Next Generation Security for 3G and 4G LTE Networks
Contents

Executive Summary .......................................................... 3
The evolution of mobile network security .......................... 4
Mobile data matters ......................................................... 5
Security implications of next-generation 4G LTE architecture ... 6
Securing the Gi Interface—protecting the Packet Core against Internet attacks ........................................ 7
Securing the S1 Interface—ensuring protection for LTE backhaul traffic ......................................................... 8
Securing the Gp Interface—protecting the packet core against roaming threats .............................................. 8
Next-Generation Security for Mobile Networks: In Summary ........ 9
Check Point Carrier-Grade Solutions for Next-Generation .......... 10
Executive Summary

As mobile network operators (MNOs) continue to grow their subscriber bases, and move further towards being Internet Service Providers (ISPs) instead of providers of basic voice and data services, they face three key challenges:

- Keeping their networks running with maximum performance and availability
- Delivering a rich, positive user experience to subscribers
- Protecting their mobile networks, customer data and devices against current and emerging security threats

Successfully meeting all of these challenges is critical if MNOs are to retain customer loyalty and trust, and maintain their growth and brand integrity. But the increasing capabilities and power of mobile devices, and subscribers’ hunger for richer, faster Internet services, is introducing a range of new security risks to both 3G and new 4G networks.

The dramatic growth in smartphone and mobile app usage is creating excess signalling in networks, impacting on network performance and, in effect, behaving as a non-malicious DDoS attack. Growing numbers of mobile devices and apps are also introducing new application-layer vulnerabilities. Furthermore, the move to IP-centric architecture in 4G LTE networks means that networks are now vulnerable to IP-based security attacks from the public Internet and radio access network (RAN) – presenting a security challenge to MNOs that previously did not exist, and demanding new approaches to network protection.

This document examines both the current and emerging security threats to mobile networks, the impact of these on network integrity and performance, and how the requirements of mobile network security have changed.

It will then show how MNOs can respond to protect their next-generation networks and subscribers, while enabling new value-add security services, using solutions from Check Point which integrate stateful firewall, IPSec VPN, IPS, Web security and other advanced security technologies.

Check Point is an established leader in Telco security, and its new carrier-grade security solutions protect LTE infrastructures end-to-end with a holistic solution, enabling unified security policies, monitoring and reporting for all carrier interfaces with unique security features. This dramatically reducing the risks to networks, secures subscriber data, reduces TCO, increases operational efficiency and availability, and maximizes revenues.
The evolution of mobile network security

Until just a few years ago, demand for mobile data networks was limited, representing a very small percentage of MNO revenues. This lack of scale meant that connections between operators’ mobile networks and the public Internet could be protected using relatively simple security architectures.

These architectures typically consist of:

- A firewall at the Gi interface between the mobile packet core and the public Internet, and the Gp interface to secure connection to roaming partners
- Stateful packet filtering to avoid spoofing attacks
- Protection against over- or underbilling attacks
- Network Address Translation (NAT) to convert users’ private IP addresses to public IP addresses
- And more recently, more sophisticated IPS and threat detection solutions to identify known attack signatures in inbound data traffic

MNOs were able to control and manage the exposure of their networks to Internet-based risks and threats with relative ease. However, the past five years have marked a significant change in the mobile devices being embraced by consumers, and seismic changes in mobile data usage and traffic volumes. These changes are having a major impact on mobile network security.

Mobile data matters

In Q1 2008, at the start of widespread availability of Apple’s iPhone, total mobile data traffic globally was around 20 petabytes per month. In Q1 2012, traffic was nearly 700 petabytes per month—a 3,500% increase in volume.

More importantly, data traffic doubled in a short 12-month period between Q3 2011 and Q3 2012, and is expected to grow 12 times between 2012 and 2018, driven mainly by video content on smartphones, which accounted for approximately 40% of all phones sold in Q3 2012. Of course, the increase in subscribers roaming while travelling is also contributing to increases in data traffic volumes for MNOs, especially with new types of roaming partner introducing traffic such as VoIP calls and more.

