

FireWall-1 GX

Advanced Security for 2.5G and 3G Wireless Infrastructures

PRODUCT FEATURES:

- Protection for GPRS/UMTS Infrastructure
- Protection Against Over-billing Attacks
- Integration with Fraud Management Systems
- Session Hijacking Protection
- Granular Control of Cellular-specific Services
- Extensible with Range of Check Point and OPSEC Products
- Centralized, Policy-based Management with Detailed Auditing and Tracking of GPRS/UMTS Traffic

PRODUCT BENEFITS:

- Delivers Maximum Security for Your GPRS/UMTS Network
- Intelligently Secure Connections Between GPRS/UMTS Carriers
- Enables Revenue-generating Services
- Streamlined, Centralized Management with SMART Management

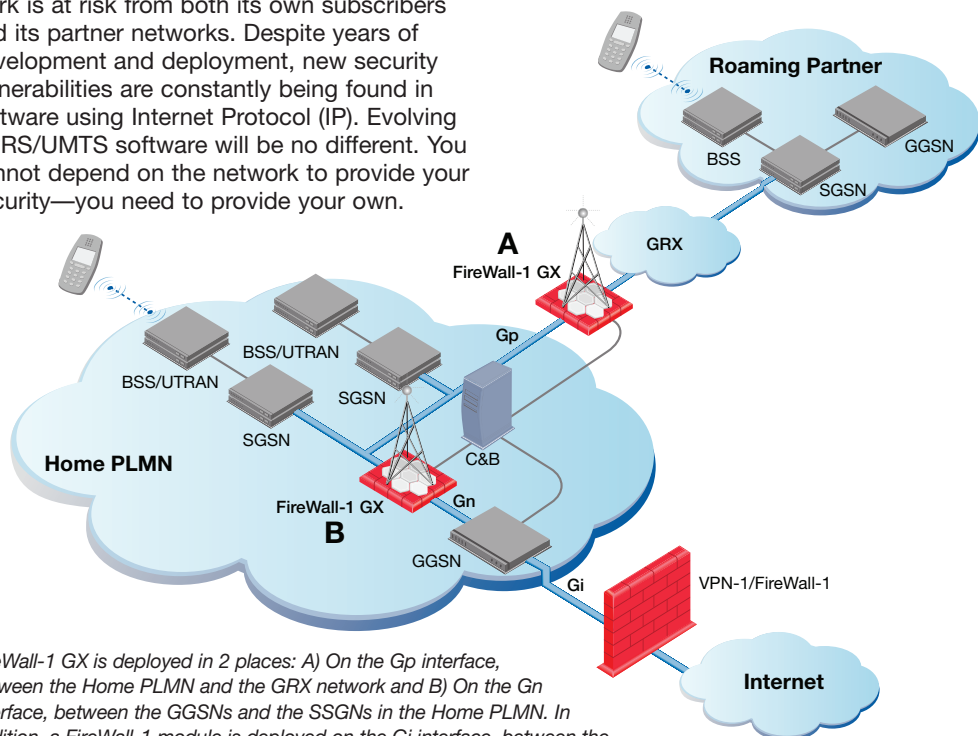
YOUR CHALLENGE

The most widely deployed wireless networks worldwide are those based on GSM technology. Today, GSM wireless operators are able to deliver high-speed Internet access for mobile subscribers using GPRS (2.5G) and UMTS (3G). The infrastructure deployed by wireless operators—networking equipment, protocols, signaling services, and computing platforms—is unique. This infrastructure requires a security solution that is aware of the challenges of the environment and is compliant with the appropriate standards.

Wireless operators rely on a key network protocol—the GPRS Tunneling Protocol (GTP)—for the delivery of these mobile data services. However, GTP itself is not designed to be secure. The GTP protocol specifically states: “No security is provided in GTP to protect the communications between different GPRS networks.” The GPRS/UMTS network is at risk from both its own subscribers and its partner networks. Despite years of development and deployment, new security vulnerabilities are constantly being found in software using Internet Protocol (IP). Evolving GPRS/UMTS software will be no different. You cannot depend on the network to provide your security—you need to provide your own.

