Gartner

Research

Publication Date: 7 June 2005 ID Number: G00128097

Deploying Secure IP Telephony in the Organization

Bjarne Munch

Secure IP telephony deployment remains a key business concern, although most deployment can be fully secured. The threat of privacy invasion, service downtime or an overinvestment in security means risks must be evaluated and mitigated for all sites and externally hosted IP-PBX or IP Centrex.

The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

TABLE OF CONTENTS

LIST OF FIGURES

ANALYSIS

While a range of generic risks can be identified, it is important to recognize that not all risks are present or critical in all deployments. Thus, from a solution-design-and-deployment point of view, these risks must be evaluated and mitigated within the context of the specific IPT solution. The following is a recommended security mitigation process for three typical IPT uses:

- Office internal deployment — Single site
- Office internal deployment — Multiple sites
- Externally hosted IP-PBX or IP Centrex

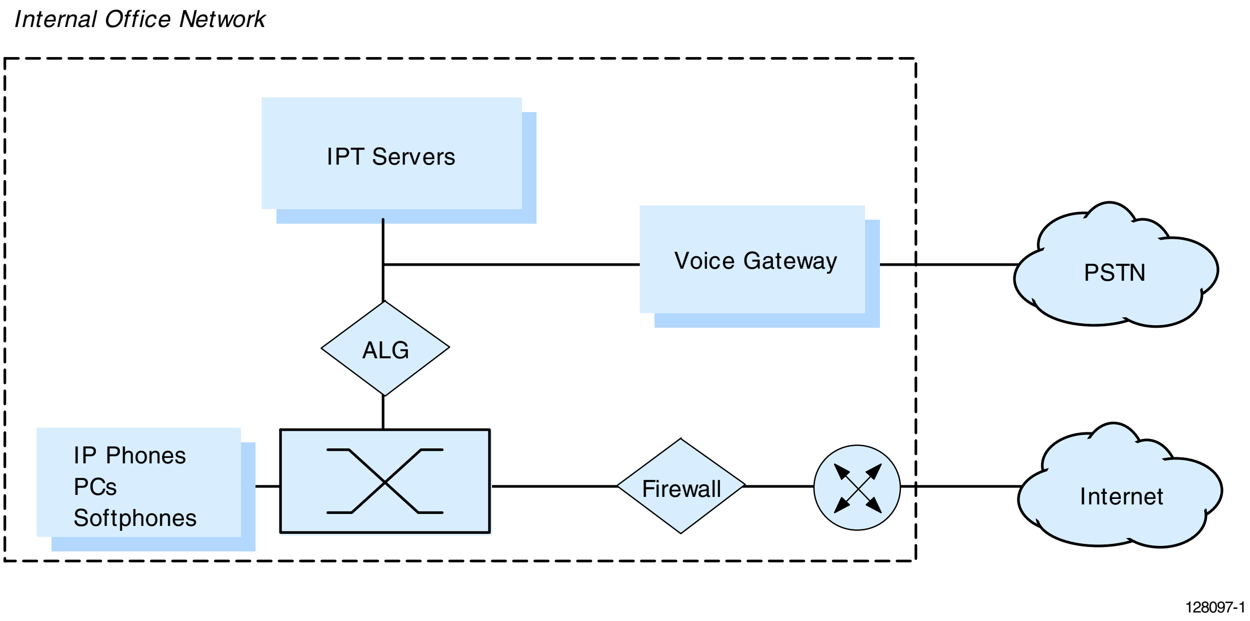
The following recommended security best-practice solutions follow the security architecture and principles outlined in "IP Telephony Security Principles."

1.0 Office Internal Deployment on a Single Site

In the first case, an IPT solution is deployed solely within a single enterprise network site, as illustrated in Figure 1. The IPT system does not support IPT traffic to and from any phones external to that specific site. This is a typical deployment scenario for "Greenfield" sites, PBX upgrades or small and midsize business (SMB) installations, and for most large organizations this is typically the first step in migration toward corporatewide, multisite deployment.