Total mobile subscriptions will continue to grow from just under 7 billion currently to 9.3 billion in 2018. Of these, around 55 million are for LTE services, and these are predicted to reach 1.6 billion by 2018. The figure for growth in LTE subscriptions is particularly striking: subscriber numbers will grow nearly 30X, generating a colossal amount of data traffic. This near-logarithmic growth in traffic is helping to create a security issue for MNOs.

Signalling spikes and latency

While the majority of this growing tide of traffic is user data or video content, a significant proportion is signalling created by smartphones or mobile apps. These are the underlying "I'm active" messages which update the network on the device’s or app’s availability, or deliver updates from the network to the device. The proportion of signalling traffic varies according to the device and app being used, but a typical average figure is 20% to 30% of total data traffic.
Signalling traffic not only consumes resources throughout the network core, it can also be in sufficiently high volume that it appears as a denial-of-service (DoS) attack on network or security management consoles. This is because it is difficult to distinguish ‘normal’ network traffic from maliciously-generated traffic. And if an MNO cannot distinguish ‘normal’ volumes of traffic from a malicious attack, it faces a real security challenge.

This signaling traffic also contributes to network latency. While latency has not been a major issue in recent years, especially with MNOs offering unlimited, fixed-price data plans, increasing uptake of LTE will reduce subscribers’ and MNOs’ acceptance of latency. MNOs want to position LTE as a premium product and charge for it accordingly; and subscribers who want the benefits of high throughput, will not be happy paying a premium price for lagging service.

MNOs need their networks and infrastructure—including the security solutions used to guard that infrastructure—to be able to scale to meet the ever-increasing demands of subscribers, offering maximum performance with minimum latency at all times, while enabling the MNOs to monitor and manage their infrastructure effectively.

Security implications of next-generation 4G LTE architecture
The roll-out of new 4G LTE network architecture also presents new security challenges. Unlike 2G and 3G services, which use TDM and ATM backhaul, LTE uses IP-based backhaul. As more IP-based communications is introduced to mobile infrastructures, the more it becomes vulnerable to Internet-based attacks.

As mentioned previously, MNOs could secure their 2G and 3G services against attack from the public Internet and roaming interfaces by investing in IP security for their core network assets, while being reasonably confident that their backhaul was secure—especially non-shared, private backhaul. However, the all-IP architecture of LTE networks introduces more security risks. Attackers could potentially access unencrypted user traffic, or network control signalling.

An additional security risk for both 3G and 4G networks comes from the increasing deployment of public-access microcell base stations, aimed at providing additional local capacity in public areas such as shopping centres, shared offices and more. These small devices placed in areas accessible to the public cannot be physically secured in the same way as a conventional base station, giving attackers a potentially easier entry point from which to attack the network.

Further security challenges in the LTE network architecture and packet core include interdiction of the SCTP and Diameter transport and application protocols, and distributed denial-of-service (DDoS) attacks across different elements of the mobile networks. Data signaling gateways, mobile packet core and Radio Access Network infrastructure all have potential vulnerabilities.
Mobile packet core interface issues
To exploit any of these vulnerabilities, an attacker will target at least one of the three major interfaces on the mobile network infrastructure:

- **The Gi/SGi interface**, where the GPRS / LTE mobile network connects millions of devices to the Internet and other untrusted networks—exposing networks to a full range of Web threats including malware, DoS attacks, botnets, spoofing, port scanning and more
- **The S1 interface**, which connects and authenticates thousands of eNodeB cellular base stations and towers to the mobile network
- **The Gp/S8 interface**, which connects the mobile networks of MNOs’ roaming partners and gives access to internal packet core services and data

Here, we will examine the threats and attacks that these three interfaces are vulnerable to, whether from external sources or within the provider’s network, that can disrupt the network itself or target specific systems such as billing or accounting. We will also consider the security requirements to protect against these threats.

