SecurityGen
Telecom Security. Transcending Generations.

Signalling Firewalls: The first line of defence for telcos. But are they enough?

80%	Of signalling networks are vulnerable despite firewall (FW) presence[1]
65%	Of the distributed denial-of-service attacks targeted CSPs[2]
$28.3	Billion in global revenue losses to the telecom industry due to telecom fraud[3]
153	Major telecom security incidents across Europe in 2019; resulting in a total impact of almost **1 billion** user hours lost[4]

Legacy Signalling Firewalls have inherent limitations, which adversaries can easily exploit to breach the core network.

1 **Partial visibility:**
Simple signalling firewalls (FWs) cannot fully visualize the perimeter of signalling networks. FW can analyse and protect only the part that passes through it. Thus, leaving a vast majority of traffic susceptible.

2 **Stateless nature of firewalls:**
FWs are stateless, cannot collect information about current subscriber location and cannot protect against Category 3 **(CAT3)** breaches - the most preferred route for attackers looking to intercept SMS and voice communication, disrupting network using DoS and enabling location tracking.

3 **Limited coverage:**
While most FWs are effectively able to identify and block Category 1 (**CAT1**) and Category 2 (**CAT2**) threats, they are often found lacking when it comes to securing networks against advanced **CAT3** attacks.

4 **Lack of scalability and evolution capabilities:**
It is complicated to constantly fine-tune and update FW rules without breaking the roaming services. Therefore, the FW is often configured once at a usually long implementation stage, thus limiting the protection.

5 **Static architecture:**
Mobile networks are live and ever-evolving with updates, reconfigurations, and integration of new functions and features. Implementation of new equipment might change the signalling traffic routing scheme; as a result, some traffic might end up bypassing existing FWs.

Clearly, legacy Signalling Firewalls cannot protect your core network against advanced, sophisticated threats.

How do you then ensure comprehensive signalling security?

It's time for change:

Gain full visibility and real-time monitoring for complete protection with

IDS - Intrusion Detection System

IDS presents a comprehensive yet easy approach for security monitoring and signalling traffic analysis. It offers end-to-end coverage - from security monitoring and anomalous-activity detection, to protecting signalling network perimeter across **HTTP/2, Diameter, GTP-C and SS7 signalling protocols.**

Stay Tuned!

Learn more about how IDS provides enhanced visibility for early threat detection.

Connect:

contact@secgen.com
www.secgen.com

*Source:

1) SecurityGen research paper
2) Nexusguard's Q3 2018 Threat Report
3) https://www.totaltele.com/511110/90-of-operators-are-striked-by-fraudsters-on-daily-basis
4) https://www.enisa.europa.eu/news/enisa-news/annual-report-on-telecom-security-incidents-in-2019