Security Strategies for UC

digium®
The Asterisk Company®

Security Strategies for UC

Security Strategies for UC

Why is security important in the SMB (small and medium-sized business) space?

In the days of legacy phone systems, voice information was transmitted over the dedicated PSTN (Public Switched Telephone Network). In many ways the PSTN is the largest, most robust communications infrastructure on the planet and it is still in use today. With the advent of VoIP (Voice over IP), telecommunications is moving away from this legacy platform onto the Internet. The SMB business phone system, rather than being separate equipment, is now another network device able to interoperate with many new and emerging technologies.

Security Strategies for UC

Understanding Why UC Systems are Vulnerable

A UC business phone system combines voice, video, chat, email and presence together into one unified messaging system. As the technology has become more complex, and more accessible from the public Internet, the security threat has increased. In many ways it is easier than ever to attack business communications. Companies must be diligent to protect their communications as they are vital to business operations.

Why is UC Security Important?

A History Lesson in Telephony Security

Security has long been a problem for telecommunications networks. Even in the legacy days of the PSTN, threats existed. Attackers who were able to compromise phone systems were known as “phreaks.” Not all phone phreakers were malicious. Many simply sought to study the technology. A few were able to manipulate the system for financial gain.

Early telephone networks used in-band frequencies to transmit call level signaling. For example, AT&T used a single 2600hz tone on the line to signal that the line was ready to dial long distance calls. A famous phone phreaker, John Draper, discovered that the toy whistle found in a Cap’n Crunch® cereal box could be used to emit a 2600hz tone. By blowing the whistle into the phone, he was able to make free long distance calls.

A History Lesson in Telephony Security

This vulnerability helped usher in greater use of DTMF (Dual Tone Multi-Frequency) **signaling**. By using two tones instead of one, the call control signaling was more difficult to reproduce, but not for long. Phreaks soon built devices called the “Blue Box.” This device was able to produce DTMF tones necessary to gain control over the telecommunications system. Steve Wozniak, who later went on to help found Apple Inc., is known for being a phreaker using blue boxes.

A History Lesson in Telephony Security

To avoid this vulnerability, the telecom network moved to out-of-band signaling; however, DTMF still exists today. The tones you hear when you press the keys on a touch tone phone are DTMF tones. Many mobile and VoIP phones still use these tones simply because they are familiar to us, even though they are not needed for signaling.

The historical lesson to learn is that technology must evolve to stay ahead of those who seek to exploit it. Although historical phreaks like John Draper and Steve Wozniak are a type of folk hero, modern attackers can do real damage to your system and cost your business large amounts of money. As technologies evolve, so do the malicious attackers. It is imperative to stay up-to-date on information security in order to protect your business' assets.

Common threats against UC systems

There are many threats that can affect a business phone system. Four of the most popular are: Toll Fraud, Denial of Service, Man in the Middle, and Social Engineering. Knowing what kind of damage can be done serves to illustrate the importance of securing your phone system.

Toll Fraud

Toll Fraud is a common attack against business phone systems. In this type of attack the malicious agent attempts to gain access to your long-distance, toll-bearing trunks. If they are able to make calls using your long-distance account then they can get free calls and you end up paying long distance fees to your upstream provider. This can be especially damaging if international calls are made. Companies with VoIP systems that are compromised by toll fraud are often left liable for tens of thousands, or even hundreds of thousands of dollars in long distance fees.

Common threats

Denial of Service

A “DoS” or Denial of Service attack is one in which an attacker compromises your system in such a way as to make it inaccessible to your users. DoS attacks can be targeted at specific services, such as stopping the ability to dial out trunks, or access to remote UC features, or in a worst case scenario, can bring down the entire system so that even interoffice calls cannot be made. When your system is unavailable to users due to a DoS attack you will see this cost in terms of lost time and productivity. Not to mention the loss of reputation in the eyes of your customers who are unable to communicate with you.

