iBASIS
BE THERE FIRST

iBASIS SECURITY iQ360™
INTELLIGENCE
TO DETECT, PREVENT, AND DEFEND
AGAINST SECURITY ATTACKS

SIGNALING FIREWALL

Protect and secure your network
with multi-protocol Signaling Security

KEY OPERATOR CHALLENGES

As roaming increases in complexity, operators need to look at maximizing their roaming revenues while facing significant issues, such as:

- Ever-increasing numbers and sophistication of attacks on mobile networks and their customers
- Insufficient visibility into what is happening and, in a best scenario, awareness only when attacks enter the network
- Increased pressure from regulators to improve telecom security
- Limited technical resources and expertise to correctly maintain up-to-date security solutions
- High-cost CAPEX-based security investments paired with high OPEX (staff) costs
- Increased operational complexity to maintain 2G, 3G, 4G, and 5G networks

iBASIS SOLUTION: OPTIMIZING FIREWALLING FUNCTIONALITY

Telecom networks are becoming increasingly vulnerable to advanced attacker techniques, which are escalating in complexity and similar to those experienced in the IT world.

The iBASIS Signaling Firewall solution was developed with this evolution in mind, using independent feeds for traffic analysis and protection.

It has been designed to respond to the ever-growing issue of Bypass and represents the next generation of firewall, as defined by the industry.

KEY BENEFITS

Full protection for Diameter, SS7, and GTP vulnerabilities with Next Generation Firewalls

Access to unmatched security threat database

Quick deployment and rules customization at initial setup

Automatic Rules updates through APIs possible

Powerful and flexible rules management interface

Maximized revenues and minimized losses from security attacks

BE THERE FIRST

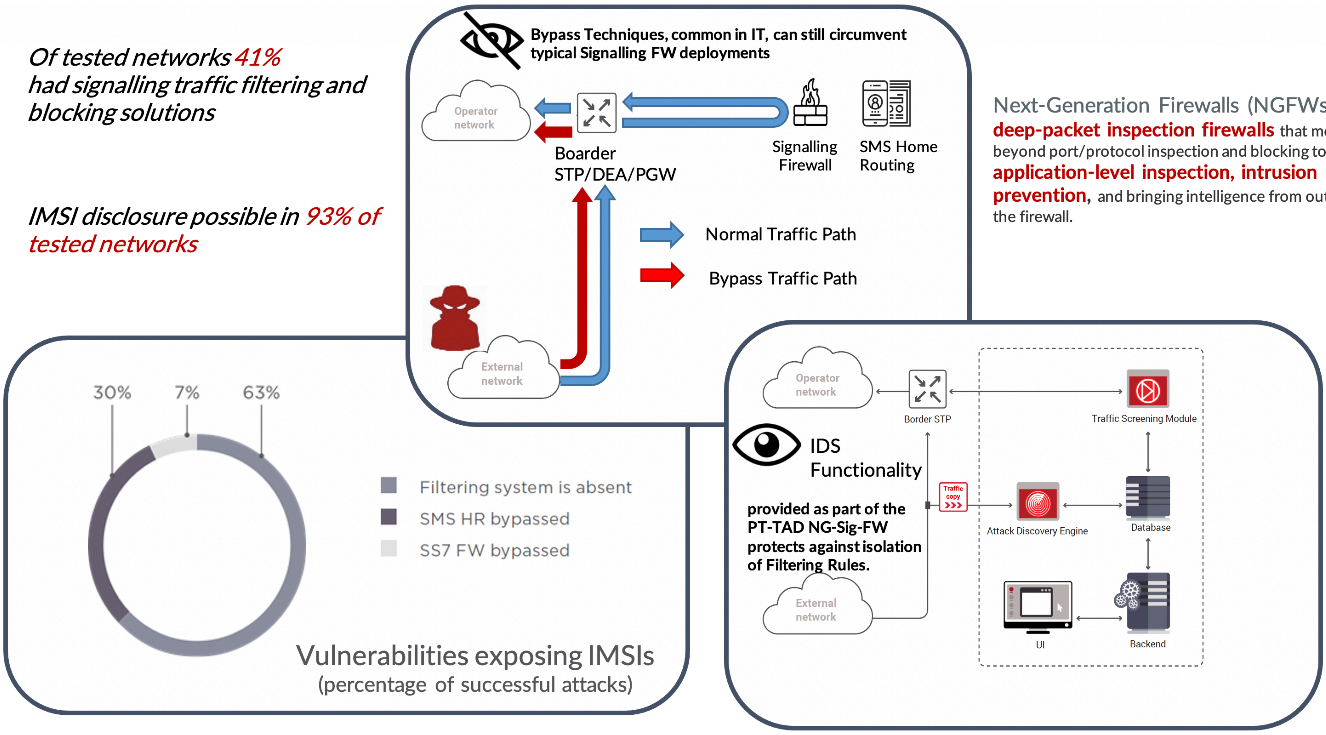
Looking for a customized solution?

Talk to one of our specialists at **info@iBASIS.net.**

iBASIS.COM

Of tested networks 41% had signalling traffic filtering and blocking solutions

IMSI disclosure possible in 93% of tested networks



Next-Generation Firewalls (NGFWs) **are deep-packet inspection firewalls** that move beyond port/protocol inspection and blocking to add **application-level inspection, intrusion prevention,** and bringing intelligence from outside the firewall.

