

SecurityGen

Telecom Security. Transcending Generations.

NGFW: 5G-READY NEXT GENERATION FIREWALL

Solution Overview Datasheet

www.secgen.com

The advent of edge-based computing and 5G is more than just a generational step; it opens up whole new possibilities for every tech industry and most specially for the world of telecommunications. Designed to have faster speeds, larger capacity and reduced latency, 5G is expected to provide users with next-generation experiences and deliver new services.

However, this massively connected environment created by 5G and edge-based computing presents a new and highly vulnerable threat landscape with potentially more significant security risks to consider as cloud, data and IoT threats merge. Adversaries will be able to spread malware via IoT networks, disrupt core functions and use routers as IoT botnets to launch DDoS attacks. In this scenario, protecting the legacy LTE network will be as crucial as the standalone 5G networks – as while a few 5G networks will be built from scratch; most will need to integrate and interoperate with existing technologies and infrastructure. All this means that traditional, rule-based security systems will no longer be enough. A fundamental shift in security approach will be absolutely critical in ensuring holistic security of networks in the 5G era.

SecurityGen's Next Generation Firewall (NGFW), is one such state-of-the-art platform built on cutting-edge Intrusion Detection Systems (IDS), Internet Protocol Firewalls (IPFW), and Artificial Intelligence (AI) modules. It offers a revolutionary way of delivering firewall and other network security capabilities to Communications Service Providers (CSPs) and empowers mobile operators to secure signaling networks, protect subscribers, and safeguard core assets against advanced attacks. This new technology combines comprehensive visibility, with intelligence and high-powered analytics to protect the network and the extended 5G ecosystem. It also provides enhanced protection by integrating detection and protection capabilities and allows for complete application-level inspection and intrusion prevention.

Built using cutting-edge technologies and our team's global expertise in advanced telecom security systems, SecurityGen's NGFW provides:

Real-time Visibility & Active Protection:

The system blocks all malicious messages for SS7, Diameter, GTP, and 5G core. It helps identify targets and sources of illegitimate traffic and responds quickly and decisively. Real-time notification capabilities have an immediate positive impact and boost overall security levels.

Comprehensive Network Visibility:

This provides a complete picture of what is going on in the perimeter of signaling networks and helps identify security flaws that could result in compromises. As 5G platforms get implemented, CSPs can get critically supported with threat prevention and detection on HTTP/2 and PFCP layers.

Powerful Threat Intelligence:

Backed by insights from our research team, SecurityGen's NGFW is updated with state-of-the-art capabilities and offers both detection of and protection from new-age hackers and cyberattacks.