Common threats

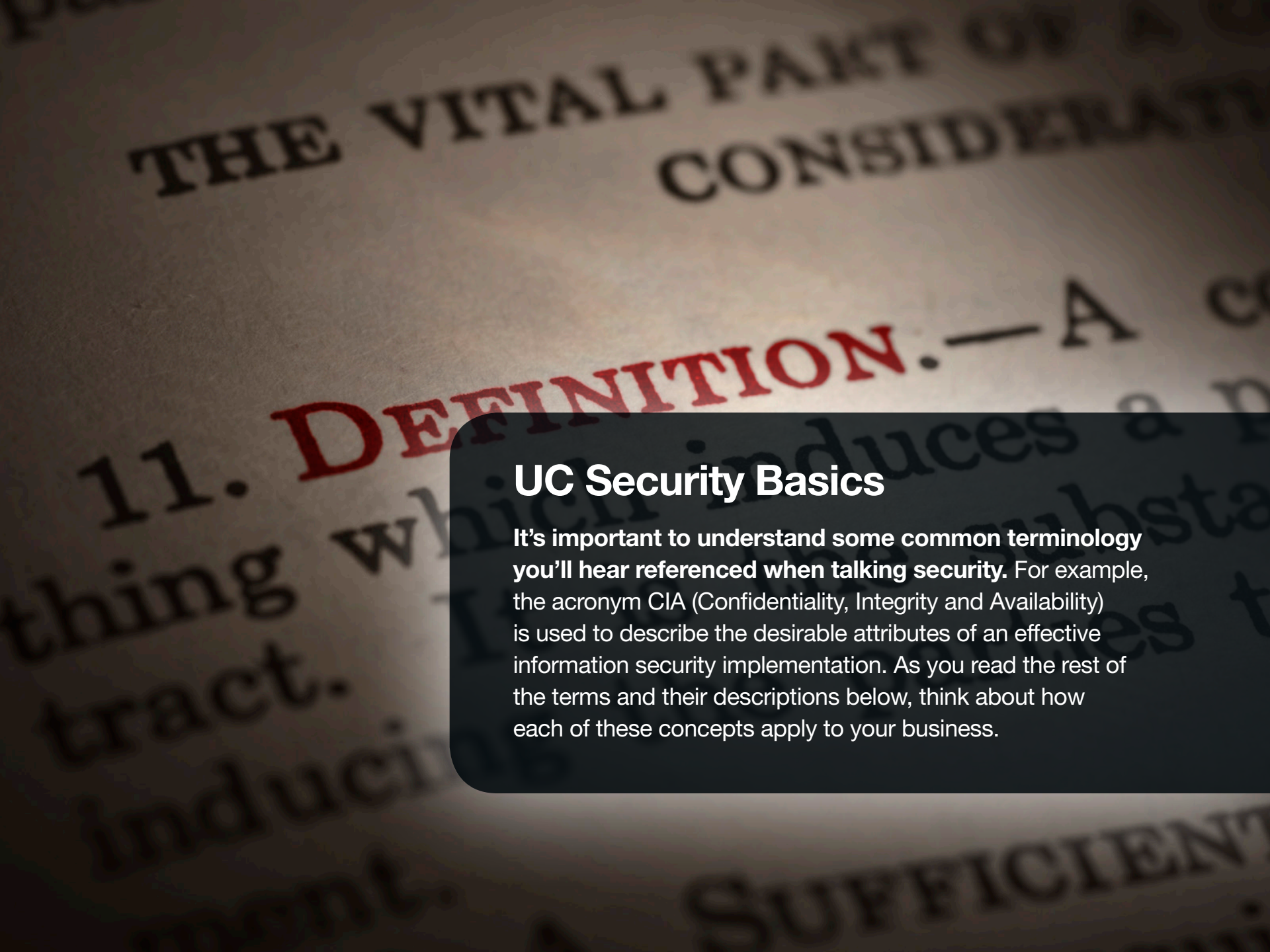
Man in the Middle

A Man in the Middle attack occurs when an attacker is able to intercept your traffic and then passes it along. You may not know that a Man in the Middle attack is occurring because your services appear to be working like normal. However, if an attacker is able to intercept authentication credentials they could use this information to perform a DoS or Toll Fraud attack. Additionally, the attacker could gain access to private or privileged information.

Common threats

Social Engineering

The easiest way to exploit a technology is to attack humans instead of attacking the technology. Modern, sophisticated attackers will often try to gain access to your system via social engineering rather than technical exploits. An example would be a malicious attacker calling one of your users pretending to be your IT department. They might ask the user for their password in order to fix an imaginary problem. The unsuspecting user offers their authentication credentials freely. The attacker now has access to your system.



UC Security Basics

It's important to understand some common terminology you'll hear referenced when talking security. For example, the acronym CIA (Confidentiality, Integrity and Availability) is used to describe the desirable attributes of an effective information security implementation. As you read the rest of the terms and their descriptions below, think about how each of these concepts apply to your business.

