



CoralIPx **Coral FlexiCom**TM
The flexible way to communicate

**Coral[®] Security Aspects
IP Telephony Risks from PSTN and IP Networks
White Paper**

The information contained in this document is proprietary and is subject to all relevant copyright, patent and other laws protecting intellectual property, as well as any specific agreement protecting TADIRAN TELECOM® LTD.'s (herein referred to as the "Manufacturer") rights in the aforesaid information. Neither this document nor the information contained herein may be published, reproduced or disclosed to third parties, in whole or in part, without the express, prior, written permission of the Manufacturer. In addition, any use of this document or the information contained herein for any purposes other than those for which it was disclosed is strictly forbidden.

The Manufacturer reserves the right, without prior notice or liability, to make changes in equipment design or specifications.

Information supplied by the Manufacturer is believed to be accurate and reliable. However, no responsibility is assumed by the Manufacturer for the use thereof nor for the rights of third parties which may be affected in any way by the use thereof.

Any representation(s) in this document concerning performance of the Manufacturer's product(s) are for informational purposes only and are not warranties of future performance, either express or implied. The Manufacturer's standard limited warranty, stated in its sales contract or order confirmation form, is the only warranty offered by the Manufacturer in relation thereto.

This document may contain flaws, omissions or typesetting errors; no warranty is granted nor liability assumed in relation thereto unless specifically undertaken in the Manufacturer's sales contract or order confirmation. Information contained herein is periodically updated and changes will be incorporated into subsequent editions. If you have encountered an error, please notify the Manufacturer. All specifications are subject to change without prior notice.

© Copyright by TADIRAN TELECOM® LTD., 2010.
All rights reserved worldwide.

The Coral is protected by U.S. Patents 6,594,255; 6,598,098; 6,608,895; 6,615,404

All trademarks contained herein are the property of their respective holders.

Table of Contents

1	IP Telephony Risks from the PSTN	4
1.1	Introduction.....	4
1.2	Risks to the Internal LAN from the PSTN via VoIP Gateway.....	4
1.3	Mitigation of Risks to the Internal LAN from the PSTN	6
1.4	Conclusions.....	7
2	Risks from IP Networks	8
2.1	Introduction.....	8
2.2	Risks to the Internal LAN from the Internet.....	8
2.3	Mitigation of Risks to the Internal LAN.....	9
2.4	Improving the integrity of VOIP clients	12
2.4.1	Central Call Control and Related Components Segment	12
2.4.2	Peripheral VoIP Elements Segment	12
2.4.3	Voice Associated Work Stations Segment	13
2.4.4	Administrator Data Segment	13
2.4.5	General Intranet Data Segment.....	13
2.4.6	Bastion Segment.....	13
2.4.7	Internet Segment.....	13
3	Tadiran Coral Solution	14
3.1	Nat Traversal.....	14
3.2	Stateful Inspection	14
3.3	Authentication.....	14
3.4	Encryption.....	15
3.5	DoS Protection	15
3.6	Zone Isolation	15
4	Appendix	16

1 IP Telephony Risks from the PSTN

1.1 Introduction

This paper discusses the risks to an enterprise's internal LAN from the telephone network when a Voice-over-IP (VoIP) gateway is installed between these two networks. The paper analyzes the means by which these risks may be exploited and the likelihood of exploitation. It goes on to discuss the reasons why Tadiran Telecom's Coral VoIP servers are not susceptible to these risks.

This VoIP security white paper is written for IT personnel, in general, and specifically for information security managers.

1.2 Risks to the Internal LAN from the PSTN via VoIP Gateway

Attacks on an enterprise's internal LAN from the public telephone system via VoIP services are rare in comparison with attacks from the Internet via VoIP. In fact, PSTN-based attacks, although theoretically possible, are almost unknown. This is probably due in large part to the fact that phone networks consist mainly of closed special-purpose systems that tend to change rather infrequently. General-purpose systems, common in the Internet, are susceptible to multi-stage attacks in which a new vulnerability in one part of the system is created by exploiting an existing but unrelated vulnerability in another part of the system.

Special-purpose systems are less susceptible to such multi-stage attacks, since their functionality is limited and dedicated to a specific task. Change may fix old vulnerabilities, but they often introduce new vulnerabilities, usually more than they fix. This does not imply that you should not install new fixes! Most security fixes plug critical holes in software, so that you really have no choice. It is just that most changes overlay old code with new code and, as Donald Knuth said, the more code you have, the less debuggable it becomes. So if PSTN systems change less frequently, then they present fewer opportunities for phone hackers to exploit.

