Report Number: I332-009R-2006

Recommended IP Telephony Architecture

Systems and Network Attack Center (SNAC)

Updated: 1 May 2006
Version 1.0

SNAC.Guides@nsa.gov

This Page Intentionally Left Blank

Warnings

- Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.
- This document is only a guide containing recommended security advice. It is not meant to replace, but to supplement, well-structured policy and sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- Following the recommendations in this guide does not guarantee that an IP telephony system will be secure against all attacks, but will make successful attack more difficult.
- Revisions may be made at any time; the Changes section will track modifications.

This Page Intentionally Left Blank

Table of Contents

Introduction

IP telephony (IPT) systems are replacing legacy PBX systems in both government and enterprises due to expectations of cost and feature advantages. It is important that taking advantage of these benefits does not put sensitive information and mission continuity at risk. It is also imperative that U.S. Government agencies carefully consider the security implications of deploying IP telephony systems. While IP telephony systems can be secured, doing so requires careful evaluation, detailed planning, measured deployment, continuous testing, and vigilant maintenance.

IP telephony systems are considered to be any primary voice communication system, which uses an IP network as the underlying transport for signaling and media. An IP telephony system that is replacing an existing legacy PBX system would fall into this category. The primary goal of this architecture is to supply highly reliable, available, and secure unclassified voice services. IP telephony also creates an opportunity to use applications that were not possible or convenient with legacy systems. While this architecture does make provisions for using these applications, such use is a secondary goal.

This architecture is not an implementation guide and is pertinent to IP telephony systems from all vendors. It provides a high-level view of the necessary aspects of a secure IP telephony system. Elaboration on points made in this architecture can be found in *Security Guidance for Deploying IP Telephony Systems* at http://www.nsa.gov/snac.

General Architecture Guidance

IP telephony security should be tailored to the specific threat environment. Doing this successfully requires developing a security policy which specifies the importance of the information to be protected and defines what security mechanisms are needed to adequately protect that information. Securing IP telephony also requires developing a deployment plan, which does not leave the IP telephony system vulnerable before it is completely deployed.

A defense-in-depth approach is required to protect the many components of IP telephony systems. Defenses should be deployed in the network, at the network perimeter, within the IP telephony applications, and in all IP telephony end points.

Network security mechanisms limit attacker access to crucial IP telephony services, prevent impersonation of network hosts by insiders, make eavesdropping on calls more difficult, and help ensure availability of service. Perimeter security controls keep unauthorized users from accessing the internal network and ensure both Public Switched Telephone Network (PSTN) and voice over IP (VoIP) connections to the outside do not compromise the network. Authentication and encryption in the application-layer prevent eavesdropping and impersonation of IP telephony end points. Finally, security hardening of end points and servers reduces vulnerabilities and limits extraneous functionality.

Best practices are also essential for IP telephony systems. While this guide describes a high level architecture, security hardening of the many devices, computers, operating systems, and applications involved is critical. Other guides, such as those from the NSA (http://www.nsa.gov/snac), Defense Information Systems Agency (http://iase.disa.mil), and National Institutes of Technology (http://csrc.nist.gov), can assist in securing these other portions of IP telephony systems.

IP Telephony Architecture

The recommended architecture aims to provide highly reliable, available, and secure IP telephony services. Figure 1 illustrates the logical network architecture. Not shown or discussed here is the network architecture necessary to provide the bandwidth for IP calls and redundancy necessary for high availability.