UC Security Basics

Confidentiality

User data should be confidential.

The only people who should be able to access your confidential information are those for whom it is intended. In the case of business Unified Communications (UC) systems the data could be voice traffic or chat messages. Confidentiality is important both to protect trade secrets and personal privacy. In the same way you might close your office door in order to have a confidential conversation, you would likewise expect that a phone call between two parties would be similarly private. You would not want an uninvited third party to be able to eavesdrop on the conversation.

Integrity

The integrity of information refers to the quality being unchanged. If you receive an email from a colleague, you should have a reasonable expectation that the text you are reading is the actual message they sent. A malicious attacker intercepting your message and modifying it could cause havoc.

Availability

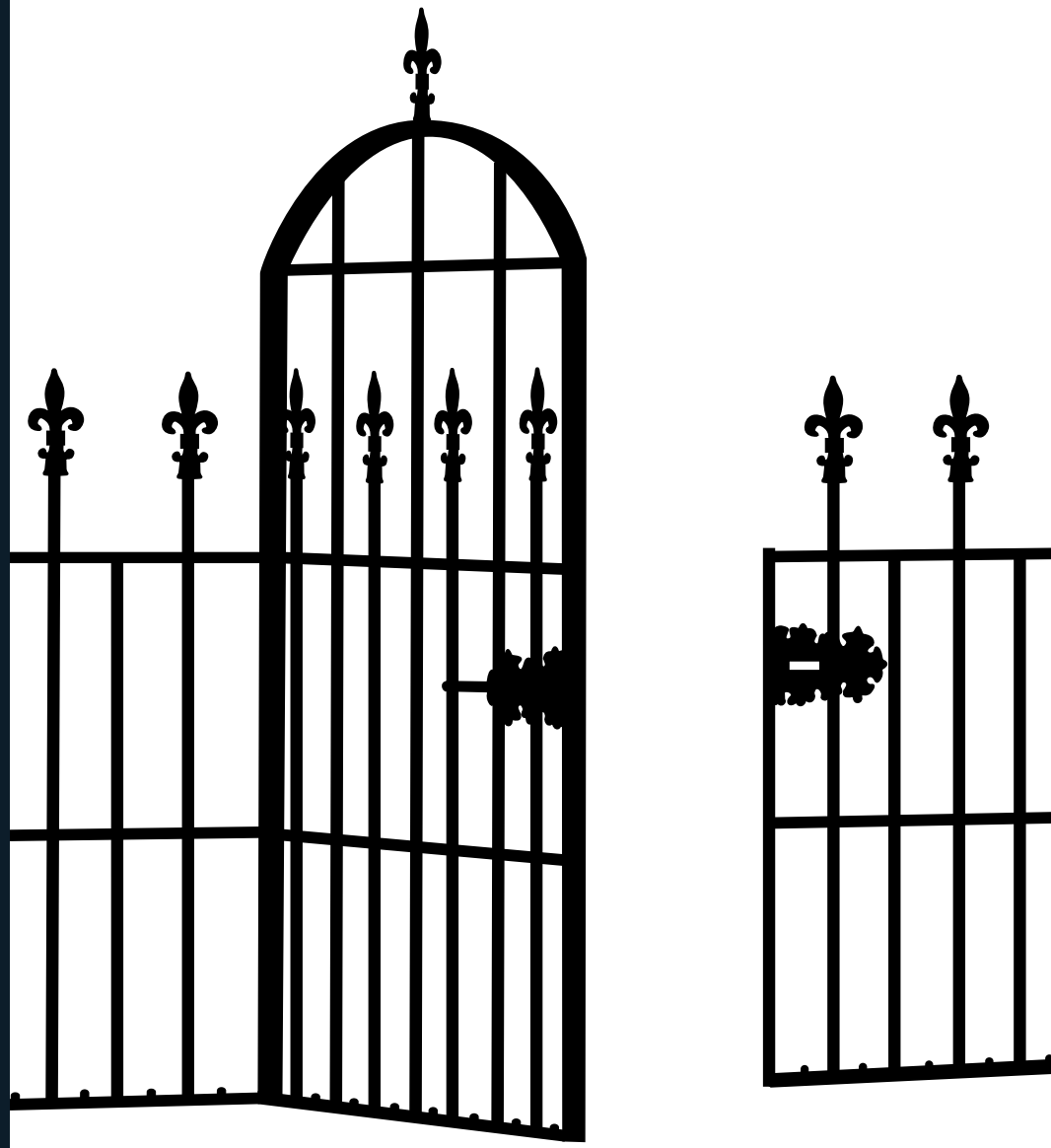
Having a secure network with confidentiality and integrity is of little value if your services are unavailable to your users. A DoS (Denial of Service) attack is one in which an attacker prevents access. For example, imagine an attacker who gains physical access to your server closet and disconnects the power to your UC server. The disruption to your phone service would impact your ability to provide customer service.

