



Acme Packet Net-SAFE – a comprehensive security framework for enterprise IP communications

Whitepaper

Executive summary

Enterprises are deploying IP telephony and UC solutions to increase productivity, improve collaboration and reduce expenses. Traditional corporate voice security methods and practices designed to safeguard private circuit-switched telephony networks aren't adequate for interactive IP communications. Conventional IP security products weren't conceived with interactive IP communications in mind, and leave the enterprise vulnerable to a variety of security threats. Enterprises must adopt new methods to safeguard IT assets and confidential information, mitigate financial loss and legal exposure, protect against system overloads and maintain the high service levels users have come to expect from the corporate phone system and the public telephone network.

The Acme Packet Net-SAFE™ security framework is specifically designed to address the unique security challenges businesses encounter when delivering interactive IP communications over private IP networks, the Internet and new SIP-based services. The Net-SAFE framework includes advanced security features, a highly-scalable product architecture, a back-to-back user agent approach, and comprehensive monitoring and reporting capabilities to help enterprises reduce risk in IP telephony and UC infrastructure, services and applications, and ensure the confidentiality, integrity and availability of interactive IP communications.

Interactive IP communications security implications

Businesses are implementing SIP-based voice and unified communications (UC) platforms to improve collaboration, boost worker productivity and enhance business agility. By replacing legacy TDM voice networks with end-to-end IP networks and converging voice, video and data onto a common IP infrastructure, enterprises can reduce CAPEX and OPEX, weave interactive communications into applications and business processes, and leverage the Internet and new SIP-based services to extend enterprise communications to teleworkers, small offices, mobile professionals and business partners.

To be successful, businesses must implement new security methods and practices when implementing interactive IP communications. Traditional corporate voice networks, based on circuit-switched technology, are closed in nature and can be reasonably well protected against eavesdropping, impersonation and other threats using physical security measures. Legacy voice services are implemented using proprietary telephony equipment and isolated, voice-only networks. An attacker must gain physical access to the private voice network and have particular knowledge of vendor-specific telephony protocols.

IP networks, by contrast, are inherently less secure than traditional circuit-switched voice networks. Because they are shared by many users and applications, IP networks expose the enterprise to a variety of internal and external security threats. In a converged IP infrastructure, interactive communication services are delivered in a manner similar to other IT applications – via software running on standards-based computing platforms powered by Linux or other real-time operating systems. Voice, video and multimedia traffic is transported alongside other data across private IP networks and the Internet, exposing the IP communications infrastructure, services and applications to a wide range of threats (see Table 1). Attackers can leverage standards-based network analyzers and public domain scanners and diagnostic tools to identify and exploit security weaknesses from inside or outside the enterprise.

Type of Threat	Example	Potential Implication
Reconnaissance scan	Address or port scan used to footprint network topology	Targeted denial of service, fraud, theft
Man-in-the-middle	Attacker intercepts session to impersonate (spoof) caller	Targeted denial of service, breach of privacy, fraud, theft
Eavesdropping	Attacker “sniffs” session for the purpose of social engineering	Breach of privacy, fraud, theft
Session hijacking	Attacker compromises valuable information by re-routing call	Breach of privacy, fraud, theft
Session overloads	Excessive signaling or media traffic (malicious, non-malicious)	Denial of service
Protocol fuzzing	Malformed packets, semantically or syntactically incorrect flows	Denial of service
Media injection	Attacker inserts unwanted or corrupt content into messages	Denial of service, fraud

Table 1: Interactive IP communications security threats

Conventional IP firewalls and IP security appliances weren’t conceived with interactive IP communications in mind and don’t adequately address IP telephony and UC security concerns. Enterprises must adopt new security practices and implement new security platforms to ensure application and service integrity, mitigate risks and maintain business continuity.

A complete IP communications security solution must:

- **Safeguard confidentiality:** Ensure the privacy of IP communications sessions to prevent leakage of sensitive data or loss of intellectual property.
- **Ensure service integrity:** Prevent unauthorized system access and deter toll fraud and service theft.
- **Guarantee service availability:** Deliver PSTN-like reliability and service quality. Protect against malicious attacks, network and system failures, and service overloads.
- **Enable regulatory compliance:** Accommodate the special privacy, call recording, and session prioritization requirements imposed by industry and government regulations.
- **Provide multiple layers of security:** Defend against a wide array of internal and external threats and protect against systematic, multi-faceted attacks.
- **Offer rich policy management:** Enforce compliance with corporate security policies and procedures that mandate the use of strong passwords, encrypted communications, call recording, etc.