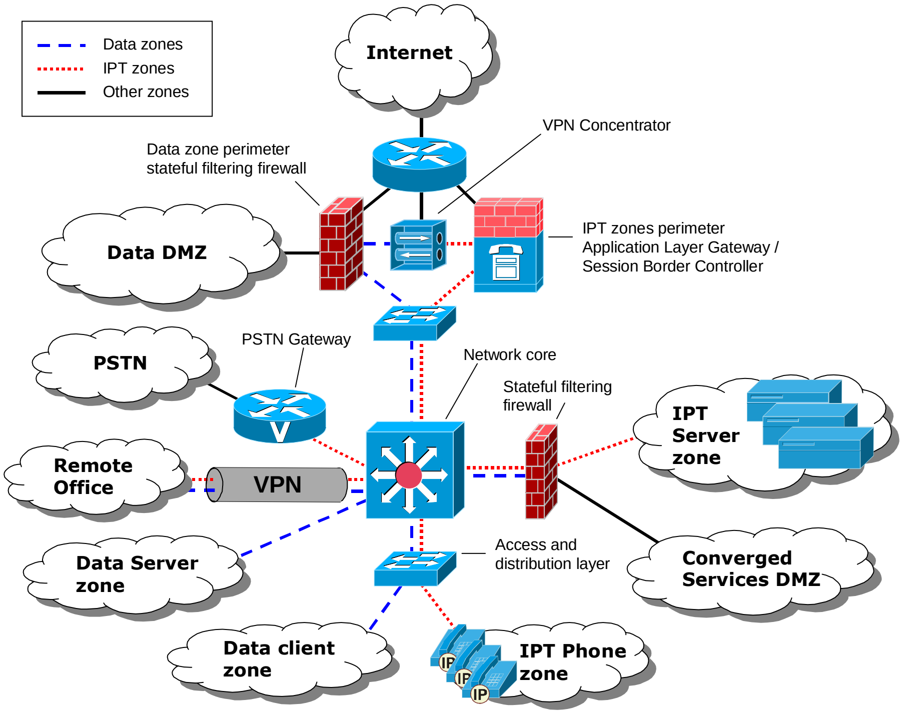

Figure 1 - IP telephony recommended network architecture. The network is divided into security zones represented by network clouds. The administrative security zone is not shown.

Establishing Security Zones

The network should be divided into multiple security zones. A security zone contains a common set of devices that need similar protections. It controls access to these devices from the rest of the network by allowing only authorized hosts and protocols access to the security zone.

Security zones are implemented using a combination of virtual LANs (VLANs) and access control lists (ACLs). Each security zone should have one or more dedicated VLANs. A specific IP address space should be assigned to each zone. Traffic between security zones should be filtered using ACLs on the routers and switches connecting security zones. Filtering should limit the interactions of devices in different security zones. Different products use different protocols and different mechanisms to provide service, and thus will have different filtering requirements. Properly configured, security zones make it more difficult for an attacker to move throughout the network and to attack more critical portions of the network.

Traffic allowed between security zones falls into four categories. Signaling traffic is used for call setup and control. Media traffic consists of voice, video, and other real time multimedia. Administrative traffic includes the protocols for managing and auditing devices. Network services traffic is protocols needed by end points to make use of the network, such as DNS and DHCP.

The following security zones should be established:

- Data security zone – Contains existing data IP services such as email, DNS, DHCP, file servers, web servers, and end user PCs. This zone could be broken into additional zones per an organization's security requirements. No network traffic is allowed directly between this zone and the IP telephony zones.
- IP Phone security zone – Contains IP phones. Call control signaling, phone configuration, and network services traffic is allowed between this zone and the IPT Server zone. Media traffic is allowed between this zone and the IPT Gateway zone.
- IP Telephony Server security zone – Contains IP telephony servers implementing IP phone and gateway call control signaling, configuration, authentication, authorization, and DHCP for the IP telephony zones. Provides network services to the IP Phone and IP Telephony Gateway zones. If local security policy allows, this zone may share media traffic with the IP Phone zone when servers provide automated services, such as voice mail and teleconferencing, which are limited to IP telephony devices only.
- IP Telephony Gateway security zone – Contains PSTN gateway devices. Signaling and network services traffic is allowed between this zone and the IPT Server zone. Media traffic is allowed between this zone and the IP Phone zone.
- Administrative security zone – Contains workstations used to administer the network and IP telephony infrastructure. All management of network and IP telephony devices is done from within this zone. Only this zone is allowed to access remote administration services or interfaces on devices in other zones.
- Converged Services security zone – Contains devices necessary to offer services, such as unified messaging, which need access to both the IP telephony and Data security zones.