Figure 1 illustrates the main components that need consideration for the security solution. IPT servers is a general description of all call control servers, mail servers and conferencing servers involved in a specific IP telephony product. Voice gateway is the component performing a conversion between IP telephony to traditional TDM based telephony (of both voice and signaling). A firewall is a traditional firewall, while an Application Level Gateway (ALG) is defined as IPT-specific screening (session oriented screening of signaling protocols and voice streams) which can be a stand-alone device or embedded within a firewall.

Figure 1. Simplified Network for Single Site Internal Deployment



Source: Gartner (May 2005)

1.1 Protecting the Voice Conversation

Clients should recognize that eavesdropping protections are rarely the place to start or the top concern. With proper network design, it will require more knowledge to intercept and play back an IPT conversation than to tap a traditional analog telephone conversation. However, the focus on eavesdropping is strong within the press, and vendors have launched IP phones with native encryption of both voice and signaling. Three basic common practices will ensure that privacy is equal to that of traditional PBX deployments, if not better:

- Deploy a fully switched Ethernet connection from all IP phones to the wire closet; if possible, ensure Layer 2 connectivity end-to-end
- If routing is required because of network size, ensure physical protection of the router, as well as hardening of the router (that is, restrict Telnet and Simple Network Management Protocol access, turn off unneeded services, ensure strong management access control and log all activities).
- Guard against physical access to the wire closet and all active network devices as in most traditional PBX deployments.

The principle, as always, is to keep it simple. While encryption is increasingly being discussed, it is also desirable to avoid it, because it will mean less latency, fewer complications, and less maintenance. Public switched telephone network (PSTN)-comparable privacy is possible without encryption in most cases. As a basic rule, if data traffic is encrypted then voice traffic should also be considered encrypted.

1.2 Protecting IPT Components

The main risks relevant to IPT components are hack attack and denial-of-service (DOS) attack or virus attack. Hack and DOS attacks can be assumed to originate predominantly from external parties, and effective protection is obtained by ensuring strong perimeter security. The perimeter firewalls need not be IPT-aware but must block all IPT-related port numbers and protocols, because the IPT traffic is purely internal. All platforms should be hardened (unused ports closed, unnecessary executables removed, patching updated, and so forth) and, as an added precaution, intrusion prevention should monitor for abnormal traffic patterns to and from the IPT platforms. Any type of administrative interaction should be from dedicated and protected computers, and only via strong access control (that is, two-factor authentication or frequently changed, well-formed passwords with usage logging).

The most critical risk to IPT components are related to virus attack, worms and so forth. These enter the corporate network via e-mail, file-downloads and unprotected computers and propagate to the IPT components. The following standard virus protection should be implemented:

- Install antivirus software on critical IPT servers
- Harden all platforms (remove all unneeded services, close all not used ports)
- Keep up to date on all new patches.
- For high-reliability requirements, install fully redundant control servers on a separate network segment.
- For IP phones with an embedded Web-browser, prevent access to external Web-content.
- As an extra precaution, place all critical servers on a dedicated network segment behind an IPT-aware firewall.

1.3 Protecting Against Fraudulent Use

Fraudulent use can originate either from unauthorized users gaining access to the system or from authorized users with unauthorized traffic patterns. Traditional PBX-type practices to provide protection must be applied, which means controlling users call profiles (local, long-distance, and international), restricting call routing tables (such as rerouting of incoming calls to the PSTN) and hardening message servers to prevent outgoing calls. While fraudulent use is often discussed, it is relatively easy to prevent; unauthorized users should be prevented via strong access control, as well as intrusion prevention.

1.4 Protecting Management Access

Remote management of the devices can be done "out of band" or "in band." Best practice dictates out of band, because dedicated network access is easier to secure than in-band access where user telephony and management traffic are mixed on the same access.

