SANGOMA

VOIP SECURITY AND BEST PRACTICES

For SIP Trunking and Branch Offices Applications

White Paper

TABLE OF CONTENTS

Overview

This document will bring knowledge to IT & VoIP Administrators about VoIP Security specific to SIP Trunking and Remote Phone applications. Topics such as understanding what some types of VoIP Attacks are, and how to deploy VoIP Security solutions in common applications such as SIP Trunking and Remote Phones. In the end, no one device is responsible for VoIP Security, but rather all VoIP devices and solutions must have some responsibly to overall VoIP Security. This document complements common computing security implementations and expands into various ways to implement VoIP Security and discuss what features can be used on these devices to best deploy a secure VoIP Solution.

To understand the need for VoIP Security, you first need to understand the types of VoIP attacks and threats presented on the network. Topics such as the availability of access to VoIP and the various types of directed and indirect attacks on VoIP solutions and devices. Discovery of VoIP solutions by means of Reconnaissance, then denial of VoIP Services by means of Denial of Service attacks, and the most common Toll Fraud.

One major application of VoIP is SIP Trunking. SIP Trunking is typically a Peer to Peer relationship between the Service Provider and Enterprise. Topics specific to securing SIP Trunking will be discussed, securing SIP Trunking solutions with a Firewall only, and also with a Session Border Controller. In both methods, even the IP-PBX has a role to play to provide a secure SIP Trunking solution.

Another major application is the deployment of Remote Phones in branch offices or work-from-home situations. Remote phone deployments are dynamic in nature, with phones registering abroad to a central IP-PBX, where the location of the Remote Phones is constantly changing and updating. There is also the type of traffic to and from the phones which is vastly different than a SIP Trunk with all the dynamic call control requirements. Topics specific to securing Remote Phones will be discussed, as will solutions with Firewalls only and the use of a Session Border Controller. And it bears repeating in both of these methods, the IP-PBX still has a role to play in providing a secure remote phone solution.

Why Security is Important with VoIP

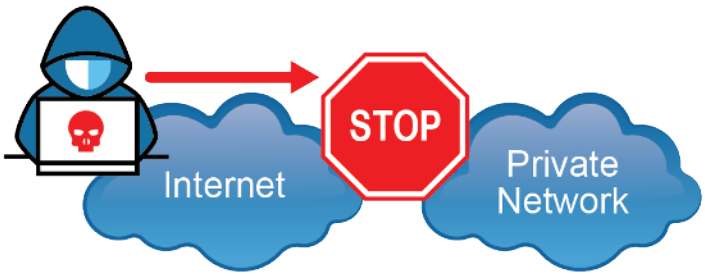
Security is one of the most frequently discussed topics, yet the importance of securing VoIP is hard to overstate. In this section, topics will include a few of the more prominent reasons why VoIP Security is so important, by understanding some of the common threats. Due to VoIP solutions and services growing, there is more attention to understand the types VoIP attacks and to counter with various methods when deploying VoIP security solutions. Every device and service are in part responsible for providing a secure VoIP solution, but there are a few different ways to deploy a secure VoIP solution.

End of Geography

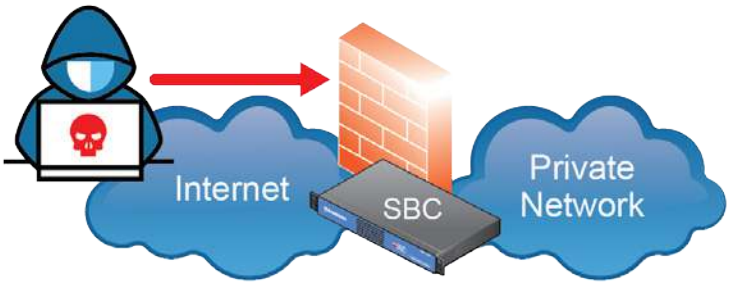
Traditional telephony delivered via analog or digital involves transmission over some physical medium. Security attacks to traditional telephony such as eavesdropping required physical presence with access to the physical lines.

Toll Fraud over traditional telephony has several forms, one common attack was to hairpin telecom traffic. This is when inbound calls into a voice network weresent back out to an alternate destination. Now that Voice Networking has merged with Computer Networking there is an “End of Geography”. Physical presence is no longer required to gain access to a voice system. Computer Networking is an OPEN network system, as any IP Address can connect with any other IP Address.
IP Protocol (IPv4 RFC 791 & IPv6 RFC 8200) and IP Addresses are fundamental in both public and private networks used in everyday communications for both voice and data. This leads to computer networking attacks having tremendously more access and tools available to conduct malicious attacks on VoIP infrastructures.

Carriers and businesses are concerned about exposing VoIP resources and VoIP information to hackers. Obviously, the exposure of VoIP resources over the Internet (public) is required, but internal (private) also needs some attention. A method is needed to prevent fraudulent VoIP activities between public and private Networks, monitoring and securing VoIP traffic.



Firewalls have become ubiquitous in the deployment of computer networks, for implementing Security policies and for the protection of private networks and business services. Voice applications over computer networking is growing substantially and requires similar implementation for the protection of private networks. Firewalls do not have the needed Real-Time and Protocol Security requirements for VoIP, but Firewalls still need consideration when deploying VoIP as they are a part of every network deployment. Session Border Controllers are better at providing VoIP Security and can work to complement Firewalls in providing a complete security solution.



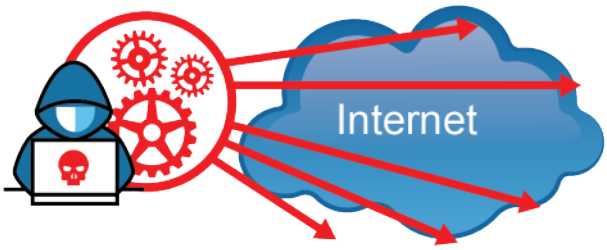
Types of Attacks

Analogies between War tactics and Internet Security are becoming more common as the proliferation of attacks on Internet services increase in strength and diversity. Part of these attacks are focused on VoIP Attacks of various types and strength. This section discusses various types of VoIP Attacks and their purpose. What is the Hacker trying to accomplish with the attack?

Reconnaissance

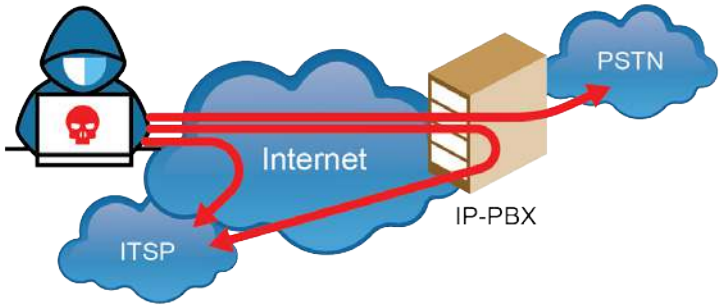
In many cases the first component of an attack is the search for VoIP services. Port Scans and other-directed VoIP discovery scans search through the Internet looking for VoIP Services. The hackers'

objective is to search through the range of IPv4 and IPv6 IP Addresses looking for VoIP Services to target with other forms of attacks. Once a VoIP Service is discovered, other types of attacks can then follow. It is best to understand the tools and methods used to discover VoIP Services and simply detect these methods and not acknowledge the VoIP Service back to the hacker. If the hacker does not know there is VoIP Service, they are most likely going to overlook and move on.



Toll Fraud

Various forms of Toll Fraud have been around since the infancy of telecommunications. Toll Fraud is a type of Intrusion of Service. Within VoIP, Toll Fraud has more possibility of exposure, as VoIP Services have more accessibility throughout the Internet. Toll Fraud has several different scenarios, this includes the hairpin of calls through an IP-PBX, as well as spoofing Carriers as legitimate customers. In every case the intension of the hacker is to avoid paying carrier billing by directing telecommunications traffic through someone else's service.



Intrusion of Service

The forcible act by a hacker to gain access to the VoIP Service is a common type of attack. The hacker gains access to the IP-PBX by registering a phone or application to the IP-PBX. Then acting as a valid extension, they can make calls as a local extension or disrupt normal operation by leaving voicemails or sending broadcasts to other users. Spoofing, Identity Theft, and SPIT are some specific types of Intrusion of Services.

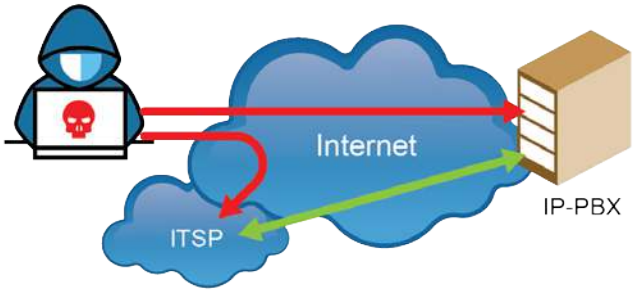
Spoofing

Spoofing is when a hacker attempts to mimic the attributes, such as a VoIP Phone or SIP Trunking service and uses their own Spoofing device to make calls into the IP-PBX. The hacker attempts to

mimic attributes such as IP Address, Endpoints, Username and Password of an existing device or service. Or on a lesser extent, mimicking the IP-PBX and calling the phone directly or calling the SIP Trunk provider directly.

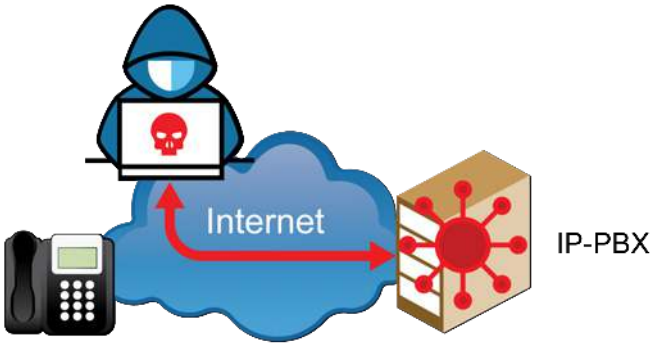
Identity Theft

Similar to Spoofing, but slightly different, is Identity Theft – also called Phishing. Although the terms Spoofing, and Phishing may sound similar, Phishing attacks generally use Spoofing as a strategy to steal information; however, Spoofing attacks are not necessarily Phishing. Spoofing attacks can be used to cause damage without stealing information. Identity Theft is where the hacker has stolen the identity of a legitimate party and poses as them. They can then take the configuration of a remote phone endpoint and makes calls posing as the legitimate phone to get access from the VoIP Server. In many cases, this is accomplished by obtaining the configuration files from the provisioning server on the
IP-PBX.



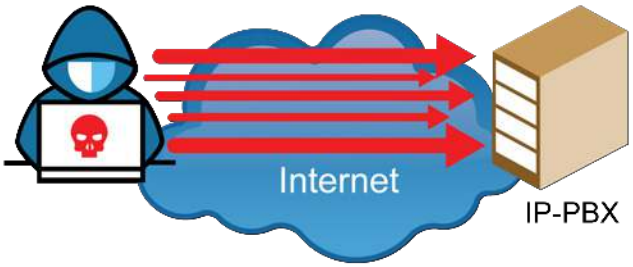
SPIT

SPAM over Internet Telephony (SPIT), once the hacker has either Spoofed or Phished their way into the IP-PBX, they begin calling every possible number with the intension of broadcasting a pre-recorded message or simply using or changing Voicemail, Auto-attendant and Conference resources. Just as the name suggests “SPAM”, but this time SPAM using VoIP technology to deliver unwanted messages.



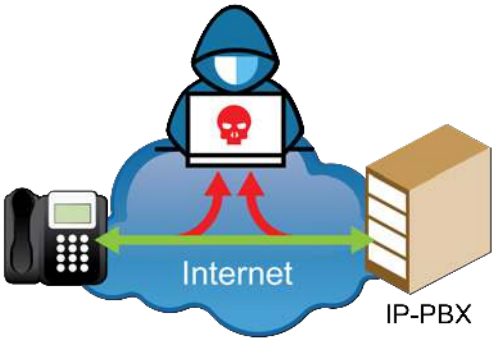
Denial of Service

Denial of Service is when the hacker seeks to make the VoIP Service unavailable to its intended users or carriers by temporarily or indefinitely disrupting services connected to the Internet. Typically accomplished by flooding the targeted VoIP Service with superfluous VoIP and other requests to overload systems and prevent the legitimate service from being operational.



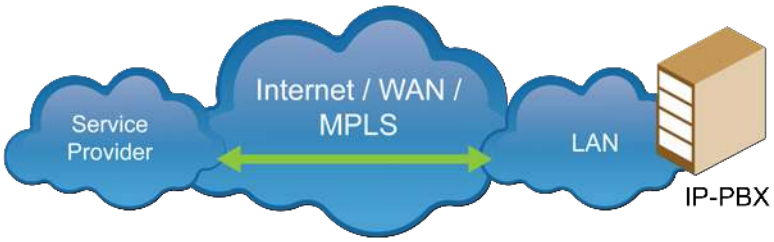
Eavesdropping

Eavesdropping is a very time-consuming process for a low return but has a high impact. It typically involves a number of different compromised endpoints and/or network devices – a Man-In-The-Middle type attack. When Hackers want to listen to VoIP conversations they need to record the media stream. The attack is performed similarly as capturing any other type of traffic travelling across the Internet, finding compromised devices to record directly from or stream the media to a recording device.

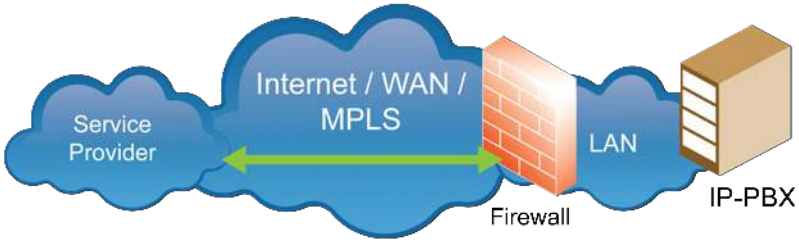


SIP Trunk Security with Firewalls

SIP Trunking is often a Peer to Peer connection for the primary use of delivering PSTN connectivity over VoIP. SIP Trunking is delivered over a couple of different methods, Internet Telephony Service Providers (ITSP) deliver SIP Trunking over the Internet and Managed Service Providers deliver SIP Trunking over the dedicated carriers WAN connections. The application of security solutions involves providing a Firewall in combination with an IP-PBX that are used to define the Peer to Peer relationship at various networks and VoIP application layers, and also ensuring signaling and media are secure as well.



