clavister
SolutionSpotlight

Clavister GPRS Exchange (GRX) Security Solution

Intelligent and Robust Security for peering between mobile operators

SOLUTION AT-A-GLANCE

- GPRS Exchange, or peering, means that the core network is exposed to security threats and needs protection.
- Security threats includes service interruptions, over-billing attacks and compromised data integrity.
- Consequences of a single security breach in the GRX scenario can result in massive loss of revenues, damage to brand and even legal / compliance issues.
- Clavister GRX Security Solution enables flexible peering with other operators with minimized risk exposure.

KEY FEATURES

- Carrier-grade Firewalling
- Robust and secure VPN to ensure data integrity and minimized risk exposure.
- Flexible deployment options including turn-key hardware appliances and virtualized software for SDN/NFV environments.
- Flexible Configuration and Scalability for smooth interconnection with other operators equipment.

The Challenge

Mobile Network Operators (MNOs) need to interconnect with other operators both to service their own customers currently roaming on other operators networks as well as to hand over guest users to their respective home operators. This interconnectivity, or peering with roaming partners, is typically done over the GPRS Roaming Exchange (GRX) network and the so called Gp interface.

Peering with other operators basically means exposing the core network to a different security domain and comes with significant security threats.

MNOs must protect their networks to avoid costly disruption and damage to brand and business while also providing safe access to and from the networks of external partners.

Solution Overview

When mobile operators peer with each other they connect their respective core networks over the Gp interface, which is a point of vulnerability that can give access to internal packet core services and data.

Deploying GRX-Gp security solutions are considered mandatory since the GPRS Tunneling Protocol (GTP) does not include any security in itself for protecting communication between GPRS networks.

Potential security threats include:

- **Denial-of-Service attacks**, using techniques such as bandwidth saturation, data flooding, spoofing or cache poisoning
- **Overbilling attacks**, when a mobile device is able to hijack an IP address of a legitimate device and start unauthorized data downloads
- Interception and **compromising of data integrity** and confidentiality

Clavister's GRX Security Gateway solution solves these problems, securing subscriber data and revenues by mitigating the risk of network attacks, and enhancing network uptime/performance.

Protecting the Gp/GRX Interface

The most effective solution to mitigate issue related to exposing the core network over the Gp interface is to minimize the attack surface by limit all exposure and communication to run over encrypted and authenticated VPN tunnels.

Authentication minimize exposure

Exposure of the core network equipment and services must be done in order to avoid any hacker, from anywhere in the world to exploit vulnerabilities in the core network. The Clavister GRX Security Solution can achieve this by blocking all access and exposure of the Gp interface and only allow trusted peering partners to connect using VPN tunnels that are authenticated.

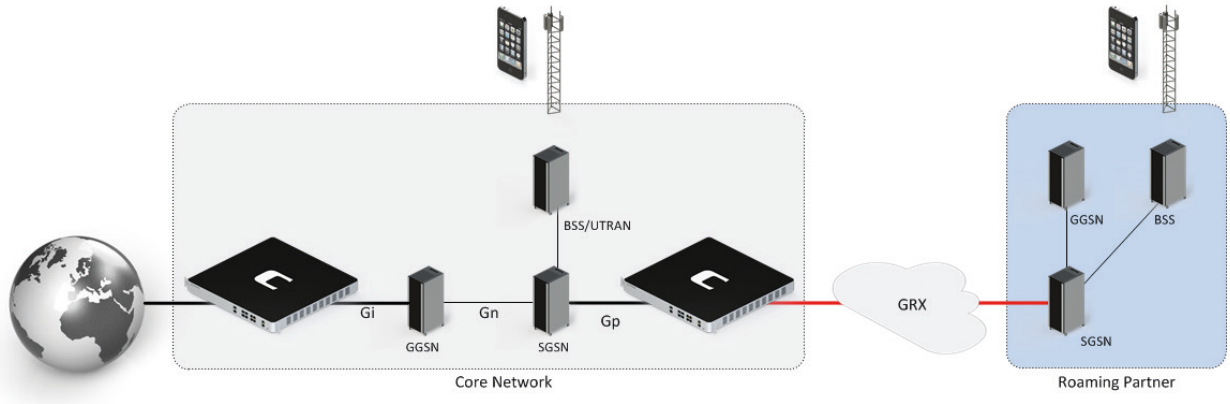
Data confidentiality

It is crucial to encrypt all roaming traffic in order to maintain integrity and confidentiality for the users when communicating with direct roaming partners or the GRX network, especially if transported over the public Internet. The Clavister GRX Security Solution can achieve data confidentiality by encrypting the VPN tunnels with a wide variety of strong encryption algorithms such as AES.