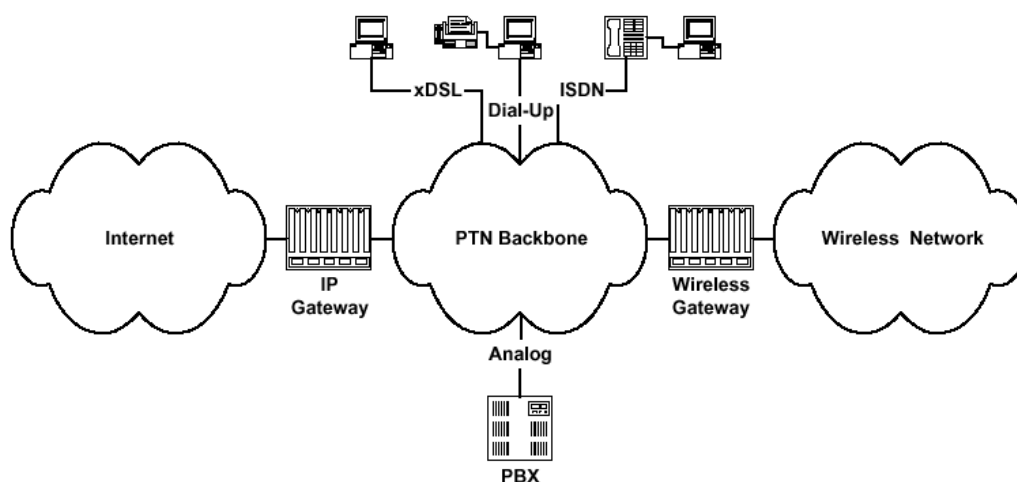
Of the few potential threats from the Public Telephone Network, analog and pre-SS7 phone networks cause the least impact, while the threats from SS7 networks are capable of causing the greatest potential damage.

Public Telephone Networks are massive heterogeneous networks consisting of a PTN backbone, the Internet, and wireless networks. Phone networks were designed for a closed telecommunications community. The telecommunications community was an exclusive group of carriers, usually nationalized or monopolized, in which everyone knew everyone else. Authentication was weak to non-existent. Since deregulation, phone companies are required to provide SS7 connections to anybody willing to pay a modest fee. This introduces potential risks from poorly secured SS7 networks and well-armed phone hackers on a limited budget. ISDN devices are an additional source of unauthorized entry into a phone network.

The older legacy networks carry signaling and transmissions, in-band, over the same copper wires. This solution is not very efficient and does not support the advanced services available from SS7. Neither does the solution allow a hacker to tunnel through a signaling packet traversing through the phone network, because there are no signaling packets. A legacy PBX can be attacked by modem or over the Internet, if one or the other is actually connected to the PBX. The only legitimate reason to connect a PBX to a modem is to receive support from a vendor. The modem should be disconnected as soon as the support session is finished. The only reason to connect a PBX to the Internet is to provide outgoing and/or incoming VoIP services over the Internet. The PBX should be protected and monitored just like any other server connected to the Internet; that is, with a firewall and an IDS probe. A legacy PBX can also be

attacked by someone with physical access. Improving authentication, even if only by strengthening password policy for PBX administrators, will ensure that only those with legitimate business can access the PBX. Once a phone hacker gains entry to a legacy PBX, the potential for damage is usually local (it cannot traverse the PSTN) and limited to telephony (it cannot harm servers or workstations lacking phone functionality). The type of damage may involve phone charge fraud (spoofing), call tracing, or phone tapping.

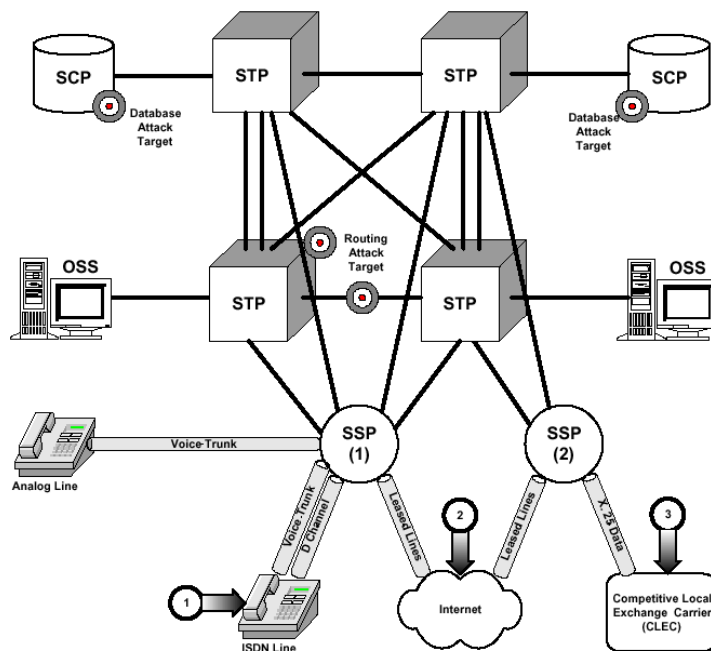
Figure 1: Public Telephone Network Schematic



SS7 networks use out-of-band signaling, separating voice transmission from the data used to manage the calls. SS7 sets up and tears down calls, collects billing information, and returns busy signals. It supports basic communications, call routing, and database access across PTNs. SS7 provides advanced services, such as Local Number Portability, Toll-free, and Toll services. It offers enhanced features, such as call forwarding, caller ID, and conference calls. SS7 is more efficient and more secure than in-band signaling systems, but not secure enough, in light of the increased assets it exposes to hackers. Although SS7 reduces in-band attacks, such as fraud, it introduces other vulnerabilities. A majority of the SS7 vulnerabilities arise from the number and complexity of the interfaces between SS7 entities. Moreover, some advanced services like call forwarding are inherently vulnerable to attack on SCPs containing forwarding destinations. Anyone capable of generating SS7 messages and delivering them to the network can disrupt PTN services. Figure 2 includes some points of vulnerability within the SS7 system.

