BROCADE

SOLUTIONS BRIEF

Brocade Network Visibility and Analytics Solutions

HIGHLIGHTS

- Advanced security solution purpose-built for mobile networks
- Detects and mitigates volumetric attacks, errors, and anomalies in the mobile network
- Employs out-of-band security analytics that operate without disrupting the mobile network
- Provides agile and elastic scalability through an NFV architecture
- Enables real-time closed loop security policy enforcement via SDN, REST, and other integration mechanisms

Mobile Network Security

Service providers, businesses, and consumers alike are frequently victims of cyber-attacks that, when not preempted, can result in significant revenue loss, opportunity and remediation costs, and diminished brand perception. While it is commonly perceived that Internet properties and connected enterprises are the primary targets of cyber-attacks, a survey conducted by Light Reading in 2015 showed that nearly 50 percent of all mobile service providers in developed markets had experienced two or more malicious attacks, lasting an hour or longer, in the past 12 months.

As mobile networks transition from legacy architectures to all-IP architectures, they risk becoming easier targets for experienced cyber-attackers that operate on the Internet. With the growth of mobile traffic and an explosion in the number of applications, many of which are "always on," the scenario becomes even grimmer. An attacker can now infect a large number of handsets in a mobile network and initiate a Distributed Denial-of-Service (DDoS) attack on the access and core infrastructures.

A cyber-attack on a mobile network can originate at either the subscriber edge or at a provider edge (interconnection points with other service providers such as ISPs). Adequately securing a mobile network requires comprehensive monitoring at all entry points to the network, as well controls that track and manage internal access to network elements.

Most security solutions today are network agnostic and designed to generically monitor plain-IP traffic. In mobile networks, security monitoring solutions are typically deployed at the packet-data edge of the mobile core (known as the Gi-LAN), where traffic gets routed to or from the Internet. These solutions fail to adequately address attacks on mobile infrastructure (from the subscriber edge to the mobile packet core, for instance) because such attacks can cause outages or degradation before or without hitting the Gi-LAN.

These generic solutions employ mechanisms such as attack signature detection, which are rapidly becoming irrelevant as a growing volume of IP traffic becomes encrypted. Moreover, most incumbent security solutions are deployed inline in the traffic path, but their legacy, appliance-based architectures do not scale well, making them congestion or failure points in the network.