In the example below, the IP-PBX resides behind a typical network Firewall. The Firewall is the border element between Internet or Untrusted Network Zones and Local Area Networks or Trusted Zones. The Firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

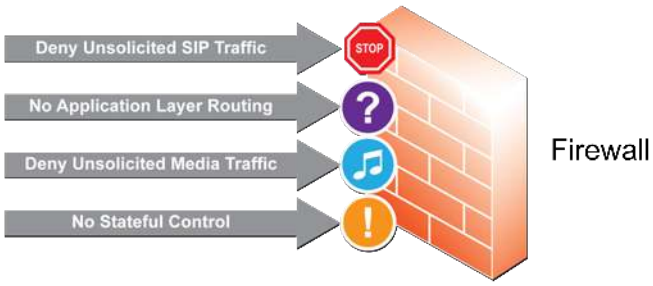


Firewall Features & Setup

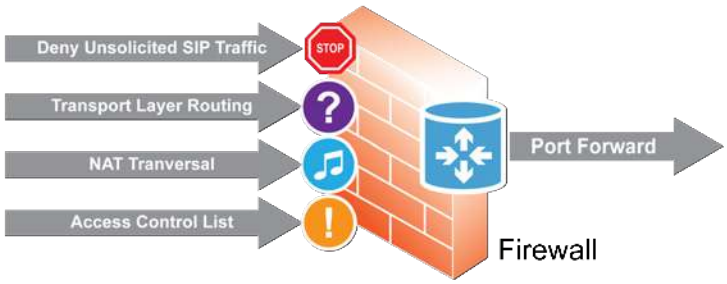
The Firewall controls the traffic by redirecting SIP signaling and Audio Media streams to the defined destinations. In this solution the Firewall is controlling communications for allowing SIP Trunk traffic from carriers to be directed into the IP-PBX.

Port Forwarding

One of the primary functions of a Firewall is to Deny ALL unsolicited traffic from Untrusted Networks.



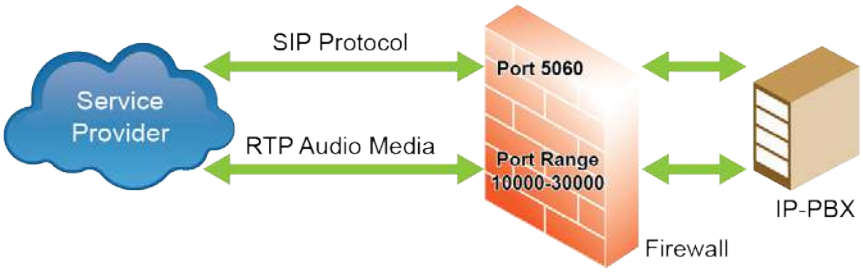
To work around this, firewalls provide Port Forwarding or Port Mapping that redirects a communication request from one UDP/TCP IP address and port number combination, to another while the packets are traversing a Firewall. Also, Port Forwarding and NAT does not validate or inspect if the packet being sent is the application for intended use. If the Firewall receives ***any*** UDP or TCP packet, it will redirect the packet to the defined destination, no matter the content within the packet.



Access Control Lists

Instead of allowing any packet to redirect through the firewall with Port Forwarding, the firewall typically has configuration that will define a Source IP Address(es), whereby the UDP/TCP packet within the Source IP Address must match the defined value. Essentially creating an Access Control List (ACL), which is useful in the Peer to Peer SIP Trunking application as one peers IP Address can be accepted and redirect to a defined destination. The limitation is the use of Domains, where the source IP address can be dynamic.

SIP Protocol typically operates on UDP/TCP Port 5060. SIP signaling messages are sent from one peer and redirected to another peer on this UDP/TCP port. Thus, setting up a Port Forward of the SIP Protocol from one peer to another to allow the SIP messaging. Audio Media RTP Packets can operate on any UDP port, but typically from 10,000 up to 30,000. That is a tremendous amount of ports to Port Forward and could limit other applications use of these ports. This is not always a viable solution, and not very secure as tens of thousands of ports are open on the firewall and directed to the IP-PBX.



In addition, spoofing source IP Address is the most common and easiest ways to bypass Access Control Lists on Firewalls, it is easy to setup spoofing IP Addresses on many computer operating systems. Be aware that ACL should not be the only security feature in operation. Keep in mind that SIP Protocol is an Application Layer protocol of the OSI Model and addressing is independent of Transport Layer IP Addresses. Spoofing the IP Address will have little to no effect on the SIP Addressing of the VoIP.

SIP ALG

Some Firewalls have a built in SIP Protocol Application Layer Gateway (ALG), also called SIP Helpers. SIP Protocol resides in the Application Layer of the OSI Model. A SIP ALG is a basic SIP Protocol Application feature that changes Private IP Addresses to Public IP Address. ALGs are rudimentary at best, they are stateless as they don't understand the state of the call, and often have undesired effects on SIP calls that are more complex than a basic call. It is recommended to turn SIP ALGs off or consider using a Session Border Controller. More importantly, as ALG simply help SIP signaling to traverse NAT'ing firewalls and other Interoperability needs, they typically don't offer any security related features.

IP-PBX Features & Setup

In this scenario, the Firewall is the initial control point for the voice traffic, but the Firewall is not very strong in VoIP Security. Firewalls can provide IP Address level of Security with ACL, but everything else is simply Port Forwarded, which is like Poking a Hole in the Firewall. The IP-PBX will bear the brunt of directed VoIP attacks and will require VoIP security features, the IP-PBX becomes the main

VoIP Security device. This may cause the IP-PBX to use valuable IP-PBX Server resources, such as CPU and Memory for running the VoIP communications of the business and CPU dedicated to preventing an attack.

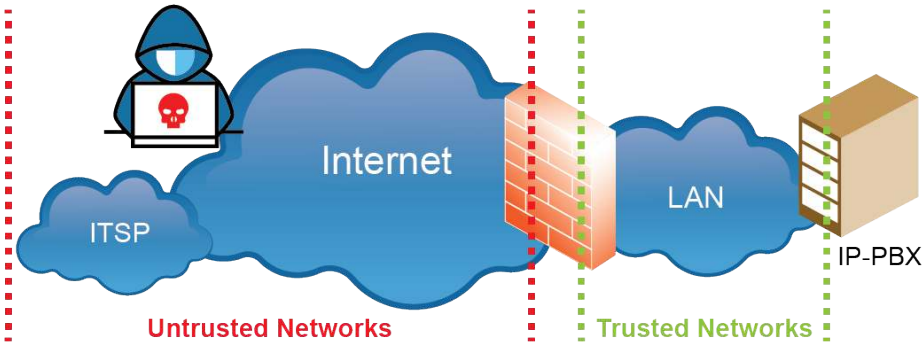
The Firewall will assist in securing the VoIP environment, but this solution the IP-PBX has a major role to play in securing the overall VoIP environment.

IP-PBX Firewall

As we discussed earlier, a Firewall is a network security application that monitors and controls incoming and outgoing network traffic based on predetermined security rules. When a Firewall is imbedded as an application within an IP-PBX, the Firewall typically establishes a barrier between a trusted internal network and untrusted outside network, such as the Internet. A Firewall on the IP-PBX is focused on network identifications and determining if these networks are Trusted or Untrusted and applying access policies.

IP-PBX Firewalls must also responsive to VoIP, where if the registration attempt from a Phone or Peer is successful, the remote host is then added to a 'Known Good' zone, that has permission to use that protocol, and is additionally granted access to UCP, if UCP is enabled. If the incoming connection attempts are invalid from the Phone or Peer, traffic from that source device will be dropped for a short period of time. If attempts to authenticate continue without success, the attacking host will be blocked.

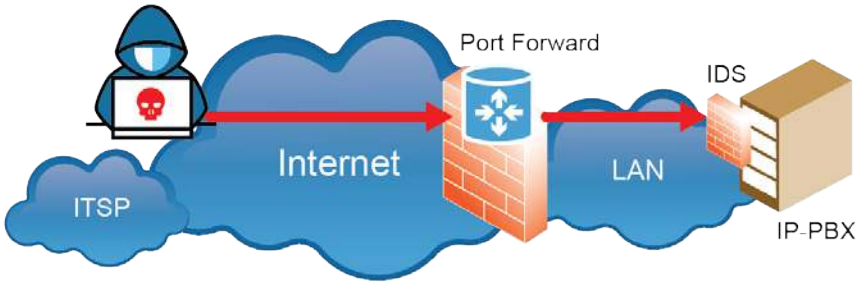
IP-PBX Firewalls must also be flexible in defining Trusted and Untrusted Zones not only for VoIP Services like SIP and RTP, but also for other management and configuration services like SSH and HTTP. For example, to Allow SSH and HTTP on local Trusted Zones, but not Untrusted Zones.



IP-PBX Firewalls must be allowed to predetermine and manage Blacklists. A Blacklist is a list of network addresses that are in a permanent Deny All policy. Where any IP Address(es) defined on the Blacklist will not have any communication with the IP-PBX.

Intrusion Detection

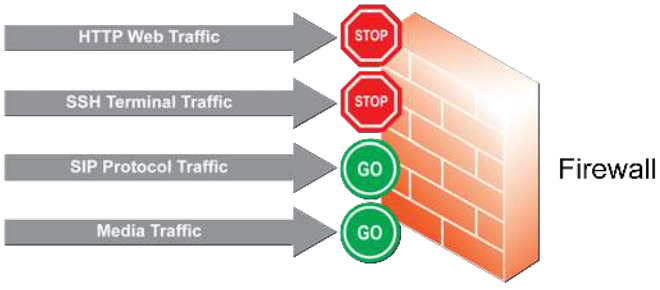
An Intrusion Detection System (IDS) on an IP-PBX is an application that monitors communication into the IP-PBX for malicious activity or policy violations. Any detected activity or violation is typically notified to the IP-PBX administrator. Typical IDS policies include Registration Attempts, Password Failure Attempts, SIP Packet signature detection (known patterns), and anomaly detection (deviations from good traffic). The Intrusion Prevention System (IPS), usually associated with the IDS, acts as the automated response system by proactively denying the malicious activity upon detection. This includes terminating connections and blacklisting offending parties.



Specifically, in this scenario where the IP-PBX resides behind a Firewall and the Firewall is Port Forwarding UDP/TCP traffic to the IP-PBX, the IP-PBX must have IDS/IPS to detect and protect from Registration Attempts, Password Failure Attempts, SIP Packet signature detection, and anomaly detection.

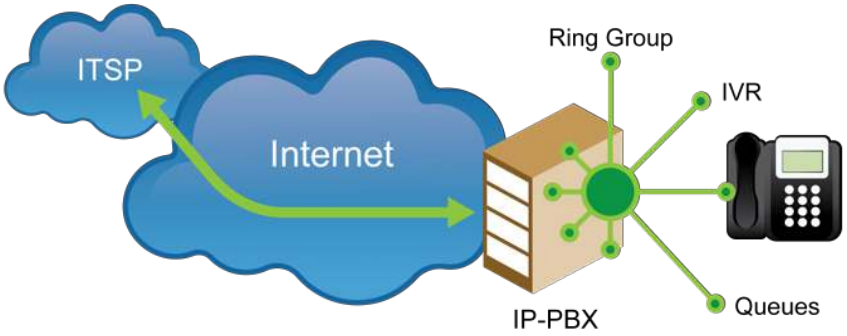
Port Management

Various applications within the IP-PBX use datagram sockets to establish host-to-host communications. An IP-PBX application binds a socket to its endpoint of data transmission, which is a combination of an IP address and a service port. For complete operation of an IP-PBX the Service Ports may include SIP Protocol (5060), HTTP (80), HTTPS (443), FTP (23), SSH (22) and plenty more. It is important to turn on only the Ports needed, and leave the optional Port disabled. Also, where possible, to use custom Ports for common applications, such as HTTP (port 80) for WebGUI Administration access is extremely common, to change to any arbitrary port reduces exposure.



Inbound Routes

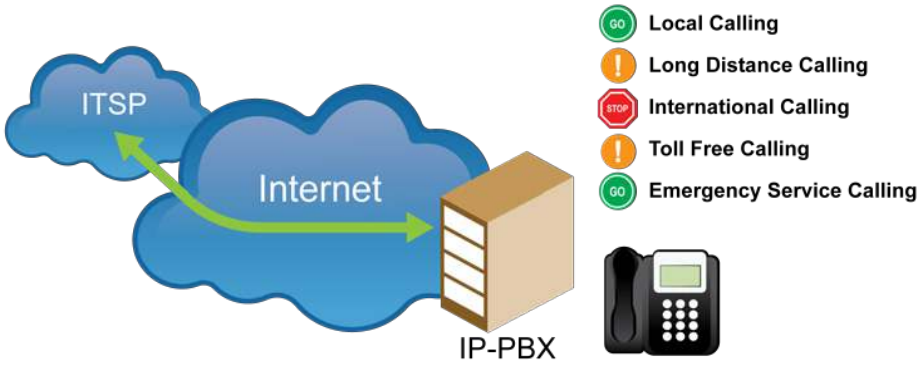
Inbound Routes are important on an IP-PBX for all SIP Trunking applications, as the define where calls from Service Providers are to be routed within the IP-PBX. The important concept for Security within an Inbound Route is not to leave any ambiguity in the Inbound Route, make sure that every inbound Direct Inward Dialed (DID) number has a legitimate answer point. Not having directed answer points may lead to unknown and vulnerable routing within the IP-PBX.