Still, if damage were limited only to phone services, an information security manager of an enterprise might be willing to live with the threat. The problem with SS7 is that a new potential vulnerability has been uncovered that could spill over into the enterprise data networks; that is, general-purpose servers and workstations without phone services, on a LAN connected to an SS7 gateway, could be attacked via SS7. The vulnerability was actually discovered in SNMP. SNMP uses ASN.1 syntax and parsers for MIBs. Buffer over-runs in poorly implemented ASN.1 parsers could grant unauthorized root/administrator/supervisor access and arbitrary command execution. Maliciously constructed ASN.1 syntax could cause a remote buffer over-run. The problem with SS7 is that it uses ASN.1 as the syntax for many of its messages, including IAM and ISUP messages. A phone hacker could construct a malicious IAM message, destined for a specific target, which would install a Trojan horse in that target. If the target sits on the interface of an enterprise LAN, it may be capable of attacking non-phone targets, as part of a multi-stage attack.

Figure 2: SS7 Network Schematic

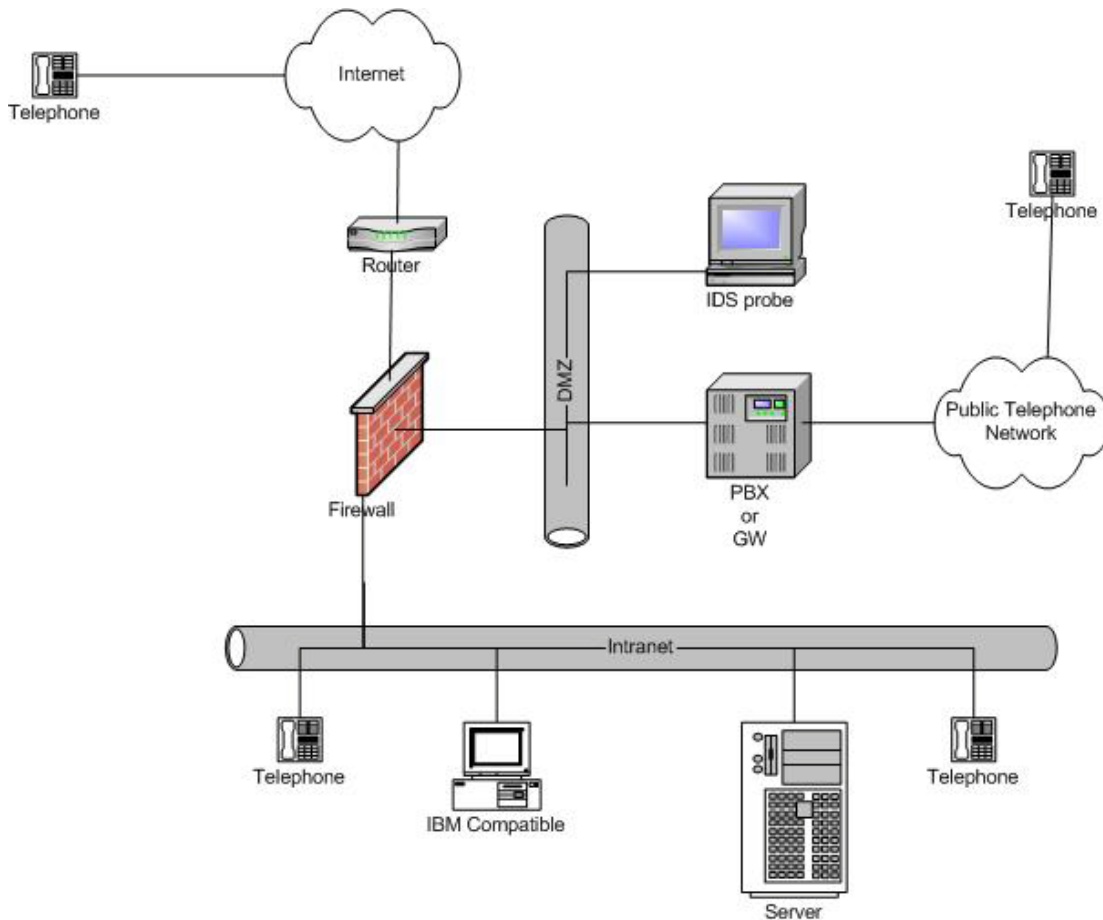


1.3 Mitigation of Risks to the Internal LAN from the PSTN

Coral’s VoIP gateway mitigates most of the theoretical vulnerabilities mentioned in the previous section. In the first place, the Coral VoIP gateway does not interface with SS7. It does not respond to IAM or ISUP messages, or any other ASN.1 syntax messages. The Coral VoIP gateway and call agent perform fine-grain screening of all signaling requests and responses passing through their control.