**Securing the Gi/SGi Interface—protecting the Packet Core against Internet attacks**
As we saw earlier, smartphone sales are approaching 50% of all devices sold and it is estimated that by 2014, average per-device data usage will triple. This rapid growth in smartphone usage and increasingly sophisticated apps mean that MNOs need a scalable, robust method of handling the growing number of subscriber IP addresses, and for tracking the individual devices behind the public IP address, as carriers translate from private to public IP addresses.

This is made more complex by the need to handle the migration from IPv4 to IPv6 addressing as networks move to IPv6. This will demand that MNOs support both address schemes for a period of time. As such, MNOs need a resilient Gi/SGi Carrier-Grade NAT (CGN) solution.
One of the main reasons for using a CGN solution is to reduce the risk of ‘signaling storms’ on core and radio networks, and to avoid overbilling attacks. These storms and attacks can be caused by ‘Internet noise’—the random port scans and sweep activities that constantly happen on the Internet. These can also be generated by targeted attacks against specific operators’ infrastructure or individual mobile devices. In the latter case, the attacker can flood the mobile network with excessive traffic compromising radio and packet core signaling, blocking legitimate data traffic and causing subscribers to lose network access and operators to lose money.

Using a CGN solution on the Gi/SGi interface hides the IP address of core services and devices from the public Internet, helping to keep them secure against being targeted by malicious parties using DoS techniques. It also protects against the hijacking of a device’s or mobile station’s IP address, which can lead to ‘overbilling’ attacks.

Security requirements for protecting the LTE Gi/SGi interface

The CGN solution for securing the Gi interface should be a stateful NAT firewall solution optimized to service Internet, voice and session-based applications and protocols. Only a stateful firewall can reduce the risks arising from the sharing of IP addresses in the CGN solution, reducing the risks of overbilling attacks against subscribers and carriers.

The NAT firewall should ideally act as a single, scalable gateway, managed by a single IP address and enabling single-console security and policy management. This is preferable to chassis-based solutions that stack multiple gateway modules on top of one another, because of ease of management, simplicity and more efficient traffic balancing and management.

The solution should support IPv4 CGN, enabling NAPT and NAT44(4) with both static and dynamic mapping of addresses and ports, including port block allocation. It should also support IPv6 CGN, with v4v6 Dual Stack, 6 over 4 Tunneling, 4 over 6 Tunneling, NAT64, NAT46 and NAT66 for seamless address translation and migration.

NAT performance and throughput is also critical: as the volume of network traffic and the number of subscriber devices multiply, the NAT firewall needs to support and service tens of millions of concurrent connections, and multi-gigabit throughput of real-world mobile traffic.
The NAT firewall should be intelligent, and able to identify ‘hanging’ data sessions that are initiated in overbilling attacks. The firewall should be able to detect when the initiating party has exited the session, and terminate that session. It is also useful if the solution can 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.

It should also deliver deep packet inspection with additional security functions including IPS, Antivirus, URL filtering, Application Control and Anti-Bot. These deliver protection against attacks on the mobile network infrastructure, and also stop the network from being used for launching DoS attacks. The ability to inspect data packets provides the foundation for delivering subscriber managed security services from the same security solution.

**Securing the S1 Interface—ensuring protection for LTE backhaul traffic**

We looked earlier at how the LTE architecture’s flatter, IP-centric architecture presents new security implications for mobile networks, especially in the backhaul elements of the network. Another consideration for LTE network security is the growth in cellular sites. Analyst Heavy Reading expects that the global number of cellular sites will grow to nearly 4 million by the end of 2015, from 2.7 million in 2011. Many of these new sites will be small cells, driven by the twin demands of lower costs while delivering additional bandwidth per subscriber. This means more cell sites placed in public areas, where they are vulnerable to unauthorized tampering.

