Sangoma

A Sangoma SBC Playbook

VoIP Security

Why Your Network Needs an SBC

Session Border Controllers by Sangoma

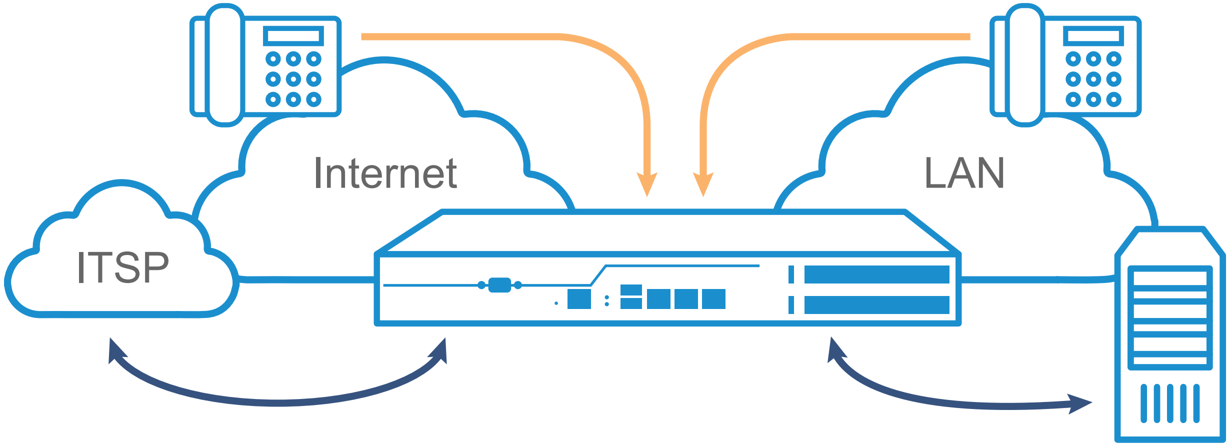
As VoIP networks have become the de facto standard for modern business telecommunications, the number of threats and malicious actors have multiplied. Securing your VoIP network is more important now than ever before.

To help support organizations as they tighten up the security of their VoIP networks, we’ve put together this guide to VoIP security, including plenty of general VoIP security information as well as some of the ways in which a Sangoma Session Border Controller (SBC) can enhance security and offer the highest level of protection for your VoIP network.

- Protects SMBs, enterprises, and service providers from VoIP threats
- Securely connects remote users to the corporate phone system without requiring a VPN connection
- Compatible with virtually all phone systems, including Sangoma's own Unified Communications (UC) solutions
- Session-based licensing with all features included
- Supports 5 - 4,000 simultaneous calls
- Field-upgradeable session expansion available
- Compatible with virtual environments
- Browser-based GUI for easy configuration
- Hardware-based transcoding and media handling
- Provides business continuity, quality of service, interoperability, and more
- Annual support and maintenance plans available

Security Concepts:
Security Starts with a Policy

Security is the last requirement (if at all) addressed in too many deployments, when it should be the first and most important topic to be discussed. When planning or implementing a VoIP solution, make security a priority.



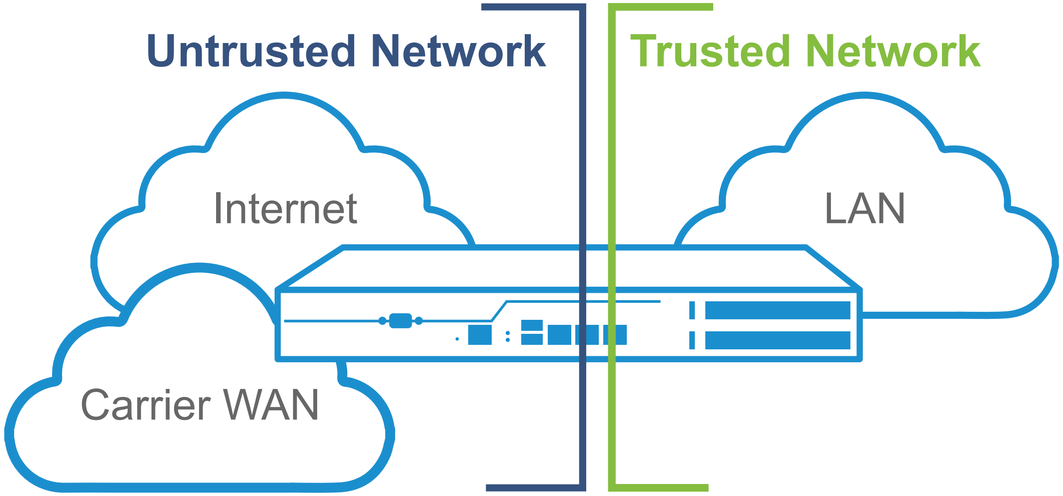
Security breaches don’t come exclusively from the public Internet but may very well also come from within trusted networks, in the form of worms, trojans, and other malware. Although there are few widespread malware threats targeting VoIP— don’t rule it out! Internal breaches can come from misconfiguration and unattended devices. Remember, IP networks are open—if someone knows your IP address, they can communicate with it.

