EMERGING SECURITY CHALLENGES IN CARRIER-CLASS FIREWALLS

The shift from 2G/3G to 4G/LTE not only requires a transition to an all-IP network, but it is also a significant demand driver. Over the past five years, mobile network subscribers have grown at a greater than 139% compound annual growth rate, and data traffic is growing at a rate greater than 60% per year. Both are expected to hold steady at these growth rates over the next several years.

The near logarithmic growth in subscribers and data has led to a series of security challenges. Mobile network operators were able to secure their 2G and 3G services against attacks by deploying IP security for their core network assets.

In modern all-IP 4G/LTE networks, however, attackers can access unencrypted user traffic, or network control signaling. In addition, carriers need to address the security challenges associated with the increasing deployment of public-access microcell base stations. These have become popular options in shopping centers, shared offices, underground facilities, etc. but suffer from being physically accessible by potential attackers. Diameter traffic, or the signaling protocol used for authentication, authorization and accounting of LTE networks, now constitutes as much as 20-30% of the network traffic.

Further, SDN and NFV concepts have become increasingly integrated into LTE mobile networks. Even though the shifting of platforms from traditional security appliances to virtual solutions will help lower costs and improve network performance, SDN will create new security challenges as it places network control and access in a more central position while enabling virtualized network functions.

According to an October 2014 report from Gartner[1], Check Point is estimated to be the third largest provider of carrier-class network firewall (CCNFW) security solutions, outside of Cisco and Juniper who provide most of the CPS router and switch architectures (based on CCNFW 2013 market share revenue estimates). The Check Point Carrier-Grade platforms provide advanced inspection and security for LTE protocols including GTP, SCTP and Diameter to protect against sophisticated attacks such as Spoofing, DDoS, Signaling Storm, over-billing attacks and malware.

DIFFERENTIATORS FOR CARRIER CLASS NETWORK FIREWALLS

In their 2014 competitive landscape report, Gartner cites[2] the key differentiators all carriers should demand in their Next Generation Firewall solutions:

- **Speeds**—CCNFWs must be capable of at least 40 Gbps throughput, 10 million concurrent sessions, 100,000 connections per second and the ability to generate 100,000 logs per second while introducing no more than three milliseconds of latency.
- **Standards and protocol support**—Common TCP/IP protocols, common routing protocols (such as BGP and OSPF), encryption protocols (IPsec/SSL), multicast protocols (UDP), authentication services (RADIUS/Diameter) and optional support for LTE protocols (such as GTP, SCTP, Diameter and SIP) and both IPs (IPv4 and IPv6).

[1] Gartner, Competitive Landscape – Carrier-Class Network Firewalls, pp.4-7, Gartner, October 2014
[2] Ibid, p 3

- **Management**—They must support command line interface (CLI), Web graphical user interfaces (GUIs), fat/rich/thick client capabilities and (optional) API interfaces. They must have features such as multitenant logging and reporting, applying policy across multiple domains, strong role-based workflow management and integrations with trouble ticketing systems.
- **Form factor**—They can run on either commercial off-the-shelf (COTS) servers, supporting x86 and virtual machines (VMs), or purpose-built hardware. They must support tight integration with the evolving software-defined networking (SDN) and network function virtualization (NFV) standards, so they can be managed as part of a larger orchestration ecosystem.

Check Point is well known in the carrier space with over 2500 communication service provider (CSP) customers worldwide, many deploying the Check Point 61000-Carrier firewall. Check Point's 61000-Carrier Security System delivers a throughput of up to 400 Gbps and supports 3 million concurrent connections and 210 million sessions per second. Check Point is also the only vendor to offer inspection on all LTE protocols, including GTP, SCTP and Diameter. This gives integrated security for LTE networks, protecting IP internet connectivity for devices with IPv4 and IPv6 addresses with the most scalable carrier-grade NAT (CGNAT) firewall.

CHECK POINT CARRIER-CLASS NETWORK FIREWALL (CCNFW) OPTIONS

Check Point offers several carrier-class network firewall options. Our most popular firewall solution, the 61000-Carrier shown in the table on page 5, we believe meets or exceeds all of the key performance measures Gartner identifies as differentiating in next generation carrier class firewalls. For smaller carriers requiring less capacity, we also offer the 41000-Carrier, and 21000-Carrier platforms that carry all of the same advanced features only at lower capacities. Even our smallest 21000-Carrier platform, a compact 2RU appliance with best price/security in the industry for S1 and CGAN security, has clean pipe value-add services, carrier-grade NAT (CGNAT) supporting IPv4 and IPv6, and supports LTE protocols including GTP, SCTP and Diameter.