Acme Packet's Net-SAFE (Session Aware Filtering and Enforcement) security framework is specifically designed to address the unique security challenges enterprises encounter when delivering interactive communications over private IP networks, the Internet or new SIP-based services. Net-SAFE delivers unmatched protection for IP telephony and UC infrastructure, services and applications, providing:

- A comprehensive set of SBC security features and functions
- A highly-scalable architecture that meets the security needs of small to very large enterprises without compromising user quality of experience
- A back-to-back user agent (B2BUA) approach that uniquely delivers capabilities not possible with data-focused or in-line “passive” security elements
- Extensive security monitoring and reporting capabilities

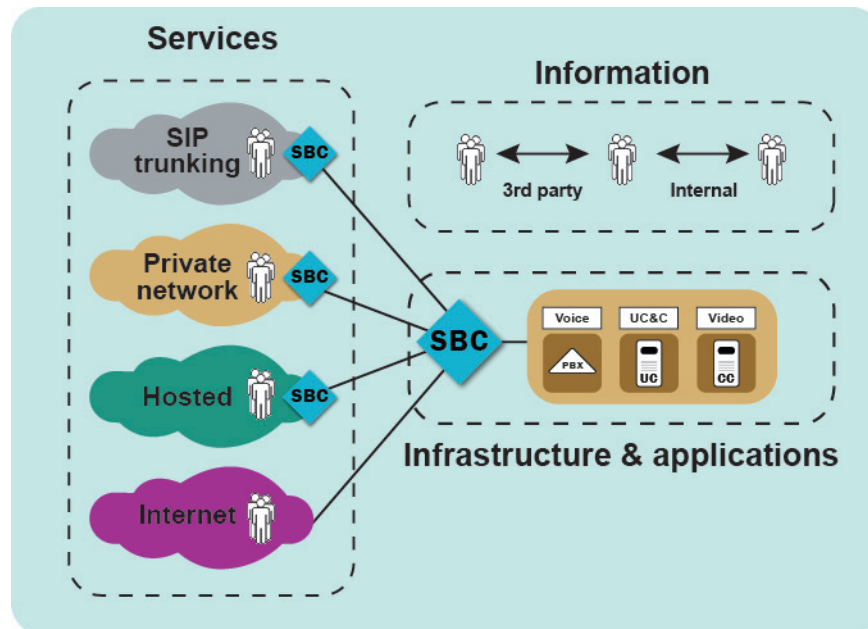


Figure 1: Net-SAFE protects interactive IP communications infrastructure, services, applications and information

Advanced SBC security features and functions

Net-SAFE safeguards IP telephony and UC security infrastructure, applications and services, employing advanced security techniques to defend against a broad array of threats. Comprehensive features include:

- **Overload protection:** Denial of Service (DoS) attacks and extraordinary network events such as registration floods can overwhelm IP communications infrastructure (border elements, application servers, endpoints) and impair critical applications and services. Net-SAFE utilizes wire-speed packet classifiers and dynamic trust-based control mechanisms to regulate signaling and media streams, and protect IP communications infrastructure against malicious attacks and unusual network events.
- **Protocol conformance enforcement:** Attackers can attempt to disrupt applications and services by generating malformed messages to impair IP-PBXs, UC servers or other infrastructure. Net-SAFE inspects and validates all SIP traffic and blocks non-compliant sessions to combat these malicious attacks.
- **Access control:** Net-SAFE utilizes static and dynamic Access Control Lists (ACLs) to control access to enterprise communications based on a broad set of administratively-defined criteria. Granular access control policies help prevent toll fraud and service theft, thwart certain types of denial of service attacks, and help enterprises enforce compliance with corporate security policies.
- **Topology hiding:** Attackers often initiate reconnaissance scans to uncover IP telephony and UC address or port information that is subsequently used to penetrate or disrupt IP communications. Net-SAFE conceals enterprise topology information to hamper reconnaissance scans.
- **Encryption and authentication:** Net-SAFE implements standards-based authentication mechanisms along with standards-based encryption (TLS, SRTP, IPsec and SSL) to ensure the privacy and integrity of IP communications sessions (SIP signaling and RTP media streams) and prevent the loss of confidential information.

