SIGNALING SECURITY PLAYS A KEY ROLE IN MEETING NEW 5G REQUIREMENTS

PROTECT CONTROL-PLANE INTERFACES FROM SERVICE-IMPACTING ATTACKS & EVENTS

A10®

TABLE OF CONTENTS

GROWING CONCERN FOR SIGNALING SECURITY

5G promises higher speeds, lower latency, a multitude of new IoT applications and new 5G revenue opportunities for the mobile network operator. However, security is a top concern for operators as they undertake 5G roll-outs. Maintaining the highest level of network and service availability is of utmost importance. Attacks on mission-critical applications can disrupt service and cause network outages. When they occur, it could derail revenue potential and cause significant damage to both brand and reputation. The expected volume of IoT devices, increased efficacy of cyber criminals, and high-risk botnets make protecting evolving mobile networks strategically important. Control-plane signaling, which manages the traffic flow within the mobile network, is an area of vulnerability and concern and the vast majority of mobile operators perceive strong levels of signaling threats, as shown in Figure 1.

Mobile-signaling protocols have become a favorite target of cyber criminals in recent years. The creators of mobile protocols paid little attention to security for the simple reason that mobile communications were relatively free from attacks. Older generations of mobile technology were proprietary and inherently difficult to penetrate, so the protocols themselves did not need additional security. As the industry moved to IP-based technology, the lack of security in the protocols themselves has become a vulnerability. Signaling networks using protocols such as GTP, DNS and Diameter are under attack from a number of bad actors, exploiting vulnerabilities.

One defining characteristic of the modern mobile network is that successive generations of standards overlap, not replace, previous generations. Today's mobile threats are traditional IP-based threats within the all-IP 4G network combined with legacy 2G and 3G technologies. As the industry moves to 5G—with significant overlap of 3G and 4G— the range of new services and technologies will only expand the attack surface. Figure 2 (page 4) describes the differences in signaling control-plane approaches in 3G, 4G and 5G.

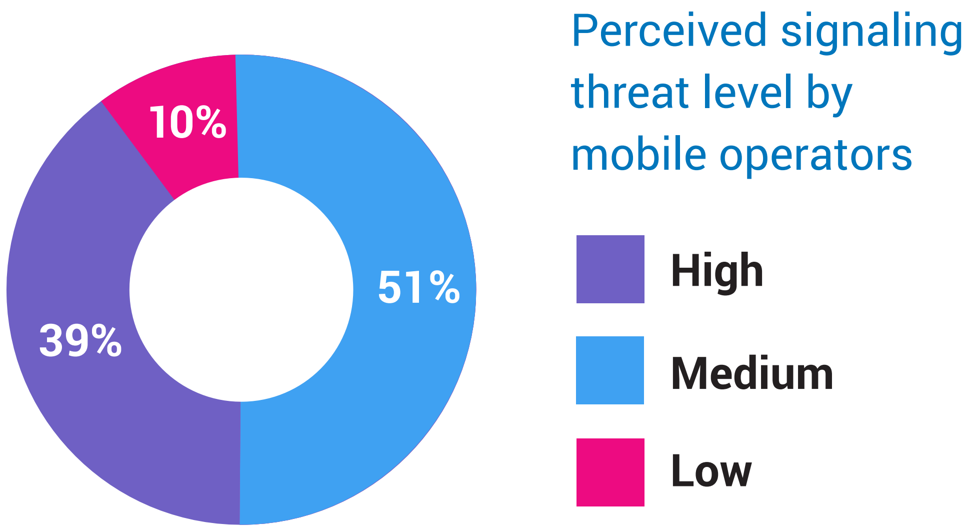


Figure 1: 90% of mobile operators perceive high to medium danger to signaling.
ENISA, Signaling Security in Telecom