Figure 2 further illustrates the traffic allowed between IP telephony security zones.

In most cases, stateless filtering is sufficient between security zones. However, the IP Telephony Server and Converged Services security zones need additional and more complex protection. A stateful filtering firewall, possibly with VoIP specific capabilities, is necessary to secure these zones.

Perimeter Protections

IP telephony connections to the public switched telephony network (PSTN) are made using PSTN gateways, which convert VoIP to circuit-switched PSTN trunk lines. The PSTN gateway should authenticate all VoIP connections and not allow IP phones to control the gateway without authorization from the IP telephony servers. If possible, the gateway should only accept signaling traffic from the IPT Server zone and signaling traffic from the IP Phone security zone should be disallowed.

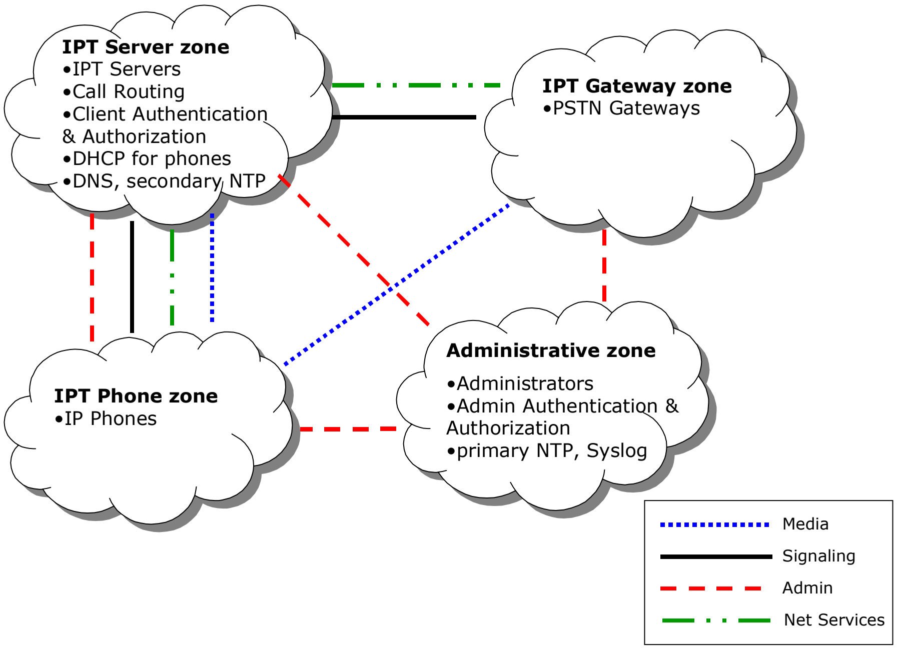

Figure 2 – Types of network traffic allowed between IP telephony security zones. Media traffic includes voice, video, and other real time multimedia traffic. Signaling traffic is used for call control. Admin traffic consists of protocols used to manage and audit devices. Network services traffic is protocols needed by end points to use the network, such as DHCP and DNS. Filtering can and should be more restrictive than shown if specific architecture implementations do not require a particular traffic type between security zones.

Instead of a traditional circuit-switched connection to the PSTN, an agency may interconnect with other organizations using VoIP over public networks or VoIP trunks from a service provider. In this case, a VoIP application layer gateway (ALG) or session border controller (SBC) should be used between the internal and external networks. VoIP ALGs and SBCs serve similar functions. This device should be able to dynamically open ports for media traffic based on the contents of the signaling traffic and perform sanity checks on signaling protocols. If network address translation (NAT) is used, then either the ALG must be able to translate the IP addresses inside the signaling traffic or IP telephony end points must use protocols such as Simple Traversal of UDP through NAT (STUN) to learn externally valid IP addresses.

