Securing Your VoIP System Before It’s Too Late

Can Your VoIP Implementation Pass Our Security Checklist?

A White Paper for Ensuring VoIP Security

November 2011
## Contents

Introduction ........................................................................................................ 3

How Topology Influences Risk ............................................................................ 3

**Top Security Threats** ........................................................................................ 6

  - Denial of Service (DoS) Attacks ................................................................. 6
  - Toll Fraud .................................................................................................. 6
  - Eavesdropping ......................................................................................... 6

**VoIP Security Best Practices** ......................................................................... 7

  - DoS Attacks ............................................................................................... 7
  - Toll Fraud Protection ................................................................................. 10
    - Secure Passwords .................................................................................. 10
    - Rates Tables .......................................................................................... 11
    - Restrictive Dial Plans ........................................................................... 11
    - Pre-Pay Accounts .................................................................................. 12
    - Call Log Monitoring ............................................................................. 12
    - Authentication-Based IP Addresses ..................................................... 13
  - Confidentiality – Secure Calls ................................................................. 14
    - Encryption—TLS and SRTP ................................................................. 14
    - Certificates ........................................................................................... 15
    - Plug and Play and Certificates ............................................................ 15
    - VPN ....................................................................................................... 16
  - Lock Out the Phones ............................................................................... 16

**Conclusion** ..................................................................................................... 17
Introduction

Organizations are implementing VoIP technologies in an effort to reduce costs and operating expenses and to take advantage of its feature-rich technology. While quality-of-service (QoS) is often the biggest concern companies have when migrating to VoIP, convergence of the voice and data worlds requires careful attention to security risks. Unlike traditional phone systems, which were inherently secure since the devices using its services had a physical connection to it, this is not the case with VoIP. The Internet environment can be a hostile place for VoIP deployments, as an IP-PBX can be reached from potentially anywhere in the world and is vulnerable if not properly secured. Security measures such as encrypting voice services, placing VoIP equipment behind firewalls, and defending against Denial of Service (DoS) attacks are just some of the steps you can take when introducing VoIP into your organization’s network infrastructure. Other measures include guarding against toll fraud, securing phone records, and protecting the phones. This paper identifies common security vulnerabilities and provides some of the best practices for guarding against them.

<table>
<thead>
<tr>
<th>IP-PBX Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS Attacks</td>
</tr>
<tr>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>CPU Usage Graphs</td>
</tr>
<tr>
<td>Email Warnings</td>
</tr>
<tr>
<td>Toll Fraud Protection</td>
</tr>
<tr>
<td>Password Control</td>
</tr>
<tr>
<td>“Weak Password” Flags</td>
</tr>
<tr>
<td>Mechanisms to Limit Calling Ability</td>
</tr>
<tr>
<td>Restricted Dial Plans</td>
</tr>
<tr>
<td>Call Log Monitoring</td>
</tr>
<tr>
<td>Authentication-Based IP Addresses</td>
</tr>
<tr>
<td>Eavesdropping</td>
</tr>
<tr>
<td>Encryption techniques (TLS and SRTP)</td>
</tr>
<tr>
<td>Certificates</td>
</tr>
</tbody>
</table>

How Topology Influences Risk

As VoIP evolved and different topologies came to fruition, various levels of security risk were introduced. For example, the first IP-PBX deployments were configured with the network between the phones and the IP-PBX (Figure 1), and a VoIP gateway was used to terminate and originate calls. Because this kept the existing PSTN lines involved, the phones were fairly safe since they were on the local or private LAN and did not touch the public Internet.
As that implementation took root, the IT department began adding remote users to the network, exposing the system (Figure 2). To decrease security risk, a VPN could have been installed or the existing VPN infrastructure leveraged, but not many phones supported VPNs natively, and VPN equipment in general, especially IPSEC, is not interoperable. While those with a working VPN could seamlessly add a softphone to the PC without running into security issues, those without a VPN faced challenges when trying to build their network. Port forwarding rules had to be set up on the router to guard against the public Internet, but if one-way audio was an issue, port forwarding had to be set up on the side of the remote phones as well. It was possible but technically challenging.

