

Securing the global voice interconnect

How the international SIP and IMS roaming boundary is attacked, and why a signalling-aware SIP IDS closes the gap an SBC leaves.

By Jimmy Billaud, P1 Security.

Contents

1. Introduction: why all-IP interconnect changes the security picture	5
2. The evolving voice landscape: from circuit-switched to all-IP	6
3. Anatomy of an international SIP interconnect	8
4. How P1 Security tests: methodology and perspectives	10
5. Real-world SIP threats on roaming interfaces	11
5.1 Fraud and toll abuse	11
5.2 SIP tampering and identity spoofing	11
5.3 Interception and information disclosure	12
5.4 Denial of service	13
5.5 Other recognised interconnect attack classes	14
6. The role of a SIP intrusion detection system (SIP IDS)	14
7. Governing frameworks: standards and GSMA guidance	16
8. A multi-layered defence framework for the SIP interconnect	17
9. SIP interconnect security checklist for operators	19
10. Frequently asked questions	20
11. How P1 Security helps	21
12. References and further reading	22

Executive summary

Home-routed roaming (S8-HR in 4G, N9-HR in 5G) tunnels a roaming partner's traffic straight back into the subscriber's home core, which is why the SIP and IMS interconnect concentrates security risk at the IP border rather than at the radio edge.

The migration to all-IP voice rebuilt the international voice interconnect on SIP. Voice over LTE (VoLTE), Voice over WiFi (VoWiFi) and Voice over New Radio (VoNR) all run on the IP Multimedia Subsystem (IMS), and IMS speaks SIP. That change delivered richer services, but it also moved the trust boundary. In the 2G and 3G circuit-switched world, international roaming lived inside a relatively closed, operator-to-operator environment. In the IMS world, voice signalling now rides IP interconnect through the IP exchange (IPX) and the network-to-network interface (NNI). Home-routed roaming (S8 home routing in 4G, N9 home routing in 5G) tunnels a partner's traffic straight back into the subscriber's home core. The interconnect is trusted by design and, in practice, frequently under-protected.

This whitepaper draws on what P1 Security's team finds when it tests those interfaces, and it explains why a signalling-aware SIP intrusion detection system (IDS) has become a necessary complement to the session border controller (SBC) and the firewall. The findings are drawn from penetration testing on live international roaming interfaces (Gi/SGi, S8 home routing, N9 home routing) rather than from a standards review.

We group the recurring threats into four families:

1. Fraud and toll abuse
2. SIP tampering and identity spoofing
3. Interception and information disclosure
4. Denial of service against IMS nodes and subscribers

These threats share one property: they are reachable across roaming interfaces, and they often slip past perimeter controls because the controls that should stop them, IPsec on the NNI and policy on the SBC, are

misconfigured, exception-ridden, or simply absent. This happens on a link that everyone assumed was safe because a partner sits on the other end.

Prevention alone does not close this gap. The interconnect carries live subscriber traffic from hundreds of partners, and a static perimeter cannot reason about SIP behaviour. Detection is the control that closes the remaining gap. A SIP IDS positioned at the interconnect boundary, tapping traffic before and after the encryption boundary and performing deep, real-time protocol analysis, turns subtle header manipulation and quiet information leaks into signals a security team can see and act on. It complements the SBC rather than replacing it: the SBC handles known, high-volume threats such as floods, while the IDS provides the passive surveillance and protocol depth that catch the subtle and the novel.

Securing the SIP interconnect is a combination of foundational hardening (real IPsec, no null-encryption, strict segmentation, a genuine walled garden around core nodes) and continuous, protocol-aware detection at the border. Neither half is optional.

This paper is written for IMS and core network teams, roaming and interconnect teams, telecom SOC and fraud teams, network equipment vendors, and the regulators and operators who set and verify the security baseline.

Key takeaways

- Home-routed roaming (S8-HR in 4G, N9-HR in 5G) gives every voice-roaming partner a trusted SIP signalling path back into the home IMS core, concentrating risk at the IP interconnect rather than at the radio edge.
- The recurring field failure is unenforced standards, not missing ones: mandated IPsec on the NNI is bypassed, confidentiality is disabled via null-encryption, or core SIP ports are reachable directly without an IPsec tunnel.
- Interconnect threats cluster into four families: toll and data fraud, SIP tampering and caller-identity spoofing, interception and information disclosure (IMEI/IMEI-SV and P-Access-Network-Info cell-ID leakage), and denial of service from a single malformed SIP INVITE.
- A session border controller stops high-volume floods but cannot reason about subtle single-message attacks; a signalling-aware SIP IDS is the complementary control that catches the malformed-INVITE crash, the leaked identifier and the quiet null-encryption negotiation.
- A SIP IDS must observe traffic both before and after the encryption boundary (in the clear at or behind the A-SBC or P-CSCF) and should extend detection across Diameter, HTTP/2 and GTP, not stop at SIP.
- Closing the gap needs both tiers together: enforced IPsec with no null-encryption, an S-CSCF walled garden and an isolated HSS/UDR, layered with protocol-aware detection at the interconnect border.

1. Introduction: why all-IP interconnect changes the security picture

For most of mobile history, international voice was a circuit-switched affair carried between operators that knew each other and interconnected through a comparatively closed environment. Securing SIP was not a headline concern because SIP was not on the wire between networks. That world is gone. VoLTE, VoWiFi and VoNR are all IMS services, and IMS is built on SIP for session control and on Diameter or HTTP/2 for subscriber data and authentication. When a subscriber roams and makes or receives a call, the signalling that sets up that call now traverses IP interconnect, and increasingly it is routed back to the subscriber's home network.

That architectural choice, home routing, is deliberate and sensible. It keeps the home operator's policies, charging and lawful-interception obligations in force wherever the subscriber travels. But it has a security consequence that is easy to under-appreciate: it creates a direct, trusted tunnel from a foreign network into the home core, and it concentrates risk at the IP border. Every voice-roaming partner is, in effect, granted a signalling path toward sensitive home network functions. The security of that path depends entirely on how well the boundary is built and watched.