All Inbound Routes are typically configured to accept call requests directly from the Service Provider, as the Firewall, which sits in between has simply a Port Forward to direct traffic from the Service Provider directly to the IP-PBX.

SIP Trunks & Outbound Routes

As Inbound Calls are managed by the Firewalls Port Forward and the IP-PBX Inbound Routes, call for the Outbound direction needs some consideration. SIP Trunks are setup to communicate with the Service Provider directly, all Interop Settings, and other CallerID is all managed directly on the IP-PBX. The IP-PBX will send calls directly to the IP Address or FQDN of the Service Provider. The Firewall is typically the Default Gateway of the LAN, thus all traffic is naturally routed out the Firewall. Firewalls are not typically setup to deny outgoing traffic, so there is no need to consider Port Forwarding for outgoing traffic.



Outbound Routes need to consider Numbers Dialed by use of Class of Service or other methods, to restrict International Dialing to trusted endpoints.

IVR & Voicemail

SIP Trunk calls inevitably land in an IVR/Auto Attendant or in someone's voicemail box, it is important to ensure that the configuration of these two IP-PBX features don't allow hackers to call back out again. For example, dialing into an IVR, Pressing the DTMF digit 9 followed by any number and utilizing that open line to call back out to the PSTN. Some voicemail boxes have similar IVR like features to redirect calls to other numbers.

Passwords

Security is fundamentally based on the strength of the Passwords. All the different applications need the consideration of a good strong password policy - passwords such as User Web Passwords, Device & Phone Passwords, Authentication Passwords, and others. Review and enforce strong password policies that are long and robust, in addition to having policies to regularly change passwords. Specific to SIP Trunking, passwords can be around Service Provider User Accounts, IP-PBX User & Admin Accounts, and other secondary breaches where hackers can collect information about your SIP Trunking Service.

SIP Trunk Authentication

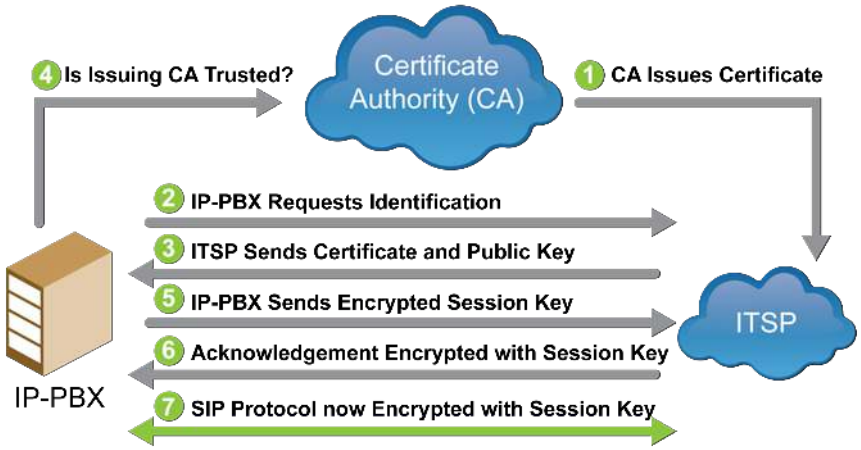
Many SIP Trunk Service Providers will require a level of Authentication within the SIP Trunk. The Service Provider requires Registration Authentication and Call Initiation Authentication from the IP-PBX. When the IP-PBX initiates a call to the Service Provider, the IP-PBX must provide Authentication within the SIP Protocol for the Service Provider to accept and process the call. This is a good step in conjunction with Access Control Lists, as the ACL will check the source peer IP address, then the application will check the SIP Protocol Authentication before processing the call.

This addresses the upstream call but does not address the downstream call – calls into the IP-PBX. Unfortunately, not many Service Providers can provide Authentication in the downstream direction.

TLS & SRTP

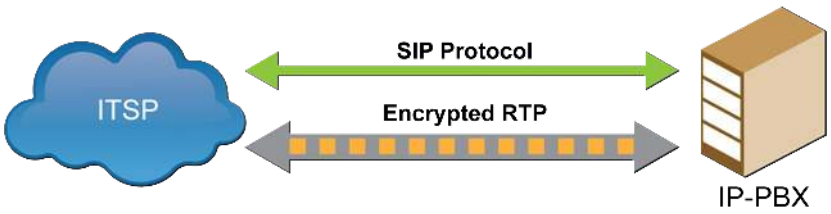
Transport Layer Security (TLS) and Secure RTP (SRTP) are encryption of the SIP Protocol and Audio Media stream respectively.

TLS is a Peer to Peer transport – using TCP, where the peers use a handshake with an encryption key (CA Certificate) and an asymmetric cipher to establish not only cipher settings but also a session-specific shared key with which further communication is encrypted using a symmetric cipher. TLS typically relies on a set of trusted third-party certificate authorities to establish the authenticity of CA Certificates.



In a SIP Trunking solution, TLS between the IP-PBX and the Service Provider will encrypt all the SIP Signaling. Contained within the SIP Signaling is all the CallerID, Media setup and other pertinent information useful to a hacker. When SIP is encrypted, there is nothing for the hacker to see.

SRTP is also Peer to Peer, but as Media RTP uses UDP Transport, the setup is a bit different than TLS which uses TCP. Contained within the SIP signaling is the SRTP setup of the media stream, then the devices sends RTP that is encrypted. If the hacker does not have the SIP Signaling they cannot decode the media stream.



In a SIP Trunking solution, SRTP is great to encrypt the Media Stream to ensure there is no eavesdropping of the audio.

Pros & Cons

In this security solution where you are providing security for a SIP Trunk with a Firewall and features available on an IP-PBX, there are some advantages and disadvantages. Take note that the IP-PBX must be regarded as a 'Mission Critical' application, with direct ties to business operations and revenue.

Pros

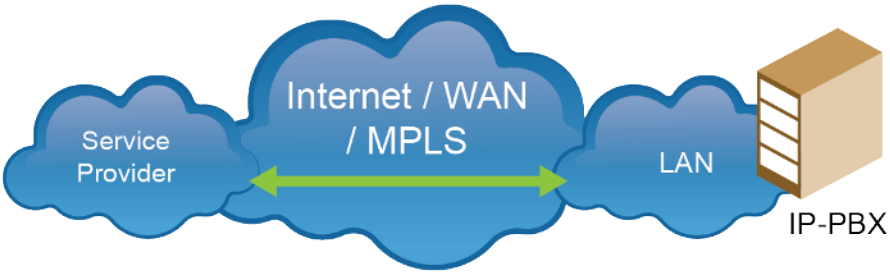
- Simple, Easy and common Network Architecture
- Reduced Complexity
- Reduced number of devices to configure

Cons

- IP-PBX must deal with VoIP Security threats directly
- Requires some Firewall configuration knowledge
- Poking Holes in Firewall to route insecure traffic into a Private Network

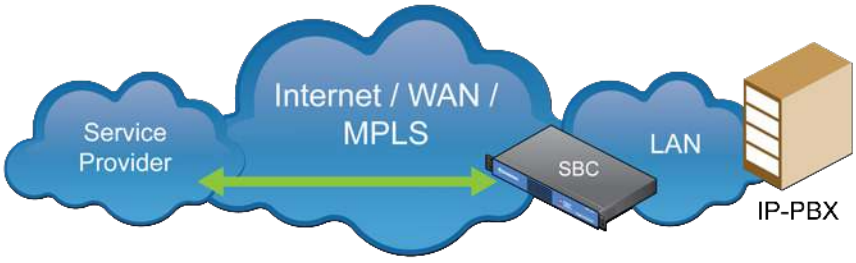
SIP Trunk Security with Session Border Controllers

As discussed in the previous section, SIP Trunking is often a Peer to Peer connection for the primary use of delivering PSTN connectivity over VoIP, and is delivered over a couple of different methods using ITSPs and Managed Service Providers. In this section, the application of security solutions involves providing a Session Border Controller (SBC) element that is used to define the Peer to Peer relationship at various networks and VoIP application layers, and additionally ensuring signaling and media are secure as well.



IP-PBX with SBC

In this example, the IP-PBX resides behind a Session Border Controller (SBC). The SBC is the border element between Internet or Untrusted Network Zones and Local Area Networks or Trusted Zones. The SBC is a network security device as well as a VoIP security device that monitors incoming and outgoing network and voice traffic and decides whether to allow or block specific traffic based on a defined set of network and voice security rules.



SBC Features & Setup

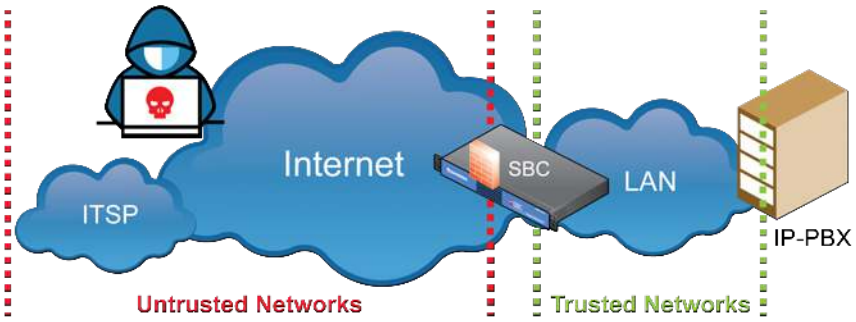
The SBC controls the voice traffic by processing SIP signaling and Audio Media streams to the defined destinations. SBCs typically use B2BUA technology for processing SIP traffic. In this solution, the SBC is intelligently controlling communications for allowing SIP Trunk traffic from carriers, to be directed to the IP-PBX.

There are many VoIP Security features the SBC adds to the SIP Trunk call flow. One of the SBCs primary functions is to provide VoIP Security, analyzing and protecting mission critical VoIP

applications from malicious activity, so these mission critical applications are protected from direct attacks. There are several different security features on the SBC to ensure complete coverage.

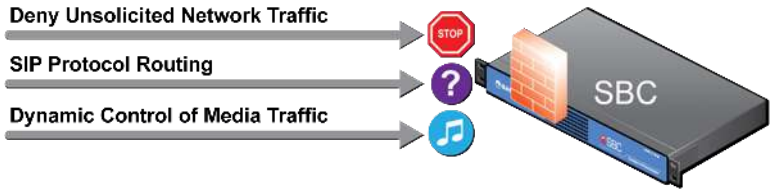
SBC Firewall

SBCs integrate many Firewall features as important components to ensure overall security of the platform and VoIP Solution. SBCs often reside between Trusted and Untrusted Networks, having an integrated Firewall allows the SBC to protect itself, as well as trusted internal networks, from malicious activities.



Firewalls on their own introduce a few challenges with VoIP as discussed earlier. There are major benefits when a Firewall is integrated within an SBC. Some benefits included: NAT'ing issues when using SIP Protocol are resolved, poking holes in the firewalls using Port Forwarding is no longer required and VoIP routing and addressing are vastly improved.

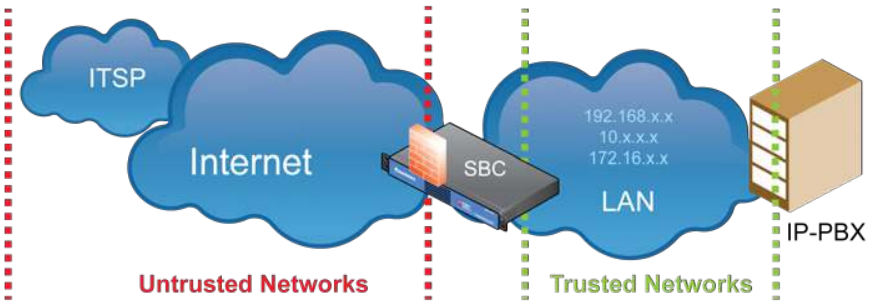
Firewalls integrated within SBCs provide similar features as Firewalls deployed on their own. Keeping ALL UDP/TCP ports closed and inaccessible, except for the few that are needed for VoIP.



Topology Hiding

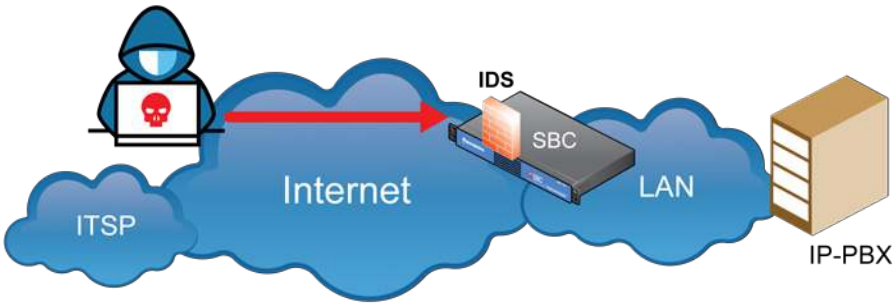
Network Address Translation (RFC 2663) is a method of remapping one IP address space into another by modifying network address information in TCP/UDP packets. NAT is a Network Layer IP Address translation, not an Application Layer translation. But the SIP Protocol (Application Layer) also needs a method of remapping one IP address space into another by modifying network address information in the SIP Protocol.

The typical use case of Topology Hiding is for the SBC to hide private & trusted networks from public & untrusted networks. It is important for the SBC to hide the private addresses within the SIP Protocol.



IDS/IPS

An Intrusion Detection System (IDS) on an SBC is an application that monitors communication into the SBC for known types of malicious activity or policy violations. Any detected activity or violation is typically noted and the SBC administrator is notified. Typical IDS policies include Registration Attempts, Password Failure Attempts, SIP Packet signature detection (known patterns), and anomaly detection (deviations from good traffic). The Intrusion Prevention System (IPS), usually associated with the IDS, is the automated response system, proactively denying the malicious activity upon detection. This includes terminating connections and blacklisting offending parties.