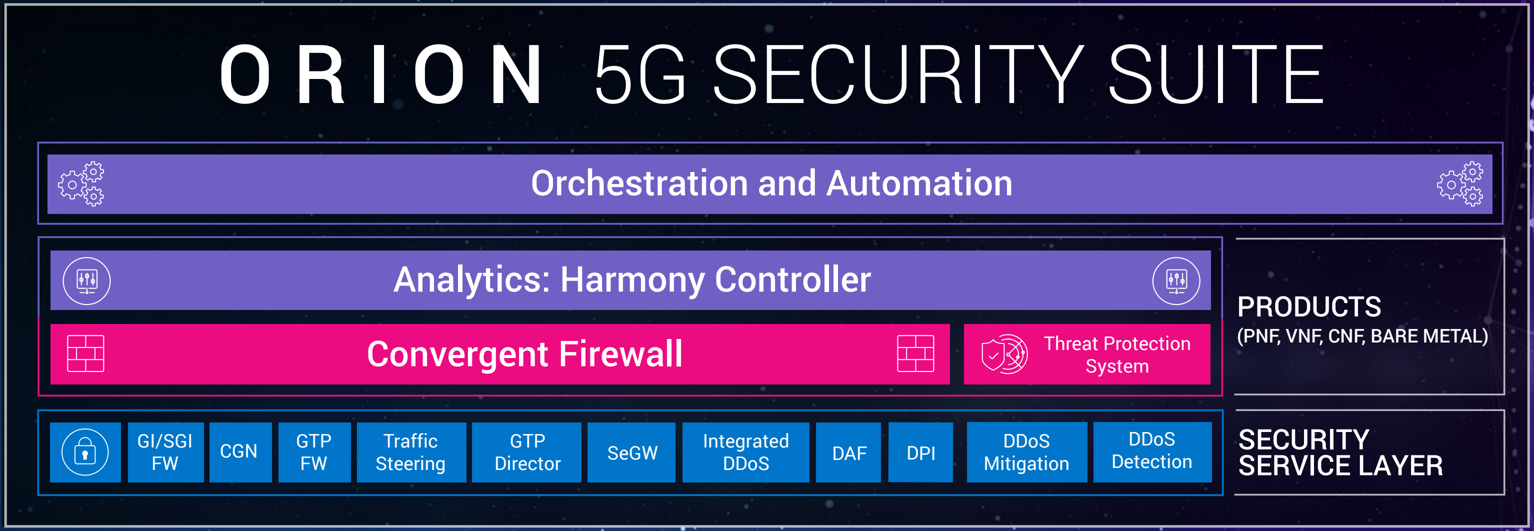
3G, 4G, 5G SIGNALING PROTOCOL VULNERABILITIES

3G/4G	5G
Network entities with combined control-plane and user-plane functionality: SGSN/SGW, GGSN/PGW	Separate control-plane and user-plane entities: control-plane: SMF, AMF user plane: UPF
Multiple signaling protocols: GTP-C, SS7, Diameter, etc.	Uniform and consolidated approach: Rest-based API calls
Point-to-point communication interfaces restricting flexibility: MME talks to PGW via the SGW	Service-based interface (SBI) with any-to-any communication
Inherently insecure with well-known security vulnerabilities	Secures communication through use of HTTP2 and TLS
Comparatively smaller attack surface as protocols used are not commonly deployed in enterprises	Comparatively larger attack surface as the protocols are commonly used and deployed elsewhere

Figure 2: Comparison of 3G, 4G, 5G signaling protocol vulnerabilities

YOUR GUIDE TO SIGNALING SECURITY IN EVOLVING MOBILE NETWORKS

The A10 Networks Orion 5G Security Suite provides highly cost-efficient security solutions with the flexibility, scalability and protection mobile operators need as they evolve their networks to 5G and integrate cloud and edge capabilities. The suite provides comprehensive security at service provider scale with additional functions most needed in mobile networks, including a firewall for all network peering points, deep packet inspection (DPI), carrier-grade network address translation (CGNAT), integrated distributed denial of service (DDoS) threat protection, intelligent traffic steering, DDoS detection and mitigation and analytics.



ORION 5G SECURITY SUITE

Orchestration and Automation

Analytics: Harmony Controller

Convergent Firewall

Threat Protection System

PRODUCTS
(PNF, VNF, CNF, BARE METAL)

GI/SGI FW | CGN | GTP FW | Traffic Steering | GTP Director | SeGW | Integrated DDoS | DAF | DPI | DDoS Mitigation | DDoS Detection

SECURITY SERVICE LAYER

Figure 3. Orion 5G Security Suite provides comprehensive protection for mobile networks

This guide describes key solutions offered by A10 Networks for protecting control-plane signaling in hybrid, multi-generational networks, including 3G, 4G, 5G SA, 5G NSA and MEC. Visit a10networks.com/5G for more information on the A10 Networks Orion 5G Security Suite for service providers.

- DNS Infrastructure protection
- DNS application security
- GTP-based DDoS attacks
- SCTP attacks
- IMS infrastructure security
- Diameter signaling protection

DNS INFRASTRUCTURE PROTECTION

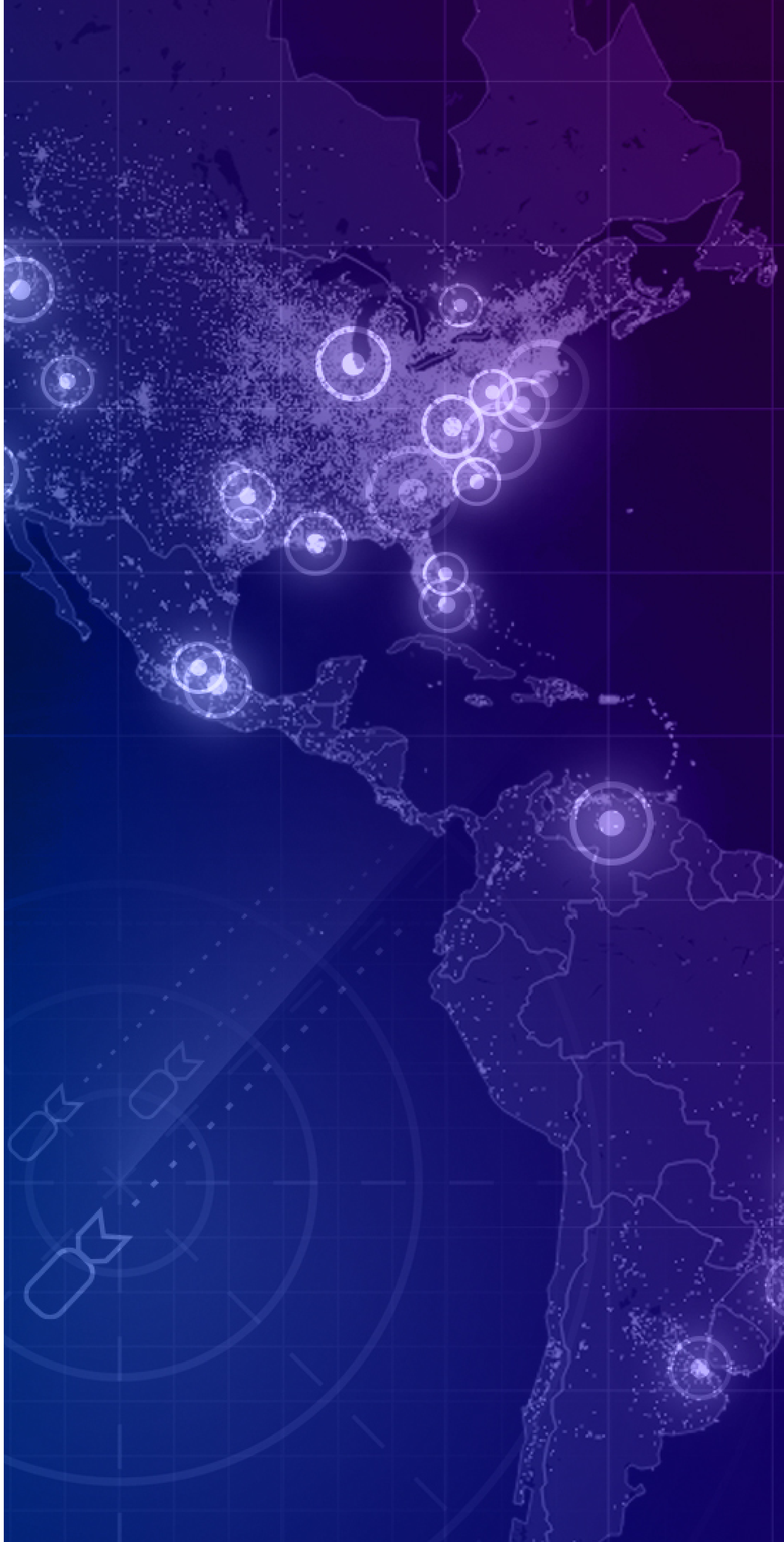
The Domain Name System (DNS) is the critical infrastructure that service providers depend on for their subscribers to smoothly navigate the internet and access mobile services.

