SOLUTION BRIEF

GI/SGI FIREWALL PROTECTION FOR MOBILE NETWORKS

ADVANCED SECURITY FOR SERVICE PROVIDER MOBILE AND CLOUD NETWORK DEPLOYMENTS

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.

CHALLENGE

Service providers must defend mobile network infrastructure, applications and subscribers against malicious online threats and multi-vector attacks, while maintaining always-on network availability and the best possible subscriber experience.

SOLUTION

Protect mobile core infrastructure and subscribers from multi-vector attacks and ensure applications are highly available, accelerated and secure. A10 Thunder CFW, with integrated Gi/SGi firewall capabilities, provides highly scalable, flexible and high-performance security at strategic locations in the mobile network.

BENEFITS

- Simplify operational tasks and reduce CAPEX and OPEX by integrating CGNAT, stateful firewall and DDoS protection capabilities
- Gain best-in-class performance and scale in a compact form
- Protect data centers and hybrid cloud deployments with high-performance IPsec VPN and traffic inspection
- Securely interconnect remote sites via hardware-based IPsec cryptographic security for 3G, 4G LTE and 5G networks supporting IoT and machine-to-machine (M2M) deployments

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 (PGW) 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:

- Gi-LAN consolidation of L4-L7 services including CGNAT, firewall and application visibility services
- GTP firewall with granular SCTP filtering
- DPI-based application visibility and control
- Integrated DDoS protection to prevent multi-vector volumetric attacks and secure resources, such as NAT IP pools to ensure that its operational functions are not compromised

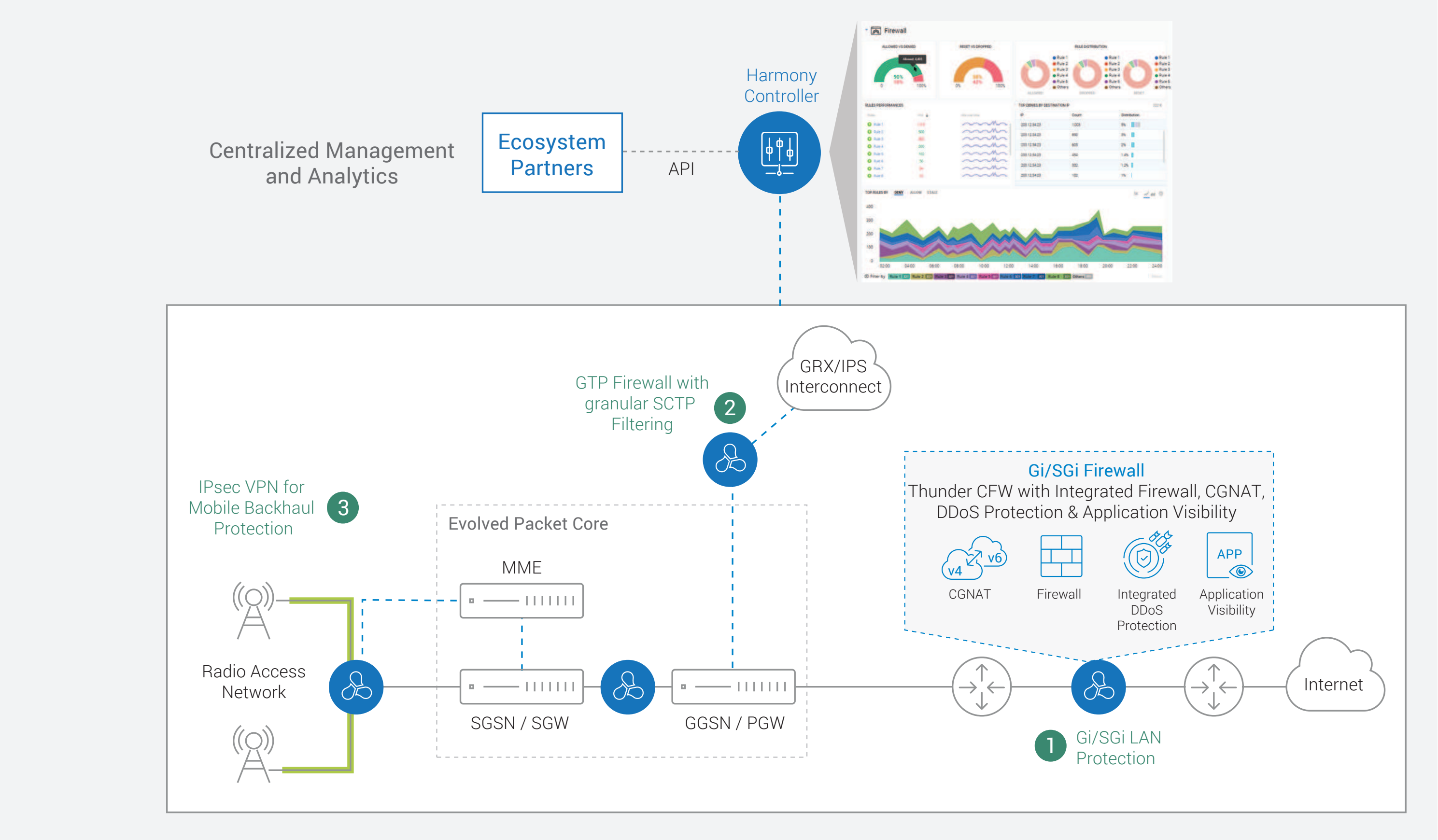
Centralized Management and Analytics
Ecosystem Partners
API
Harmony Controller
Firewall
GTP Firewall with granular SCTP Filtering
2
GRX/IPS Interconnect
IPsec VPN for Mobile Backhaul Protection
3
Evolved Packet Core
MME
Gi/SGi Firewall
Thunder CFW with Integrated Firewall, CGNAT, DDoS Protection & Application Visibility
v4
v6
CGNAT
Firewall
Integrated DDoS Protection
APP
Application Visibility
Radio Access Network
SGSN / SGW
GGSN / PGW
Internet
1
Gi/SGi LAN Protection