Only Coral phones and FXO and FXS gateways can obtain services from a Coral call agent. Currently Coral end-point authentication is based on layer-2 MAC address. Phone fraud is thereby minimized. If an intruder tries to send data via the digital trunk directly to the built-in Media Gateway (the Coral UGW module), whose job is to encapsulate the data and pass it to the LAN, the Media Gateway will only respond to a command from the call agent before establishing a voice session (CRCX). The Media Gateway also sends out RTP packets only to registered phone terminals. Coral VoIP servers are based on special-purposed proprietary embedded software, which prevents any intruder from using the Coral maintenance modem or ISDN connection to gain access to the local LAN via the PBX. The only packets the Coral PBX can send to the LAN are MGCP and keyset commands to registered entities.

Additional measures should be taken to minimize risk to the enterprise LAN by the VoIP servers (and vice-versa) by putting a firewall and IDS probe on the network between the LAN and the VoIP servers. This makes good sense whether the VoIP servers are Coral or from another manufacturer.

Figure 3: Secure Enterprise VoIP Topology

1.4 Conclusions

The business value proposition of VoIP is probably too good to ignore: it cuts costs and increases market opportunities. VoIP also introduces new risks, due to security vulnerabilities in the VoIP systems and in the IT systems. Security managers may mitigate vulnerabilities and reduce risks by treating VoIP servers like any other server capable of being damaged or causing damage.

In addition, Coral VoIP gateways are currently unaffected by the critical vulnerabilities discovered in the public phone networks of late.

2 Risks from IP Networks

2.1 Introduction

This paper discusses the risks to an enterprise's internal LAN from the Internet when Voice-over-IP (VoIP) services are offered over the Internet. The paper analyzes the means by which these risks may be exploited and goes on to discuss how to mitigate these risks.

This second part of white paper deals with VoIP security risk management (the first part discussed risks to an enterprise's internal LAN from the Public Telephone Network, as a result of installing a VoIP gateway between these two networks).

This VoIP security white paper is written for IT personnel, in general, and specifically for information security managers.

2.2 Risks to the Internal LAN from the Internet

As with all computerized systems, security risks come from system vulnerabilities and opportunities to exploit those vulnerabilities. It is a truism that all useful software contains flaws. Some of those flaws come from the software design; some come from the source code, some from the default configuration, and some from the distribution. Some of the flaws affect the usability or the operability of the product. Other flaws affect the manageability or the security of the product. In this paper, we are concerned only with security issues.

Hackers and vendors are always playing leap-frog with each other. A vendor creates the flaw, hackers (ethical or otherwise) discover the flaw, and the vendor fixes the flaw and introduces a new one. It is not likely that all vulnerabilities found in a software release will be fixed up by proper configuration, administration, or patches, and certainly not as soon as the vulnerabilities are discovered. The vendor's product documentation may not adequately explain how to secure the system. The vendor may not explain or disclose the impact of introducing his product on an organization's security posture. Often the default configuration is not adequately secured. Sometimes the vendor records too much "security data", so that the only evidence that a system has been infiltrated is buried under a mountain of detail in a log, so huge that nobody reads it.

Users introduce vulnerabilities by trying to bypass password, encryption, or firewall controls to simplify their workload or to obtain better performance. Users may reveal their passwords or keys to others in order to help them out of a temporary problem or they may leave the password or key where anyone can see it.

If a hacker cannot achieve his objectives in one shot, he may resort to a multi-staged attack, in which he diagnoses a system for vulnerabilities, exploits one or more vulnerabilities, and reiterates these steps until he achieves his ultimate objective. After exploiting the initial vulnerability, the attacker may find himself in a better position to diagnose vulnerabilities that were previously hidden and then gain access.

A VoIP system suffers security concerns similar to those experienced by other devices connected to the Internet. SIP or MGCP servers, VoIP Gateways, and MCU servers stand out as inviting targets for malicious individuals and groups.

The main problem with VoIP, from a security point of view, is that it breaks the conventional security model that only permits Internet connections to be initiated from within the organization. One would assume that no rational security manager would permit someone from the Internet to initiate a connection directly into an organization's internal network. If you want to receive in-coming calls from the Internet to the VoIP phones

connected to your internal network, then your security manager will have to permit someone from the Internet to initiate a connection directly into your organization's internal network.