CHALLENGE

Crushing distributed denial of service (DDoS) attacks targeting websites and infrastructure are creating greater awareness around the critical nature of DNS for reliable internet services and the catastrophic effects of DNS outages. DNS attacks come in a variety of forms – all designed to tie up infrastructure resources and deny or degrade service to legitimate subscribers and applications.

- **Reflection/amplification:** Attackers make numerous spoofed requests to globally distributed open DNS resolver servers on the internet to flood the victim's authoritative servers. To maximize the impact, reflection attacks leverage DNS protocol amplification capabilities to create very large responses.
- **Random query names:** Random query name attacks make DNS queries to invalid or non-existent domains. The DNS server spends significant resources searching for records that don't exist.
- **Flood:** DNS services are run on servers with networking functionality and, as a result, are subject to general network flooding attacks like malformed packets, User Datagram Protocol (UDP) packets to random ports, Transmission Control Protocol (TCP) SYN floods and other resource-exhaustion attacks. Attackers leverage botnets to create a large scale of irrelevant network functions or high rates of malicious DNS queries that tie up the server from servicing legitimate users.

Mobile network operators must take an active role in applying adequate defenses to build DDoS resilience into their DNS infrastructure or suffer the inevitable consequences.



DNS INFRASTRUCTURE PROTECTION (CONTINUED)

SOLUTION

The Orion 5G Security Suite includes Thunder Threat Protection System (TPS), a surgical multi-vector DDoS protection solution that ensures availability of business services at any scale.

Thunder TPS detects and mitigates multi-vector DDoS attacks at the network edge and scales to defend against the DDoS of Things and traditional zombie botnets. It does this by tracking 27+ traffic behavioral indicators to detect anomalous behavior against learned peacetime traffic to surgically distinguish legitimate users from attacking bots.

Multiple layers of protection are provided for DNS services that include source-based rate limiting, authentication challenges, blocking abusive requests, blacklisting and more. Thunder TPS provides extensive customization capabilities from the graphical user interface, command line interface (CLI) or over open API. This gives defenders the ability to create customized defenses to ensure DNS services are resilient to targeted multi-vector DDoS attacks.

