Secure IP Communications Design Guide

Design Guide edition 6b

Central Presales

Alcatel·Lucent
Enterprise

Table of Contents

Table of Figures

Preface

Traditional telephony solutions have been constructed with monolithic products, barely accessible by the outside world, using principally proprietary protocols. The security aspects of such applications are therefore primarily based on the problems of controlling access to the application (taxation, telephony discrimination, type of service for telephony users…)

Telephony over IP (ToIP), as opposed to traditional telephony, use converged support and standard protocols that allow greater integration within the business world. ToIP solutions must provide more advanced security mechanisms than traditional systems and be able to integrate simply into the security policy of the business. Unified communications, with strong convergence between Voice and Data worlds, but also facilities of mobility and multi-devices, bring new challenges in terms of security as we must re-think control on IP flows inside the corporate network and openness to external clients.

In order to address the security question, this document is divided into three main sections:

- **A Global Security View** aims to explain the issues and challenges a customer must deal with when a converged solution is implemented. It describes what security means in a business environment, how security must be anticipated and how telephony system implementation within customers' infrastructure can be integrated into the security policy of the business.

  This section is primarily aimed at IT directors, project managers or consultants.

- **OmniPCX Enterprise and Unified Communications applications Security** describes the mechanisms, tools and protocols employed in our products allowing the construction of a secure global solution.

  This section includes products description and is aimed at presales voice engineers and network/telecommunications architects.

- **Recommendations & Best Practices** focuses on implementation. Covering different scenarios and indicating Alcatel-Lucent recommendations, it explains how to implement a secure IP telephony and Unified Coms solution.

  This section has been created specifically from a technical and architectural engineering point of view. It is a targeted at designers working in architecture or network systems and security technicians.

A Global Security View

1 Today's Security Landscape

1.1 Introduction

For many years the world has been blindly un-secure. Each day we can read newspaper reports about new threats to computer security. These threats result from operating system (OS) vulnerabilities or holes in application security due to the difficulty of keeping up with the number of software patches that are constantly being released. As time has progressed, new types of threats have surfaced, making each area of the computer vulnerable to a wide range of exploits. The following list highlights some of the top vulnerability categories:

- **Operating System vulnerabilities** -- OS vulnerabilities, although not the most common, tend to gain the most media coverage. OS vulnerabilities are one of the security aspects targeted by patch management.
- **Application vulnerabilities** -- In addition to the OS being vulnerable to exploits, the applications that run on the OS can also require patching. Some prominent applications for which patches are regularly released include Microsoft Office, Microsoft SQL Server, and Microsoft Exchange Server as well as third-party Independent Software Vendor (ISV) software products.
- **Viruses** -- A virus is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document. Viruses can be transmitted as attachments to an e-mail message or in a downloaded file, or be present on a USB key or CD-ROM. Antivirus software application vendors perform a double-duty by providing, through their updating mechanisms, fixes to exploits that ultimately should be dealt with through patch management.
- **Worms** -- A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an OS that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks. Worms most commonly take advantage of known software flaws or weaknesses.
- **Spam** -- Spam is unsolicited email. From the sender's point-of-view, spam is a form of bulk mail, often to a list obtained from a spambot or by companies that specialize in creating email distribution lists. To the receiver, it usually seems like junk e-mail. It's roughly equivalent to unsolicited telephone marketing calls except that the user pays for part of the message because everyone shares the cost of maintaining the Internet. Spam can also carry viruses that, upon viewing, infect a system.
- **Spyware** -- Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, Spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.

Exploits are growing not only in number but also in complexity. For example, the Sasser worm exploited Microsoft Windows vulnerability, and it required no user interaction to do damage. In other words, the user did not have to click an email attachment or run a virus-infected program. This type of attack is extremely dangerous because little can be done by a system user to stem its aggressive replication and self-distribution.

Granted, there are many factors outside of the control of companies that contribute to the spreading of worms and viruses (home users for example.) If companies had had an effective patch management solution in place, Sasser would not have been so successful in replicating itself across their networks. The patch to plug the exploit Sasser utilized was available several weeks prior to the worm's release. In the same respect, it is alarming how the patch-to-exploit time is decreasing. By the time a patch is made available by a software vendor; virus writers are already developing and releasing their terrorist code.

Even with the patch-to-exploit time decreasing substantially, many virus and worm writers still attempt to develop viruses based on old exploits. These viruses and worms target those uninformed or uneducated end users that have not taken steps to become familiar with system vulnerabilities or common security practices. Even in this day and age, where computers are everywhere and in use every minute of the day, there are still those computer users that have failed to receive the message that computer security responsibility resides with them first.

1.2 Different threats for different impacts

CERT (Computer Emergency Response Team) is a team for emergency reaction in information technology. This team is in charge of competitive intelligence security, launching alerts to administrators and to research how to handle the faults created by the attacks.

CERT defines five main categories of incidents:

1) Information collection

This type of attack is essentially the scanning of the different services activated on a network or on a server. This phase can be called the recognition period. Two very precise objectives are researched in this category of attack:

- Identify the existence of a target and understand the network topology and towards where communications launched from this environment are going.
- Identify vulnerabilities that could be exploited on the target in question or its environment.

2) Access attempts

In general this type of attack consists of accessing servers without any authorization with the aim of using its services or to extract data.

Examples:

- Attempts to extract password files
- Attempts to obtain licenses
- Connection to the services available on the servers (ftp, telnet, Web. Etc.)

3) Denial of service

Denial of service attacks can be carried out in different ways, but their objective is to make sure that servers, networks or applications no longer respond to user demands.

The majority of denials of service attacks are anonymous, as they do not require a re-sending of information on the part of servers towards the attacker. This is what is called a Distributed Denial of Services attack (DDoS). In a distributed attack, the attacking computer hosts are often zombie computers with broadband connections to the Internet that have been compromised by viruses or Trojan horse programs. This allows the perpetrator to remotely control the machine and direct the attack, often through a botnet. With enough slave hosts, the services of even the largest and most well connected websites can be denied.

4) Worms and viruses

A virus is a vicious attack and auto reproductive, which attaches itself to an application, program or other executable and does not necessarily leave a trace of its presence.

A worm is an independent program that spreads from computer to computer or from server to server across a network connection often resulting in the weighing down of networks as it passes through.

5) Suspect activities

This category includes incidents and traffic that is not associated with any of the current activities on a network, server or application.

Depending on the kind of incident the enterprise is facing, consequences are different and considering business context in which the enterprise has activities, the same incident will have a different level of potential impact. This must be taken into account when defining a security policy for the enterprise.

1.3 Protection of the Enterprise resources

In the face of ever-present business-critical applications, escalating threats, rising standards compliance pressures, increasingly complex solutions, and purchasing sophistication and savvy that continues to demand solution maturity of information security investments; the security solution landscape is rapidly evolving.

A recent investigation reveals that since 2000, Internet attacks have generated costs of more than 1 600 billion dollars over time in different North American companies. In total, these companies will have wasted 3.3% of their time between unemployment due to defects caused by the attacks and the damage repairs.

Faced with such statistics, the majority of decision-makers and IT managers consider IT security as being the new major priority for their company. However, budgets dedicated to this are actually minimal and managers are not ready to invest. Only those companies having already suffered attacks increase their security budgets. These budgets concern as much the hardware and software as guidelines and human resources.

2 The Focus of Alcatel-Lucent on Security

“Security is a process and not a product”.
(Bruce Schneier, described by The Economist as a "security guru”)

Today, a company’s information system is required to be secure, whether it is at the level of its infrastructure, its servers or even its applications. Security is not a tangible product or feature that can be bought, but rather a process in which the method for the organization protection practices of information systems against non-authorized access.

Security has become a must in the architectures of global solutions. There is an endless balance to strike between the value of the data which needs protection and the cost of this protection. This obviously means that the “sensitive” data to protect has been previously evaluated and considered as valuable.

The same balance also needs to be defined in relation to final users, because too much security can brake technology success and too much complexity can discourage customer and client contact.

2.1 Defense In-Depth

Securing the core of the Information system and consequently security of the solution and the network implies handling the security and also the awareness of potential vulnerabilities at each level. Based on this approach, Alcatel-Lucent integrates Security as a whole and at different model.

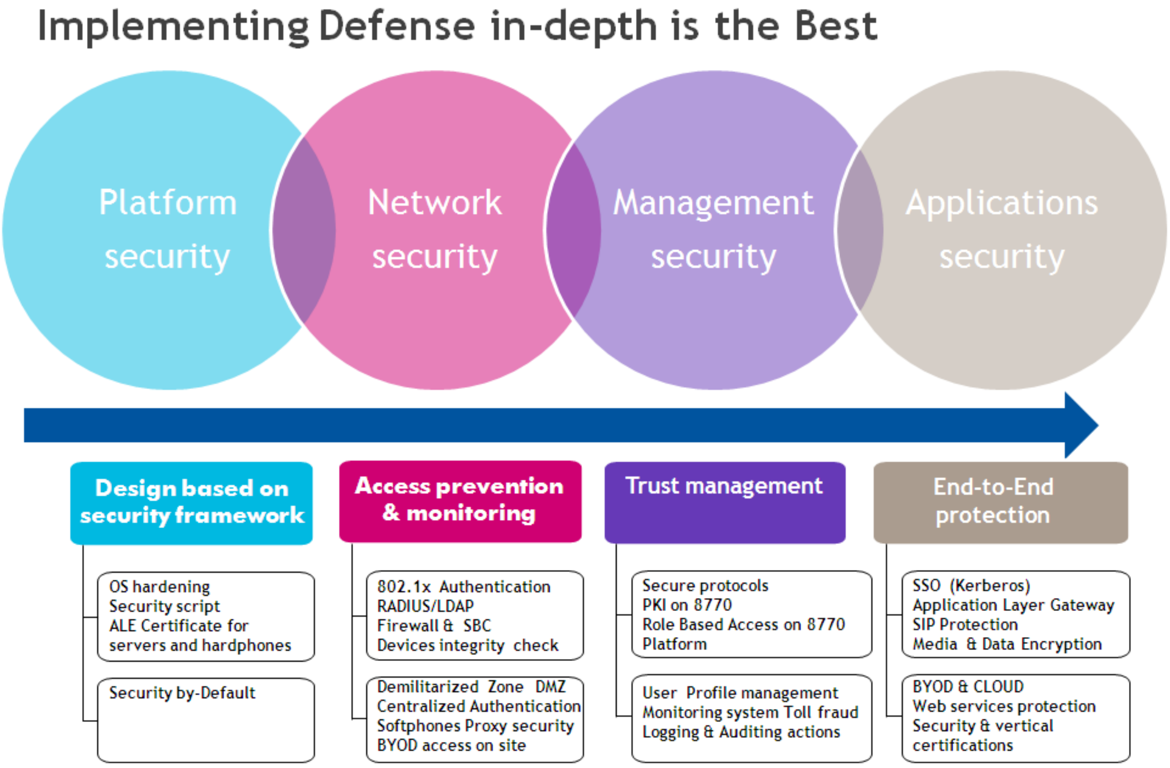


Figure 1: Defense In-Depth

Defense in depth is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical for the duration of the system's life cycle.

Security is not just a function that is implemented at a given level. Taking into account Security efficiently means at all the different levels in order to address multiple types of potential vulnerabilities. Security must be global and has to adapt to environment constraints.

This security approach also takes place in the OpenTouch Security Policy where the guiding principles are to provide customers with communication solutions that are secure. The vendor’s factory floor must stay secure during all processing steps and milestones. Within product development rules set the following have been defined: Security in Design, Security by Default, and Security in Deployment.

3 OXE conformance regarding Security Standards

Alcatel-Lucent is working to offer comprehensive solutions that maintain compliance with regulatory requirements including:

- SOX (Sarbanes-Oxley)
- GLBA (Gramm-Leach Bliley Act)
- HIPAA (Health Insurance Portability and Accountability Act)
- BALE II
- PCI DSS (Payment Card Industry Data Security Standard)
- ISO 17799 and BS 7799

HIPAA and PCI DSS requires sensitive information (in the context of medical environment or banking/payment environment) to be handled by the system with respect to privacy and confidentiality. The OmniPCX Enterprise solution is able to address this strong requirement by providing encryption of all the communications over the network based on the IP Touch Security feature (see ***c***

ISO/IEC 17799 is an information security standard published in June 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This standard was renumbered ISO/IEC 27002:2005 in July 2007.

ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad:

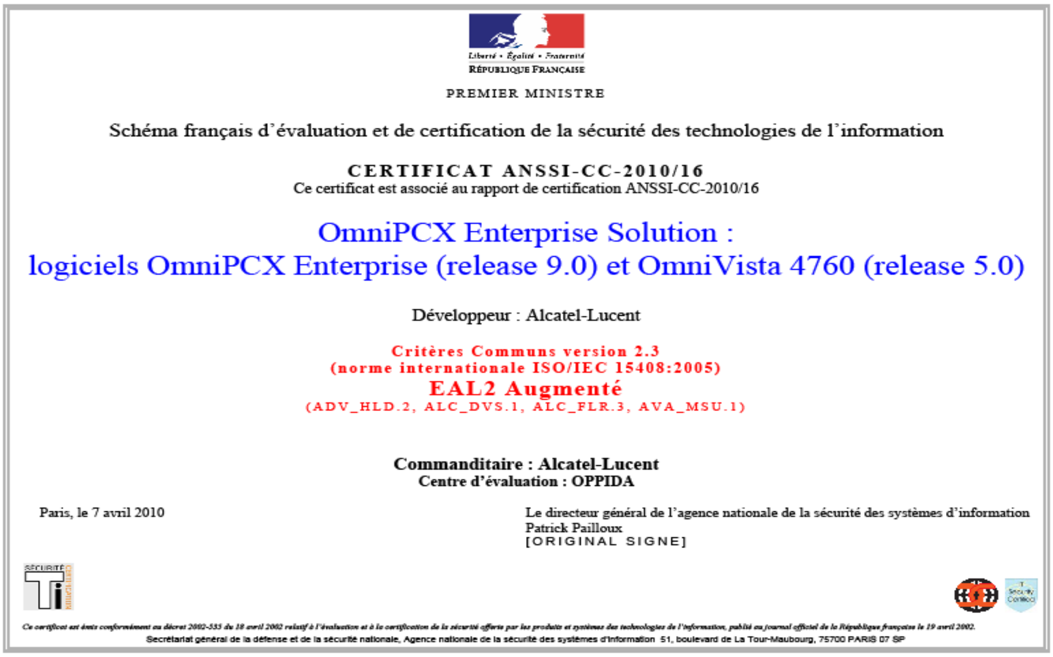
1) **Confidentiality**
In ISO 27002 standard context, confidentiality on information resources is based on a strict control of access to those resources. So we need to consider all the features and mechanisms integrated into the solution to guarantee a strong authentication and also authorization levels depending on user profile.
The OmniPCX Enterprise solution addresses those different issues at the administration and system levels (see chapter **11.2** ***"Secure Telephony Services"***).

2) **Integrity**
Safeguard the accuracy and completeness of information and processing methods. The OmniPCX Enterprise solution integrates different features to ensure integrity of both system and database files (see chapter **12.9** ***"System Integrity Check"***).

3) **Availability**
Architecture of OXE solution allows for a high level of availability for services and resources. It is based on different mechanisms at server level (redundancy) and telephony services level (public to private overflow). For more details see chapter **8.1.15** ***"High Availability"***.

Common Criteria (ISO 15408) provides assurance that the process of specifying, developing, and evaluating a computer security product has been conducted in a rigorous manner. The **Evaluation Assurance Level (EAL)** is the numerical rating assigned to a product to reflect the assurance requirements fulfilled during the CC evaluation. Common Criteria lists seven levels, with EAL1 being the most basic and EAL7 is being the most stringent. Levels from EAL1 to EAL4 are for products in a civil context. Levels from EAL5 to EAL7 are reserved for military context.

*Alcatel-Lucent has certified his IP Telephony solution for Common Criteria level EAL2+. The target perimeter includes **OmniPCX Enterprise R9** and **OmniVista 4760 R5** products. Objective of this certification is to demonstrate adequacy between common security threats against a communication solution (IP PBX and its management platform) and mechanisms and features used to design, validate, deliver and install our products. This certification process has been conducted under the authority of the French government agency ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), that is in charge of validation for our products and certification delivery in France.*



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT ANSSI-CC-2010/16
Ce certificat est associé au rapport de certification ANSSI-CC-2010/16

OmniPCX Enterprise Solution :
logiciels OmniPCX Enterprise (release 9.0) et OmniVista 4760 (release 5.0)

Développeur : Alcatel-Lucent

Critères Communs version 2.3
(norme internationale ISO/IEC 15408:2005)
EAL2 Augmenté
(ADV_HLD.2, ALC_DVS.1, ALC_FLR.3, AVA_MSU.1)

Commanditaire : Alcatel-Lucent
Centre d'évaluation : OPPIDA

Paris, le 7 avril 2010

Le directeur général de l'agence nationale de la sécurité des systèmes d'information
Patrick Pailloux
[ORIGINAL SIGNE]

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information, publié au journal officiel de la République française le 19 avril 2002.
Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Why is the Alcatel-Lucent offer adapted to a company's security ?

Alcatel-Lucent's construction vision in terms of security strategy is similar to that of a user company; it is designed in the following way:

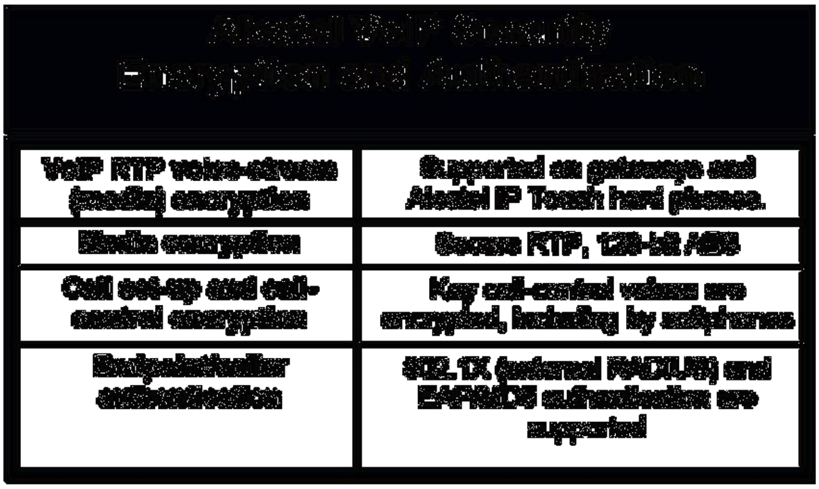
- Strengthening of the infrastructure supporting our customer's application through the choice of a proven operating system and continual tests for attacks.
- Securing the point of access on an application: for all types of wired or wire-less support with technologies such as 802.1X, the use of Vlans with different attribution modes or the study on the use of certificates.
- Detection of a diversion of applications: who are the users and where are they?
- Isolation of equipment and final users in order to protect them from malevolent traffic with intrusion prevention technologies against attacks such as DoS or DDoS.
- Confidentiality of information flowing on its architecture by means of encryption algorithms in real time.
- Assurance that critical applications such as voice, benefit from a service quality which allows them to be available even in the case of network delays.

Alcatel-Lucent's voice solution should be considered as a simple application which will adapt itself to the secure environment defined in the company.

Recognized secured communication solutions

In addition to internal product quality assurance process, where Alcatel-Lucent has designed specific security test campaign for all products, and security audit (performed by Bell Labs dedicated teams of security experts), Alcatel-Lucent participates on a regular basis to external lab tests such as Miercom to compare to competitors.

In that context the OmniPCX Enterprise solution has been recognized for many years now as a highly secured communication platform for enterprises (rated "*Best Secured IP PBX solution*" by the independent Miercom Labs).



Alcatel VoIP Security
Encryption and Authentication

VoIP RTP voice-stream (media) encryption	Supported on gateways and Alcatel IP Touch hard phones.
Media encryption	Secure RTP, 128-bit AES
Call set-up and call-control encryption	Key call-control values are encrypted, including by softphones
Endpoint/caller authentication	802.1X (external RADIUS) and EAP-MD5 authentication are supported

Rated Highest Score in Security Miercom HE IP PBX

Miercom RATED BEST

4 Alcatel-Lucent Security Strategy

4.1 Security as a process

“Security is a process and not a product”.

(Bruce Schneier, described by The Economist as a "security guru”)

All business requirements for security technology should be focused on delivering appropriate and not excessive security.

On these assumptions, internal Alcatel-Lucent security processes and frameworks have been defined both at the corporate level and at the Business Unit level.

Our Quality Assurance and Customer Care Central organization hosts the corporate-wide Alcatel-Lucent Product Security Incident Response Team (**ALPSIRT**).

This team is in charge of centrally receiving and storing vulnerability reports, and internally distributes them to the relevant product groups contact persons (Product Security Primes). The Alcatel-Lucent product groups are then requested to investigate the impact on their products and create detailed mitigation information and actions.

Within Quality Assurance and Customer Care, the ALPSIRT is manned by persons belonging to Security and Reliability Group. The ALPSIRT is the main gateway between ALU and the general public:

- The external inputs are centralized by the ALPSIRT: from CERT-US, CERT-IST and other mailing lists, user input (email: psirt.security@alcatel-lucent.com).
- The communication to security organisms like the various CERTs and to the general public is centralized by the ALPSIRT.

For more details on the process implemented by Alcatel-Lucent to manage vulnerabilities you can refer to the application note “**Description of the security flaw remediation process**” (available in Alcatel-Lucent enterprise Business Portal website).

5 IP Telephony and Security

5.1 General principles and topologies

The OmniSolutions family is composed of a number of building blocks which are used to create the most suitable communication solution for an enterprise. These components are:

- IP Communications software suite, comprising telephony communication servers (including the OmniPCX IP Communication Server) and value-added applications like the OmniTouch Contact Center and Instant Communications Suite (ICS), as well as applications from Application Partners.
- Hardware servers that run the IP Communication software suites.
- Media gateways, which are the basic building blocks for connecting legacy terminals and networks.
- Fixed phones (IP phones, Softphones, traditional analog phones, digital phones) and mobile phones (cellular, Digital Enhanced Cordless Telephony (DECT) / Private Wireless Telephony (PWT), Voice over WLAN (VoWLAN)).

In a large enterprise network, standard IP Telephony solution deployment can be divided into:

- **Headquarter**: ToIP servers are deployed in the HQ. Presence of Media Gateway equipments depends on public network interconnectivity choice (through PSTN or IP public trunking). It can be a backup site with redundant Communication Server/MGW and Application servers. IP Telephony servers can be deployed in a Data Center of the company or hosted by a sub-contractor.
- **Regional Office**: A remote location connected to headquarters through IP-VPN or an IPSec VPN where another OXE node (Communication Server and Media Gateways) is found.
- **Branch Office:** A remote location connected to headquarters through IP-VPN or an IPSec VPN where a media gateway is present along with IP phones (hard and soft, NOE and SIP).
- **Remote Office:** A remote location connected to headquarters through IP-VPN or an IPSec VPN with only IP phones (no media gateway).
- **Home Office:** User working at home and connected to the enterprise with IPSec VPN client (on the PC and on the dual-mode wifi mobile phone).

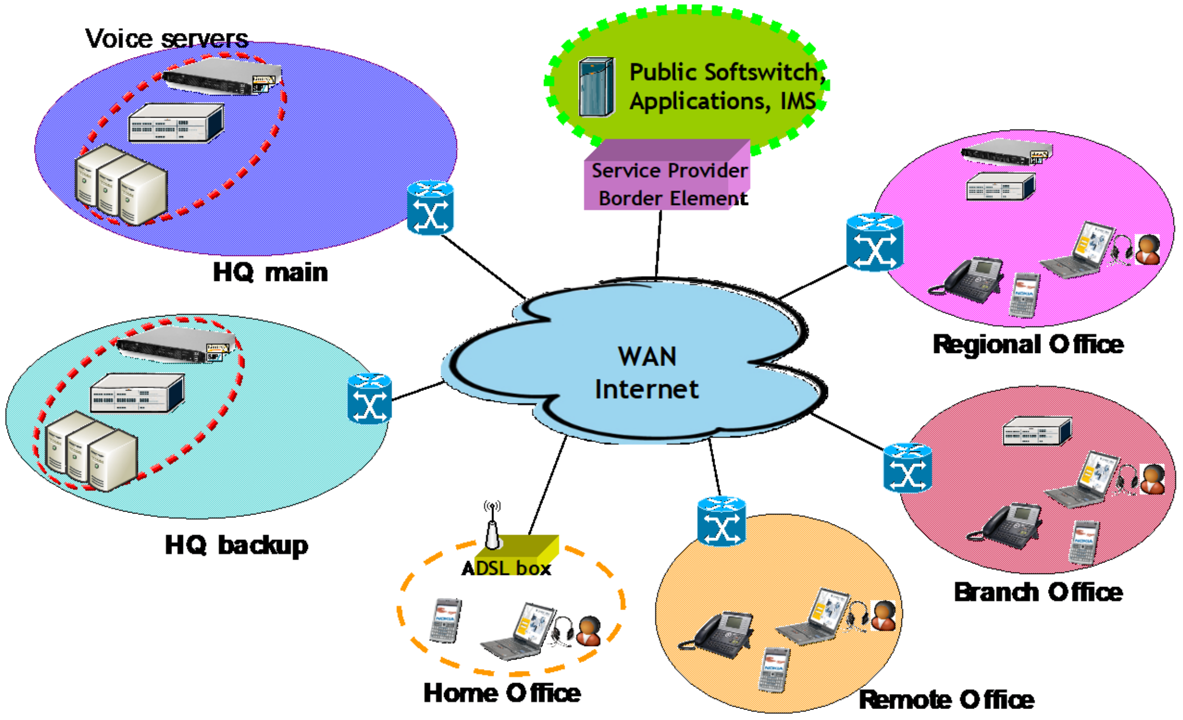


Figure 2: Standard IP Telephony deployment in large enterprise

All ToIP components are interconnected through the customer IP network. On each site the LAN is used for switching all the company's traffics: voice and data. This enables an enterprise to select the most suitable vendor for each function in order to build the best possible solution that matches its needs.

At the heart of Alcatel-Lucent's enterprise strategy is the objective of deploying enterprise IP telephony solutions over any data network (LAN switches, routers, etc), whether provided by Alcatel-Lucent or a third party. This approach ensures that customers are not locked into a single data vendor, which might be against their long-term interest.

What are the best practices to secure a VoIP deployment?

This document is published as a guideline tool to assist in securing the data network design supporting VoIP deployment. Some security mechanisms have been implemented in the Alcatel-Lucent voice components and Alcatel-Lucent IP Communication Software Suite to offer solutions regarding:

- Authentication (e.g. pin code used by callers).
- Access control (e.g. trusted host mechanism).
- Hardening of the call processing or VoIP components as voice mail, Media Gateway (e.g. Alcatel-Lucent provides the minimum programs of a Linux distribution for the OmniPCX *Enterprise* needs).
- Secured management : All sessions are user/password protected with encryption of management based on protocols such as SSH, SSL/TLS, SNMPv3.
- High Availability (e.g. Communication Server duplication, Backup Signaling Link between the Communication Server and remote IP Media Gateways).

Public/Private network applications

The IP network is protected from the "public" IP network (e.g. the Internet) through different layers of security (Firewalling, Access Control lists, Authentication, etc…).

An IP-PBX solution has no direct connection to the Internet, therefore benefits from the different layers of security around the internal LAN.

Nevertheless, an IP Telephony solution can have a direct connection to the public network through:

- TDM interfaces , supported on IP media gateways,
- IP interfaces , referred as Public IP Trunks (using H323 or SIP protocols),
- Remote maintenance devices through modems connected on the PSTN public network.

Main concern is to understand if these accesses allow intrusion onto/into the IP data network thus bypassing the different layers of security on the data network.

Interactive Communication

Compared to a classic PBX architecture, an IP Telephony solution involves many more factors, including the voice products (PBX boards and IP terminals), the data network equipment, and the applications using it. Each one of them can have an impact on the Quality of Service (QoS) or Voice Quality in the final solution.