General-purpose computers with VoIP software are more vulnerable than single-purpose dedicated IP phones with embedded VoIP firmware due to the undesirable synergies involved in operating systems providing multiple well-known services. For example, a PC with IP-phone software may inadvertently download a virus or Trojan horse which attacks a VoIP server, a network of IP-phones, or an SS7 network. A Call Manager may also run web, FTP, and/or email services and its VoIP services may be attacked via the other services. Networks that mix voice and data are more vulnerable to undesirable synergies than networks that isolate voice from data.

VoIP systems are particularly vulnerable to the following kinds of attacks:

- Denial-of-Service attacks on VoIP servers may render a group of VoIP terminals useless. VoIP applications are more sensitive to DoS attacks due to the fact that delays or jitters of a few hundred milliseconds can render a voice session virtually useless.
- It may be possible to compromise a VoIP system containing billing information, credit card or calling card numbers, current locations, physical mailing addresses, or traditional PSTN phone numbers.
- An open relay VoIP server could forward calls either anonymously or under the name of the compromised organization.
- VoIP data exchange today typically transpires over unencrypted messages. This means that anyone with a network sniffer can eavesdrop on a VoIP conversation.

2.3 Mitigation of Risks to the Internal LAN

Countermeasures should be undertaken to protect the most critical and the most vulnerable components. All it takes to defend systems from attack is to fix known vulnerabilities or to prevent the discovery or exploitation of the residual vulnerabilities left over from the previous round of fixes.

Solving VoIP security vulnerabilities involves several steps to improve the integrity of VoIP servers. This is accomplished by hardening both the operating system and the services running on the server and protecting the server behind a firewall. To harden the operating system of a VoIP server, apply all the patches and fixes to your operating system (MS-Windows 2000, Solaris, Linux, etc.). Then follow the best practices for securing, for example, MS-Windows 2000 (Cox's "[Hardening Windows 2000](#)") or Linux (Seifried's "[Linux Administrator's Security Guide](#)"). If MS-IIS is installed for web-based management, then apply all the patches and fixes and follow the best practices for securing MS-IIS (Zvi's "IIS: The Paranoid Zone"). There are similar best practices for Apache, iPlanet, and Web Sphere.

Firewalls can provide a significant deterrent to server compromise. Modern firewalls also provide limited protection against DoS attacks. Unfortunately, placing a VoIP server behind a firewall is not a trivial task. The rules of the firewall must be modified to permit traffic to the VoIP server. The firewall should support stateful inspection for SIP and/or MGCP, RTP and possibly RTCP, as well as other VoIP protocols. If SIP terminals also exist behind the firewall and are permitted to call users outside the firewall, RTP must be allowed through the firewall. As may be seen, the number of connections (sockets) that a firewall must pass to enable VoIP is significant. This poses a challenge to many existing firewalls to add support for these connection types. Further complicating the problem is the need for stateful inspection of these packets. Since many of these connections use dynamic port assignments,

the only mechanism for tracking each connection as a part of a permitted call involves extracting information about related connections from existing connection headers and data payloads.

VoIP servers should be placed in a firewall DMZ segment, to prevent the possibility of a single attack vector from the Internet into an organization's internal networks. Firewalls may perform additional functions besides stateful inspection and security policy enforcement of VoIP as well as other IP network traffic. Firewalls often provide Network Address Translation (NAT), Virtual Private Networking (VPN), proxies for web, FTP, and SMTP, bandwidth management, user authentication, and malicious content inspection. Many large organizations distribute these additional functions to separate dedicated servers to achieve better over-all performance and to avoid single points of failure.

NAT is used for the following purposes:

- To conserve public IPv4 addresses
- To provide a level of indirection between the internal servers and external clients
- To hide the internal network topology

Firewall and NAT traversal presents grave challenges for VoIP traffic flows and topologies. The problem is that many NATs translate the IP addresses and ports of devices differently for each destination or each TCP session or UDP flow. Even if the Call Manager sees both the original IP phone address and port in the VoIP packet payload and the NATed device address and port in the VoIP packet header, it cannot predict for certain what the NATed device address and port will be when that IP phone talks to another IP phone. This is only a problem if the signaling traffic follows one flow (IP phone to Call Agent to IP phone) while the media traffic follows another flow (IP phone to IP phone). The solution to the problem is to have the Call Agent server, which handles the signaling, also include a Media Proxy or Relay so that signaling and media flow through the same point, thereby making the NATing consistent between IP phones and Call Agents. The signaling/media relay solution may add hops and delays to the media stream, which may require compensation.

VPNs not only enhance security by authenticating connection partners and encrypting connection traffic, they also solve the VoIP traversal problem mentioned above. VPNs create a tunnel for VoIP packets to pass through NATs and firewalls transparently and unscathed. There is also a special kind of IP tunnel, called a GRE (Generic Routing Encapsulation) tunnel, which only provides the tunnel, without end-point authentication or encryption. VPNs are easy to configure between sites. A single VPN may be set up to handle all traffic between any two sites. VPNs eliminate the need to NAT packets traversing the Internet between two private address realms; however, an ISP may force all traffic to flow through a NAT, whether or not it is tunneled. If that is the case, then the VPN will have to be converted from IP to UDP in order to pass it through the NAT. This is due to the fact that NATs utilize TCP and UDP header port numbers to keep track of address mapping, but the IP headers of a VPN tunnel have no ports. VPN clients also may be installed in remote PC's needing a secure tunnel through the Internet into a corporate site. Such VPN clients may be public domain or proprietary, as in the case of CheckPoint SecuRemote and SecureClient. It might be advisable to limit usage of dedicated IP phones to intra-site or inter-site topologies, where VPNs are unnecessary or provided by other means, while general-purpose, software-based IP phones should take advantage of 3rd party VPN products.