An SBC has the ability to apply a tremendous amount of security policies for VoIP and IP networks. SBCs enable IT Administrators to enhance their overall security solution with a device that leads in VoIP security.

Trusted and Untrusted Networks

A common security concept we encounter every time we connect a device to a network is deciding whether the network is trusted or untrusted. For example, whenever you take your laptop into a coffee shop for the first time and use their open Wi-Fi connection, you're typically prompted to define the network zone to which you are connecting, whether it be home, work, or public. Depending on what's selected, the appropriate security settings are enabled.

In the context of VoIP and IP networking, trusted and untrusted zones are defined by where the security control devices are located. Firewalls are typically used as an IP network control point, and SBCs are used as VoIP control points.



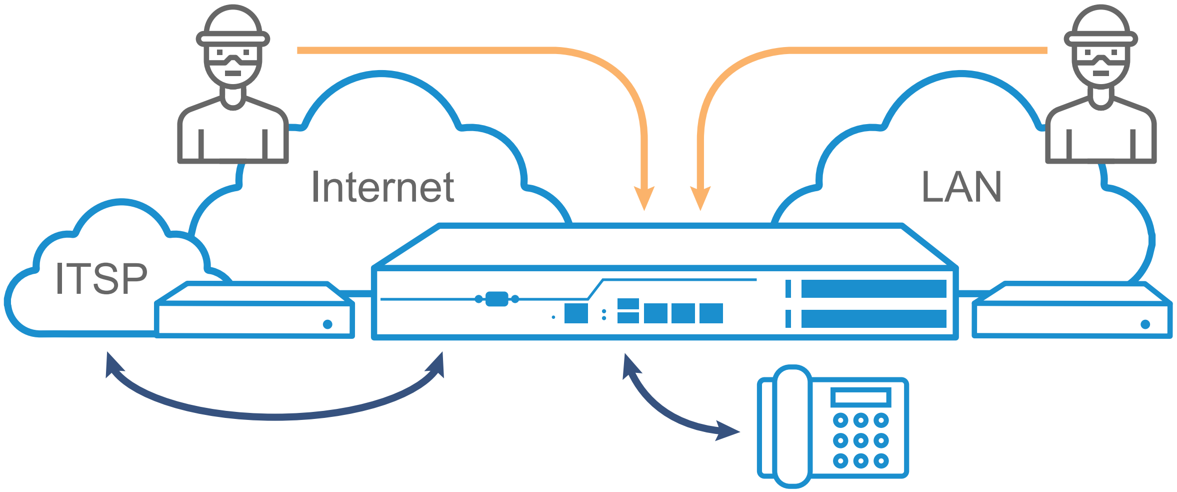
It is important to place an SBC between trusted and untrusted IP networks to provide security policies and ensure that each network does not have a direct connection. The Internet is the most untrusted IP network, and even private WAN IP networks should be considered untrusted for the security of the enterprise trusted LAN network.

End of Geography

With respect to traditional TDM technology, security issues such as toll fraud, intrusion of services, and eavesdropping are about point of presence. To listen in on someone's telephone line, the malicious person needs to be physically located beside the line.