One solution for adding remote users is to put the IP-PBX on a public IP address. This usually makes connecting much simpler, especially if the IP-PBX has Network Address Translation (NAT) technology built into it to patch the SIP packets. Figure 3 depicts the IP-PBX with a dual NIC, which allows the phones to be connected on the private side and remote phones on the public side. It’s a good idea to have a software firewall on the...
IP-PBX, opening only the ports necessary for the IP-PBX to function. At this stage, SIP trunks were being looked at to help drive down monthly recurring line charges and to take advantage of international rates. Remote branches could be trunked directly, bypassing toll charges altogether in larger companies.

Figure 3. IP-PBX Connected via SIP Trunks—External Calls Going through the Internet

Another way to facilitate remote users is to use a Session Border Controller or a SIP-aware firewall/router between the PBX and the Internet (Figure 4). This helps to protect the IP-PBX from prowlers and is a good idea if you can justify the expense and you have the expertise to manage it. This may be an issue for smaller companies that don't have a dedicated IT department.

Figure 4. SBC or SIP-Aware Firewall
Top Security Threats

Denial of Service (DoS) Attacks

One of the most widely talked about security breaches is the denial of service (DoS) attack. A DoS attack is an assault on a network or device, denying it of a service or connectivity. Normal tasks like processing phone calls will be in jeopardy depending upon how your system handles a DoS attack. Attackers carry out a DoS attack by flooding a target with unnecessary SIP call-signaling messages, thereby degrading the service, making it unavailable to legitimate users. A hacker could easily flood your SIP server with bogus requests, making it impossible to send or receive calls. Imagine a hacker spamming a 4MB file to 4,000 phones? Or transmitting 500 bogus voice mail messages instantly? Or continuously ringing your phone? You pick up—no answer. Hang up—it rings again. The only way to stop it is to remove the battery or throw it out the window. Denial-of-service attacks can essentially disable your network. Depending on the nature of your enterprise, a DoS attack can effectively disable your organization.

Toll Fraud

Toll fraud is just as much of a problem as it has been with the legacy PBX world. The popular feature (DISA) that allowed users to call into legacy PBX systems, authenticate themselves via a voice mail PIN, and make an outbound call made the system vulnerable to hackers who often discovered the default account and hacked into it. In the VoIP world, we have a similar problem, but what is new here is that an intruder can also crack your IP-PBX, register an extension, and send lots of traffic your way for termination. Oftentimes, by the time a company discovers this, it’s too late and the hacker has racked up tens of thousands of dollars in fraudulent calls. The expense of toll-fraud attacks can very quickly (i.e., within hours) reach into the tens of thousands of dollars. Stories about VoIP toll fraud are extremely common, but the story of a Perth company (Australia) where hackers made 11,000 calls via the company’s VoIP and ran up a bill of AU$ 120,000 (£57,000) is among the most expensive of documented toll-fraud attacks.

Eavesdropping

Eavesdropping is one of the most common threats in a VoIP environment. Because most VoIP traffic over the Internet is unencrypted, anyone with network access can listen in on conversations. Unauthorized interception of audio streams and decoding of signaling messages can enable the eavesdropper to tap audio conversations in an unsecured VoIP environment. Imagine the mailroom attendant overhearing the CEO and HR director discuss the latest round of layoffs. Eavesdropping is also how most hackers steal credentials and other information; for example, customers reciting their credit card numbers to an airline booking attendant. All that's needed is a packet capturing tool (freely available on the Internet) or switch port mirroring, and hackers can save the files, take them home, and cause disaster with the stolen information. Keep in mind that most times the enemy is within and that hackers can often be employees or visitors already on the LAN.
VoIP Security Best Practices

While there is no such thing as a bulletproof VoIP implementation, there are a handful of features to look for when scouting out a good IP-PBX system for your VoIP migration.