Availability

Availability is also important to keep in mind when selecting security equipment. There is a such thing as “too much security.” For example, imagine you wanted to secure the hard disk of your PC. You could remove the disk, encase it in cement and bury it in the ground. The data on the disk would be highly confidential — no unauthorized person would be able to get to it. It would have high integrity, and be nearly impossible for an attacker to modify the data on the disk. However, it would also be completely unavailable and as such this security tactic is a futile one. It may seems obvious that “cement” is a poor choice for securing UC equipment, however often the same type of over-handed security polices are put in place, making the data so “secure” no one can get to it, even your users.

Mitigation vs Elimination

A truly secure network is one that is not only protected from attack but is also accessible when it needs to be. In this spirit, the goal of information security should be mitigation not elimination. To “mitigate” a threat means “to lessen or make smaller.” It’s never possible to completely eliminate all threats against your UC system. If an attacker is determined enough they will find a way to break in to your system, however most attackers are not determined. In general VoIP security threats most commonly arise from attackers looking for an easy, unsecured target. By implementing a baseline of security best practices you make your system unattractive to potential attackers looking for an easy target.



UC Security: What You Need to Know

Unified communications presents unique security challenges because it brings together disparate technologies. Using VoIP, video, chat and presence together has proven to provide productivity gains for businesses, but also presents security risks.

In particular, securing VoIP networks is not the same as securing data networks. Most data traffic is transported over TCP and as such, security built-in to networking devices such as routers and firewalls are built around TCP data-centric transport. VoIP is UDP-based and time sensitive. Dropping a few packets while downloading a website is for the most part benign — the packets can simply be retransmitted. Voice and video streams are more fragile. Dropping too many UDP packets in a voice stream can cause call quality issues. As such, securing your unified communications requires a balanced approach. You must mitigate threats while also maintaining quality of service.

Likewise, managing security for an SMB offers unique challenges when compared to the larger, enterprise space. While large businesses can often dedicate substantial resources toward securing their communications, those in the SMB space need security solutions that are both effective and simple. This actually works in favor of the SMBs since security and simplicity can work together. For example, installing an expensive and complex solution to secure you network can work against you. Improperly configured equipment can affect your call quality and potentially stop your VoIP equipment from functioning properly. Remember, accessibility is key to a secure network.

7 Tips for Effective UC Security

Despite being in a niche field, securing unified communications as an SMB follows many of the same security best practices that are effective in the enterprise for a variety of technologies.
The following best practices can help keep communications flowing.

1. Deploy a Properly Configured Firewall
2. Enable a VPN for Remote Users
3. Use Strong Passwords
4. Update Regularly
5. Turn Off Unused Services
6. Monitor Your Call Logs
7. Use built-in UC security tools

1 Deploy a Properly Configured Firewall

Due to the variety of firewall models and topologies available, giving specific advice is difficult. So, here are some practical tips for almost any configuration. For starters, it's always advisable to keep high importance on security. This means being technically familiar with your equipment and it's configuration. It is a responsibility you should take with the utmost seriousness. When shopping for firewalls favor those that offer simple configuration and are designed for the SMB.

