual firewalling is also required to control and secure data between virtual machines on the same servers and any data that remains in the virtual layer.

Follow The White Rabbit

As virtual machines are created and relocated between physical servers, security protection must follow in an automated and orchestrated manner.

Multitenancy

Sharing the cloud's resources and allowing access to different groups of users is crucial for a cost-effective and competitive cloud operation. Providing the security between these groups of users and the resources available in the cloud via multitenancy is a must.

Zero Performance Impact

The security platform in place, both physical and virtual, should not impact the performance, QoS and QoE of the services and applications delivered by the cloud.

Single Pane Of Glass Management

Centralized and simplified management, visibility and analysis must be in place, for the physical, virtual or hybrid security deployments.

Securing Applications

Contextual Security

With the stagnation of traditional revenue streams, CSPs are looking at new multimedia applications as a growing revenue source. As threats have evolved to now target the applications, protecting them must also evolve to address the changes brought by new types of applications, social behavior and technologies.

The availability and integrity of these multimedia applications and service platforms must be guaranteed. Enforcing fine-grained security policies to identify and eliminate threats is a must in a dynamic environment where users and applications are increasingly virtual. Modern security platforms must allow the CSP to create contextual security policies that bring together the user, application and content to protect against threats that may impact the delivery of the required application/service to the correct user/device with the appropriate QoS/QoE.

To enable the effectiveness and continuity of application delivery and protection, the following security foundations are required:

Application Context

Intelligent scanning, analysis and actions based on multitude of contextual application usage variables, such as type of application, the usage pattern, type of UE, etc.

Contextual Granularity

Security actions for applications must be as precise as possible and can be based on the contextual variable analysis, ranging from blocking a user from accessing an application, to traffic shaping and rating.

ASIC-Based DPI

Deep Packet Inspection is required in order to be able to provide the raw data for analysis and decisions making process. This processing intensive activity must be performed without performance degradation and with a consistent and very low latency.

Carrier-Grade Performance

The above actions must be performed on the very large quantity of data and transactions flow between users and applications in a manner that guarantees complete security enforcement with zero service and QoE degradation for the application's users.

Managed Security Service Provider

Many CSPs now provide a managed security service to both internal and external customers.
MSSPs face considerable challenges:

1. They must ensure compliance with regulations of the outsourcing organisations
2. They must guarantee that the enterprise, its infrastructure, data and employees are well protected from an ever-growing set of threats
3. They must ensure the cost-effective scalability and manageability of their solution.
4. They must be cost-effective and competitive based on the market segmentation and requirements.

The CSP's Managed Security Service Platform and appliances should have the flexibility to provide, using the same platform, tailored managed security services to any or all of the below:

- Home workers and teleworkers
- Small and Medium Enterprise
- Large Enterprise
- Institutions and government agencies
- Cloud environments

The following MSSP models should be enabled through the Managed Security Services platform:

1. "Clean Pipe" model

Secure Internet connections to the home users and to very small businesses. To enable cost-effectiveness and competitiveness, the platform should support a very significant number of "clean pipes", thus reducing significantly the per-subscriber CAPEX.

2. "Centralized" Model

Cost effective, centralized and tailored security services for SMEs. This is achieved by allowing the Managed Security Service Platform to support thousands of virtual domains, or virtual firewalls. Each or several virtual firewalls providing a wide range of security capabilities can then be associated with an individual customer, making the investment in this model a highly competitive offering for the SME business segment and an attractive ROI for the CSP.

3. "CPE" Model

This model enables the MSSP to meet demanding security needs from large, distributed enterprises and the cloud. This model is based on a centralized platform and CPEs to provide full security to the distributed enterprise. The availability of both physical and virtual appliances is crucial for the enablement of an adapted managed solution for virtualized datacenter and cloud security.

Fortinet's Security Platform

Sound Foundations for a Changing Environment

With Fortinet's security platform, illustrated in Figure 4, security becomes an organic part of the CSP infrastructure. Its architecture, security operating system and extensive line of physical and virtual security appliances, come together to provide an intelligent, highly adaptive and high-performing "security DNA".