Standards anticipate this. The GSMA defines the NNI, mandates IPsec on it, and publishes guidance on VoLTE, IMS roaming and SIP network security. The problem P1 sees in the field is not a gap in the standards. It is the distance between the standard and the deployment. IPsec is mandated but sometimes bypassed. Confidentiality is expected but sometimes disabled for local reasons. Core nodes are supposed to be isolated but are sometimes reachable from the interconnect. This whitepaper deliberately moves past the architecture diagram and into what actually happens on live roaming interfaces, and into what operators can do to detect and close the gaps.

2. The evolving voice landscape: from circuit-switched to all-IP

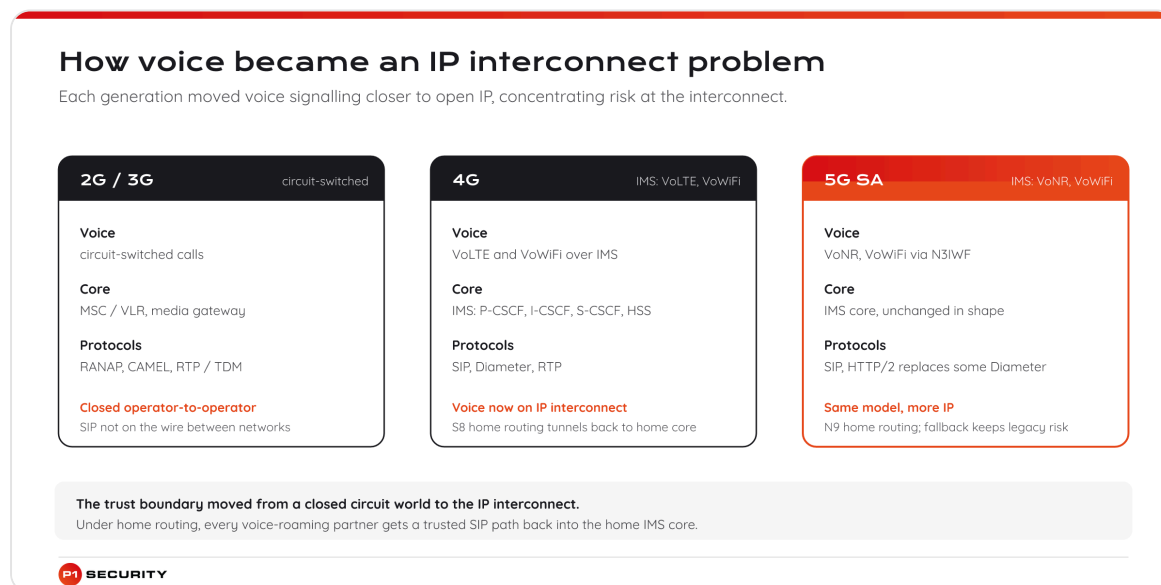


Figure 1. How voice became an IP interconnect problem

Understanding today's exposure requires a short look at how voice got here. Each generation retired some risks and introduced others.

2G and 3G: the circuit-switched walled garden. Foundational mobile voice was circuit-switched. Core nodes such as the mobile switching centre and visitor location register (MSC/VLR) handled the control plane, and the media gateway (MGW) handled the user plane. Control relied on protocols such as RANAP and CAMEL, with the media gateway controlled via H.248 (Megaco) and media carried over RTP or TDM using codecs such as AMR. International roaming worked through direct operator agreements: when a roaming subscriber was called, the visited MSC/VLR allocated a mobile station roaming number (MSRN) on request via the home HLR (home location register), so the call could be routed to the correct MSC/VLR in the visited network. The security model was a trusted, closed environment. That model was fundamentally changed once IP interconnect arrived.

4G and the rise of IMS. With 4G, operators chose between keeping legacy voice through circuit-switched fallback (CS-Fallback) or deploying a full IMS to deliver native all-IP voice. IMS enabled VoLTE and VoWiFi and shifted the control plane to IP: SIP for session management, Diameter for authentication, and media carried over RTP and RTCP with media handled by the media resource function (MRF). For international roaming, S8 home routing ensured that calls involving a roaming subscriber were routed back through the home network's packet gateway. This centralised control back at the home operator, and it created the trusted tunnel into the core described above.

5G standalone: same model, new options, lingering risks. 5G standalone continues the IMS-based voice model, adding VoNR over 5G radio and VoWiFi through the non-3GPP interworking function (N3IWF). The core voice architecture stays consistent with 4G IMS; the main change is that HTTP/2 replaces Diameter for some functions, such as subscriber-secret and charging-data exchange. Roaming evolves to N9 home routing, which serves the same purpose as its 4G predecessor. One point of clarification for the 5G reader: the service-based control-plane roaming path secured by the security edge protection proxy (SEPP) over the N32 interface is a separate concern from the IMS SIP voice interconnect this paper addresses, and the two should not be conflated.

One risk is worth calling out explicitly because it survives every generation: fallback. 5G networks can be configured for EPS-Fallback to 4G, and further fallback to circuit-switched 2G/3G remains possible in some deployments. A capable attacker operating a rogue base station and forcing registration failures can push a modern device to downgrade onto an older, better-understood network, and then exploit the legacy weaknesses of that network. All-IP does not erase legacy risk while legacy paths remain reachable.

The net effect of this evolution is that risk has concentrated on the IP-based components and interfaces that now form the global interconnect. That makes an anatomical view of the interconnect the right starting point for defence.