As there are no Radio Network Controllers (RNC) in LTE backhaul networks, a compromised eNodeB cell station can be used to access and attack the Mobile Management Entity (MME) and consequently take down the entire core service. And unlike 3G, a single eNodeB may connect to multiple MMEs residing in different packet cores—meaning that an attacker could reach MMEs in different core networks from a single compromised cell site.

IPSec is the standard recommended by 3GPP for MNOs who consider their LTE backhaul networks between eNodeBs and the packet core as physically insecure. However, MNOs should be assured that their IPSec deployments are highly scalable, and also offer high availability. The expected growth of LTE traffic and its bandwidth demands will demand truly carrier-grade throughput capabilities as well as compliance with latest 3GPP security standards.
Security requirements for protecting the LTE S1 interface

The security gateway should support authentication between LTE cell sites and the packet core, to prevent unauthorized access from eNodeBs to the packet core network. As such, interoperability with third-party PKI solutions is essential. This also enables certificate authentication for the eNodeB’s control plane, as well as the data plane.

The security gateway should also support ESP and IKEv2 to deliver data traffic confidentiality and integrity with AES, SHA-1 or TripleDES encryption algorithms. This protects against eavesdropping and data tampering on the control plane and with user traffic.

The gateway should also deliver SCTP deep packet inspection for the S1-MME control plane with the MME, which protects against attacks such as injection of false traffic into applications.

The security solution should also be fully scalable, offering carrier-grade IPSEC throughput and performance so that it does not introduce network latency.

Securing the Gp/S8 Interface—protecting the packet core against roaming threats

Operators must allow their mobile subscribers to access the Internet even when roaming, which means MNOs must interconnect their networks. This is done using the Gp/S8 interface to access the GPRS roaming exchange (GRX) network, which acts as a hub for connections from roaming users, removing the need for a dedicated link between each service provider.

When connected to an LTE network, mobile devices should be able to roam to both LTE and 3G networks. During the LTE transition period, operators will continue to maintain their 3G network and allow data traffic to roam from LTE packet core to 3G packet core and vice versa.

Therefore, MNOs’ packet core elements must stay secure while enabling roaming interconnectivity between other operators and untrusted networks. As the Gp/S8 interface is currently used for inter-network roaming traffic, the most common type of security threat is against the service’s availability, using DoS techniques as bandwidth saturation, data flooding, spoofing or cache poisoning. The Gp/S8 interface is also susceptible to overbilling attacks, if a mobile station is able to hijack an IP address of a legitimate station and start an illegitimate data download.
Next Generation Security for 3G and 4G LTE Networks

Security requirements for protecting the Gp / GRX interface
The key concern is protecting GRX networks against DoS or DDoS attacks between different MNOs’ networks. DoS attacks can occur if a hacker is able to maliciously insert IP packets into the GRX network domain from another IP network domain.

The security gateway should be able to deliver deep stateful packet inspection of the three protocols used over the Gp interface:

- **GTP**, used in delivering mobile data services. Monitoring GTP traffic helps in enforcing roaming agreements using carrier identity-based policies, and protects against DDoS & overbilling attacks
- **SCTP**, used in the IP transport layer for mobile networks. Monitoring SCTP traffic also helps to prevent DoS attacks using corrupt packets, and unauthorized network access
- **Diameter**, the signaling protocol used for authorization, subscriber authentication, charging and quality of service (QoS). Monitoring Diameter traffic safeguards subscribers’ data against interception on untrusted, public IP transport networks between service providers

As SCTP and Diameter traffic is growing rapidly with LTE uptake, the ability to inspect this traffic is critical to gaining early visibility of possible malicious attacks, such as Data Exposer attacks from the packet core that use unauthorized GTP or Diameter commands. And as with the security solutions for the Gi and S1 interface, performance, scalability and throughput are critical, as traffic volumes in both the control plane and data plane continue to accelerate.
Next-Generation Security for Mobile Networks: In Summary

As we noted at the start of this white paper, mobile data connections must be secure and be available at any time, and from any location. MNOs must also protect their mobile networks, customer data and devices against current and emerging security threats.