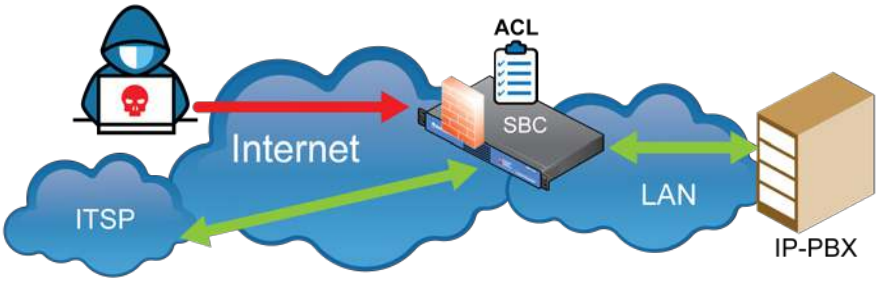


Specifically, in this scenario where the SBC resides in front of the PBX and connected to public internet traffic, the SBC must have IDS/IPS to detect and protect from Registration Attempts, Password Failure Attempts, SIP Packet signature detection, and anomaly detection. Having the SBC in front of the IP-PBX, ensures that the “Mission-Critical’ Call Control is not having to manage the attack directly, further protecting the valuable voice application.

Access Control Lists

Access Control List is a list of permissions attached to the SBC, whereby the SBC grants access to specific IP Addresses. ACLs are great for SIP Trunking applications. Trunking has a lot to do about communication with known peers. These peers are SIP Trunking Service Providers, other SBCs, other IP-PBX s, and specific End-points. These peers are static and have specific and never changing IP

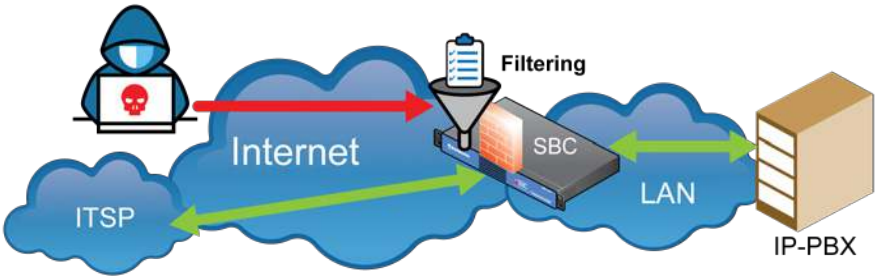
Addresses or FQDNs. This allows for the creation of ACLs, where the SBC can define precisely which IP Addresses from known trusted trunking peers can have access to the SBC.



Keep in mind that SIP Protocol is an Application Layer protocol, and not a Transport Layer (TCP/IP) protocol, and that ACLs operate at the TCP/IP Layer, resulting in obvious VoIP malicious activity where spoofing source IP Addresses is a common attack to overcome ACLs and keep SIP actively processing calls. Further control of the SIP Protocol can be done in the next few sections, SIP Filtering, CAC and SIP Request Rate Limiting as these are SIP Protocol filtering methods.

SIP Filtering

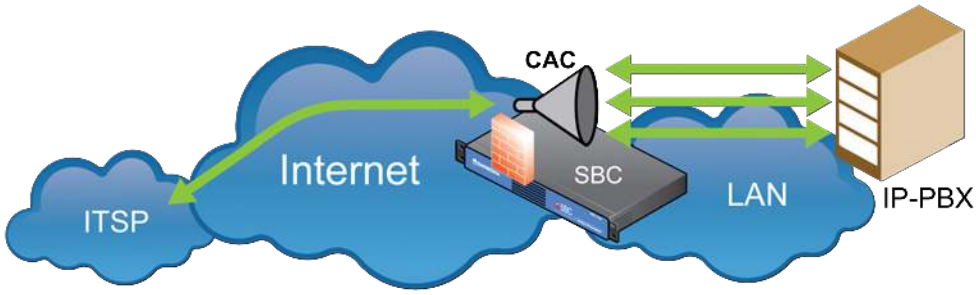
One of the components of a SIP Reconnaissance attack is to scan networks with SIP REGISTERs to determine if there is an IP-PBX available to register with. SIP Filtering allows the SBC to apply filters to the REGISTER SIP Method, filters to remove REGISTERs based on Source IP Addresses, SIP Accounts, and User-Agent Header. In many cases, SIP Reconnaissance attacks are made using known applications, such as SIPvicious and SIP-CLI. These have known User-Agent headers that can be identified and filtered.



Call Admission Control

Call Admission Control is used as a proactive Security feature in an SBC, but more towards a restriction of traffic in case there is a security breach, limiting the exposure to a specified Call Rate Limit. Understanding the business requirements for Call Rates, and then using CAC to ensure that these call rates are never exceeded is important. For use in SIP Trunking, this ensures that for both Carrier deployments and Enterprise deployments, pre-determined Call Rates are not exceeded to

upstream or downstream trunking peers. When a breach occurs, there is a hard limit to trunking call rates, so as not to over extend the service.



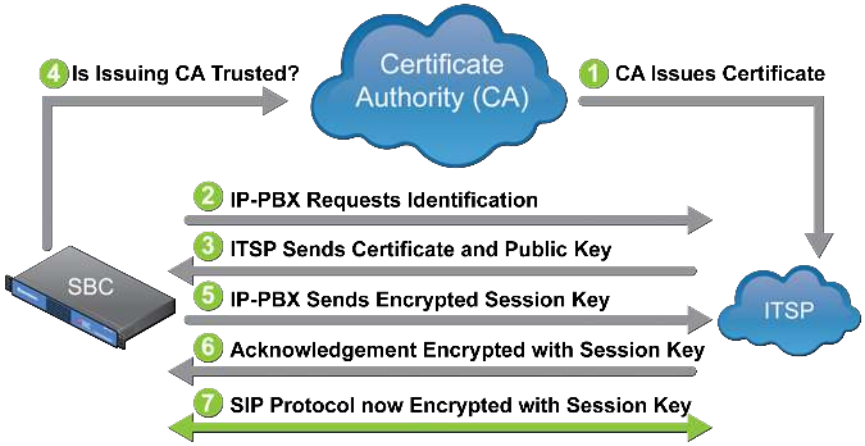
SIP Request Rate Limiting

Similar to Call Admission Control, SIP Request Rate Limiting operates at a lower level, looking at the individual SIP Requests within the SIP Protocol, like INVITE, REGISTER, SUBSCRIBE, NOTIFY, BYE and others. SIP Request Rate Limiting applies a rate limit to any of the SIP Protocol. For the SIP Trunking application, this can be applied to limit any sort of Denial of Service attack at the SIP Protocol level, and also to further scrutinize any trunking traffic to specified rate limits.

TLS & SRTP

Transport Layer Security (TLS) and Secure RTP (SRTP) are encryption of the SIP Protocol and Audio Media stream respectively.

TLS is a Peer to Peer transport – using TCP, where the peers use a handshake with an encryption key (CA Certificate) and an asymmetric cipher to establish not only cipher settings but also a session-specific shared key with which further communication is encrypted using a symmetric cipher. TLS typically relies on a set of trusted third-party certificate authorities to establish the authenticity of CA Certificates.



In a SIP Trunking solution, TLS between the SBC and the Service Provider will encrypt all of the SIP Signaling. Contained within the SIP Signaling is all the CallerID, Media setup and other pertinent information useful to a hacker. When SIP is encrypted, there is nothing for the hacker to see. This is useful when the IP-PBX does not support TLS, or when the SBC is in place providing other benefits and TLS is needed.

SRTP is also a Peer to Peer, but as Media RTP uses UDP Transport, the setup is a bit different than TLS which uses TCP. Contained within the SIP signaling is the SRTP setup of the media stream, then the devices send RTP that is encrypted. If the hacker does not have the SIP Signaling they cannot decode the media stream.

In a SIP Trunking solution, SRTP is great to encrypt the Media Stream to ensure there is no eavesdropping of the audio.

Peering & Authentication

Many SIP Trunk Service Providers will require a level of Authentication within the SIP Trunk. Where the Service Provider requires Registration Authentication and Call Initiation Authentication from the SBC. When the SBC initiates a call to the Service Provider, the SBC must provide Authentication within the SIP Protocol for the Service Provider to accept and process the call. This is a good step in conjunction with Access Control Lists, as the ACL will check the source peer IP Address, then the application will check the SIP Protocol Authentication before processing the call.

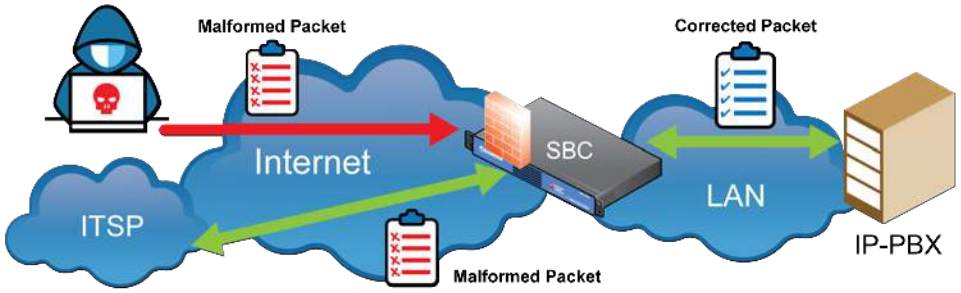
This is for the upstream call but does not address the downstream call – calls into the SBC. Unfortunately, not many Service Providers can provide Authentication in the downstream direction.

Interoperability

Although Interoperability settings are not specific to Security, interop settings are one of the primary features of an SBC. SBCs are designed to maximize customization and integration with any Service Provider or vendor application. In addition, SBCs are designed to be able to change and manipulate SIP Protocol to ensure that any vendor equipment can communication to any other application. In the

SIP Trunking application, this allows for any IP-PBX to connect to any Service Provider, ensuring that each of the different SIP deployments have the needed SIP communications to integrate with each other.

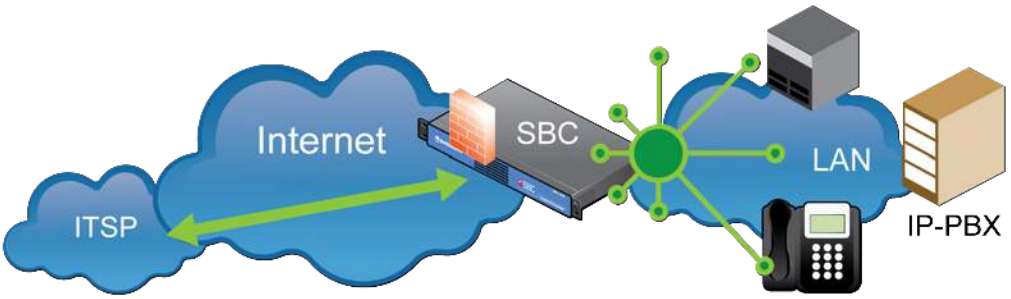
Leveraging the ability of the SBC to rewrite SIP packets, one security interop feature the SBC can provide is the detection and correction of Malformed SIP Packets. One type of VoIP Attack is a Fuzzy Attack, whereby SIP Packets are sent knowingly malformed in an attempt to provoke an undesired behavior, such as a device reset or lockup. SBCs can ensure that all SIP Packets received are corrected automatically and conform to the SIP Protocol standard.



There are many different VoIP equipment vendors deployed around the world and no common deployment style of SIP Trunking. Each Service Providers uses countless variations of features and deployment styles to deploy SIP Trunking, making connecting to SIP Trunking Service Providers quite diverse. The SBC ensures that no matter the provider or vendor, the tools are available to connect.

Flexible & Resilient Routing

In terms of Security, it is important to secure the routing within the SBC. Strict definitions of Source and Destination dial plan patterns. Accepting calls from known peers with known numbers and accounts and routing the VoIP calls to defined trusted destinations. Don't leave open ended and catch-all dial plan patterns that will collect any dialed number and process the call through the SBC. In the trunking scenario, if you are expecting only 10-digit numbers being dialed, then set up a dial plan that only accepts 10-digit numbers. This prevents the possibility of malicious calls for numbers of longer or shorter lengths, such as International dialing which can require more digits. There are other examples that need consideration, such as Toll Free, International, Long-Distance and specific country numbering plans for dial plan patterns. Prevention of illegitimate number dialing is important to trunking solutions.



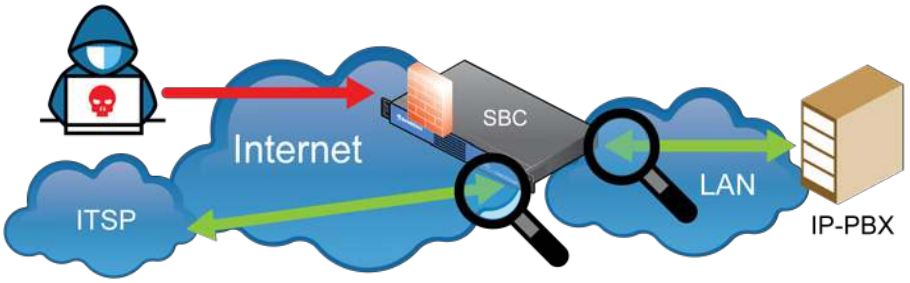
SBC's also provide the ability for Primary and Secondary flexible routing, should the Primary destination be unavailable, the SBC can reinitiate the call with a Secondary destination to ensure communications.

Transcoding & Dynamic Media Port Allocation

Transcoding is a common SBC feature that changes one codec to another within a VoIP call. More importantly, for security purposes it is important to constantly change the UDP ports used for VoIP Media. This prevents injecting or modification of a media stream. If the media port were to remain constant, unsolicited and unwanted media can be directed to the media port which may result in unwanted media being heard over the VoIP device.

Troubleshooting

Troubleshooting is not necessarily a Security feature, but it is important to have an SBC with good troubleshooting tools. This allows administrators to quickly and effectively investigate any activity within the SBC. These tools will help Identify malicious traffic and help the administrator make configuration changes to protect the trunking solution. For trunking, the troubleshooting can be directed towards peer identification, dialed numbers, routing, registrations, and several other requirements.