These Internet-connected, highly dynamic and transaction-rich environments require high performance and flexible security both at the physical infrastructure and the virtual planes. Visibility into virtual machine traffic and the ability to tie security policies to virtual machines is a mandatory requirement. A viable and cost-effective security policy for the cloud must be based on the following foundations:

Security In And Out

Fortinet's security platform has been designed and built to specifically address the security requirements that span a CSP's IT infrastructure, services and applications. It relies on two main pillars:

1. A purpose built operating system, FortiOS, which provides the intelligence and features to actively secure the CSP's domains.
2. A high-performance hardware platform, FortiGate, which allows CSPs to meet their service and customer QoE expectations. The FortiGate platform is powered by custom developed FortiASIC hardware processors to enable deep packet inspection while delivering carrier grade throughput performance.

Scalability

As the CSP's infrastructure evolves in terms of the volume of customers and the range of services and applications it offers, Fortinet's security platform uniquely scales up to effectively deal with the traffic, analysis and treatment of the multimillion sessions and transactions generated per second. And it does so in a cost-effective and manageable fashion to meet the required QoS and QoE for its customers.

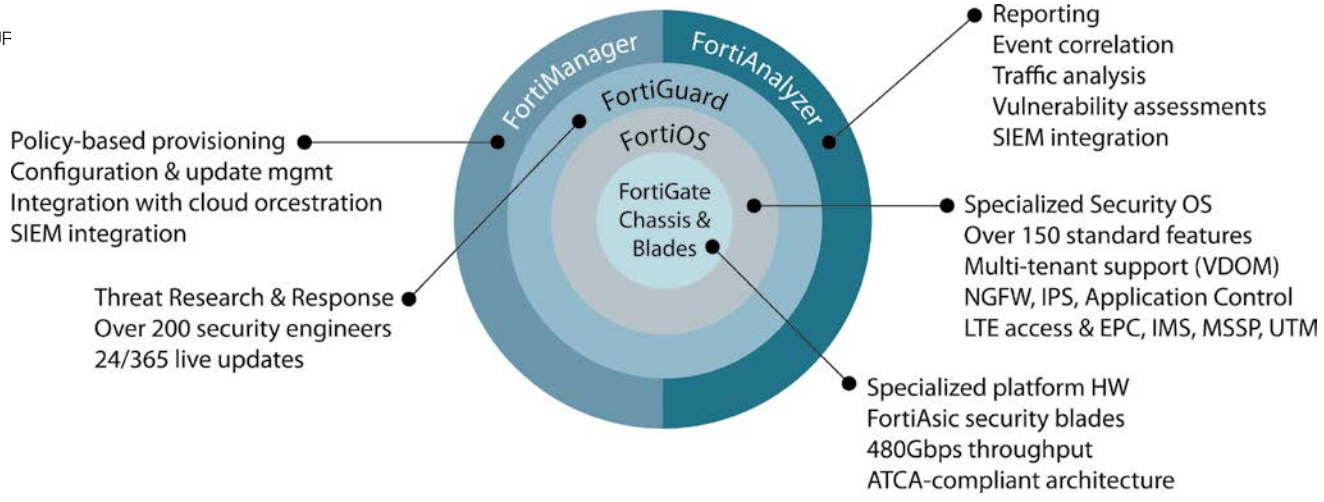
Evolution Friendly Architecture

The growing pace of the Internet and technology forces a rapid evolution of the CSP's infrastructure, services, and applications and increases the severity of the threats that it faces. Fortinet's security platform, through its FortiOS operating system, provides a common architecture for both virtual and physical environments to address those challenges. This architecture allows the CSP to obtain a maximum return on their investment and to evolve its security solutions with minimal CAPEX and OPEX implications.

Learning Intelligence

In order to proactively secure and protect, a security platform must be able to keep up with the ever-changing threat landscape facing the CSP and its customers. At Fortinet this is achieved by continuous research and response to the evolution of threats by FortiGuard Labs. The FortiGuard threat research and response service keeps FortiOS continuously updated to ensure its maximum efficiency.

FIGUF



Fortinet's Security Platform Components

FortiGate

FortiGate firewalls are high-performance, Application-Specific Integrated Circuit (ASIC) based hardware platforms developed in-house by Fortinet. Fortinet's FortiASICs allow FortiGate appliances to achieve levels of latency and consistent throughput unparalleled in the industry. Complementing the ASIC design is high density10 Gbs and 40 Gbs Gigabit Ethernet support, giving the FortiGate the ultra performance and architectural flexibility needed for the demanding CSP environment.