As MNOs open their network packet cores to roaming partners, the public Internet and other untrusted external networks, the security risks increase exponentially. In order to secure their entire infrastructure, MNOs must secure all LTE Interfaces, including the Internet Gi Connection, S1 LTE Radio Access, and Gp roaming connectivity.

Using a single security platform that integrates stateful inspection of each interface, together with other advanced security applications including IPS, VPN tunneling, secure NAT, Antivirus, Anti-Bot and Web security, MNOs can secure their entire carrier infrastructure end-to-end with an holistic solution.

They can also manage that security with unified policies, monitoring and reporting for all carrier interfaces. With a single, unified view of the network infrastructure and security policies, network administrators get a clear picture of events and their current security position. This in turn dramatically reduces risks to their networks, protecting subscriber data, reducing TCO, increase operational efficiency and maximising revenues.

Check Point Carrier-Grade Solutions for Next-Generation Networks

Check Point is an established leader in Telco security, with hundreds of deployments worldwide. Built on the award-winning, proven technologies used by Fortune 100 companies and Telcos all over the world, Check Point’s Telco Security solutions secure all LTE interfaces, protect the mobile packet core, secure roaming connectivity, and support a range of subscriber value-add security services. This enables MNOs and carriers to maximise their infrastructure investments with comprehensive protection, scalability, and opportunities for managed security service offerings.

Check Point has two carrier-grade platforms for delivering security for 3G and 4G LTE networks. Check Point’s Telco security solutions deliver these benefits:

Securing a carrier’s entire infrastructure

Check Point’s solutions give a single, integrated platform for securing all LTE Interfaces:

- Secure communication between thousands of radio stations (eNodeBs)
- Secure Internet connectivity with the most scalable Carrier-Grade-NAT firewall
- Secure roaming connectivity according to partner business agreements
- Control infrastructure security with unified policy, monitoring and reporting for all carrier interfaces
- Consolidate gateways and secure multiple networks with Virtual Systems, enabling seamless scaling to meet demand and simplified management
Next Generation Security for 3G and 4G LTE Networks

The strongest 3G & 4G security
Check Point offers the only solution to inspect and secure all LTE protocols including GTP, SCTP and Diameter. Check Point is the only vendor in the industry offering solutions with the capability to inspect Diameter traffic.

Our Telco solutions enable support and delivery of subscriber-based value-add security services including IPS, Antivirus, Web security and Anti-Bot.

World's fastest LTE-grade security
Check Point’s dedicated 61000, 21700 and 21600 Carrier Security platforms offer a scalable solution with optimal price-performance for carriers of all sizes.

They are the World’s fastest security platforms, with real-world traffic throughput of 30Gbps on the 2U 21600 and 21700 Carrier appliances, and up to 56Gbps on the 61000 Carrier chassis: ensuring the minimum possible latency and the capacity to scale to future mobile traffic demands.

The 61000 Carrier Security solution supports up to 70M concurrent connections, giving scalability to support the demands of leading global mobile operators and telcos.

Features & benefits of Check Point Telco solutions
Securing the LTE Gi interface

- Up to 200Gbps Firewall throughput with large UDP Packets. Supports up to 70 Million concurrent connections
- IPv4 CGN supporting NAPT and NAT44(4) with static and dynamic mapping of addresses and ports, including port block allocation
- IPv6 carrier-grade NAT solution supporting v4/v6 Dual Stack, 6 over 4 Tunneling and 4 over 6 Tunneling and NAT46 and NAT64*
- Application Layer Gateway (ALG) to enable applications that have problems with NAT (e.g. FTP, media, p2p) or NAT-Unaware
- Carrier-scale detailed central logging
- Protect against overbilling (over-charging) attacks
- Link RADIUS accounting records to IP addresses through Identity Awareness
- Multi-gigabyte CGN with deep packet inspection including, Intrusion Prevention, Antivirus, URL Filtering, Application Control and Anti-Bot
Securing the LTE S1 interface