Figure 1: A10 Thunder CFW Gi/SGi Firewall Deployment Scenarios

MOBILE NETWORK DEPLOYMENT OPTIONS

1 GI/SGI INTERFACE

The mobile core infrastructure is vulnerable to attacks due to the evolving threats and rising attack vectors on the Gi/SGi interface from the Internet, 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.

2 ENABLING SECURE AND INTEROPERABLE ROAMING

Service providers are experiencing a growing need to provide roaming services to their 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, and to ensure service continuity while roaming.

GTP firewall with granular SCTP filtering capabilities provides security and scalability, while protecting the mobile core against GTP-based threats such as information leaks, malicious packet attacks, and DDoS attacks coming in from access networks and GRX/IPX interconnect to support uninterrupted operations.

3 MOBILE 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.

4 APPLICATION VISIBILITY AND CONTROL

Deep Packet Inspection-based application visibility classifies more than 3000 applications in over 40 categories to provide granular insights into network traffic, even for encrypted traffic, which is critical for effective policy enforcement. Understanding network and application traffic trends allows for effective network planning, deeper business intelligence, enhanced Law Enforcement Agency (LEA) compliance and service monetization.

CENTRALIZED MANAGEMENT AND VISIBILITY

Gain application and network services visibility along with Gi firewall analytics when Thunder CFW is deployed in conjunction with the A10 Harmony™ Controller. Get customizable drill-down views for analysis and actionable insights for faster troubleshooting. Centrally configure and manage policies across Gi firewall services in a multi-cloud environment.

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)
- GTP Firewall with Granular SCTP Filtering
- Application Visibility and Control
- 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, L7 application visibility, GTP firewall with granular SCTP filtering, integrated DDoS protection and CGNAT. This comprehensive and consolidated approach provides best-in-class performance, efficiency 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.

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 a10networks.com/firewall.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19169-EN-03 JULY 2018