01 용어 정리

용어 정리

Carrier Security는 이동통신 사업자 망(GPRS·UMTS·LTE)을 GTP 수준에서 보호 하는 솔루션입니다(옛 이름 Firewall-1 GX). 이 가이드를 읽는 데 바탕이 되는 핵심 용어를 흐름에 따라 풀어 둡니다.

이동통신 세대와 망

이동통신은 세대로 나뉩니다 — **GSM**(2G), **GPRS**(2.5G, 패킷 데이터), **UMTS**(3G), **LTE**(4G)입니다(개요). 데이터망의 핵심 요소는 **MS**(Mobile Station, 단말), **SGSN**(Serving GPRS Support Node), **GGSN**(Gateway GPRS Support Node) 이고, LTE에서는 **eNodeB**, **MME**, **S-GW**, **P-GW** 가 그 역할을 합니다.

GTP — 보안의 핵심 대상

GTP(GPRS Tunneling Protocol) 는 이동 데이터 서비스를 전달하는 핵심 프로토콜입니다. 가장 중요한 사실은 GTP가 설계상 보안이 없다(Insecure By Design) 는 점입니다 — 그래서 별도 보안이 필요합니다(소개). GTP는 버전이 여럿(GTPv0/v1/v2)이라, Carrier Security는 모든 GTP 버전을 인식(GTP-aware) 합니다.

Carrier Security의 핵심 개념

GTP-Aware Security Policy 는 GTP 터널의 모든 필드를 패킷과 터널 양쪽 맥락에서 검사해, 어떤 시그널링 메시지·출발지를 허용할지 선택적으로 정하는 정책입니다(UMTS/LTE 보안). **GTP Tunnel** 은 SGSN과 GGSN 사이에 데이터를 캡슐화해 나르는 터널 이고, **APN(Access Point Name)** 은 단말이 접속할 패킷 데이터망을 가리키는 이름 으로 APN 기반 정책에 쓰입니다.

게이트웨이가 검사하는 망의 접점(interface)으로 **Gn**(SGSN↔GGSN), **Gp**(다른 사업자망 간), **Go**, **S1·S5·S11**(LTE) 인터페이스 가 있습니다.

위협·운영 용어

GTP 망을 노리는 위협으로 DoS, IP spoofing, **Overbilling**(과금 조작), tunnel hijacking, flooding, DNS cache poisoning 등이 있습니다(소개). 운영에는 **Monitor-Only Mode**(차단 없이 관찰만), GTP Tracking 로그, SNMP 통계 가 쓰이고(모니터링), 고급 구성으로 **GRX**(GPRS Roaming Exchange) 이중화, **SCTP·Diameter** 인식 등이 있습니다(고급 구성).

02 GSM/GPRS/UMTS/LTE 개요

GSM/GPRS/UMTS/LTE 개요

Carrier Security를 이해하려면 먼저 이동통신망이 어떻게 생겼는지 알아야 합니다. 이 장은 세대별 망과 그 구성요소, 그리고 핵심 프로토콜 GTP를 정리합니다.

이동통신 세대

이동통신은 세대를 거치며 발전했습니다 — **GSM**(2G, Global System for Mobile Communications, 음성 중심), **GPRS**(2.5G, General Packet Radio Services, 패킷 데이터 도입), **UMTS**(3G, Universal Mobile Telecommunications System), **LTE**(4G, Long Term Evolution) 입니다. **IMS**(IP Multimedia Subsystem)는 IP 기반 멀티미디어 서비스를 위한 구조입니다.

핵심 흐름은 폐쇄적·전용 망에서 개방형 IP 세계로의 전환 입니다. 이 전환 덕에 편리해졌지만, 동시에 인터넷의 온갖 위협에 노출 되게 됐습니다(소개).

망의 구성요소

GPRS/UMTS 망 의 기본 요소는 **MS**(단말), **SGSN**(Serving GPRS Support Node, 단말을 관리·추적), **GGSN**(Gateway GPRS Support Node, 외부 패킷망으로의 관문) 입니다. SGSN과 GGSN 사이를 GTP 터널이 잇습니다.