In the recommended architecture, two firewalls are used between the internal network and the public network. One firewall handles data traffic and the other is a VoIP ALG or SBC. Appropriate traffic is routed to each firewall by the border router.

VoIP trunks may also be used to provide voice services to remote offices over public IP networks. In this case, VoIP trunks should be tunneled over encrypted VPN connections between offices. Separation of security zones should be maintained across the VPN. This can be done with separate VPN tunnels for each security zone, or by carefully configured routing and policy rules at each end of a VPN tunnel.

Network Layer-2 Protections

To prevent easy spoofing of media access control (MAC) addresses and IP addresses, layer-2 protections should be enabled on all Ethernet switches. This is especially important for protecting critical devices such as servers and default IP gateway routers.

Limits should be placed on the number of MAC addresses allowed per port to prevent MAC table overflow attacks against the switch. When possible, static MAC addresses should be assigned to each port. This is always recommended for critical devices such as servers and default IP gateway routers.

To make device impersonation more difficult, no devices should accept gratuitous Address Resolution Protocol (ARP) messages.

Additional security features, available from some vendors, monitor DHCP messages and, based on the contents of DHCP messages, build a table associating switch port, MAC address, and IP address. Ethernet frames and IP packets inconsistent with the table are dropped. This allows the safe use of DHCP to configure IP phones while preventing spoofing of MAC and IP addresses.

Authentication and Encryption

Strong authentication and encryption of all signaling and media traffic prevents eavesdropping and impersonation by attackers. Strong mutual authentication of signaling is a minimum requirement. Multiple mechanisms are available to accomplish this. Many enterprise level IP telephony systems support application-layer authentication and encryption of signaling traffic using Transport Level Security (TLS) and of media traffic using the Secure Real Time Protocol (SRTP). IPSEC is another option that may be offered by some IP telephony vendors. An IP telephony system that utilizes a proven and standardized protection protocol such as TLS, SRTP, and IPSEC is recommended. Systems using proprietary or non-standard mechanisms should be evaluated before use.

All cryptography should meet policy requirements of the agency implementing the IP telephony system.

Availability

IP telephony services depend on the underlying IP network to provide signaling and media transport. Thus, availability of telephony services depends on the availability of the underlying network as well as of the IP telephony components. The necessary availability level should be determined during security policy development.

In case of a power outage, telephony services should continue to operate for a defined period of time. This requires that all network devices and IP telephony components be provided with backup power. IP phones could use power over Ethernet. In this case, the backup power for the Ethernet switches should be sufficient to power both the switches and the IP phones attached to them. If power over Ethernet is not used then an IP phone with its own backup power supply should always be accessible to users.

To ensure quick recovery from power outages, system crashes, and attacks, data backups of all network and telephony devices should be kept in multiple secure locations. A tested backup and recovery procedure should also be in place.

All essential IP telephony components should feature high availability hardware. IP telephony servers should immediately failover to standby servers.

Denial of Service Protections

IP telephony systems are vulnerable to denial of service (DoS) attacks. Rate limiting is the recommended way of dealing with DoS attacks. VoIP connections from outside the network should be limited so there is always sufficient capacity inside the network to handle essential call volumes. Traffic into the IP telephony security zones should be controlled to prevent loss of service. If VoIP trunks over public IP networks are used, then either a secondary IP network connection or circuit-switched PSTN trunk should be maintained in the event an attack disables the primary network connection.

Quality of service tags should be applied to media and signaling packets, and routers should prioritize these packets such that if the network becomes congested, routers will forward media and signaling packets and drop other packet types first.