- Interoperability with any 3rd party PKI solution using certificate authentication for the eNodeB’s control plane with the MMEs and data plane with the S-GWs. Preventing unauthorized access of eNodeBs to the packet core network.
- Use ESP and IKEv2 for traffic confidentiality and integrity with AES, SHA-1 or TripleDES encryption algorithms. Protect against eavesdropping and data tampering on the control plane (S1-MME) and user traffic (S1-u).
- Unmatched IPSec performance from 30Gbps on a 2U appliance model and up to 56Gbps on a chassis-based model (measured with real-world IMIX mobile S1 traffic).
- Support up to 50,000 IPsec tunnels with Check Point 61000
- Fast IPsec provisioning with remote eNodeB
- Check Point low-latency firewall protecting core network elements from spoofing and DoS attacks
- Using the Check Point SCTP deep packet inspection for the S1-MME control plane with the MME. Protect against application injection of false traffic and attacks.
- High availability platform with dead peer detection capability, ensuring service availability

Securing the LTE Gp interface

- Check Point Packet Core Security provides policy enforcement and deep stateful packet inspection for GTP, GTP’ (GTP "prime"), SCTP and Diameter protocols
- Granular “GTP-aware” security policies for GTP v0, GTP v1 and GTP v2
- High performance 13Gbps deep packet inspection of packet core protocols with a 2U 21600 Carrier appliance and 15Gbps with a 2U 21700 Carrier appliance
- Protects against, Denial of Service (DoS) attack
- Protects against overbilling attacks that lead to subscribers being billed for data not requested
- IP spoofing prevention
- Secures the Gp, Gi, Gn and Ga interfaces of 3G networks
- Secure the S4, S3, S11, and Gi interfaces of the LTE network
- Secure MME and S-GW on the S1-u, S1-MME interfaces of the LTE networks
- Virtualization of appliances, supporting up to 250 Virtual Systems to enable easy consolidation, scalability and network segmentation
# Next Generation Security for 3G and 4G LTE Networks

## Performance

<table>
<thead>
<tr>
<th></th>
<th>21600-Carrier</th>
<th>21700-Carrier</th>
<th>61000-Carrier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Power</td>
<td>2,501 / 3,300</td>
<td>3,300 / 3,551</td>
<td>3,000 / 14,600</td>
</tr>
<tr>
<td>Firewall Throughput</td>
<td>Up to 110Gbps</td>
<td>Up to 110Gbps</td>
<td>Up to 200Gbps</td>
</tr>
<tr>
<td>SCTP Throughput</td>
<td>18Gbps</td>
<td>20Gbps</td>
<td>80Gbps</td>
</tr>
<tr>
<td>GTP Throughput</td>
<td>13Gbps</td>
<td>15Gbps</td>
<td>80Gbps</td>
</tr>
<tr>
<td>GTP Concurrent PDP Context</td>
<td>3M</td>
<td>3M</td>
<td>20M</td>
</tr>
<tr>
<td>VPN IMIX Throughput</td>
<td>Up to 30Gbps</td>
<td>Up to 30Gbps</td>
<td>Up to 56Gbps</td>
</tr>
<tr>
<td>IPSec Tunnels</td>
<td>10,000</td>
<td>10,000</td>
<td>50,000</td>
</tr>
<tr>
<td>IPS Throughput (Default/Recommended Profiles)</td>
<td>21Gbps / 6.8Gbps</td>
<td>25Gbps / 8Gbps</td>
<td>Up to 110Gbps / 40Gbps</td>
</tr>
<tr>
<td>Concurrent Sessions</td>
<td>13M</td>
<td>13M</td>
<td>Up to 70M</td>
</tr>
<tr>
<td>Connections per Second</td>
<td>140K / 300K</td>
<td>170K / 300K</td>
<td>Up to 600K</td>
</tr>
</tbody>
</table>

## Virtual Systems

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual System Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td># of VS Supported</td>
<td>Up to 250</td>
<td>Up to 250</td>
<td>Up to 250</td>
</tr>
</tbody>
</table>