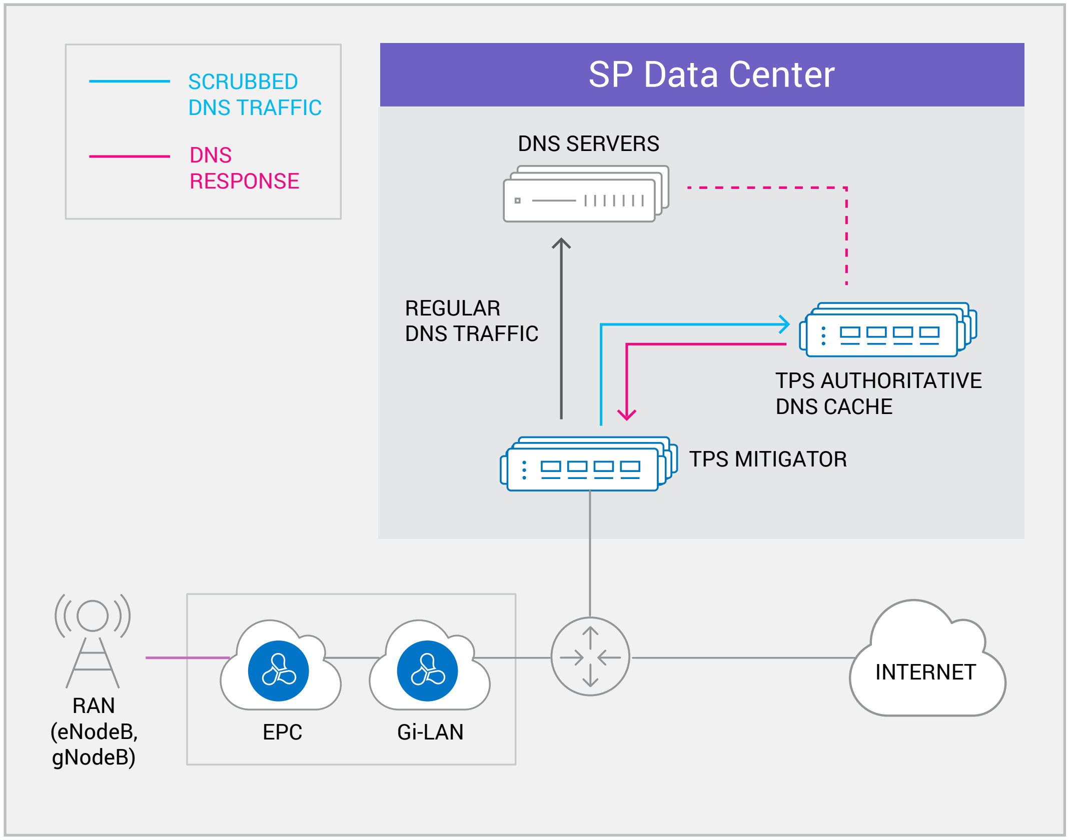


Figure 4. Thunder TPS protects DNS infrastructure

DNS APPLICATION SECURITY

DNS servers are a top attack target. Taking DNS servers offline is an easy way for attackers to keep thousands or millions of internet subscribers from accessing the internet or disabling a service provider's DNS servers. DNS attacks can prevent the service provider's subscribers from resolving domain names, visiting websites, sending email and using other vital internet services.

CHALLENGE

Protect data center services and assets from increasingly sophisticated threats, while providing a high-performance solution that can scale with growing traffic demands. Amplification or DNS reflection attacks have brought down service providers' DNS services for hours, even days. Enterprises can suffer lost revenue and damage to their reputation if an attacker disrupts access to DNS infrastructure and prevents users from accessing vital services.

SOLUTION

The Orion 5G Security Suite includes Thunder CFW with the DNS application firewall (DAF) to secure DNS servers against various types of threats. The A10 Orion 5G Security Suite shields DNS infrastructure from attacks with its powerful and comprehensive DNS application firewall.

The A10 DAF inspects all DNS traffic to verify that it is legitimate, and blocks or redirects malicious traffic for additional inspection. DNS attacks, such as sending malformed DNS packets from spoofed source IP addresses, can be easily stopped by dropping traffic that does not conform to standard DNS packet types. The A10 DAF provides advanced protection against DNS infrastructure exploitation with granular application rules for query behavior and mitigation methods, such as IP rate limiting. In addition to protecting the network DNS servers, the DNS application firewall prevents network equipment from becoming an unwanted participant in a DNS reflection or amplification attack by using the DNS response rate limiting (RRL) feature.

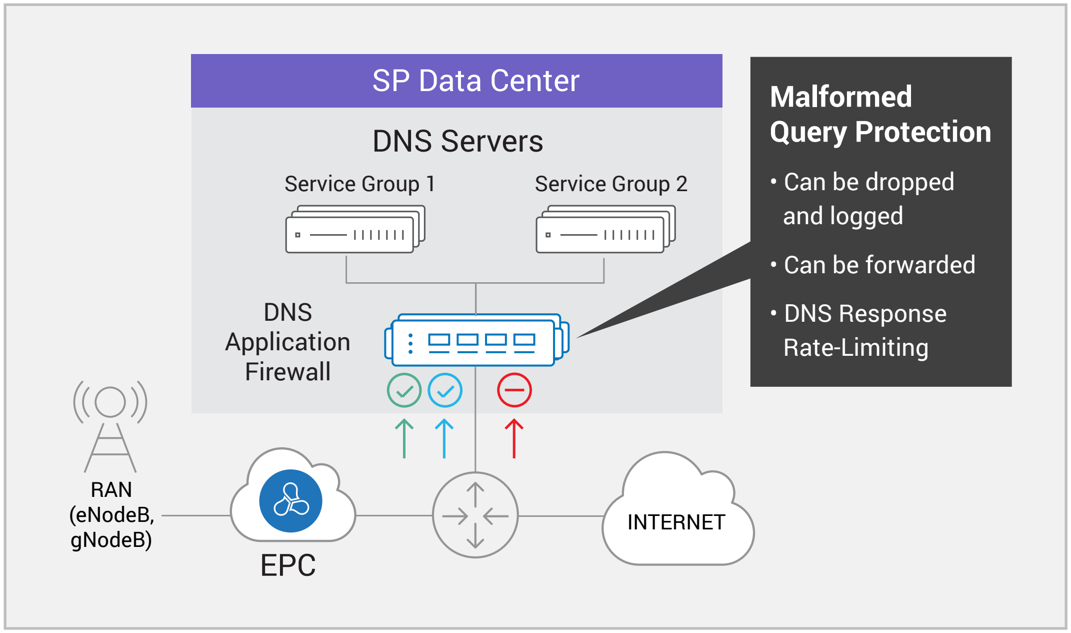


Figure 5: DNS application firewall in service provider data center

GTP-BASED DDOS ATTACKS

The General Packet Radio Service Tunneling Protocol (GTP) is essential for the proper functioning of today's mobile networks. GTP enables packet networks to signal and carry data between devices and applications. Within the mobile core, GTP is the primary protocol used to exchange user and control data between serving and packet gateways. For roaming scenarios, GTP connects the home and visited network, enabling subscribers to move seamlessly between networks. Due to the long history of attack-free networks, mobile signaling protocols such as GTP were designed without an authority model, instead relying on assumed trust within a closed industry and trusted roaming partners.