3. Anatomy of an international SIP interconnect

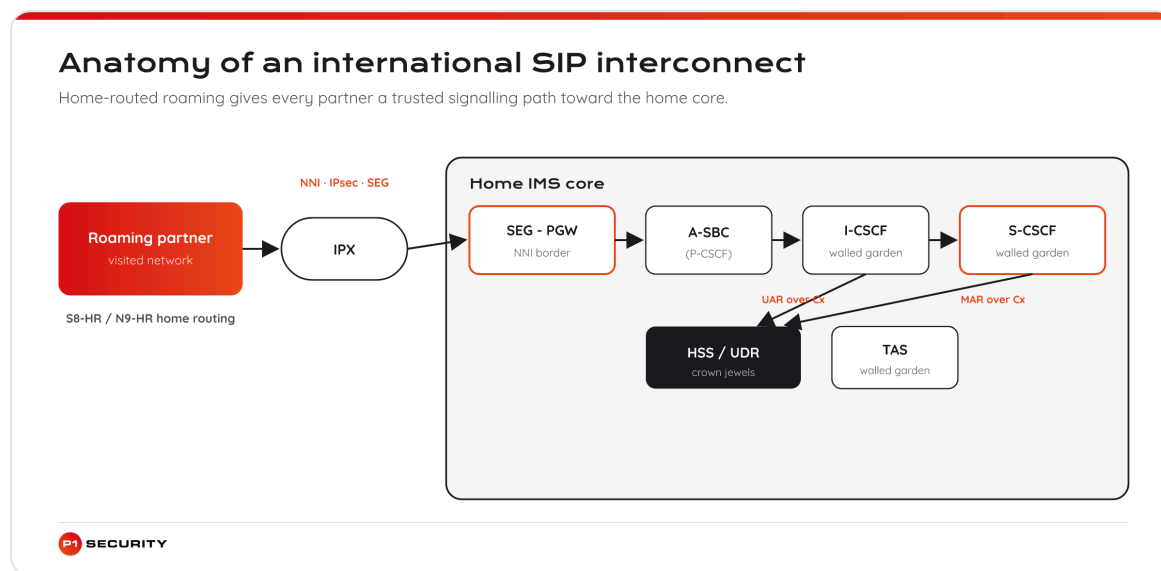


Figure 2. The IMS core and the roaming interconnect that reaches it, from partner to home core

An international SIP interconnect is the IP-based path, running over the IPX and the network-to-network interface (NNI), that carries VoLTE, VoWiFi and VoNR signalling and media between roaming partners and, under home routing, back into a subscriber's home IMS core. To secure the interconnect you first have to deconstruct it. The IMS core and its roaming connections form an ecosystem of nodes and interfaces, each with a function and an exposure profile.

The IMS core itself is built from a handful of key functions:

- **P-CSCF (proxy call session control function).** The main entry point for subscribers and the first node to handle session signalling. As the front door, it is the first line of defence against malformed signalling and a prime denial-of-service target.
- **I-CSCF (interrogating CSCF).** A directory-style function that queries the subscriber database to locate the correct serving CSCF. Its position in the call flow makes it a critical link: compromise it and sessions can be redirected or blocked.
- **S-CSCF (serving CSCF).** The session brain. It maintains state, enforces policy and controls services. Keeping it inside a strict walled garden, reachable only through controlled call flows, is essential to network stability.

- **HSS/UDR (home subscriber server / unified data repository).** The central store of subscriber profiles, permissions and authentication material. This is the crown jewel, and its isolation from external interfaces is non-negotiable.
- **TAS (telephony application server).** Service logic for value-added voice features such as voicemail and conferencing. A misconfigured or vulnerable application server can be abused to bypass policy or to attack subscribers.
- **BG (border or breakout gateway).** The node that interconnects the operator with partner networks and IPX hubs. It is the trusted edge, and a misconfiguration here can open a direct, unmonitored path into the core.

International roaming stitches these functions together across operator boundaries through specific interfaces and interconnect designs:

- **The network-to-network interface (NNI).** The logical connection that carries both the control plane (SIP) and the user plane (RTP) between roaming partners. Standards mandate IPsec on the NNI, terminated by a security gateway (SEG) at each end. In home-routed roaming the SEG sits with the home packet gateway (PGW) that anchors the roaming subscriber's traffic, shown together as SEG-PGW in the figures, and it is the border where the roaming tunnel terminates and where network isolation must be enforced before signalling reaches the P-CSCF and A-SBC. P1's field experience is that misconfigurations and policy exceptions on the NNI are common, which leaves this critical interface exposed more often than operators expect.
- **S8 home routing (4G) and N9 home routing (5G).** Both designs compel voice signalling and media involving a roaming subscriber to be tunnelled back to and routed through the home network. This applies home-operator policy consistently, and it also creates the direct, trusted tunnel from a foreign network into the home core.
- **Gi/SGi and the IPX.** The IP data and interconnect points through which roaming voice traffic transits between the visited network, the IPX and the home network. These are the links where interconnect traffic is visible and, therefore, where it can be monitored.

The recurring theme across the anatomy is trust that is asserted but not verified. The NNI is trusted to be encrypted. The border gateway is trusted to filter. Core nodes are trusted to be isolated. The attacks in the next sections are, almost without exception, the result of one of those trust assumptions being false on a live link.

4. How P1 Security tests: methodology and perspectives

The findings in this paper come from hands-on penetration testing on live international roaming interfaces, not from a documentation review. A few points about method explain why the findings look the way they do.

Telecom penetration testing is not IT penetration testing. The protocols (SIP, Diameter, GTP, RTP), the interfaces (NNI, S8, N9, Gi/SGi, the IMS reference points), the equipment and the failure modes are specific to mobile networks. Generic IT and web scanners do not understand SIP call flows, IMS-AKA (IMS Authentication and Key Agreement) authentication, IPsec-on-the-NNI expectations, or the way IMS nodes trust one another, so they miss most of what matters here.