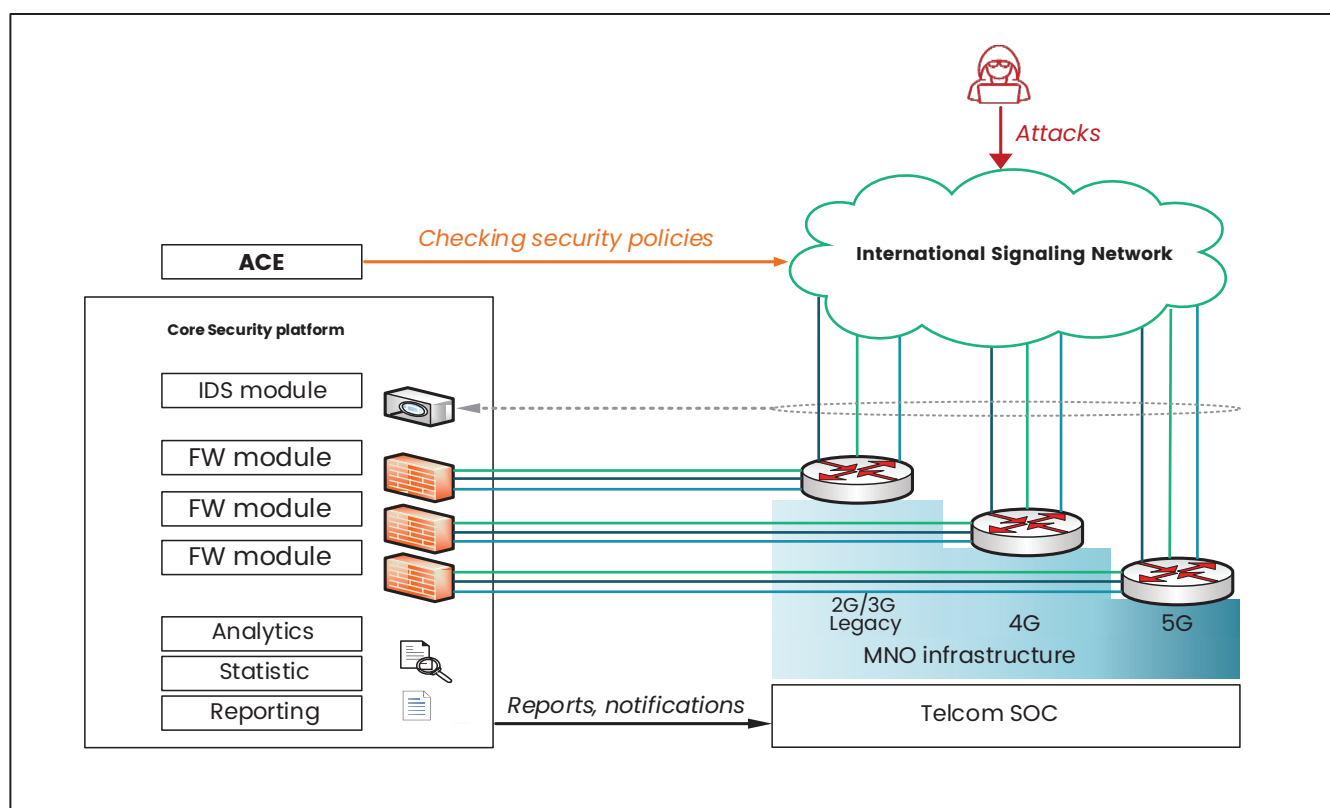
Synergy Effect:

- Detect, Protect and Control in one screen
- One-click rule creation IDS to FW
- Correlation between IDS attacks and FW events
- Control security policies and FW settings, detect FW bypass

NGFW modules

Core Security NGFW platform includes several modules:

- IDS (passive analyze) & FW (active filtering) 5G Standalone & Non-Standalone protection Information disclosure: Subscriber and network DoS: Subscriber and network Subscriber data interception
- 4G/3G/2G - Legacy protection: Information disclosure: Subscriber and network DoS: Subscriber and network Subscriber data interception (SMS, calls, data) Fraud: SMS, calls, online charging
- Analytics
- Statistics
- Reporting

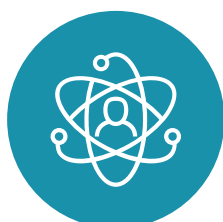


Use cases:



Automate & Simplify Security Operations

The system combines the best-in-class signaling intrusion detection and business intelligence (BI) modules with active firewall modules. It turns security monitoring, signaling traffic analysis, and blocking attacks into a single straightforward process. The system offers out-of-the-box detection and prevention of all types of attacks targeted at subscribers and CSPs infrastructure, allowing for faster incident response and investigation.



Incident Investigation & Response

The system provides rich analytics and reporting capabilities that enable MNOs to take immediate actions and respond to threats as they arise. The comprehensive dashboard with aggregated data, actionable attack and event-related reports helps mitigate attack consequences and perform real-time or retrospective incident investigation.



Incident Reporting

In the event of a security incident, it is imperative to collect information and transfer it to the regulator or management/special service. By using a simple and efficient procedure, the system helps security officers collate all necessary information about security incidents into one pack.



Making SOCs & Other Security Measures More Effective

The system helps evaluate the adequacy of other security countermeasures and provides valuable information to improve their performance. It provides SOCs with complete signaling network visibility, thus making it easier to verify if an attack was successful, reconstruct the kill chain, and gather evidence.

About SecurityGen

Founded in 2022, SecurityGen is a global start-up focused on telecom security. We deliver a solid security foundation to drive secure Telco digital transformations and ensure next-gen enterprise intelligent connectivity.

Connect With Us

- ✉ Email: contact@secgen.com
- 🌐 Website: www.secgen.com

UK | Italy | Czech Republic | Brazil | Egypt
India | South Korea | Japan | Malaysia | UAE