GTP通信網専用のセキュリティ監視ソリューション

SecureSoft Sniper® MIS (Mobile Infrastructure Security)

SecureSoft Sniper MISは3G/4G網のGTP区間の異常トラフィックや不正アクセスを利用した攻撃から効果的に防御するGTP通信網専用のセキュリティソリューションです。
GTPv1のControl/User Data Plane、GTPv2のControlをサポートし、PGW(GGSN)の保護を目的とします。

SecureSoft Sniper MISは、IPベースのセキュリティマシンだけでは検知・防御することができないモバイル網のセキュリティ脅威に対して、様々な角度から繊細な分析を行い、本当の攻撃を検知・防御する事ができる移動通信網専用の不正侵入検知･防御システムです。

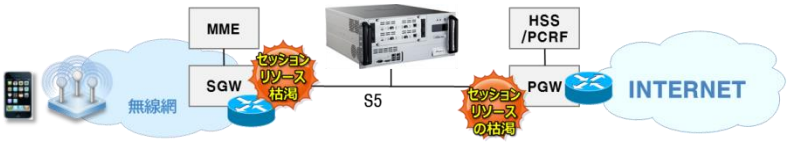
GTP区間で異常パケットが持つ特徴的なパターンを保有し、該当する接続を検知・遮断機能、管理者へ通知(アラート)機能ならびに記録(ログ)を保存します。

▼製品特徴

- ✓ GTPプロトコルDecode機能
- ✓ GTPプロトコルの脆弱性分析及び応用攻撃の検知
- ✓ GTPトンネルのセッション管理機能
- ✓ GTP関連の攻撃に対する端末情報の提供機能

制御装置(PGW/SWG)のセッション管理

●全体連結されたTEID数を基にPGWセッション数をモニタリングし、SGW IP別のTEID数を基にSGWセッション数をモニタリング



GTPプロトコルの有害性検知

正常または異常なGTPパケットの受信・応答パケットの解析

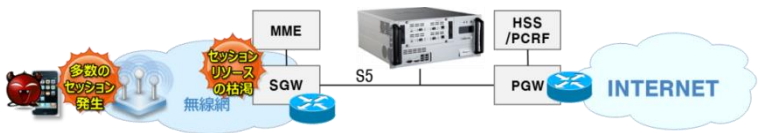
●メッセージフィールド値の操作(異常フィールド)
●Protocol Stackの操作
●GTPメッセージの操作(正常フィールド)

端末別のセッション管理

●UEサービス接続時にGTP-c区間に送られる認証情報を認知し、UE制御のためのテーブルを生成
●UE IP別にTEID数をモニタリングし、異常セッション発生のIP(UE)を確認
●DPI検査で有害性パケットの交換及びポリシー違反のTEIDを抽出
●異常発生端末のIP/TEID情報を利用し、UE区切り子のマッピング

有害トラフィックの管理

●G5区間のGTP-uヘッダだけではなく、インターネットパケットに対する有害性検証
●有線網で検証済みの安定した7段階のIPSエンジンに送られたパケットに対する有害性の検証

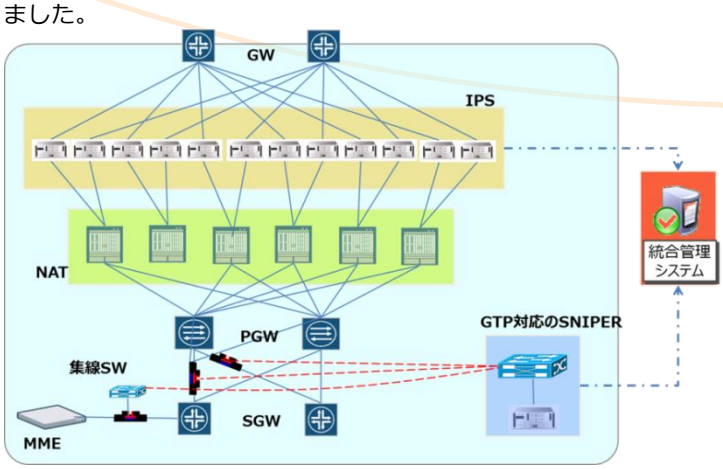


導入事例

SecureSoft Sniper MISを導入したISP社の事例は下図となります。Sniper MISを導入することで、GTPパケットをリアルタイムでモニタリングすることができるようになりました。

▼導入メリット

- ✓ モバイルリソースに対する管理
- ✓ 不正アクセスを試行する端末に対し、リアルタイム対応
- ✓ Heavyユーザに対するモニタリング
- ✓ アプリサービス毎にトラフィック使用率及び回線高度化のためのベースデータの確保
- ✓ ネットワークサービス安定性強化



MNO･MVNO事業者様向けセキュリティソリューション

securesoft 株式会社セキュアソフト
〒150-0011 東京都渋谷区東3-14-15 MOビル 2F
TEL:03-5464-9966 FAX:03-5464-9977
http://www.securesoft.co.jp sales@securesoft.co.jp