We test the interconnect the way an attacker reaches it, from the position of a roaming partner or an IPX-connected entity that has legitimate signalling reachability toward the home network. That perspective is the whole point: the interconnect grants a trusted path, and the question is what a malicious or compromised partner can do with it.

We reproduce realism in the lab. Part of the work is building labs that simulate real telecom contexts, so that attacks and their effects can be studied safely and demonstrated conceptually without touching production or subscribers. Proof-of-concept work stays in that controlled environment; nothing in this paper is a reproduction recipe.

We follow the chain, not just the single finding. The most instructive results are rarely one flashy exploit. They are the sequence: a mandated IPsec tunnel that turns out to be bypassable, then a core SIP port reachable directly, then a malformed message that a node fails to handle safely. Where the boundary is weak, that chain is short.

The rest of the paper is organised around what those chains repeatedly reveal.

5. Real-world SIP threats on roaming interfaces

SIP threats on roaming interfaces fall into four families: fraud and toll abuse, SIP tampering and identity spoofing, interception and information disclosure, and denial of service, plus a set of further classes worth testing. The attacks below were observed by P1's penetration testing teams on live international roaming interfaces (Gi/SGi, S8 home routing, N9 home routing) and are echoed in P1's telecom Vulnerability Knowledge Base.

5.1 Fraud and toll abuse

Fraud on the SIP interconnect exploits weaknesses in traffic policy and charging logic rather than breaking cryptography. Representative patterns:

- **Free data.** An adversary exploits incorrect traffic policies, or abuses the fact that VoLTE signalling traffic is often not billed, or abuses a VoLTE dedicated bearer, to obtain free and high-priority access to the internet or to another mobile station.
- **Overbilling.** An adversary injects unwanted traffic (for example spam over the signalling bearer) to impose an excessive data bill on a victim subscriber, exploiting incorrect traffic policies and a lack of routing and forwarding control on the IMS signalling bearer.
- **Pre-emptive data priority.** An adversary's device obtains undeserved higher-priority data access, exploiting incorrect traffic policies, a lack of rate limiting on the signalling bearer, and the absence of restrictions on simultaneous calls.

The business impact is financial and reputational: revenue leakage, disputed bills, and customer churn. None of these require exotic tooling, which is precisely why they persist.

5.2 SIP tampering and identity spoofing

Because SIP is a text-based signalling protocol, an attacker with a signalling path can manipulate messages that a poorly protected interconnect will accept and act on:

- **Caller identity spoofing (impersonation).** Where the interconnect lacks IPsec for SIP signalling and lacks IMS-AKA authentication, an adversary can send SIP messages with a spoofed calling identity. This is hard to detect and hard to prevent after the fact, and it erodes trust in caller identity. The STIR/SHAKEN framework (RFC 8225 defines the PASSporT token and RFC 8224 the SIP Identity header that carries it) exists to authenticate caller identity, but it is a caller-ID authentication mechanism deployed within and between participating networks,

not a roaming-interconnect silver bullet, and coverage across international voice-roaming partners is uneven.

- **Silent calls and battery drain.** An adversary can place silent calls toward a target device, forcing it into a high-power radio state (RRC) without the user's awareness, exploiting weaknesses in the VoLTE signalling used for call establishment toward the terminating subscriber. The subscriber experiences degraded battery life and, potentially, churn, without ever seeing an incoming call.

5.3 Interception and information disclosure

This family is the most sensitive, because it touches confidentiality and subscriber privacy.

- **Null-encryption and eavesdropping.** This abuses IPsec configuration on the interconnect. An attacker forces the connection to use integrity protection while disabling confidentiality through a null-encryption cipher. With confidentiality off, both control-plane traffic (who is calling whom) and user-plane media (the call itself) can be observed. This is sometimes a deliberate policy choice driven by lawful-interception requirements, which puts operators in a genuine tension between regulatory compliance and subscriber privacy. Where regulations permit, null-encryption should be prohibited.
- **IPsec tunnel bypass via direct port access.** A fundamental edge-security failure in which a roaming partner reaches a core SIP port directly (for example over TCP) without first establishing the mandatory IPsec tunnel that is supposed to protect the NNI. When this is possible, the foundational border control has failed, and an external entity can interact directly with internal services.
- **Subscriber IMEI disclosure.** A SIP response, such as a session-progress message, can unnecessarily carry the called party's international mobile equipment identity (IMEI) or its software-version variant (IMEI-SV). An attacker who initiates a call can harvest this. On its own it looks minor, but device model and firmware version are the first step of a targeting kill chain: with them, an attacker can research known device vulnerabilities and aim a specific exploit at a specific handset.
- **Subscriber location tracking.** A severe privacy breach that occurs when the cell identifier carried in the `P-Access-Network-Info` header is disclosed from the core to a roaming context. That identifier reveals the specific cell a subscriber is attached to, which allows physical-location tracking with meaningful precision. The attack is silent and hard for the victim to detect.

5.4 Denial of service

DoS on the SIP interconnect is frequently a robustness problem, not a volume problem. A single malformed message can be more effective than a flood.

- **Node crash via malformed SIP INVITE.** By adding unexpected characters to a sub-header that defines a call's destination, an attacker can trigger a flawed implementation in the handling node. The malformed message crashes the node, denying service to every subscriber that node was processing. This is exactly the class of subtle, single-message attack that a volume-oriented control will not catch.
- **Service halt through malformed input or misconfiguration.** More broadly, improper input validation, node misconfiguration and missing hardening let an attacker cause service unavailability with crafted messages or by abusing weak network configuration.
- **Data DoS and muted voice against a subscriber.** An attacker can shut down a victim's ongoing data access by abusing incorrect traffic policies and a lack of rate limiting on the bearer, or mute an ongoing VoLTE call where there is no data-rate control for RTP when the signalling bearer is also used to deliver voice.