The transport of voice on IP network imposes particular characteristics on the performance level of the data network, particularly as a result of the real time nature of voice transport. The design of the VoIP solution and the data infrastructure has to respect the following characteristics (for a MOS score of 3 that is an acceptable audio quality):

- Transmission delay (round trip delay less than 400 ms),
- Variation of transmission delay (jitter less than 50 ms),
- Packet loss ratio (less than 3%).

Standards and Protocols

A VoIP solution is a sum of standard and proprietary protocols. Two common standards can be used to provide a VoIP solution: ITU-T H323 protocol and IETF's Session Initiation Protocol (SIP). Each standard uses distinct methods and protocols for call signaling and call control.

VoIP introduces many factors, such as Gateways, IP-Phones, many IP addresses, protocols (e.g. H323 stack), etc. Also, the matrix of flows is complex, as there are different flows for voice and signaling/ direct voice between IP phones, as opposed to "data applications" (where the flows are generally client-server).

To design a secure solution, a logical and/or physical network partitioning is mandatory and in order to do this, it is necessary to control/know the IP flows matrix.

5.2 Threats against VoIP

With VoIP, voice and telephony signaling flows operate on a converged (voice, data and video) network. Thus, VoIP information is susceptible to the same threats and therefore inherits all the vulnerabilities associated with data networks. Therefore, the voice network has to be secured as any other service on the IP customer network.

This section identifies some of the main threats against IP communication solutions. We try here to perform a risk analysis even if it is a difficult exercise as this kind of solution involves so many different services and technologies. For each threat, we mention potential counter measure that could be used at both detection and prevention level.

Chapter 8 **-** ***Overlay Security Approach* -** of this document describes associated product features to those counter measures and **chapter 12** **-** ***Alcatel-Lucent Recommendations* -** details our design recommendations.

➢ Theft of Services / Phreaking

“Phreaking” is a slang term coined to describe the activity of a subculture of people who study, experiment with, or explore telecommunication systems, like equipment and systems connected to public telephone networks. The term "phreak" is derived from the words "phone" and "freak". It is associated with traditional telephony system hacking activities. First objective of hackers was toll fraud exploit as it allows them to communicate for free everywhere in the world while it was the attacked company that was actually charged for those calls !

Context of the threat is that of a malicious person wanting to access services offered by the solution without corresponding rights. It could be a well known user trying to escalade privilege or an external person abusing authentication mechanisms of the solution.

The most common form in the current PSTN is called subscriber fraud, where a subscriber sets up an account with a service provider using false billing information, for example a stolen credit card. Other forms of theft are more technical, often utilizing black boxes or similar to fool the network into providing free service.

Even in a VoIP access network using for example DSL, bandwidth is still a limited resource especially the low packet loss and jitter required for good voice quality. Therefore, the network needs to be protected from subscribers misusing this high-priority bandwidth, one example would be if two SIP User Agents could set up a direct call between them, accessing the high priority bandwidth but bypassing the SIP Server(s) and hence not get billed.

Here after are the capabilities of OmniPCX Enterprise solution to counter this kind of threat:

- ■ Prevention
    - AAA framework used for user authentication and authorization (usage of standard protocol like RADIUS for a centralized authentication of users).
    - User authentication (login/password associated to every users).
    - User authorization (access rights definition based on pre-defined profiles or user category definition).
- ■ Detection
    - Detection of brute force attack on authentication control mechanism (user accounts are put under quarantine if authentication attempts number reaches a pre-defined threshold).
    - User accounting for all actions performed (service access). For each communication an accounting ticket is issued and stored on a centralized database for future audit.

➢ Eavesdropping

Due to shared physical network, sniffing or eavesdropping, it is very easy to catch the IP packets and can result in disclosure of confidential information or communication. It also allows malicious users to collect information about the customer systems, servers or applications that can be used to mount an attack on other systems or data that might not otherwise be vulnerable.

- Prevention
  - Secure physical access to network elements.
  - Logically separate elements of the solution by using VLANs (at a minimum separate voice and data traffics). Usage of VLANs is also a plus when talking about quality of service assurance.
  - To ensure that no unknown device could be able to connect to the network, use the 802.1x protocol at infrastructure level.
  - Encryption of all sensitive flows carrying service or user data (signaling and voice media).
  - Encryption of all management information.

- Detection
  - For dynamic data flows (voice, video etc…) that could be intercepted “on the fly”, detection is not easy. Only traffic observation or filtering elements in the network itself could be able to reveal abnormal activity.

➢ Denial of Service (DoS) / Distributed Denial of Service (DDoS)

One of the more prevalent methods currently employed by network attackers is the Denial of Service (DoS) attack. A DoS attack is one that seeks to disrupt normal network operation and thus affect normal business activity. Unlike the fabled “hacker” attacks of old, which normally had a goal of acquiring forbidden information, DoS attacks normally seek only to make a network unusable for a period of time. DoS attacks can be loosely grouped into three general categories.

- **Bandwidth Consumption:** Attacks of this type normally seek to generate excessive quantities of network traffic, though some seek to reduce the capacity of network infrastructure to the same effect. The result of such attacks, often called “storms,” is a complete inability to use the IP network for any form of communication.

- **Resource Consumption:** Attacks of this type target specific network services with the goal of making the attacked service unavailable for legitimate use and/or affecting other associated services.

- **Destruction:** “When all else fails, destroy” is the general motto of destruction attack creators. Attacks of this type seek simply to destroy data and thus eliminate its availability to the enterprise user.

DoS attacks target weaknesses in infrastructure, anti-virus and application controls. Since Voice over IP solutions depend on the IP network at a transport mechanism, DoS prevention is more important than ever before. Two different types of attacks are possible:

- By sending some specific IP packet(s) with erroneous data or bad sequences of data.
- Or by bringing the network or host (e.g. servers, desktops, …) to its knees by flooding it with useless traffic. The capacity for a host to accept an IP flooding depends mainly on its processor power.

Each type of attack can be designed to inhibit or reduce the service at different levels:

- Physical layer level.
- Operating system level. Many attacks, exploiting limitations in the TCP/IP protocols / stacks, are designed to simply try to disable this TCP/IP interface.
- Application layer level (e.g. SIP, H323, HTTP, …).

DDoS is a combination of DoS attacks staged or carried out in concert from various hosts to penalize the target host/network from further serving its function. The 'Distributed' aspect is a reference to the fact that the source of the DoS attack is actually multiple network clients (often called zombies) and not a single point. Because of this, DDoS cannot be eliminated by merely filtering a source IP as it is often launched from multiple points installed with varied agents.

- **Prevention**
  - System hardening: remove unused services, reduce listening ports number.
  - Best practices programming (code review). Usage of standard at maximum (operating systems, protocols).
  - Secure emergency calls but applying higher priority.
  - Load balancing to reduce massive DDOS impact.
  - Process management (monitor and restart killed processes if needed).
  - Infrastructure recommendations (filtering elements to block or reduce impact of packet storm).
  -
- **Detection**
  - System monitoring to detect anomaly.

6 OmniPCX Enterprise and Instant Communication Suite product releases

Here after is the list of products composing ALU IP Telephony and Unified Communication solution that are covered in this document, with release number allowing readers to refer to corresponding presales presentations or technical documentations to get additional information on security features:

- **OmniPCX Enterprise release 11.0**
- **OmniTouch Instant Communications Suite release 6.7.x**
- **OmniVista 4760 release 5.2.x / OmniVista 8770 release 1.3**

7 Security Perimeter Approach

This section aims to describe many of the security mechanisms and technologies implemented within the Alcatel-Lucent Enterprise portfolio related to IP Telephony.

The implementation practices described here explain how Alcatel-Lucent products can and should be integrated into the enterprise security schemes for highly robust PCX designs.

Trying to simultaneously address all security aspects of any given PCX design is simply not practical or feasible. Alcatel-Lucent approaches system security with a “divide and conquer” technique.

It is imperative that areas of security concern are segmented into general disciplines and then further dissected into specific focuses. This allows for a “perimeter approach” that is easier to implement, manage, audit and maintain over time.

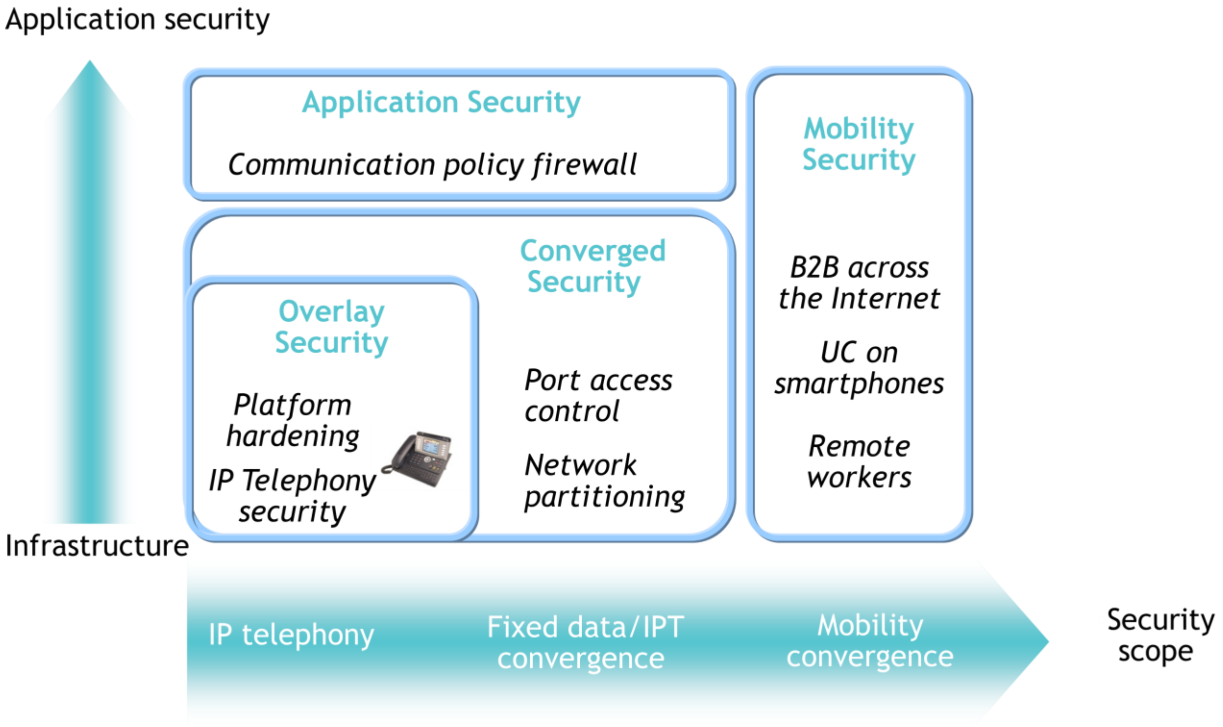


Figure 3: Security Perimeter Approach

8 Overlay Security Approach

8.1 OXE Communication Server

The Operating System used by the OmniPCX Enterprise Communication Server is based on Linux (kernel 2.4.17).

Historically, the open nature of the Linux source code has allowed the Linux community to audit operating system development and solve potential security problems before they become real problems on customer systems. Alcatel-Lucent has invested time and effort to further harden the Linux operating system environment for OmniPCX Enterprise use.

8.1.1 Linux OS Advantages

The advantages that make Linux one of the most stable and secure operating systems available as a free operating system include:

- A source code which is completely open for the kernel and utilities - there is no 'security by obscurity'.
- A large and active developer base that ensures constant auditing of the source code for potential security problems.
- The massive worldwide user base for Linux ensures that each aspect of Linux security is tested within a vast range of different computing environments on all sorts of hardware.
- The on-going development of Linux ensures that it stays on the cutting edge of many Unix security developments.

8.1.2 Customized Linux for OXE

As part of Alcatel-Lucent's hardening of the Linux operating system, all non-essential software has been removed from Alcatel-Lucent's customized version of the OS. The advantages include reducing:

- the provided distribution size (Alcatel-Lucent package = 50 MB versus public version = 700 MB)
- the potential security risks imposed by the excess

Although Alcatel-Lucent has eliminated over 85% of the standard Linux core distribution, several optional features do remain within Alcatel-Lucent's distribution. Only services that are vital for operation are enabled by default. For example telnet remains within Alcatel-Lucent's distribution of Linux, but is disabled by default because it is unsecured and is replaced by SSH. There are no Graphic User Interface (GUI) environments such as X11, KDE or Gnome.

There are no resource tools for remote file and print sharing available to Alcatel-Lucent's distribution. Features such as LPR, NFS and Samba (Microsoft compatible) are not present in any format.

8.1.3 Denial-of-Service Defenses

The Communication Server is hardened to resist attacks by broadcast flooding. An internal defense mechanism allows for a minimum reservation of processor power to the primary function of the Communication Server: Call Handling

For each release, test campaigns are systematically carried out to address all categories of attack. Alcatel-Lucent Enterprise Solutions Division has implemented the set of security tools recommended by the Corporate Alcatel-Lucent Network Security Group to audit, test and harden the products, and track the potential issues:

- Regarding the “erroneous data” attacks, tools (generating Teardrop, Teardrop Timeout, Land, Ping of Death) and Nessus suite are used which address the most famous DoS attacks. Part of the test campaign is also based on tools (built by companies like Codenomicom) for verifying the implementation and the resilience of protocols such as H323, SIP, …
- Regarding the storm packets or flooding attacks, various tools generating TCP flood - SYN, ACK, FIN, URG, RST, PSH - Ping flood, Echo Reply flood, Bad TTL flood, and broadcast storm are used.

All the results are analyzed by the R&D department. For instance, any abnormal result reported by the Nessus vulnerability scanner is corrected in the maintenance releases of the OmniPCX Enterprise.

Independent consultants (Miercom, Hervé Schauer Consulting, …) have already tested our solutions, including the security aspects. For example, using similar tools they confirmed Alcatel-Lucent’s results with regards to DoS attacks.

8.1.4 Access Controls (passwords, filters, etc)

Our ToIP application is installed on a customized Linux system. The number of generic system accounts is reduced to the minimum and some specific system accounts used to access functions of our application are automatically created during installation phase.

Here is a summary of available system accounts after installation (since OmniPCX Enterprise R5.1):

Name	function	Origin	Creation	Login	FTP
root	superadmin account	linux	by default	YES (console only)	NO
bin	owner of several binaries	linux	by default	NO	NO
daemon	owner of /var/spool/at	linux	by default	NO	NO
ftp	anonymous FTP access	linux	by default	NO	YES
httpd	HTTP owner	linux	by default	NO	NO
nobody	owner of TFTP daemon	linux	by default	NO	NO
ppp	setup IP link on V24	linux	by default	NO	YES
swinst	software installation and configuration	Alcatel-Lucent	by default	YES (console only)	YES
mtcl	maintenance and configuration	Alcatel-Lucent	by default	YES	YES
adfexc	file transfer with 4760	Alcatel-Lucent	by default	NO	YES
client	limited maintenance access	Alcatel-Lucent	optional	YES	YES

The “client” account, not present by default can be optionally created. Shell access is restricted to some accounts. It is the same for FTP function access.

Only system accounts present in this table are available and no new account may be created.

As a result, the use of shared system Ids for logging to the Communication Server is mandatory.

Note: Certain accounts that were available in the previous release(R3.0 to R5.0), but are unnecessary for system operations, have been suppressed in order to restrict unauthorized access by a backdoor. The list of accounts includes "mtch, adm, halt, sync, shutdown and install."

Security by default design:

During the initial installation of the product, security is activated and password management for the system (accounts access) is forced into operation by default. The passwords for the users (root, mctl, swinst, and adfexc) must be changed by the customer.

Expiring passwords:

The expiration of passwords is activated; the "time to live" of the password is configurable with a maximum of 999 days before access to the account is blocked by the system. Five days before the expiration date, a warning "the password will expire in x days" is displayed at each login.

Password policy:

Minimum length	New password must be composed with a minimum of 8 digits (lower or capital letter, number, punctuation)
Comparison between new password and old ones	New password must be different from the last 3 passwords At least half of the digits must be different from the last used password
Maximum useful life	From 11 to 999 days
Warning before expiration time	5 days (for each login)
Maximum number of failed authentication attempts	3

Note: It is not possible to use the "root" access directly by Telnet; access is only available directly via the console port, and the user must be physically on site.

Disabling account:

A quarantine mechanism can be configured by the administrator which allows to block access to a system account during a short period (15 seconds) when the maximum number of failed authentication attempts (3 by default) is reached. This mechanism is a protection against brute force attacks.

Note: during login connection, if there is no user action for 300 seconds, the login session is stopped.

8.1.5 Shadow Passwords

On a Linux system without the Shadow Suite installed, user information including passwords is stored in clear in the well known /etc/passwd file. With the Shadow Suite, the MD5 algorithm is used to hash all passwords and then they are stored in a specific file /etc/shadow with restricted access right. Although not impossible, it is very difficult to take a randomly encoded password and recover the original one.

8.1.6 Trusted Hosts Management and TCP Wrapper

The OmniPCX Enterprise solution, as any other VoIP system, uses many different IP based protocols, most of them being standard protocols that can be managed by firewall equipments in an agnostic approach. ALU can provide the list of protocols and port numbers used by each component of the OmniPCX Enterprise solution allowing a customer to configure his security infrastructure (eg. firewalls) accordingly.
In addition to the security infrastructure of the customer, different security mechanisms are available in the OmniPCX Enterprise solution providing a second level of protection, by providing access control and filtering rules for the network services available in the Communication Server. Those internal mechanisms (available by default at the system level of the Communication Server) are:

- **Trusted Host Management**
- **TCP Wrapper**

Trusted Hosts Management feature isolates the OmniPCX Enterprise network interface from the LAN. No dialogue (incoming or outgoing) is allowed between any IP equipment on the network and the Communication Server's Ethernet access except for the ones explicitly allowed (the trusted hosts). The trusted hosts list can be composed of the IP phones, the media gateways, the network management stations etc...

Enabled by default, this security feature allows the customer to deny remote access for any unfamiliar IP devices to the Enterprise Communication Server.

TCP Wrapper is a public domain tool that provides filtering services for Linux or Unix systems. When an unprotected Linux computer is connected to a network, the computer's system is exposed to other computer users connected to the network. A hacker can determine which users are logged on to a given server, and may also be able to find out the identities of individual computers. The hacker can then determine when a workstation is likely to be idle, and access and use that workstation while it is unattended. TCP Wrapper acts as an internal firewall to prevent this.

TCP Wrapper operates by intercepting and filtering incoming requests for the network services. For example, if an external host attempts to use the FTP service, TCP Wrapper checks to see if that external entity is authorized to transfer files. If it is authorized, then access is permitted; if not, access is denied.

For each IP device defined in the list of Trusted Hosts list, the administrator needs to specify the profile of the device/host. It is possible to assign a profile that contains a minimum list of services available in the Communication Server.

The available profiles are:

- VoIP resources (IP phone, INTIPA/INTIPB, GA, GD, and LIOE): only TFTP is allowed
- 47XX (management): FTP, Telnet, Netaccess, Saverrest are allowed
- CPU: Shell, FTP, Telnet, TFTP, Rlis, Saverrest, Builddistant, Loaddistant are allowed.
- Router: no services are allowed

8.1.7 Antivirus software and the OmniPCX Enterprise

The OmniPCX Enterprise Communication Server runs on a Linux platform. Today, installation of a third party application such as an antivirus product directly on top of this platform is forbidden by Alcatel-Lucent for several reasons:

1) This Linux platform is especially customized by Alcatel-Lucent to run real-time application and at the same time, hardened to ensure a high level of security by reducing the number of installed packages and services. The Communication Server must be considered as an embedded system, on which only application developed or customized by Alcatel-Lucent can be executed.
2) The Communication Server is not accessed directly by human users and thus cannot be considered as a vector of contamination for viruses even though it uses internally some of the IP flows known to be prone to carry viral loads: FTP, HTTP, SMTP, IMAP.
3) It could have bad side effects on the performances of mission critical, real time software such as OmniPCX Enterprise Communications Server.

At the difference of Windows platform where anti-virus support and update is mandatory, running an antivirus on Linux depends on the role of the application. The following discusses the different ways that worms or viruses use to thrive and how OmniPCX Enterprise is protected.

The penetration vector of a virus is through a user-focused service, and results in the upload of a compromised file containing executable information that eventually gets executed thus propagating the virus throughout the system. This propagation happens either through network probing (in this case the virus is rather called a worm) or through scanning of a user-owned directory of other users like a phonebook.

Natively, Linux provides an environment on which viruses do not thrive as easily, and in the case of OmniPCX Enterprise, a virus has even less possibilities of infecting the Communication Server since there is no user account except a short list of system accounts (used internally or for few of them used for restricted maintenance or configuration operations) that are created during installation phase.

A possible penetration vector of a virus can be through an email and impacts **Mail servers** (SMTP, IMAP flows). OmniPCX Enterprise Communication Server only deals with internal mail (system communication and voice mail transmission from Voice Mail system) and thus cannot act as a contamination actor.

Concerning **Voice Mail systems** like A4645, respectively A4635, it is a mail server that can be connected to other mail servers through VPIM protocol. But A4645, respectively A4635, is not a unified messaging system as it supports voice messages only. There are at the moment no virus identified that are carried on voice media, so the risk of viral attack on A4645 (respectively A4635) is largely mitigated by the fact that these platforms support voice only. Furthermore IMAP4 protocol only allows to retrieve messages from the server and not to put files on the mail server.

Another source for virus propagation is **Web browsing** (HTTP flows). This possibility is not offered on the OmniPCX Enterprise Communication Server that only proposes optionally a limited access to a web service for configuration purpose.

Another source is through **File uploads** (FTP flows) with copy of executable files on the system. This kind of operation will only occur in case of software patches installation. Those patches are produced and distributed directly by Alcatel-Lucent. In that case, a checksum mechanism is used to perform integrity control at system level.

Management stations are not a source of viral attack for the Communication Server as they only permit changes in the configuration (restore) and no upload of non Alcatel-Lucent executables. Nevertheless, Alcatel recommends that PCs used for management are dedicated to that task and should hold the Java client permanently (to avoid time for downloading the applet). On Communication Server side, these machines should also be filtered using Trusted Hosts mechanism.

As a conclusion, at the moment, Alcatel-Lucent has not been received any report of viral attack affecting its OmniPCX Enterprise Communication Server.

Antivirus on Windows platform running Applications

The following statement concerns all the Windows applications (like OmniVista 4760, Contact Center or Business Applications).

Alcatel-Lucent recommends anti-virus solution to be installed on those systems. There is no recommendation for a specific antivirus, and Alcatel-Lucent applications can coexist with any anti-virus that is used by the customer.

In case of problem, Alcatel-Lucent will analyze technically the problem: Alcatel-Lucent is ready to support the customer/the business partner:

- if there is a bug in the Alcatel-Lucent application, Alcatel-Lucent corrects it.
- if there is a problem of use of common resources, Alcatel-Lucent gives explanations on the way to use resources without changing anything.
- if there is a bug on the anti-virus side, the customer or BP should escalate the problem to the anti-virus vendor.

This position allows business partners to validate a global security offer including one or several anti-virus software with the support of Alcatel-Lucent.

OmniVista 4760 specific recommendations for anti-virus

- **Compatibility:**

The OmniVista 4760 applications (server and client) operate correctly in the presence of MacAfee and Norton anti-virus systems.

1) **Other anti-virus programs:**

Any other anti-virus system can be deployed on a PC hosting a 4760 server or client. In the event of an incompatibility being detected, we recommend that you contact the Alcatel-Lucent OmniVista 4760 support department.

1) **Incompatibility or malfunction:**

An anti-virus can slow down the PC and application performance.
Case of slowdown in client launch:

➢ The anti-virus is configured to analyse compressed and/or .jar extension files. In this case, the first launch of the 4760 client is slowed down by 2 to 3 minutes. Under McAfee, the file extension option: *.jar or Scan inside archive is enabled.

➢ Wormstopper function: When the anti-virus integrates the Wormstopper function, the alarm notification e-mails are blocked. Since most new viruses are propagated by electronic mail, WormStopper stops these new viruses distributed by mass mailing by detecting any activity. The WormStopper function:

- Detects transmission of e-mails to more than 40 recipients,
- Detects transmission of more than 5 e-mails in less than 30 seconds,
- Checks the content of repetitive e-mails.

The anti-virus must be reconfigured to allow OmniVista 4760 to send an alarm by mail. OmniVista 4760 waits at least 3s between sending 2 mails, if other alarms occur, this period is increased.

Version 8 of MacAfee integrates this Wormstopper function (Menu: Advance ActiveShield setting). We recommend setting the authorization for sending 5 successive emails to 15s.

8.1.8 Network Time Protocol

The need for synchronized time is critical for today's network environments. As organizations grow and the network services they provide continue to increase, the challenges involved with providing accurate time to their systems and applications also increase.

Every aspect of managing, securing and debugging a network involves determining when events occur. Time is the critical element that allows an event on one network node to be mapped to a corresponding event on another by using a log.

In many cases, these challenges can be overcome by deployment of the NTP Service. The NTP (RFC 1305) is an Internet protocol used to synchronize the clocks of devices to a designated time reference, providing the benefits of a standards based time and the synchronization of logs and traps.

The clocking information is synchronized via UTC (*Universal Time Coordinated*).

NTP service is based on client-server architecture where a server provides clocking information to multiple clients over an IP network. The OmniPCX Enterprise operates as an NTP client in order to get clocking information from one or many NTP servers.

8.1.9 Logging/Accounting

All the management operations performed by an administrator are stored in a dedicated log file. This ensures traceability and accountability to comply with most regulatory requirements (e.g. Sarbanes-Oxley in finance business). Thanks to an external RADIUS authentication, the administrator is identified with its corporate identity that will be carried out into the log file. Provided by the Communication Server, the NTP service (Network Time Protocol) allows an automatic and accurate synchronization of the clock with a central server. Information in the log files can therefore be cross matched between several systems. It is also possible to activate an “on the fly” transmission of the log files to an external secured server (based on standard Syslog mechanism).

Log files are available for several OmniPCX Enterprise’s applications/system operations:

- storage of all management operations performed on the Communication Server (syslog mechanism),
- storage of telephonic database updating,
- storage of communication costs,
- storage of OXE applications "incidents".

8.1.10 Syslog Server

Syslog has become the de facto standard for forwarding log messages within IP networks. The term "syslog" is often used in reference to both the actual syslog protocol, as well as the application or library sending syslog messages.

In concept, syslog is a very simplistic tool used to send small textual messages (usually less than 1024 bytes) to a logging server via UDP and/or TCP. In the most common configurations, syslog messages are sent across a network in an unencrypted "cleartext" form, but options do exist to use SSL/TLS services to transport syslog messages in encrypted form.

Syslog has typically been used for computer system management and security auditing. While it does have shortcomings, its advantage is that syslog is supported by a wide variety of devices. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository.

Alcatel-Lucent recommends using syslog in combination with NTP to aggregate logging information and increases the ease with which auditing events can take place.

As of R6.2, all system logs managed by the syslog daemon (stored under /var/log directory) can be recorded on a remote syslog server. This includes the **/var/log/shell.log** files used to store the history of logins and UNIX commands performed by a user. All system command executed through remote shell by an administrator is logged in the **shell.log** file and flagged with administrator identity (user name used for authentication).

8.1.11 Syslog file for Intrusion Management

With the security-by-default mechanism, the Syslog support is enabled on the Communication Server and registers all network events, as part of the process for preventing security issues.

All events, regarding the kernel, the network interface, the login, etc. seen by the Linux system are distributed by origin and severity in files under the directory /var/log (ex: messages, secure, auth.log, etc.). The Syslog files keep records or logs regarding:

- Connections (who is connected, and at what time),
- Unauthorized attempts to enter the system,
- History of system commands used,
- Kernel and registration of the daemons used on devices.

No user interface exists through swinst or netadmin to access to these files. The only way to read or modify them is via Linux commands like “vi” or “more.” To avoid congestion on the disc, which is caused by these files, an automatic mechanism rotates the log files. They are compressed and renamed by this mechanism. The rotational schedule is weekly and/or when the file exceeds 500 Kb (before compression).