OUR SOLUTION

Check Point FireWall-1® GX™—based on the industry’s leading Internet security gateway, FireWall-1—is a dedicated solution to protect GPRS and UMTS networks. By providing a GTP-level security solution that blocks illegitimate traffic “at the door,” your mobile communications are ultra-secure. FireWall-1 GX is specifically designed for wireless operators. It is based on Check Point’s patented Stateful Inspection technology provided with full GTP awareness. FireWall-1 GX inspects all GTP tunnel fields in the context of both the packet and the tunnel. This enables granular security policies that deliver the highest level of security for wireless infrastructures. FireWall-1 GX is managed by Check Point’s SMART management solution, a centralized console that efficiently manages multiple FireWall-1 GX deployments as well as other Check Point gateways.



FireWall-1 GX is deployed in 2 places: A) On the Gp interface, between the Home PLMN and the GRX network and B) On the Gn interface, between the GGSNs and the SGSNs in the Home PLMN. In addition, a FireWall-1 module is deployed on the Gi interface, between the Home PLMN and the Internet.



PROTECTION FOR GPRS/UMTS INFRASTRUCTURE

Mobile wireless network operators have been accustomed to proprietary systems and closed networks. With the deployment of GPRS and UMTS networks, they are now confronted by an unfamiliar world of open systems and vast open networks, where anyone with a PC or mobile device has easy access to the hardware, software, and knowledge needed to compromise security and disrupt communications.

FireWall-1 GX Deployment

Deployed at the Border Gateway (Gp interface) and on the Intra PLMN backbone (Gn interface), FireWall-1 GX secures the GPRS backbone when connecting to roaming partners and roaming exchanges (GRX). FireWall-1 GX also protects distributed GPRS backbone environments where operators have connections to Gateway GPRS Support Nodes (GGSNs) outside their own network or to GGSNs that are geographically dispersed.

Only FireWall-1 GX enables operators to define and enforce customized, granular “GTP-aware” security policies for both GTP v0 and GTPv1. FireWall-1 GX is fully configurable, and is capable of producing GTP-specific detailed logs and alerts.

GTP-Aware Security Policy

FireWall-1 GX enables the administrator to define a single GTP-aware Security Policy using Check Point’s intuitive GUI tools, and provides the following features:

- APN awareness
- IMSI Prefix awareness
- MS-ISDN Prefix awareness
- APN Selection Mode awareness
- End User IP address Static Mode assignment

GTP Protocol Integrity

FireWall-1 GX strictly enforces legitimate use of the GTP protocol, both in structure and in flow, protecting GSN servers from harmful traffic.

- The FireWall-1 GX parser verifies that each GTP message contains the correct set of Information Elements in the proper sequence.
- GTP Stateful Inspection ensures that only legitimate GTP traffic is passed through—for example, data packets (G-PDUs) are allowed only for open PDP contexts, and PDP context update messages are not allowed for closed PDP contexts.

Intra-Tunnel Inspection

In addition to securing the GTP protocol layer, FireWall-1 GX is able to inspect the encapsulated end user network traffic.