In a telecom context these are not merely application crashes. Depending on the node hit, the effect ranges from a single dropped call to loss of service for every subscriber behind a crashed element, with the corresponding financial and reputational cost.

What to verify (attack portfolio)

- Is IPsec genuinely enforced on every NNI/roaming link, with confidentiality enabled, and are exceptions documented and justified rather than quietly tolerated?
- Can any core SIP port be reached from an interconnect partner without an established IPsec tunnel?
- Are IMS nodes robust against malformed SIP messages, validated against recognised torture-test suites?
- Do outbound SIP responses leak sensitive identifiers (IMEI, IMEI-SV, cell identity) toward roaming contexts?
- Are traffic policies, charging rules and rate limits on the signalling and data bearers tested against abuse, not just against normal use?

5.5 Other recognised interconnect attack classes

These are further attack classes recognised in SIP and IMS security practice and worth testing at the interconnect. They were not the primary focus of this assessment, but they belong in any thorough interconnect test plan:

- **SIP enumeration.** Differential responses to registration or probing requests can reveal which subscriber identities or endpoints are valid, giving an attacker a target list.
- **Registration abuse.** Manipulation of registration bindings can be used to hijack or disrupt where a subscriber's sessions are delivered, where registration handling on the interconnect is insufficiently authenticated.
- **ISUP-in-SIP injection (SIP-I / SIP-T).** For interworking with circuit-switched networks, ISUP signalling is encapsulated inside SIP bodies (SIP-I and SIP-T). Where the encapsulated content is not validated, an attacker may manipulate or inject ISUP parameters to influence call handling across the PSTN boundary.

6. The role of a SIP intrusion detection system (SIP IDS)

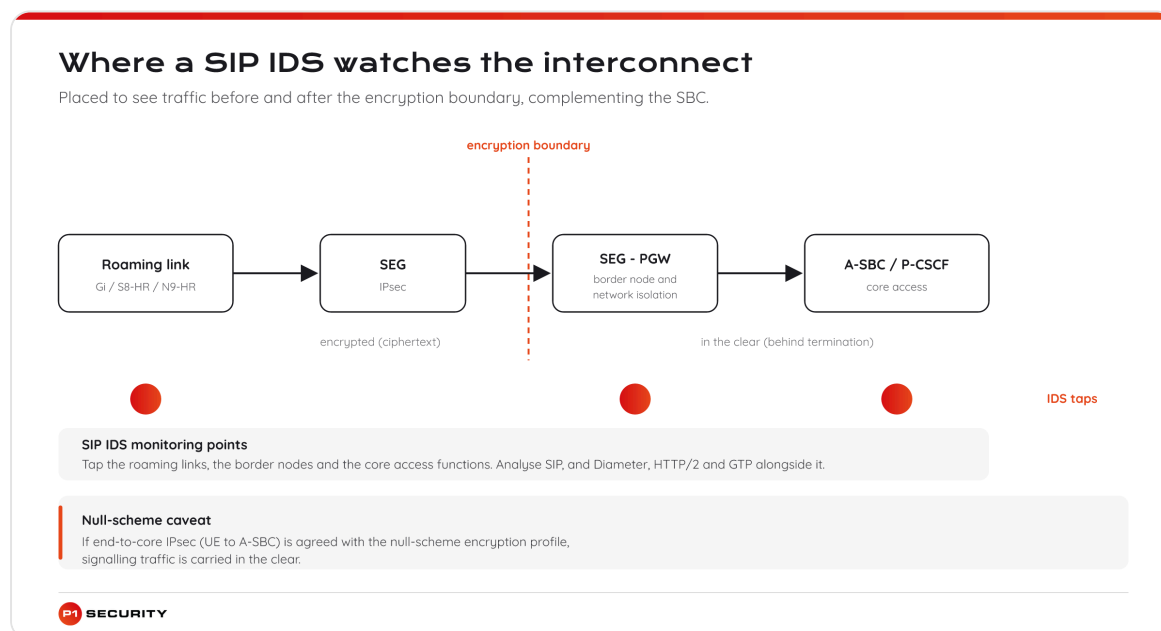


Figure 3. Signalling-aware SIP IDS placement: tap points before and after the encryption boundary

A SIP intrusion detection system (IDS) is a signalling-aware sensor that performs deep, real-time analysis of SIP and the protocols around it (Diameter, HTTP/2, GTP) at the interconnect boundary, to detect fraud, identity spoofing, information leakage and malformed-message attacks that volume-based controls miss. Foundational

hardening reduces the attack surface, but it cannot reason about live signalling behaviour across hundreds of partners. That is the job of detection, and at the interconnect the right detector is a signalling-aware SIP IDS.

Why signalling-aware detection matters. Many of the attacks above are subtle by design. A malformed INVITE sub-header, an IMEI that should not be in a response, a cell identity leaking outward, a null-encryption negotiation: none of these are high-volume events, and none look like an attack to a control that watches only rates and volumes. Detecting them requires deep, real-time analysis of the SIP protocol itself, and of the related protocols around it. Preventing signalling access and fraud outright is genuinely hard on an interconnect that must remain open to legitimate partners, which is why detection, not just prevention, is the pragmatic centre of gravity.

How an IDS complements the SBC and firewall. An IDS is a complementary service to existing security nodes, not a replacement for them. An SBC is effective at handling known, high-volume threats such as signalling floods, and it should keep doing that. An IDS adds passive surveillance and deep protocol visibility to catch the subtle and the novel: it is the protocol analysis of the IDS, not the flood control of the SBC, that detects the malformed-INVITE node crash or the unexpected IMEI disclosure. A firewall enforces reachability; the IDS explains behaviour.