CHALLENGE

The extensive use of GTP within and between mobile networks has made it an attractive target for attackers. GTP-based exploits are successful in part because of the inherent vulnerabilities of the GTP, which lacks built-in security features such as encryption and sender authentication. Malicious actors can eavesdrop on subscriber communications, exfiltrating sensitive information that can be used for fraudulent purposes.

- **Malformed packet flood:** Attackers can also take advantage of poorly implemented operator equipment and send malformed packets or other invalid packets in enough volume to cause the signaling network to malfunction.

- **Malicious or compromised peers:** Mobile operators work with partners to provide seamless interconnect. Once the contractual agreements and physical connections are established, the GRX/IPX links used to support these connections are built on a trust relationship. If a roaming interface is breached, a variety of attacks can be launched including throttling, blocking, intercepting, and manipulating user data, tracking large numbers of subscribers, eavesdropping on calls and messages to gather information about user credentials and the mobile network, modifying GRX/IPX traffic.

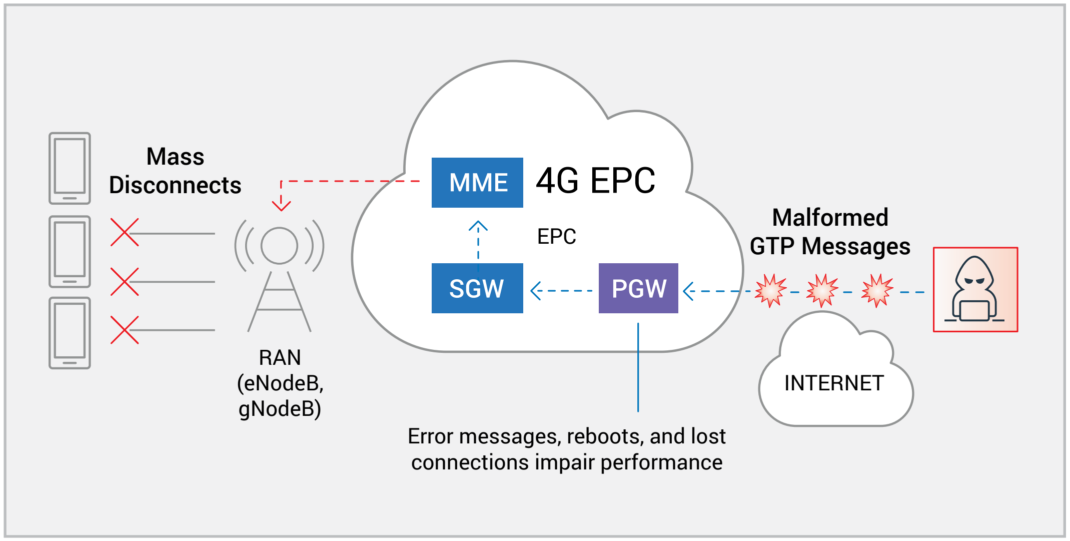


Figure 6. Attackers can manipulate GTP messages to create subscriber DDoS

GENERAL PACKET RADIO SERVICE TUNNELING PROTOCOL

GTP-BASED DDOS ATTACKS

(CONTINUED)

SOLUTION

The Orion 5G Security Suite includes a GTP Firewall, which provides extensive capabilities including stateful inspection, filtering and rate limiting, and filtering of traffic for protocol abnormalities, invalid messages, and other suspicious indicators. It protects against GTP protocol vulnerabilities such as fraudulent use, confidentiality breaches, DDoS attacks by malicious peers and other threats.

The GTP firewall module can be inserted into multiple interfaces carrying the GTP traffic. In the primary use case, it is inserted on S5-Gn and S8-Gp (roaming) interfaces. The GTP firewall provides security and scalability, while protecting the mobile core against GTP-based threats such as information leaks, malicious packet attacks, and DDoS attacks through GTP interfaces in the access networks and GRX/IPX interconnect to support uninterrupted operations.

SCTP ATTACKS

Stream Control Transmission Protocol (SCTP) is a transport protocol used extensively in mobile networks to carry higher-level protocols. SCTP messages are made up of “chunks.”

CHALLENGE

SCTP malicious attacks or misconfigurations can create network failures or outages. In 3G networks, SCTP is the transport protocol in SIGTRAN (IP-based SS7 protocol stack, which consists of IP layer, SCTP transport protocol, and an adaptation layer: M2UA, M2PA, M3UA and SUA. In 4G networks, on the S1, SCTP is used to carry the S1-AP control-plane traffic between the RAN and the MME in the core.

SOLUTION

The Orion 5G Security Suite includes the Thunder CFW which provides protection against SCTP attacks. For 2G and 3G networks, the A10 Thunder CFW provides SCTP chunk filtering with static NAT, based on the PPID such as M3UA, M2PA, etc. Multi-homing is also available with up to eight IP addresses. In 3G and 4G networks, SCTP filtering with static NAT enables operators to hide the internal IP address from roaming partners. The Thunder CFW provides stateful inspection and packet validation for SCTP messages. In 3G, SCTP filtering can be used to filter specific xUA message types using the PPID field in “data chunk.”