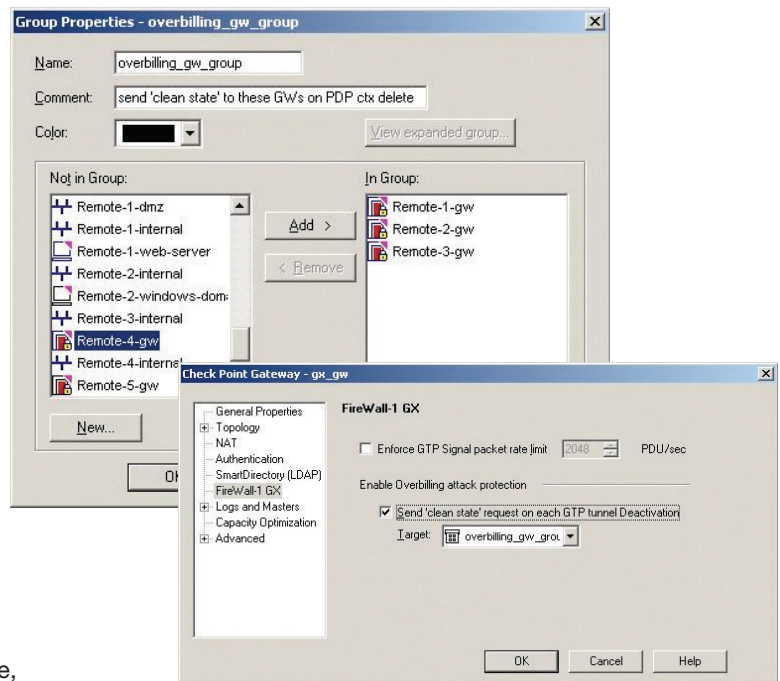
- FireWall-1 GX can prevent mobile subscribers from accessing specific network resources as well as limit the communication between mobile subscribers based on APN.
- FireWall-1 GX can prevent mobile subscribers from injecting GTP packets by preventing GTP within GTP traffic.
- The GTP Antispoofing capability can prevent mobile subscribers from using the operator’s GPRS connection from launching spoofed network traffic.

Standards Compliant

FireWall-1 GX complies fully with GSM standards for GTP, including GTPv0 (3GPP TS 09.60) and GTPv1 (3GPP TS 29.060).

PROTECTION AGAINST OVER-BILLING ATTACKS

Protection against over-billing attacks can be implemented quickly and simply on networks with a FireWall-1 GX and a FireWall-1® enforcement module on the Gi interface. Check Point resolves the vulnerability inherent in deleted PDP contexts by sending a “clean slate” message to the FireWall-1 enforcement module on the Gi interface. Over-billing attack protection can be enabled with a single click.



Over-billing attack protection can be enabled with a single click.

INTEGRATION WITH FRAUD MANAGEMENT SYSTEMS AND BILLING SYSTEMS

To be effective, fraud management systems and billing systems both require the ability to collaborate and integrate with the security solution. With APIs developed by Check Point for our OPSEC partners, these third-party solutions can be fully integrated with FireWall-1 GX. As an integrated solution, GPRS services can be controlled at the level of specific mobile users based on IMSI, MSISDN, and APN. Users can be blocked due to pre-paid expiration or fraud detection.

SESSION HIJACKING PROTECTION

FireWall-1 GX provides session hijacking protection during a subscriber handover. Handover is a fundamental feature of GPRS/UMTS, which enables subscribers to seamlessly move from one area of coverage to another with no interruption of active sessions. Session hijacking can come from the SGSN or the GGSN, the result of a situation where a fraudulent GSN can intercept another GSN and redirect traffic to it. This can be exploited to hijack GTP tunnels or cause a denial of service. To counter this threat, FireWall-1 GX provides Handover Groups, sets of IP addresses among which handovers are allowed. Handover groups typically consist of the IP addresses of a GPRS/UMTS operator's GSNs. The same mechanism is used to enforce GTP redirection, which enables load sharing among xGSNs.