1 Deploy a Properly Configured Firewall

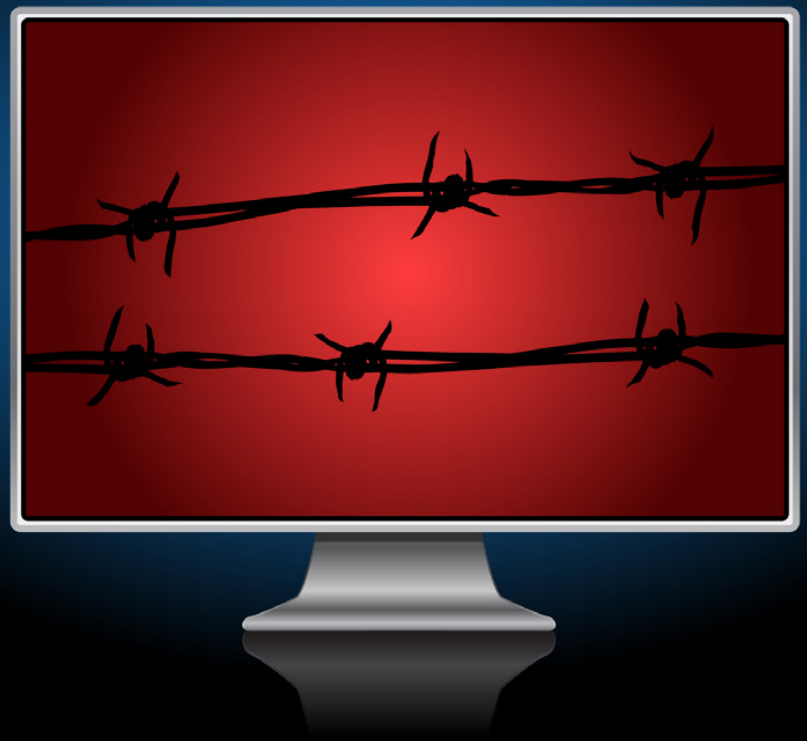
A good general rule of thumb is to block all unknown traffic into your network and then only allow traffic from trusted sources. This strategy doesn't usually work well for your web server, but your UC server should absolutely be sequestered behind your firewall. In most cases, you should only allow Internet traffic from your ITSP (Internet Telephony Service Providor) or VoIP provider. This is the company that supplies you SIP truck or hosted VoIP services. Allow access only on the ports necessary and only to the IP or block of IPs that your provider uses.

1 Deploy a Properly Configured Firewall

Some complex firewalls tout features such as SIP ALG (Application Level Gateway). Although SIP ALG is advertised as a security feature for VoIP, it tends to not work as advertised. Instead, ALGs have a tendency to mangle SIP packets or modify headers in a way that breaks functionality. A general best practice is to do extensive interoperability testing prior to deployment or simply disable SIP ALG in your firewall and/or router.