Controlled communication with trusted partners

Even if peering partners are connected using authenticated and encrypted VPN tunnels and might be considered trusted partners they still belong to a different security domain and traffic must be filtered using e.g. firewall policies.

To increase security for the inter-operator communication the Clavister solution offers fine-granular traffic policies as well as anomaly detection features. This helps avoid security breaches that may originate from inside a "trusted" partners network or from a user device.



Security Features

Feature	Benefit
Carrier-grade Firewalling	Minimize risk and control who is allowed to communicate with the core network and how.
VPN	Ensures that only "trusted" roaming partners are able to connect to your core network and that all communication is encrypted.
Flexible configuration	Smoothly interconnect with your roaming partners equipment and still maintain a rigid security without compromises due to inflexible policy configuration.
Anomaly detection and traffic policies	Avoid disruption of the network based on abnormal traffic patters related to e.g. Denial of Service attacks. Detect and blacklist / quarantine misbehaving hosts and maintain full operation for your other subscribers.
Application Control / Deep Packet Inspection	Advanced protocol proxies designed to inspect traffic to verify that it is legit GTP traffic helps avoid attacks with evasive behavior designed to penetrate normal SPI firewall policies.
3GPP/NDS Compliance	The Clavister GRX Security Solution helps MNOs to ensure compliance with 3GPP and NDS by protecting the GTP traffic between different security domains.

Benefits and Conclusions

In addition to securing the core network when peering with roaming partners over the Gp interface and the GRX networks, MNOs can be assured that the Clavister solutions, designed and developed in Sweden, are not shaped by external government or political influences, adding a critical element of trust.

Key benefits include:

- **Flexible platform deployment options**

  Turnkey hardware appliance and virtualized software that runs on COTS hardware / hypervisors and even in NFV/SDN environments.

- **Scalable Capacity and Network Design**

  Scalable performance in combination with flexible platform options makes it easy to fit the Clavister solution into both centralized core networks as well as de-centralized environments.

- **Unified Security Architecture**

  The Clavister GRX Security Solution is based on the Clavister Security Gateways which is the same technology used in order to protect e.g. the Gi and Gn interfaces which also expose the core network to security threats.

- **Reliable and Carrier-Grade**

  The Clavister GRX Security Solution is a mature product designed for carrier grade environments.

Thanks to the unique design and strong partnership with Intel MNOs can deploy the Clavister solution in both turn-key hardware appliances and NFV scenarios using exactly the same software, using the same administration tools and the same security features

Using Clavister's scalable, flexible GRX Security Gateway, which offers advanced IPsec capability and supports other advanced security applications, MNOs can protect GRX networks infrastructure against threats and attacks, and easily manage their security deployments. This boosts trust, helps to increase operational efficiency, and protects revenues.

Where to Buy Clavister

For more information about where to buy Clavister products, visit www.clavister.com/partners. Additional resources and customer testimonials can be found at www.clavister.com/support/resources.

About Clavister
Clavister (NASDAQ: CLAV) is a leading security provider for fixed, mobile and virtual network environments. Its award-winning solutions give enterprises, cloud service providers and telecoms operators the highest levels of protection against threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the Product Quality Leadership Award from Frost & Sullivan. The company was founded in Sweden in 1997, with its solutions available globally through its network of channel partners. To learn more, visit www.clavister.com.

Where to Buy
www.clavister.com/partners

Contact
www.clavister.com/contact

clavister®
WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
■ **Phone:** +46 (0)660 29 92 00 ■ **Fax:** +46 (0)660 122 50 ■ **Web:** www.clavister.com