Firewalls are limited in scope as to their inspection and enforcement of network traffic passing through them. All firewalls examine the network, transport, and session layers of all IP packets. Some firewalls provide proxies to examine the presentation or application layers

of IP packets, like HTTP/S, FTP, and SMTP. That is, they monitor and control the methods, commands, and requests of those services. However, HTTP/S may carry active content from even higher-level applications, like Java, ActiveX, XML, SOAP, UDDI, WSDL, XSLT, URL, and SQL. This meta-application active content is treated by firewalls transparently as uninteresting data from the packet payload and is usually not examined.

Meta-application active content may be inspected and enforced by specialized application-layer firewalls, such as Sanctum AppShield or Kavado InterDo. AppShield protects against all the HTTP vulnerabilities mentioned above with the exception of SQL injection. InterDo protects against the above-mentioned HTTP vulnerabilities, SQL injection, and more.

Whereas firewalls provide an active defense against attacks, network-based Intrusion Detection Systems provide a passive defense. An NIDS can examine VoIP traffic promiscuously, compare it against known attack patterns or assumptions regarding proper network behavior, and dynamically block suspicious traffic. The problem with NIDSs is that they need a probe on every switch segment they monitor and their performance is usually inadequate to capture and analyze all the traffic passing over a LAN. NIDS probes can be rather expensive (especially when you multiply them by the number of switch segments in an organization), so they should be placed on a strategic segment through which most VoIP traffic traverses, as long as they can keep up with all the traffic. If an NIDS probe does not keep up with the traffic, place them downstream (closer to the individual server(s) they must defend) or cluster a group of NIDS with an NIDS load balancer.

Firewalls and NIDSs generate a lot of log detail. The log data should be time-stamped and include source and destination IP addresses and ports. Raw log data should be summarized, sorted, graphed, and color-coded; otherwise, the little bits of interesting data will be buried under a mass of uninteresting data.

Non-repudiation can be achieved through the exchange of publicly recognized 3rd party digital certificates and the use of digital signatures attached to each message. Non-repudiation is a feature of PKI that prevents message senders from denying that they sent a particular message to a particular destination. It creates accountability.

VoIP server maintenance should be performed over HTTPS/SSL, SSH, or an IPsec VPN, in order to guarantee that only an authorized administrator performs the maintenance and that non-authorized users may not view the maintenance data from inside or outside the organization.

VoIP system administrators should be authenticated strongly. Regular VoIP users may be authenticated strongly, weakly, or not at all, according to the organization's VoIP usage policy. Strong authentication implies two-factor authentication and/or usage of PKI signatures. There are three factors involved in user authentication (not including PKI):

- Reusable secret user password (what you know)
- Non-reusable user password generator (what you have)
- Biometric sensor (what you are)

Two-factor authentication implies the use of any two of the above methods to authenticate a user. Examples of non-reusable password generators include S/KEY (public domain), SecureID/ACE, DigiCard/VacMan, and CryptoCard. Examples of biometric sensors include retinal scans, iris scans, hand prints, finger prints, and voice prints.

Strong authentication should be implemented over a RADIUS platform. The VoIP server should implement a RADIUS client, so that login requests are referred to a central RADIUS server for authentication. If the VoIP service (Gate Keeper, Call Agent, etc.) does not implement a RADIUS client, then a RADIUS client may be installed for the login service of the server OS (unix or windows).

The three factors of authentication are relevant only to authenticating users interactively. PKI signatures also authenticate users interactively, but they may also be used to authenticate servers, devices, software code, or documents.

All VoIP gateways should deny MGCP or SIP connection attempts from the Data Network. There is no way to enforce a centralized dial-plan if any PC can use VoIP GWs in an ad-hoc manner for calling.

2.4 Improving the integrity of VOIP clients

SIP Phone software PC's and FlexSet-IP Phone software PC's based on MS-Windows 9x or ME cannot be secured adequately. The operating systems are single-user with no protection against unauthorized multiple serial use. The FAT filesystem has no user access authorization. The minimum Microsoft workstation capable of being secured is MS-Windows 2000 or XP. Both W2K and XP have the ability to isolate user environments from each other. Both support NTFS, a file system with user, group, and global read, write, and execute authorization. Both provide standardized TCP/IP protocol stacks with access control lists to block undesired network behavior.