LTE 망 은 요소가 다릅니다 — **eNodeB**(기지국), **MME**(Mobility Management Entity, 제어), **S-GW**(Serving Gateway), **P-GW**(PDN Gateway, 외부망 관문) 입니다. 역할은 GPRS/UMTS와 비슷하되 더 분화되어 있습니다.

시그널링 프로토콜과 GTP 버전

망 안에서는 여러 **시그널링 프로토콜** 이 오가는데, 그 중심이 **GTP(GPRS Tunneling Protocol)** 입니다. GTP는 제어용(GTP-C)과 사용자 데이터용(GTP-U) 으로 나뉘며, 버전이 여럿입니다 — **GTPv0**(GPRS 초기), **GTPv1**(UMTS), **GTPv2**(LTE) 입니다. 버전마다 메시지·필드가 다르므로, Carrier Security는 모든 GTP 버전을 인식(GTP-aware) 해 검사합니다.

정리하면, 이동통신망은 세대(GSM→GPRS→UMTS→LTE)를 거치며 IP 기반으로 개방됐고, 그 데이터의 핵심 운반 프로토콜이 GTP 입니다. 왜 이 GTP에 보안이 필요한지는 소개에서 이어집니다.

03 Carrier Security 소개와 배포

Carrier Security 소개와 배포

Carrier Security(옛 이름 Firewall-1 GX)는 무선 사업자를 위해 설계된, GTP를 완전히 인식하는 보안 솔루션입니다. 이 장은 왜 필요한지와 어떻게 배포하는지를 정리합니다.

GPRS/UMTS 망에 보안이 필요한 이유

개요에서 봤듯, 망이 폐쇄형에서 개방형 IP로 전환 되면서 단말과 망 모두가 인터넷의 온갖 위협과, 무선 망을 노린 특수 공격 에 노출됐습니다 — DoS, IP spoofing, Overbilling(과금 조작), tunnel hijacking, flooding, DNS cache poisoning 등입니다.

GTP — 설계상 보안이 없다

핵심 문제는 GTP 자체에 보안이 없 다는 것입니다. GTP 명세조차 이렇게 인정합니다.

> *No security is provided in GTP to protect the communication between different GPRS networks.*
>
> — Carrier Security AdminGuide, "GTP - Insecure By Design"

즉 망이 알아서 보안을 제공해 주길 기대하지 말고, 직접 보안을 마련 해야 합니다.

Check Point의 해법

Carrier Security 는 2001년부터 GPRS·UMTS·LTE(2.5/3/4세대) 망을 보호해 왔습니다. 핵심은 Check Point의 특허 Stateful Inspection에 GTP 인식(GTP-awareness)을 결합 한 것입니다 — GTP 터널의 모든 필드를 패킷과 터널 양쪽 맥락에서 검사 해, 부적합한 트래픽을 "문 앞에서" 차단 합니다. 모든 GTP 버전에 대해 맞춤형·세밀한 "GTP-aware" 정책 을 정의·집행합니다.

배포

Carrier Security는 전용 라이선스 가 필요하며, Security Gateway에 얹어 배포합니다. 배포 위치가 중요한데, 개요에서 본 망의 접점에 둡니다 — **Gn 인터페이스**(SGSN↔GGSN), **Gp**(사업자망 간), **Go**, LTE의 **S1·S5·S11** 입니다. 게이트웨이를 이 접점에 두면, Gn/S5에서는 APN 기반 정책, Go에서는 GSM-SIP·SCTP·Diameter 인식 방화벽 같은 추가 보안을 쓸 수 있습니다(UMTS/LTE 보안).

정리하면, GTP는 설계상 무방비이므로 사업자가 직접 보안을 마련해야 하고, Carrier Security가 Stateful Inspection + GTP 인식으로 그 역할 을 합니다. 실제 보호 방식은 UMTS/LTE 네트워크 보안에서 이어집니다.

04 UMTS/LTE 네트워크 보안

UMTS/LTE 네트워크 보안

이 가이드의 핵심 장입니다. Carrier Security가 GTP 망을 실제로 어떻게 보호하는지 — GTP 프로토콜 보안, GTP-aware 정책, 터널 내부 검사, 가입자 트래픽 보호 — 를 정리합니다.