Security-optimized, highly-scalable architecture

Net-SAFE is based on a highly-scalable architecture that addresses a broad range of customer requirements and market segments in a unified manner with common administrative and management interfaces. The framework addresses the price/performance requirements of virtually any customer or environment – from small businesses and small offices to large enterprises and large data centers. Net-SAFE enables software-based SBCs for smaller customers and environments as well as SBCs with special-purpose processing and hardware-acceleration for larger enterprises and sites. By leveraging a highly-scalable product architecture Acme Packet is able to cost-effectively address the security needs of any business – small or large – without compromising user quality of experience.

Back-to-back user agent (B2BUA) approach

Unlike SIP FW/ALGs and other passive SIP elements, Net-SAFE leverages fully-functional SIP B2BUAs which are actively involved in both the signaling and media paths providing greater protection against well-orchestrated attacks. A B2BUA can perform deep packet inspection and intelligently control SIP sessions in response to real-time network conditions by:

- Terminating, inspecting and re-initiating SIP sessions (including encrypted traffic)
- Detecting and rejecting non-compliant SIP sessions
- Blocking non-compliant endpoints and all irrelevant traffic (ICMP, HTTP, etc)
- Controlling legitimate registrations in a stateful manner, even during overload conditions
- Dynamically monitoring and controlling SIP signaling flows based on session counts and rates
- Rerouting SIP signaling and media in response to path failures

Extensive security monitoring and reporting

Net-SAFE provides comprehensive security monitoring and reporting capabilities to help IT compliance and security personnel detect, identify, isolate and contain security breaches. The framework provides mechanisms for monitoring IP telephony and UC infrastructure and notifying operations personnel of potential attacks and overload conditions in real-time. Net-SAFE exposes detailed historical records including audit trails, call detail records, QoS statistics and security logs, and provides packet capture and analysis capabilities to help security teams track and analyze threats.

Most security events aren't isolated incidents. Attackers often act in a systematic fashion – identifying security vulnerabilities, penetrating the network, and then covering their tracks. In a typical scenario, an attacker might:

1. Perform a reconnaissance scan to obtain network topology information and identify free addresses and ports
2. Eavesdrop, reroute or intercept sessions to capture sensitive information, appropriate services or commit fraud
3. Inject malformed packets or flood the network to overwhelm resources and disrupt service
4. De-register legitimate users and endpoints to avoid detection

An effective security plan must defend against multi-faceted attacks. Net-SAFE delivers a multi-layered defense framework that protects against a wide range of threats and combats each step of a well-orchestrated assault. In particular, Net-SAFE:

- Inhibits reconnaissance scans by hiding topology information, applying dynamic access controls, blocking irrelevant protocols and encrypting signaling and media flows.
- Defends against man-in-the-middle attacks, hijacking and eavesdropping by authenticating sessions to ensure integrity, encrypting media and signaling flows, blocking outgoing sessions to unauthorized destinations and maintaining detailed call records and audit trails.
- Protects against session overloads by proactively defending against malicious DoS/DDoS attacks, shielding border and infrastructure elements against floods and overloads, and ensuring legitimate sessions and emergency calls can be established even during overload conditions.
- Combats protocol fuzzing (malformed packets, semantically or syntactically incorrect flows) by acting as a session-aware SIP B2BUA that performs deep packet inspection on both signaling and media streams, blocking all non-compliant SIP sessions and all traffic unrelated to interactive communications.
- Prevents media injection by encrypting signaling headers (which contain information about the media stream) as well as media streams and acting as a SIP B2BUA that is able to terminate, inspect, manipulate and re-terminate sessions.