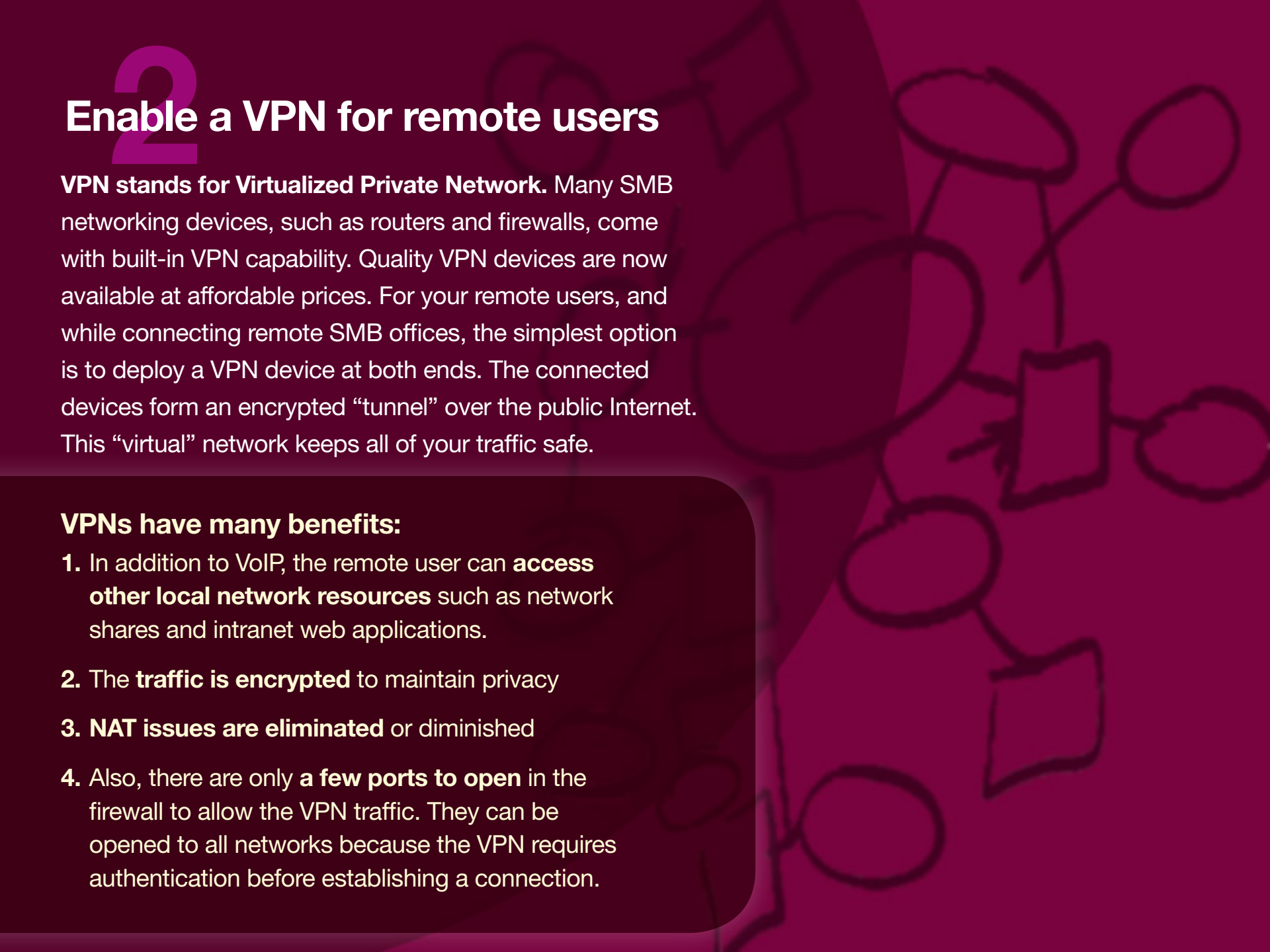
1 Deploy a Properly Configured Firewall

Surprisingly enough, many small, and even medium-sized businesses do not deploy a firewall. Or, they deploy a firewall, but open ports to all networks to allow remote users. This is almost the same as having no firewall at all. Although some UC servers, like Switchvox have built-in attack mitigation mechanisms, these should not be solely relied upon. Your firewall is designed to sort traffic, your UC server is not. Using each device for its intended purpose will keep your network the most secure. In the SMB, managing remote users is better done through a VPN.



2 Enable a VPN for remote users

VPN stands for Virtualized Private Network. Many SMB networking devices, such as routers and firewalls, come with built-in VPN capability. Quality VPN devices are now available at affordable prices. For your remote users, and while connecting remote SMB offices, the simplest option is to deploy a VPN device at both ends. The connected devices form an encrypted “tunnel” over the public Internet. This “virtual” network keeps all of your traffic safe.



VPNs have many benefits:

1. In addition to VoIP, the remote user can **access other local network resources** such as network shares and intranet web applications.
2. The **traffic is encrypted** to maintain privacy
3. **NAT issues are eliminated** or diminished
4. Also, there are only **a few ports to open** in the firewall to allow the VPN traffic. They can be opened to all networks because the VPN requires authentication before establishing a connection.

3 Use Strong Passwords

Using strong (system) passwords is an extremely effective, yet often over looked security measure. Strong passwords should be used for every instance required in your UC solution. Business VoIP phones should especially be protected by unique strong SIP passwords. Re-used or weak passwords make it extremely easy for an attacker to get access to SIP credentials. Once authenticated with a SIP account, attackers can make high fee toll calls as though they were using that phone.

Another area of concern is **user passwords**.

If your UC solution requires user login, then you will want to ensure that you require strong passwords for your users. Switchvox, Digium's UC solution, mitigates both of these threats by default: strong, unique SIP passwords are automatically generated and used for Digium phones attached to Switchvox.