Where to place a SIP IDS. Placement determines what the IDS can see, and the interconnect has natural monitoring points:

- **Roaming links.** Traffic mirroring or tapping on the Gi/SGi, S8 and N9 links, on top of a roaming signalling firewall, gives visibility into all traffic entering the home network from roaming partners.
- **Border nodes.** Positioning the IDS as a watchdog over the SEG-PGW border, where the roaming tunnel terminates and network isolation is enforced, provides the earliest possible detection of malicious activity.
- **Core access functions.** Monitoring the access-facing (ingress) side of key SIP access functions such as the A-SBC and the P-CSCF gives insight into traffic after it has passed initial perimeter controls.

One placement detail matters more than any other: the IDS should be able to observe traffic both before and after the encryption boundary. Signalling on the NNI is (or should be) inside IPsec, so a tap placed only outside the SEG sees ciphertext. To analyse SIP behaviour, the IDS needs a vantage point where the traffic is in the clear, which in practice means at or behind the A-SBC or P-CSCF termination point, while still correlating with what arrives at the border. This is also why null-encryption is so damaging: it changes what every downstream control, including the IDS itself, can assume about confidentiality.

Measuring effectiveness. IDS value is measurable, not a matter of faith. Meaningful key performance indicators include the number of detected DoS attempts, identified fraud schemes, and observed null-encryption control-plane flows, all assessed against a realistic false-positive rate to gauge sensitivity and relevance. Detection throughput measured against these counters lets a team demonstrate that the IDS is doing useful work and tune it over time.

Beyond SIP. The interconnect does not carry SIP alone. An IDS positioned here can and should extend its analysis to the related protocols that share the roaming boundary: Diameter and, in 5G, HTTP/2 for subscriber data and authentication, and GTP for the user plane. Continuous monitoring of key IMS reference points (for example Mw and Mb for SIP and RTP, and Rx and Cx for Diameter) lets an IDS catch not only SIP attacks but also anomalies in the underlying protocols, such as brute-force behaviour visible as anomalous responses on the Cx interface.

What to verify (detection)

- Is there a SIP IDS on the roaming interconnect at all, or is the SBC being asked to do a job it was not designed for?
- Can the IDS observe SIP in the clear (behind the encryption termination) as well as correlate with the encrypted border?
- Are the monitoring points (roaming links, the SEG-PGW border, A-SBC/P-CSCF) actually tapped, or only nominally in scope?
- Are IDS KPIs defined, baselined and reviewed, including false-positive rate?
- Does detection extend across SIP, Diameter/HTTP/2 and GTP, or stop at SIP?

7. Governing frameworks: standards and GSMA guidance

The defence measures in this paper are not arbitrary. They align with published specifications and operator guidance, and adherence supports both a higher security baseline and interoperability between partners.

3GPP and IETF (core technical specifications):

- **3GPP TS 33.203**, access security for IP-based services, the core reference for IMS access security and IMS-AKA authentication.

- **3GPP TS 33.210**, network domain security (NDS/IP), the standard basis for the mandated IPsec and security gateways on inter-operator interfaces (the Za and Zb reference points).
- **3GPP TS 33.102**, 3G security architecture.
- **3GPP TR 33.830**, feasibility study on IMS firewall traversal.
- **3GPP TS 33.328**, IMS media plane security, the key reference for protecting IMS media.
- **IETF RFC 4475**, SIP torture test messages, an essential resource for validating SIP implementations against malformed input and for preventing the node-crash attacks described above.
- Supporting IETF references from the source set: **RFC 6404** (SPEERMINT security threats and countermeasures), **RFC 6271** (requirements for SIP-based session peering), **RFC 3702** (AAA requirements for SIP), **RFC 5764** (DTLS extension for SRTP keying), **RFC 5630** (the SIPS URI scheme), **RFC 5393** (amplification via SIP forking proxies), **RFC 4474** (authenticated identity management in SIP, since superseded by RFC 8224 for STIR) and **RFC 7651** (3GPP IMS option for IKEv2).

GSMA (operational best practice):

- **GSMA FS.21**, interconnect signalling security recommendations. Identifies key interconnect security risks and suggested operator responses.
- **GSMA FS.22**, VoLTE security analysis and recommendations. Provides detailed vulnerabilities and test-case scenarios.
- **GSMA FS.38**, SIP network security. Describes techniques and tools for producing tortured test cases against SIP networks, aligning directly with proactive testing.
- **GSMA IR.92**, IMS profile for voice and SMS, the commonly cited VoLTE profile.
- **GSMA IR.65**, IMS roaming, interconnection and interworking guidelines.
- **GSMA NG.113**, 5GS roaming guidelines.

8. A multi-layered defence framework for the SIP interconnect

Effective security at the interconnect is defence in depth: proactive hardening and strict isolation, plus real-time, protocol-aware detection. The measures below are organised into three tiers and map directly to the threats in section 5.

Tier 1: confidentiality and integrity on the interconnect

- **Mandate comprehensive IPsec on the NNI.** Every NNI and roaming link should be encapsulated in IPsec, using a full security association and IMS-AKA authentication, terminated by a security gateway at each end. Treat IPsec as mandatory, not aspirational, and eliminate direct-port paths that bypass the tunnel.
- **Prohibit null-encryption.** Where national regulation permits, disallow null-encryption ciphers so that both integrity and confidentiality are maintained. Where lawful-interception requirements force a trade-off, document it and compensate for it with detection.
- **Add end-to-end encryption.** Enable SIPS (SIP over TLS) for the control plane and SRTP for the media plane as an additional layer, with consistent termination points, including for VoWiFi through the evolved packet data gateway (ePDG) or N3IWF toward the PGW or UPF.

Tier 2: segmentation and isolation

- **Isolate core nodes from roaming exposure.** Core control-plane interfaces to nodes such as the HSS/UDR, PGW/UPF and PCF/PCRF, carrying Diameter, HTTP/2 and charging records, must be kept isolated from roaming and external exposure.
- **Keep the S-CSCF in a walled garden.** Central session functions such as the S-CSCF should be reachable only through controlled, predefined call flows. Failure to enforce this means a compromise on a single externally facing node can cascade into the core, including subscriber data and billing.
- **Harden the border and validate input.** Enforce hardening and strict input validation on border and access nodes so that a malformed message does not become a service outage, and so that outbound responses do not leak sensitive identifiers toward roaming contexts.