Table 1. VoIP Security Checklist

<table>
<thead>
<tr>
<th>Issue</th>
<th>IP-PBX Safeguard</th>
<th>snom ONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS Attacks</td>
<td>• Intrusion Detection—Access Lists</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>• snom ONE’s Media CPU Usage Graph</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>• Email notifications of high CPU when call is rejected</td>
<td>✔️</td>
</tr>
<tr>
<td>Toll Fraud Protection</td>
<td>• Secure Passwords</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>• “Weak password” flags that notify the administrator of</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>weak passwords on the system</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>• Mechanisms that place limits on an extensions</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>calling ability</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>• Restrictive Dial Plans</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>• Call Log Monitoring</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>• Authentication-Based IP Addresses</td>
<td>✔️</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>• Encryption techniques like TLS and SRTP</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>• Certificates</td>
<td>✔️</td>
</tr>
</tbody>
</table>

DoS Attacks

The topology of your system will determine how vulnerable you are to these attacks. If you are on a private network and have no remote users or use a VPN server, then you should be at minimal risk. Conversely, if you are depending upon the logic of the IP-PBX to defend you, then you must ensure that your system has automatic intrusion detection capability. Therefore, if the system is on a public IP address or if port forwarding is set up in the firewall router, then you need to ensure that you’re protected. Intrusion detection systems (IDSs) are not a new technology, but when they are used, they must act quickly; otherwise, it will be too late when an attack occurs. An IDS is a key component of an IP-PBX. The IP-PBX should monitor the CPU and send out SNMP or email alerts when it is spiking when under attack. Automatic IDS is accomplished by setting up access lists as depicted below:
Figure 5. Intrusion Detection—Access Lists

Once an access list has been set up, the system notifies the administrator via email whenever a blacklisted IP address tries to access the system and has reached the number of tolerated attempts that has been set for that IP address. This allows the administrator to investigate whether it was an incorrect password typed in by a user or if the system is indeed under attack. The email sent to the administrator includes a link to a map that indicates the geographic location of the origin of the attack so that it can be determined quickly whether an employee lives in that area or if the system is indeed under attack.

From: pbx@companya.com
Sent: Friday, March 30, 2012 10:09 AM
To: pbx@companya.com
Subject: Company A Phone System: Address 118.10.192.1 has been blacklisted

The IP address 118.10.192.1 has been blacklisted for 1440 minutes because there were 10 unsuccessful authentication attempts (sip).

Please click on http://thisisasampleurl.com/118.10.192.1 if you wish to know the details about this IP address.
Also contained in the email (as an attachment) is the packet in question so that it can be scanned for the user agent string, enabling you to determine whether it is the friendly scanner or a familiar phone.

```
REGISTER sip:107@173.166.77.210 SIP/2.0
Via: SIP/2.0/UDP 127.0.0.1:5075;branch=z9hG4bk-687111338;rport
Content-Length: 0
From: "107"<sip:107@173.166.77.210>;
tag=3130370133393731363439313938
Accept: application/sdp
User-Agent: friendly-scanner
To: "107"<sip:107@173.166.77.210>
Contact: sip:107@173.166.77.210
CSeq: 1 REGISTER
Call-ID: 2518265916
Max-Forwards: 70
```

A security-focused IP-PBX should also send out daily reports that include details about the CPU. snom ONE’s “Media CPU Usage” graph details the average CPU load, as well as the number of calls and peak usage in the last 24 hours. It’s a good idea to lower the CPU threshold from the default of 75% to 25% if your system is constantly at 10%.

Figure 6. snom ONE’s Media CPU Usage Graph

snom ONE also notifies the administrator via email when new calls are being rejected because of performance problems. This allows the administrator to see when the system is getting increasingly overloaded, which could be an indication of toll fraud.
Sometimes a power failure of a PoE switch at a remote site could cause what would look like an attack, so some investigation is needed. Also, a simple trace route can help determine where the attack has come from. Both SIP and HTTP attempts should be counted. Many “test” programs are available on the Internet that can be used to send traffic to your IP-PBX to see how it behaves. These tools can be easily tweaked to wreak havoc on the net. Since they already send a lot of traffic, one need only wrap a few lines of code around them, and they are off and running.

The friendly VoIP scanner is not so friendly and has been reported to cause widespread issues. It basically sprays out SIP requests and peppers the responder with traffic that spikes the CPU to 100%, since it has to deal with an onslaught of REGISTER requests and other SIP messages. Before the scanner will stop sending the requests and seek out a new victim, the system must detect them and stop responding to them. While the good hackers find vulnerabilities and give manufacturers enough time to fix them before telling the world, the bad hackers cause grief and in some cases financial gain for themselves.