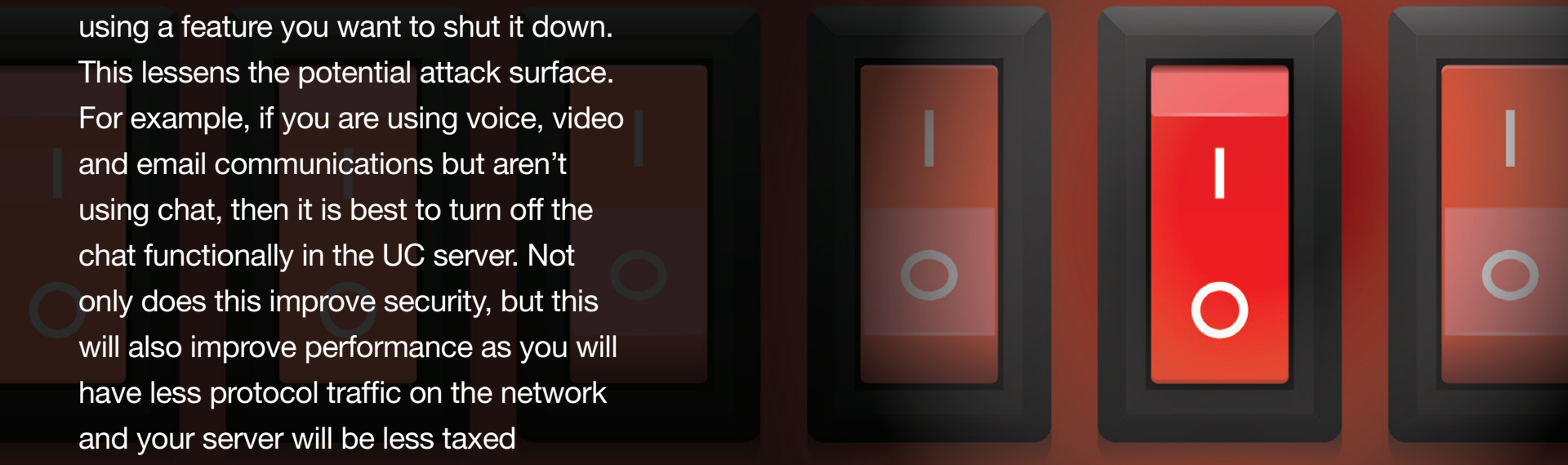
4 Update Regularly

A standard security best practice that is almost universal to all technologies is to keep software up to date. As well as obtaining bug fixes, keeping your software updated helps improve security. As potential exploits are found, security patches are then released as software updates. The most recent version is typically the most secure.

Whenever you update your UC server you will want to follow the best practices for updating. Be aware of what has changed and how the update could impact your system; backing up the system first, and performing the update during a scheduled maintenance window also helps to ensure your users will have access to your system when they need it.

5 Turn Off Unused Services

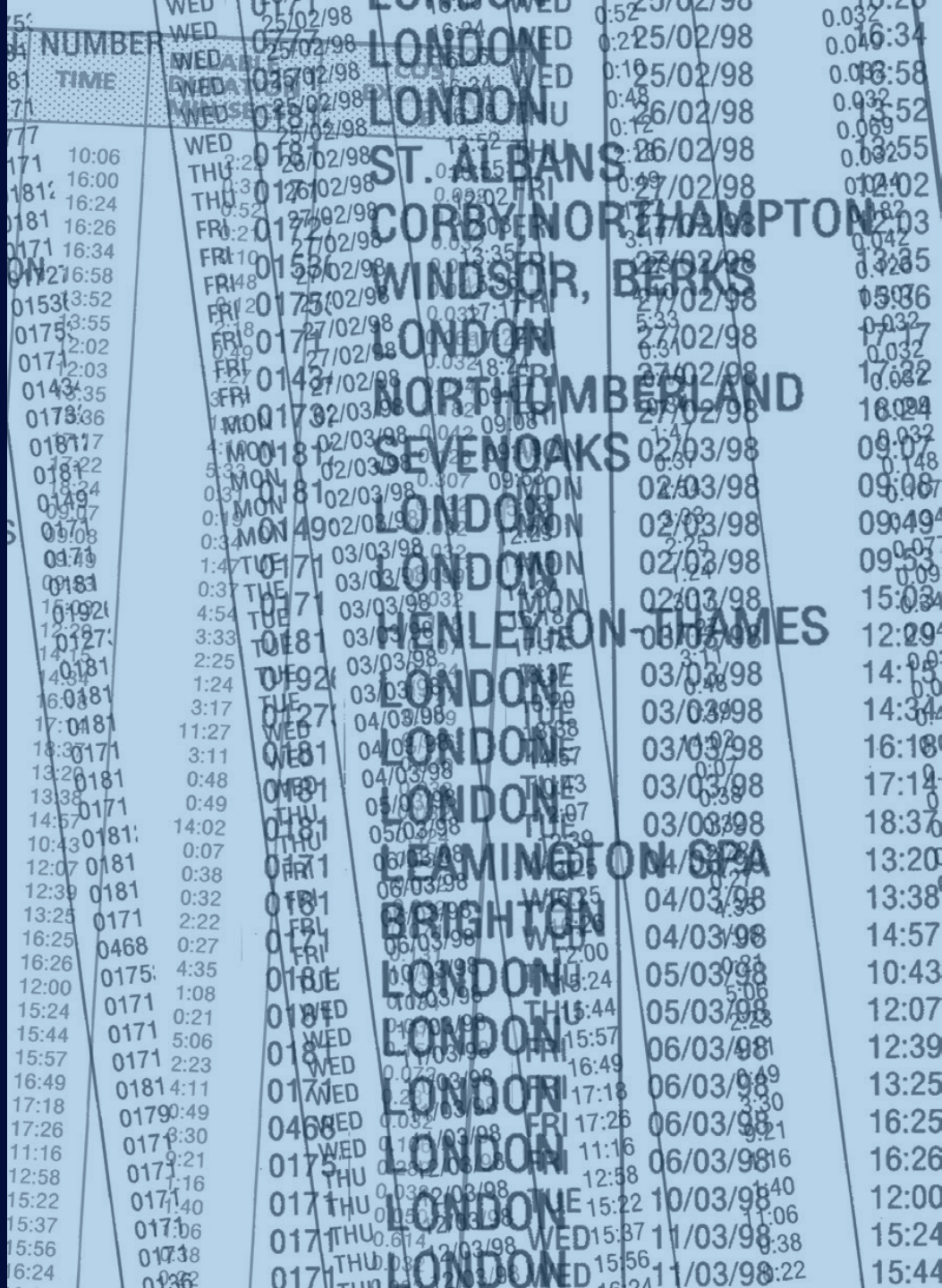
Another standard hardening practice is to turn off any unused services. A good rule of thumb is that if you aren't using a feature you want to shut it down. This lessens the potential attack surface. For example, if you are using voice, video and email communications but aren't using chat, then it is best to turn off the chat functionally in the UC server. Not only does this improve security, but this will also improve performance as you will have less protocol traffic on the network and your server will be less taxed because it is doing less work.