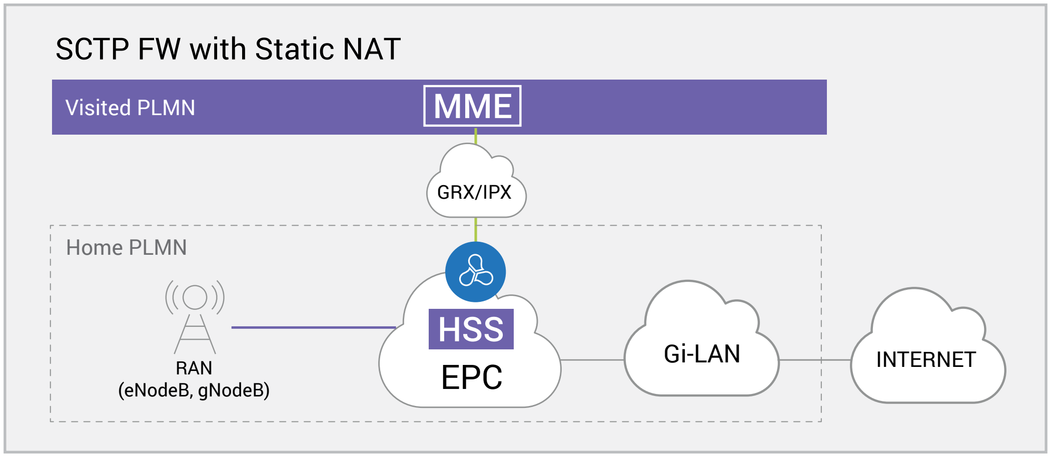
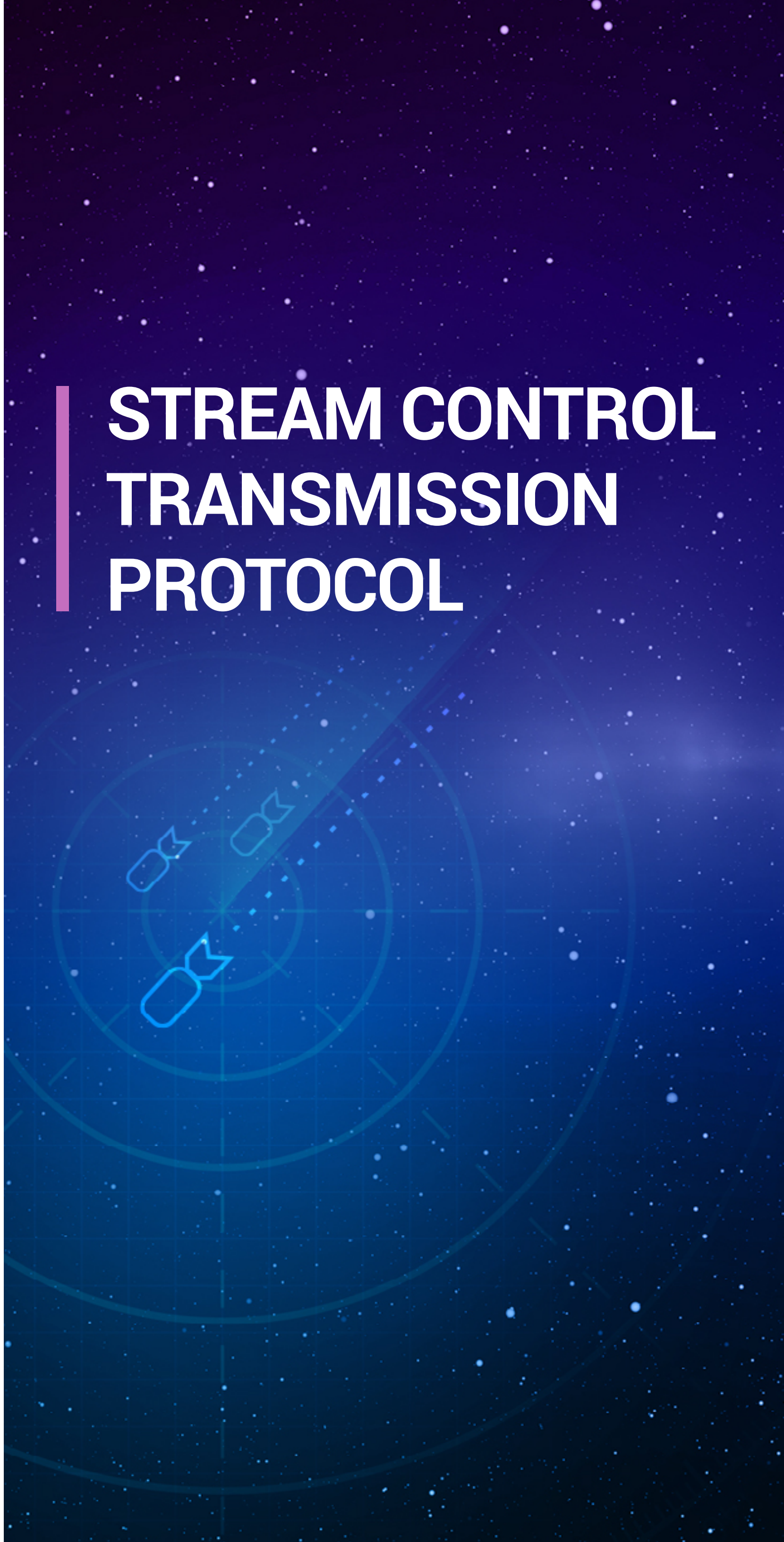


Figure 7. SCTP firewall with Static NAT hides internal IP address from roaming partners



STREAM CONTROL TRANSMISSION PROTOCOL

IMS INFRASTRUCTURE SECURITY

The IP Multimedia Subsystem (IMS) is an open, standardized, multimedia architecture for mobile and fixed IP services. It is used for VoIP and is based on a 3GPP variant of SIP. Session Initiation Protocol (SIP) today is the standard protocol for multimedia signaling,

CHALLENGE

SIP-based application services can suffer from denial of service (DoS) attacks that can severely compromise its reliability.