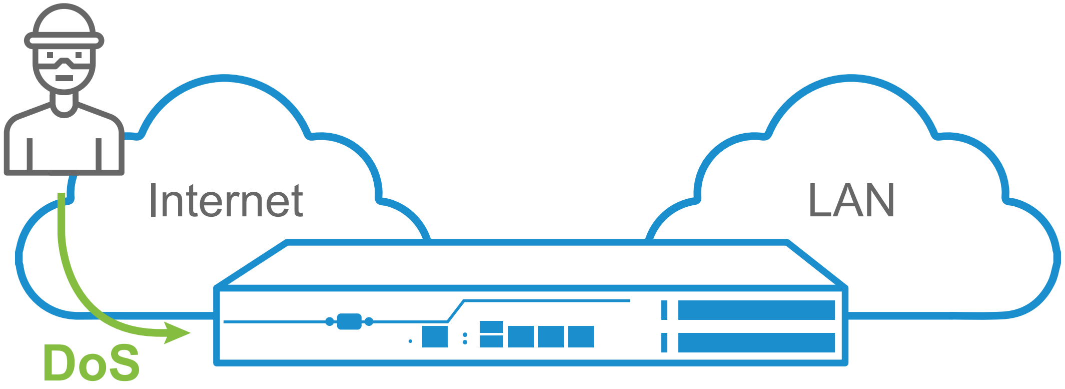
This changes with Voice over Internet Protocol (VoIP). The Internet is an "open" system. If someone knows your IP address, they can get to it. Similarly, if someone knows the path you are taking, they may be able to get in the middle of the path and intercept data. This holds true for both public traffic as well as private traffic, independently. No longer does someone need to be physically beside the equipment to tamper or breach the security of the equipment. Security breaches can come from anywhere, private or public networks.

To minimize the threat, one can enable VoIP security and routing policies on their IP network using an SBC—which will provide a Network Address Translation (NAT) firewall along with Intrusion Defense Systems (IDS) or Intrusion Prevention Systems (IPS).



Rate Limiting

In order to protect servers from overload and DoS attacks, enterprises may limit the amount of calls to or from a specific peer or device, either by the number of new calls within a given period, by the overall limit of concurrent calls, or both.



The method for Rate Limiting on SIP is to determine the number of INVITEs or new calls that the SBC is going to allow to traverse through to the VoIP servers. This is beneficial when wanting to restrict the number of new calls presented in a given period of time.

Concurrent Session Limiting is used on the SBC to limit the number of overall concurrent calls. This policy limits the overall call capacity dynamically between the peers.

SBCs are designed to dynamically apply limiting policies. If the limit is reached, the peer or device will be blocked for the duration of the limit period.

Why Firewalls Are Not Enough

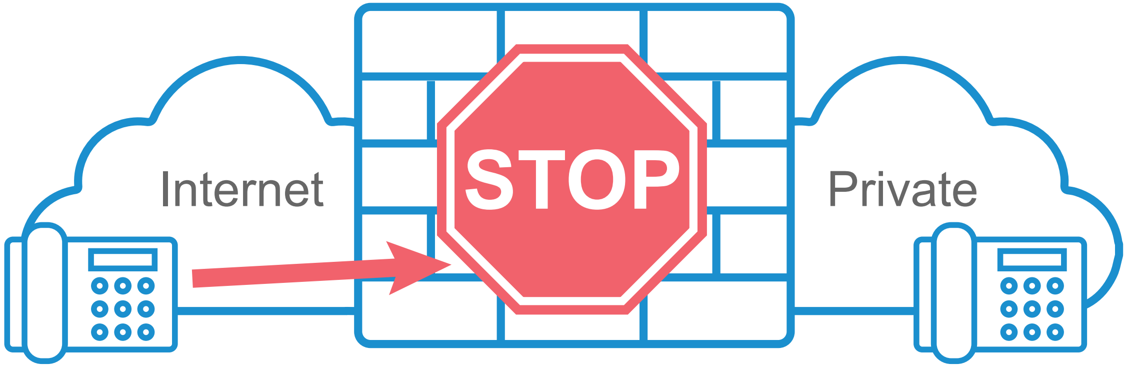
Firewalls and Unified Threat Management (UTM) are ubiquitous in today’s networks as they offer comprehensive protection against blended threats. But these devices offer little coverage in VoIP security protection.

Firewalls and UTM focus on data security, email, web, worms, trojans, and so on. None of these data applications are “real time”, where VoIP requires immediate application of security policies.

In addition, the inherent function of firewalls is to deny all unsolicited traffic. For example, the act of making a phone call is an unsolicited event; thus, firewalls can be counterproductive to an effective VoIP deployment by denying VoIP traffic.