GTP Protocol Security

GTP는 설계상 보안이 없으므로, 어떤 보안 체계든 GTP를 고려해야 합니다. Carrier Security는 GTP를 인식하는 정책으로, 악성 데이터나 프로토콜 오용 시도를 식별·거부 하고, GTP로 캡슐화된 데이터 패킷 속까지 검사 합니다.

대표 위협이 **Overbilling 공격** 입니다 — 공격자가 GTP 터널을 조작해 다른 가입자에게 요금을 떠넘기거나 무료로 데이터를 쓰 는 공격인데, Carrier Security가 이를 막습니다. 이 밖에도 프로토콜 오용·비정상 메시지를 GTP 수준에서 걸러냅니다.

GTP-Aware Security Policy

핵심이 **GTP-Aware Security Policy** 입니다. 일반 방화벽 규칙이 IP·포트만 본다면, 이 정책은 GTP 시그널링 메시지를 이해해 어떤 메시지를, 어떤 출발지에서 오는 것을 허용할지 선택적으로 정합니다. 예를 들어 특정 SGSN에서 온 특정 GTP 메시지만 허용 하는 식의 세밀한 제어가 가능합니다.

여기에 **APN 기반 정책** 이 더해집니다 — Gn/S5 인터페이스에서 단말이 접속하려는 패킷망(APN)에 따라 정책을 다르게 적용합니다.

Intra-Tunnel Inspection과 가입자 트래픽

Intra-Tunnel Inspection(터널 내부 검사) 은 GTP 터널 안에 캡슐화된 실제 사용자 데이터까지 들여다보 는 것입니다. GTP 헤더만 보는 게 아니라 터널 속 트래픽에도 보안 정책을 적용 해, 터널을 악용한 공격을 막습니다.

Mobile Subscriber Traffic Security(가입자 트래픽 보호) 는 가입자(단말)가 주고받는 실제 트래픽을 보호 합니다 — 가입자를 노린 공격과 가입자발 공격 양쪽을 다룹니다.

구성

이 보호들은 SmartConsole에서 GTP-aware 정책과 관련 객체를 구성 해 적용합니다 (Configuring Security). 큰 줄기는 GTP 서비스·APN·게이트웨이 객체 정의 → GTP-aware 규칙 작성 → 터널 내부 검사·가입자 보호 설정 → 정책 설치 입니다. 방대한 구성 항목은 원문 해당 절을 참고하세요.

정리하면, Carrier Security는 ① GTP 프로토콜 오용·Overbilling 차단, ② GTP-aware 정책으로 메시지·출발지·APN 선택 허용, ③ Intra-Tunnel Inspection으로 터널 속 데이터 검사, ④ 가입자 트래픽 보호 의 네 겹으로 UMTS/LTE 망을 지킵니다.

05 GPRS 네트워크 보안 모니터링

GPRS 네트워크 보안 모니터링

GTP 망의 보안이 제대로 동작하는지 들여다보는 방법을 정리합니다. GTP 추적 로그, Monitor-Only 모드, SNMP 통계가 핵심입니다.

GTP Tracking 로그와 알림

Carrier Security는 GTP 트래픽을 추적해 로그·알림(alert)을 남 깁니다. 어떤 GTP 터널이 열리고 닫히는지, 어떤 메시지가 허용·거부되는지 를 기록해, 망의 보안 상태와 비정상 활동을 파악하게 합니다. 로그 메시지의 자세한 내용은 로그 메시지에서 다룹니다.

Monitor-Only Mode

Monitor-Only Mode 는 트래픽을 차단하지 않고 관찰·기록만 하는 모드입니다. GTP-aware 정책을 본격 적용하기 전에, 실제 망 트래픽이 정책에 어떻게 걸리는지 미리 관찰 해 오탐·과차단을 점검하는 데 유용합니다. 운영 망에 영향을 주지 않으면서 정책을 검증할 수 있습니다.

SNMP 통계

SNMP Extensions for GTP Statistics 로 GTP 통계를 SNMP로 외부 모니터링 시스템에 노출 할 수 있습니다. 활성 터널 수, 처리량, 거부된 메시지 같은 GTP 지표 를 SNMP로 수집해, 기존 NMS(Network Management System)에서 함께 모니터링합니다.