8.1.12 Telephonic database updating

Log files are available when the telephonic data is updated by management tools or by the phone sets. It is a file with the 1000 last operations (up to 2000 with the 500 first ones since the last CPU reset -up to 3000 since the last CPU reset- and 1500 last incidents). Each log is filled in with the date, the time, the "operator" (A47xx, mgr, set, attendant, broadcasting application), operation type (create, set, delete).These log files are created locally to each node. It is possible to import the log of each node into the OmniVista 4760 NMS for consolidation (Audit feature of the OV4760) and backup of those log file on external data storage.

From R3.0, the object model offers the details (attribute by attribute) of the operations carried out by management tool/ machine (mgr, 47xx), not by phone set.

8.1.13 Communication costs

For each communication (external incoming, outgoing calls), an accounting ticket can be stored in compressed hourly files. There are up to 30 days of records.

These accounting tickets can be exploited by management stations:

- Analysis of communications can be achieved by using a filter on accounting fields in a generated report,
- With OmniVista 4760, alarms can be generated when a cost threshold is reached.

8.1.14 OmniPCX Enterprise's "incidents"

For each OmniPCX Enterprise application (call handling, internal accounting, …), "incidents" are generated. Examples of incidents:

- Release update installation,
- Running of call handling,
- Loss of telephonic equipment,
- Process loss.

The OmniPCX Enterprise solution stores up to 2000 local "incidents" and 2000 network "incidents" in distributed call processing solutions.

An "incident" contains the following information: Date, Time, Node number, Source (RMA, Main CPU or Stand by CPU), Object in fault, Incident gravity, Incident number, Comments.

All the "incidents" can be sent in real time to the management tools for analysis and topological animation:

- to 4760 (200 maximum) via CMIP (IP stack using)
- to external stations (10 maximum) via SNMP traps.

Note: Filters are used to select which incidents are sent.

8.1.15 High Availability

Service continuity in any situation is the highest priority for most companies which business relay on capability to reach and to be reached by their customer. In that context the OmniPCX Enterprise solution is ranked 5/9 that means it is able to deliver telephony service with availability assurance of 99,999%. Actually that means the system could be unavailable less than **5 minutes per year** !

8.1.15.1 Redundancy/Backup call routing

Duplication of the Communication Server

Providing a CPU standby function is often required in a telephony environment serving emergency or 24 hr/7 days-a-week services (without interruption).

The Enterprise Communication Server software platform redundancy (duplication) allows switchover from one communication server to its mirrored communication server through an IP link. This provides:

- continuous service in the unlikely event of CPUs failure
- possibility to conduct maintenance operations

In the case of duplication, two communication servers coexist in the same system. One of the Com Servers operates as “main” the other as “standby”. Server databases are duplicated and coherently maintained. In the event of the slightest problem on the main Com Server, the system switches over to the standby Com Server which then becomes the main Com Server:

- Calls already in progress are maintained
- Calls being connected during switch-over are lost
- Calls connected after switch-over are treated

When hosted in Common Hardware or Appliance Server, both Com Servers are active and standby and can be located in a different location (Geographic duplication in different subnets).

Availability of telephone resources with load balancing and mutual aid

Within the same Media Gateway, it is possible to define several specialized boards offering the following telephonic resources:

- voice compression and coding
- frequencies and dial tones detectors / generators
- voice guides
- conference calls with N participants (3 to 29)

Each of the Media Gateway boards can be used independently. This allows them to deal with a possible failure of one of them.

In addition, a mutual aid mechanism makes it possible for the vocal guide resources in a distant Media Gateway to be used when all the local accesses are inaccessible (for whatever reason). Call processing is able to offer a load balancing mechanism between the various boards of a Media Gateway for the voice compression and coding functions. In this way, Therefore, it can handle board failure, Ethernet connection loss or DSP malfunction.

Automatic Routing System (ARS) is a routing mechanism which allows, amongst other things, public or private trunks to be selected when a user dials an external number. If one of the routes is inaccessible, the Communication Server will search for another. This provides a method of handling a possible public or private trunk failure.

Passive Communication Server

The Passive Communication Server (PCS) provides telephony service availability in case of:

- Loss of the two duplicated Communication Servers or loss of the non duplicated CS (e.g. massive outage in the central site)
- Breakdown of the IP links between the remote sites and the central site (hosting the duplicated Communication Server)

Note: This switchover causes all communications in the PCS domain to be broken for a minimum period of time. Initialization is required for the Media gateways and IP phones.

Media Gateway survivability: Backup signaling for IP Media Gateway

If the IP link between the communication server and a common hardware IP media gateway is lost, a backup signaling link is used to re-establish the signaling path over the PSTN. This service is designed to ensure continued telephone service at remote sites.

During the backup connection, users can make and receive calls over the local PSTN network connection, and VoIP calls between the remote and central site can be redirected via the public network.

The communication server then attempts to reach the remote media gateway over the PSTN (via GD internal modems).

Private to public voice overflow

In addition to the backup signaling of the Media Gateway mechanism, an evolution of this function includes making private-public translation decisions, facilitating inter-area calls when the IP network is unavailable (saturated or out of service).

Dialed internal numbers are translated automatically into public numbers so that inter-site communications can be established via the public network.

Both features, “back up signaling” and “private to public voice overflow” make it possible to offer business continuity without adding cost (there is no additional software or database to maintain and update for each site):

1. all the advanced telephone services are available locally to the remote sites (including voice mail)

- a minimum number of telephone services (PSTN) are offered for inter-site communications

8.1.15.2 Power Autonomy

Power supply and battery back-up for Common Hardware

Alcatel-Lucent has designed several solutions for power supply and battery back-up.

- The first family solution is a data oriented environment relying on data UPS back-up solutions for optimized price and short autonomy. This solution is based on 110/230 V rack modules. In addition the rack modules are equipped with a cable to connect external batteries to provide up to 4 hours of autonomy.
- The second family is more dedicated to a telecom oriented environment with its own power back-up solution and for optimized price and long autonomy. This solution is based on 48 V rack modules. The rack charger provides up to 8 hours of autonomy.

Power supply for Crystal Hardware

The VH rack needs to be supplied with a 230 V / 110 V (depending on country) external power supply or 48 VDC external power.

In case of power failure, the internal batteries provide standalone power for a short period. Automatic detection of battery discharging initiates a system shutdown.

A –48 VDC external power supply connection is available for situations where standalone power of more than thirty minutes is required.

8.1.16 SIP protection

There are different mechanisms integrated in the OmniPCX Enterprise to secure the communications with a SIP phone or a SIP server.

8.1.16.1 Quarantine list

As of R5.1, a mechanism can be used to protect the proxy and SIP gateway from DOS (Denial Of Service) type attacks. This mechanism is based on two lists, a list of addresses in quarantine and a list of trusted addresses.

IP addresses in quarantine are the IP addresses of sets whose messages are ignored for the duration of the quarantine period. Sets can be placed in quarantine either:

- Manually: by configuring set IP addresses
- Automatically: the trigger threshold is **25 messages** received by the proxy in **less than 3s**, quarantine lasts for **30 minutes** (this can be configured under SIP parameters of OXE system)

Under the SIP proxy parameters:

```
Framework Period : 3
Framework Nb Message By Period : 25
Framework Quarantine Period : 1800
```

Trusted IP addresses are the addresses of sets that cannot be placed in quarantine, even if the number of messages from these sets exceeds the automatic quarantine threshold.

8.1.16.2 SIP phone authentication

A shared secret (login of the set) is stored between SIP phone and Communication Server. When the SIP phone tries to register the Communication Server sends a challenge based on authentication DIGEST principle. If the SIP phone is not able to answer correctly, the Communication Server rejects its registration and it won't be able to communicate on the network.

8.1.16.3 SIP TLS

As of OXE R10.0, TLS standard protocol is available and can be used for mutual authentication between OXE ComServer and external SIP Gateway (for SIP Trunking). The mechanism is based on digital certificates and requires the installation of a hardware SSM-RM (Server Security Module) in front of the OXE ComServer. TLS and digital certificates are managed at the level of the SSM-RM.

8.2 IP Media Gateways

8.2.1 Resistance to DoS

There is no Operating System to be exploited on interface boards or media gateway controllers, only function specific LINUX micro-kernels.

Flood Limiting: Similar to the protection provided Alcatel-Lucent IP Phones, the TSC-LIOE, LIOE, INTIP, IOIP, GD and GA boards are designed to identify excessive Ethernet broadcast traffic rates, and ignore all broadcast traffic in excess of 300 pps. If an Alcatel-Lucent OmniPCX IPMG interface receives traffic in excess of 300pps, only the first 300 packets will be accepted.

8.2.2 Separation of TDM and IP traffic

No service has been implemented (by Alcatel-Lucent or any third party) in OmniPCX media gateway devices that would allow user access from TDM resources (ISDN, PSTN, analogue trunk, etc.) to IP networking resources within the IP Media Gateway. IP networking functions are completely isolated from voice and signaling transport contamination.

The only services supported through the TDM trunking interfaces to IP are:

- Tunneling of trunk signaling protocols (ISDN, CAS, etc.) to the Communication Server through IP, where it is processed by the call handling application. Call processing of the Communication Server is an automated function that is dedicated to specific signaling packets. All other packets that are not in strict compliance with the Alcatel-Lucent specification are discarded.
- Media (voice) is encapsulated into RTP streams. The destination of RTP streams is under the control of the Communication Server and can only reach RTP capable devices which excludes standard PCs (with the possible exception of IP softphones).
- The e-Remote Maintenance application provides network administrators the ability to access and manipulate IPMG resources remotely. This optional feature can terminate inbound calls to the local console interface, but does not allow for any PPP/SLIP style of remote access.

In addition to the above, it is important to remember the primary functions performed by IPMG:

- IP Media Gateways host Public and Private TDM trunking interfaces (e.g. PRA boards) which are only capable of processing signaling protocols (ISDN, QSIG, etc.) and transferring Voice streams to and from the TDM backplanes of the IPMG.
- IP Media Gateways host VoIP interface/resource boards that are only able to process signaling protocols (H323, H245, H225, RAS, etc.) and transfer Voice streams to and from the LAN.

The Linux micro-kernels of Alcatel-Lucent IP Media Gateway VoIP boards offer a link between the circuit-switched and packet-switched realms. This means that a hard barrier exists between the TDM and IP halves of the IPMG which only voice media and call control signaling can traverse, and only then in the form of payload, not as an interactive element of the communication. There is no IP routing, IP forwarding, or ICMP redirect between the TDM and IP portions of the IPMG.

For security reasons, remote IP console (telnet) sessions to GD boards of IP Media Gateways are only possible from the Communication Server.

8.2.3 Binaries signature check

When a new binary is produced by Alcatel-Lucent for IP Media Gateway, it is signed with a specific Alcatel-Lucent private key. When the IP Media Gateway receives its binary through TFTP, it first checks the integrity of the file using corresponding Alcatel-Lucent public key (mechanism based on **SHA1 and ECC 384 bits**). If control fails then the new binary is ignored and the IP Media Gateway starts with the previous verified binary stored in flash memory.

8.3 OXE MS (Media Services)

The goals of OXE MS are to built solutions without Hardware ALE Media Gateway and mainly to address Hosted Offers

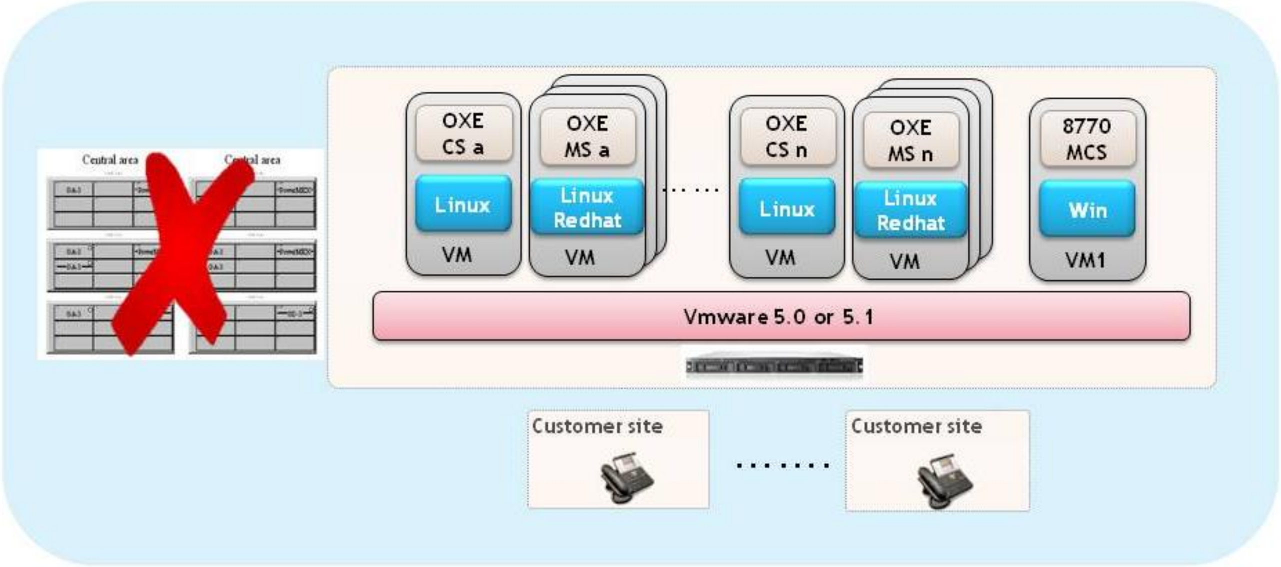


Figure 4: OXE Media Services

OXE MS application runs in virtual machine VMWare based on OS Linux RedHat 6.3 version for OXE only configuration.

Up to 240 OXE MS are supported per OXE

OXE MS is compatible with :

- Com Server redundancy (dual IP subnet or not)
- OXE ABC network deployment
- IP Touch Security (via SSM-RM / MSM/RM)

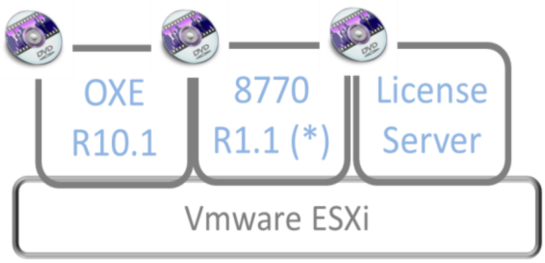
Serviceability :

- Installation via Alcatel-Lucent Enterprise Deployment Tool (ALEDS)
- OXE mechanism for upgrades (as for HW IPMG)
- Alarms for troubleshooting
- Displayed as a large MG in the 8770 Topology

8.4 Virtualization

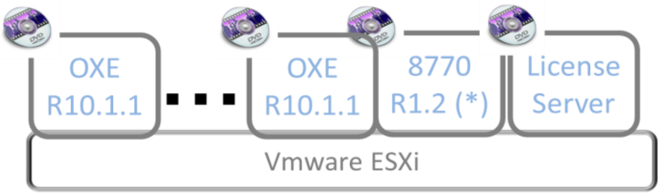
Virtualized IP Telephony

The OmniPCX Enterprise offer (from R10.1) can be virtualized:

 	xxxx : Virtual Machine (*): Option Each component can be virtualized independently. OXE and Flex Server can be duplicated.

The provisioning levels are unchanged, compared to non virtualized solutions.

For very large configuration, several OmniPCX Enterprise can be virtualized:

 OXE R10.1.1 OXE R10.1.1 8770 R1.2 (*) License Server Vmware ESXi	xxxx : Virtual Machine (*): Option A single Flex Server for all OXE instances. Each component can be virtualized independently. OXE and Flex Server can be duplicated.

Virtualization and encryption:

- For the IP Touch Security feature, the SSM-RM module is required in front of physical server/blade (hosting Virtual Machine for the OXE ComServer)
- In case of multi-OXE instances on the same server or multiple blades in a chassis with one OXE ComServer installed on each blade, then multiple SSM-RM modules are required, one per OXE ComServer instance installed. Network configuration has to be done at the level of the VMware virtualized layer (VLAN configuration) and an external switch is required to be able to connect the different SSM-RM modules.

8.5 IP Terminals

8.5.1 Resistance to DoS attacks

Alcatel-Lucent IP Touch terminals use a simplistic, but very effective, **Ethernet Flood Limit** mechanism to counter many Denial of Service attack schemes. Basically, the Ethernet interfaces of IP Touch terminals will ignore all broadcast Ethernet traffic in excess of 300 Packets Per Second (pps). Since typical IP Phone communication is based on unicast traffic and not broadcast traffic, this protective mechanism has no effect on voice flows. It is important to note that the Flood Limiting measure described here does not apply to traffic traversing embedded IP Touch Ethernet switches for clients attached behind the terminal.

IP Address duplication can cause disruption to VoIP flows of communication. As this is an inherent vulnerability of IP, little can be done by Alcatel-Lucent (or other vendors) to counter this problem. If the IP address of an Alcatel-Lucent IP Touch terminal is duplicated (usurped by another network client), a message will be displayed indicating the error and the IP Phone will reboot to request a new address from the DHCP server (if a DHCP server is configured in the system).

Alcatel-Lucent IP terminals use either proprietary Signaling Call Control protocol (named as UA/NOE protocol) or standard SIP protocol. For voice media streams, standard RTP/SRTP/RTCP protocols are used. There are no HTTP servers, telnet servers, FTP servers or direct JAVA interfaces hosted by the terminal that would allow an external network client to push information. XML applications are delivered via data link established between the terminal and the OXE Communication Server.

Alcatel-Lucent IP Handsets cannot be used in Distributed Denial of Service attacks. By not supporting direct connections via HTTP, telnet, ftp, TFTP and other IP protocols, Alcatel-Lucent IP Phones are of limited interest to network attackers. All JAVA, XML and call control functions must be provided by the centralized Presentation Server (PRS) elements.

8.5.2 Resistance to ARP attacks

Level of trust in an IP Telephony solution is based on mutual authentication between phone set and Communication Server. This mutual authentication is provided through several mechanisms integrated in our solution.

8.5.2.1 ARP attacks protection

First of all, Alcatel-Lucent IP Touch device itself provided native features to address **ARP attacks**. When a network client needs to resolve the MAC address of another network client/host (as is the case when only an IP address is known, i.e. new communication between endpoints), Address Resolution Protocol (ARP) messages are exchanged. Alcatel-Lucent IP Touch devices are IP endpoints, thus they rely on ARP functions in order to build MAC address tables for IP communications peers. When, for example, an IP Touch initiates a new communication request with another IP terminal (or with the Communication Server), it first uses ARP to determine the MAC address of the target terminal or the appropriate IP router interface required to handle the session. There are two kinds of ARP messages (request and reply); ARP requests are sent in broadcast format, ARP replies in unicast.

There is a cache (the ARP table) which maintains the association between MAC and IP addresses within each IP client. To reduce ARP traffic, most IP Clients exploit all ARP messages that are received and store them for a determined length of time. Indeed, when a host receives an ARP request, it deduces that a connection is going to be performed, and creates a new entry for this host in its ARP table.

A generic IP Phone can be attacked in two different ways:

- ARP spoofing: (falsification of ARP reply after an ARP request) In this attack scheme, following a valid ARP request made by the IP terminal, an attacker can attempt to provide a falsified ARP reply with MAC information that seeks to redirect traffic to a different target. Since the ARP table of the IP phone has no prior entry for the requested IP address/MAC, it has no ability to differentiate the correct MAC address from the falsified one.
- ARP cache poisoning: (injection of gratuitous ARP packets) In this attack scheme, an IP Phone can be forced to receive an ARP reply without the phone being required to send an ARP request. The goal of this attack is to prevent IP clients from requesting valid MAC address information by regularly providing falsified information to “poison” ARP tables.

IP Touch Protection:

- **Anti-ARP Spoofing**: Alcatel-Lucent IP terminals are able to recognize multiple (differing) ARP replies and recognize that this could indicate an attack. After sending an ARP Request the phone set automatically launch a configurable timer that defines the window during which ARP Reply message can be received (maximum 60 seconds). The first ARP Reply message is taken into account and in case of subsequent ARP Reply messages for the same IP address but from different equipments (ie MAC addresses) then it is considered as a potential attack. After detection, the IP Touch set logs information about attacks (MAC address, IP address, Time) and sends an incident to the Communication Server. This information can then be passed from the Communication Server to OmniVista 4760 platform for administrator notification (through SNMP TRAP). It may happen that the IP address registered by the IP Touch set during this sequence is the one of a rogue equipment, but at least an incident is sent and network administrator can perform a control on this identified set.
- **Anti-ARP Cache Poisoning**: Alcatel-Lucent IP terminals only update their internal ARP tables after they have initiated an ARP request. An Alcatel-Lucent IP terminal will reject any ARP reply that is not offered in direct response to an ARP request made by itself. Gratuitous ARP replies are ignored by Alcatel-Lucent IP terminals, thus eliminating this attack as a threat.

8.5.3 IP Phone/Communication Server Trusted Communication

To ensure a better level of trust in communication between IP Touch sets and the Communication Server, different mechanisms have been integrated:

- **TFTP Request Check**: during its initialization, the first action performed by an IP Touch set is to send a TFTP request (to internal TFTP server) that contains MAC address of the set. There is a mechanism at CS level that will check if a signaling link is not already established with a set corresponding to this MAC Address. In that case it could be an attack where the hacker is trying to spoof identity of an existing set (based on its MAC Address). The Communication Server will react by rejecting the rogue TFTP request.
- **Connect Message Filtering**: during initialization phase, an IP Touch set will receive a Connect message from the Communication Server initiating the control link between the two elements. It is critical to ensure at that time it is really the Communication Server that sent this message, to avoid possible Man-In-The-Middle attack where the phone set could be finally controlled by a rogue server. To protect the IP Touch set, source IP address of the Connect message is compared to real Communication Server IP address received previously in configuration file. If IP address doesn't match, then Connect message is refused.
- **Anti-IP Touch MAC Spoofing**: this is an additional control on Communication Server side. At the end of IP Touch set initialization, the Communication Server requests its MAC address through specific message. When returned by the set, it is compared to the one previously given by the IP Touch thanks to startnoe message. If MAC address doesn't match, a reset order is sent by the Communication Server to the set.

8.5.4 Binaries Check

The IP Touch phone uses TFTP protocol to download new binaries at initialization. Prior to use, binaries are checked by the set based on a Alcatel-Lucent public/private key infrastructure (PKI). The IP Touch binaries are digitally signed at production time with a specific Alcatel-Lucent private key. Based on corresponding public key, the IP Touch set is able to check integrity of files before starting to use them (default behavior with Extended Edition models). If the verification fails the IP Phones maintain existing binaries.

Digital signature also applies to configuration files if the IP Touch Security feature is configured in the OXE system. In that case, the SSM (Server Security Module) is used to sign the configuration files to be used by the IP Touch sets. This mechanism uses an **ECC 384 bits algorithm**.

8.5.5 MMI Protections

Man Machine Interface Control is a mechanism to restrict access to the configuration of IP Touch terminals. The passwords are managed by the Communication Server to restrict entry into the local configuration menu with a password (6 to 12 character).

The global password is the same for all terminals.

All local terminal menus and data are protected in a 'secure' zone of the flash memory.

The only method of disabling this protection is to reset the phone locally to factory default settings.

8.5.6 Strict VLAN control

The goal of this parameter is to protect the IP Touch software by filtering all incoming frames.

As soon as a VLAN number is configured for an IP Touch (from a DHCP/AVA server or directly in the IP Touch menu at set start-up), the parameter "**strict VLAN**" is also configured (default value). This parameter can be deactivated from the IP Touch menu.

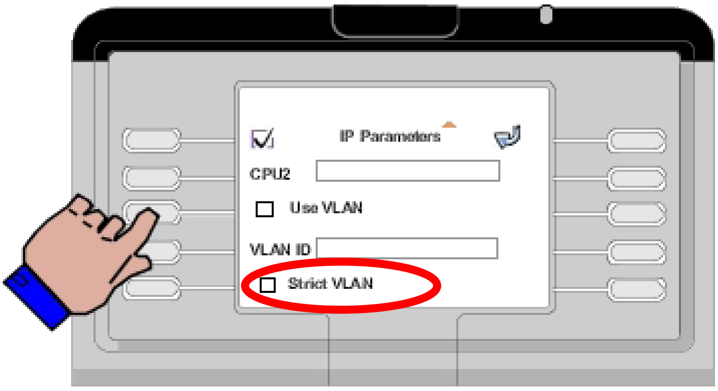


Figure 5: Strict VLAN

If a voice VLAN is used and "strict VLAN " is activated, the IP Touch software rejects all the frames with a "non matching" VLAN tagging (without VLAN ID or with a different VLAN ID).

If the IP Touch does not use a voice VLAN and strict VLAN is used, the IP Touch software rejects all frames tagged with a VLAN ID.

This parameter has no influence with the PC port security behaviour.

8.5.7 PC port and Trafic Isolation

The IP Touch telephones have two Ethernet ports, one of which can be attached to a PC. The Embedded Switch Controls this "PC" port. The Communication Server has the ability to disable secondary switch port of IP Touch terminals (global and/or phone by phone setting).

Three different behaviours can be configured independently for each IP Touch :

a) <u>PC port security not activated</u> (default) : the integrated switch of the IP Touch passes transparently all traffic from/to the PC port
b) <u>block PC port</u> : the traffic from/to the PC is blocked (RX and TX bits of the PC port are disabled)
c) <u>filter VLAN</u> : the IP Touch replaces any 802.1q tag to VLAN ID 0 for frames coming from the PC to the LAN, and remove 802.1q tags for frames coming from the LAN to the PC. **The goal of this mode is to protect the voice network against possible intrusions from the PC port, by preventing the PC from sending traffic in the voice VLAN.**

This configuration is not accessible from the IP Touch menu.

In case of a PC connected behind the IP Touch:

The switch equipment the IP Touch set is connected to can support two VLAN IDs which are sent/received on one physical LAN switch port :

- one VLAN ID for the IP Touch,
- the other for the PC connected behind the IP Touch, which is not the default VLAN ID 0.

Conditions : the PC must be able to perform 802.1q tagging by itself, and the IP Touch must be configured with "PC port security not activated".

or

“filter VLAN” is activated and the IP Touch. It will then tag frames coming from the PC with Vlan ID 0. The PC is included in the default VLAN managed at the LAN switch level.

8.5.8 802.1X on IP Touch sets

Since OmniPCX Enterprise Rel 7.0, **ALL** x8 series IP Touch terminals (4008, 4018, 4028, 4038 & 4068 with 8Mb of RAM or more) support 802.1X.

This standard protocol is used to authenticate IP devices at switch level before it is allowed to communicate to other resources in the network. Switch equipment acts as the guardian that verify only known and trusted devices will be accepted.

The authentication request always comes from the switch. It happens when:

- the IP Touch set is physically plugged to the network
- the IP Touch set reset (in case of IP link loss to the Communication Server, switchover to a backup IPMG or PCS etc…)
- the switch is configured for periodic re-authentication (time period defined at switch level)

The switch (called the authenticator in 802.1X terminology) relays the authentication replies from the IP Touch set (called the supplicant) to a RADIUS server (called the authentication server). After a pre-defined time period, if the switch has not received an answer from the RADIUS server, it sends back an authentication failure message to the IP Touch set. The message is displayed briefly on IP Touch set screen (as “802.1X authentication failure”).But the IP Touch will nevertheless continue its initialization and retry an authentication attempt thirty seconds later. The IP Touch set has a maximum of three authentication attempts before it’ll reset and restart its initialization from the beginning.

If a PC is connected behind the IP Touch through dedicated PC port, a second 802.1X authentication will be performed by infrastructure equipment if multi-session is available (as delivered by Alcatel-Lucent OmniSwitch products).

TLS authentication method can also be used for IP Touch phones. Based on X509 digital certificates, it allows for strong authentication of the device. This method is available since OmniPCX Enterprise R9. Each IP Touch set embeds from factory a default digital certificate produced from Alcatel-Lucent PKI. This default certificate can be used for Plug&Play authentication or a customized certificate can be produced at customer’s PKI level and downloaded directly in the IP Touch set.