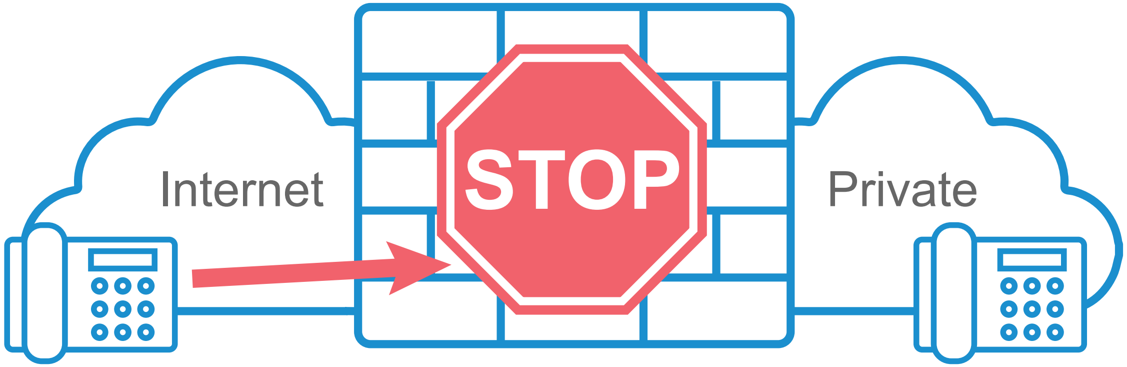
Furthermore, firewalls do not provide the SIP protocol addressing needs to rewrite and re-address proper SIP signalling and media negotiations.

The purpose of an SBC is to enhance the “real time” VoIP security policies of the existing security infrastructure, and focus on establishing reliable SIP communications instead of just “poking holes” in your firewall to allow phone calls through at the risk of breaching security.



Why Firewalls Cause Problems

When deploying remote phones, whether as a carrier in a hosted solution or as an enterprise with home or remote employees, these phones will have to reside behind some type of firewall. Firewalls are meant to provide security by hiding the private network addresses of end user devices and, at the same time, preventing all unsolicited network traffic from entering the private network.

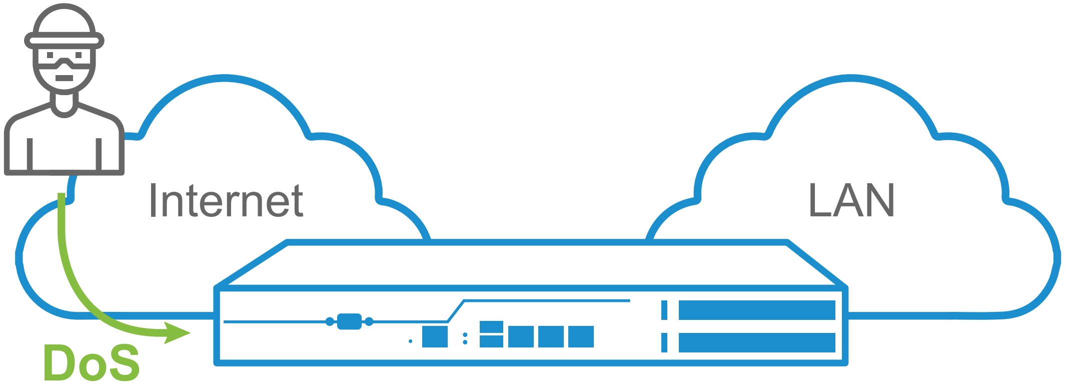


However, VoIP uses SIP (RFC 3261) as a communications protocol, which is an application and not a network routing protocol. Firewalls don't provide application support. Making a phone call by its very act is an unsolicited event, an event that every firewall will block or deny traffic. And, in most cases, poking holes in the firewall to allow these phone calls through simply causes more security and audio problems.

An SBC provides several features to enhance the deployment security of VoIP. It works with firewalls by accepting the VoIP traffic and applying security and routing policies to the phone calls, in essence "vetting" the calls for the network firewall. In addition, SBCs provide Far End NAT solutions for SIP phones deployed behind firewalls whose traffic is coming from across the Internet.

Security Threats:
Denial of Service

A Denial of Service (DoS) attack is when there is concentrated effort to ‘flood’ an available application, transport, or connection with overwhelming traffic in an attempt to slow down or disrupt an available service. In the context of VoIP, a DoS attack is focused on the telecommunication services, attempting to slow down, disrupt, or even outright stop VoIP from occurring.



The SBC is designed to protect mission critical Unified Communications (UC) applications such as IP PBXs, IVR, call centers, and more. The SBC contains features, such as Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), specifically designed for SIP applications, detecting attacks and automatically adjusting to prevent the DoS attack from traversing into the private network.