Toll Fraud Protection

Secure Passwords

Your first line of defense in preventing toll fraud is to assign very long, cryptic passwords to each extension. While this might be easier said than done, it is always the first thing to do. Never use obvious passwords. For example, extension 101 should not be using password 101 since it will be the first password checked by the hacker’s software, which no doubt will be equipped with a dictionary file to be used specifically against extension 101.

The IP-PBX must have an option for strict passwords, and it should be turned on so that repercussions do not ensue. snom ONE allows the administrator to choose from three password levels when configuring the level of complexity that will be required of the user; each password level requires the user to create passwords that meet certain criteria and which total to a specified number of points.
The system should also be capable of flagging the administrator when a weak password exists on an account so that action can be taken. snom ONE flags the administrator using a yellow triangle, as shown below:

<table>
<thead>
<tr>
<th>Account</th>
<th>Type (Name)</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>401</td>
<td>Extension (Sandra Kelly)</td>
<td></td>
</tr>
<tr>
<td>402</td>
<td>Extension (Steve Perry)</td>
<td>1 Rags 1</td>
</tr>
<tr>
<td>403</td>
<td>Extension (Jerry LeBlanc)</td>
<td></td>
</tr>
<tr>
<td>404</td>
<td>Extension (Theresa LeBlond)</td>
<td></td>
</tr>
<tr>
<td>408</td>
<td>Extension (Kathy Smith)</td>
<td></td>
</tr>
<tr>
<td>409</td>
<td>Extension (Cindy Travis)</td>
<td>1 Rags 1, 1/0 Msg</td>
</tr>
</tbody>
</table>

Rates Tables

Rates tables (available from your service provider) allow you to assign a dollar value—either on an extension, the trunk, or on the whole system—and thereby minimize damage in the event the system is compromised. Outgoing calls cannot exceed the assigned dollar value.

Restrictive Dial Plans

Limiting the dial plan will go a long way in preventing toll fraud. Most dial plans send all the traffic out a particular trunk with a wild card * in the pattern field. While this may be okay in some cases, if you have employees who don’t need to make international calls, then prevent international calls from ever being made from their extensions in the first place. This can be done by putting a 1* in the pattern field. This way, 011 calls will be blocked. The occasional international call that needs to be made from that extension can be dealt with on an individual basis.
If employees need to make international calls throughout the day, but you would still like to block these types of calls after hours, a service flag can be assigned on the trunk that is used for international dialing (denoted below with 011* in the replacement field). Once configured, users would be unable to make calls outside the hours specified in the service flag account (e.g., when the office is closed). Another safety measure would be to require a PIN on a particular trunk (denoted below by the P checkbox). When a PIN is required, calls cannot pass through that trunk without the user first entering the correct PIN. The “Not Allowed” feature (shown below with 900 in the Pattern field) allows you to restrict certain numbers completely. Our example restricts users from calling 900 numbers, but this field can also be used to restrict expensive numbers that companies typically don’t call, like the Caribbean Island of the Dominican Republic. In this case, 809xxxxxxx would be the pattern.

To further reduce exposure, dial plans can be adjusted so that specific numbers can be blocked that would otherwise go through in certain calling plans. For example, if you have a plan that includes the United States and Canada, you might be under the impression that all NANPA numbers (i.e., 1 + 10 digits) are free, but calls made to the Bahamas, which also use the “1 + 10 digit” format, can range from 10 to 18 cents a minute, depending on whether the call is placed to a cell phone. To guard against surprises like this, specific ranges of numbers can be blocked (for example, 1.242.xxxxxxx) in the dial plan of users who have no need to make these types of calls.

Pre-Pay Accounts

Another good measure against toll fraud is to use pre-pay accounts. Talk to your service providers and request a pre-pay account or at least have some limits placed on the account. PSTN providers usually don’t have this capability since they are mostly post-pay, but it is something to check out since VoIP gateways can be hacked as well.