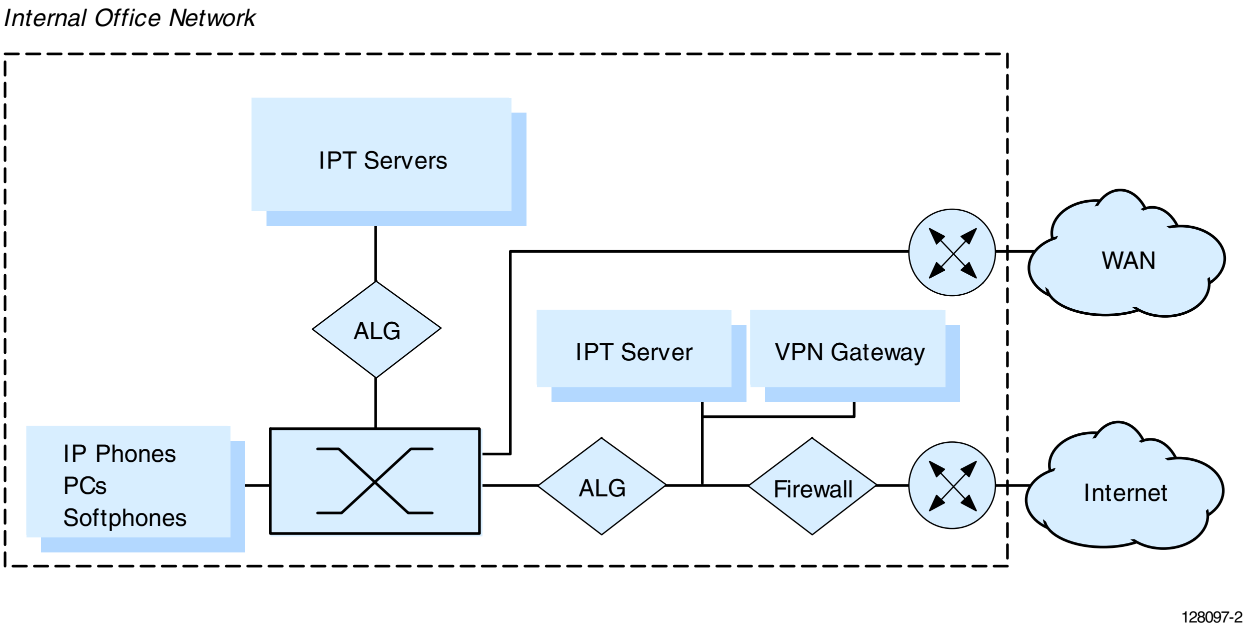
- Out-of-band management requires a dedicated network interface from the device and, preferably, a dedicated connection to the WAN. This could be via a dial-back PSTN/Integrated Services Digital Network connection, as for traditional private automatic branch exchange management, or a properly secured IP connection.
- In-band management should be used only when out of band is not feasible and only if a dedicated IP VPN can be established directly from the management system to the device. Access from the production network should not be allowed with a dedicated IP VPN tunnel.

In both cases, management access should be controlled via strong authentication, and any IP VPN tunnels should be locked down to pre-configured hosts and port numbers.

2.0 Office Internal Deployment Over Multiple Sites

In this case, the IPT solution is deployed solely within the organizational network but distributed over a number of sites. The IPT system will, thus, need to support IPT traffic across the corporate WAN or across the Internet for remote workers and small offices, as illustrated in Figure 2. This is a typical deployment scenario for large corporations with a strategic view that are consolidating small distributed key systems, and to support home workers, traveling employees and SMB deployments.

Figure 2. Internal IP Deployment With Geographical Distribution



Source: Gartner (May 2005)

Risk mitigation similar to the internal single site deployment must be applied, but additional measures must be implemented because of the potentially increased external exposure. Support of remote workers, or even external partners, using the IP-PBX service via the Internet must be secured via an IP VPN. Typically, an IP VPN is utilized for such remote data connectivity, and this IP VPN can be shared with voice traffic. However, overhead costs associated with IP VPN tunneling (packet overhead, latency and so forth) must be taken into account. To protect the internal network from DOS attack or hack attack, a call-control server can be placed in the demilitarized zone (DMZ) to manage all calls from Internet connected users. This is illustrated in Figure 2, where the DMZ is described as an application-aware firewall and a firewall. The external perimeter firewall in this case needs no IPT awareness, because all external traffic is tunneled by IP VPNs, and the firewall needs to block all specific IPT ports. The internal firewall, however, must be implemented with IPT awareness or application-aware firewall to fully control traffic into the network.