Our carrier-class network firewall appliances support Virtual Systems. Virtual Systems deliver network security consolidation and utilize software blade modularity providing Firewall, VPN, Identity Awareness, Advanced Networking and Clustering, Mobile Access, IPS, and Application Control and Anti-Bot. Virtual Systems can be orchestrated using SDN and NFV concepts to achieve the elasticity and security on demand while reducing the overall operational costs.

Find a full list of our available carrier-class firewall solutions at the end of this paper.

21000 Appliances

41000 and 61000 Security Systems

ADVANCED CCNFW FEATURES

Check Point's Carrier-Class Network Firewall platforms provide the industry's most powerful Telco security solution with utmost performance and capacity to protect the continuous growth of 3G and 4G LTE network infrastructures. These unique platforms enable Mobile Network Operators to use a unified platform to secure all interfaces including Radio Access, Internet and Roaming. Each scalable platform comes with advanced inspection and security for LTE protocols to protect against sophisticated attacks such as Spoofing, DDoS, Signaling Storm, Over-billing attacks and Malware. Some of our other advanced carrier-class network features include:

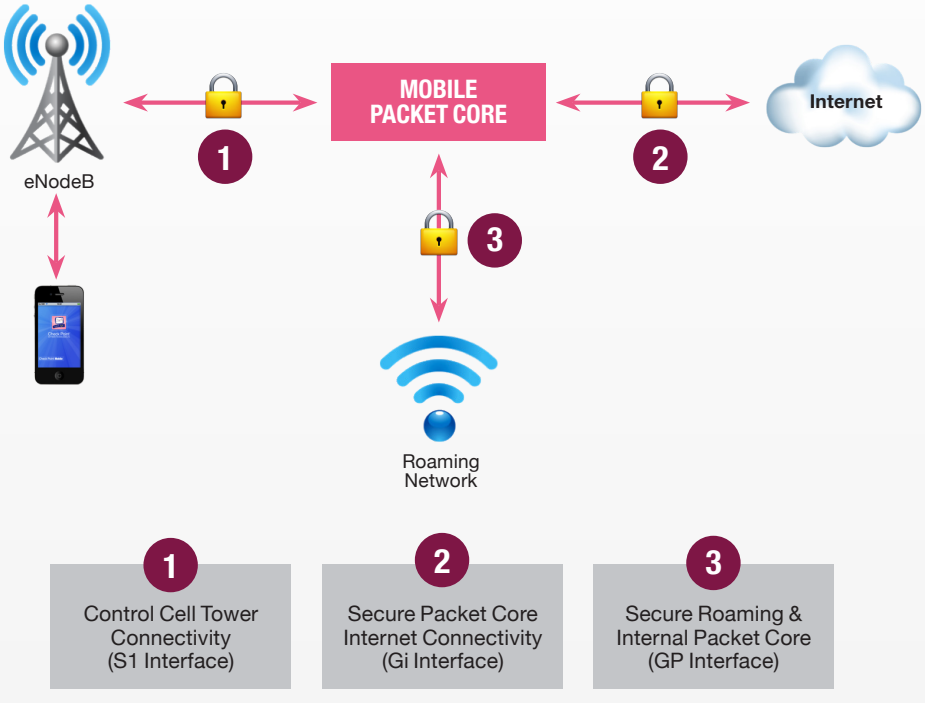
- **Carrier Grade NAT:** Our large scale NAT allows Internet access control to millions of mobile subscribers. Mobile devices using both IPv4 and IPv6 can securely connect to the Internet. We protect the Mobile Packet Core network from DDoS attacks, signaling storm, port scan, sweep scan, spoofing, over billing attacks and advanced application malwares and threats. The solution can also link RADIUS accounting records to the device's IP through Identity Awareness, enabling the Telco to provide user-specific information at the request of the relevant authorities.
- **Radio Access IPSEC Security:** Our CCNFW products securely connect thousands of 4G LTE Radio Stations (eNodeBs) to the Evolve Packet Core network. The IPSec can authorize Radio Stations' connectivity, encrypt user data traffic and easily provision the IPSec connectivity when adding more Radio Stations. It also ensures service availability with backend services using Dead-Peer-Detection and it is a fully redundant hardware platform. ESP and IKEv2 are supported to deliver data traffic confidentiality and integrity with AES, SHA-1 or Triple DES encryption algorithms. We also protect against eavesdropping and data tampering on the control plane and user traffic.
- **LTE Protocol Security:** We inspect and secure 3G and 4G IP protocols including GTP, SCTP and Diameter. Mobile Operators can securely connect the packet core to untrusted interfaces such to roaming partners or the radio network. We enforce roaming agreements using Carrier Identity-Based Policy and provide protections for DDoS, over billing attacks, data leakage and unauthorized access. We use advanced Diameter and GTP protocols policy to protect subscribers' data in MME and HSS, and advanced security with Software Blades including IPS, Anti-Virus, URL Filter, Application Control and Anti-Bot to inspect subscriber traffic within the GTP data plane.
- **Intrusion Prevention System (IPS):** The IPS Software Blade is NSS Labs' top-rated delivering complete and proactive intrusion prevention. It was also ranked #1 in Microsoft and Adobe threat coverage 3 years in a row. It secures your network by timely and effectively preventing browser and application vulnerability exploits.
- **Integrated Security Management and Logging:** Our unified security management simplifies the complex task of managing the large carrier distributed resource environment. Our comprehensive, centralized security management system controls all Check Point gateways configured on all mobile network interfaces. Our intuitive graphical user interface enables IT managers to easily manage a wide range of security management functions, and our carrier-grade central lawful logging with advanced log analyzer delivers split-second search results providing real-time visibility into billions of log records over multiple time periods and domains.