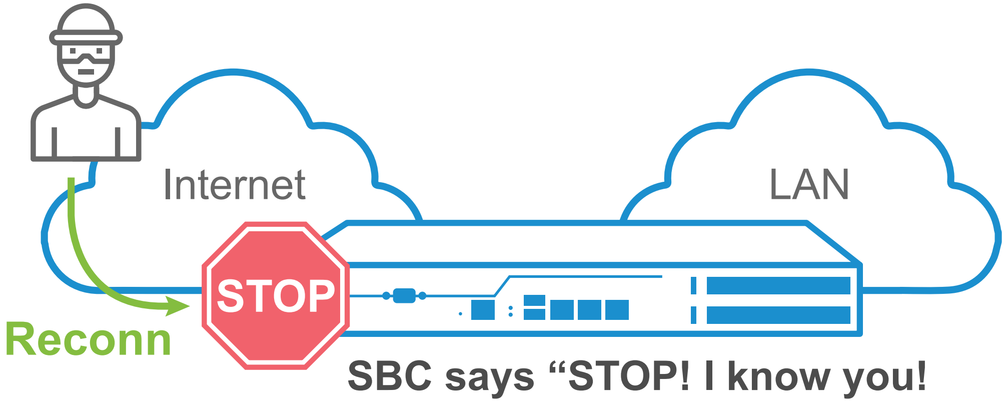
In addition, the SBC has other features such as call admission control, rate limiting, and advanced call routing with ACL to prevent unwanted DoS traffic.

Reconnaissance Attacks and Signature Recognition

In the context of VoIP, a reconnaissance attack occurs when a malicious party tries to learn information about your network. Place a SIP device directly on the Internet and watch the network activity. It won't take long before you see a number of erroneous SIP packets searching for SIP devices. Before any concentrated effort to purposefully attack a VoIP service, there first needs to be a process of information gathering.

In most cases, reconnaissance attacks precede an actual access or DoS attack. First is the discovery of a VoIP service, as the malicious party conducts a SIP scanner sweep of the target network to determine which IP addresses have live SIP services. Sending specific SIP packets, these SIP scanners can provoke a response from the SIP device and confirm its availability. Then the malicious party determines which VoIP services, accounts, extensions, and trunks are active on the live VoIP addresses. From this information, more activity may potentially follow, such as DoS attacks, toll fraud, and others.

There are a number of common SIP scanners that have a unique 'signature' within SIP. The best way to deal with these SIP scanners is to identify its 'signature' within the SIP, and then outright reject the packet.

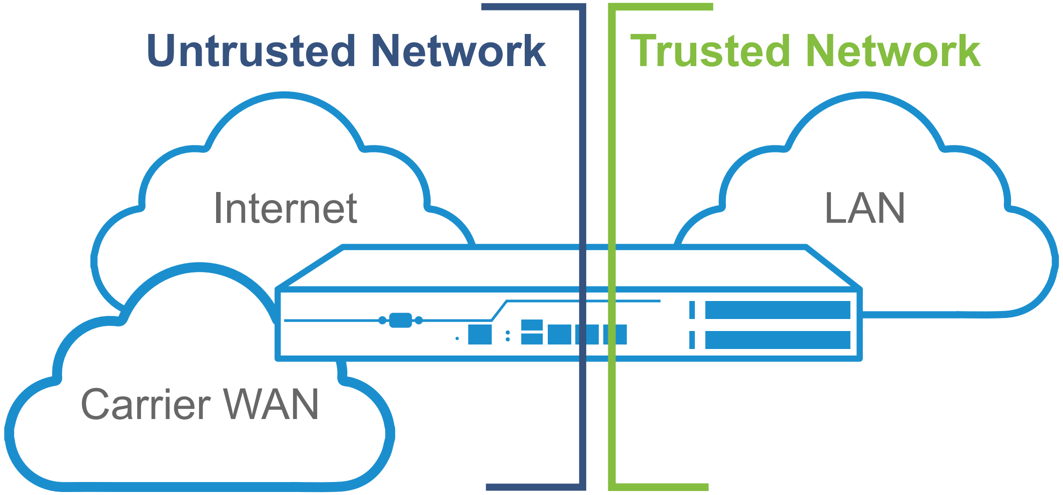


The SBC is designed to do just that. It recognizes these SIP scanners by their 'signature' and rejects them. Not responding to SIP scanners allows the VoIP deployment to be hidden from future security attack attempts, making it harder for malicious parties to compromise your network.

Toll Fraud

Toll fraud is the most common and costly security problem in the telecommunications industry, in both legacy telephony as well as Voice over Internet Protocol. With VoIP, the opportunity for toll fraud is greater due to the accessibility and connectivity to the public Internet.