2.1 Protecting Voice Conversation

Protective mechanisms similar to those described earlier should be implemented. However, protective measures must be added for the following voice transmission between sites:

- For remote workers and small offices connected via the Internet, a secure IP VPN must be used.
- For traffic between sites interconnected via a traditional WAN carrier service, voice traffic would typically not need to be encrypted. However, the evaluation as to whether the WAN needs to be secured should be made for all business important services. As a basic rule, if data traffic is encrypted then voice traffic should also be considered encrypted.

2.2 Protecting IPT Components

Protective mechanisms similar to those described earlier should be implemented. However, as a result of exposure to the Internet, the following additional considerations are required:

- Only voice traffic arriving via the IP VPN or via the WAN should be accepted.
- IPT traffic from outside the IP VPN must be blocked by the external firewall. Because all voice is transmitted via the VPN, this firewall does not need to be IPT-aware, but it must block all IPT-specific port numbers and protocols, except carefully controlled signaling traffic
- The firewall on the inside of the DMZ should be an IPT-aware Application Level Gateway (ALG) and must be capable of performing IPT-specific DOS protection (for both signaling and voice traffic).
- As an additional measure, a call-control server can be placed in the DMZ for control of all traffic over the Internet. This will add extra protection of the core system against DOS and other attack types.
- Virus protection must be performed throughout the organization, at minimum there should be antivirus software on all PC, as well as e-mail proxy and Web server.
- IPT-aware intrusion prevention should be placed strategically within the network, as a minimum in the DMZ, toward the public Internet and if possible as Host Intrusion Prevention on the IPT servers.

2.3 Protecting Against Fraudulent Use

Unauthorized use protection starts with the protective mechanisms described earlier. However, because of exposure to the Internet, additional considerations are required:

- Only voice traffic arriving via the IP VPN should be accepted.
- Traffic arriving from outside the IP VPN must be blocked by the external firewall.

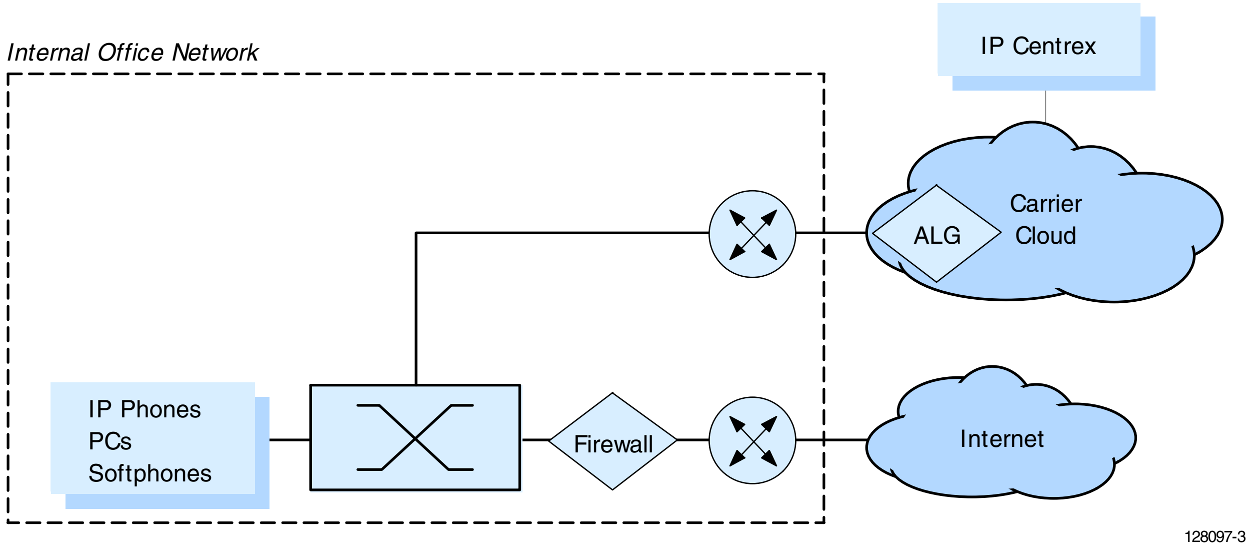
2.4 Protecting Management Access

Protective mechanisms as described earlier should be implemented.