Tier 3: detection and continuous vigilance

- **Deploy a SIP IDS at the interconnect boundary.** Place it to observe roaming links, the SEG-PGW border and core access functions (A-SBC/P-CSCF), with visibility both before and after the encryption boundary, as described in section 6.
- **Analyse across protocols.** Extend detection across SIP, Diameter or HTTP/2, and GTP, covering the relevant reference points (for example Mw, Mb, Rx and Cx), so context-specific threats are not missed.
- **Measure and tune.** Track DoS, fraud and null-encryption KPIs against a realistic false-positive rate, and review them so detection improves over time.

The logic is cumulative: real IPsec and strict isolation remove the easy paths, hardening turns malformed input into a handled error rather than an outage, and a protocol-aware IDS makes the remaining subtle activity visible and actionable. A perimeter-only or SBC-only posture is no longer sufficient for the interconnect.

9. SIP interconnect security checklist for operators

A condensed, practical checklist drawn from the sections above.

- ☐ IPsec enforced on every NNI/roaming link, with confidentiality enabled and full security association plus IMS-AKA authentication; no undocumented exceptions.
- ☐ No direct access to core SIP ports from any interconnect partner without an established IPsec tunnel.
- ☐ Null-encryption prohibited wherever national regulation permits; any mandated exception documented and compensated with detection.
- ☐ SIPS and SRTP enabled as an end-to-end layer, with consistent termination points including VoWiFi paths.
- ☐ Core nodes (HSS/UDR, PGW/UPF, PCF/PCRF) and their Diameter, HTTP/2 and charging interfaces isolated from roaming and external exposure.
- ☐ S-CSCF kept in a walled garden, reachable only through controlled call flows.
- ☐ IMS nodes hardened and validated against malformed SIP input using recognised torture-test suites.
- ☐ Outbound SIP responses checked for sensitive-identifier leakage (IMEI, IMEI-SV, cell identity via `P-Access-Network-Info`).
- ☐ Traffic policies, charging rules and rate limits on signalling and data bearers tested against fraud and abuse.
- ☐ SIP IDS deployed at roaming links, the SEG-PGW border and core access functions (A-SBC/P-CSCF), with visibility before and after encryption.
- ☐ Detection extended across SIP, Diameter/HTTP/2 and GTP, covering the relevant reference points.
- ☐ IDS KPIs (DoS, fraud, null-encryption flows) defined, baselined and reviewed against false-positive rate.
- ☐ Fallback/downgrade risk assessed (EPS-Fallback and CS-Fallback), given that legacy paths reintroduce legacy exposure.

- ☐ Regular, telecom-specific penetration testing of the roaming interconnect from a partner perspective.

10. Frequently asked questions

Why is the international SIP interconnect a security risk?

VoLTE, VoWiFi and VoNR run on IMS over SIP, and home-routed roaming (S8-HR, N9-HR) tunnels partner traffic back into the home core. Every voice-roaming partner gets a trusted signalling path toward sensitive home network functions, often protected by IPsec and SBC policy that is misconfigured or absent.

What is a SIP IDS and why is it needed?

A SIP intrusion detection system is a signalling-aware detector that performs deep, real-time analysis of SIP, and the related Diameter, HTTP/2 and GTP, at the interconnect boundary. It catches subtle header manipulation, information leaks and malformed-message crashes that a volume-oriented SBC or firewall misses.

Does a SIP IDS replace the SBC?

No. The SBC handles known, high-volume threats such as floods. The SIP IDS adds passive, protocol-deep surveillance for the subtle and novel, placed to see traffic before and after the encryption boundary. They are complementary.

What attacks target IMS and SIP roaming interfaces?

Fraud and toll abuse, SIP tampering and caller-ID spoofing, interception and information disclosure (null-encryption, IMEI and cell-identity leakage, IPsec bypass via direct port access), and denial of service from malformed SIP messages.

What is null-encryption on the interconnect?

A configuration where the NNI IPsec association keeps integrity protection but disables confidentiality with a null cipher, exposing both the control plane and the media. Where regulation permits, it should be prohibited.

What is S8 home routing (S8-HR)?

S8 home routing is the 4G roaming design that compels voice signalling and media involving a roaming subscriber to be tunnelled back to and routed through the home network. This keeps the home operator's policies, charging and lawful-interception obligations in force wherever the subscriber travels, and it also creates a direct, trusted tunnel from a foreign network into the home core. N9 home routing (N9-HR) serves the same purpose in 5G.

How is the N32/SEPP roaming path different from the SIP voice interconnect?

They are separate concerns and should not be conflated. The service-based control-plane roaming path is secured by the security edge protection proxy (SEPP) over the N32 interface, whereas this paper addresses the IMS SIP voice interconnect that carries VoLTE, VoWiFi and VoNR signalling and media between roaming partners.

11. How P1 Security helps

P1 Security is a specialist mobile network and telecom security company. We help operators, governments, regulators and network equipment vendors find, detect and understand vulnerabilities across telecom signalling and core and RAN infrastructure, using protocol-aware methods that generic IT security cannot provide.