SOLUTION

The Orion 5G Security Suite includes Thunder TPS and Thunder CFW which provide protection for IMS infrastructure. Thunder TPS, a SIP template is bound to the DDoS service port, it can enable malform checks to verify SIP packet integrity and set rate limit options for SIP message types. This prevents anomaly packets and resource attacks from reaching the SIP server. Additionally, Thunder CFW can provide load balancing for SIP traffic over UDP and TLS/TCP, distributing traffic to multiple servers to prevent overload. Dynamic and static NAT in CFW will hide public IP addresses, further strengthening the security posture.

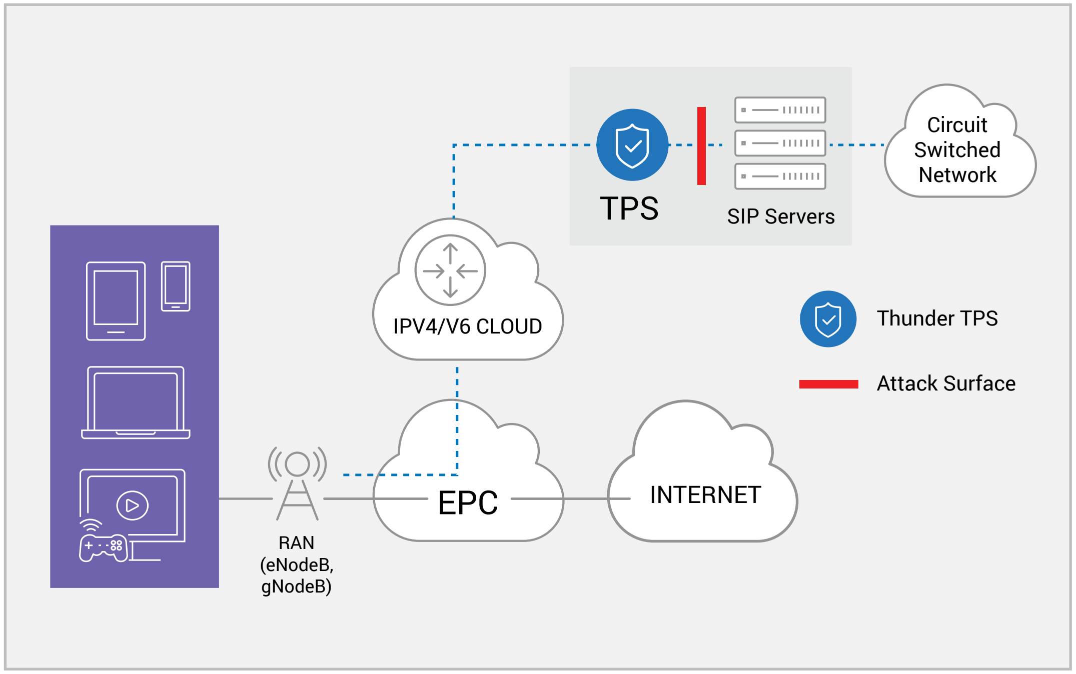


Figure 8: SIP Signaling Protection with Thunder TPS

DIAMETER SIGNALING PROTECTION

The Diameter protocol is used between several core elements in 4G, in both home and visited scenarios. Diameter, derived from RADIUS (Remote Authentication Dial-In Service) supports authentication, authorization and accounting processes within the core network. Diameter uses many of the same concepts as SS7 and therefore has many of the same vulnerabilities. There is risk of an intruder gaining access through hacking.

CHALLENGE

There are multiple attack vectors that manipulate Diameter. These include fraud, authentication theft, SMS theft, message manipulation and subscriber DDoS. Diameter vulnerabilities are widely documented and could be exploited by the cybercriminal community. If interconnect traffic is not inspected, Diameter attacks can go undetected and operators unable to identify malicious traffic.

SOLUTION

With AFleX® scripting, the Orion 5G Security Suite can provide protection for Diameter interfaces within 4G and 5G networks against DDoS and other attacks. Capabilities, including roadmap features, provide load balancing, monitoring, centralized reporting and analytics with performance and scalability based on clustering solutions. The Diameter firewall can be inserted in-line, tap-mode or inline-view only between home MME-HSS (S6a), visited MME- HSS (S6a) and between visited PCRF and home PCRF (S9a).