Toll fraud is achieved through compromised IP-PBXs, IVRs, subscription/identity theft, compromised account authentication, and a host of other methods. It is important to note that toll fraud is not restricted to just public Internet connections, as carriers with private WAN networks can be compromised by their own customers if their carrier equipment is compromised.

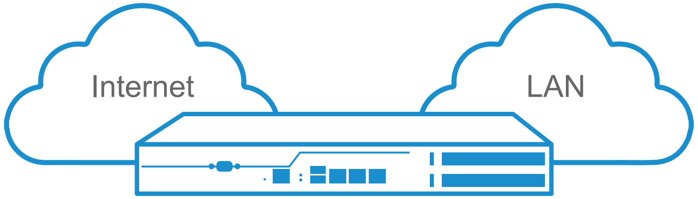


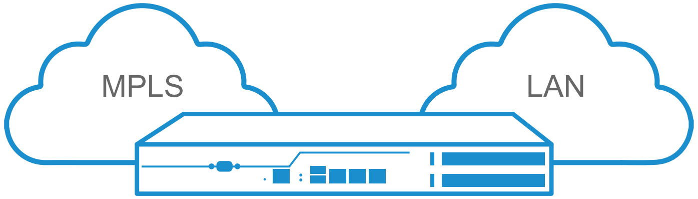
Every VoIP device in the call flow path is responsible to prevent toll fraud, but the SBC may be the most important. Tools built into the SBC, such as rate limiting, blacklisting, and advance call control, help identify potential toll fraud activities. Other features, such as SNMP and SMTP alert notifications, alert IT administrators to potential issues. Simply put, the SBC is designed to play an integral role in toll fraud prevention.

SBC Deployment & Use Examples:

Enterprise Network Edge

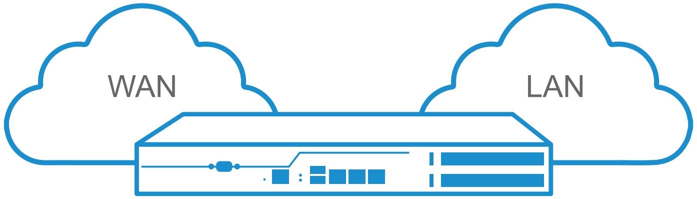
The SBC is designed to sit on the network edge, between different networks, expanding the business communication network's ability to be flexible and resilient – no matter who is in the communication path, making the future of the business communications more about connectivity and less about delivery.





To accomplish this, simply place an SBC at the edge of two networks. This can take different forms. One interface will always be on the private LAN, while the other can be on the Internet or on the carrier WAN. From there, you can create a control point where policies can be applied to provide solutions for:

- Security and routing
- Resiliency and interoperability
- Quality of service
- Failover and troubleshooting
- SLA management and encryption
- Access control, call admission control, and authentication
- And more.



VoIP in the Cloud

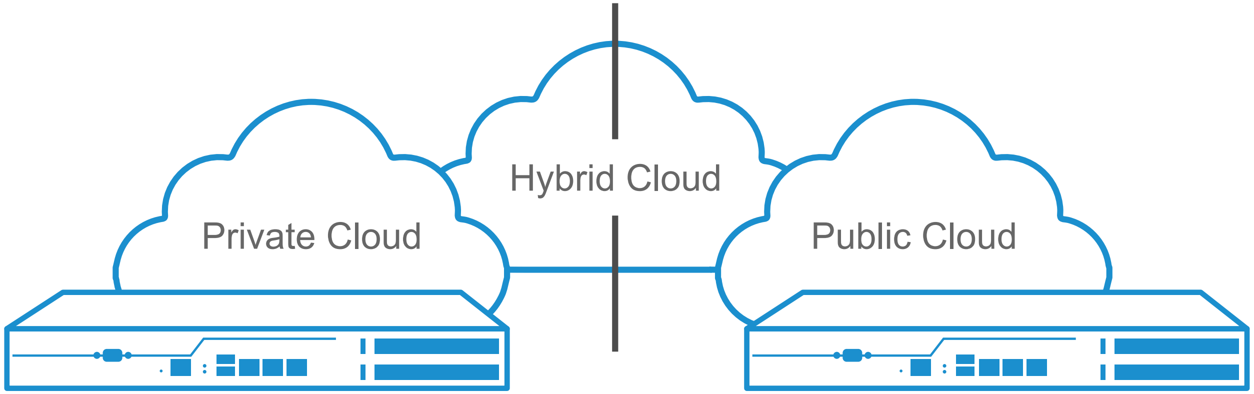
Cloud solutions offer greater flexibility in many VoIP and SBC deployments. Public cloud services (like those offered by Google, Amazon, and others), a private cloud, or some hybrid cloud service all essentially provide a virtual office to give the flexibility of connecting to business VoIP services anywhere, any time.