IP-PBX Features & Setup

In this scenario, the SBC is the initial control point for the voice traffic, bearing the brunt of the attacks and security features, but now the IP-PBX can provide a secondary level of security which will complement the SBC and the overall security solution. Also having the SBC as the initial control point

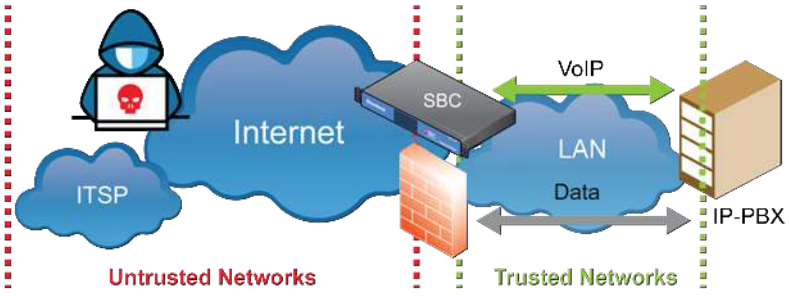
for voice traffic will free up valuable IP-PBX Server resources, such as CPU and Memory for running the VoIP communications of the business, rather than CPU dedicated to preventing an attack.

The more layers of security implemented the more difficult it is for hackers to breach VoIP environments. Every device on a network is responsible to provide a layer of security in order to protect itself and others on the network.

IP-PBX Firewall

Different than just having a Firewall in front of the IP-PBX, the IP-PBX now also has an SBC in addition to the Firewall. The Firewall continues to provide the security protection of VPN, Provisioning, Administrator Web Access, and other typical services, but the SBC adds the additional VoIP security to the Trunking solution. The IP-PBX now communicates with the SBC separately for trunking and other services with the Firewall.

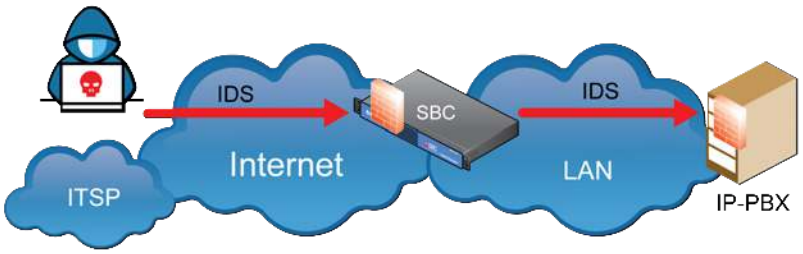
As with the previous section – “IP-PBX with Firewall”, when the IP-PBX was connecting solely with a Firewall, it is important to maintain the Firewall feature on the IP-PBX as there are other applications in use to connect to the IP-PBX and the IP-PBX needs to be protected. The IP-PBX Firewall will continue to focus on network identifications and determining if these networks are Trusted or Untrusted and applying access policies. The IP-PBX Firewall will continue to be responsive to VoIP, but now has an SBC to assist in this role, moving some of this Security requirement to the edge of the Trusted / Untrusted border.



In terms of VoIP, the SBCs can provide the first barrier to predetermine and manage Blacklists through Access Control Lists. And the IP-PBX will be protected by the SBC, ensuring only legitimate VoIP traffic is reaching the IP-PBX. Having the Firewall active on the IP-PBX provides a secondary boundary making breaches in security that much harder.

Intrusion Detection

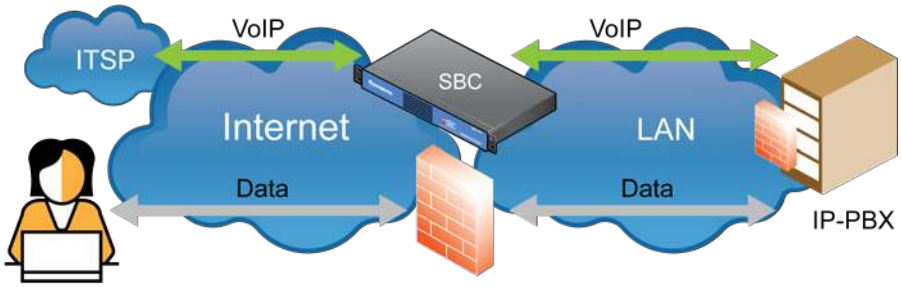
The SBC is also providing an IDS feature for VoIP, moving it out to the border of the Trusted and Untrusted networks.



In this Trunking scenario where the IP-PBX resides behind an SBC, the IP-PBX IDS/IPS is a secondary protection to detect and protect from Registration Attempts, Password Failure Attempts, SIP Packet signature detection, and anomaly detection.

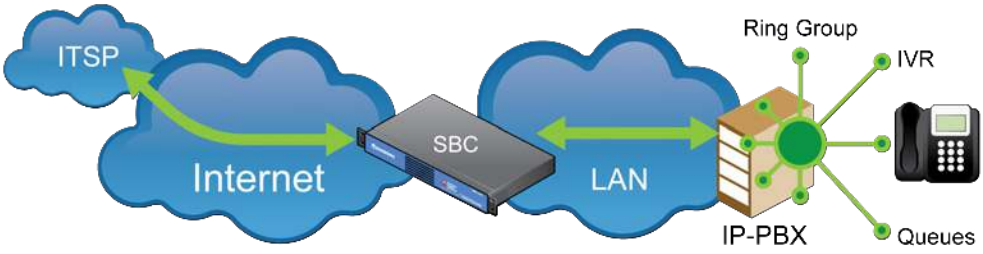
Port Management

In this SBC and Firewall scenario, communications with the IP-PBX, the SIP Trunking is coming from the SBC and other applications will traverse the Firewall. Port Management continues to be important to ensure complete connectivity.



Inbound Routes

Inbound Routes are the same as the previous section – “IP-PBX with Firewall” and are important on an IP-PBX for all SIP Trunking applications, as they define where calls from Service Providers are to be routed within the IP-PBX. The important concept for Security within an Inbound Route is not to leave any ambiguity.

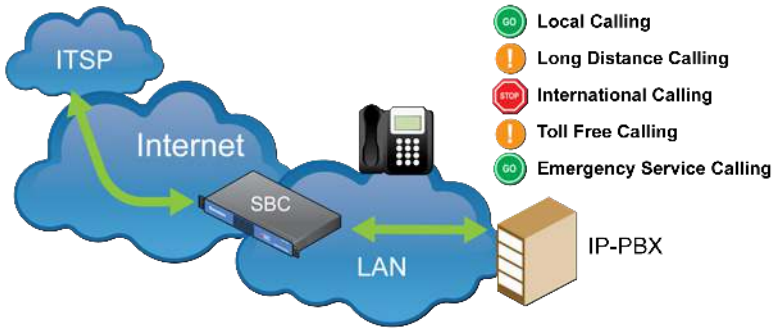


The difference when an SBC is in use, is that all Inbound Routes are typically configured to accept call requests directly from the SBC.

SIP Trunk & Outbound Routes

Outbound Routes from the IP-PBX are now directed to the SBC. SIP Trunks are setup to communicate with the SBC, and in turn the SBC connects with the Service Provider, the SBC provides all the Interop Settings, and other CallerID is all managed directly on the IP-PBX. The SBC can also apply security features towards the IP-PBX, ensuring outgoing policies are enforced.

Understanding Inbound to Outbound Call Flow ensures that there is no Hairpin of calls. Ensure that restrictions are applied to restrict hair-pinning of calls through the IP-PBX.



IVR & Voicemail

IVR & Voicemail setup is the same as the previous section – “IP-PBX with Firewall” and are important on an IP-PBX for all SIP Trunking applications as SIP Trunk calls inevitably land in an IVR/Auto Attendant or in someone voicemail box, it is important to ensure that the configuration of these two IP-PBX features don’t allow hackers to call back out again.

Passwords

Passwords setup is the same as the previous section – “IP-PBX with Firewall” and is important on an IP-PBX for all SIP Trunking applications, Security is fundamentally based on the strength of the Passwords. All the different applications need consideration of a strong password policy. Specific to the SBC and VoIP, any sort of Call Authentication between the SBC and the IP-PBX needs to be considered.

SIP Trunk Authentication

When an SBC resides in front of the IP-PBX, the SBC provides authentication with the SIP Trunk Service Providers and this is a good step in conjunction with Access Control Lists, as the ACL will check the source peer IP address. But this does not exclude the ability to have the IP-PBX authenticate calls from the SBC as a further level of authentication.

The SBC can provide Authentication upstream to the Service Provider, and downstream to the IP-PBX for ultimate SIP Trunking authentication.

TLS & SRTP

Transport Layer Security (TLS) and Secure RTP (SRTP) setup is the same as the previous section – "IP-PBX with Firewall" these are important on an IP-PBX for all SIP Trunking applications. When the SBC resides in front of the IP-PBX for SIP Trunking, all SIP Signaling and Audio Media communications are encrypted, for the ultimate level of secure communications.

In a SIP Trunking solution, TLS is between the IP-PBX and the SBC and in turn the SBC provides TLS to the Service Provider. The SBC will encrypt all of the SIP Signaling in both directions. Similarly, the SBC will provide SRTP in both directions, the IP-PBX will encrypt with the SBC and in turn the SBC will encrypt with the Service Provider.

Pros & Cons

In this security solution, where you are providing security for a SIP Trunk with an SBC prior to sending the VoIP traffic to an IP-PBX, there are some advantages and disadvantages. Take note that the IP-PBX must be regarded as a 'Mission Critical' application, with direct ties to business operations and revenue.

Pros

- Most Secure Trunking deployment
- SBC Provides VoIP Security control point prior to 'Mission Critical' IP-PBX
- Reduced IP-PBX Server resources
- Increase VoIP Security features
- SBC resides on the border between Trusted and Untrusted Networks
- No Untrusted Traffic allowed on Trusted Zones

Cons

- Requires More VoIP Networking and Security complexity
- Requires more understanding of VoIP and Data traffic requirements
- Cost disadvantage in very small VoIP solutions – buying an extra device

Remote IP-Phones Security with Firewalls

A Remote Phone deployment in branch offices or work-at-home employees is completely different than SIP Trunking, Remote Phones are dynamic in location, and require significantly more calling features. Remote Phones cannot be considered as peers, as phones register for services and change IP Addresses often, across multiple devices and locations. Remote Phones require automatic provisioning with file servers and possibly require web access and REST API access to the IP-PBX. The interconnectivity between Remote Phone and IP-PBX is complicated with many communication requirements.

The application of security solutions involves providing a Firewall solution that is used to define the Remote Phone to IP-PBX relationship between various networks using VoIP application layers, file provisioning, and other services, while ensuring signaling and media are secure. Meanwhile, Remote Phones most often are located behind other Firewalls, presenting additional communication issues.

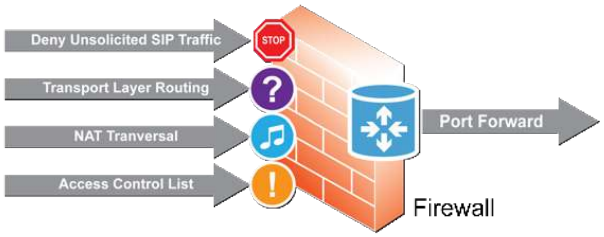
In this example, the IP-PBX resides behind a typical network Firewall. The Firewall is the border element between Internet or Untrusted Network Zones and Local Area Networks or Trusted Zones. The Remote Phone is located on a remote network across the Internet. The Firewall is monitoring network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewall Features & Setup

The Firewall controls the traffic by redirecting SIP signaling and Audio Media streams to the defined destinations. In this solution, the Firewall is controlling communications for allowing SIP VoIP traffic from Remote Phones to be directed to the IP-PBX.

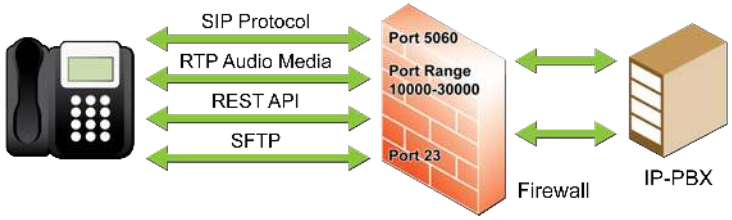
Port Forwarding

As mentioned earlier, one of the primary function of a Firewall is to Deny ALL unsolicited traffic from Untrusted Networks. The Firewall feature Port Forwarding or Port Mapping, will be used to redirect SIP and RTP from the Internal to the IP-PBX. As a reminder, Port Forwarding and NAT do not validate or inspect if the packet being sent is the application for intended use.



In the SIP Trunking application, ACLs can be used to restrict Port Forwarding from specific peers, in the case of Remote Phones, IP Addresses can be dynamic, as residential and mobile networks provide dynamic IP Addresses. Thus, ACLs are required to be open to all Internet traffic, this is not a very secure solution, but necessary for Remote Phones.

Remote Phones, as with SIP Trunking, operate using SIP Protocol. Thus, UDP/TCP Port 5060 will need to be Port Forwarded through the Firewall. Remote Phones send more and different SIP Methods for more phone features. These SIP signaling messages are sent from many different Remote Phones and redirected to the IP-PBX. Remote Phones also send Audio Media RTP Packets, as well as REST API and File Provisioning applications and are used on a variety of different ports. Understanding each application and the TCP/UDP Port requirements is necessary for proper operation.



Note, with Remote Phones the use of ACLs on the Firewall becomes a challenge, as Remote Phone locations are dynamic, thus leaving the Firewall open to all to gain access to the IP-PBX.

SIP ALG

Some Firewalls have a built in SIP Protocol Application Layer Gateway (ALG), also called SIP Helpers. The problem with ALGs with Remote Phones is the complexity of SIP Signaling to/from the Remote Phones. In BLF/SLA, Message Waiting, Transfers, and many other applications where the SIP Signaling is required, the ALG will not provide the needed support. In addition, Remote Phones are most often behind another Firewall, ALG do not provide Far End NAT Traversal (FENT) solutions and would also break any FENT solution provided by the IP-PBX, as it would be re-writing some of the SIP Address information. Recommendation is not to use an ALG in a Remote Phone deployment.