3.0 Externally Hosted IP-PBX or IP Centrex

In this case, the IPT solution is deployed as a hosted IP-PBX or as an IP Centrex solution, all IPT control servers are placed in the carrier network, and only IP phones or softphones are placed within the organizational network, as illustrated in Figure 3. All telephony control signaling will pass to the IP Centrex, and the voice traffic will either stay within the network or flow to other sites across the carrier cloud.

Figure 3. Externally Hosted IP-PBX or IP Centrex



Source: Gartner (May 2005)

The risk mitigation in this deployment scenario is significantly different from the earlier scenarios, because this solution is based on trust in the carrier's ability to deploy and maintain a secure and reliable infrastructure. Because of the carriers' limited experience in delivering this type of service, it is highly recommended that businesses evaluate design principles, personal training and operational processes. In particular, the carrier infrastructure used for IPT services must be fully private and not shared with any public Internet service.

Because only fully trusted providers should be used for this type of service, no specific need exists to separate access connections for data and voice traffic. The WAN is an extension of the LAN and should be deployed with similar security architectural principles, as in case No. 2 above. This means that as an added precaution, the carriers must maintain separate VPN configuration for voice and data, and this separation should be controlled via an ALG placed within the carrier network. If different carriers are used for data and voice services, they should maintain separate access connections.

3.1 Protecting Voice Conversation

Within the organizational network, voice conversation is protected, as described earlier, by maintaining a switched connection. Within the carrier "cloud," protection will depend on the carrier, and it can not be assumed that encryption can be used end to end, because it may interfere with such carrier functionality as call control, three-way calls, conferencing and voice messages. As part of the carrier requirements listed earlier, it should be mandatory that transmission within the carrier cloud be performed only via controlled tunnels permanently established among all IPT components.

3.2 Protecting the IPT Components

Within the organizational network the only IPT components are the IP phones and softphones. These need to be protected, as described earlier, in the following way against virus attack, DOS attack and other types of hack attack:

- Only voice traffic arriving from the IP Centrex connection should be accepted. This must be controlled by an ALG within the carrier network.
- IPT traffic arriving from the Internet must be blocked by the perimeter firewall. This firewall need not be IPT-aware, but it must block all IPT-specific port numbers and protocols.
- A firewall must be placed at the edge of the carrier network. It must be an IPT-aware ALG and be capable of performing IPT-specific DOS protection for signaling and voice traffic.
- Assuming that the IP phone will be configured with the address of a corporate managed Dynamic Host Configuration Protocol server and thus part of the corporate IP address space. The ALG must also be capable of IPT-specific network address translation between the internal network and the carrier network.
- Virus protection must be performed throughout the organization; at the very least, there should be antivirus software on all PCs as well as e-mail proxy and Web server.
- IPT-aware intrusion prevention should be placed strategically within the network, as a minimum in the DMZ toward the public Internet.

3.3 Protecting Against Fraudulent Use

In this deployment scenario, any type of prevention against fraudulent use must be implemented by the carrier. These measures should include the following:

- Ensure strong authentication and access control to enterprise account usage.
- Ensure that all traffic use for a specific organization is, in fact, originating from that organization. This can be done by establishing tunnels from all edge ALGs to the IP Centrex and accepting traffic only from those tunnels.

4.0 Bottom Line

IT organizations must evaluate all risks in context of the desired IPT solution, otherwise appropriate solution design can not be performed. Without properly evaluating specific risks, the business is exposed to an increased likelihood of privacy invasion or service downtime, or a significant overinvestment in security mitigation.

Acronym Key and Glossary Terms

ALG	application-level gateway
DOS	denial of service
DMZ	demilitarized zone
IPT	Internet Protocol telephony
PSTN	public switched telephone network
SMB	small and midsize business
SNMP	Simple Network Management Protocol

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509