## Hardware Specifications

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10/100/1000Base-T Ports</td>
<td>13 to 37</td>
<td>13 to 27</td>
<td>N/A</td>
</tr>
<tr>
<td>1000Base-F SFP Ports</td>
<td>Up to 36</td>
<td>Up to 36</td>
<td>N/A</td>
</tr>
<tr>
<td>10GBase-F SFP+ Ports</td>
<td>Up to 13</td>
<td>Up to 13</td>
<td>16 / 32</td>
</tr>
<tr>
<td>40GBase-F Ports (Max)</td>
<td>N/A</td>
<td>N/A</td>
<td>4</td>
</tr>
<tr>
<td>Security Acceleration Module</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Enclosure</td>
<td>2RU</td>
<td>2RU</td>
<td>14RU / 15RU</td>
</tr>
<tr>
<td>Dimensions (Standard/Metric)</td>
<td>17” W x 28” D x 3.5” H 431 mm W x 710 mm D x 88 mm H</td>
<td>17” W x 28” D x 3.5” H 431 mm W x 710 mm D x 88 mm H</td>
<td>17.5” W x 15.16” D x 24.3” H 445 mm W x 385 mm D x 618.3 mm H</td>
</tr>
<tr>
<td>Max Weight</td>
<td>26 kg (57.4 lbs.)</td>
<td>26 kg (57.4 lbs.)</td>
<td>90 kg (198.4 lbs.) (Chassis, 5 PSUs, fans, 2 CCM, 12 SGM, 2 SSM)</td>
</tr>
<tr>
<td>Operating Environment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temperature: 32° to 104° F / 0° to 40° C Relative Humidity 20% to 90% (non-condensing)</td>
<td>Temperature: 32° to 104° F / 0° to 40° C Relative Humidity 20% to 90% (non-condensing)</td>
<td>Temperature: 23° to 131°F / -5° to 55°C Relative Humidity 5% to 90% (non-condensing)</td>
<td></td>
</tr>
<tr>
<td>Non-Operating Environment</td>
<td>Temperature: -4° to 158° F / -20° to 70°C Relative Humidity 5% - 95% (non-condensing)</td>
<td>Temperature: -4° to 158° F / -20° to 70°C Relative Humidity 5% - 95% (non-condensing)</td>
<td>Temperature: -40° to 158° F / -40° to 70°C Relative Humidity 5% to 90% (non-condensing)</td>
</tr>
<tr>
<td>AC Power Supplies</td>
<td>100–240VAC, 47–63Hz</td>
<td>100–240VAC, 47–63Hz</td>
<td>No. of modules: 5 (max) Input: 100–240VAC, 47–63Hz Single module output: 1200–1500W</td>
</tr>
<tr>
<td>Power Consumption (Max)</td>
<td>449W / 744W</td>
<td>489W / 784W</td>
<td>5000W</td>
</tr>
</tbody>
</table>

## Certifications

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety: UL, cUL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emissions: CE, FCC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class A Environmental: RoHS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety: UL, cUL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emissions: CE, FCC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class A Environmental: RoHS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 With Security Acceleration Module
2 With memory upgrade and GAiA OS
3 With AC power supplies
Enabling Value Added Security Services for Subscribers

In addition to securing a carrier’s entire infrastructure, deploying Check Point’s optimized Telco security solutions also provide a platform for comprehensive subscriber value-add security services, using Check Point’s Software Blade architecture to enable a wide range of security protections for mobile users.

These include mobile-identity-based web security, malware protection, parental controls and more, which can all be offered by MNOs and service providers to their subscribers as opt-in, value-add services to boost subscriber and network protection, and differentiate service offerings from those of competing networks.
About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to innovate with the development of the software blade architecture. The dynamic software blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

CHECK POINT OFFICES

Worldwide Headquarters
5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
e-mail: 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
URL: http://www.checkpoint.com