정리하면, GTP Tracking 로그로 무슨 일이 일어나는지 기록하고, Monitor-Only 모드로 정책을 안전하게 검증하며, SNMP로 GTP 지표를 외부 시스템에 노출 하는 것이 모니터링의 세 축입니다. 구성(Configuring Monitoring)의 세부는 원문 해당 절을 참고하세요.

06 로그 메시지

로그 메시지

모니터링에서 본 GTP 추적 로그가 어떤 메시지를 담는지 를 정리합니다.

Carrier Security 로그 메시지

Carrier Security는 GTP 트래픽에 대한 전용 로그 메시지 를 남깁니다. 이 로그는 어떤 GTP 이벤트가 일어났는지(터널 생성·삭제, 메시지 허용·거부, 프로토콜 위반 등) 와 그 맥락을 담아, 보안 분석과 문제 해결의 바탕이 됩니다. 로그는 다른 Check Point 로그와 마찬가지로 Logs & Events에서 봅니다.

각 로그 메시지는 무슨 일이 왜 일어났는지를 식별 하게 해 줍니다 — 예를 들어 어떤 GTP 메시지가 정책에 의해 거부됐다면, 그 이유(프로토콜 위반·정책 불일치 등)가 로그에 남습니다.

로그에 Information Element 추가

GTP 메시지는 여러 **Information Element(IE)** 로 이뤄집니다 — 터널 식별자(TEID), APN, 가입자 식별자(IMSI), 단말 IP 등 의 필드입니다. Carrier Security는 이런 IE를 로그에 추가 할 수 있어, 어느 가입자·어느 APN·어느 터널의 트래픽인지 까지 로그에서 식별하게 합니다.

이는 분석에 큰 도움이 됩니다 — 예를 들어 IMSI를 로그에 넣으면 특정 가입자의 GTP 활동을 추적 할 수 있습니다. 다만 로그에 IE를 많이 넣을수록 로그 크기·부하가 늘므로, 필요한 IE만 선택합니다.

정리하면, Carrier Security 로그는 GTP 이벤트를 기록하고, 필요한 Information Element(IMSI·APN·TEID 등)를 더해 가입자·터널 단위까지 추적 하게 합니다. 메시지 종류·IE 목록의 세부는 원문 해당 절을 참고하세요.

07 고급 구성

고급 구성

기본 보호를 넘어 대규모·로밍 환경에 맞춘 고급 설정 들을 정리합니다 — GRX 이중화, Information Element 제거, 용량 관리, SCTP입니다.

GRX Redundant Deployment

GRX(GPRS Roaming Exchange) 는 사업자 간 로밍 트래픽이 오가는 교환망 입니다. **GRX Redundant Deployment** 는 GRX 접점에 게이트웨이를 이중화해 배치 해, 한 게이트웨이가 죽어도 로밍 트래픽 보호가 끊기지 않게 합니다(ClusterXL 개념을 GRX 환경에 적용). 로밍은 다른 사업자망과 직접 맞닿는 만큼 가용성과 보안이 모두 중요합니다.

Stripping Information Elements

Stripping Information Elements 는 GTP 메시지에서 특정 Information Element(IE)를 제거 하는 기능입니다(로그 메시지에서 본 IE). 민감하거나 불필요한 정보(특정 식별자 등)를 다른 사업자망으로 내보내기 전에 제거 해, 정보 노출을 줄이고 상호운용성을 맞춥니다.

Capacity Management와 SCTP

Capacity Management(용량 관리) 는 GTP 터널·연결의 용량을 관리 해, 대규모 망에서 자원 고갈이나 과부하를 막습니다 — 동시 터널 수 등을 제어합니다.

SCTP(Stream Control Transmission Protocol) 는 Diameter 등 신호 프로토콜이 쓰는 전송 프로토콜 입니다(소개에서 본 Go 인터페이스의 SCTP·Diameter 인식). Carrier Security는 SCTP를 인식해 그 위에서 도는 시그널링을 검사 할 수 있어, LTE·IMS 환경의 제어 트래픽까지 보호합니다.

정리하면, 고급 구성은 GRX 이중화로 로밍 접점의 가용성·보안을 높이고, IE Stripping으로 정보 노출을 줄이며, 용량 관리·SCTP 인식으로 대규모·차세대 망을 지원 하는 손질들입니다. 세부 절차는 원문 해당 절을 참고하세요.