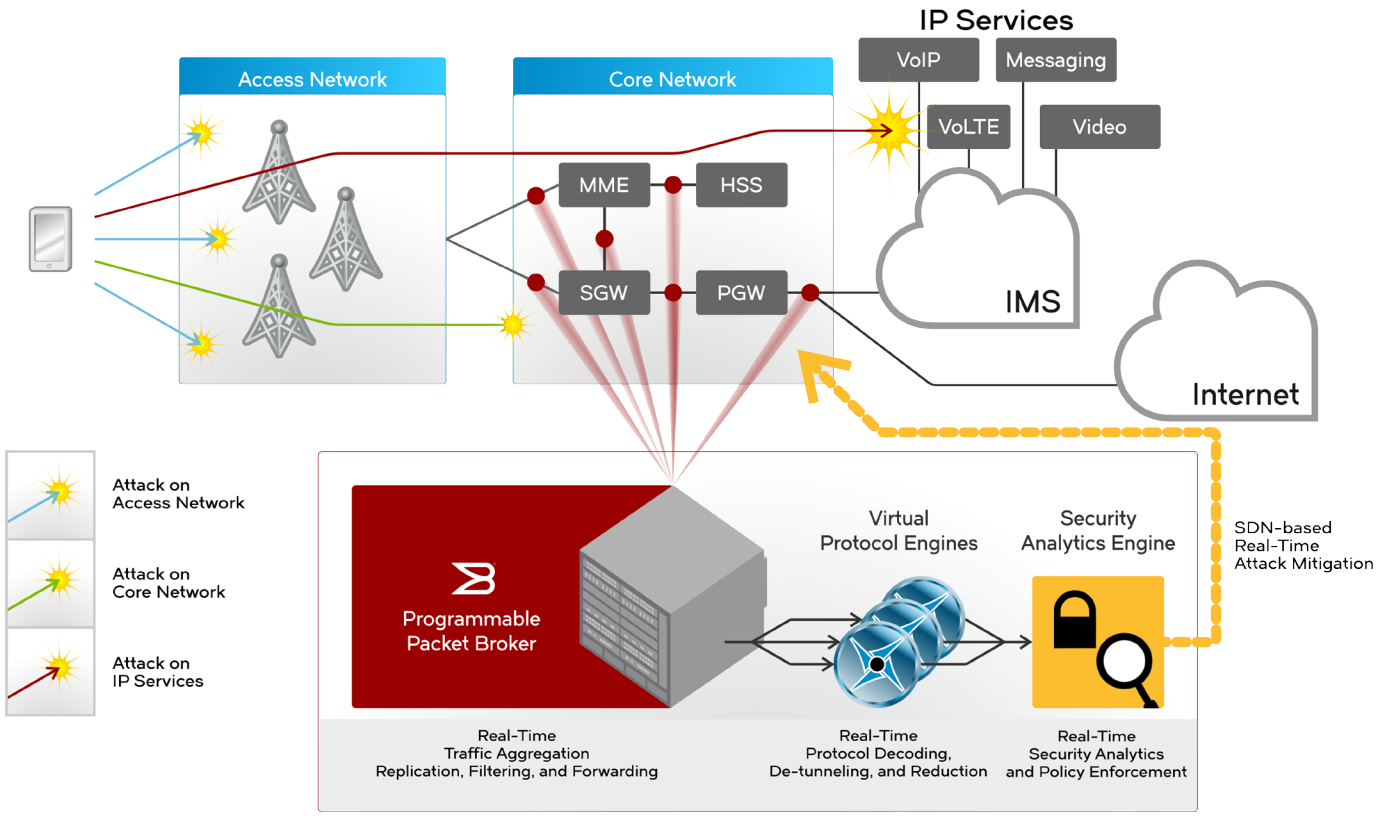

Figure 1: Brocade Mobile Network Security solution architecture.

Mobile service providers require security monitoring solutions that are purpose-built for mobile networks, leveraging the wealth of information available in mobile protocol traffic.

The Brocade Solution

The Brocade® Mobile Network Security solution monitors mobile protocol traffic in addition to plain-IP traffic to detect and mitigate attacks across the mobile network. It is a software-based monitoring solution that is deployed out-of-band, but can dynamically loop-back threat mitigation policies into the network via SDN, REST, and other interfacing mechanisms. Its agile, NFV architecture offers elastic scalability as traffic surges or drops.

Solution Architecture

The Brocade Mobile Network Security solution uses a series of line-speed software engines that decode/de-tunnel and reduce replicated mobile protocol traffic on 3GPP interfaces—such as S1-MME, S1-U, S6a, S11, SGi/Gi, and Gn—for scrutiny by a Security Analytics engine (see Figure 1). The Security Analytics engine correlates traffic from the above interfaces (for subscriber and session-level awareness) and monitors it for attack patterns, errors, and anomalies.

When anomalous traffic patterns are detected, the Brocade solution can trigger notifications to operator personnel via mechanisms such as SMS, e-mail, messages on the operator portal, or custom mechanisms the operator wishes to use. Further, it can dynamically trigger remediation functions (in-band elements such as firewalls, routers, and other policy enforcement points) via SDN, REST, and other interfacing mechanisms to address service degradation or contain malicious attacks.

Volumetric Signaling Attacks on the Mobile Packet Core

Signaling storms are floods of mobile signaling traffic that may impair the control infrastructure of the network, degrading the ability of network elements to serve new traffic and sometimes making them completely unavailable. While signaling storms often occur from the concentration of a large number of active devices in a small geographic area, they can also be caused by cyber-attackers aiming to destabilize the mobile network.

The Brocade solution helps detect and mitigate signaling storms by monitoring signaling traffic volume against acceptable volume thresholds (defined by the service provider based on the capacity of its network elements, backhaul, and other factors) as well as against historical trends. Over time, the Brocade solution continuously learns and evolves predictive capabilities as it trains on increasing volumes of data.

Following are descriptions of different volumetric attacks and ways that the Brocade solution detects and mitigates them.

Attach Floods

Attackers may use software programs to generate a large number of fake subscriber IDs (IMSI) and attempt to connect to a mobile network. Even though these fake IDs are prevented by the HSS from attaching to the network, the large volume of signaling traffic generated by these attach attempts can potentially crash or debilitate the MME, HSS, RNC, or HLR elements in the mobile network.

Similarly, rogue applications that simultaneously switch a number of devices in and out of airplane mode for a sustained period of time can create similar consequences.

The Brocade solution tracks attach requests per device, node, and region, as well as the total number of attach requests encountered by a particular network element in a given time interval. Any significant deviations from "normal" traffic trends are immediately reported for evaluation and can also be dynamically remedied by triggering a temporary deactivation of a subscriber, device, or base station—or by instantiating new virtual instances of the EPC element under duress.