FIREWALL FEATURES

DISCOVERY ENGINE, INCLUDING TWO KEY COMPONENTS:

THE SENSOR: Captures raw network traffic from a network interface, extracts data from that traffic, and sends it to the Correlator. In a case where the source or destination number in a captured message matches a whitelisted GT prefix, the Sensor does not send this message to the Correlator and no attack is detected.

THE CORRELATOR: Checks whether messages received from the Sensor match attack signatures. If a message or a sequence of messages matches an attack signature then an attack is detected. Detected attacks are saved to the Database.

TRAFFIC SCREENING FEATURE

Based on the Access Control List (ACL), the Screening Feature filters incoming messages before they reach the operator network. The ACL consists of default rules configured by firewall administrators that address GSMA CAT1, 2, & 3 and allow the configuration of additional rules via the GUI of the security monitoring and Analytics/Intrusion Detection System (IDS) module.

DATABASE

A centralized storage system based on a transactional database management system (PostgreSQL).

BACKEND

Processes data from the Database to provide UI with information about detected attacks. The module performs the following functions:

- Authenticates and authorizes users
- Processes user-customized settings (references, filters, attack views) and saves them to the Database
- Searches for, aggregates, and filters data taking into account user-customized settings
- Exports detailed information about attacks to JSON files available for download from the user interface
- Generates statistical reports in ODS format available for download from the user interface or regular email distribution

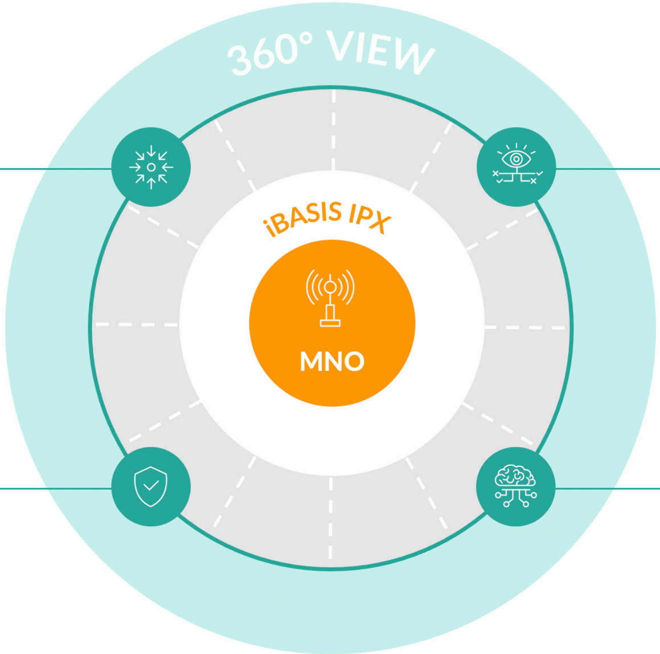
WEB-BASED PORTAL

A web server that provides firewall administrators with a web-based user interface.

iBASIS
BE THERE FIRST

iBASIS SECURITY iQ360™
INTELLIGENCE
TO DETECT, PREVENT, AND DEFEND
AGAINST SECURITY ATTACKS

360 INTELLIGENCE TO DETECT, PREVENT, AND DEFEND AGAINST SECURITY ATTACKS



Vulnerability Assessments

- Automated vulnerability assessments
- Complex manual vulnerability assessments
- Detailed report

Visibility Automatic Attack Detection & Alerts

- Detects and alerts on Cyber Attacks
- Statistics about impact, types
- Drill down to attack detail

Firewalls

- Cloud-based managed firewall solution
- Protection for all signaling: SS7, Diameter, GTPC & 5G http2 on development

DDoS Prevention

- Protects for high value assets as signaling & voice
- Prevents overload with unwanted traffic and lets the genuine traffic pass

The iBASIS Security iQ360™ portfolio is a hosted and fully managed 24/7 solution for attack detection, signaling firewall, and DDoS rule management.

The cloud-based platform sits on the iBASIS network, which eliminates the need for multiple upfront mobile operator network investment and intensive project deployment.

The solution relies on in-depth visibility, monitoring, and attack detection complemented by automatic rule updates against continuously evolving threats and access to one of the largest telecom threat databases.

For signaling firewalls already installed on customer's premises, automatic rule updates via APIs enable superior monetization of existing investments.

The iBASIS security portfolio leverages best-in-class partnerships in cyber security and DDoS protection and ensures optimized efficiency to customers' security teams through one single point of contact.

Combined with its unique anti-fraud platform, iBASIS delivers a holistic approach to security, based on 360-degree solution intelligence to fully protect the global operator's network.

ABOUT iBASIS

iBASIS is the leading communications solutions provider enabling operators and digital players worldwide to perform and transform. Powered by Tofane Global, iBASIS is the first independent communications specialist, ranking third largest global wholesale voice operator and Top 3 LTE IPX vendor with 700+ LTE destinations. iBASIS today serves 1,000+ customers across 18 offices worldwide.

CORPORATE HEADQUARTERS

10 Maguire Road, Building 3
Lexington, MA 02421

T +1 781 430 7500
F +1 781 430 7300
E info@iBASIS.net

For more information, **please visit iBASIS.COM**