Virtual Local Area Networks (VLANs) provide a certain degree of security for the MAC layer. Most modern LAN switches provide VLANs to isolate work groups and broadcast domains from each other. The only problem with depending on VLANs for MAC-layer security is that when some LAN switches fail, their VLANs break down and all traffic floods through all ports. Physical segmentation is more secure. If possible, implement the following seven VLANs or physical network segmentation for VoIP controls:

- Central Call Control and Related Components Segment
- Peripheral VoIP Elements Segment
- Voice Associated Work Stations Segment
- Administrator Data Segment
- General Intranet Data Segment
- Bastion Segment
- Internet Segment

2.4.1 Central Call Control and Related Components Segment

This segment contains the call agent/manager and the database. This network provides the signaling control for the VoIP systems and their associated processes. This network segment is crucial to VoIP service.

2.4.2 Peripheral VoIP Elements Segment

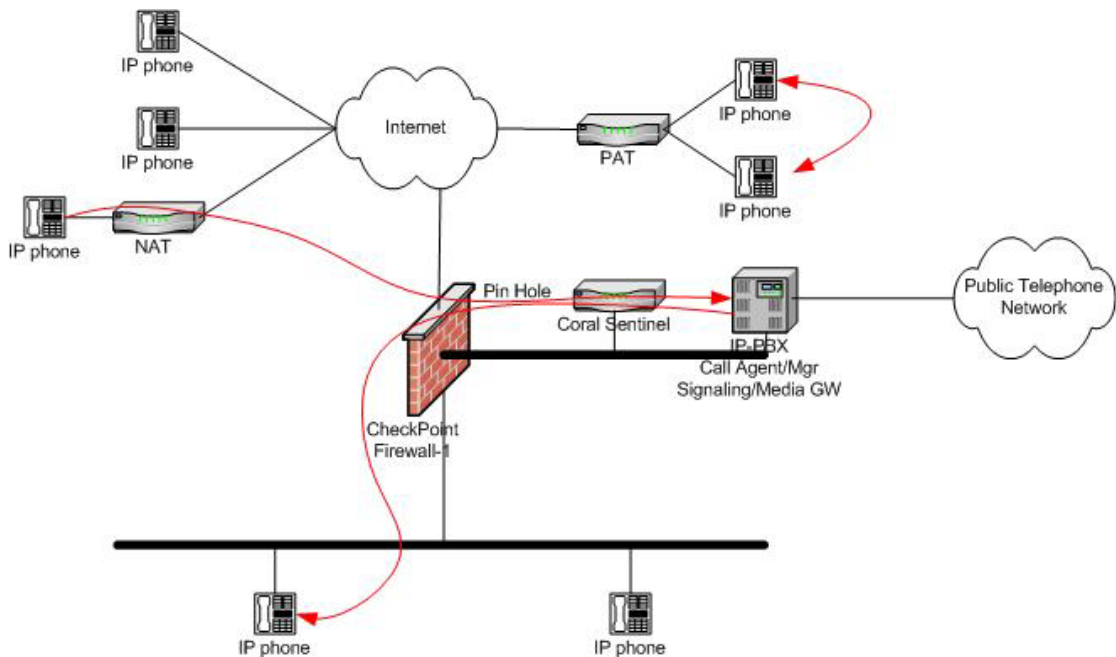
This segment contains those endpoints that receive VoIP media traffic. It includes VoIP Gateways, phones, and voice mail boxes. It excludes VoIP devices that reside on both the Voice and Data networks; that is, this grouping does not include general-purpose PC-based VoIP terminals.

3 Tadiran Coral Solution

3.1 Nat Traversal

In the case of Tadiran's Coral IP-PBX the underlying architecture is based on a special purpose real-time operating system. The current release of Tadiran Coral IP-PBX supports either static or dynamic NAT traversal for IP phones and gateways by means of signal/media proxy ("Coral Sentinel Pro"). All IP phones and gateways that are located behind a NAT server go through the Coral Sentinel Pro for NAT services, as depicted in the following diagram:

Figure 5: Coral Sentinel Pro Signal/Media Proxy Relay



The lower set of red arrows illustrate an IP phone somewhere on the Internet carrying on a conversation with an internal IP phone through a pinhole in the firewall via the Sentinel Pro with a NAT device in the way. The upper red arrow shows two IP phones behind the same PAT device conversing without the aid of a Sentinel Pro.

3.2 Stateful Inspection

The Coral Sentinel Pro provides stateful protocol inspection ensuring, for example, that create-session signaling occurs before RTP media traffic. In addition, the Coral Sentinel Pro complements and support third party firewall stateful inspection of MGCP protocols, such as that of CheckPoint Firewall-1 NG FP2 and above. Sentinel Pro supports SIP and MGCP.

3.3 Authentication

Coral IP-PBX and Sentinel Pro support user and MAC authentication. MAC refers to the network media address of Coral IP phones and gateways. Users may set a password (pass number) that is saved in the Call Agent server. The password is used to lock or unlock the phone's telephony functions.