With the growing number of voice and video-enabled devices used in today's business environment, access to VoIP services is even easier.

There are many benefits to moving VoIP to the cloud:

- Reduced IT costs
- Scalability
- Collaboration efficiency
- Flexibility of VoIP deployments

The SBC provides the ability to operate in various cloud services, allowing carriers and enterprise deployments to reduce costs, scale effectively, and increase continuity with other cloud VoIP applications, all ultimately increasing the flexibility of VoIP deployments.



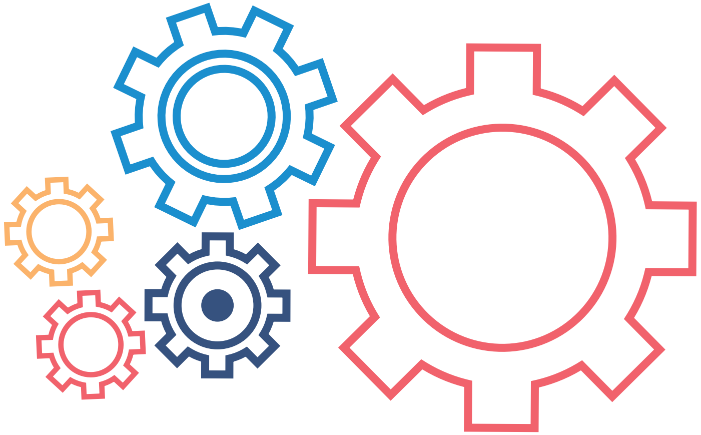
Interoperability

Interoperability is the ability of a system or a product to work with other systems or products without special effort on the part of the customer.

Internet Telephony Service Providers (ITSP) offer many different services to different customers. Therefore, their products and services come in many different deployment forms utilizing many different policies and utilizations of SIP.

In addition, SIP itself is written in a manner that is open for interpretation, with some 40+ RFCs in use, all with some form of interpretation. Accommodating this diversity can be very challenging for many deployments.

While each provider may use similar commonly deployed carrier grade vendor equipment, these devices can be configured in many different ways to provide a number of different solutions meeting the needs of the individual service provider. This makes interacting with each provider uniquely different.



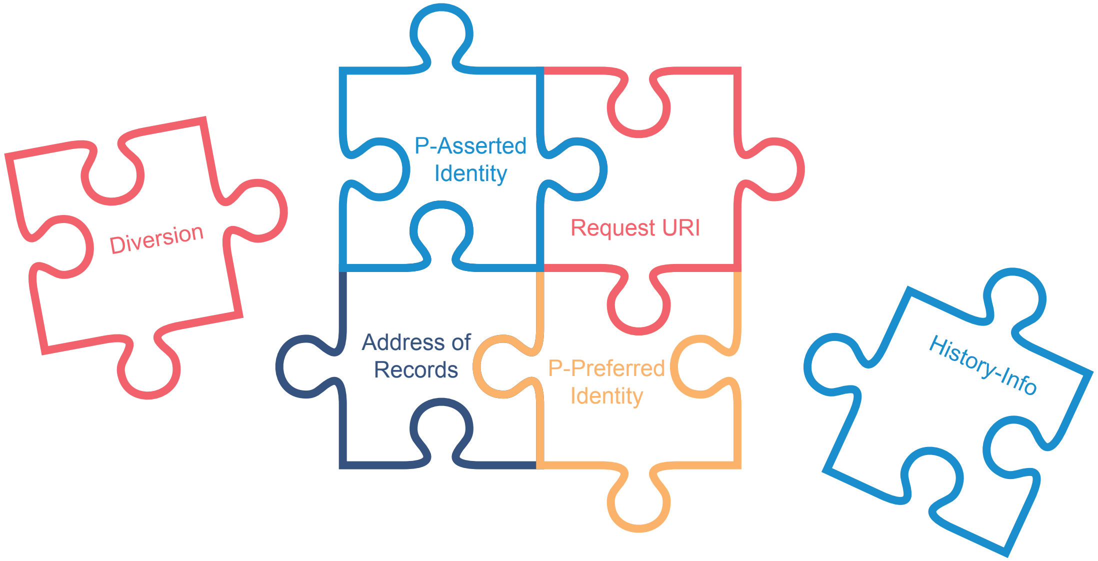
The SBC allows the IP PBX and ITSP to standardize on one implementation of SIP trunking, while handling all of the configuration and adjustment to the corresponding services as well. This allows for greater flexibility by allowing the enterprise deployment to be independent of any external factors imposed by the service provider.