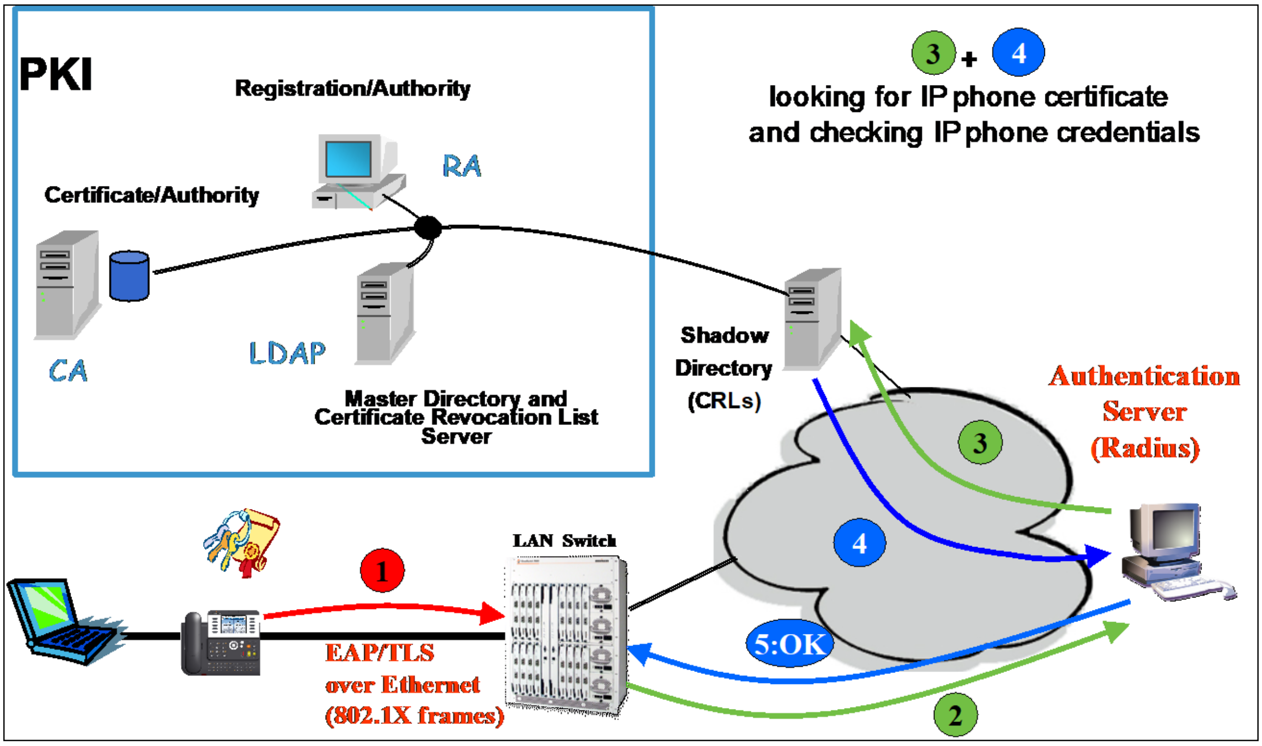

PKI
Registration/Authority
RA
Certificate/Authority
CA
LDAP
Master Directory and Certificate Revocation List Server
3 + 4
looking for IP phone certificate and checking IP phone credentials
Shadow Directory (CRLs)
Authentication Server (Radius)
3
4
LAN Switch
1
EAP/TLS over Ethernet (802.1X frames)
5:OK
2

Figure 6: 802.1X TLS on IP Touch sets

8.5.8.1 EAP-Logoff on IP Touch sets

Without EAP-Logoff Feature

If a PC behind the IP Touch is already authenticated, it is possible to unplug this PC and connect another device to the network without the need to re-authenticate this device.

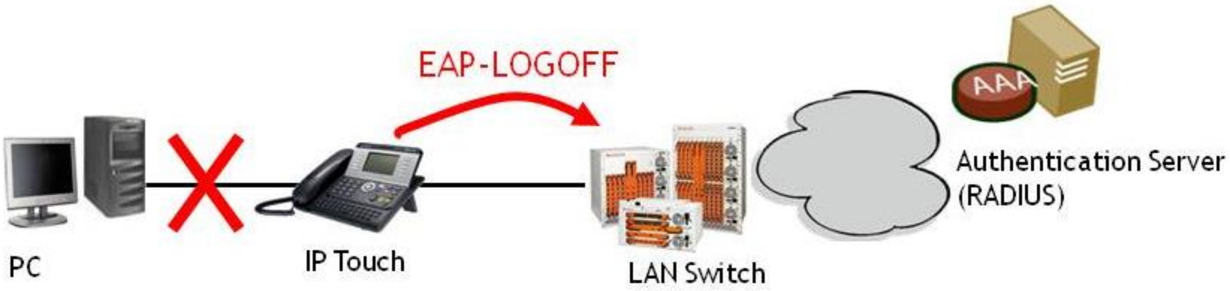


Figure 7: EAP-Logoff

With EAP-Logoff Feature

If the PC behind the IP Touch is unplugged, the IP Touch sends an EAP-LOGOFF message on behalf of the PC to the switch. The switch sets the specified MAC address to an unauthenticated state. When the PC is plugged back, this PC will need to re-authenticate.

8.6 OmniTouch Instant Communications Suite

OmniTouch Instant Communications Suite (ICS) is a suite of software applications to improve real-time communications across the enterprise.

ICS provides unified messaging, audio/data and video conferencing, personal routing, instant messaging (IM), sophisticated softphone capabilities, universal directory access and presence information. The different services delivered by ICS are named as:

- Telephony service
- Messaging service
- One Number service
- Teamwork service

In addition to internal authentication and confidentiality mechanisms, ICS integrates seamlessly within security policies of the enterprise.

8.6.1 Authentication

The aim of the authentication process is to control who can access to the resources. This is done at the resource level (i.e. application) by controlling the user ID and the password.

1) **External LDAP/LDAPS authentication**

ICS can authenticate users based on an existing LDAP server with existing user accounts.

2) **External RADIUS authentication**

RADIUS implemented in ICS software provides strong central server authentication mechanism for ICS users (and ICS system administrators). For redundancy and high availability purpose, a secondary RADIUS server may be defined in case of a primary RADIUS server failure.

3) **Single Sign On through NTLM**

Single Sign-On (SSO) is a mechanism whereby a single action of user authentication and authorization can permit a user to access all systems where he has access permission, without the need to enter multiple passwords.

Single sign-on reduces human error, a major component of systems failure and is therefore highly desirable. Kerberos is the protocol used for the SSO mechanism. This authentication process is only available for desktop interface. This functionality applies for One Number Services, Messaging Services and Phone Services.

Since OmniTouch ICS R6.6, NTLM Kerberos is used for SSO authentication.

8.6.2 Log and activity reporting

As of OmniTouch ICS R6.7, an audit trail or audit log for administrator activities is a chronological record of system activities performed via the Web Administration tool to enable the reconstruction and examination of the sequence of events and/or changes in an event (e.g. modification of system parameters, user suppression, etc).

Administrator activities are stored on the ICS server in a dedicated log file, which contains following information:

- Creation/suppression of entities (users, voicemails, applications…)
- Modification of entities (list of properties that have been changed with the current and previous values)
- System configuration changes

Each activity contains a timestamp and additional information such as:

- IP address used to connect to the system
- Administrator name
- Action type (creation, modification, suppression)

Following administrator tasks are tracked:

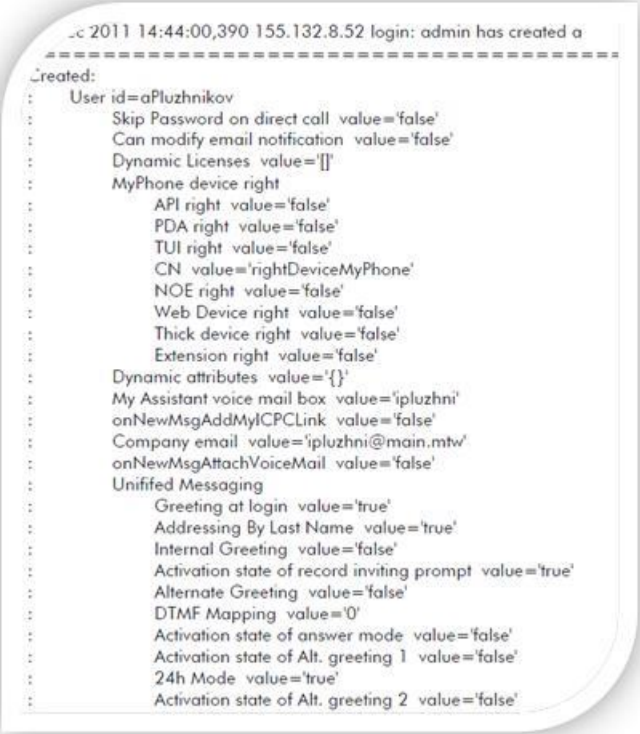
- Creation, modification or suppression of:
  - Users, as well as system parameters linked to users
  - Voicemail boxes, as well as system parameters linked to voicemail boxes
  - Administrators
  - Applications
  - Servers (Device Management data are however not considered)
- Modification of system parameters
- Modification of voicemail system parameters
- Mass provisioning

Audit logs are enabled by default and localized in English only. Following parameters can be specified (in a property file) for the logs:

- Activated (default)/deactivated
- Path
- Max size

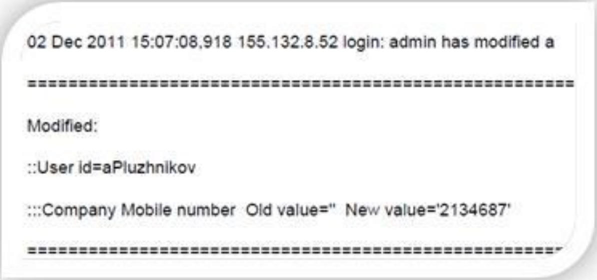
Examples:

- Creation of an ICS user



```
c 2011 14:44:00,390 155.132.8.52 login: admin has created a
=====================================
Created:
:     User id=aPluzhnikov
:           Skip Password on direct call  value='false'
:           Can modify email notification  value='false'
:           Dynamic Licenses  value='[]'
:           MyPhone device right
:                 API right  value='false'
:                 PDA right  value='false'
:                 TUI right  value='false'
:                 CN  value='rightDeviceMyPhone'
:                 NOE right  value='false'
:                 Web Device right  value='false'
:                 Thick device right  value='false'
:                 Extension right  value='false'
:           Dynamic attributes  value='{}'
:           My Assistant voice mail box  value='ipluzhni'
:           onNewMsgAddMyICPCLink  value='false'
:           Company email  value='ipluzhni@main.mtw'
:           onNewMsgAttachVoiceMail  value='false'
:           Unififed Messaging
:                 Greeting at login  value='true'
:                 Addressing By Last Name  value='true'
:                 Internal Greeting  value='false'
:                 Activation state of record inviting prompt  value='true'
:                 Alternate Greeting  value='false'
:                 DTMF Mapping  value='0'
:                 Activation state of answer mode  value='false'
:                 Activation state of Alt. greeting 1  value='false'
:                 24h Mode  value='true'
:                 Activation state of Alt. greeting 2  value='false'
```

- Modification of an ICS user parameter



```
02 Dec 2011 15:07:08,918 155.132.8.52 login: admin has modified a

=====================================================

Modified:

::User id=aPluzhnikov

:::Company Mobile number  Old value=''  New value='2134687'

====================================================
```

8.6.3 High Availability

Operating system used for OmniTouch ICS servers is Red Hat Enterprise R5. This OS provides native redundancy mechanism based on cluster duplication principle and allows an “n+1” backup for ICS servers:

- “n+1” redundancy for the global functionality (Telephony/One Number/Messaging services)
- An additional “n+1” redundancy capability for Teamwork service.

8.6.4 MyIC Desktop client

MyIC (My Instant Communicator) Desktop client is an application installed on employee PC station that allows him to manage the usage of advanced telephony and unified communications features. For example the MyIC client on the PC station can be seen and considered by the IP Telephony system as an entire phone with full telephony features. This kind of application is traditionally called “softphone” but level of feature really depends on IP Telephony system that controls this softphone.

It is essential when deploying softphone application in customer network to ensure that this kind of application will not decrease the overall level of security of the IP Telephony solution.

In some network configurations or if required to conform to the security policy rules defined by the customer, an additional component called softphone proxy can be required to ensure connectivity between data and voice VLANs and control/filter media sessions from PC based clients (softphones) to Communication Servers. The softphone proxy component is usually based on a **Session Border Controller** (**SBC**) product to manage SIP sessions (for voice and video). The A-LE **OpenTouch SBC (OT SBC)** product can be used for this purpose (refer to the document *OpenTouch Suite MLE Standard Offer / Security chapter* for more details on the OT SBC product and its capabilities).

The MyIC Desktop client is able to support **SIP/TLS** to secure the signaling call control protocol and **SRTP** to encrypt the voice media up to a secure gateway installed in the customer’s network. This secure gateway can be an SBC component such as the OT SBC product from A-LE.

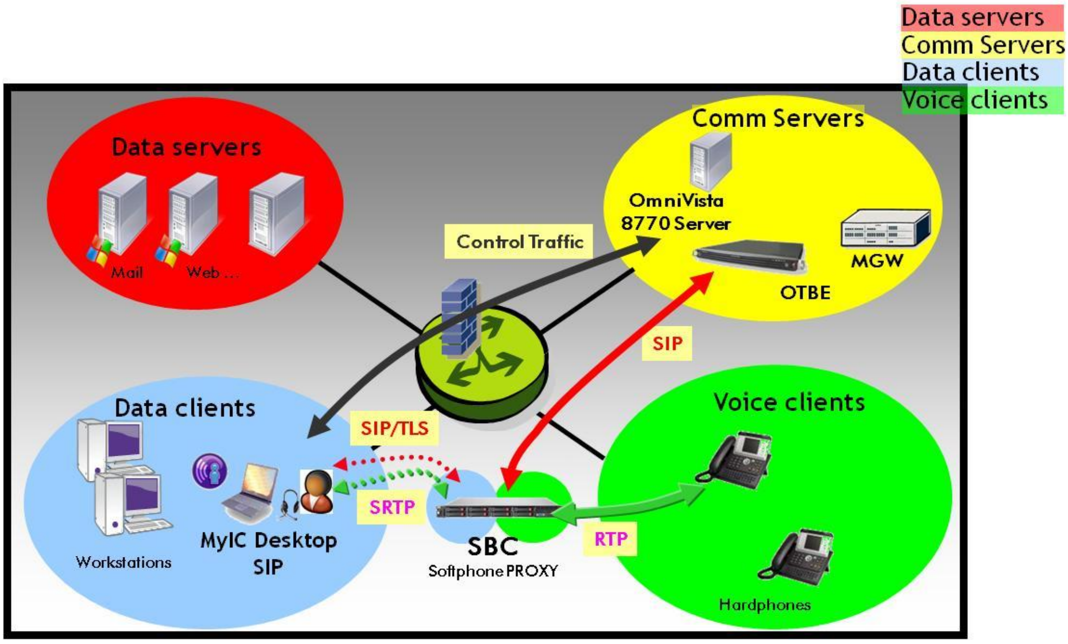


Figure 8: OT SBC product used as Softphone Proxy component

8.7 OpenTouch SBC

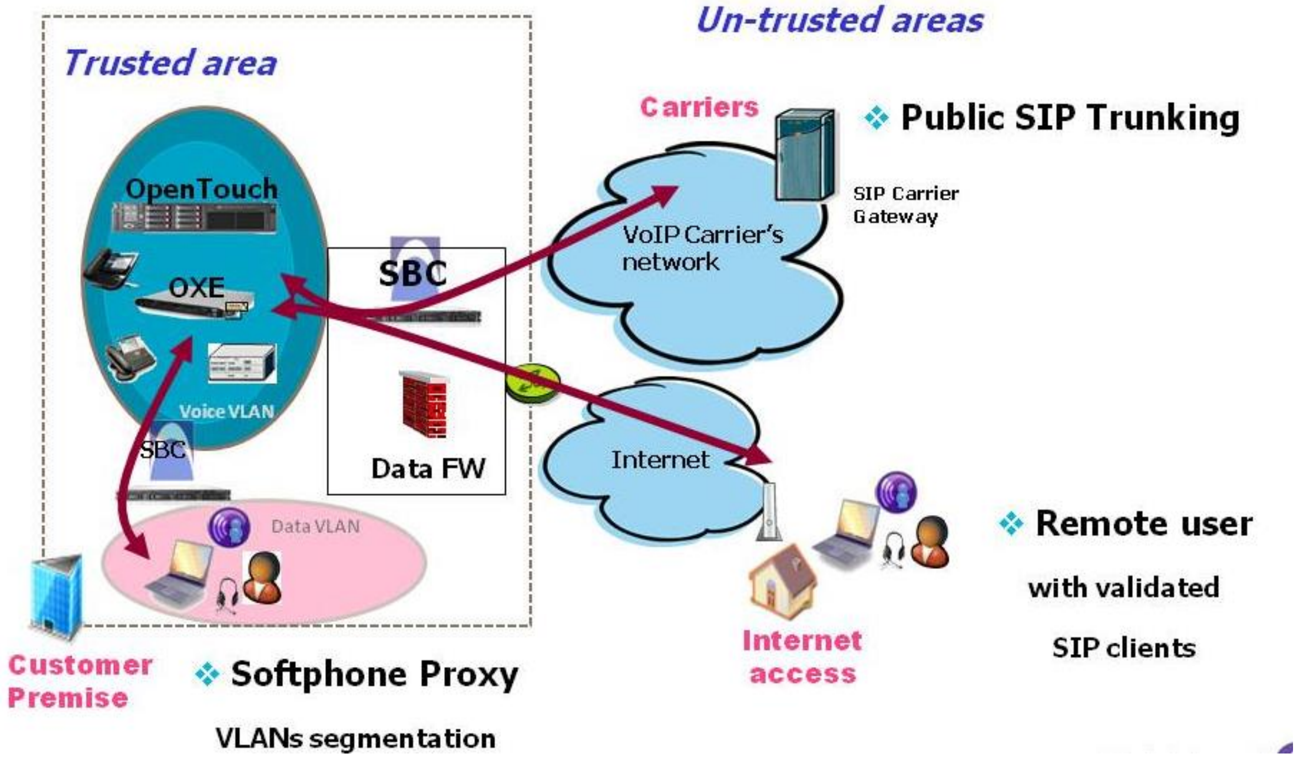


Figure 9: OpenTouch SBC

OpenTouch SBC is part of customer infrastructure. It is installed at the border of the corporate network, as a companion to the existing data firewall. It does not replace the firewall, it just manages all incoming and outgoing SIP sessions.

The SBC is useful in the following cases:

- interconnection with Carriers Service Providers through Public SIP Trunks
- openness to remote SIP clients, for example teleworkers connected from their home spot or external people that you may want to invite into a voice and video conference
- to ensure secure softphone deployment in the Enterprise network

8.8 Voicemail applications

Three Alcatel-Lucent voice mail options are currently available for the OmniPCX Enterprise:

- **OmniMessage 4635**: Used for large legacy configurations.
- **OmniMessage 4645**: Developed for smaller user populations and simple service environments.
- **OmniTouch 8440/OTMC VoiceMail**: the new voice mail solution that can be a classical voice mail system for the IP Telephony solution but can also provide unified messaging services.

Depending on the voice mail system there are different security mechanisms that are provided:

- Transfer control performed from the voice mail service
- Mailboxes protected by a personal password
- Checking message recipient before the message is sent
- Restricted access to distribution lists
- Secure access to voice mail management
- Supervision data

8.8.1 OmniMessage 4635

Alcatel-Lucent's OmniMessage 4635 platform draws its lineage from the much revered Octel voicemail product line. Octel based systems are among the most widely deployed voicemail platforms in the world, and enjoy an incredibly rich feature set and an industry setting level of product maturity and completeness.

8.8.1.1 Security of voice mail boxes

The 4635 system allows the number of failed attempts of the secret code on the same voice mail box to be controlled. The maximum number of failed attempts is by default 3. After this maximum number, the call is automatically released. The voice mail access is not forbidden; this means that the user can recall this voice mail box.

Secret code format: it is possible (optional) to prohibit some simple numbers (same consecutive digit, its set number …).

Users can be obliged to periodically change the secret code of their voice mail box.

8.8.1.2 Access mode to the voice mail management application

The access to the voice mail system is possible via a VT100 console connected:

- in local with predefined V24 port
- in remote with RMA / modem.

In both cases, a password is required to access to voice mail data. This password is the password of "A4635 system manager" box.

In addition, OmniMessage 4635 voice mail solution is compatible with IP Touch Security feature to provide encryption of the user communications to their voice mailboxes.

8.8.2 OmniMessage 4645

Alcatel-Lucent's OmniMessage 4645 voice mail application can be hosted on the OmniPCX Enterprise Communication Server or on a dedicated processing platform. 4645 Voicemail is based on the same system platform as the Communication Server and benefits from the same integrated security features.

OmniMessage 4645 voice mail application is compatible with IP Touch Security feature to provide encryption of the user communications to their voice mailboxes.

8.8.3 OmniTouch 8440/OTMC Voicemail

OT8440/OTMC voicemail solution provides several security features to ensure protection of both system and user data managed by the system.

The voicemail system is based on an hardened Red Hat Enterprise 5.0 Linux. It can be configured with high availability mechanism (N+1 mode). Administrator can perform backup/restore operation for both system and user data. Administration is secured by using specific protocol (HTTPS) and strong user authentication can be configured based on external authentication server (RADIUS).

OT8440/OTMC voice mail solution is compatible with IP Touch Security feature to provide encryption of the user communications to their voice mailboxes.

8.9 OmniVista management platform

The OmniVista management platform has been designed to address specific security issues of an administration application. Architecture itself is based on a server/client principle. The client function is embedded on a PC to allow creation and modification of the management settings. It can connect to OmniVista server through secured IPSec channels. There is no direct interaction between OmniVista clients and OXE Communication Servers: only OmniVista server can connect to a CS using secured protocols.

Two product lines are currently available:

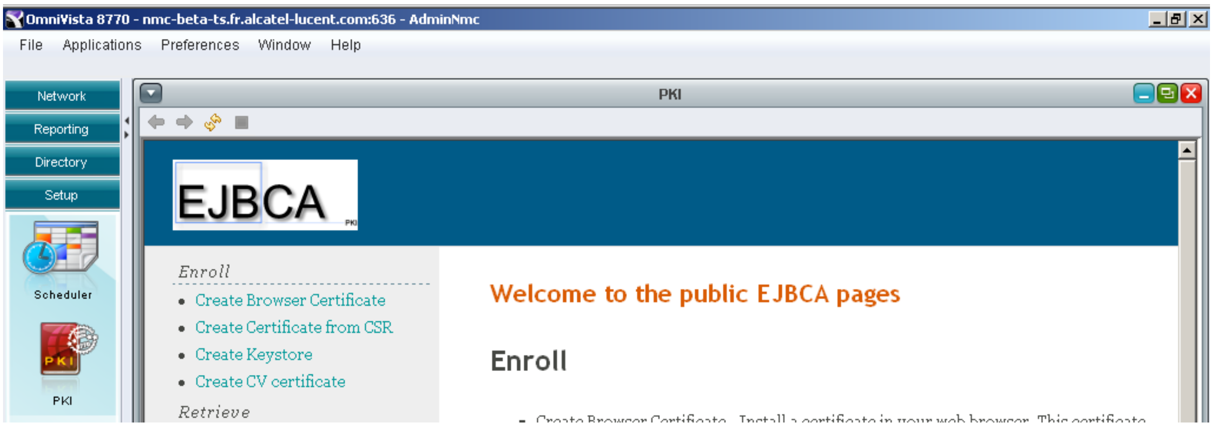
- OmniVista 4760
- OmniVista 8770

OmniVista 8770 is the new generation of the management platform for the OmniPCX Enterprise solution and OpenTouch solution. OmniVista 8770 benefits from the same security features and capabilities than legacy OV4760.

8.9.1 PKI module in OmniVista 8770

Features	▪ Certificate Authority (creation) ▪ Sign CSR ▪ Certificate Revocation List
Usage	▪ In case the end customer has no PKI for Voice Product and wants to customize the certificate of the xSM modules (SSM-RM and MSM-RM)

The PKI module integrated into the OmniVista 8770 solution can be used by the customer to generate and administrate the certificates that are used by the SSM and MSM modules. Once generated with the PKI, the certificates must be downloaded on each SSM and MSM.



Welcome to the public EJBCA pages

Enroll

- Create Browser Certificate
- Create Certificate from CSR
- Create Keystore
- Create CV certificate

Retrieve

Enroll

- Create Browser Certificate - Install a certificate in your web browser. This certificate

Figure 10: 8770 PKI module

8.9.2 Password policy enforcement

Administrator and user authentication (to access directory information for example) is required and is based on login/password principle. This mechanism is enforced by allowing strict conformance to security policies based on standard:

- password policies to check minimum length, avoid trivial passwords, remember previous passwords, force password change after the first login.
- Configure automatic lock of a user account after multiple failed authentication attempts.
- Aging password (expiration time, minimum time, warning before expiration)

Those mechanisms are available on OmniVista server and are made by the Sun One directory.

Password check can also be performed with external RADIUS server.

8.9.3 OmniVista back up and disaster recovery process

Critical Information like configuration, phone book, call accounting tickets are regularly saved in a database. The archiving of this data can be done automatically on a daily basis on the OmniVista network management platform. It has two main objectives:

- enable automatic report generation on billing and network performance
- storage of up to date data enabling fast and easy recovery in case of disaster.

Raid array and optical disk storage can be used for this backup. Up to four unique release and configuration combinations can be stored to offer rapid roll back recovery from upgrade/modification failures.

Specificities of the back-up feature:

- Automatic OmniVista database back up: Call Detail Recorders, performance counters, carriers tariffs, reports, LDAP directories, network data, etc. can be regularly and automatically saved on a directory viewable by the server
- Defense against database saturation: there are warnings if disk usage exceeds specific thresholds. Two thresholds can be set up. When the disk usage exceeds the first threshold, a minor alarm is generated, and a major alarm is generated when the second threshold is reached. There is also an automatic data purge that can be configured based on specific information (data age, specific data filters, defragmentation of the ASA/LDAP databases, etc…)

Available the back-up mechanisms to prevent from outage and facilitate a disaster recovery plan:

- **RAID5** to secure the OmniVista Database (Call Detail Recorders, reports), onto Network Drive
- **UPS** to secure the PC servers against power outage
- **Standby OmniVista PC server**: a standby server can be synchronized with the OmniPCX network and the active OmniVista server. Object models will be synchronized, allowing update of the network system directory, company directory, and update of topology and accounting orgmap costs centers and users. Alarms are sent in real time to both OmniVista servers.

If the active server crashes, the standby server can take over instantly, for all the applications. The users have to change the address on their browser or client.

Conditions: the IP address of each node is not automatically updated. If a CPU IP address is changed, the administrator has to update the information in both OmniVista servers. It is the same for the customizations, except for the customized report definitions that can be regularly exported and imported, and for the directory that can be replicated.

8.10 IP Touch Security solution

The security of voice over IP communications is generally judged to be less secure than in a TDM (Time Division Multiplexing) environment.

Voice flows over a shared network are susceptible to being intercepted and listened to by anybody with access to the LAN, with the help of “freeware” tools. A package of measures at the infrastructure level of the network allows the essential limitation of interception risks (switched LAN environment, VLAN voice segmentation, management of ACLs between VLANS, protection against ARP spoofing or flooding), but the only way of being certain that voice flows are well protected is end-to-end encryption: even if they are intercepted they will then be inaudible.

This allows a level of confidentiality superior to that found in a TDM environment (without special equipment).

In order to have a sustainable encryption solution, it is equally necessary to secure the phases preceding the establishment of voice flows. To this end, the encryption and also the integrity of the signal between the communication server and IP telephones/ Media Gateways must be established.

The authentication of the different elements comprising the IP telephony solution must be a prerequisite to the establishment of secure communications, if not there is a risk of a certain number of attacks of the “man in the middle” type which put the confidentiality of the message in danger through the interception of private information.

The initialization of IP terminals must be secure in order to avoid a binary downloaded from a rogue server from being executed on the set. To this end, IP phones initialize in a secure way validating the signature of downloaded files.

Alcatel-Lucent is partnered with Thales, a major security player in the domain of Defense and Enterprises, in order to be better able to provide clients with vital security solutions, a high performance encryption solution responding to real time voice criteria (delay and commutation time) and with a high level of security.

The solution allows the encryption of all communication flows linked to voice at the moment they cross through LAN and even WAN. It does not encrypt TDM flows for example on a T2 junction or on a link to an analogue post, even if the IP section of the communication is encrypted.

IP Touch Security feature provides protections in the following areas:

- **Confidentiality**: Encryption of Voice & Signaling call control flows.
- **Integrity**: Ensuring messages exchanged between Communication Server and IP phones are not modified.
- **Authentication**: Pre Shared Key mechanism provides a mutual authentication between Communication Server and IP phones. PSK can be customized by the customer. As of OXE R10.0, standard TLS can also be used for mutual authentication based on digital certificates.
- **Binary signature**: Digital signatures verify authenticity of binaries and configuration files for hardware security modules, IP phones and Media Gateways during download.
- **Visual control**: Padlock icon to indicate on the phone set that the communication is secured.

The equipment concerned with encryption is as follows:

- The OXE Communication Server (on ALU proprietary hardware boards, appliance server or Blade server) and Passive Communication Server (PCS)
- The Media Gateways IP range (Common Hardware or Crystal)
- The OXE MS (Media Services)
- The IP Touch range (series 8)
- OmniTouch ICS servers (application servers and media servers)

The solution strongly depends on the standards in order to guarantee the sustainability of the solution and the future possibilities in regards to SIP environments, for example.

- Voice encryption by SRTP (RFC 3711) protocol with AES encryption in counter mode. The symmetrical voice keys are derived from receipts from when the CS crossed the encryption signal.
- The encryption of the signaling call control by IPSec ESP (RFC 2406) in transport mode with AES encryption in block mode (AES CBC). The signal keys are negotiated between terminals and Com Server with the help of IKE (Internet Key Exchange – RFC 2409) based on a calculated PSK (Pre Shared Key). As of OXE R10.0, standard TLS can also be used to secure SIP signaling for trunks managed by the OXE ComServer to external SIP Gateways.

Alcatel-Lucent and Thales have decided to separate the communications and encryption functions at Communication Server level to guarantee the solution’s flawless security.

Security hardware module (derivatives of Thales military programs) is inserted on Ethernet access of Communication Server.

The advantage of this approach is an avoidance of deactivation, either accidental or intentional, of the encryption without the user being made aware of it.

This approach provides a dual level of security for the communication services:

- first level with the Communication Server and its own security mechanisms (for access and administration)
- second level with the hardware module, physically separated from the Communication Server

(see reference documentation IP Touch Security Design Guide in OXE R11.0/ICS R6.7.x)

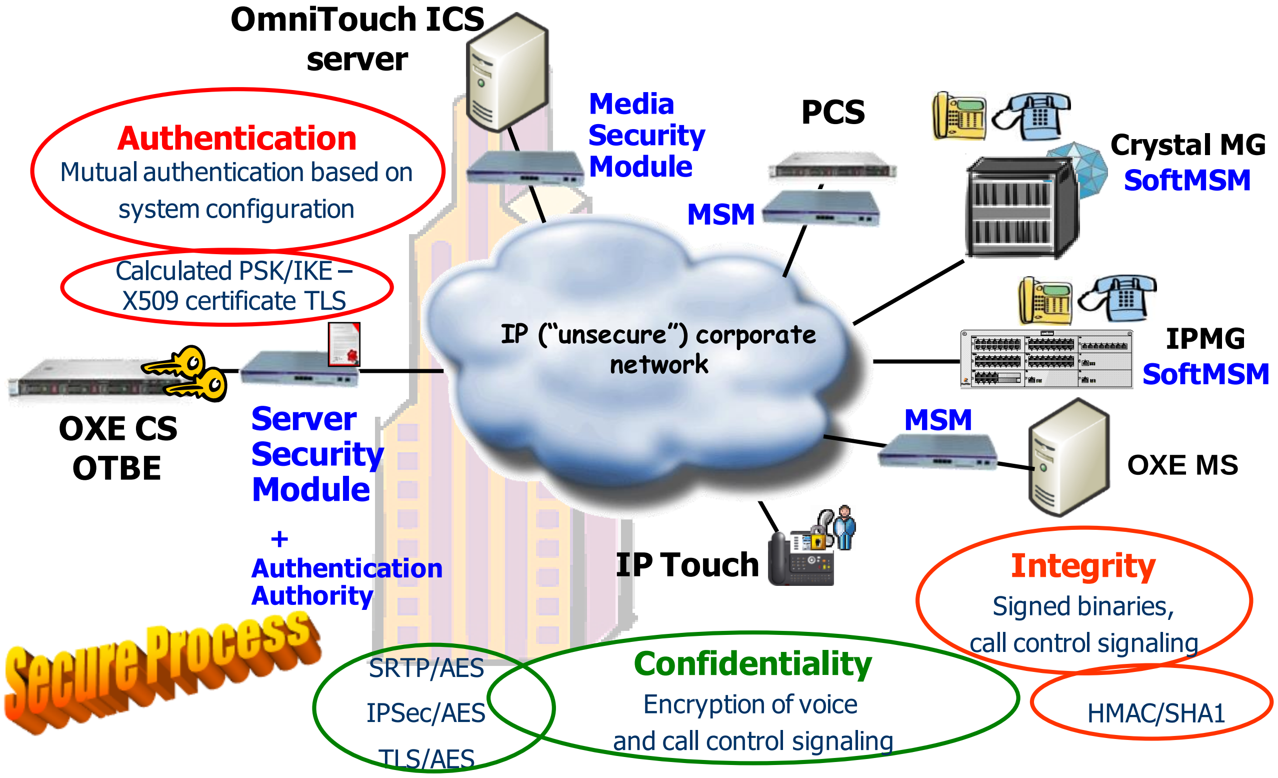


Figure 11: IP Touch Security feature overview

IP phones are equally protected against encryption deactivation. They do not accept to de-secure when the file signatures indicate that they were passed in non-secure mode.

It is equally important that the encryption does not affect the quality of service of the IP communications system. Moreover, IP communications impose significant real time constraints especially at the level of Com Server (management of thousands of sessions in real time) and at the level of IPMG (commutation and transport of several dozen real time voice communications).

9 Converged Network Security Approach

9.1 Strong Network Authentication

In order to perform a strong authentication at network level, IEEE 802.1X provides a framework for authorizing station access to the Ethernet. 802.1X uses the Extensible Authentication Protocol (EAP) to relay port access requests between LAN stations ("supplicants"), Ethernet switches or wireless access points ("authenticators"), and RADIUS servers ("authentication servers"). This solution is described in chapter 8.5.8.

9.2 Segregation of Traffic

Virtual LANs (VLANs) allow enterprises to logically segment the LAN using their existing switches without physical changes or new capital costs. VLAN segmentation can bring dramatic and immediate performance improvements, as well as simplify network administration.

To optimize bandwidth utilization and help secure real-time traffic, it is recommended to segment the network into separate VLANs for Voice and Data. This scheme limits the Layer 2 broadcast traffic to ensure a higner priority to the real-time voice flows. It also prevents from malevolent person to easily access to a voice equipment (client or server) from a data VLAN.

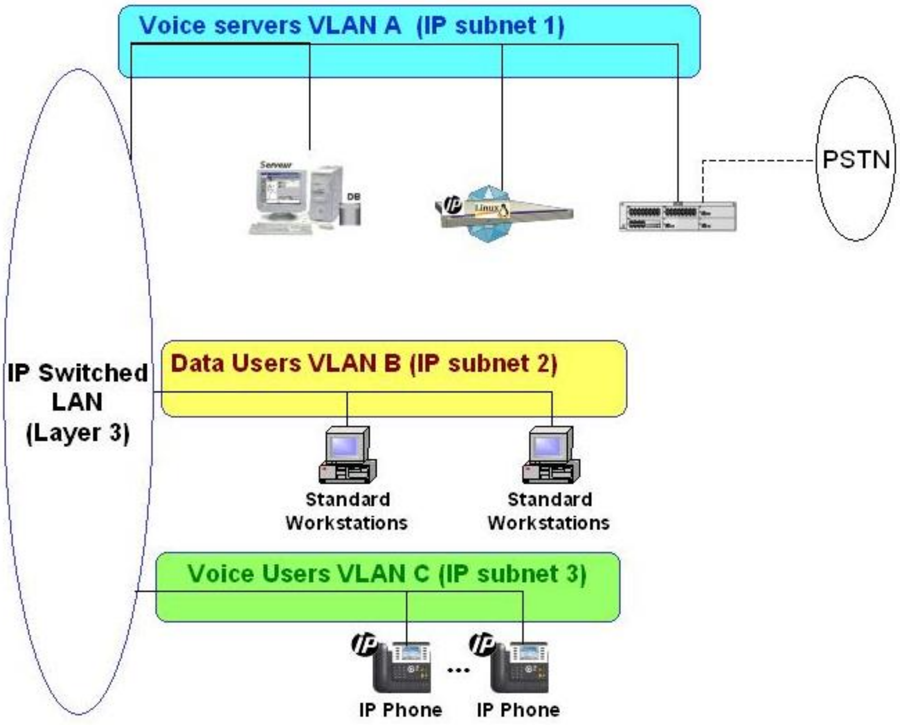

Voice servers VLAN A (IP subnet 1)
Serveur
DB
Linux
PSTN
IP Switched LAN (Layer 3)
Data Users VLAN B (IP subnet 2)
Standard Workstations
Standard Workstations
Voice Users VLAN C (IP subnet 3)
IP Phone
IP Phone

Figure 12: VLAN segmentation

9.3 Access Controls

The **Access Control List** (**ACL**) is a concept in computer security used to enforce privilege separation. It is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request. The list is a data structure, usually a table, containing entries that specify individual user or group rights to specific system objects, such as a program, a process, or a file. The privileges or permissions determine specific access rights, such as whether a user can **read** from, **write** to or **execute** an object. The ACL can be used to filter traffic between 2 VLANS (ie Voice and Data VLANs).

VLAN Access Control List Example

```
******** VLAN ACL  ***********
1  deny ip 0.0.0.0 255.255.255.0 any
2  deny ip 0.0.0.255 255.255.255.0 any
3  deny ip any 0.0.0.0 255.255.255.0
4  permit ip any host 239.255.255.255
5  permit ip any host 255.255.255.255
6  deny ip any 0.0.0.255 255.255.255.0
7  permit tcp any range 0 65534 any range 0 65534
8  permit udp any range 0 65534 any range 0 65534
9  permit icmp any any
10 permit ip any any
```

9.4 Infrastructure Redundancies

Redundancy at network level is an important aspect of the global security. Critical network functions like DHCP servers, TFTP servers, DNS servers, etc. must be duplicated to insure seamless operation during a failure occurrence. In addition to this consideration it is highly recommended installing the backup system on a different site or in a separate building (disaster recovery).

9.5 VPN Environments

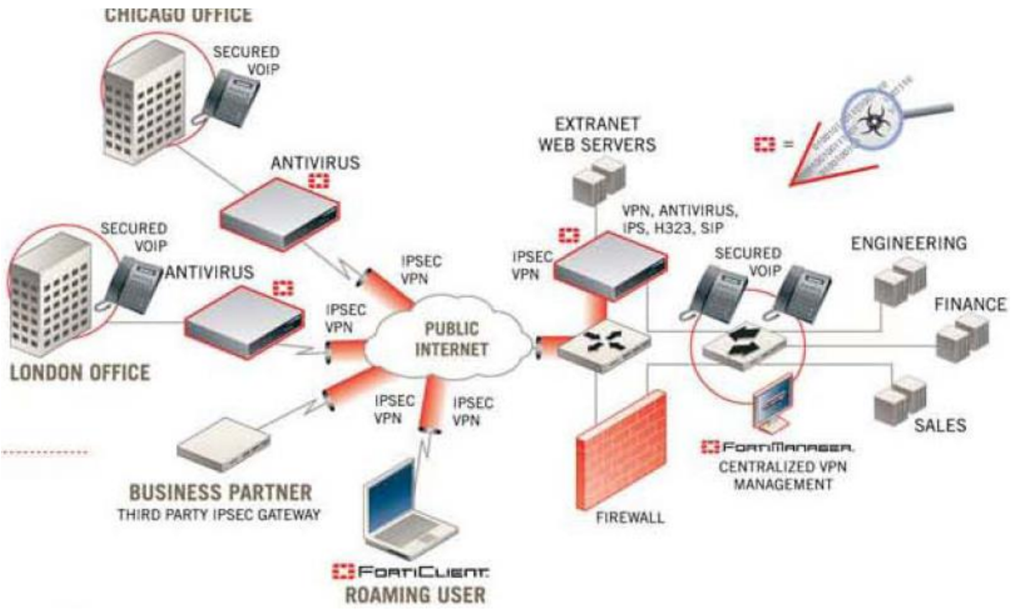
A VPN is a "virtual" network constructed by connecting computers together over the Internet and encrypting their communications so that other people cannot understand the communications. The benefit is that people can connect to a local LAN from anywhere on the Internet. This allows easier connectivity and lower phone bills for travelling salespeople. They just sign up with a national ISP and call local POPs from their hotels as they travel the country, easily connecting back to their company's local network.

When the use of IPSec or PPTP is desired, Alcatel-Lucent switches provide full VPN termination capabilities using hardware acceleration. All encryption protocols are run in hardware, with encryption hardware being appropriately sized to handle a full load of access points.

The following section contains VPN topology examples from Fortinet vendor (security solutions resold by Alcatel-Lucent).

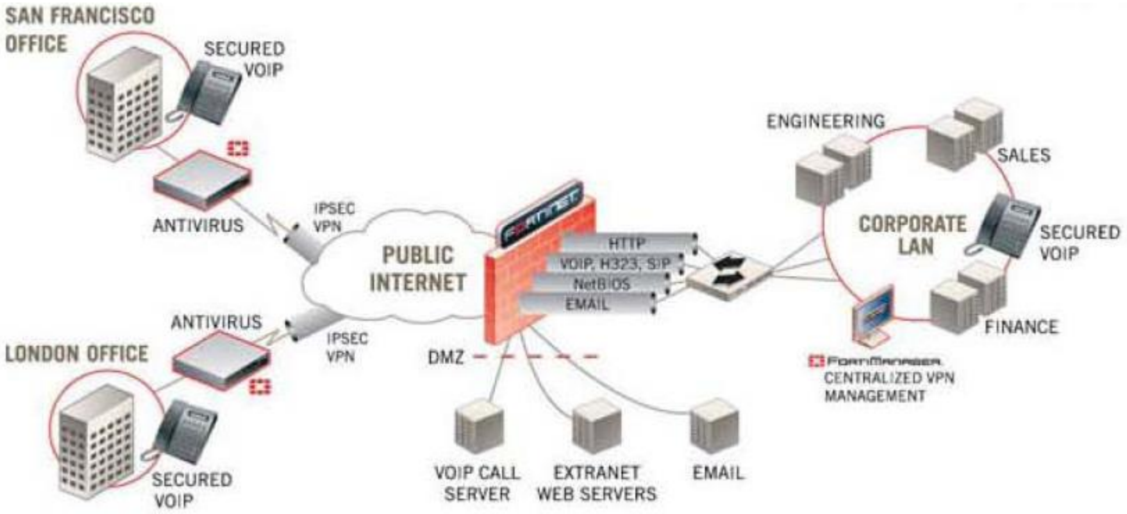
Enterprise Remote Office and partner Extranet VPN

Deployed in parallel with an existing firewall, a FortiGate VPN gateway terminates VPNs from branch offices and extranet partners that require limited access to DMZ servers. With the integrated security features, the administrator can configure granular security policies to control access to resources on the corporate LAN and DMZ.



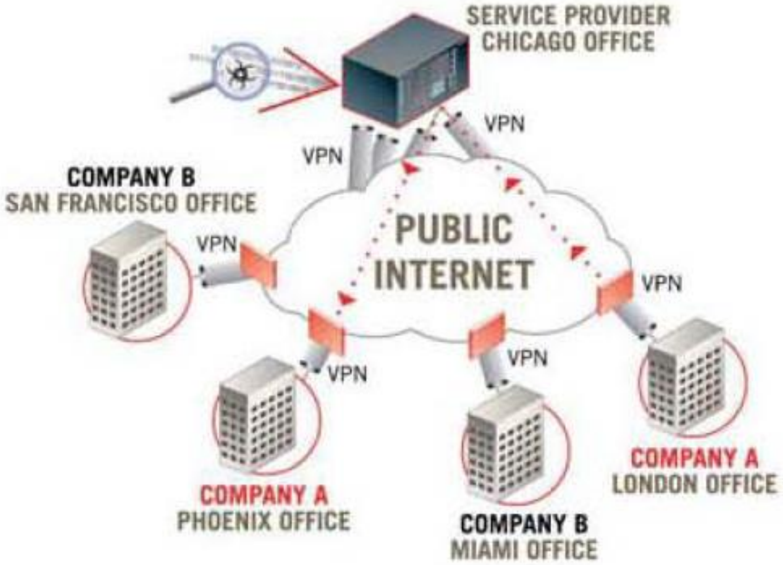
Enterprise Hub-and-Spoke VPN

Hub-and-Spoke VPN configurations allow multiple remote sites to connect together without having dedicated tunnels to each site. An ideal application for this design is to transport VoIP traffic across the VPN's to reduce long-distance toll charges. Traffic shaping features ensure VoIP traffic receives priority even through a VPN tunnel.



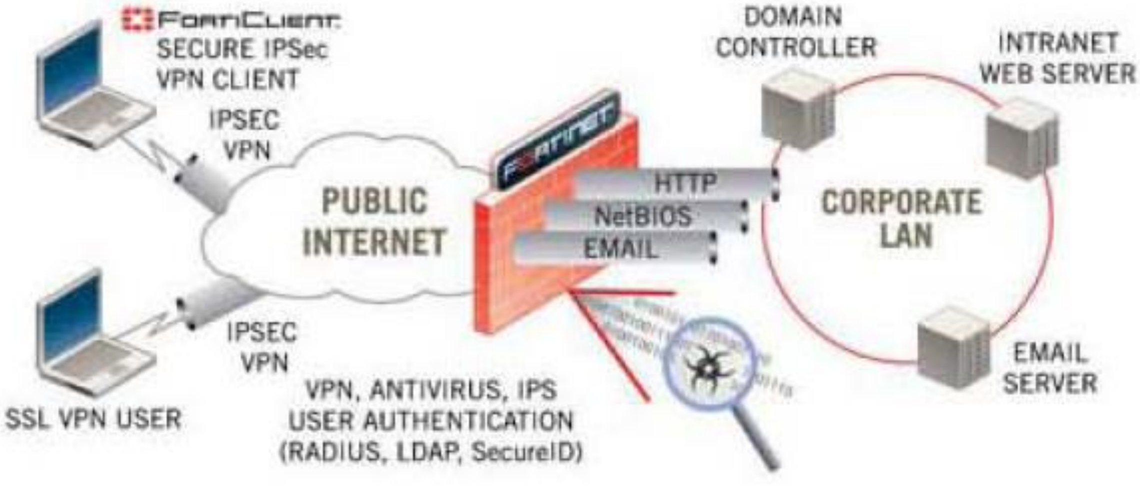
MSSP: Virus-Free managed VPN Service

Taking advantage of integrated antivirus protection, managed service providers can deliver the industry's most secure VPN service by enabling advanced antivirus engine to block incoming and outgoing VPN traffic that contains viruses, worms, trojans, spyware and other malicious content to prevent virus outbreaks from spreading from office to office. As an added benefit, flexible VPN architecture allows for interoperability with most IPSec VPN gateways. Regardless of the VPN CPE the customer has in place, the security system deployed at the core will ensure virus-free VPN traffic.



Enterprise Remote Access (IPSec and SSL)

This solution is ideal for roaming users such as remote sales people needing secure access to resources on the corporate LAN such as email and intranet resources. This topology offers both a secure IPSec client (FortiClient™) and clientless SSL VPN for hotspot access in areas where IPSec may be blocked by a firewall. Strong authentication mechanisms are used to enforce border security (RADIUS, LDAP, SecureID).



10 Mobility Security Approach

10.1 DECT communication security

OmniPCX Enterprise offers all the security levels defined in the DECT standard:

- **Identification**: the minimum and mandatory level based on unique physical number of the DECT.
- **Authentication** (including identification level): using random key, authentication key and standard DECT algorithm.
- **Encryption** of voice and signaling (including authentication level): based on an encryption key calculated during authentication. This level is implemented for both RBS and IBS based stations.

DECT security algorithm is covered by two proprietary algorithms:

- DSAA (DECT Standard Authentication Algorithm) for authentication
- DSC (DECT Standard Cipher) for encryption

User Authentication Key length (bits): 128 bits

Derived Cipher Key Length (bits): 64 bits

Thanks to the IP Touch Security feature of OXE, it is possible to provide end-to-end encryption from a DECT set to an IP Touch set:

- Over the Air with DECT standard based encryption (64bits random key)
- Over the wired network with embedded encryption capabilities of Media Gateway (on which the DECT Base Station is connected) and IP Touch set

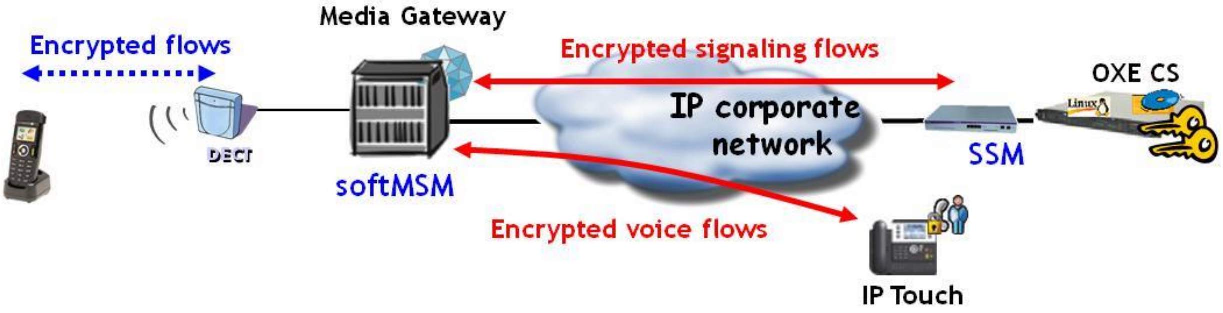


Figure 13: Encryption for DECT technology

10.2 DECT security considerations against potential attacks

All current DECT products (RBS, IBS, 4080 AP and terminals: MR100/200, 300/400/ 8232 DECT) are compliant with the DECT standard.
It means that all ALE DECT equipments are secured by two algorithms:

- DSAA (DECT Standard Authentication Algorithm) for authentication,
- DSC (DECT Standard Cipher) for encryption

These algorithms encompass User Authentication Key length (128 bits) and Derived Cipher Key Length (64 bits)

ALE DECT equipments are not based on proprietary algorithm. Like all other competitors on the enterprise market ALE DECT equipments rely on the DECT Forum and ETSI standard implementation.

According to some reports 20% of attacks were successful in less than 2 hours.
Several points that mitigate this risk:

- DECT communication duration is 10/15 minutes on average, 30min/1hour max, because people prefer fixed phone for long conversation

- Let us assume a long DECT communication with a successful attack, the hacker could be able to intercept the call (after the delay needed to run the attack). However any new communication issued by this same DECT handset will use another key, forbidding the hacker to intercept further calls from the beginning…

- Another mitigating point is the fact that even within the same Base Station several inter-handovers take place regularly between Time Slots for the duration of the call.

- In case of DECT user move, several Base stations may be involved during a single DECT call making the situation much more difficult for a potential hacker (the attack must be launched before the call moves to another TS, or to another Base Station with a different TS.

As a result running a DECT attack on a real customer premise is not an easy thing, even if we agree that a successful DECT attack remains possible statistically…

10.2.1 ALE Recommendations to increase DECT security

1. As all attacks can only be performed inside or close to a building, Physical access restriction must be checked:

    a. The DECT base stations must only cover inside part of the building. No outside coverage, in order to avoid distant attack over the air
    b. Make base station access difficult in the building
    c. Follow generic recommendation explained in the dedicated section (page 80…) of the attached “Secure IP communications design guide”.

2. Thumb rules for DECT user:

    d. Long conversation => use fixed phone
    e. Normal conversation with user move => usee DECT handset

Anyway DECT forum launched working group assembly wih deDECTed.org and ETSI TC DECT to improve the DECT standard security. The first “answer” is the StepA to rectify the security weaknesses. This improvement will release the following features:

- **Registration procedure and time limits for setting of a44 bit:** The base station will not be kept "open for registration" for longer than 120 seconds
- **"Encryption activation FT initiated" (Base & Handset)**: The base station and handset will support encryption activation, and the base will activate it for all calls (including voice calls, List Access sessions, SUOTA/Light data services, etc).

Note: All voice calls must be encrypted

- **On air key allocation (Base & Handset):** The base station will create and allocate a 64 bit authentication key (UAK) when the handset is registered.
- **Authentication of PP (Base & Handset):** The base can authenticate the handset (utilizing its UAK), to ensure it is the genuine handset, and not an intruder or an attempt to imitate the real handset.
  NOTE: the combination of authentication and encryption convey the principle of “mutual authentication”, by which each side is assured that the other side is genuine
- **Evaluation of peer sides behavior regarding encryption including timeout values for triggering of call release:** If the peer behaves differently as expected, e.g. it doesn’t initiate encryption in a timely manner, then the device will assume it is an attempt to breach security and the call will be dropped
- **Early encryption:** Guarantees encryption activation immediately after connection establishment, before any higher layer protocol messages are exchanged (including Caller ID, dialed digits, etc.)
- **Procedure for re-keying with a new derived cipher key during a call:** The cipher key used by the encryption engine is updated at least once per 60 seconds, to foil any attempt to crack the ciphering by brute-force techniques e.g. like super computing

10.3 Voice Over Wireless LAN

Wireless technology has evolved quickly and so providing a higher level of security is gaining importance with the same speed.

WEP

Wired Equivalent Privacy (WEP) is recognized as being a weak security option due to the static nature of the encryption key. Derivation of the key is possible through simple passive scanning techniques and data analysis. To counter this problem, the Wi-Fi Alliance has defined a standard known as WPA. WPA, in reality, is WEP enhanced with TKIP key rotation. This prevents key derivation through passive scanning and brute force attacks. WPA-PSK can be implemented in most infrastructure environments through simple software upgrades, making it a universally available, simple and effective scheme for content protection.

WPA (RC4)

WPA (Wi-Fi Protected Access) is a second generation security standard that solves most of the encryption issues of WEP by utilizing TKIP (Temporal Key Integrity Protocol) to eliminate the weak static key, but WPA/TKIP remains vulnerable to password cracking attacks if users rely on a weak passphrase. WPA embeds an RC4 ciphering algorithm.

2 modes of operation are available with WPA:

- Personal mode that is based on WPA/PSK and requires a PreShared Key to be entered
- Enterprise mode relaying on WPA and 802.1X authentication (PEAP mschapv2, PEAP TLS)

WPA2 (AES)

WPA2, embeds a stronger ciphering technique known as AES (Advanced Encryption Standard.) The greatest advantage of WPA2 over other security schemes is that AES offers a level of encryption which meets the US Federal Government requirements for National Insitute of Standards and Technology (NIST) FIPS-140 certification.

Both “Personal and Enterprise modes are also available with WPA2.

802.11i

the IEEE 802.11i specification has been ratified and applied to all variants of 802.11 technologies. 802.11i specifically focuses on the application of WPA2 (with AES) authentication.

The 802.11i architecture contains the following components: 802.1X for authentication, RSN (Robust Security Network) for keeping track of associations, and AES-based to provide confidentiality, integrity and origin authentication.

Recommendations: Alcatel-Lucent recommends using WPA2 (AES) to cipher VoWLAN with a strong 802.1X authentication (PEAP mschapv2 or TLS).

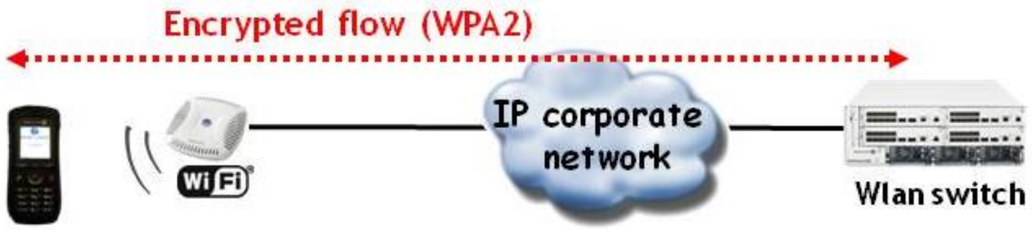


Figure 14: Encryption for VoWLAN technology

Once configured, Encryption (WEP, WPA or preferably WPA2) takes place from the Wireless device through the Access Point, the edge LAN switch, the core LAN switch (within the IP corporate network) and up to the WLAN controller

11 Applications Security Approach

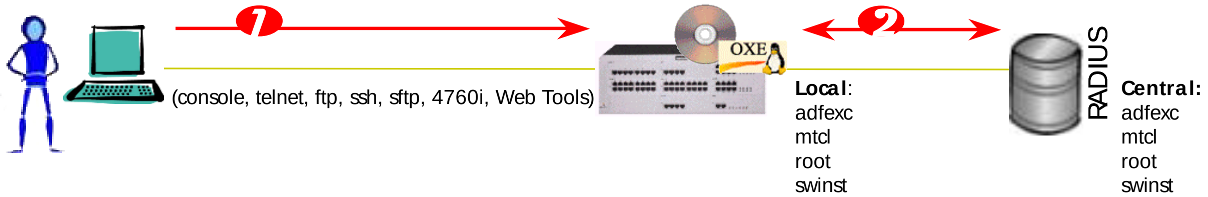
11.1 Secure IP Communications solution Management

11.1.1 Communication Server Authentication

1) External authentication with RADIUS server

To improve the Communication Server security, management accounts can be protected by a strong authentication mechanism based on a Radius server. This process offers the great advantage of centralizing the password database for the full OmniPCX Enterprise network. In that case, specific entries for OmniPCX Enterprise system accounts must be added in RADIUS user database.

This feature is available since OmniPCX Enterprise Rel 7.0.



Corporate identities authentication

As of **OmniPCX Enterprise R7.1**, corporate identities present in RADIUS user database (for instance Jim Smith, Mr Dupont, etc.) can be used for authentication in place of OmniPCX Enterprise system account identities (mtcl, root, swinst, etc.). If the user is authorized to access the system then it is mapped to existing system account (mtcl, swinst, root) . System logs corresponding to user actions contain corporate identity and allow modification traceability. Authorization right and identity mapping are managed at Communication Server level.

2) Two-Factor Authentication

With RADIUS, strong OTP (One Time Password) authentication tools (like RSA password tokens) can be used to increase the security of system management.

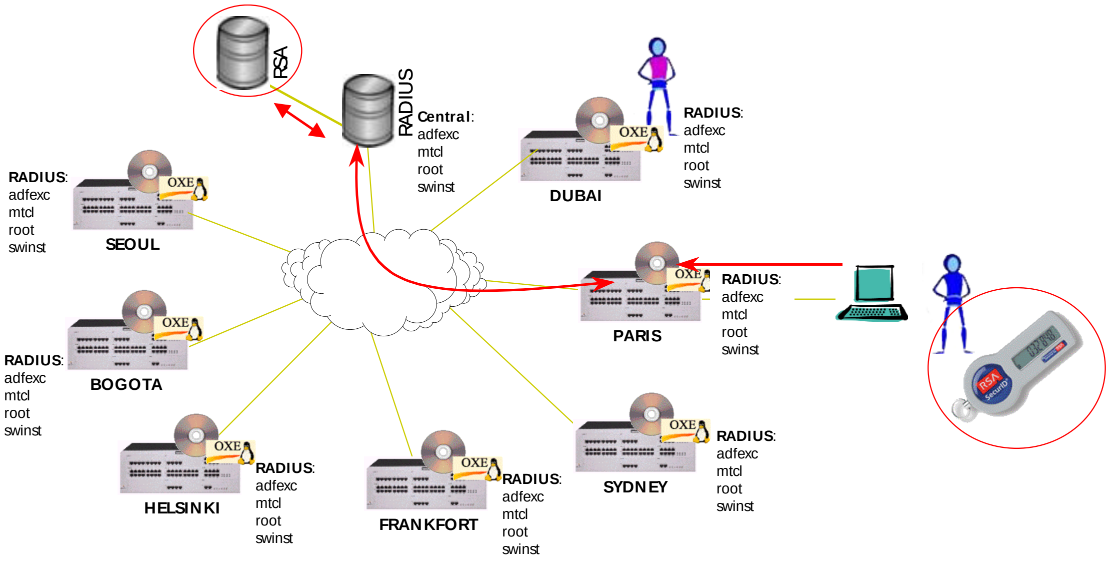


Figure 15: Two-Factor authentication

11.1.2 Omnivista Authentication

A password policy management can be used to secure passwords of defined user accounts (strength and aging). Password policy and password aging is able:

- to check the length of the password (manageable from 2 up to 512)

- to check the content of the password based on trivial user information (name, email etc…)

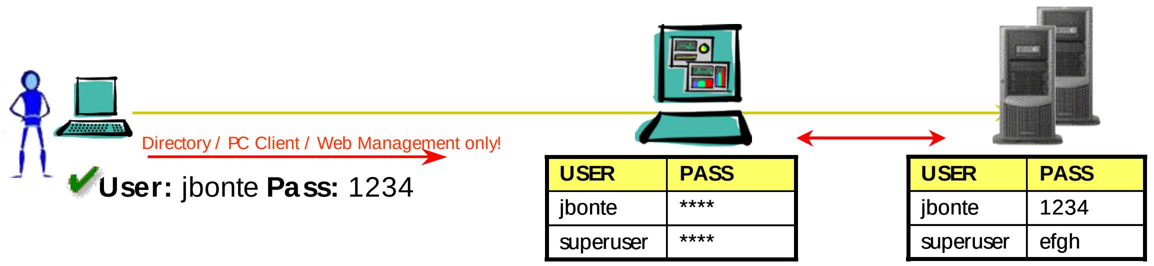
- to check the password expiry (manageable from 1 up to 24855) & also give the message to the user

- to lock the user account when it exceeds the maximum number of login attempts (manageable from 1 up to 32767)

- to set the type of the password encryption

- to store the last {n} password(s) in the history and restrict the usage of last {n} password(s) if needed (manageable from 0 to 24)

Admin accounts on OmniVista management station can have its security level improved with Radius authentication.

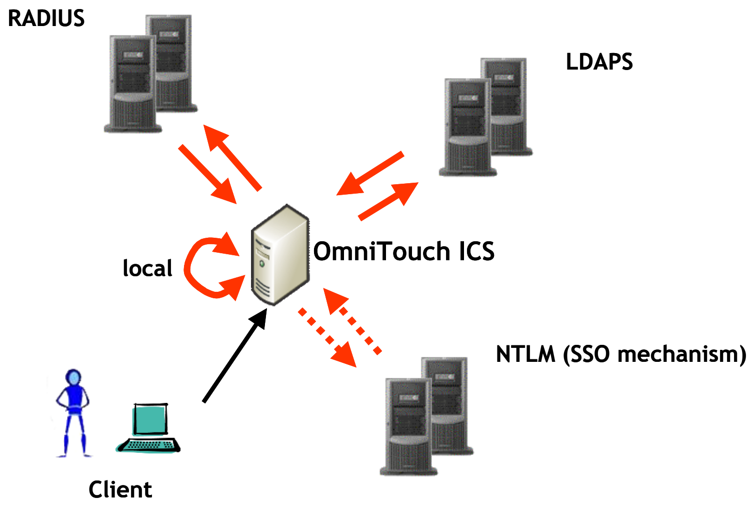


USER	PASS
jbonte	****
superuser	****

USER	PASS
jbonte	1234
superuser	efgh

11.1.3 OmniTouch ICS Authentication

The ICS **administrators** and **end-users (eg. MyIC client)** can be authenticated via an external Radius or LDAP (LDAPS) server. SSO (Single Signed On) mechanism is also available with NTLM Kerberos.



On **Messaging service** of OmniTouch 8400 Instant Communications Suite, the end-user is authenticated using TUI interface when accessing his voicemail box from his phone set. Management of TUI password is performed using following rules:

Minimum TUI password size	. Minimum length required for the TUI password . Possible values are 1-16 . *Default value is 3*
TUI Password history length	. Specify the history length of the TUI password . Possible values are 0-10 . *Default value is 5*
TUI Password Validity Period	. Specify the Validity Period for the users TUI passwords in days . Possible values are 0-365 . *Default value is 0, which means infinite*
Maximum TUI logon failures	. Specify the maximum number of consecutive TUI login failures (wrong password typed) . Possible values are 0-10, with 0 meaning infinite . *Default value is 3*
Locked period after Maximum logon failures reached	. Specify the duration in minutes during which the TUI access to a mailbox is blocked when the maximum TUI logon failures is reached . *Possible values are -1 to 1440 minutes, -1 meaning infinite*

11.1.4 Authorization Management

11.1.4.1 Login / password policies & Role Based management

There are 2 levels of password in the Alcatel-Lucent network management server:

- one linked to the Operating System used by the OmniVista (Microsoft Windows)
- another one for the users of the OmniVista application

When a new user is created in the OmniVista application, an administrator tool checks if the password is composed of 8 characters minimum.

The password security policy allowing users to access to the physical network management machine depends on the Operating System. For example, with Windows NT, it is possible to create the OmniVista host in an NT domain and to apply a password security policy to the domain thanks to the domain server (for instance, a minimum number of characters, a validated period for the password, mandatory minuscule, majuscule letters …).

11.1.4.2 Customized access levels

Customized access levels can be defined for each user. The administrators with the right level of privilege can grant a different access level for each user. This access level can be different for each application, i.e., Mr. Doe has "read" access to the alarms, "modify" access to the reports and no access to the configuration.

11.1.4.3 Predefined access levels

In addition, to simplify the administrator’s task, predefined access levels have been created according to standard profiles, and listed in the Directory:

16 predefined user profiles have been defined and are included within the product:

- 8 user profiles only concern the directory access,
- 8 user profiles define global access levels to the OmniVista applications.

The 8 profiles for global access are:

- Administrators
- Network experts
- Network managers
- Accounting experts
- Accounting managers
- Directory experts
- Simplified management
- Access to the masked information

Simplified management is an intermediary profile allowing non IT managers to add, move or change directory objects. This profile can handle users, hunting groups, and speed dialing attributes. This profile can be tailored to the customer’s needs (managed objects, attributes, etc…).

The profile "Access to the masked information" allows the addition of more information in the accounting reports (telephone numbers, real call costs, PIN, etc.). For further information, refer to the Accounting section. The administrators have access to the masked information.

A user can have several profiles. In this case, access rights are added. For example, an accounting manager can also be a directory expert.

Applications User Profiles	Config.	Alarms	Topo.	PTP/Acc.	Report	Schedul.	Directory	Maint.	Security
Administrator	All	All	All	All	All	All	All	All	Yes
Network expert	Manag. Level 0	Manag.	Manag.	Manag.	Manag.	Manag.	Manag.	OXE	No
Network manager	Manag. Level 1	Clear	Read	No	No	Advance Modify	Read	OXE	No
Accounting expert	No	Read	No	Manag.	Modify	Modify	No	No	No
Accounting manager	No	Read	No	Read	Read	Modify	No	No	No
Directory expert	No	Read	No	No	No	Modify	Read	No	No
Simplified Administration	Manag. Level 10	No	No	No	No	No	No	No	No

11.1.4.4 Predefined accounts

In addition to the predefined access levels for specific people with a password, there are also predefined accounts within OmniVista, which are not specifically granted to everyone but only to a specific type of user (e.g. attendants). These predefined accounts allow OmniVista applications to start immediately, even if, for example, there is no user login and password configured in the directory.

There are 2 predefined accounts:

- **Adminnmc**: in the Administration directory. This is the default access to start the server for the installer. Only the Administrators can view this account. The password is created during the installation and has full administration access.
- **Alcatel-Lucent 4059**: in the Management directory. This is the common account for the attendants using an Alcatel-Lucent 4059 Multimedia Attendant Console, allowing them to have access to the OmniVista directory with no restrictions from their switchboard.

The Management directory can be viewed by anyone with access to the orange list (see Directory chapter), and can be managed by the members of the group **total**: Modification Company, Network Expert and Directory Expert.

The combination of the customized and predefined access levels granted to the people in the directory provides great flexibility and accuracy in security management.

11.1.4.5 Confidentiality of the directory entries

There are 3 levels of confidentiality on directory entries:

- *Green* entries can be viewed by anyone with access to the directory (default value),
- *Orange* entries can be viewed by users with the access level orange,
- *Red* entries are the most confidential ones (e.g., entry of the company's CEO is a red entry which can only be viewed by authorized people).

The **personal** fields can only be viewed or modified by users having the **total** view or modification right. The personal fields are:

- Home phone,
- Home postal address,
- Employee number.

For example, a user can only view your home telephone number if the user has **total** view rights to your entry.

The administrator chooses which fields are displayed or not displayed in the web directory. He can also change the name of the fields according to the organization of the company.

11.1.4.6 Directory user profiles

Predefined users profiles are created as group entries in the company directory. These groups and persons are located in the directories Administration and Managers in the directory tree. Only the administrators can view the administration directory.

There are eight predefined user profiles (or groups) to access the company directory:

- Total modification company (highest level): the user can create/modify/delete all the fields and all the entries in the company directory.
- Partial modification company: the user can modify the non-personal fields of all the entries.
- Total view red list: the user can access all the fields of all the entries.
- Total view orange list: the user can access all the fields of the orange and green entries.
- Total view green list: the user can access all the fields of the green entries.
- Partial view red list: the user can access the non-confidential fields of all the entries.
- Partial view orange list: the user can access the non-confidential fields of the orange and green entries.
- Partial view green list: the user can access the non-confidential fields of the green list.

In addition, there are:

- The **anonymous access** (default), no need to be logged, which is the same as the partial view of the green list, without two fields that are masked: car license and cost center name.
- The **personal access**, which allows the same things as anonymous, plus the view and modification of all the fields of one's own entry, except the fields Employee number, and cost center name which cannot be modified.
- One predefined account concerning the directory application in the Management directory, **Alcatel-Lucent 4059** , which is the common account for the attendants using an Alcatel-Lucent 4059 Multimedia Attendant Console with the rights Total modification company.

A user can belong to several groups, adding rights.

11.1.4.7 Configuration by domain

Large companies with several network managers, multi-company, or organizations with a security/confidentiality policy use configuration by domains. This feature provides specific access rights on a domain to each manager.

On each Domain, a specific manager can have for each object, instance or attribute:

- No access
- Read only
- Read/Modify
- Read/Modify/Create/Delete

Administrators and service providers have the highest access rights and manage the security (access rights).

Up to 32 domains can be created within a sub-network.

A domain related to an OmniPCX Enterprise homogeneous sub-network consists of a set of:

- Users and/or data terminals
- Hunt groups members
- Phonebook entries.

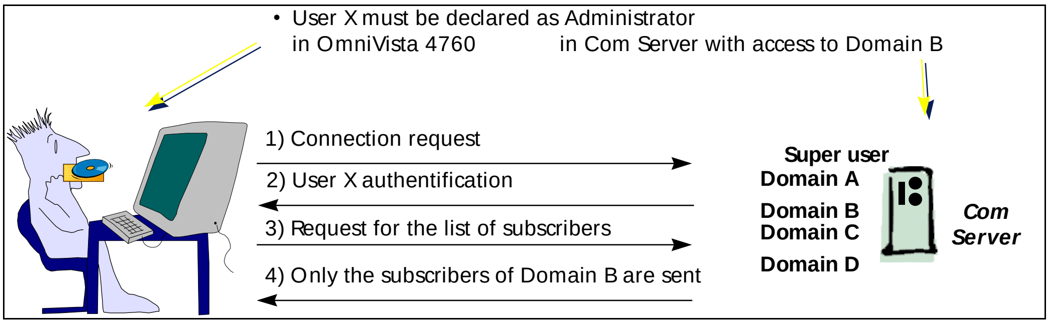
These domains are only related to configuration, and have no link with the other OmniVista applications.

A domain is a homogeneous set of users, for example:

- Manager/assistant must belong to the same domain
- Supervising and supervised sets must belong to the same domain

How does it work?

Example: User X, managing the Domain B, accesses the list of users


• User X must be declared as Administrator
in OmniVista 4760
in Com Server with access to Domain B
1) Connection request
2) User X authentification
3) Request for the list of subscribers
4) Only the subscribers of Domain B are sent
Super user
Domain A
Domain B
Domain C
Domain D
Com Server

Note: The configuration by domain is linked to the OmniPCX Enterprise security software license.

11.1.5 Confidentiality Management

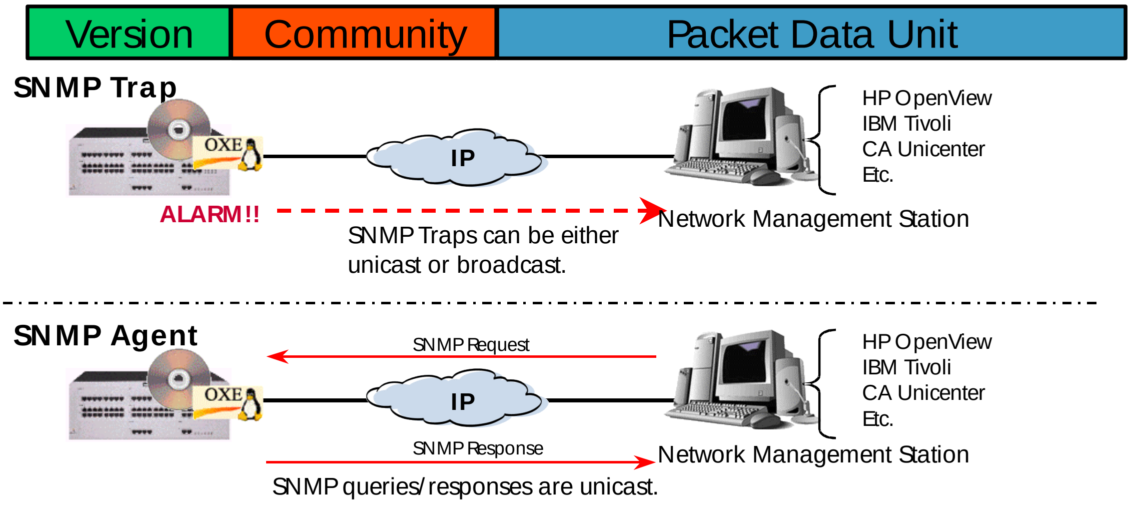
11.1.5.1 Secured SNMP

Simple Network Management Protocol (SNMP) is a protocol which provides configuration, interrogation and alarm notification for managed devices on IP networks.

SNMP protocol has evolved with increased security needs:

- SNMP v1 : Community Name and information are sent in the clear.
- SNMP v2c : Community Name is ciphered, but all information is sent in the clear
- SNMP v3 : Community Name and information are ciphered

SNMP message areas:



11.1.5.2 Secured Shell (SSH)

Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled.

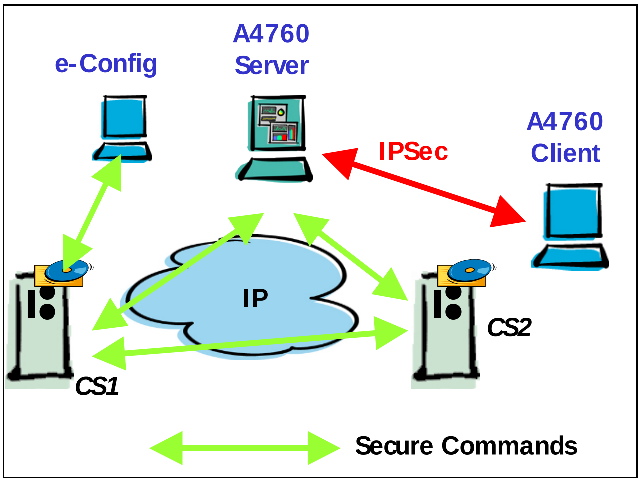
When using ssh's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted; therefore it is almost impossible for an outsider to collect passwords.

Secured SSH/SFTP protocols can be implemented between the **OmniVista Server** and the **OmniPCX Enterprise Communication Server**.

In this case, SSH is used to secure Telnet accesses (OmniPCX Enterprise configuration – technical interface), SSH/SFTP for the file transfers of Accounting and Past Time Performance applications.

In network configuration, with multiple OmniPCX Enterprise Servers, it is possible to mix FTP and SFTP protocols. This secure option offers the encryption of files, data transfers and passwords required during the connection.

Windows® IPSec is used by the Omnivista to secure the exchanges between the OmniVista Server and client(s) for mutual authentication, encryption and a non corruption data mechanism.



11.1.5.3 Secured HTTP (HTTP over SSL)

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

HTTPS is used to perform some operations in **OmniPCX Enterprise** solution:

i. Connecting the Communication Server with a web browser it is possible to download JAR file to install **eConfig** (**4760i**) application on the remote station.

ii. It is also possible to access **Webtool/UMT** application (Unified Maintenance Tool) for maintenance and support purpose of the Communication Server.

When the **OmniMessage 4645** application works in collaboration with OmniTouch ICS solution (Unified Messaging), the **OmniTouch ICS server** can send commands through HTTPS to control the voice mail.

11.1.5.4 Legacy Remote Management & Administration

To secure the remote maintenance & management accesses from the public PSTN network to the **OmniPCX Enterprise**, Alcatel-Lucent uses an interface named RMA or eRMA (embedded on IP Media Gateway-Common hardware), which separates the internal network and the external network in order to authenticate remote users.

Through RMA, the administrator can access the two communication servers (main and standby), as well as the communication server applications.

An automatic call to a remote maintenance center is possible for event alarms. According to the event alarms and configuration, two alarm centers can be called.

The remote access is secured in three ways:

- User authentication based on a login & password
    - 16 logins and managing privileges by login (RMA management right, reset, etc.)
    - After five failed attempts, the RMA is unavailable from the outside during 15 minutes
- Call-back from the RMA system to identify the call origin:
    - The RMA can disconnect, and then dial back to a predefined number.
    - The RMA can ask for the number to dial back, can disconnect and call the remote user back.
- Traceability of actions: whether the connection is set up or not, a history record is created with the date, time, login used, and external number called back.

RMA configuration example to open a "character mode" session:

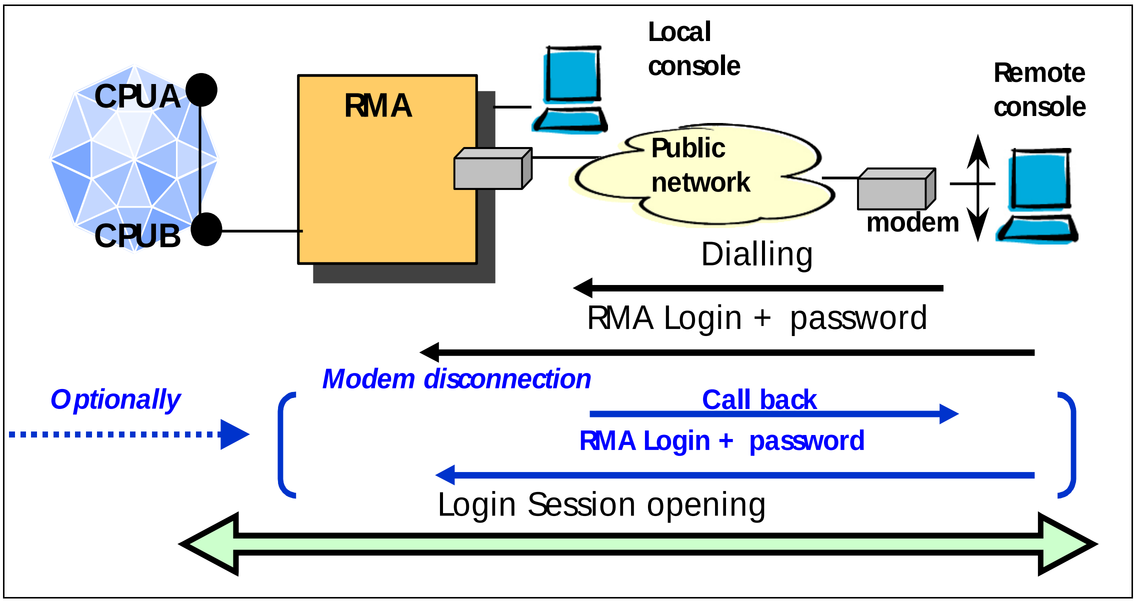


Figure 16: RMA

11.2 Secure Telephony Services

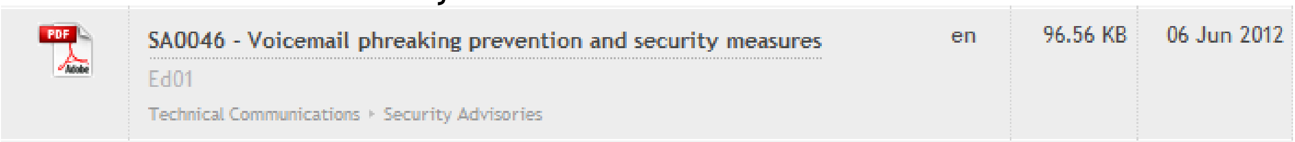
The objective is to protect the telephony system against Toll Fraud.

11.2.1 What is Toll Fraud?

It is a dial-through fraud that can occur when an enterprise's voice system is used by unauthorized people, potentially outside of the enterprise, to make free long distant calls. Toll fraud is a threat that can lead to heavy economical consequences. Historically, the primary target for toll fraud has been larger companies with expensive and powerful telephone systems. Nowadays, it is recognized that smaller or medium enterprises can be also potential targets.

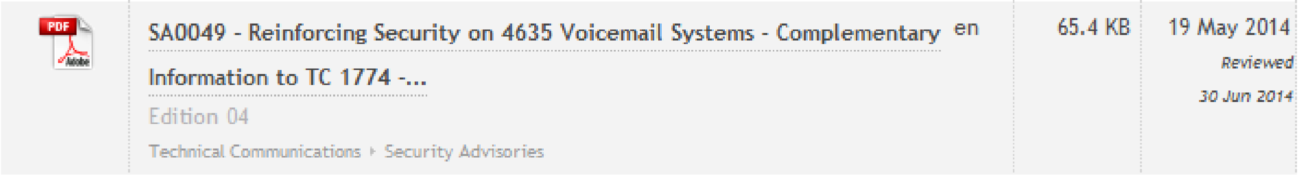
As an example of Toll Fraud alert, Alcatel-Lucent has sent the following Security Advisories/documents related to **Voicemail Fraudulent Use.** These documents are available under the Alcatel-Lucent Enterprise Business Portal (eBP):

- **Alcatel-Lucent Security Advisory No. SA0046: Voicemail Phreaking Prevention and Security Measures**



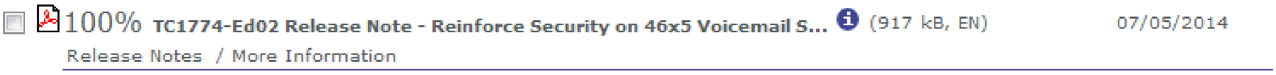
SA0046 - Voicemail phreaking prevention and security measures Ed01 Technical Communications ‣ Security Advisories	en	96.56 KB	06 Jun 2012

- **Alcatel-Lucent Security Advisory No. SA0049: Reinforcing Security on 4635 Voicemail Systems Complementary Information to TC 1774**



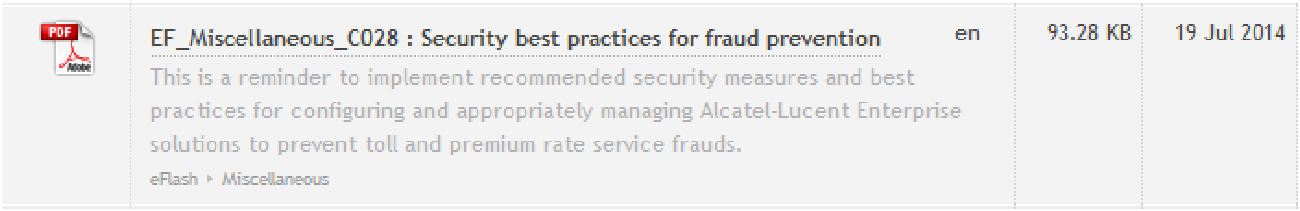
SA0049 - Reinforcing Security on 4635 Voicemail Systems - Complementary Information to TC 1774 -... Edition 04 Technical Communications ‣ Security Advisories	en	65.4 KB	19 May 2014 Reviewed 30 Jun 2014

- **Technical Communication TC1774: Reinforce Security on 46x5 Voicemail System**



□ 100% TC1774-Ed02 Release Note - Reinforce Security on 46x5 Voicemail S... (917 kB, EN) 07/05/2014
Release Notes / More Information

- **E-Flash C028: Toll and Premium Rate Frauds. A reminder on Alcatel-Lucent Enterprise security best practices**



EF_Miscellaneous_C028 : Security best practices for fraud prevention This is a reminder to implement recommended security measures and best practices for configuring and appropriately managing Alcatel-Lucent Enterprise solutions to prevent toll and premium rate service frauds. eFlash ‣ Miscellaneous	en	93.28 KB	19 Jul 2014

Different features are available in the Alcatel-Lucent OmniPCX Enterprise solution to address this protection need.

11.2.2 Transfer Protection

The Alcatel-Lucent OmniPCX Enterprise Communication Server allows an internal user to perform a transfer between two external incoming or outgoing calls (in a standard configuration, this feature is not active). It is possible to restrict transfers to authorized people only. For example, a user may be allowed to transfer an incoming call to an outgoing call, but not between two outgoing calls.

11.2.3 Forwarding Protection

A dedicated COS restriction (barring category) allows forwarded calls to be regulated. Rerouted calls are associated with a specific restriction or barring table. For example, a user may be allowed to make an international call, but is not allowed to forward to an international number or a public cellular number.

11.2.4 Protection on Internal Phones

Internal call control is based on the following features:

- Call COS (class of service) restriction (barring) adapted to the extension
- Speed dialing numbers
- Phone locking when user is away
- PIN code for private calls with/without call restrictions (barring)

11.2.5 External Call Restriction (Barring)

During access to a public or private external line, it is possible for the system to monitor the dialing by the user and authorize the call according to pre-defined rights. The first digits dialed are checked. If the first digits dialed correspond to an authorized number, the number is sent; otherwise, the user receives the busy tone or a voice guide. External numbers up to 20 digits may be analyzed. Each station has four classes of service restrictions, according to the installation state (day, night, forwarding 1, forwarding 2).

The attendant can transfer a trunk to an extension after the user dials the outgoing prefix or outgoing prefix and the country code, so that the user may make outgoing calls to specific destinations on a one-at-a-time basis. The cost of the call is charged to the user.

11.2.6 Restrict access to phone set

When it is setup on the set, a user secret code (Pin code) is requested:

- On external call number dialing,
- On telephone facilities activation/inactivation (e.g. forward, …).

Pin code policy:

After a defined number of consecutive errors on pin code:

- All telephonic features using secret code are denied on this extension,
- On UA set with display: “password forbidden”,
- The substitution (DISA or by extension) on this extension is denied,
- An incident is generated for the extension.

The secret code is "unlocked" by the administrator or after a configurable timer.

The number of error attempts can be 0 to 7, where 0 means there is no control over the number of attempts.

11.2.7 Out Of Service option

The user can put its desk phone in a specific “out of service” state where it will be necessary to enter its extension number and its PIN code to be able to perform any operation. If the user is not physically present in its office, this mechanism ensures that nobody can use the desk phone and spoof user’s identity.

11.2.8 Discrimination calendar for external calls

Calendar for the week is available to forbid the external calls by the entity data: for each day of the week, it is possible to have up to 4 system state changes.

11.2.9 DISA (Direct Inward System Access) Protection

DISA allows the teleworker or mobile worker remote access to internal company communications or telephone services. This can include call cost management features, such as least cost routing or breakout. DISA service must be protected against hackers. The Alcatel-Lucent OmniPCX Enterprise Communication Server offers two levels of protection:

1) Password control
2) Caller line identification with automatic substitution

11.2.9.1 Password Control

In a standard configuration, the Alcatel-Lucent OmniPCX Enterprise Communication Server offers a password control feature. If an incorrect password is entered (three attempts per call), the Alcatel-Lucent OmniPCX Enterprise Communication Server stops the call and locks access for a temporary programmable time (five minutes minimum). Repeated attempts during the locked period will double the delay through an iterative mechanism without limit. The Alcatel-Lucent OmniPCX Enterprise Communication Server generates alarms in real time according to each event. DISA access can be unlocked:

- After the temporary period
- By dialing a prefix number from a phone with specific rights

11.2.9.2 Caller Line Identification

The Alcatel-Lucent OmniPCX Enterprise Communication Server identifies the caller line or device by analyzing the CLIP provided by ISDN, cellular, or other public network features. If the line or device is authorized, the caller may be automatically substituted for the office phone.

11.2.10 Monitoring with OmniVista of the telephony services usage

In addition to those mechanisms used to prevent from fraudulent usage of the telephony services of the system, there are some means of usage monitoring of the OXE services in general thanks to the OmniVista management platform and more specifically with the objective of detecting abnormal usage. The mechanisms available in the OmniVista are described here below:

- **Secure remote administration**
  - SSH, HTTPS, SNMP v3, IPSEC (between client and server)

- **Manage profiles and rights for administrators**
  - RBAC (Role Based Access Control)

- **Configure a « real time » monitoring**
  - Daily or Monthly
  - Per user, cost center, trunk etc...

- **Configure automatic alarms generation**
  - if costs, length, or number of calls thresholds are exceeded
  - Automatic sending of alarms to the administrators by email

- **Use Monitoring Reports**
  - Reports on Monitoring (threshold crossing detection) for DISA use, traffic peaks, accounting reports on cost variation

Recommendations & Best Practices

12 Alcatel-Lucent Recommendations

Security is a critically important aspect of any modern network. The addition of telephony services to an existing IP network has implications which must be carefully considered for the benefit of both the network and the voice application. For this reason, you will find below Alcatel-Lucent's advices for the secure VoIP implementation practices.

These recommendations can be viewed as complementary and supplementary to existing security policies already defined by/for an enterprise. In no way does Alcatel-Lucent state that the following recommendations are in any way obligatory for proper OmniPCX Enterprise installation, but rather highly recommends their consideration for any VoIP project.

IP (Internet Protocol) has improved the efficiency and revenue generating capability of many companies by enabling e-business applications. For the most part, these applications require highly reliable networks that accommodate real-time traffic transactions. They must be scalable in order to support increasing numbers of applications and users and they must be resistant to a wide array of potential threats.

To combat a plethora of malicious threats and to ensure that the customer applications are not compromised; security technology must play a major role in today's network designs.

The first step to developing a secure network is the development of strong security policies that can be used to ensure the following:

1. Only secured devices are connected to the network.
    a. PC Servers must be configured and well protected before they are allowed to interact with other entities attached to the network.
    b. Network clients must be configured so as to mitigate their potential role in attack strategies.
2. The networking environment should present strong authentication, containment, isolation and attack prevention/resilience capabilities.
3. Management systems should be aggressively protected and controlled.
4. Client interactions should be protected to a level equivalent to sensitivity and importance of the media they manage (the more sensitive the voice/data, the more aggressive the measure of protection).

Why must the infrastructure be secured for voice?

Without a focused security effort, any part of any network can become susceptible to attack or unauthorized activity. Routers, switches and IP hosts can be violated by external hackers or internal employees. To determine the best ways to protect a Voice over IP project hosted on a customer network, the Design Engineer must understand the various types of the technologies and strategies that can be used to mitigate attacks.

This chapter is written to provide a description of the steps and recommendations a Design Engineer should take into consideration in order to ensure a highly secure network infrastructure for Voice over IP projects.

12.1 General Security Best Practices

As for any internal resource on the LAN, Alcatel-Lucent requires to be protected from any external networks and public Internet via appropriate deployment schemes and with the help of security border equipments (e.g. SBC, Reverse Proxy, Firewall, etc.) that are able to prevent from external threats.

First security best practice is <u>not to expose</u> OmniPCX Enterprise solution or any other A-LE solution directly to the Internet without these security equipments.

In addition to the below described equipments, it is strongly recommended to place appropriately firewall systems which are able to prevent from possible internal attacks (and network scanning attempts) against servers and equipments provided by A-LE and installed in the customer's network.
Firewall provides valuable alert systems for administrators when detecting unexpected or suspicious traffic both inbound and outbound.

12.2 Physical Infrastructure Security

Physical access restriction is a fundamental and essential aspect of any complete security policy. Protecting mission critical equipment, such as PBX resources, to maintain their availability is the primary mission of a security policy. Locating the PBX equipment in locked rooms and/or locked cabinets helps to defend against the most simple and effective Denial of Service attacks conceivable, the manually disconnection of servers/gateways from power and LAN receptacles.

It is important to note that many cabinet enclosures from Alcatel-Lucent incorporate locking facilities (PSC, M1, M2 and M3.) Whenever locking cabinets are not supplied as part of Alcatel-Lucent's product offer (as is the case for RM1, RM3, VH and WM1), it is advisable to specify third-party sourced 19" racking systems to secure PCX components.

A locked door is only the first step in a sound Physical Security posture. While a locked cabinet can protect a PCX from most casual low-tech attacks, the possibility still exists that a particularly intent aggressor will be able to overcome or circumvent physical boundaries and gain direct access to critical components. Natural disaster (fire, flood, etc.) can also present total facility outages that cannot often be overcome by a simple padlock. This makes spatial redundancy (incorporating more than one physical location) an additional essential aspect of physical security.

Design Recommendations: Physical Security

To ensure the best possible resilience to physical threats, Alcatel-Lucent recommends:

- Communication Servers, IP Media Gateways and all other telephony components should be housed in secured processing environments with adequate physical access restrictions. Whenever possible, locking cabinets/enclosures should be employed (and utilized) to further restrict physical access.
- Communication Servers, IP Media Gateways and all other telephony components should be provided ample backup power facilities. (this applies to their data network resources as well)
- Whenever possible, Communications Servers and other telephony components should be made redundant. For optimal protection, redundant components should be placed in geographically separated locations.

Implementation Recommendations: Physical Security

- If at all possible, avoid attaching redundant components to the same network infrastructure. Having redundant Communication Servers is of little value if they are all attached to one common data center Ethernet switch or one PSU.

12.3 Network Logical Segmentation (VLAN)

The common network infrastructure has tremendous potential for increased efficiency and cost reduction. It also carries the potential for greatly increased accessibility. This can be a positive and/or a negative aspect, depending on your frame or reference. Carelessly mixing different types of network traffic can be dangerous. For Quality of Service, ease of management and security reasons; voice and data traffic should be logically separated whenever possible.

Although traffic can be prioritized via 802.1p and PBR (policy based routing) techniques without actually separating the traffic into multiple broadcast domains (VLANs); it is far easier and less complex to develop, deploy and manage QoS schemes that use traffic segmentation.

From a security perspective, separating traffic into differing Ethernet broadcast domains provides for better DoS resilience and allows for the establishment of strong boundary security practices. Boundary controls can be as simple as switch/router based ACL (access control lists) or far more complex solutions based on dedicated hardware appliances (intrusion detection, packet inspection, VPNs, etc.) In either case, logical traffic separation is the key that allows boundary security to be effective.

One of the most significant threats to VoIP is the DoS attack. VoIP systems are not often the direct target of DoS attacks as the hardened nature of such platforms and terminals makes them difficult to infect. Absolute reliance on the IP network however, makes VoIP systems highly susceptible as direct targets. For this reason it becomes very important to separate real-time traffic from non-real-time traffic by using the following methods:

- **Dedicated Switch Ports:**
  - Access ports of Ethernet switching gear can be dedicated to a specific IP broadcast domain (IP subnet) dedicated to specific functions/hosts. This type of configuration is typical in consolidated communication processing centers (data centers or computer rooms) as only one device is connected to an Ethernet switch port.
- **Dynamic VLAN:**
  - Most IP terminals support 802.1q tagging, meaning that all traffic originating from the IP phone is tagged with and 802.1q header allowing the voice traffic to be separated from other traffic types and placed into dedicated and isolated IP broadcast domains.
  - Many Ethernet switches also have the ability to identify traffic based on MAC addresses or other unique characteristics. In this way, Alcatel-Lucent IP phones could be identified by their MAC mask (00:80:9F:xx:xx:xx) and automatically isolated from other LAN traffic.

In a modern switched data network environment, VoIP flows can and should be separated from the data flows through the use of Virtual Local Area Network (VLAN) schemes that allow for the creation of logical layer-2 IP broadcast domains. This allows for the logical separation of traffic without the need of independent network switching equipment and topologies. This logical separation protects VoIP traffic sources from excessive traffic typical of most network attacks, and isolates VoIP interfaces from much malicious activity.

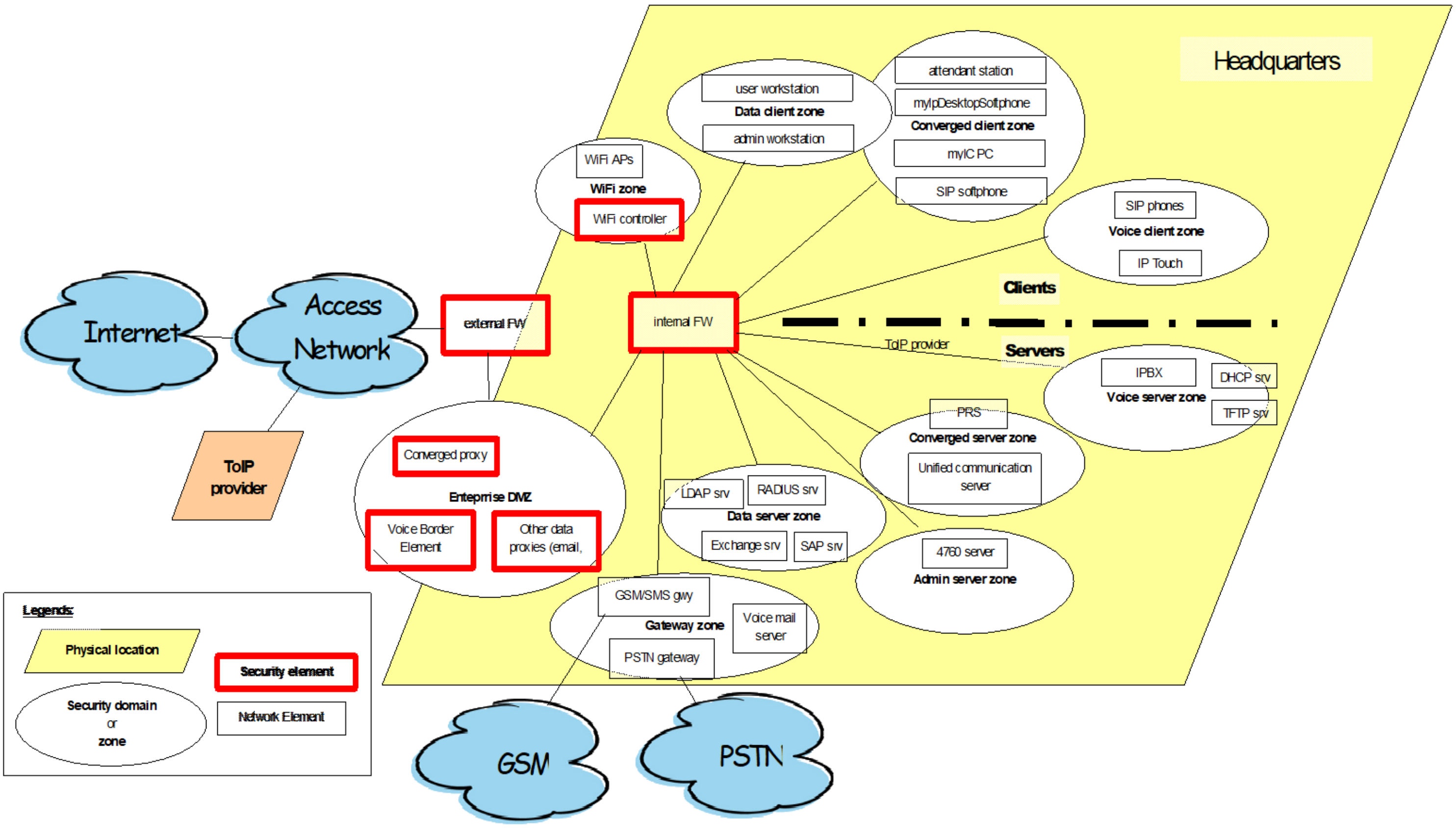
In most cases, network segmentation is a standard component of established network security policy. Most network administrators concerned with security will have clearly defined rules on how traffic can and cannot be mixed. It is imperative that the introduction of a VoIP system does not violate these guidelines.

As with people and fingerprints, different networks often employ different configurations:

- Dedicated Port: In some networks, IP phones can be connected to a dedicated Ethernet switch ports. This eliminates much complexity in the network, but is very expensive as it effectively doubles the number of client access ports required (if PCs are also used by network users.) VLAN tagging from IP phone is not necessary in this model.

- Policy Switching: Some modern Ethernet switching platforms posses the ability to monitor and analyze network clients and the traffic they generate. Information gathered eluded
- MAC VLAN
- DHCP VLAN
- Traffic VLAN
- When a PC is connected behind an IP phone (on the same switch port), the VLAN policy of VoIP interfaces should be configured by MAC address (e.g. see OmniStack/OmniSwitch products). In this way, the default VLAN (so called native VLAN) of the switch is applied to the PC. Explicit VLAN tagging from IP Phone is not necessary.
- If the Switch is not able to use VLAN by MAC address (Vendor Identification), the IP phone must explicitly tag and use IEEE 802.1q (DHCP, TFTP, signaling and voice are tagged) and the default VLAN value for the frames sent by the PC is dynamically assigned by the switch. The explicit tag is managed from the IP Phone.

Example of VLAN segmentation for VoIP by IP components:



Each zone represented in this illustration shall be considered as one or several Vlans. In terms of end-user network equipment, it is important to distinguish:

- data users, that should not be able to communicate with VoIP servers
- voice users, meaning using IP phones, that are allowed to communicate with VoIP servers in order to establish calls over the corporate network
- converged/multimedia users, who are using a softphone or a client running on a PC along with other data applications (mail, web browser). Those users should be isolated from voice users and inter-VLANs filtering rules carefully managed. If applicable, a proxy component for softphone applications (based on SIP) can be installed to provide signaling connections control and filtering and media anchoring.

To simplify the VLAN management, Alcatel-Lucent has implemented a mechanism to affect automatically the voice VLAN to IP Phones: Automatic VLAN Assignment. This mechanism is based on double DHCP request.

Design Recommendations: Traffic segmentation and filtering

In addition to this VLAN segmentation, and if information exchanges are necessary between the different logical networks, a security policy should be deployed to control the flows between VLANs using **Access Control List**. This security policy can be based on addresses end-users and IP flows used by these end-users or VLAN identities. **Firewall** equipments can be deploy to manage those filtering rules between VLANs and ensure that only allowed network elements can communicate with sensitive voice servers. **Proxy** component can be installed specifically for softphone applications based on SIP protocol for call control. Some of these Proxy Softphone also support TLS and SRTP for secure calls to softphones.

12.4 Network Traffic Filtering / Inspection

Traffic Filtering and Inspection are tasks essentially devoted to a **Firewall** that is able to perform different levels of analysis, according to the selected model and type. Other equipments like routers are able to provide traffic filtering between IP sub networks.

A Firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

Firewalling mainly observes the following rule: "Everything is forbidden, except what is expressly authorized". Some applications like VoIP require opening some specific TCP and UDP ports. Whatever the Firewall type is, filtering always uses an Access Control List.

The Access Control List (ACL) is a process to test packets crossing the network and that is able to determine whether these packets must be forwarded to their destination or simply discarded. An ACL can check different parameters like source and/or destination IP address, source and/or, destination TCP/UDP port, specific protocol, etc.).

Firewall can also implement ALGs (Application Layer Gateways). An ALG controls protocol conformance to avoid any kind of fuzzing attack and can also be used to perform packet manipulation (for NAT or dynamic pinholing operation). It applies security mechanisms to specific protocols like FTP or HTTP. ALGs can also be implemented for VoIP specific protocols like H323, SIP, CSTA.

Design Recommendations:

For Filtering/Inspection Alcatel-Lucent recommends:

- Using a "stateful inspection" and "VoIP aware" firewall that is compatible with OmniPCX Enterprise environment.

- Enforcing the Access-control by an Access Control List to limit access between Voice and Data VLAN and hence avoiding DoS attack propagation coming from the Data network.

Implementation Recommendations:

Firewall and ACL implementations and topology choices are part of the customer security strategy and remains under his responsibility.

12.5 Private Addressing and NAT

Implementing Network Address Translation (NAT) or Network Address Port Translation (NAPT) allows the communication between a private Network (non-Internet routable private IP addressing plan) and the public network (Internet routable addresses).

The NAT/NAPT scheme brings some additional part of Security in hiding the Private Network from Internet. When packets need to cross the domain boundary (NAT router), some modifications must be done on packet headers in order to reflect the temporary association (source IP, destination IP, and port number). However while this process is fully applicable for data, it is not the same story for Voice over IP. Some applications carry addressing information inside their payload (e.g. H.323, SIP, etc.) and that is also the case for VoIP. For instance UDP ports of the H.245 sessions contained in the IP payload cannot easily be interpreted by a generic NAPT router. As a result, UDP session synchronization is lost.

In most cases, VoIP does not work when a NAT/NPAT router is installed between VoIP components.

Design Recommendations:

When there is a pre-existing NAT/NPAT router in the network, Alcatel-Lucent recommends:

- Bypassing the NAT/NPAT router for all VoIP traffics.
- Use a bridged VPN Tunnel function through WAN.
- The **Remote AP solution** can be installed to allow connectivity over the Internet with an IP phone or Wifi phone used at home by a teleworker.
- For remote SIP users (hardphone and softphone), a solution based on a **SBC** (Session Border Controller) can be proposed to address NAT issues.

12.6 Infrastructure Services Integration

As communications networks have evolved, so has the intelligence of malicious code authors. The game of “IT Security” is full of leaps in technological sophistication by both network owners and attackers.

In the early days of virus and worm creation, the ultimate goal was the compromise of information on mainframes and/or personal workstations. Operating system suppliers, software vendors and network administrators responded to these threats by making it far more difficult for such attacks to be successful. This led to a reduction of attacks for information collection and a rapid increase in Denial of Service attacks.

In keeping with the theme of leaps in technological sophistication and shifts in attacker focus. Malicious code authors and network attackers are often considered opportunists and lazy. They often carefully assess the landscape of a target network(s) in order to determine how the most amount of damage can be inflicted with the least amount of effort. A pattern that has appeared in their work over the last few years is a strong trend towards the targeting of network infrastructure elements that are poorly protected, can be easily overpowered and provide some critical service to the network at large. Amongst these new targets are VPN Gateways, Core IP Routers, Print Spoolers/Servers, Database Systems and DHCP resources. The elimination or degradation of any of these infrastructure services can disable or seriously handicap an otherwise healthy network.

With the above mentioned changes in attack behavior, network administrators have become increasingly sensitive to the configuration of protections provided to infrastructure services. Enterprise Security Policy documents now routinely include sections that define how infrastructure services can and cannot be used and how new services may or may not be introduced to the network. Requiring additional DHCP and TFTP servers to be added to the network, with the associated adjustments to router configurations to accommodate discovery and forwarding, is no longer considered an acceptable practice.

While the **OmniPCX Enterprise** has the ability to host DHCP and TFTP services for IP telephony instruments and media gateways, use of these embedded services is not recommended in secure environments. Alcatel-Lucent’s OmniPCX Enterprise solution can, and should, be deployed in a manner that takes advantage of existing network infrastructure services and the redundancies and protections already given to them.

Design Recommendations: Infrastructure Service Integration to ensure the best possible resilience to DoS threats to infrastructure services, Alcatel-Lucent recommends:

- The ability of existing DHCP Server equipment to utilize “Vendor Specific Attributes” should be verified in order to supply Alcatel-Lucent IP phones with adequate and full configuration information and to ensure that schemes such as AVA (automatic VLAN assignment) are viable.
- The ability of existing TFTP Server equipment to receive and host BINARY and CONFIG file uploads from the OmniPCX Enterprise Communication Server should be verified in order to ensure transparent operation with the OmniPCX Enterprise.
- Use of existing DHCP and TFTP infrastructure services for voice related activity elevates the need for redundancy and attack resilience. Network administrators should be informed of this requirement in order to evaluate whether or not additional protections are required.

Implementation Recommendations: Infrastructure Service Integration to maximize system security:

- Network routers and ACL filtering points should control DHCP and TFTP requests to the Communication Server to eliminate ‘saturation’ style attacks.
- AVA services should be configured on existing DHCP Servers in compliance with the guidelines defined in the Alcatel-Lucent ‘Automatic VLAN Assignment – PreSales Communication.’

12.7 Authentication Framework

Common Authentication Elements

When asked, most network users agree that one of the most difficult issues that they are forced to contend with on a daily basis is Identity/Credential Management. It is not uncommon for a modern user to require username and password combinations for more than a dozen independent systems. (Network logins, VPN accounts, Proxy Server accesses, etc.)

While originally intended to increase system security, the challenge of maintaining so many independent username-password combinations often leads network users to take simplification matters into their own hands. They will:

- Write the long list of usernames and passwords on sticky notes attached to their PC.
- Try to use very simple passwords (dog's name, mother's birthday, etc.)
- Attempt to manually change all passwords to the same phrase, regardless of differences in system sensitivity.

Obviously, writing the passwords down on little yellow sticky notes is a huge security weakness.

The use of very simple passwords is one of the most serious threats that network administrators face. In spite of all other efforts made to protect the network and its population, poor password selection can provide intruders and network attackers with ample resources to circumvent many layers of network security.

Along the same line as threats posed by simple passwords, is the threat presented by the use of the same password for systems of varying levels of sensitivity. Allowing a user to use the same password for business critical systems as is being used for minimum security WEB applications can also be an open invitation for disaster. How many times have you read/heard about an internet user who lost thousands of dollars because a "hacker" was able to login to his/her bank account and transfer money? The details are usually similar. The user signed-up for a new online service (eGretting Cards, Photo Sharing, Online Auction, etc) and used the same username and password as they do for their bank. The "hacker" didn't need to break the bank security; rather they just needed to break the security of a simple online FREE eGreeting Card or WebMail server.

To eliminate most of these threats, network administrators have turned to dedicated authentication servers. These elements and protocols aim to simplify the authentication demands for users as well as provide an enforcement point for network password policy. At the core of these systems are Microsoft NTLM, RADIUS, TACACS and LDAP server technologies. When used correctly, these systems can offer:

- granular controls of when and where users are allowed to access to network systems
- an authentication aggregation point to reduce the number of passwords a user must remember and simplifying password administration.

A viable and versatile authentication strategy involves detailed plans for integration at all layers of the network. To be effective, the strategy must be very flexible, yet offer strong enforcement capability. In most cases, this results in a strategy that involves at least two authentication server elements – Microsoft NTLM and RADIUS. These two architectures can work well together. A bulk of network access authentication (dial-up, 802.1X for wired and wireless clients, VPN, etc.) can be performed via RADIUS processes that are tightly linked to Microsoft NTLM, which can authenticate server and application access requests in the native Microsoft environment.

More important than the actual authentication processes, however, are the network policies that govern their use. It is imperative to have sound, logical policies and rules that provide adequate business process protection. Policies that are easily bypassed and/or make little business sense are easily ignored.

Design Recommendations: Authentication Infrastructure Integration

To ensure ease of use and management while also maintaining the highest possible level of network security, Alcatel-Lucent recommends that:

- Network designs should utilize common network authentication server elements for all voice and data traffic. The same RADIUS Servers that authenticate remote VPN access requests, dial-up access requests, etc. should also be used to perform 802.1X authentication of IP Phones and other endpoints.
- It is important that ALL elements of the network participate in a structured authentication scheme. IP telephones, PC clients, wireless clients and all other endpoints MUST participate. In most cases, this means that all clients must support 802.1X authentication, and the network infrastructure must be capable of authenticating multiple 802.1X requests per Ethernet switch port.

(It is of little good to force PC workstations to authenticate if IP telephones are not held to the same standard. A malicious user need only spoof the identity of an IP phone in order to gain access to sensitive network resources.)

- Proposed authentication systems must include necessary redundancies in order to prevent their potential use in Denial of Service attacks.

(If only one RADIUS Server is used within a network design; it becomes a single point of failure that, if interrupted, could cause massive outages throughout the network.

- Multi-site designs should include local authentication resources, or backup authentication resources, at each location to prevent simple WAN outages from significantly affecting telephony system operation.

Implementation Recommendations: Authentication Infrastructure Integration

- If at all possible, avoid attaching redundant components to common network infrastructure. Having redundant RADIUS Servers if of little value if they are all attached to a common data center Ethernet switch that has failed.

Strong Authentication Options

In some business/government environments, static text passwords are not considered sufficient. This is due to the theory that any password that does not change frequently provides a window of opportunity for forced or analytical derivation. The primary method of increasing authentication security is through the use of Two Factor Authentication (T-FA), of using both a password and an additional element (something else you know or have, like a PIN code or fingerprint) to complete the identity validation process. Several T-FA schemes have become very popular in the financial and government sectors, and are quickly being adopted by commercial enterprise; Asymmetrical Certificates schemes, One Time Password solutions and Token systems.

The most commonly used method is the Token system. Token systems can operate in multiple ways, leveraging biometric data (fingerprints), keypads with PIN codes, and/or time sensitive and synchronized password rotations. What makes Token systems effective in high-security applications is the fact that the user “password” is never the same twice, and some critical factors of the authentication process (PIN code, fingerprint, etc.) are never sent over the network at all.

While some applications and products support direct linkage to Token system authentication servers, direct connection are not always necessary. Most RADIUS Server offerings have the ability to tightly integrate with Token system authentication servers, acting as a kind of middleware for strong authentication. Any application or product that can use RADIUS authentication capabilities can benefit from strong Two Factor authentication via a Token system. In most cases, this configuration offers the most flexibility and allows some sessions to be authenticated via Token while allowing others to utilize simple password authentication. This is especially important when a single authentication infrastructure is wanted for users requiring strong authentication options, as well as automated systems – which often cannot use Two Factor authentication.

It becomes very important to know which applications can, and which applications cannot, use Token authentication and what limitations may exist. It is often best to choose strong authentication whenever possible. So, when is Two Factor Authentication not possible?

- **When the authentication is conducted as part of automated processes.** Systems management platforms, such as OmniVista for example, connect to PBX systems every few minutes to retrieve status information and carry out scheduled functions. Since these connections are automatic, and the management application has no way of interacting with a security Token, there is no way to leverage strong authentication.
- **When constant and rapid re-authentication is critical for operation.** Some applications, such as Voice over Wireless LAN, require the authentication process to repeat at very frequent intervals. The interruptions to normal telephony use presented by a constant need to re-authenticate every time a Wi-Fi terminal subscriber roamed from one Access Point to another would make the system unusable.
- **When the account must be accessible by more than one person.** Shared accounts pose special challenges and require special consideration. Some systems require a very specific account for administration and maintenance. This account is often known to more than one person, making Token authentication very difficult as linking multiple Token identities to a single account is either impossible or not advisable in most Token systems.

Design Recommendations: Strong Authentication

To ensure enhanced network and telephony application security through strong authentication, Alcatel-Lucent recommends the following:

- Two-Factor Authentication should be used wherever possible when such solutions and policies for use exist within a customer network. Due to deployment complexity, however, it is seldom advisable to propose a Token system solely for use with an IP Telephony system.
- It is important to clearly define where Two-Factor Authentication can and should be used (system administration, OmniVista administrative access, OmniTouch ICS administration & user access, etc.) and where it cannot and should not be used (automated 4760 accesses, 802.1X terminal authentication, user PIN code validation, etc.)

Implementation Recommendations: Strong Authentication

- It is critical for system reliability that RADIUS and Token Authentication Server elements have sufficient redundancies to ensure availability.
- Multi-site designs should include local authentication resources, backup authentication resources, or backup On-Demand Network links for each location to prevent simple WAN outages from significantly affecting telephony system operation by cutting off access to authentication servers.

Application Authentication

The previous sections have focused on Network Access Controls and authentication infrastructure, but it is also very important to consider the value and importance of strong application authentication and the viability of Single Sign-On solutions.

Logic dictates, that having a single password to manage all access requests is a bad thing. If that one password is ever compromised, then so is access to all the applications using the same password. Several passwords are commonly considered a good thing – but only to a point. Being required to remember too many passwords leads users to utilize password lists, or password over-simplification practices, or some other violation of password integrity and strength. It is, therefore, important to strike a balance between too-few and too-many.

Many network administrators group applications into three or four classifications that run the range from minimal risk to very-very-very high risk. For the most part, applications that exist within the same general class of risk can often be linked in order to grant access based on a single authentication request or Single Sign-On (SSO). An example of SSO is a single authentication request for a PC client that grants access to the physical network (802.1X), access to the Microsoft/Linux/Novell network domains, and several other applications such as Internet Proxy services and Instant Messaging clients.

Some applications should always be considered individually critical and require a separate authentication request and/or a separate set of user credentials. For many companies, email and access to online Human Resources applications fall into this category.

The choice of which applications share or do not share authentication credentials should be left, whenever possible, to the customer. Applications should, whenever possible, have the ability to support common account authentication and/or Single Sign-On.

<u>Design Recommendations</u>: Application Authentication

To ensure enhanced telephony application security through strong and coordinated authentication, Alcatel-Lucent recommends the following:

- Telephony applications should be clearly grouped by 'level of risk' for alignment in authentication services.
- It is highly recommended that management applications (OmniVista, OmniTouch ICS administration accounts) do not participate in Single Sign-On operations.

IP Phone Authentication

End-point authentication has been used for many years in both voice and data networks. Specific to voice systems, authentication in legacy non-IP platform solutions has been rare and seldom used, save for application accesses such as voicemail and specific substitution and administration functions. As discussed in previous sections:

- Authentication is a valuable security tool so long as it universally applied
- Any authentication solution that can be easily bypassed often is.

Historically, authentication has been an application level access control. That is to say, authentication requests were made only after a user/device had access to the network. The problem is, malicious entities often do not need to authenticate with the application in order to monitor and/or disrupt the network. A simple example that most computer users can identify with is that of a virus infected PC disrupting all network communication even though it is not authenticated with network servers. Simply put, controlling who/what has access to the network can be just as important as the provisioning of access controls for specific applications.

In response to the need for greater authentication capability, many networks now leverage **IEEE 802.1X authentication** for all network clients. In this authentication model, Ethernet switches require that devices (PC clients) validate their identity before being granted network access. Again, any system that can be bypassed probably will be – making it important to authenticate all devices that attach to the network, not just PC clients.

It is an unfortunate fact that Voice over IP systems have evolved at an incredibly swift pace, often providing ease of use in lieu of security. What made VoIP very attractive a few years ago, the near plug-and-play nature of server elements and telephones, has become a major liability to network security. To combat this, Alcatel-Lucent has included device authentication options for its range of IP Touch terminals.

Using IEEE 802.1X authentication, Alcatel-Lucent IP terminals can provide credentials (EAP-MD5 or EAP-TLS) for authentication with the network. In conformance with the 802.1X scheme, this authentication precedes any actual access to the network or any of the applications that it supports. Alcatel-Lucent's IP Touch terminals are also transparent to the authentication requirements of devices attached to the network via the "guest" port (available Ethernet port used to provide access to PC clients behind the IP phone.)

Note: 802.1X terminal authentication does not provide any immediate authentication of the terminal user. The terminal authentication process provides verification that the telephone set is allowed to interact with the network. Once the terminal has been authenticated with the network, the user can authenticate with the PCX via traditional PBX methodologies (extension number and PIN-code as an example.)

Design Recommendations: Terminal Authentication

To ensure enhanced network and telephony security through authentication, Alcatel-Lucent recommends:

- Network infrastructure (Ethernet switches) should be capable of authenticating multiple 802.1X clients on each switch port.
- 802.1X protocol requires for Authentication Server (RADIUS) that aims to verify matching between credentials (login/password or X509 digital certificate) sent by the terminal and the identity database, attached to the authentication server or centralized for global corporate usage.

12.8 Wireless Network Considerations

Security related to VoWLAN implies separating voice and data. This method avoids any intrusion from the data network to the Voice network. This requires the use of different SSIDs for Voice and Data. Each SSID is linked to a WLAN and then to a VLAN.

Forbidding the SSID broadcast does not provide an additional level of security, because it implies longer delay when doing handover with Wireless phones.

Encryption is an excellent method for protecting Wireless flows against eavesdropping. Different solutions for ciphering are now available. While WEP is considered as a very weak solution, WPA PSK based on TKIP provides a good level of Security. WPA2 PSK built on AES algorithm (802.11i standard) gives the strongest level of Security.

Rogue Detection is a security scheme that can detect and block at wireless level, intrusion attempts or traffic redirection to a Rogue AP. This defense mechanism is provided by the WLAN infrastructure.

Authentication is a complementary security process to filter the access to the WLAN. White-listing and black-listing represent a first level of authentication. WPA and WPA2 provides a higher level of authentication as the encryption key it is required to associate to the AP. Firewall rules (if available on the WLAN Switch) filter the access to the WLAN.

12.8.1 RF Protection

The optional RF Protection (RFP) license provides spectrum analysis showing RF channel usages, interferences and the following Security features:

ROGUE AP PREVENTION

- Rogue AP detection, classification, location and automatic containment

DENIAL OF SERVICE (DoS) ATTACK DETECTION

- Management frame floods
- Deauthentication attacks
- Authentication floods
- Probe request floods
- Fake AP floods
- Null probe responses
- EAP handshake floods

PROBING AND NETWORK DISCOVERY

- Detection of NetStumbler and broadcast probes

CLIENT INTRUSION PREVENTION

- Honeypot AP protection
- Valid station protection

NETWORK INTRUSION DETECTION

- Wireless bridges
- ASLEAP attacks

SURVEILLANCE

- Detection of weak encryption implementation

IMPERSONATION DETECTION AND PREVENTION

- MAC address spoofing
- AP impersonations
- Man-in-the-middle attacks
- Sequence number anomaly detection

__Design Recommendations__:

To improve Security at WLAN level Alcatel-Lucent recommends:

- Assigning a SSID for Voice and another dedicated to Data for flow separation but maintaining SSID broadcast to minimize delay when roaming with OT81x8 WLAN handsets.

For confidentiality Alcatel-Lucent suggests to use WPA or ideally WPA2 to encrypt Voice. These encryption schemes allow a strong authentication as well.

__Implementation Recommendations__:

Wlan switch configuration to reduce intrusion from Voice network to Data network:

- Assign a SSID dedicated to Voice, link this SSID to a Voice WLAN and then to a Voice VLAN and finally allow SSID broadcast. Use a separate SSID for Data traffic.
- WPA or preferably WPA2 to ensure encryption and authentication.
- Rogue detection and Firewall rules on WLAN switch to limit access to Voice WLAN/VLAN.
- As an additional security option, the RF Protection (RFP) module includes support for detection/prevention of network probing, client impersonation, DoS attacks, and unauthorized devices.

12.9 System Integrity Check

To ensure consistency of data and configuration of the system, several mechanisms are available in OmniPCX Enterprise solution. Directly embedded as administration services or provided by Alcatel-Lucent Application partners, those features allow verifying integrity of software release installed on servers, log access and modification to databases, check consistency of system configuration.

On the Communication Server, there is a mechanism to control binaries checksum in dynamic patch before installation. At any time, system administrator can also verify that Linux distribution packages are the ones installed during installation operation. History file is available that log all version update or system configuration file modification.

Database of the system, containing resources description (users, directory, terminals, accesses etc…) can be managed from the OmniVista platform. Database interface is designed to be able to take into account up to 10 simultaneous requests for retrieving data. All the operations performed by the administrator are logged with its identity into in the system. This feature is called “Audit” and can be used to verify all MAC (Move/Add/Change) operations that are performed on managed systems.

IP equipments (IP Touch phones and Media Gateways) that need to download binaries during the initialization phase perform integrity check of the new binary before installation (based on digital signature). If integrity check fails then the equipment doesn’t take into account the binary file and starts with the previous correctly downloaded file.

12.10 Communications Confidentiality

In terms of security and particularly in a VoIP environment, confidentiality represents the most important criteria to take into account. Some sensitive information can be easily stolen using internally or externally driven attacks by hackers.

Among the risks identified on IP are the Denial of Service attacks which could have an impact on the availability of the system but also risks of eavesdropping conversations.

As IP networks are “shared” networks, IP flows can be captured either by sniffing directly on the path or by redirecting the flow to a sniffer by using Man In the Middle attacks and identity spoofing. The risk is increased because the tools required to perform these attacks can be found easily on the Internet and any user with a PC could become a threat to the confidentiality of communications.

There are solutions to limit risks of capturing IP communication flows on IP at the infrastructure network level (LAN switching, Voice and Data VLAN partitioning, protection against Gratuitous ARP on IP phones) but VoIP encryption (i.e securing at the application level instead of network level) is the most adapted solution to protect confidentiality, and adds an additional layer of security to the network layer: even if the flow is captured, it is not possible to decrypt it.

In TDM environment, end-to-end voice encryption requires specific equipment, and therefore is only deployed for specific users. With VoIP encryption, confidentiality of communications is native and will therefore be stronger than on standard TDM phones.

To ensure confidentiality (protection against eavesdropping), both Voice and Control Signaling flows need to be encrypted. Integrity of the call control signaling implies that messages have not been modified (avoiding Man in the Middle attacks).

Design Recommendations:

Alcatel-Lucent strongly recommends implementing the **IP Touch Security** Solution to ensure Confidentiality, Integrity and Authentication:

- Mutual Authentication of VoIP elements to prevent identity-spoofing
  - Using Factory Loaded or Site Specific Certificates. Easy to deploy and manage.
- Real-time Encryption (*<1ms delay*) of traffic to prevent eavesdropping
  - IPSec & TLS with SRTP (with 128 bit AES) to protect both signaling and voice payload
- Digital Signing of binaries and configuration files to prevent tampering
  - Preventing malicious configuration modifications
  - Preventing encryption deactivation/bypass
- Modular Deployment of components and software elements
  - Provides dedicated processing power and granular control of flows/costs
  - Leverages imbedded processor/firmware strengths of ALL current IP Touch models

Implementation Recommendations:

IP Touch Security implementation in **Standalone Node mode**:

- The OmniPCX enterprise R6.2 or above is required.
  – A Server Security Module (SSM) protecting the Com Server and a Media Security Module (MSM) protecting the IPMG. SoftMSM option (full software) is available for IPMG from OXE R9.1
  – A second SSM is needed in case of Com Server redundancy
  – Any IP Touch family belonging sets (4008, 4018, 4028, 4038 & 4068) for encryption capability

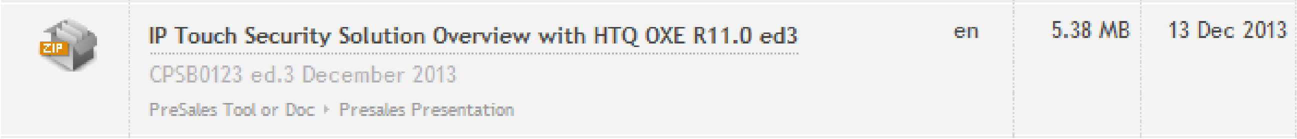
IP Touch Security implementation in **Networked Node mode**:

- The OmniPCX Enterprise R8.1 or above is required on all OmniPCX Enterprise nodes,
- All nodes must be able to do encryption
- An ABC IP Hybrid link is required between Secured OmniPCX Enterprise Nodes
- Compatibility with SIP/TLS & SRTP configured for SIP Trunks

Reference documents

The following documents are available under the Alcatel-Lucent Enterprise Business Portal (eBP):

[1] PreSales Presentation - IP Touch Security Solution in OXE R11.0 *(eBP)*

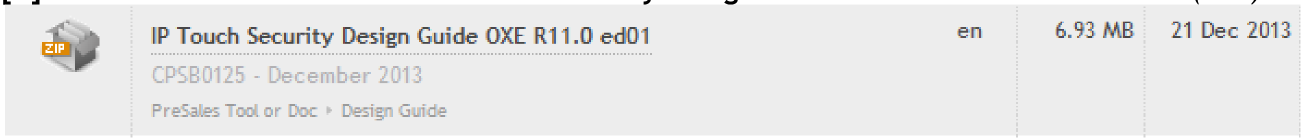


IP Touch Security Solution Overview with HTQ OXE R11.0 ed3 en 5.38 MB 13 Dec 2013

CPSB0123 ed.3 December 2013

PreSales Tool or Doc ‣ Presales Presentation

[2] PreSales Communication - IP Touch Security Design Guide in OXE R11.0/ICS R6.7.x *(eBP)*



IP Touch Security Design Guide OXE R11.0 ed01 en 6.93 MB 21 Dec 2013

CPSB0125 - December 2013

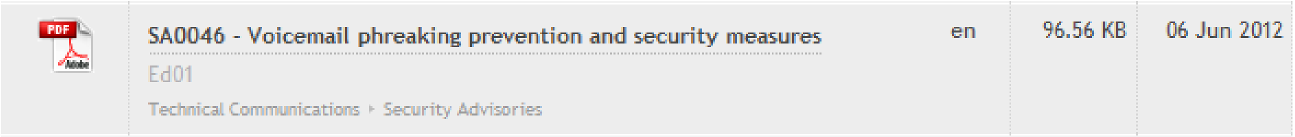
PreSales Tool or Doc ‣ Design Guide

[3] Technical Support Communication - IP Services and Ports number
Technical Knowledge Base (product OXE)

[4] Technical Support Communication : OmniVista 8770 Security Guide
Technical Knowledge Base (product OV4760 - OV8770)

[5] OpenTouch Suite for MLE Standard Offer / Security chapter *(eBP)*

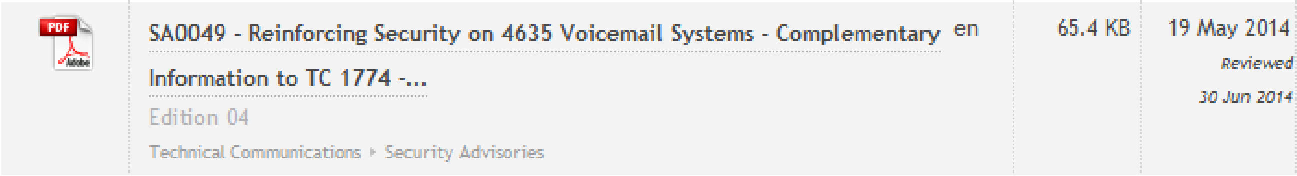
[6] Security Advisories: SA0046 SA0049 *(eBP)*



SA0046 - Voicemail phreaking prevention and security measures en 96.56 KB 06 Jun 2012

Ed01

Technical Communications ‣ Security Advisories

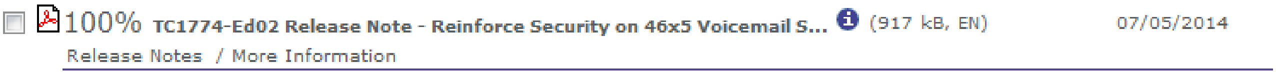


SA0049 - Reinforcing Security on 4635 Voicemail Systems - Complementary Information to TC 1774 -... en 65.4 KB 19 May 2014 Reviewed 30 Jun 2014

Edition 04

Technical Communications ‣ Security Advisories

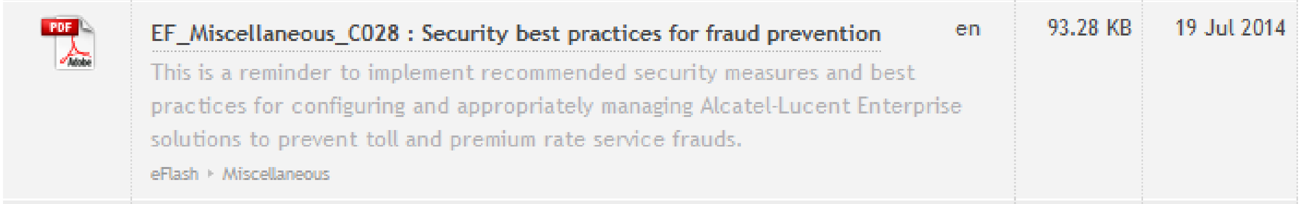
[7] Technical Support Communication: TC1774 *(Technical Knowledge Base)*



□ 100% TC1774-Ed02 Release Note - Reinforce Security on 46x5 Voicemail S... ℹ (917 kB, EN) 07/05/2014

Release Notes / More Information

[8] E-Flash C028: Toll and Premium Rate Frauds. A reminder on Alcatel-Lucent Enterprise security best practices *(eBP)*



EF_Miscellaneous_C028 : Security best practices for fraud prevention en 93.28 KB 19 Jul 2014

This is a reminder to implement recommended security measures and best practices for configuring and appropriately managing Alcatel-Lucent Enterprise solutions to prevent toll and premium rate service frauds.

eFlash ‣ Miscellaneous

Glossary

802.1X: it is an IEEE standard for port-based Network Access Control; it is part of the IEEE 802 (802.1) group of protocols. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. It is used for certain closed wireless access points, and is based on the EAP, Extensible Authentication Protocol (RFC 2284). RFC 2284 has been made obsolete by RFC 3748.

Adware: it is any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. The justification for adware is that it helps recover programming development cost and helps to lower the cost for the user.

Antispam: E-mail has become the subject of much abuse, in the form of both spamming and E-mail worm programs. Both of these flood the in-boxes of E-mail users with junk E-mails, wasting their time and money, and often carrying offensive, fraudulent, or damaging content.

Firewall: A firewall is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

FTP: File Transfer Protocol. This is the language used for file transfer from computer to computer across the WWW. An anonymous FTP is a file transfer between locations that does not require users to identify themselves with a password or login. An anonymous FTP is not secure, because any other user of the WWW can access it.

HTTP: The Hypertext Transfer Protocol (HTTP) is a set of rules for exchanging information (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

IMAP: Internet Message Access Protocol) IMAP is gradually replacing POP as the main protocol used by email clients in communicating with email servers. Using IMAP an email client program cannot only retrieve email but can also manipulate message stored on the server, without having to actually retrieve the messages. So messages can be deleted, have their status changed, multiple mailboxes can be managed, etc.

IPSec: IPSec (IP security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment.

Phishing: “Phishing” is a form of Internet fraud that aims to steal valuable information such as credit cards, social security numbers, user IDs and passwords. A fake website is created that is similar to that of a legitimate organisation, typically a financial institution such as a bank or insurance company. An email is sent requesting that the recipient access the fake website (which will usually be a replica of a trusted site) and enter their personal details, including security access codes.

RADIUS: Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization, and accounting) protocol for controlling access to network resources. RADIUS is commonly used by ISPs and corporations managing access to Internet or internal networks across an array of access technologies including modem, DSL, wireless and VPNs.

SMTP: a protocol for sending e-mail messages between servers; most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP; in addition, SMTP is generally used to send messages from a mail client to a mail server; this is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

Spam: Spam refers to electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited e-mail. In addition to being a nuisance, spam also eats up a lot of network bandwidth. Because the Internet is a public network, little can be done to prevent spam, just as it is impossible to prevent junk mail. However, the use of software filters in e-mail programs can be used to remove most spam sent through e-mail.

Spyware: Any software that covertly gathers user information through the user's Internet connection without his or her acknowledgement, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

SRTP: The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications. It was developed by a small team of IP protocol and cryptographic experts from Cisco and Ericsson including David Oran, David McGrew, Mark Baugher, Mats Naslund, Elisabetta Carrara, Karl Norman, and Rolf Blom. It was first published by IETF in March 2004 as RFC 3711.

SSH: Secure Shell or SSH is a network protocol that allows data to be exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.

TLS/SSL: Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers. There are slight differences between SSL and TLS, but the protocol remains substantially the same.

Annex A

Introduction

This annex presents the list of main security features that have been implemented over the past years to harden security of the OmniPCX Enterprise solution.

Heritage from the past

The OmniPCX Enterprise product (starting from release 5.0) is the successor of OmniPCX 4400 product (ending with release 4). Logically it benefits from the security features provided by its predecessor:

- Toll Fraud Protection
- Access Control (Trusted Hosts, TCP Wrapper)
- Log and Incidents Management

Features list details

For each product release, the list of security features introduced is detailed.
For more explanations on those features you can refer to the Presales Presentation related to the release available under the eBusiness Portal.

Product release	Description
OXE R5.1	Global Security Enhancements - Suppress unused system accounts (mtch etc…) - Default passwords change on first logon - Trusted hosts profiles and IP ranges - Remove unused remote commands (rlogin)
	NTP - Time log correlation - Server and Client modes
OXE R6.0	SSH - Replace unsecured services telnet/ftp/rcp - Integration of OpenSSH/OpenSSL
OXE R6.1	HTTPS - New web server Apache - Optional activation/deactivation of web server
OXE R6.2	Password Policy Management - Secure Passwords by default - Centralized password changing and aging - Quarantine mechanism for system account on unsuccessful authentications
	External Syslog server - Export of full system log - Export of shell command history

	IP Touch Security - Signaling call control encryption IPSec (AES 128bits) - Voice encryption SRTP (AES 128bits) - Dedicated hardware modules (SSM, MSM) - Mutual authentication (Diffie-Hellman) - Call control messages integrity (HMAC/SHA1)
OXE R7.0	RADIUS external authentication - OXE/CS as RADIUS NAC for remote access control - Support in OTUC (R4) for external authentication
OXE R7.1	RADIUS enhancement - Use of corporate identities instead of OXE default system identities - Support in OmniVista 4760 (R4) for external authentication
	SNMPv3 - Support of standard SNMPv3 protocol (in addition to SNMPv1 and SNMPv2c) for secured supervision of OXE nodes - Administrator password control and encryption of data over the network
	Passive Communication Server (PCS) - Enhanced local survivability with the PCS to rescue IP Touch sets and Media Gateway in case of WAN outage
	Protection of IP Touch sets - Password to access parameters of the set (MMI interface) - PC port control (lock/unlock, VLAN ID filtering)
	802.1X (EAP-MD5) - Authentication of IP Touch sets based on standard protocol 802.1X
OXE R8.0	Protection of IP Touch sets - Defence mechanism against ARP poisoning attack - Defence mechanism against ARP spoofing attack
	Secured Unified Communications (OTUC R5) - Integrity control and encryption of all signaling and voice media flows to Applications and Media servers
OXE R8.0.1	OXE Networking encryption - Enhancement of IP Touch Security feature to deliver encryption of communication for OXE in network (ABC links)

OXE R9.0	802.1X (EAP-TLS) - New method for 802.1X protocol allowing IP Touch sets authentication based on X509 digital certificates. - Integration in customer PKI (download of customized certificate)
	Encryption of Signaling on Media Gateway - IP Touch Security feature option to have software integrity control and encryption of signaling call control embedded in Media Gateway (without hardware module)
OXE R9.1	“soft”MSM on Media Gateway (GD3/GA3, INTIP3) - IP Touch Security feature option to have full software integrity control and encryption of both signaling call control and voice media stream directly embedded in Media Gateway (without additional hardware module)
OXE R10.0	Encryption of SIP communications to Public Network - IP Touch Security feature option to support TLS and SRTP toward SIP trunks to PSTN Gateway (based on SIP protocol) and Public SIP Trunking - Digital Certificates (standard X509v3) for server authentication Encryption of the MyIC Desktop SIP client (ICS R6.6) - Support of TLS and SRTP at client level to provide encryption of the signalling session and voice media toward a SBC component
OXE R10.1.1	Network encryption with SIP TLS - support of SIP TLS & SRTP for SIP Trunk in an OXE homogeneous network
OXE R11.0	OXE MS encryption

End of Document