FortiOS

FortiOS - FortiOS is a security-hardened, purpose-built Operating System that is the foundation of all FortiGate network security platforms. With over 150 standard features including network level Antivirus and Antispam, Intrusion Prevention System, Data Loss Prevention, application control and Web filtering. All of these security features are designed to run simultaneously with optimum performance and minimal latency, thanks to the FortiASIC hardware design. As the FortiGate must seamlessly integrate into the network topology, FortiOS also features a full suite of routing protocols, Virtual Private Networking (VPN) and WAN optimization features.

FortiGuard

FortiGuard Lab's continuous multi-threat security research provides the foundation for the FortiGuard's subscription services designed from the ground up to optimize performance and maximize protection while giving Fortinet customers access to the company's threat intelligence capabilities as a service-based model. FortiGuard Security Subscription Services include continuous, automated updates for antivirus, Intrusion Prevention, Web filtering, antispam, vulnerability and compliance management, application control, and database security services. This service facilitates the CSP's ability to identify and protect its infrastructure, applications and services against known and potential threats, attacks, and exploitations.

FortiManager and FortiAnalyzer

FortiManager and FortiAnalyser integrate with FortiGate to deliver a consolidated "single pane of glass" management consoles for a rapid, efficient and cost effective security infrastructure management. FortiManager provides the essential tools needed to effectively manage a Fortinet-based security infrastructure while FortiAnalyzer provide the CSP with Centralized Security Event Logging, Reporting, Forensic Research, Content Archiving, Data Mining and Malicious file quarantining.

Fortinet's Security Platform

DOMAIN	FORTINET'S SECURE SECURITY PLATFORM
Securing the Mobile Network	▪ 3GPP Security Gateway ▪ High capacity IPsec VPN concentration ▪ SCTP, GTP/GTPv2 and Diameter Firewalling ▪ Diameter rate-limiting, content inspection and validation ▪ IPv4 and IPv6 Carrier Grade NAT (CGNAT)
Securing IMS Infrastructure	▪ L3 and L4 firewalling ▪ Diameter rate-limiting, content inspection and validation ▪ Application control and intrusion detection and prevention (IPS)
Securing the Cloud	▪ Support for large number of Virtual Domains (VDOM) for large scale multi-tenancy ▪ Both physical and virtual security appliances ▪ SDK for Cloud orchestration and SDN integration ▪ Single management for hybrid implementations (single pane of glass management)
Securing Applications	▪ Next Generation Firewall ▪ Deep Packet Inspection (DPI) ▪ Application awareness and control ▪ Intelligent scanning, analysis and actions based on contextual application usage variables ▪ Fine-grained security actions based on the contextual variable analysis
Managed Security Service	▪ Large range of physical and virtual security appliance ▪ Common Criteria EAL2+ and EAL4+, FIPS 140-2 and ICSA certified ▪ Up to 6000 Virtual Domains (VDOM) per FortiGate chassis ▪ Centralized management, visibility and analysis with granular control of multiple devices. ▪ Delegated administration and service portal integration for customer self-service
General	▪ Specialized FortiASIC HW for unparallel performance ▪ Extremely low latency for deep content scanning ▪ IPv4 and IPv6 Carrier Grade NAT (CGN) ▪ Network management integration with CSP SOC and SIEM platforms. ▪ IPv6 Ready ▪ FortiGuard proactive threat research service

Conclusion

The multiple changes impacting the CSP touch the very foundations of the services they provide and the ARPU upon which their business depends. As the rate in which technology and social behavior accelerates, it is imperative that CSPs embrace the necessary internal and external transformations to stay competitive, while keeping up with the evolving security threats at the same time.

Point solutions to deal with specific threats cannot be effective over time and always end up being expensive both in CAPEX and OPEX. Considering the wide range of technologies, applications and services deployed by the CSP, it may seem that a single security solution across its infrastructure and domains could be an exercise in compromise. Rather than compromise, CSPs increasingly turn to the only company who can offer a complete, end-to-end security solution. That company is Fortinet.

With industry leading performance, an extremely rich feature set and the ability to provide an end- to-end solution, Fortinet empowers the CSP to pursue its strategic goals while ensuring the security and protection of its networks, applications & services, employees, customers and partners

www.fortinet.com

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

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

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

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480