The problem with signature-based security systems

Some SIP security vendors promote signature-based defense mechanisms for ultimate security. Just as a PC antivirus program uses signature patterns to identify viruses and worms, a SIP signature-based security system searches for known patterns of data within SIP packets to detect and deter interactive communications threats. Signature-based SIP security systems suffer from the same limitations as signature-based PC antivirus programs:

- **Zero-day threats:** Signature pattern files are created on a reactive basis, in response to known threats. Well-designed signatures also tend to be polymorphic, making them extremely difficult to detect by signature-based detection mechanisms. Previously-unknown threats can arise at any time and go undetected.
- **False positives:** Signature-based systems can improperly characterize threats and mistakenly block legitimate communications.
- **Performance implications:** Low-end security appliances can exhibit degraded performance as signature libraries grow in length and complexity.
- **Malware concealment:** To avoid detection, malware is often compressed, encrypted and designed to self mutate each time it attacks. Most signature-based security systems are incapable of inspecting encrypted SIP/SDP headers or encrypted RTP streams, let alone malware that repeatedly morphs, each time with a different scheme.

Net-SAFE offers a superior alternative to signature based systems by using a proactive approach to threat management. Acme Packet SBCs act as SIP B2BUAs which terminate, inspect, and re-initiate signaling and media flows and automatically block non-compliant traffic (malformed headers, improper syntax, out of sequence, fragmented, oversized, etc) or traffic unrelated to interactive IP communications.

In addition, Net-SAFE supports a configurable rules engine that allows administrators to define and apply their own rules in a dynamic fashion. The configurable rules engine allows customers to supplement Net-SAFE's inherent anomaly detection mechanisms plus combat zero-day threats without relying on vendor signature library updates.

Threat	Applicable Net-SAFE function(s)	Result
Reconnaissance scan	<ul style="list-style-type: none"> • Topology hiding • Access control • Encryption and authentication 	Confidentiality and information integrity, prevention of targeted DoS/DDoS attacks
Man-in-the-middle	<ul style="list-style-type: none"> • Access control • Encryption and authentication 	Prevention of targeted attacks, confidentiality and integrity of communications
Eavesdropping	<ul style="list-style-type: none"> • Topology hiding • Access control • Encryption and authentication 	Confidentiality and integrity of communications, fraud and theft prevention
Hijacking	<ul style="list-style-type: none"> • Topology hiding • Access control • Encryption and authentication 	Confidentiality and integrity of communications, fraud and theft prevention
Session overloads	<ul style="list-style-type: none"> • DoS/DDoS and overload protection • Access control 	High availability of communications services, infrastructure and applications
Protocol fuzzing	<ul style="list-style-type: none"> • Deep packet inspection • Protocol qualification 	High availability of communications services, infrastructure and applications
Media injection	<ul style="list-style-type: none"> • Encryption and authentication 	High availability and integrity of communications

Table 2: Net-SAFE protects against a wide range of security threats

Conclusion: Net-SAFE delivers unmatched protection for interactive IP communications

Enterprises must implement new security systems and practices to support the adoption of interactive IP communications. Conventional firewalls and IP security devices weren't designed with IP telephony and UC platforms in mind and leave the enterprise vulnerable to a variety of internal and external threats. SIP FW/ALGs and special-purpose SIP-aware appliances are passive SIP elements which offer only limited protection against well-orchestrated attacks.

Acme Packet's Net-SAFE security framework fully addresses the unique security challenges enterprises encounter when delivering interactive communications over private IP networks, the Internet or new SIP-based services. The framework complements data-oriented security techniques, and leverages a highly-scalable, security-optimized architecture, state-of-the-art session-aware security features, and comprehensive management capabilities to protect IP telephony and UC infrastructure, services and applications against the broadest range of threats and ensure the confidentiality, integrity and availability of interactive IP communications. By implementing Net-SAFE in combination with stringent security policies and procedures enterprises can enjoy all the business benefits of interactive IP communications and SIP services without compromising usability, reliability or integrity.



100 Crosby Drive
Bedford, MA 01730 USA

t +1.781.328.4400
f +1.781.425.5077
www.acmepacket.com

© 2011 Acme Packet, Inc. All rights reserved. Acme Packet, Session-Aware Networking, Net-Net and related marks are trademarks of Acme Packet. All other brand names are trademarks or registered trademarks of their respective companies.

The content in this document is for informational purposes only and is subject to change by Acme Packet without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Acme Packet assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Acme Packet, Acme Packet has no obligation to develop or deliver any future release or upgrade or any feature, enhancement or function.