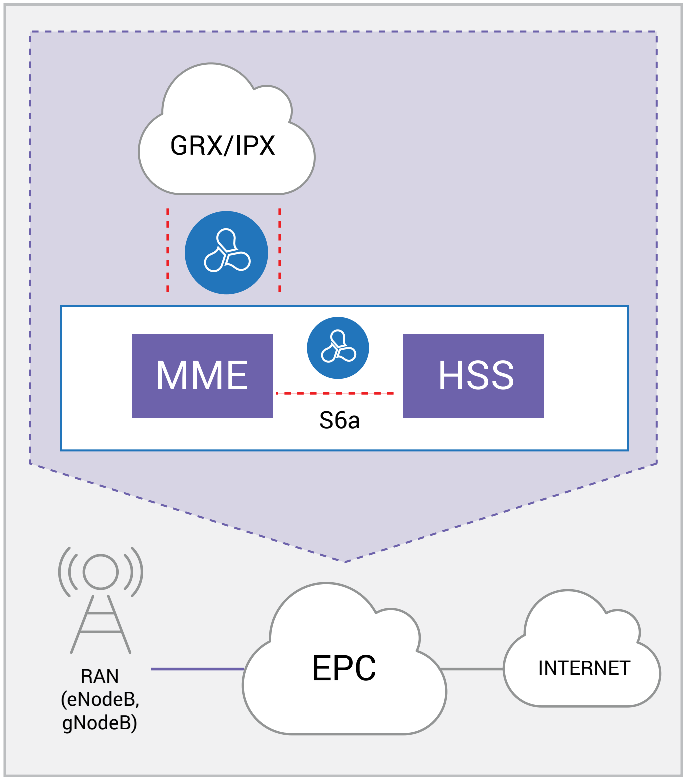
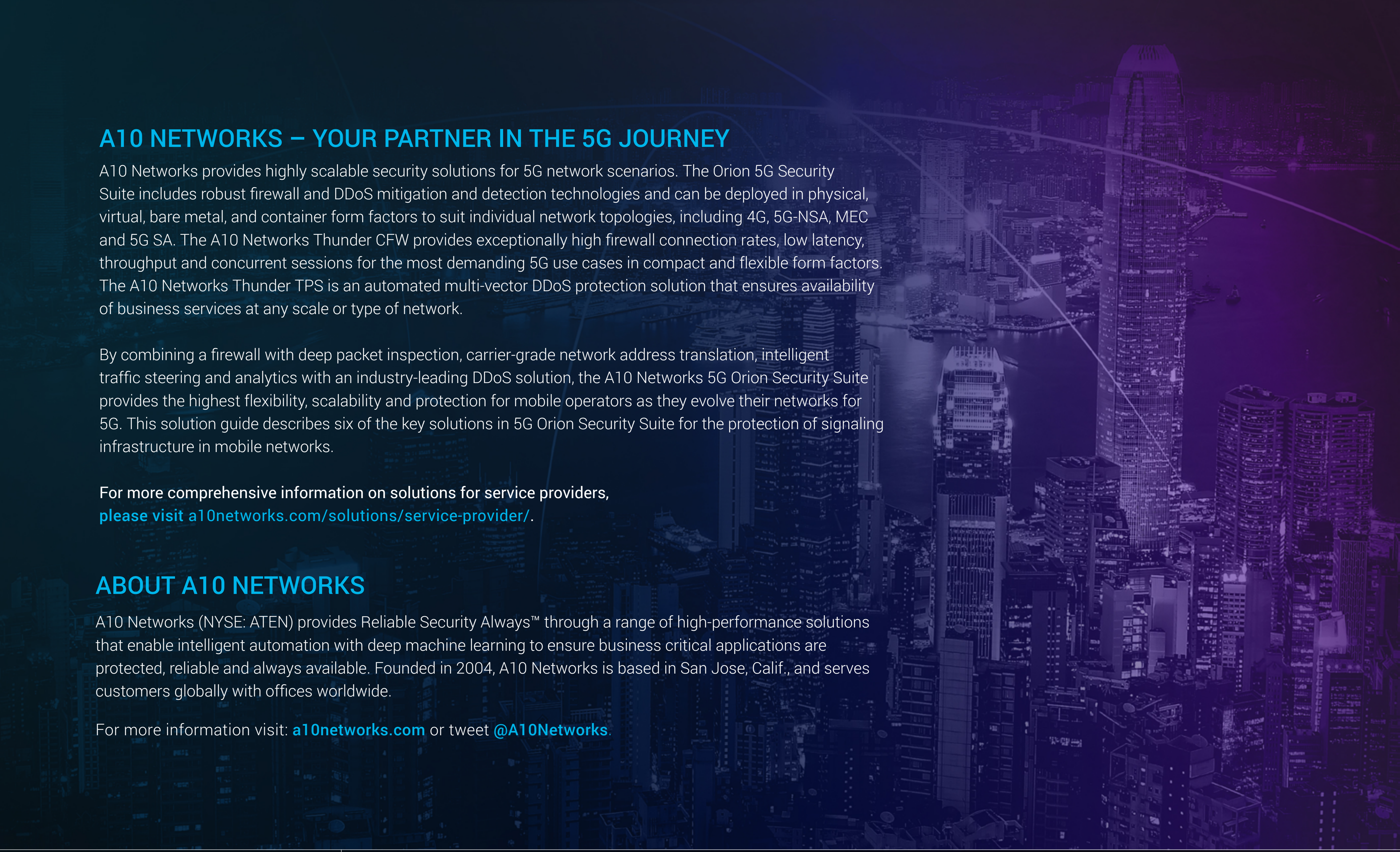


Figure 9. Diameter Firewall provides protection within the EPC



A10 NETWORKS – YOUR PARTNER IN THE 5G JOURNEY

A10 Networks provides highly scalable security solutions for 5G network scenarios. The Orion 5G Security Suite includes robust firewall and DDoS mitigation and detection technologies and can be deployed in physical, virtual, bare metal, and container form factors to suit individual network topologies, including 4G, 5G-NSA, MEC and 5G SA. The A10 Networks Thunder CFW provides exceptionally high firewall connection rates, low latency, throughput and concurrent sessions for the most demanding 5G use cases in compact and flexible form factors. The A10 Networks Thunder TPS is an automated multi-vector DDoS protection solution that ensures availability of business services at any scale or type of network.

By combining a firewall with deep packet inspection, carrier-grade network address translation, intelligent traffic steering and analytics with an industry-leading DDoS solution, the A10 Networks 5G Orion Security Suite provides the highest flexibility, scalability and protection for mobile operators as they evolve their networks for 5G. This solution guide describes six of the key solutions in 5G Orion Security Suite for the protection of signaling infrastructure in mobile networks.

For more comprehensive information on solutions for service providers, please visit a10networks.com/solutions/service-provider/.

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**.

ABOUT A10 NETWORKS
LEARN MORE

CONTACT US
a10networks.com/contact

Part Number: A10-BR-20113-EN-01 FEB 2020