Call Log Monitoring

Call Detail Records (CDRs) provide details about the system’s daily call activity and can help stop toll fraud scams before they cause an organization massive financial loss. snom ONE allows you to choose the time of day you would like to receive the CDR report. Reviewing CDR reports regularly gives you a good idea as to the call activity that typically occurs on your system and will help you identify dramatic shifts should any occur. The snom ONE web interface also has a Call History page that allows you to view the system’s call activity in real-time. This enables the administrator to monitor the system more regularly.
CDRs must be kept private. If someone discovers who’s calling you and who you’re calling, it can be a competitive advantage to them. In the past, getting possession of a company’s CDRs was difficult since they were either buried in the PBX or located at the phone company. But this has all changed with IP-PBXs. Getting access to the CDRs of an IP-PBX is as easy as hacking into the system. To lock down the web interface of the system and ensure that drives can’t be shared or accessed remotely, password management is key. Also, rather than let CDRs sit in a directory until they’re needed, it’s best to get them off the system and into a secure database or email server where they can be queried later if needed.

**Authentication-Based IP Addresses**

If you want to take a few extra steps at securing your system, then statically configure the IP phones to your extensions. In the IP-PBX, specify which IP address can use a particular extension as a trusted IP address. (In the image shown below, extension 401 can make calls only from a phone with IP address 192.168.0.56.) Remember, VoIP toll fraud occurs in two stages: (1) the attacker scans the Internet to find a VoIP system, and (2) it poses as a remote extension and attempts to make calls. By making it impossible for hackers to register and make phone calls, you’ve prevented fraud from the outset.

This works well on the LAN, but not on the WAN unless the phones have static IP addresses. Purchasing a static IP address may be worth the extra expense. This way, you can go into the DHCP server and specify which MAC address gets a particular IP address. If you don’t have employees working from home, you should always have a static IP address for that phone. Static configuration for the phones can be set through the DHCP settings in the router.
Confidentiality – Secure Calls

Encryption—TLS and SRTP

The primary responsibility of the system is to process voice calls, and the confidentiality of those calls is of primary importance. Unlike PSTN calls that traverse dedicated circuits, VoIP calls are really just data going across the Internet, and this data must be protected. This is nothing new here—banks had to figure out a way to make online banking transactions secure over a decade ago. For this, HTTPS is used, so we can borrow heavily from that. By using encryption techniques like TLS and SRTP, we can protect both the signalling and the media stream, preventing the conversation from being listened to with simple tools like port mirroring and an RTP trace using Wireshark.

SIP packets contain information such as the IP address of the phone, the SIP server, the signalling and media ports that it's expecting to listen on, the MAC address of the phone, and in some cases, even the management port of the phone. This is private information and should be sent over a TLS tunnel to hide it from snoopers. Snoopers sniffing packets will be able to see TLS packets but will have no idea what's in it. The first step in implementing TLS is to make sure your equipment supports it and then configure it accordingly. You need to add sips:IP_address_sip_server:5061 to the outbound proxy address of the phones, which is quite easy, and once done, it will try to negotiate TLS. You may use a self-signed or default certificate; though it's not the most secure method, it is better than sending the packets in clear text.

snom's new line of phones provides secure SIP signaling via TLS and audio stream encryption, incorporating SRTP (Secure Real-time Transport Protocol). SRTP is a security profile for RTP that adds confidentiality, message authentication, and replay protection to that protocol. SRTP is ideal for protecting Voice over IP traffic because it can be used in conjunction with header compression and has no effect on IP Quality of Service. These factors provide significant advantages, especially for voice traffic using low-bit rate voice codecs such as G.729.

snom phones provide TLS-based SIP signaling (SIPS) with a SIP proxy server and audio stream encryption using secure RTP based on 128-bit AES. SIPS not only prevents message manipulation and eavesdropping, but it also assures the proxy server of the identity of the client snom phone; hence, identity spoofing threats are also subdued by this mechanism. snom phones use AES in counter mode (AES-CM) for secure RTP. AES-CM creates a unique key stream for each RTP packet, making it almost impossible for eavesdroppers to retrieve the original RTP stream from the encrypted SRTP stream.
If someone is sniffing packets, they will see a TLS packet but will have no idea what is in it.