IP-PBX Features & Setup

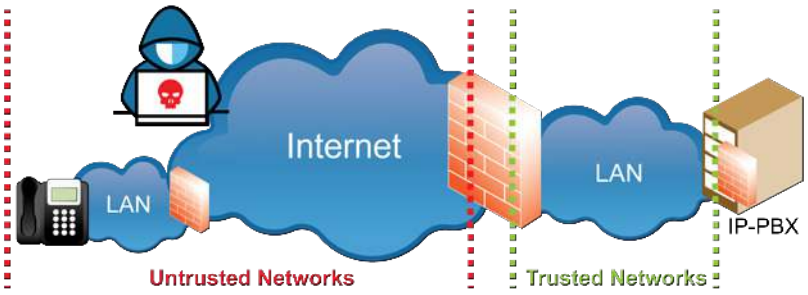
In this scenario, the Firewall is the initial control point for the voice traffic from the Remote Phone, but due to the dynamic nature of Remote Phones changing Source IP Addresses, the Firewall ACL becomes unmanageable to configure thus having open VoIP access to the IP-PBX. Now, the IP-PBX must bear the brunt of the VoIP attacks and will require security features. The IP-PBX will require CPU and Memory for running the VoIP communications of the business and preventing an attack.

IP-PBX Firewall

As previously discussed, with the use of Port Forwarding on the Firewall, the IP-PBX must use its local application Firewall as a network security application that will monitors and control incoming and outgoing network traffic. This IP-PBX Firewall will establish a barrier from the Internet.

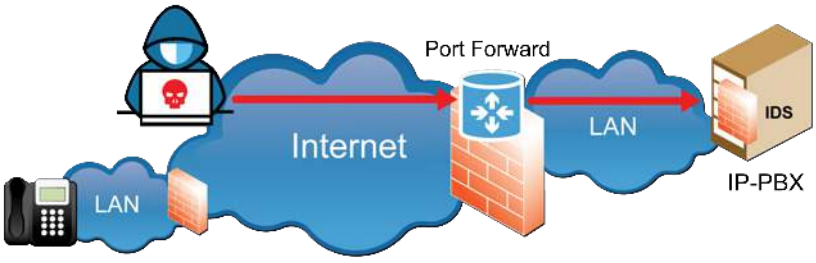
IP-PBX Firewalls will be responsive to VoIP, where if the registration attempt from a Remote Phone is successful, the remote phone is then added to a 'Known Good' zone. If the incoming connection attempts are invalid from the Remote Phone, traffic from that source device will be dropped for a short period of time. If attempts to authenticate continue without success, the attacking remote phone will be blocked.

As Remote Phones require the use of other Services, such as SFTP, FTP, HTTPS and others the IP-PBX Firewalls must also be flexible in defining Trusted and Untrusted Zones for various application Services, such as SSH, HTTP, SIP and others.



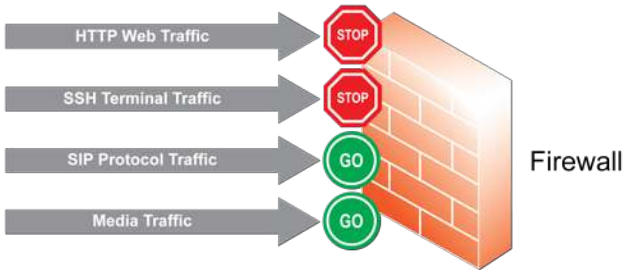
Intrusion Detection

In the Remote Phone solution, ACL on the Firewall are typically left open, this emphasizes the need to ensure that the Intrusion Detection System (IDS) on an IP-PBX is active and monitoring communication into the IP-PBX for malicious activity or policy violations. Registration Attempts, Password Failure Attempts, SIP Packet signature detection (known patterns), and anomaly detection (deviations from good traffic) are all important when connecting remote phones. The Intrusion Prevention System (IPS) will automatically deny the malicious activity upon detection. This includes terminating connections and blacklisting offending parties.



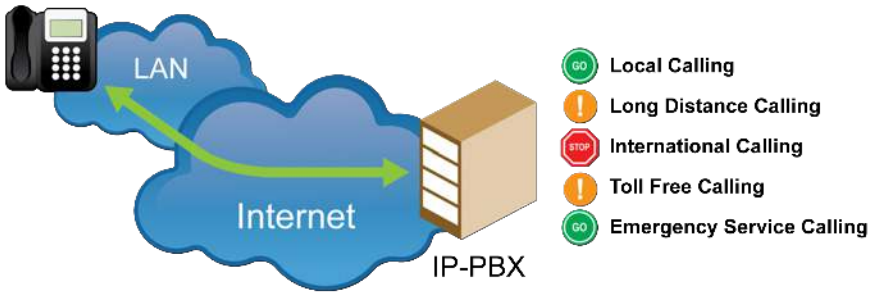
Port Management

Remote Phones will use various applications within the IP-PBX to establish host-to-host communications for applications such as Phone Apps (REST API), File Provisioning (SFTP, HTTPS) and others. It is important to turn on only the Ports needed, and leave the optional Port disabled. Also, where possible, use custom Ports for common applications, such as HTTP (port 80) for WebGUI Administration, changing any arbitrary port reduces exposure.



Class of Service & Outbound Routes

As Remote Phones are not located on the Trusted Network, assigning the Remote Phones into a different Class of Service that restricts them from dialing specific outbound numbers can be a method of securing or restricting traffic. In case there is a breach, there are limitations as to what Remote Phones can dial.



Passwords

Security is fundamentally based on the strength of the Passwords. Remote Phones are required to Register with the IP-PBX, there is a Password assigned to the Remote Phones. A strong password policy is needed for all passwords, such as User Web Passwords, Device & Phone Passwords,

Authentication Passwords, and others. Review regularly, and enforce strong password policies that are long and robust, in addition to having policies to change passwords often. Specific to Remote Phones, passwords can be around Extension Passwords, IP-PBX User & Admin Accounts, and other secondary breaches where hackers can collect information about your IP-PBX Service.

Secure Provisioning

Remote Phones require a configuration to connect with its IP-PBX. Everything needed for the Remote Phone to Register and communicate to the IP-PBX is located in the configuration files. The Remote Phone will access a Provisioning Service on the IP-PBX to obtain its configuration file. Contained within the configuration file is the account, username and password to successfully register to the IP-PBX. Malicious Attackers will attempt to breach the IP-PBX through the Provisioning Service in order to determine the account, username and password to successfully register to the IP-PBX.

Use of HTTPS and SFTP greatly reduce the exposure and compromising of Remote Phone configurations. Both HTTPS and SFTP require the use of Certified Authority Certificates, which the Remote Phones will have but the attacker will not. Use of TFTP and FTP are not recommended as the config files are exposed to everyone.

Remote Phone Security

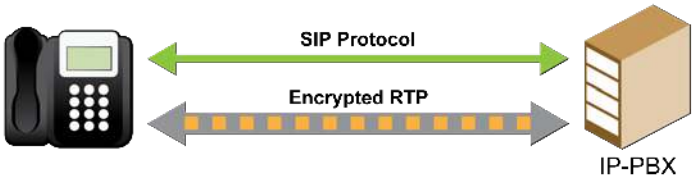
All VoIP phones have the ability to login to the device directly. A WebGUI login within the phone allows for manual configuration, as well as any local troubleshooting on the phone itself. As this is a general Web (HTTP) access to the phone, the phone requires a Username and Password to login. Many Phone vendors have a default Username and Password to login to the phone. This is a security problem that needs attention, as Malicious attackers will breach the Remote Phone directly, login, and collect the Account, Username and Password of the phone, then take this information and breach the IP-PBX with their own equipment. It is important to change the local phone default login credentials.

TLS & SRTP

As discussed previously, Transport Layer Security (TLS) and Secure RTP (SRTP) are encryption of the SIP Protocol and Audio Media stream respectively.

In a Remote Phone solution, TLS between the IP-PBX and the Remote Phone will encrypt the SIP Signaling. Contained within the SIP Signaling is all the CallerID, Authentication, Media setup and other pertinent information useful to a hacker. When SIP is encrypted, there is nothing for the hacker to see.

SRTP is also a benefit as the IP-PBX and the Remote Phone negotiate the SRTP setup of the media stream, then the devices send RTP that is encrypted. The hacker cannot decode the media stream.



In a Remote Phone solution, SRTP is great to encrypt the Media Stream to ensure there is no eavesdropping of the audio.

Pros & Cons

In this security solution where you are providing security for Remote Phones with a Firewall prior to sending the VoIP traffic to an IP-PBX, there are some advantages and disadvantages. Take note that the IP-PBX must be regarded as a 'Mission Critical' application, with direct ties to business operations and revenue.

Pros

- Simple, Easy and common Network Architecture
- Reduced Complexity
- Reduced number of devices to configure

Cons

- IP-PBX must deal with VoIP Security threats directly
- Lack of good use of an ACL on Firewall
- Poking Holes in Firewall to route insecure traffic into a Private Network
- Local & Remote Firewall traversal issues
- Firewall ALG is useless in this scenario

Remote IP-Phones Security with SBC

A Remote Phone deployment is completely different than SIP Trunking, Remote Phones are dynamic in location, and require significantly more calling features. Remote Phones cannot be considered as peers, since phones register for services and change IP Addresses often across multiple devices and locations. Remote Phones require automatic provisioning with file servers and possibly require web access and REST API access to the IP-PBX. The interconnectivity between Remote Phone and IP-PBX is complicated with many communication requirements.

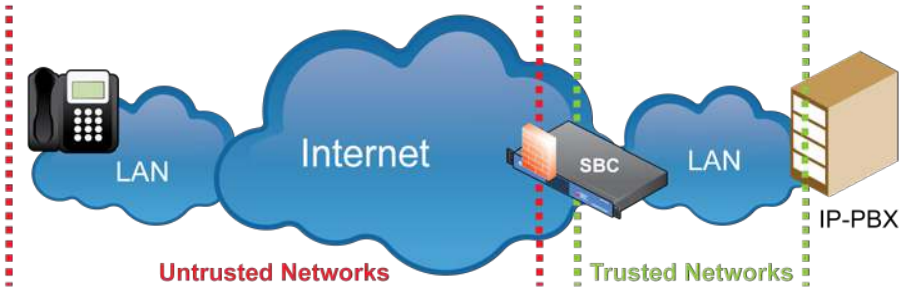
The application of security solutions involves providing an SBC solution that is used to define the Remote Phone to the IP-PBX relationship between various networks using VoIP application layers, file provisioning, and other services while ensuring signaling and media are secure. This method highlights the strength of the SBC to protect the IP-PBX, while providing solutions for Remote Phones located behind other Firewalls.

In this example, the IP-PBX resides behind a Session Border Controller (SBC). The SBC is the border element between Internet or Untrusted Network Zones and Local Area Networks or Trusted Zones. The SBC is a network security device as well as a VoIP security device that monitors incoming and outgoing network and voice traffic and decides whether to allow or block specific traffic based on a defined set of network and voice security rules.

SBC Features & Setup

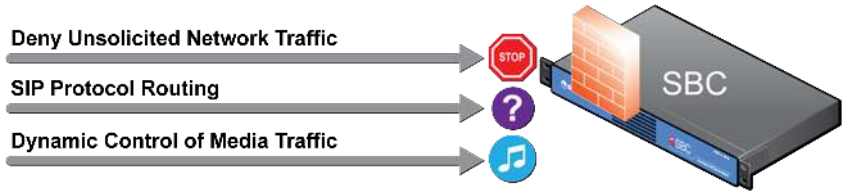
The SBC controls the Remote Phone voice traffic by processing SIP signaling and Audio Media streams to the IP-PBX. In this Remote Phone solution, the SBC is intelligently controlling communications for allowing VoIP traffic from Remote Phones into the IP-PBX.

There are many VoIP Security features the SBC adds to this VoIP call flow. The SBCs continues to provide VoIP Security, analyzing and protecting mission critical VoIP applications from malicious activity, protecting these mission critical IP-PBX applications from direct attacks.



SBC Firewall

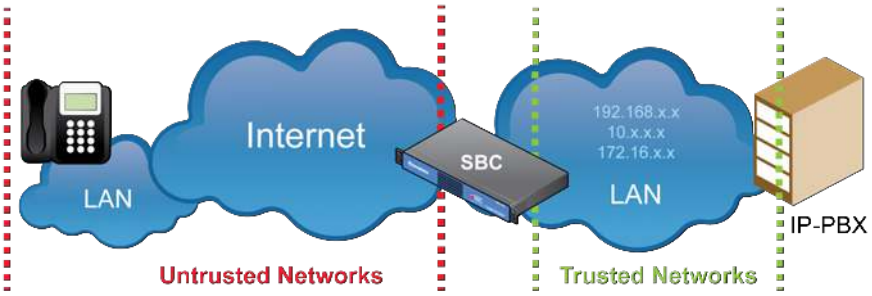
As with the SIP Trunking solution, the Remote Phone solution SBCs integrate Firewalls as an important component to ensure overall security of the platform and VoIP Solution. SBCs continues to reside between Trusted and Untrusted Networks, having an integrated Firewall allows the SBC to protect itself, as well as trusted internal networks from malicious activities.



Topology Hiding

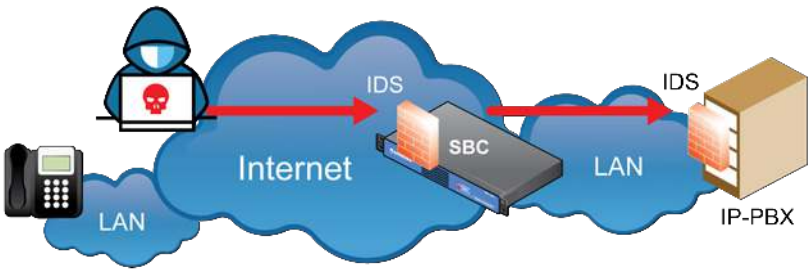
As with the SIP Trunking solution, the SBC continues to provide Topology Hiding, to hide private & trusted networks from public & untrusted networks. It is important for the SBC to hide the private addresses within the SIP Protocol. Remote Phones will only access the Public Internet side of the SBC, and don't need knowledge of the IP-PBX private IP Address. This keeps the IP-PBX hidden from attackers.