6 Monitor Your Call Logs

Often attacks go unnoticed until a great amount of damage is done. Regularly reviewing system logs could allow you to detect an attack early. Running regular reports on toll calls can help create a baseline for normal activity. You'll then be able to notice excessive activity.

Sometimes you may be able to enlist the help of your upstream provider. They may be able to notify you after a predetermined limit on toll-based calls is exceeded. Unfortunately, many providers do not offer such features. Instead it is your responsibility to monitor your logs and ensure that long distance calls are intended.



7 Use built-in UC security tools

The best way to secure your UC devices is to use dedicated security equipment, like VPNs and firewall routers. However, taking advantage of built-in security tools can add an extra level of protection. Digium Switchvox, for example, comes with security tools such as Access Control Rules, Automatic IP blocking and managed tech support access. The blocked IPs tool will block IP addresses that fail multiple registration attempts. In theory, a properly configured firewall should prevent SIP scanners from being able to reach your UC server, however this additional level of security adds peace of mind and works as a functional back-up to round out your security suite.

Security is your responsibility.

Not all security advice is applicable in all situations. Discern for yourself whether the information offered in this eBook is appropriate for your scenario and make the judgment that is best for you.

Has this eBook been helpful for you?

Share your security concerns and questions with us on Twitter @Digium

For more information on Unified Communications solutions, visit **www.digium.com/en/solutions**

digium®
The Asterisk Company

digium®
The Asterisk Company

Digium®. We're changing the way businesses communicate.

Founded in 1999, Digium is the creator and primary developer of Asterisk, the industry's first open source telephony platform. More than one million customers in 125 countries have deployed Asterisk-based systems. Digium is committed to ending the days of expensive, proprietary telecom. The Switchvox family of Unified Communications solutions is built on Asterisk and is designed to provide enterprise class features at affordable prices for small and medium businesses.

The award-winning line of Switchvox IP PBX phone systems provides more than a phone system – it delivers a Unified Communications platform that integrates multiple features that increase productivity and lower monthly communication costs. It's the affordable solution with a proven return on investment for businesses with 10 to 400 users.

Learn more at digium.com/switchvox

Want more information on Switchvox?
Take a virtual tour of this powerful Unified Communications platform:
www.digium.com/switchvox

Contact us – we're here to help.
Talk with a Switchvox specialist:
1 877 344 4861
1 256 428 6271
sales@digium.com