Ten Essentials for Securing LTE Networks

Service providers building out their 4G LTE networks are grappling with numerous complex security challenges. Learn which security capabilities are essential for them to consider and why as they begin to implement carrier-class network firewall solutions.

White Paper

by F5

Introduction

Third generation (3G) mobile telephony included built-in security from the handset through the service provider's core network. Fourth generation (4G) long-term evolution (LTE) is an IP-based system and, as such, brings with it long standing IP-based security weaknesses. From the beginning, standards bodies for LTE have included security in their system architecture evolution, yet many complex security considerations still fall to service providers to manage.

As they move away from a model where all applications live in the data center, service providers need to implement a comprehensive security framework to protect assets throughout more broadly distributed networks. This is where having strong multi-layer protection (layers 4–7) and carrier-class network firewalls come into play.

To be considered "carrier-class," a network firewall must be able to deliver massive scalability, reliability, and simplified management. It also must provide a depth of features and functionality that enables service providers to dynamically protect users and the core network infrastructure.

As service providers continue to expand their networks to support new and evolving broadband services, legacy firewall solutions are unable to effectively scale, maintain low latency, provide high quality of experience for end users, and address emerging threat vectors. They also present speed and performance challenges for service providers in their core networks as voice, video, and multimedia traffic continues to soar.

What follows are ten essential security capabilities service providers should consider as they seek to implement carrier-class network firewalls.

1. Speed and Reliability

In general, a carrier-class network firewall needs to provide 100 Gbps throughput and be able to handle a minimum of 10 million concurrent sessions, 100,000 connections per second, and 100,000 logs per second. In addition, it should introduce no more than 3 milliseconds of latency. These are considered to be typical performance numbers for the next two years.

With the anticipated growth of the Internet of Things over the next five years—and the increase in streaming video and bandwidth-hungry applications—service providers would do well to consider a firewall that can cluster up multiple appliances for totals of over 500 Gbps throughput, 100 million concurrent sessions, and 2.5 million connections per second.

Firewalls must provide carrier-grade resilience and prove five nines (99.999%) of reliability while operating in active-active or active-passive clusters with load balancing, throttling, tunneling, and full proxy. Hardware should meet NEBS compliance.

The nature of security architectures require higher and higher concurrency requirements as we move forward in time—especially with the Internet of Things expanding. Throughput will become less and less a scaling factor over time and the capability to perform many functions at the same time will become more and more prominent.

2. Advanced, Centralized Management

At a minimum, a carrier-class network firewall is expected to support a command line interface (CLI,) a web-based graphical user interface (GUI), and application programming interfaces (APIs) for setting parameters and applying application-specific security configurations. Service providers should be able to centrally provision security services either for subscribers or network functions. A good firewall must enable the application of policy across multiple domains and provide role-based workflow management.

An advanced central management system is key to a service provider's ability to manage policies for a network of multiple firewalls. To simplify the management of distributed network security, the firewall should include management authority over all instances, audit logging that provides the ability to track changes for compliance, monitoring that enables administrators to view the activity across policies, and a unified set of policy controls.

Traditionally, security information and event management solutions have collected lots of information from practically every device on LTE networks. How do we take the patterns of security vulnerabilities and tell the existing security tools (the firewalls, intrusion prevention systems, etc.) what types of things to look for that is indicative of a security threat? And, how do we implement the policies for those devices to take action to protect the network?

Security analytics can pore over the collected data, looking for indicators of compromise for ways that attackers start threats. Service providers need tools that can examine large amounts of event data quickly, and then feed the security controls in a timely manner to protect the LTE network. Network elements need specific recommendations of what to do when it's vulnerable to an attack—things like turning on denial of service prevention or blocking access to certain applications.

3. Broad Protocol Support

In addition to standard TCP/IP, carrier-class network firewalls should support encryption protocols (like IPsec), authentication protocols (like Radius and Diameter), both IPv4 and IPv6, and LTE protocols like Stream Control Transmission Protocol (SCTP), GPRS Tunneling Protocol (GTP), and Session Initiation Protocol (SIP).