3.4 Encryption

Coral IP-PBX keysets can encrypt RTP media traffic using DES or 3DES from end to end. Coral swaps encryption keys for each voice session.

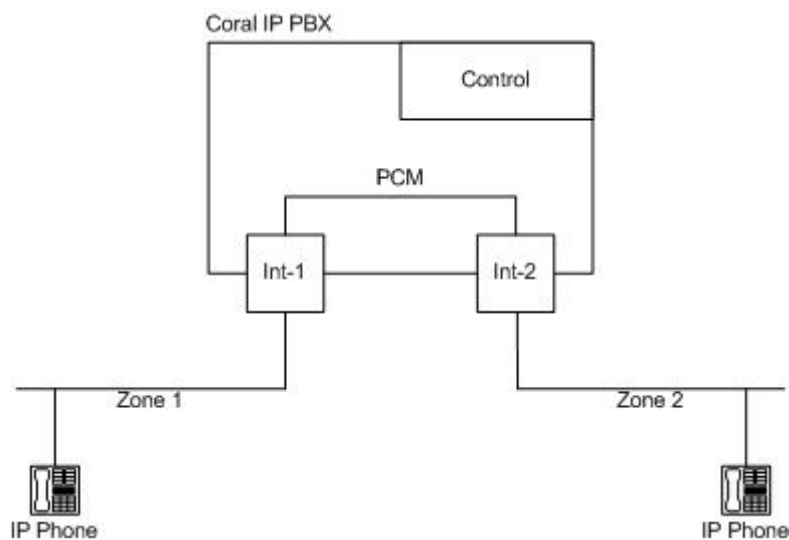
3.5 DoS Protection

The Coral Sentinel Pro also protects the IP PBX server from VoIP-specific Denial-of-Service attacks, such as attacks against codecs or signal floods (rapid on-hook/off-hook flapping). Other Coral DoS protection features include call limiting and load balancing. The Coral Sentinel Pro also prevents attacks from the IP-PBX to the LAN by allowing only VoIP signaling and RTP media through it.

3.6 Zone Isolation

Tadiran Coral IP-PBX can keep voice traffic separate from data traffic via zone isolation. Zones not only segment phone networks in terms of media characteristics, they may also be used to separate different phone networks in terms of security characteristics (data from voice and voice from voice). The Coral IP-PBX interconnects zones over a PCM bus only after the control element strips the headers from the VoIP packet and passes only the voice part. See the following diagram:

Figure 6: Coral Zone Isolation



The Coral IP-PBX currently connects up to 8 different segments.

4 Appendix

The following table describes the recommended authentication requirements for connectivity between segments:

Table 1: Recommended VoIP Connectivity

/To From/	CCC	Voice peripherals	Voice w/s's	Admin	Data	Bastion	Internet
CCC	Simple authentication; Basic access controls	Strong authentication; General authorization; encryption	Strong authentication; Detailed authorization; Detailed Log; Encryption	Very strong authentication; Detailed authorization; General Log; Encryption	Basic access control; HTTPS, SSL, or TLS	Basic access control; IPsec	No direct contact; firewall or proxy ok.
Voice peripherals	Strong authentication; General authorization; encryption	Strong authentication; General authorization; encryption (media only)	Strong authentication; General authorization; General log; encryption (media only)	Very strong authentication; Detailed authorization; General Log; Encryption	None	None	No direct contact; firewall or proxy ok; encryption (media only)
Voice w/s's	Strong authentication; Detailed authorization; Detailed Log; Encryption	Strong authentication; General authorization; encryption (media only)	Encryption (media only) but it depends on operational requirements	Very strong authentication; Detailed authorization; General Log; Encryption	Basic access control; HTTPS, SSL, or TLS	None (as far as VoIP is concerned) but it depends on operational requirements	No direct contact; firewall or proxy ok; encryption (media only)
Admin	Very strong authentication; Detailed authorization; General Log; Encryption	Very strong authentication; Detailed authorization; General Log; Encryption	Very strong authentication; Detailed authorization; General Log; Encryption	Very strong authentication; Detailed authorization; General Log; Encryption	Very strong authentication; Detailed authorization; General Log; Encryption	Very strong authentication; Detailed authorization; General Log; Encryption	Very strong authentication; Detailed authorization; General Log; Encryption
Data	Basic access control; HTTPS, SSL, or TLS	None	Basic access control; HTTPS, SSL, or TLS	Very strong authentication; Detailed authorization; General Log; Encryption	depends on operational requirements	depends on operational requirements	No direct contact; firewall or proxy ok.
Bastion	Basic access control; IPsec.	None	depends on operational requirements	Very strong authentication; Detailed authorization; General Log; Encryption	depends on operational requirements	depends on operational requirements	No direct contact; firewall or proxy ok.
Internet	No direct contact; firewall or proxy ok; IPsec.	No direct contact; firewall or proxy ok; encryption (media only)	depends on operational requirements	Very strong authentication; Detailed authorization; General Log; Encryption	depends on operational requirements	depends on operational requirements	Not specified