- **Clean Pipe Service:** We offer the option to extend additional security services to your customers by leveraging our enterprise Software Blades security with IPS, Antivirus, URL Filter, Application Control and Anti-Bot. The additional security services can be managed through the same Internet management console used to control Carrier-Grade NAT Gateways and Radio Access Gateways.
- **Virtual Systems:** We enable security consolidation of up to 250 gateways into a hardware platform providing savings on both capital equipment investments and ongoing support and maintenance. The ability to virtualize network functions is particularly important in SDN and NFV environments.

Check Point offers a free security checkup to assess your network, providing visibility into all roaming traffic, as well as uncovering potential security risks. We perform a deep traffic analysis with detailed categorization (including geo-location and protocols) to detect vulnerabilities in all LTE protocols—including GTP, SCT and Diameter—and to identify DDoS attacks for LTE protocols.

Find out more about our carrier class firewall (CCFW) platforms by visiting: http://www.checkpoint.com/solutions/carrier-security/.

CHECK POINT 3G AND 4G TELCO SECURITY



APPLIANCES

	21700-Carrier	41000-Carrier	61000-Carrier
Production Performance (SecurityPower Benchmark — version R77 and later)			
SecurityPower	3300/3551[1]	3200 to 11000	3000 to 14600
Firewall (Gbps)	25.4	Up to 40	Up to 120
Firewall and IPS (Gbps)	5.7	Up to 25	Up to 70
SCTP Throughput	20Gbps	27Gbps	80Gbps
GTP Throughput	15Gbps	27Gbps	80Gbps
GTP Concurrent PDP Context	3M	20M	20M
VPN IMIX Throughput	Up to 30Gbps[1]	Up to 23Gbps	Up to 56Gbps
IPSec Tunnels	10,000	50,000	50,000
RFC 3511, 2544, 2647, 1242 performance tests (LAB)			
Firewall Throughput (Gbps)	78/110[1]	Up to 80	Up to 400
VPN Throughput (Gbps)	11/50[1]	Up to 17	Up to 110
IPS Recommended Profile (Gbps)	8	Up to 44	Up to 130
Connections Per Second (K)	170/300[1]	Up to 1.1M	Up to 3M
Concurrent Sessions (M)	13[2]	Up to 80M	Up to 210
Network			
10/100/1000Base-T/Max Ports	13/37	NA	NA
1000Base-F SFP (MAX Ports)	36	NA	NA[3]
10GBase-F SFP+ (MAX Ports)	13	Up to 30	16/32[3]
40GBase-F MAX Ports	NA	4	4[3]
Expansion Slot	3	6	14
FONIC Option	No	No	No
Additional Features			
Storage	2x500GB RAID 1	–	–
Memory / Max	16/32 GB	24/64 GB	24/64 GB[4]
LOM Card	Included	Included	Included
Virtual Systems			
Default/Max VS Supported	150/250[2]	125/250[2]	125/250[2]
Physical			
Enclosure	2U	6U	15U
Weight	26kg (57.4 lbs)	38.6kg (84.9 lbs)	Max: 97.24kg (214.4 lbs)
Power			
Dual, Hot-Swappable Power Supplies	Yes	3AC	5AC or 2DC
Power Input	100-240VAC, 47-63Hz	100-240VAC, 47-63Hz	100-240VAC, 47-63Hz
Single Power Supply Rating	1200W	1200W @ 110V, 1500W @ 220V	1200W @ 110V, 1500W @ 220V
Power Consumption (Max)	489W/784W[1]	2300W	5000W
DC Option	Optional[6]	No	Yes

[1] With Security Acceleration Module
[2] With memory upgrade and the GAiA OS
[3] Not including Security Switch Module Management Ports
[4] Per Security Gateway Module
[5] Includes 5 AC PSUs or 2 DC PSUs
[6] Via a Solutions Center request

CONTACT CHECK POINT

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com