4. Flexibility and Elasticity

Security services provided by a carrier-class network firewall must be capable of running on purpose-built hardware or commercial off-the-shelf (COTS) servers to reduce capital expenses. It's important that those services integrate with software-defined networking (SDN) and network functions virtualization (NFV) as part of a larger orchestration system (compatible with OpenFlow and Open vSwitch, for example). In addition, they should support multiple hypervisor technologies, including OpenStack and VMware.

Virtualized security functions lead to a more elastic network that offers on-demand bandwidth and dynamic launching of services to reduce operational expenses. At best, these functions include reactive security that launches only after attacks occur and active signatures that adapt on the fly. Services should be capable of redirecting traffic as needed to bypass affected network elements.

NFV reduces the number of devices that must be configured manually, thus reducing the potential number of misconfigured elements. Intrusion prevention, DDoS protection, and URL filtering provide advantages to service providers when they can be provisioned as virtual network functions (VNFs), which can be spun up on demand (rather than statically) under SDN control.

5. Consolidation of Functions

It's to the service provider's advantage to be able to consolidate various functions within their data centers and network domains. Consolidation can simplify the overall network architecture, reduce the total cost of ownership, and improve customer quality of experience.

6. Carrier-Grade NAT

Service providers need an elastic carrier-grade NAT (CGNAT) solution to reduce the risk of signaling storms on their core networks. These can be generated by targeted attacks against a service provider's infrastructure. The attacker can flood the core network with excessive packet core signaling, which renders the network unavailable to legitimate data traffic and causes connected subscribers to lose network access. By using CGNAT on an S/Gi interface, service providers can hide the IP addresses of their core services from the Internet, helping to insulate those core services from DDoS attacks.

Since the network perimeter separates the mobility infrastructure (inside) from the Internet (outside), it is an ideal location to handle address translation. Networks that currently run IPv4 addressing are faced with a dwindling pool of available public addresses, but the number of subscriber devices these networks need to support is increasing. CGNAT solves this problem, and it needs to do so at a high scale.

7. Radio Access Network Protection

The 3G model of a single, seamless instance of encryption is distorted in LTE because the dedicated radio network controller (RNC) node is eliminated, and its radio resource management functions are distributed to the eNodeB and evolved packet core (EPC). In the LTE network, encryption terminates at the eNodeB, so the traffic that emerges from the eNodeB is clear text.

An attacker that is able to intervene in the network at the cell site (or at any point on the S1 interface) and gain access to the clear text stream can potentially gain access to the network core. From there, the attacker can trigger an outage or obtain access to the private voice and data transmissions of the service provider's customers.

Recognizing that clear text crossing the network exposes subscribers to theft or network outages by hackers, most services providers will adopt IPsec to and from the radio access network (RAN) by the end of 2017. This is especially true for service providers that use open-IP backhaul or backhaul via "untrusted" networks. The trend that will push service providers to leverage more and more of such untrusted backhaul is the deployment of outdoor small cells (outdoor picocell, Femtocell, enterprise small cells, and WiFi network integration). The more that service providers scale these deployments, the higher their risk vectors will increase on the S1 side of the network. They can protect connections by using an embedded IPsec security gateway in each node, which provides encryption of all control and data plane traffic.

8. Core Network Signaling with Partner Networks

Mobile networks strongly depend on specific, logically centralized nodes. A DDoS attack against such a node could have severe consequences, potentially denying access to connectivity over large geographical areas.

An example is the home subscriber server (HSS), a key node of the EPC that performs authentication and billing functions. This essential node, which stores information for every subscriber in the network, authenticates users and is the cornerstone of the paging infrastructure. Therefore, a DDoS attack against this node could potentially prevent the network from operating.

In the EPC, secure communications are required between networks that are run by different service providers in order to handle roaming subscribers. At the interconnection level between roaming partners, one or more of the following methods can be used to enforce security:

- A direct physical connection
- An IPsec tunnel
- A logical connection via a multiprotocol label switching (MPLS) network

Such enforcement ensures that Diameter proxies are not visible in the routing table and can't be reached by non-partner service providers. In addition, an access control list (ACL) is used on interconnect routers and Diameter edge agents (DEAs).

