Rapid proliferation of mobile devices and unprecedented mobile data growth, coupled with demand for new digital content and applications, are driving operators to massively invest in LTE — an all-IP-based network.

While this solves many challenges operators face in mobile broadband, it also opens great opportunities to introduce new types of applications and services (e.g., video calling, high-definition content streaming, etc.) that weren't possible before.

Continuously evolving into 5G to enhance mobile broadband services, next-generation networks and standards are designed for the Internet of Things (IoT), enabling a wide range of use cases for the scalable, hyper-connected IoT world.

**The Challenge**

The advent of all-IP-based mobile communication systems, such as LTE, opens more avenues for malicious intrusions. Threats such as DDoS floods, application-layer attacks and DNS exploits can arise from mobile and IoT devices infected with botnets, as well as from anywhere within the Internet or external packet data network (PDN) gateways, threatening service availability.

Increasing DDoS attacks on the mobile core is requiring service providers to deploy a comprehensive security solution capable of detecting and mitigating large-scale DDoS attacks, including evolving multi-vector attacks, and stateful firewalls to inspect subscriber sessions.

Carrier-grade networking solutions may also be implemented to scale the network infrastructure — while maintaining uninterrupted connectivity and high network availability — to provide best possible customer experience.

Data encryption for secure communication channels using IPsec within a mobile operator infrastructure is required to connect eNodeB(s) to the LTE mobile core. This secures traffic over unsecure access networks in carrier-grade Wi-Fi deployments and connects field devices to backend servers over the Internet in IoT deployments. Service providers require a solution that provides high-scale IPsec VPN tunnel capacity and throughput, while securing the mobile network core and subscribers from evolving PDN-based attacks.

**The A10 Networks Gi/SGi Firewall Solution**

A10 Thunder® CFW, with integrated Gi/SGi firewall capabilities, delivers the performance that mobile carriers require to scale and protect their networks. With the ability to provide throughput up to 220 Gbps while supporting more than 6 million connections per second (CPS) and over 250 million concurrent sessions, Thunder CFW will meet both current and future traffic requirements of any service provider.
Strategically deployed at various locations on the mobile network infrastructure, Thunder CFW enables mobile carriers to efficiently safeguard their infrastructure, including the Gateway GPRS Support Node (GGSN) and PDN gateway in the Evolved Packet Core (EPC).

IPv4 Preservation and IPv6 Transition
With integrated carrier-grade network address translation (CGNAT) functionality, Thunder CFW allows mobile carriers to preserve their current IPv4-based infrastructure investment. Also included are proven IPv6 transition technologies, such as NAT64/DNS64, to assist in providing a smooth transition to IPv6 networking and seamless subscriber access to resources, regardless of the type of IP version used.

Ensure applications remain addressable and operate transparently through address translation with integrated application layer gateways (ALG). Simplify operational tasks and maintain low TCO objectives via included IPv4 preservation and IPv6 migration support in the multi-functional Thunder CFW.

Mobile Network Security
To protect mobile infrastructure, the Thunder CFW Gi/SGi firewall provides granular control over network resources, allowing mobile carriers to block network attacks and unauthorized access. It incorporates a stateful firewall with a rich set of features to protect subscribers, along with shielding the LTE data and control plane services from a wide array of threats.

A10 Thunder CFW security capabilities for mobile communications include:

- Layer 4 and Layer 7 DDoS and protocol anomaly protection to prevent multi-vector volumetric attacks
- Web application firewall (WAF) to protect services and infrastructure under cyberattack
- DNS application firewall to shield DNS servers from attacks, including buffer overflow, malformed requests and DoS

Thunder CFW can also secure its own resources, such as NAT IP pools, to ensure that its operational functions are not compromised.

Mobile Network Deployment Options

1. **Backhaul Protection**
   Confidentiality protection and integrity of backhaul traffic running over S1 (control and data planes) interfaces can be achieved by deploying security gateways (SEG) between the E-UTRAN and EPC. Usually, IPsec tunnels are created between eNodeBs and SEG, and such devices are expected to handle high-scale IPsec VPN termination. This strategic deployment helps mitigate risks arising from mobile devices targeting the radio access network, VAS engines or the mobile core.