SIP Header Manipulation

When trying to accomplish multiple vendor integration and leverage the equipment and solutions available, you will often find firsthand that each vendor has completely different SIP protocol requirements.

In this situation, you need an "all-purpose tool"—one that accepts all the different variations of the SIP being sent and provides the ability to rewrite every possible header and field within the SIP protocol messages. This ability enables an enterprise to be less vendor-dependent, and thus, opens up the flexibility of the solution to interconnect with any other vendor.

The SBC is the key component in this multi-vendor scenario. Multiple IP PBXs, carriers, phones, and other UC applications can all be interconnected seamlessly with an SBC. Your SBC should allow you to rewrite the SIP protocol (and in the process, become less reliant on vendor certifications and recommendations) and focus on providing a solution that works for your unique business requirements.

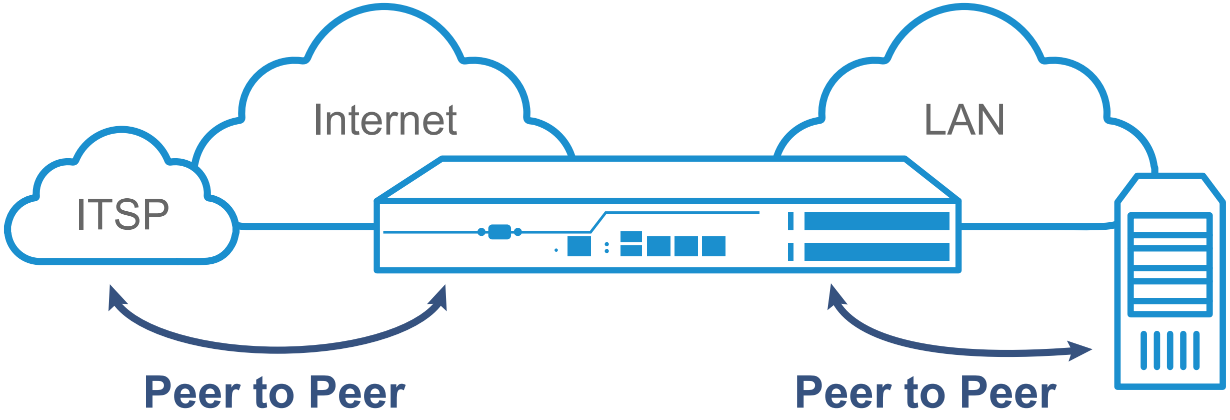


Peer-to-Peer

Some providers simply require the enterprise to provide their IP addresses, creating an IP address-to-address or peer-to-peer relationship. The authentication is based mainly on the IP addresses.

Peer-to-peer offers layers of security, along with SIP formatting restrictions. Rather than an open policy with account look-up and authentication, this deployment style is a “trusted” relationship between the provider and the enterprise equipment, processing phone calls only from trusted peers.

The SBC allows an IP PBX and other devices to connect peer-to-peer with vendor SIP trunks by acting as an integration point between the IP PBX and the ITSP. The SBC provides the same additional security features, SIP interoperability and routing requirements in peer-to-peer as it would in registration or authentication deployments.



Everything Connects, Connect with Sangoma

Sangoma (TSX Venture: STC) is the leading provider of enterprise grade, value-based communications solutions. With Sangoma, businesses of all sizes can find affordable cloud and on-premise Unified Communications (UC) systems with advanced functionality.

Sangoma's global footprint extends to millions of customers in over 150 countries who rely on Sangoma technology for their mission critical communications infrastructure.

Sangoma offers a complete portfolio of next-generation UC solutions, delivering industry-leading quality at price points that maximize customers' return on investment. Sangoma products and services are developed by the best engineers in the industry and backed by a professional services team that is second to none, offering as much support and assistance as any business needs, up to a fully managed solution.

To learn more about Sangoma products and services, visit us at www.sangoma.com.

100 Renfrew Drive, Suite 100, Markham ON L3R 9R6 Canada | +1 (256) 428-6000 or 1 (877) 344 4861 (toll free in N. America)

Sangoma