Service providers should also apply logical IP screening at the edge of the network. For example, IP packets sent to or received from a service provider should belong to the IP range assigned to that service provider.

Within LTE roaming scenarios, DNS resolution is required in order to provide mandatory addressing and routing information for home and visited networks. This makes end-users' access to packet data networks possible. Because DNS is used to support all required procedures, it's imperative that a carrier-class network firewall prevent DNS DDoS attacks and provide DNSSEC functionality.

9. Diameter Message Filtering and Topology Hiding

Service providers need the ability to apply Diameter message filtering. Specifically, they need to be able to only allow supported application IDs, command codes, and attribute value pairs (AVPs). They also need the ability to verify consistency between all related AVPs that identify origin and destination, and apply anti-spoofing mechanisms. Diameter transactions should only be allowed from a third-party service provider with which they have an LTE roaming agreement.

This type of message filtering and screening is available in Diameter routing agents (DRAs). The DRA must be capable of screening on relevant fields, such as international mobile subscriber identity (IMSI) ranges or application ID, to ensure that no unexpected or fraudulent traffic is routed. Optionally, the DRA can act as a proxy server if it needs to inspect or take any action on the content of non-routing related AVPs.

With topology-hiding in the DRA, the IP addresses and host names of the Diameter core network elements in the EPC cannot be seen by external parties, thus preventing any information about mobile management entities (MMEs), home subscriber servers (HSSs), policy and charging rules functions (PCRFs), and others from being retrieved by unauthorized parties. Also hidden are the number of certain types of network elements (for example, HSSs) and the routing within a service provider.

10. Protection from the Internet

A carrier-class firewall separates the mobility infrastructure from threats on the Internet, preferably for 3G deployments at the Gi interface and for 4G deployments at the SGi interface. Ideally, a carrier-class firewall includes carrier-grade NAT (CGNAT) to enable high-scale, seamless migration of IPv4 to IPv6 on the same platform. To manage firewall policies across the network, a centralized management solution makes it possible to deliver services across clouds, regardless of the underlying network standards frameworks.

The firewall must be capable of defending the mobility infrastructure and mobile subscribers from attacks, regardless of the source of the attacks. This includes mitigation of large-scale DDoS attacks such as network floods, port scans and sweeps, or connection floods. By detecting and stopping these types of attacks, the firewall can prevent congestion and overloading.

A full-proxy firewall can terminate and inspect incoming client connections for threats. The end result, and the benefit to service providers, is the assurance of network availability and an improved subscriber experience.

One way to defend against layer 7 floods is for the firewall to verify the “humanness” of the incoming connection. This is done by examining the frequency of user-requests. For example, if requests are greater than 20 per second, the requestor is not human. Similarly, if a client connection attempts to renegotiate more than five times within 60 seconds, the connection should be dropped. When a client connection is dropped silently, the attack tool stalls for long periods of time, fully negating the attack.

As a full proxy, the firewall can be applied to both users and applications independently and at a different parts of the application delivery session. It should provide complete flexibility and control for all users, devices, applications, networks, and any other part of the application delivery network.

Conclusion

Service providers must choose high-throughput, right-featured, and flexible security solutions to ensure their competitive advantage. Only then can they continue to build out their networks to reach more users while also protecting them, and enabling them to take advantage of the growth opportunities available in the expanding mobile market.

Even the most secure network cannot protect against the bad data packets it may receive from compromised devices. In that case, the network must have protection at the receiving end of the connection. Security within the network, especially at data centers and service nodes, must be addressed by security applications with deep packet inspection capabilities to identify hidden threats in packet streams and prevent attacks on these essential network services.

The F5 BIG-IP family of products offers solutions to many of the considerations outlined in this paper. Please go to the Security Solutions for Service Providers web page on f5.com to learn more.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. WP-SP-Top 10 0113