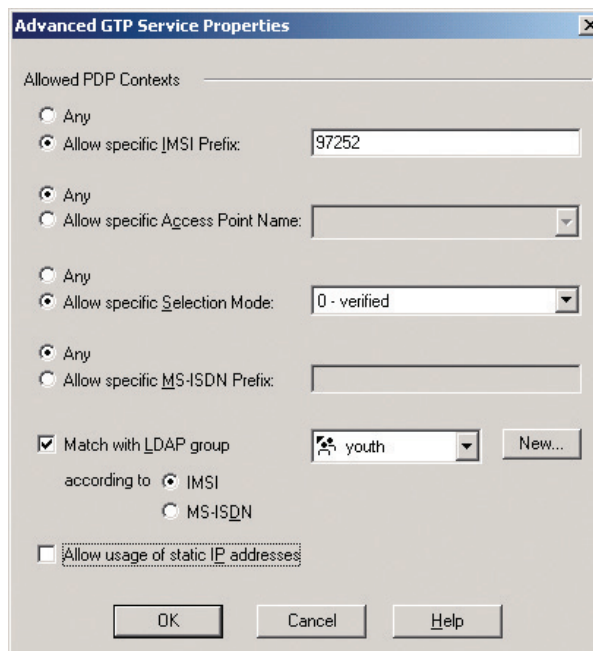
GRANULAR CONTROL OF CELLULAR SPECIFIC SERVICES

Security for the home PLMN is not the only challenge mobile operators face today. Enforcing current business models and developing new ones to meet rapidly changing technology and customer demands are constant and ongoing efforts. FireWall-1 GX enables mobile operators to deploy and manage a variety of business services.

FireWall-1 GX includes pre-defined services specially designed to meet the requirements of GPRS/UMTS operators. Cellular-specific services can be managed including WAP, MMS over WAP, and MMS over HTTP. The MMS resource can Accept, Log, or Drop any MMS transaction over WAP, as well as support redirection.

Integration with Mobile Subscriber LDAP Database

FireWall-1 GX supports the creation of a GTP-based policy based on LDAP user groups that are defined in the mobile user database. This can enable mobile operators to apply a different GTP policy to different user groups. For example, a security rule can be configured to limit mobile subscribers GPRS access to certain hours of the day.



Match users according to IMSI or MS-ISDN.

EXTENSIBLE WITH RANGE OF CHECK POINT AND OPSEC PRODUCTS

- FloodGate-1® can be used for GTP Quality of Service (QoS)
- VPN-1 can be used to encrypt a GTP session
- ClusterXL for High Availability and Load Sharing
- SecureXL for acceleration of non GTP traffic

CENTRALIZED POLICY-BASED MANAGEMENT WITH DETAILED AUDITING AND TRACKING OF GPRS/UMTS TRAFFIC

Check Point Security Management Architecture (SMART) solutions enable you to centrally manage and deploy a single firewall policy to an unlimited number of FireWall-1 GX gateways. Once a policy is created or modified, it is automatically distributed to all locations.

SMART Management for FireWall-1 GX includes the ability to generate reports specific to GTP network traffic with Check Point's SmartView Reporter. These reports can help administrators monitor the status of their GPRS network by consolidating the log files in an easy to read report.

SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
sgsn	ggsn	* Any Traffic	gtp_v0_youth	reject	Log	ludwig	late_night
ggsn	sgsn		gtp_v1_youth			amnon	

Cellular operators can apply a different GTP policy to different user groups. For example, limit users to GPRS access to certain hours of the day.

SUPPORTED PLATFORMS

Crossbeam Systems

Nokia IPSO

Solaris

Red Hat Linux

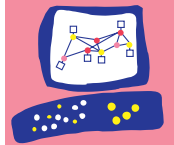
Check Point SecurePlatform™

For more information on supported platform, please visit the Check Point Platform Selection Guide at <http://www.checkpoint.com/products/protect/platforms.html>.

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies (www.checkpoint.com) is the worldwide leader in securing the Internet. It is the confirmed market leader of both the worldwide VPN and firewall markets. Through its Next Generation product line, the company delivers a broad range of intelligent Perimeter, Internal and Web security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company's Zone Labs (www.zonelabs.com) division is one of the most trusted brands in Internet security, creating award-winning endpoint security solutions that protect millions of PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from over 350 leading companies. Check Point solutions are sold, integrated and serviced by a network of more than 2,300 Check Point partners in 92 countries.

Check Point
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

www.checkpoint.com

©2004 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, ClusterXL, ConnectControl, Connectra, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, InterSpect, IQ Engine, Open Security Extension, OPSEC, Provider-1, Safe@Office, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SSL Network Extender, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, Web Intelligence, TrueVector, ZoneAlarm, Zone Alarm Pro, Zone Labs, the Zone Labs logo, AlertAdvisor, Cooperative Enforcement, IMsecure, Policy Lifecycle Management, Zone Labs Integrity and Smarter Security are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726 and 6,496,935 and may be protected by other U.S. Patents, foreign patents, or pending applications.

August XX, 2004 PN: 000000