The Firewall controls the traffic by redirecting SIP signaling and Audio Media streams to the defined destinations. In this solution the Firewall is controlling communications for allowing SIP Trunk traffic from carriers to be directed to the IP-PBX.



IDS/IPS

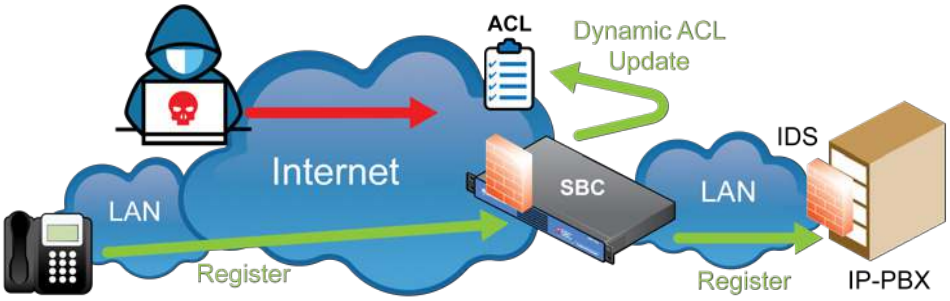
As with the SIP Trunking solution, the SBC continues to provide Intrusion Detection System (IDS). The SBC monitors communication into the SBC for known types of malicious activity or policy violations. The SBCs IDS policies include Registration Attempts, Password Failure Attempts, SIP Packet signature detection (known patterns), and anomaly detection (deviations from good traffic). The Intrusion Prevention System (IPS), will automatically respond by proactively denying the malicious activity upon detection. This includes terminating connections and blacklisting offending parties



In this Remote Phone scenario, where the SBC resides in front of the IP-PBX, the SBC must have IDS/IPS to detect and protect from Registration Attempts, Password Failure Attempts, SIP Packet signature detection, and anomaly detection. Having the SBC in front of the IP-PBX, ensure that the “Mission-Critical’ Call Control is not having to manage the attack directly, further protecting the valuable voice application.

Access Control Lists

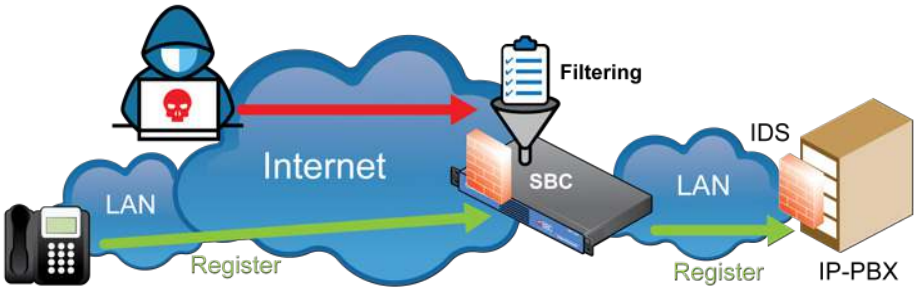
Access Control Lists define a specific list of IP addresses that will grant access. With Remote Phone deployments, it is difficult to define specific IP Addresses as Residential and mobile IP Addresses are constantly changing. Thus, static ACLs are not very good for Remote Phone applications. But, an advantage of SBCs over Firewalls and other security devices, is that an SBC combines Stateful SIP knowledge and Dynamic ACL control. SBCs can use features to monitor the state of Registrations, and once there is a successful registration of a phone, the SBC dynamically assigns the IP Address from the successful registration to the ACL list to grant access for further VoIP communications.



Keep in mind that SIP Protocol is an Application Layer protocol, and not a Transport Layer (TCP/IP) protocol. With SBCs controling both the SIP and ACLs, the SBC can effectively control traffic of dynamic remote phone solutions.

SIP Filtering

Very important to the security of Remote Phone deployments and the protection of the IP-PBX is the ability to stop SIP Reconnaissance attacks by detecting REGISTERs being used to determine if there is an IP-PBX available to register with. SIP Filtering allows the SBC to apply filters to the REGISTER SIP Method, filters to remove REGISTERs based on Source IP Addresses, SIP Accounts, and the User-Agent Header. In many cases, SIP Reconnaissance attacks are made using known applications, such as SIPvicious and SIP-CLI. These have known User-Agent headers that can be identified and filtered.

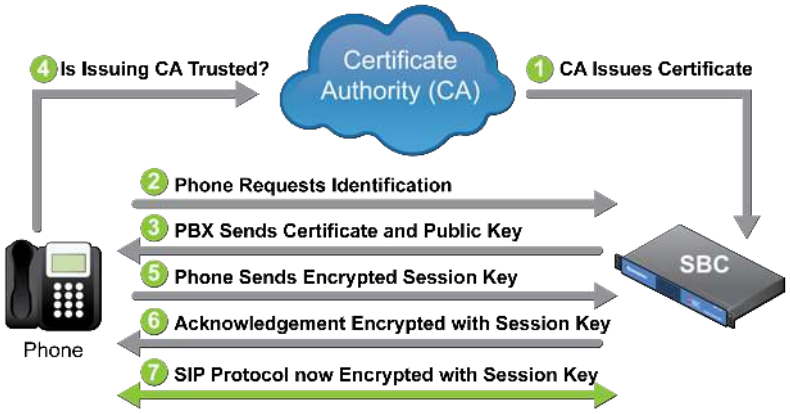


SIP Request Rate Limiting

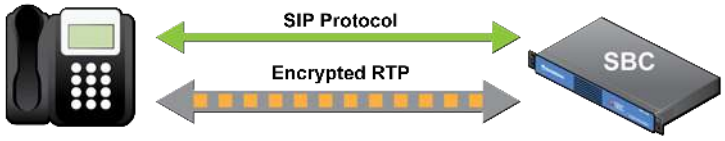
Remote Phone solutions have a significant increase in the complexity and quantity of SIP Signaling, for use with BLF/SLA buttons, Message Waiting, Transfers, Conferences and more. SIP Request Rate Limiting looks at the individual SIP Requests within the SIP Protocol, like INVITE, REGISTER, SUBSCRIBE, NOTIFY, BYE and others. SIP Request Rate Limiting applies a rate limit to any of the SIP Protocol. For the Remote Phones application, this can be applied to limit any sort of Denial of Service attack at the SIP Protocol level, and also to further scrutinize any VoIP traffic to specified rate limits.

TLS & SRTP

Transport Layer Security (TLS) and Secure RTP (SRTP) are encryption of the SIP Protocol and Audio Media stream respectively. TLS is a Peer to Peer transport – using TCP, where the Remote Phone and the SBC use a handshake with an encryption key (CA Certificate).



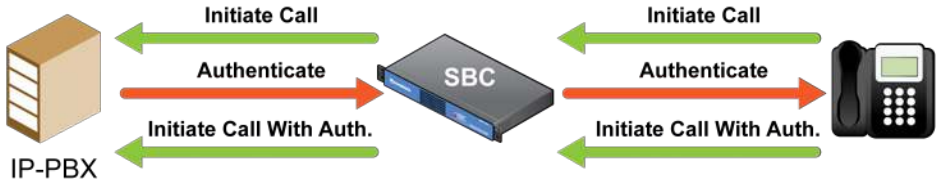
In a Remote Phone solution, TLS between the SBC and the Remote Phone will encrypt all SIP Signaling. When SIP is encrypted, there is nothing for the hacker to see. This is useful when the IP-PBX does not support TLS, or when the SBC is in place providing other benefits and TLS is needed. Contained within the SIP signaling is the SRTP setup of the media stream, then the devices send RTP that is encrypted. If the hacker does not have the SIP Signaling they cannot decode the media stream.



In a Remote Phone solution, SRTP is great to encrypt the Media Stream to ensure there is no eavesdropping of the audio.

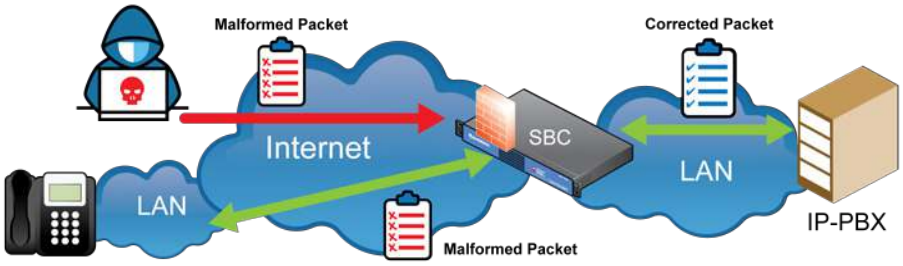
Authentication

Remote Phones have to consistently authenticate every call with the IP-PBX. The IP-PBX requires Registration Authentication and Call Initiation Authentication from the Remote Phone. The SBC is an intermediary device between the Remote Phone and IP-PBX that allows the authentication to transition between the two network locations. This is helpful in preventing malicious call attempts to the IP-PBX.



Malformed Packets

Similar to the SIP Trunking application, the Remote Phone solution can continue to leverage the ability of the SBC to rewrite SIP packets, one security interop feature the SBC can provide is the detection and correction of Malformed SIP Packets. Due to the decrease of ACL effectiveness, identifying and correcting malformed packets is more important as the exposure is increased for a Fuzzy Attack. SBCs can ensure that all SIP Packets received are corrected automatically to conform correctly to the SIP Protocol standard.



Domain Routing

IP Addresses are a known entity, Fully Qualified Domains are not. Ports Scans are IP Address based, and not FQDN based. In Remote Phone deployments, it is better to use FQDNs, then the SBC only responds to SIP addressing with the correct domain, and all other SIP messages are not routable. SIP Phones in general operate very well with FQDNs are their SIP Domain. In terms of Security, this is a major advantage over using IP Address as a SIP Domain.

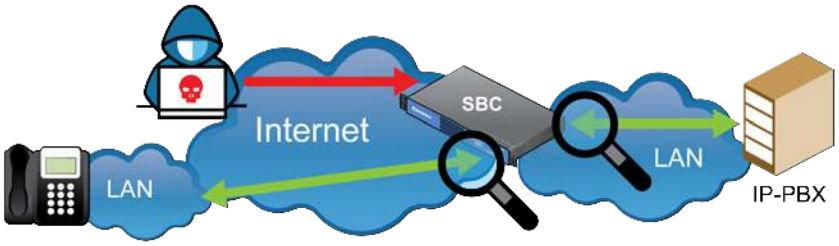
SBC's also provide the ability for Primary and Secondary flexible routing, should the Primary IP-PBX destination be unavailable, the SBC can reinitiate the call with a Secondary IP-PBX destination to ensure communications.

Transcoding & Dynamic Media Port Allocation

Similar to the SIP Trunking solution, in the Remote Phone solution the same Transcoding and Dynamic Port Allocation are important security features. As constantly changing the UDP ports used for VoIP Media is an important security feature. This prevents injecting or modification of a media stream.

Troubleshooting

Similar to the SIP Trunking solution in the Remote Phone solution, troubleshooting is not necessarily a Security feature, but it is important to have an SBC with good troubleshooting tools. This allows administrators to quickly and effectively investigate any activity within the SBC for identifying malicious traffic.



IP-PBX Features & Setup

In this scenario, as Remote Phones have dynamic locations and uses more complex call control. The use of an SBC becomes more important to provide security and as it can understand the more complex traffic. The SBC is the initial control point for the voice traffic from the Remote Phones, also bearing the brunt of the attacks and security features. But now the IP-PBX can provide a secondary level of security which will complement the SBC and the overall security solution. Also having the SBC as the initial control point for voice traffic will free up valuable IP-PBX Server resources, such as CPU

and Memory for running the VoIP communications of the business, rather than CPU dedicated to preventing an attack.

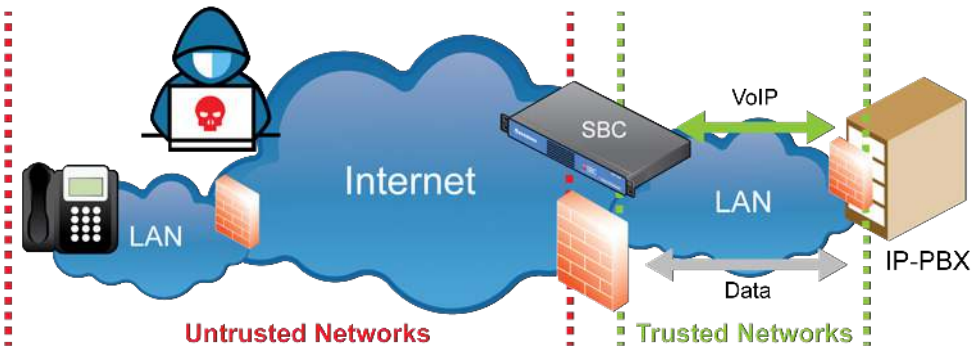
The more layers of security implemented the more difficult it is for hackers to breach VoIP environments. Every device on a network is responsible to provide a layer of security in order to protect itself, and others on the network.

IP-PBX Firewall

When deploying Remote Phones, there is a lot more to consider than just the SIP Signaling, many phones will require Auto Provisioning, Phone App (REST API), and others. In this solution, where there is an SBC, a Firewall and the IP-PBX, the Firewall continues to provide the security protection of VPN, Provisioning, Administrator Web Access, and other typical services, but the SBC adds VoIP security to the Remote Phone solution. The IP-PBX now communicates with the SBC separately for Remote Phones and other services with the Firewall.