Physical Protection

All network and telephony infrastructure devices, such as routers, switches, and servers, should be located in controlled access areas. Locks using identification cards, biometrics, or other electronic means can also provide useful auditing information about access to equipment.

These areas should also be free of any potential threats from fire or flooding. They should have appropriate fire suppression systems and be protected from water sources.

Video surveillance may be appropriate for some installations depending on individual requirements.

Device Management

To limit operational impacts and ease deployments, an IP telephony testbed is recommended for off-line verification of security features and new or additional devices.

When a phone is added to the network it must be configured with network information and told where the telephony servers reside. Using DHCP is an acceptable solution when the DHCP protections discussed in Network Layer-2 Protections are enabled in the network. Otherwise, network information should be statically configured before deployment. The phone must also be allocated an account and phone number on the IPT server. Some IP telephony systems can do this automatically. This is not recommended except during the initial deployment of a large number of IP phones. Once the phones are deployed, this feature should be disabled or unauthorized "rogue" devices could easily establish themselves on the network.

Most IP telephony systems offer the capability to remotely manage the phones and servers. Remote management of phones is particularly crucial given the large number of phones deployed. Only secure remote management techniques should be used. Often IP telephony devices will download software upgrades and configuration files using the Trivial File Transfer Protocol (TFTP) from the IP telephony server. By itself, this is not an acceptable level of protection. Either an authenticated and encrypted connection, such as TLS or IPSec, should replace or encapsulate TFTP for downloading the files, or the file integrity should be protected with a digital signature. Files should also be encrypted if they contain sensitive information, such as passwords.

IPT servers are best managed locally, but could be remotely managed over an authenticated and encrypted connection from a workstation in the administrative security zone. (For example, using HTTPS to access a web-based administrative interface.) Proprietary management solutions that do not meet these recommendations should be tunneled through a connection that does. Remote management of IP phones should meet the same requirements.

In general, for all IP telephony devices, choose a secure remote management technique that meets these requirements, disable all others, and disallow unused management protocols with network filters.

Convergence Services

Many IP telephony systems offer advanced features that converge the functionality of multiple different communication methods into a single system. For example, data services are presented through IP telephony devices or voice mail is sent to a user's email inbox and a user can access their email through the voice mail system.

These converged applications require allowing traffic between the IP Telephony and Data security zones. In order to keep the security zones as isolated as possible a separate security zone should be created that acts as a demilitarized zone between the IP Telephony security zones and the Data security zones. Converged application servers should be placed into this Converged Services security zone. Access to this zone should be controlled by a stateful filtering firewall and application layer proxies. Malware scanning should also be done in this security zone if executable content could be shared between IP Telephony and data security zones.

Emergency Services

Emergency services can be more difficult to implement in IP telephony systems. Some emergency services require identifying the physical location of the user. This can be difficult, because IP telephony allows users and their phones to easily change location. One solution is to maintain a database of phone locations, though updates may have to be made manually. Solutions to this problem are currently immature.

The level of support needed for such services should be carefully considered and incorporated into an organization's local policy.

Soft Phones

A soft phone is an application that runs on a general purpose device and provides IP phone capabilities. In general, the use of soft phones is not recommended. First, the security and availability of the soft phone is dependent on the underlying device. The general purpose nature of the device means other uses of the device may threaten voice services. Second, the use of soft phones also violates the IPT Phone and Data security zone restrictions.

When needed, soft phones should only be used as a secondary communication means. A separate security zone should be established for devices using soft phones.

Conclusion

This recommended architecture emphasizes defense-in-depth and best practices. However, the recommendations should be applied only after taking into consideration security policy and operational needs. Not all recommendations may be appropriate for all networks. Many of the recommendations can be applied to any network application that is crucial for day-to-day mission operation. These recommendations also serve to improve the general security of the network. While not all aspects of the architecture are easy to implement and maintain they do serve as a high barrier to attackers.

Changes

Version 1.0, 1 May 2006

- Initial release.