The findings and recommendations in this paper come directly from our offensive and detection work. The services and products that map to them:

- **PTM (P1 Telecom Monitor).** P1's real-time telecom intrusion detection system for signalling and core networks, detecting attacks and fraud across signalling protocols such as SS7, Diameter and GTP. Extending protocol-aware, signalling-layer detection to the SIP and IMS interconnect is exactly the role this paper describes for a SIP IDS, so the fraud, tampering, information disclosure and DoS described here become signals a team can see and act on. Talk to us about detection coverage for your SIP and IMS interfaces.
- **Audit, vulnerability assessment and red team.** Telecom-specific penetration testing and architecture review of the IMS core, the roaming interconnect and the NNI, tested from the partner perspective, to find the misconfigurations (bypassable IPsec, null-encryption, reachable core nodes, malformed-input crashes, identifier leakage) before an adversary does.
- **PTA (P1 Telecom Auditor).** Attack-surface management and telecom-protocol-aware vulnerability scanning and compliance checks across the telecom estate, so interconnect exposure is identified with remediation guidance rather than assumed away.
- **VKB (Vulnerability Knowledge Base).** The largest telecom vulnerability intelligence database, with a continuous feed from our research team, so teams understand which SIP, IMS and roaming vulnerabilities affect their network, why they matter and where risk concentrates.
- **MSSP and TSOC.** For operators without an in-house telecom security operations centre, P1 runs a managed telecom security service and a Telecom Security Operations Centre (TSOC) that converges PTM detection with VKB intelligence, so

the interconnect fraud, spoofing, information disclosure and DoS described here are monitored and triaged continuously rather than only during an engagement.

- **Training.** P1's online training and hands-on Laboratory Playground take security, roaming, IMS and SOC teams from telecom fundamentals to advanced telecom security, including hands-on trace analysis, with expert-led video, lab simulations and certification, so your own team can find and reason about issues like these.

If you want to benchmark or test your own SIP interconnect against the threats in this paper, contact us at contact@p1sec.com.

12. References and further reading

Standards and industry guidance:

- **3GPP TS 33.203:** access security for IP-based services (IMS access security, IMS-AKA).
- **3GPP TS 33.210:** network domain security (NDS/IP), the basis for inter-operator IPsec and security gateways (Za/Zb).
- **3GPP TS 33.102:** 3G security architecture.
- **3GPP TR 33.830:** feasibility study on IMS firewall traversal.
- **3GPP TS 33.328:** IMS media plane security.
- **IETF RFC 4475:** SIP torture test messages: <https://www.rfc-editor.org/rfc/rfc4475>
- **IETF RFC 8224 and RFC 8225:** authenticated identity management in SIP and the PASSporT token, the basis of STIR/SHAKEN: <https://www.rfc-editor.org/rfc/rfc8224>
- **IETF RFC 6404, RFC 6271, RFC 3702, RFC 5764, RFC 5630, RFC 5393, RFC 4474, RFC 7651:** supporting SIP peering, AAA, SRTP keying, SIPS URI, forking-proxy amplification, identity and IKEv2 references.
- **GSMA FS.21:** interconnect signalling security recommendations.
- **GSMA FS.22:** VoLTE security analysis and recommendations.
- **GSMA FS.38:** SIP network security. See the GSMA public explainers on why SIP security needs to change: <https://www.gsma.com/get-involved/working-groups/fraud-and-security-group/why-thinking-around-sip-security-needs-to-change-and-how-gsmas-new-fs-38-prd-will-help/> and <https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2021/07/SIP-Security-Why-Should-It-Matter.pdf>
- **GSMA IR.92:** IMS profile for voice and SMS (VoLTE profile).
- **GSMA IR.65:** IMS roaming, interconnection and interworking guidelines.

- **GSMA NG.113:** 5G roaming guidelines.

P1 Security resources:

- SecurityHub TelcoSec glossary entries for SIP, IMS, P-CSCF, I-CSCF, S-CSCF, HSS/UDR, SBC, SEG, NNI, IPX, VoLTE, VoWiFi, VoNR, S8 home routing and N9 home routing.
- Related P1 blog posts: [international IP-based SIP security risks and the SIP IDS role](#); [IMS and SIP vulnerabilities in prepaid and postpaid systems](#); [understanding VoLTE](#); [5G interconnect security, GSMA FS.36](#).

About P1 Security

P1 Security is a France-based specialist in mobile network and telecom security. It works with mobile operators, governments, regulators and network equipment vendors worldwide, and has been securing operators' and nation-states' critical mobile infrastructure since 2011. Coverage spans SS7, SIGTRAN, Diameter, GTP, SIP, IMS, VoLTE, LTE, 5G Core and SBA, RAN, O-RAN, Cloud RAN, NFVI, roaming and private 5G.

The work is built around three pillars: PTA to identify exposure, PTM to detect signalling attacks in real time, and VKB to understand which vulnerabilities matter. P1 Security is ISO/IEC 27001:2022 certified and a GSMA member.

Explore the P1 Security ecosystem

- [p1sec.com](#): products (PTA, PTM, VKB), services, industries, blog, webinars and advisories.
- [SecurityHub](#): telecom security reference and education, home of the TelcoSec glossary.
- [TelcoSec Arsenal](#): curated tools for telecom security practitioners.
- [TelcoASM](#): confidential telecom attack-surface self-assessment and benchmarking.
- [ApexThreats](#): telecom threat intelligence built from signalling data.
- [CVE and security advisories](#): P1 published CVEs and coordinated disclosures.
- [Online training](#): video theory, hands-on labs and certification.

Talk to us

Ready to look at your own exposure? Write to us at contact@p1sec.com, or benchmark your network with [TelcoASM](#).

Follow P1 Security

- LinkedIn: [linkedin.com/company/p1security](https://www.linkedin.com/company/p1security)
- Mastodon: [@p1sec on Infosec Exchange](#)
- X: [@p1security](#)

Legal and copyright

© 2026 P1 Security S.A.S. All rights reserved. PTA, PTM and VKB are products of P1 Security.

This document is provided for information and research purposes in good faith, with no warranty of any kind. All findings are anonymised and no client or vendor is named without their consent. Where any CVE or vulnerability is referenced, P1 Security follows a responsible disclosure process with a 180-day vendor window; see cve.p1sec.com.

P1 Security S.A.S., Paris, France.