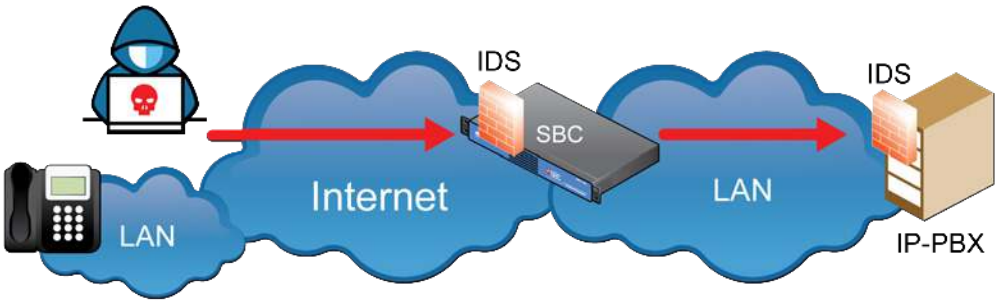
In the “IP-PBX with Firewall” example, The IP-PBX was connecting solely with a Firewall. With Remote Phones it is important to maintain the Firewall feature on the IP-PBX as there are other applications from the Remote Phones in use to connect to the IP-PBX, and the IP-PBX needs to be protected.

In terms of VoIP, the SBCs can provide the first barrier to predetermine and manage Blacklists through dynamic Access Control Lists. And the IP-PBX will be protected by the SBC, ensuring only legitimate VoIP traffic is reaching the IP-PBX. Having the Firewall active on the IP-PBX provides a secondary boundary for other Remote Phone applications.



Intrusion Detection

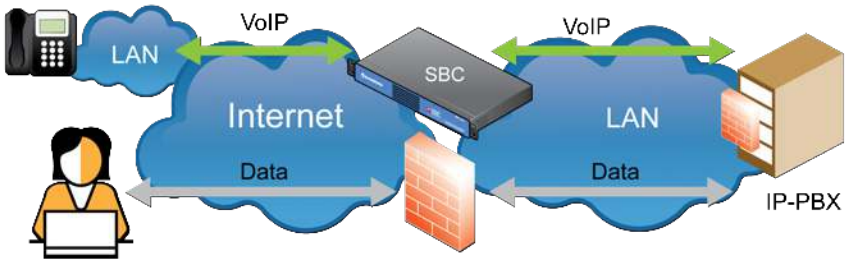
The SBC is also providing an IDS feature for VoIP, moving it out to the border of the Trusted and Untrusted networks.



In this Remote Phone scenario where the IP-PBX resides behind an SBC, the IP-PBX IDS/IPS is a secondary protection to detect and protect from Registration Attempts, Password Failure Attempts, SIP Packet signature detection, and anomaly detection.

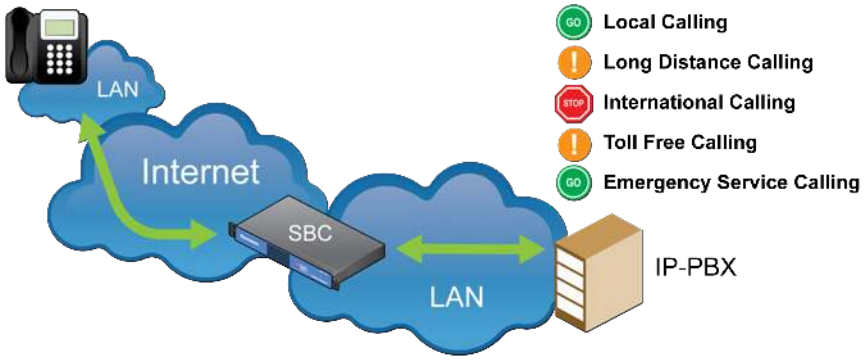
Port Management

In this Remote Phone solution, the SBC and Firewall are both in communication with the IP-PBX, the VoIP is coming from the SBC and other applications will traverse the Firewall. Port Management continues to be important to ensure complete connectivity. There are often other user interfaces into the IP-PBX, such as WebGUI access for user administration and user control of their extension. It is important to turn on only the Ports needed, and leave the optional Ports disabled.



Class of Service & Outbound Routes

As Remote Phones are not located on the Trusted Network, assigning the Remote Phones into a different Class of Service that restricts them from dialing specific outbound numbers can be a method of securing or restricting traffic. In case there is a breach, there are limitations as to what Remote Phones can dial.



Passwords

It bears repeating, security is fundamentally based on the strength of the Passwords. Remote Phones are required to Register with the IP-PBX, there is then a Password assigned to the Remote Phones. Remote Phones require strong passwords for registration.

Secure Provisioning

With or without an SBC, Remote Phones require a configuration to connect with its IP-PBX. Everything needed for the Remote Phone to Register and communicate to the IP-PBX is located in the configuration files. Use of HTTPS and SFTP are great to reduce exposure of compromising Remote Phone configurations. As both HTTPS and SFTP require the use of Certified Authority Certificates, which the Remote Phones will have, but the attacker will not. Use of TFTP and FTP are not recommended as the config files are exposed to everyone.

Remote Phone Security

Similar to the previous section when just using a Firewall, all VoIP phones have the ability to login to the device directly. It is important to change the local phone default login credentials.

TLS & SRTP

Similar to the previous section “IP-PBX with Firewall”, TLS & SRTP are important on an IP-PBX, SBC and Remote Phone for all Remote Phone applications. When the SBC resides in front of the IP-PBX for Remote Phones, all SIP Signaling, and Audio Media communications are encrypted for the ultimate level of secure communications.

In a Remote Phone solution, TLS between the IP-PBX and the SBC and in turn the SBC provides TLS with the Remote Phone, the SBC will encrypt all of the SIP Signaling in both directions with TLS. Similarly, the SBC will provide SRTP in both directions, the IP-PBX will encrypt with the SBC and in turn the SBC will encrypt with the Remote Phone.

Pros & Cons

In this security solution, where you are providing security for Remote Phones with an SBC prior to sending the VoIP traffic to an IP-PBX, there are some advantages and disadvantages. Take note that the IP-PBX must be regarded as a 'Mission Critical' application, with direct ties to business operations and revenue.

Pros

- Most Secure Remote Phone deployment
- SBC Provides VoIP Security control point prior to 'Mission Critical' IP-PBX
- Reduced IP-PBX Server resources
- Increase VoIP Security features
- SBC resides on the border between Trusted and Untrusted Networks
- No Untrusted Traffic allowed on Trusted Zones

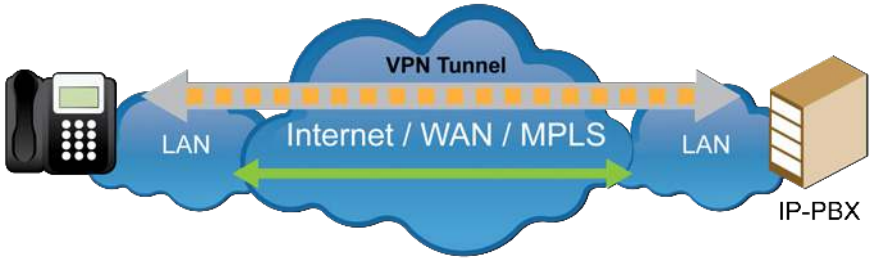
Cons

- Requires More VoIP Networking and Security complexity
- Requires more understanding of VoIP and Data traffic requirements
- Cost disadvantage in very small VoIP solutions – buying an extra device

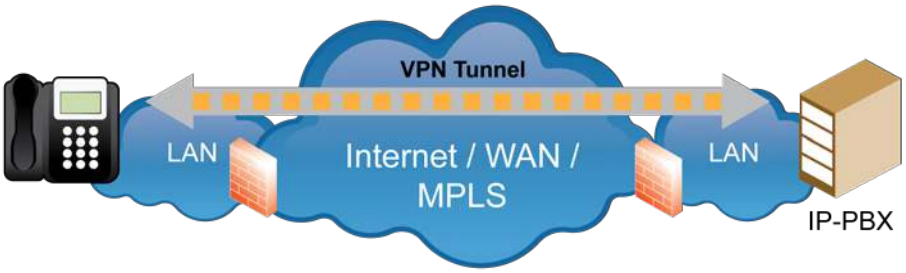
Remote IP-Phones Security using VPN

Using VPN (IP-Sec) is a completely different way to provide a secure VoIP Solution. Using already well-established encryption tunnel technologies, a secure tunnel is created between the Remote Phone and the IP-PBX.

In this example, the IP-PBX resides behind a typical network Firewall. The Firewall is the border element between Internet and LAN. The Remote Phone is located on a remote network across the Internet and the Remote Phone is establishing a VPN (IPSec) tunnel to the IP-PBX. VPN (IPSec) is a network protocol suite that authenticates and encrypts the packets of data sent over the network. The Firewall is relaying the VPN (IPSec) Tunnel from the Remote Phone to the IP-PBX.



In this example, the IP-PBX resides behind a Firewall, the Firewall is the border element between Internet or Untrusted Network Zones and Local Area Networks or Trusted Zones. The Firewall is a network security device and will forward the VPN (IPSec) traffic from the Remote Phone to the IP-PBX.



Firewall Features & Setup

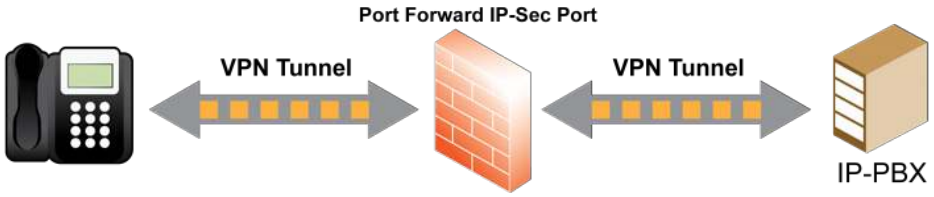
The Firewall controls the traffic by redirecting the VPN (IPSec) Tunnel to the IP-PBX destination. In this solution, the Firewall is controlling communications for allowing VPN traffic from Remote Phones to be directed to the IP-PBX.

Port Forwarding

As mentioned earlier, one of the primary functions of a Firewall is to Deny ALL unsolicited traffic from Untrusted Networks. The Firewall feature called Port Forwarding or Port Mapping will be used to redirect VPN (IPSec) Traffic to the IP-PBX.

In the SIP Trunking application, ACLs can be used to restrict Port Forwarding from specific peers, like in the case of Remote Phones. In many cases, source IP Addresses are dynamic as Residential and mobile networks provide dynamic IP Addresses. Thus, ACLs are required to be open to all Internet traffic, this is not a very secure solution, but necessary for Remote Phones.

Remote Phones will be establishing a VPN (IPSec) Tunnel with the IP-PBX, only ESP type packets will main relay through the Firewall. Remote Phones will send all of the SIP, RTP, REST API and more are encrypted within the VPN tunnel and are directed to the IP-PBX.



Note, with Remote Phones the use of ACLs on the Firewall becomes a challenge, as Remote Phone locations are dynamic, thus leaving the Firewall open to all to gain access to the IP-PBX.

IP-PBX Features & Setup

In this scenario, Remote Phones have dynamic locations and use more complex call control with all traffic from the Remote Phone being encapsulated within a VPN Tunnel to the IP-PBX. The Firewall is an important security device to protect the LAN and IP-PBX but allow the VPN traffic through to the IP-PBX. The IP-PBX has an important role and must act as the VPN Server to establish the VPN tunnel with the Remote Phone.

VPN Server

In order to manage all the Remote Phones and their VPN requests, the IP-PBX must have a VPN Server. The VPN Server will manage all of the VPN Authentication, Certificates and Client connections. The VPN Server located on the IP-PBX will allow for the Remote Phones to VPN into the IP-PBX and allow the Remote Phones to register and send all of the normal SIP and RTP required for VoIP. In addition, REST API and other applications may be needed. The VPN Server may also have the ability to do a Redirect Gateway, a function of the VPN Server to allow transient network traffic through the IP-PBX.

Pros & Cons

In this security solution where you are providing security for Remote Phones with a SBC prior to sending the VoIP traffic to an IP-PBX, there are some advantages and disadvantages. Take note that the IP-PBX must be regarded as a 'Mission Critical' application, with direct ties to business operations and revenue.

Pros

- Utilizes common Encryption tunnel technology
- Relatively easy to deploy
- Reduce Complexity of TLS & SRTP as they are not needed
- Computers connected to phone can use same VPN tunnel

Cons

- VPN Tunnels are Session oriented, if the session fails - for whatever reason - the tunnel drops
  – and the VoIP is lost.
- Firewall requires Port Forwarding, thus routing Untrusted traffic over Private network.
- Increase IP-PBX complexity and resource requirements to run VPN ServerConclusion: The Best Security Starts with a Security Policy

Conclusion: The Best Security Starts with a Security Policy

Far too often when deploying Enterprise and Carrier VoIP Solutions the application of Security is last policy to be considered, when it should be the first policy to be considered. Too often importance is placed on getting solutions operational, then later making the solution secure. When it is best to get a secure solution operational, start with Security as the first policy, and then deliver a solution that is strong and secure for the solution.

SIP Trunking is primarily a Peer to Peer communication; thus, security is driven around identifying peers and providing security features for the peer relationship. Static ACLs in Firewalls and SBCs, TLS and SRTP are peering security features that are very effective in deploying SIP Trunking.

Remote Phones is dynamic distribution of phones across the Internet to many different locations. Security is then more dynamic with the understanding of Provisioning, Device Security, Dynamic ACLs, SIP Filtering, and use of FQDNs. All combined to together to protect the IP-PBX.

We have to consider the IP-PBX as a 'mission critical' application. Loss of the IP-PBX service will have a direct loss on the revenue generation of the business. Using an SBC, a device devoted to security features, and using the security features available on the IP-PBX will help protect your VoIP application.

ABOUT SANGOMA TECHNOLOGIES

Sangoma is a leading provider of hardware and software components that enable or enhance IP Communications Systems for both telecom and datacom applications. Enterprises, SMBs and Carriers in over 150 countries rely on Sangoma's technology as part of their mission critical infrastructures. Through its worldwide network of Distribution Partners, Sangoma delivers the industry's best engineered, highest quality products, some of which carry the industry's first lifetime warranty. The product line in data and telecom boards for media and signal processing, as well as gateway appliances and software.

Founded in 1984, Sangoma Technologies Corporation is publicly traded on the TSX Venture Exchange (TSX VENTURE: STC). Additional information on Sangoma can be found at http://www.sangoma.com.