2. **Gi/SGi Interface Protection**
   The mobile core infrastructure is vulnerable to attacks due to the evolving threat, public and private clouds, data center infrastructure and other PDN gateways. These attacks can include bandwidth saturation on the Gi interface, attacks on the firewall and multi-vector DDoS attacks.

   While the data plane traffic flows between the UE and the PDN gateways are encapsulated in IPsec or GTP tunnels, the Gi interface from the PDNs (both internal and external) to the rest of the Internet is not, making it most vulnerable to multi-vector threats. Securing Gi/SGi makes it a natural deployment choice for the Gi/SGi firewall solution.

3. **Enabling Secure and Interoperable LTE Roaming**
   As service providers deploy LTE networks, there is a growing need to provide roaming services to their LTE subscribers, including connectivity between LTE and 3G roaming subscribers. Such a roaming service needs to be built without jeopardizing a service provider’s own customers on their home network.

![Figure 1: A10 Thunder CFW Gi/SGi Firewall Deployment Scenarios](image-url)
A10 Thunder CFW, with integrated Gi/SGi firewall capabilities, protects the EPC from roaming partners against IP-layer attacks, information leaks, malicious packet attacks, and DoS and DDoS attacks by applying connection rate limiting, as needed.

4 Wi-Fi Offload Interconnect Protection

The emergence of 5G — and solutions for Wi-Fi offload — presents new opportunities for integrated security gateway and firewall deployments. Operators offering carrier-grade Wi-Fi deployments need a secure gateway to protect traffic over unsecure access networks.

An ideal deployment scenario is a high-scale IPsec VPN termination device on the ePDG interface between the Wi-Fi access point and the evolved packet data gateway (ePDG). A security gateway is essential to secure data transmission from industrial IoT field devices to backend servers in IoT deployments.

High-Performance Architecture

Thunder CFW leverages unique software and hardware design advantages to deliver exceptional IPsec performance and high-throughput scale.

The A10 Networks Advanced Core Operating System (ACOS®) powers Thunder CFW appliances. Built from the ground up to maximize the performance of multicore CPU architectures, ACOS can linearly scale compute processing as more CPU cores are added, providing unparalleled performance in a compact form factor.

ACOS uses Symmetric Scalable Multi-Core Processing (SSMP) to leverage supercomputing techniques for parallel processing and maximize the performance of multicore architectures. Due to its highly scalable 64-bit operating system optimized for multicore architectures, Thunder CFW appliances deliver an unmatched comprehensive security solution to secure the mobile infrastructure.

Solution Components

- Thunder Convergent Firewall (Thunder CFW)
- Security Gateway (SeGW)
- Gi/SGi Firewall (Gi/SGi FW)
- Site-to-Site IPsec VPN
- Carrier-Grade Networking Solutions
- aGalaxy® Centralized Management System
- aXAPI® REST-based API

Summary

The Gi/SGi firewall and security gateway feature set is included in the A10 Thunder CFW, along with several other key components such as stateful Layer 4 firewall, DDoS protection and CGN. This comprehensive approach provides best-in-class performance and scale to protect the mobile infrastructure while reducing OPEX and CAPEX costs.

Thunder CFW is a powerful and comprehensive security solution built on A10’s Advanced Core Operating System platform, with the SSMP software architecture, delivering the ultra-high performance needed to meet current and future mobile and cloud network deployments.

Combining a shared-memory architecture and Flexible Traffic Accelerator (FTA) technology, the Gi/SGi firewall offers ultra-high throughput and unmatched connection rates, eliminating traditional performance bottlenecks while protecting mobile core infrastructure assets.

Note

Service providers can also leverage the Gi/SGi firewall solution on A10 Networks vThunder®, a virtual form factor, to gain a flexible, easy-to-deploy and on-demand, software-based deployment.

Next Steps

For more information, please contact your A10 representative or visit www.a10networks.com/firewall.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: www.a10networks.com