TCP Connection Flooding

With mobile networks rapidly transitioning to an all-IP architecture, the TCP protocol is often used by network elements to communicate reliably. TCP connections between two hosts are established by employing a handshake mechanism involving the exchange of SYN, SYN-ACK, and ACK messages between the hosts.

Malicious hosts can flood a target host (which may be a mobile packet core element or a connected handset) with a flood of SYN messages, to which the targeted host may respond with SYN-ACK messages. The attacking hosts then do not respond with an ACK message, which leaves the connection incomplete on the target host, locking up memory and potentially making the target host unreceptive to new legitimate connection requests, or even crashing it.

The Brocade solution monitors TCP communication for SYN request volume as well as incomplete handshakes within a specified time interval by EPC element, host, subscriber or device, node, and region/zone basis. Suspicious flows can then be forwarded to security policy enforcement systems for mitigation without impacting legitimate flows.

VoLTE SIP Flooding

The SIP protocol is used for delivering IP-based multimedia services, such as Voice over LTE (VoLTE), often across networks using disparate access technologies. A VoLTE SIP-proxy server mediates between a pair of SIP hosts or endpoints attempting to make a connection.

A malicious attacker can overwhelm the VoLTE SIP-proxy server by flooding it with a large number of concurrent or sequential SIP-Invite messages, which can result in degradation or outage of the SIP service.

The Brocade solution monitors VoLTE traffic by tracking, for instance, SIP-Invite messages per device, node, and region, as well as the total number of such messages encountered by a particular VoLTE SIP-proxy server in a given time interval. Any significant deviations from "normal" traffic trends are immediately reported for evaluation and can also be dynamically remedied by triggering a security policy enforcement function.

Attacks on the Radio Access Network (RAN)

The RAN is the most vulnerable part of a mobile network. An outage on one base station can make the service unavailable to thousands of subscribers within a service area. Moreover, the geographic spread of the RAN makes it challenging to monitor.

Following are descriptions of some forms of attacks on the RAN and mechanisms for their mitigation.

Paging Attack

Paging is a mechanism in mobile networks that is used to locate a device that is in idle state (that is, it has not sent or received any traffic for a specific amount of time). When paging an idle device, the mobile network control element (MME in the case of LTE) sends a broadcast message to all devices in the last known tracking area of the device. Idle devices routinely check for paging messages from the mobile network, and they respond by initiating a connection with the network and when they determine that they have been paged. If no response is received when a paging message is broadcast to a tracking area, the mobile network continually expands the tracking area until it finds the device.

A malicious paging attack involves a large number of infected or malicious hosts initiating data sessions (for example, to

load a video or initiate a VoIP call). These hosts then detach from the network, causing the network to attempt to page them to deliver data. A large volume of concurrent paging requests then floods the network, causing legitimate devices to become unable to connect to the network.

The Brocade solution monitors the volume of paging messages in the network by device, node, and EPC element to detect unusual traffic patterns and potentially instruct control elements to stop paging suspicious devices until the attack ceases.

Jamming Attack

One of the most difficult types of attacks to overcome in a mobile network is a jamming attack, in which an attacker can jam or damage a mobile base station by generating a high-power signal targeted at the base station.

While jamming attacks are difficult to prevent, the Brocade solution can actively monitor each base station in the mobile network for activity and notify operator staff when traffic at a base station suddenly ceases, or when no activity is detected at a base station for unexpectedly long durations.

Detecting Errors and Anomalies

The Brocade solution actively monitors TCP and mobile protocol traffic for errors and anomalies, and proactively notifies operator personnel when, for instance, an unexpectedly large number of malformed GTP packets are detected (possibly aimed at destabilizing the packet-data gateway). Other examples include verifying protocol handshake sequences (for completeness), duplicate IP addresses, unauthorized devices, and protocol packet structure adherence.

Conclusion

Generic IP traffic monitoring solutions do not adequately protect mobile networks from malicious attacks. Mobile networks require security solutions that are mobility-aware, and that can protect both access and core networks.

The Brocade Mobile Network Security solution is purpose-built for mobility. It provides comprehensive, real-time, mobile access, and packet core monitoring, and scales dynamically as data traffic volumes grow.

Learn More

Brocade partners with companies of all sizes to deliver innovative solutions that help organizations maximize the value of their most critical information. To learn more, visit www.brocade.com.

About Brocade

Brocade networking solutions help organizations achieve their critical business initiatives as they transition to a world where applications and information reside anywhere. Today, Brocade is extending its proven data center expertise across the entire network with open, virtual, and efficient solutions built for consolidation, virtualization, and cloud computing. Learn more at www.brocade.com.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE