

In All The Colors Of The Rainbow



Cellular Operators



Network Security for Cellular Packet Network

General Packet Radio Service (GPRS) is a data network architecture that is designed to integrate with existing GSM networks and offer mobile subscribers "always on" packet switched data services access to corporate networks and the Internet. GPRS provides mobile operators with an opportunity to offer higher-margin data access services to subscribers. In return, subscribers benefit from GPRS by being able to use higher bandwidth mobile connections to the Internet and corporate networks.

GPRS promises to benefit mobile data users greatly by providing always on higher bandwidth connections than are widely available today. In order to be successful, data connections must be secure and be available anytime and from any place. GPRS Tunneling Protocol (GTP) is the protocol used by GSM or UTMS operators to convert radio signals from subscribers into data packets, and then to transport them in non-encrypted tunnels. GTP does not provide for inherent security.

GPRS Tunneling Protocol (GTP) is the protocol used by GSM or UTMS operators to convert radio signals from subscribers into data packets, and then to transport them in non-encrypted tunnels. GTP does not provide for inherent security.

With the addition of GPRS to GSM, mobile operators are adding mobile Internet and virtual private network services to their existing mobile voice services. When connecting their GPRS network to a variety of external networks, mobile operators must take the appropriate steps to protect their own network from attacks initiating from these external networks, while continuing to provide access to and from them.

Bynet Data Communications' solution is based on Juniper Network's purpose-built firewall/VPN platform, which secures cellular operators infrastructure while developing GPRS-based services. Implementing IPSec between roaming partners, traffic rate limiting, and GTP stateful inspection can mitigate a significant number of threats on the roaming network. Stateful packet inspection, traffic rate limiting, and logical separation of traffic for each corporate network and the public network, can significantly reduce the threat between the operator's network and subscribers.

Juniper Networks has developed technology and solutions that include GTP-aware stateful inspection firewall, GTP aware traffic shaping, and a VPN/VLAN tunnel hub. These solutions help mitigate many of the possible threats to the GPRS network, mobile subscribers, and corporate networks.