![Diagram](snom Phones)  

**Figure 7.** Secure Audio Stream Using snom Phones

**Certificates**

If you want to increase security further, then purchase an actual certificate from a Certificate Authority (CA) like VeriSign, which is equivalent to having your documents signed by a Notary Public who is a trusted third party, verifying that you are who you say you are after looking at your identification. Most devices list the CAs that they support. Getting the certificate into the IP phones is currently the tricky part. Since some phone vendors are not burning them in at the factory using the MAC address as part of the key, you can upload it via the web interface. This way when the phone asks the PBX for its configuration file and the PBX can’t verify that the MAC address is from the remote phone since the Ethernet packets will be tagged with the gateways MAC address, then the certificates and key exchange can be used to verify that this phone is indeed associated with that MAC address.

**Plug and Play and Certificates**

Plug and play of phones on the wide area network is nothing new for hosted service providers. The phone presents a MAC address and based upon that MAC address, the IP-PBX automatically provisions the phone so that it can make calls. However, the IP-PBX is not able to verify the MAC address of the phone since it came from the WAN (the MAC address, in this case, reflects that of the router since that’s where it came into the LAN).
But the 7xx and 8xx series of phones resolves this issues. These phones have certificates burnt in at the factory, so after a key exchange, the IP-PBX can be assured that the phone is who it says it is and that a certain MAC address belongs to a particular phone. This way, the IP-PBX does not just have to trust a phone’s authenticity; it can guarantee it.

VPN

A VPN can also be used to protect the voice conversation between the phone and the IP-PBX. VPNs have been around for a long time and IT professionals are accustomed to supporting them. However, the downside is that IPSec is the predominant protocol, and interoperability is not very wide spread among vendors, i.e., the client and the servers are usually from the same company. In addition to de facto standard IPSec, other technologies include PPTP and OpenSSL. If someone already has a VPN set up, then using a softphone to contact the IP-PBX on the LAN would be easy. However, to connect a hard phone that does not support VPN, a tunnel using a piece of hardware on the client side would need to be established. Not many phones support VPNs natively, but one vendor has a built-in VPN client based on OpenSSL, which can be implemented today and OpenSSL is a free server side product. VPNs are an option, though not an easy one if you have to start from scratch.

Lock Out the Phones

Protecting the phones can be accomplished by locking out the web interface if they are not to be used by the end user and configuring everything from the IP-PBX using Plug and Play (PnP) to the phone. If you want to go a few extra steps, then statically configure the IP phones and in the IP-PBX, specify which IP address can use a particular extension as a trusted IP address. This works well on the LAN, but not on the WAN unless the phones have static IP addresses. Purchasing a static IP address may be worth the extra expense.

Disaster Recovery

PBX disaster recovery is one of the most overlooked aspects of business planning, but adequate attention needs to be given to this topic. First and foremost, always back up your IP-PBX’s configuration data, voicemail, etc. This can be done either via the file system or the web interface on most systems if the data is not too large. The vital link between you and your customers is crucial and also needs a recovery plan as well. It is best to get a code-based service so that you can automatically send your configuration data to the cloud. A code-based service can also be used as a backup of your local PBX. Find a service that automatically activates the second identity of your phones so that users can still make calls. (Most IP phones enable you to have a second registration for failover, so if the primary registration fails for any reason, you can automatically roll over to the backup.) A backup 4G wireless Internet card is also a wise investment in the event of an Internet outage and can go a long way in ensuring that your business communication never gets disrupted.
Conclusion

Organizations are increasingly implementing VoIP technologies, and many of them are drawn by the cost reductions, but deployments must be done in the most secure manner possible. Otherwise, the sought-after cost savings could result in monetary losses if the security of the VoIP infrastructure is compromised. The good news is that with proper planning and administration, VoIP need not strike fear. By taking the right approach to VoIP security, organizations can expect the quality, reliability, and security that we’ve come to know from the existing phone networks.

snom is a security-aware VoIP-vendor and our snom ONE IP-PBX is capable of implementing a complete, multi-layered security solution. Using snom phones in conjunction with a TLS/SRTP-enabled PBX provides a secure VoIP environment that is not vulnerable to security risks involved in Internet telephony. This telephony setup not only maintains the integrity of the SIP signaling messages exchanged, but also provides encrypted audio streams, providing high-end security against eavesdroppers and tapping. The TLS/SRTP feature of snom phones is interoperable with a number of PBX vendors including PBXnSIP, Asterisk and Ingate.