0. Introduction

The present manual offers a guide for installation and first time configuration of **PrivateServer** which along with **PrivateWave** composes the **Enterprise Voice Security Suite** : the solution that ensures the safety and inviolability of voice communications on both mobile and fixed phones by offering a secure voice convergence system in a corporate network.

Requirements

PrivateServer works on VoIP technology (Voice over IP) and requires an internet access. Thus the server chosen for installation (either phisical or virtual) must have almost one Network Interface Card on board.

Goals

The present manual will explain to you how to:

- install **PrivateServer** from cdrom or by virtual machine
- configure the Network
- configure your certificates
- organize the network security architecture
- perform backup and restore
- perform software upgrades

Intended audience

This guide is intended for system administrators who will configure a secure enterprise voice network based on PrivateServer . The reader should have a networking and system administration background. VoIP knowledge is not mandatory, but strongly suggested.

This manual won't explain how to manage the service itself (ie create users, groups, SIP trunk, etc). For such knowledge please refer to PrivateServer - Operator Manual.

Glossary

Audio Announcements

The **Audio Announcement** is the means used by PrivateWave for communicating to an user about the failed calls. You have several messages that can be spoken and each of them can be localised in English, French, Italian, Spanish and German.

Automatic Activation

The **Automatic Activation** is the way of create new users automatically without any need they interact with anybody. As from user's side the procedure is that he/she gets an **invite SMS** or **E-Mail** useful to download the application PrivateWave and to provide automatic configuration of the client itself. All the user has to do is to follow the links into the Texts/E-mails and PrivateWave would go automatically on line.

Call Roaming

Call Roaming is specific configuration set up by default on both PrivateServer and PrivateWave . It let any call to continue even if one network change event occur (e.g: wi-fi network got lost in favour of 3g data mobile one). During network change itself the call is muted but as soon as any connection is again available, then voice stream is back streaming. Call roaming is subject to Strictrtp and Rtp timeout options in PrivateServer .

Call Transfer

Call transfer is a typical PBX performance which is implemented in **PrivateServer** as well. One of the partecipant can hold on his/hers peer and perform a new call to the number to which trasfer the call. If the desired number picks up the call, then the transferrer can close the communication and let his/hers peer talk with the trasferred number.

> This feature is not available for end-to-end only accounts.

Conference Calls

Conference Call, as its name implies, is a call involving at least three users. It differs from Conference Room by the fact that Conference Call is one Secure Call at which third parties got invited. So it's one sort of dynamic conference room. All users invited are thus added to conversation in progress by either caller or callee.

> This feature is not available for end-to-end only accounts.

Conference Rooms

The **Conference Room** is the kind of call that more persons can partecipate. The conference calls are usually defined as "**rooms**", whose access can be limited by **time settings** or **pass code**.

> This feature is not available for end-to-end only accounts.

Extensions

A **telephone extension** is an internal telephone line attached to a Private branch exchange (PBX). The PBX operates much as a community switchboard does for a geographic telephone numbering plan and allows multiple lines inside the office to connect without each phone requiring a separate outside line. In these systems, a dialer usually has to dial a number to tell the PBX to connect with a landline to dial an external number. Within the PBX, the user merely dials the extension number of the person. Each phone line may be extended up to a fixed maximum.

Jitter

In VoIP systems audio signal is split into multiple packets, which are sent over network. Due to network equipment behavior, packets flow is never regular and constant. Especially on mobile/radio networks packets are delivered in bursts, leading to irregular and variable latency. **Jitter** is the variation in latency as measured in the variability over time of the packet latency across a network.

PBX

A **Private Branch Exchange** (**PBX**) is a telephone exchange that serves a particular business or office, as opposed to one that a common carrier or telephone company operates for many businesses or for the general public.

PBXs make connections among the internal telephones of a private organization—usually a business—and also connect them to the public switched telephone network (**PSTN**) via **trunk** lines.

Presence

The **Presence** is how we call the user's status, also known as the user's reachability. By checking an user's Presence it is possible to know if a he/she is on line and can receive a secure call before trying to.

Provisioning

The **Provisioning** is the configuration needed for delivering both for the PrivateWave application and its configuration and nowadays it's used by the **Auto matic Activation** only.

Secure Call

A **secure call** is a voice connection which can't be wiretapped and it runs over **Voice Over IP** (**VoIP**) communication protocol.

End-to-Site security model

Secure call is encrypted from client up to server.
The **end to site** security model provides a **strong** security level and can be used among two or more PrivateWave equipped devices and/or among **SNOM 300** landline devices or also for connecting other **PBX**, secure or not. If **PBX** is not secure, we face a crypto-to-clear scenario, where the call is secured between PrivateWave and PrivateServer , but is not secured between PrivateServer and **PBX**.
Given that in this security model the server can decrypt secure calls content, it is possible to provides advanced telephony features such as:

- 3-way calls
- call transfer
- conference rooms

End-to-End security model

Secure call is encrypted from client up to the other client. Despite server relays encrypted traffic, it does not knows the encryption keys, so it cannot decrypt the call content.
The **end to end** security model provides the **highest** security level but can be used only between two PrivateWave equipped devices.
This security model does cannot be used to integrate enterprise PBXs.

In this security model the server cannot decrypt secure call content, so advanced features are not available.

Multilevel security model

This is a mix of the other security model. Each call made by PrivateWave

client produces encrypted traffic based on the recipient of the secure call:

- if the call recipient is another PrivateWave client, the call is made using the ZRTP protocol for key exchange
- if the recipient of the call is not a PrivateWave client
- the call is made using the SDES protocol

This security model can be used to integrate enterprise **PBXs**.

It is also possible to provides advanced telephony features such as:

- 3-way calls
- call transfer
- conference rooms

using SDES protocol.

PrivateServer

PrivateServer is the **PBX** committed to perform **Secure Calls** both **end to end** and **end to site**. It differs from a standard **PBX** for exposing just the **Secure Call** service to VoIP PrivateWave clients and can be connected to a standard **PBX** via **SIP Trunks** if configured accordingly.

PrivateWave

PrivateWave is the VoIP client for **Secure Calls** connections. It has to be used along with PrivateServer .

Secure Message

Secure Message is a text message that can be sent and received only by using PrivateWave and that shares the same communication infrastructure of Secure Call. The maximum length of each message is 1000 character. In addition to text messages you can send and receive attached files such as photos, documents and voice notes. You can also share your location. Secure messages are end-to end encrypted.

Trunk

A **trunk line** is a circuit connecting telephone switchboards (or other switching equipment), as distinguished from local loop circuit which extends from telephone exchange switching equipment to individual telephones or information origination/termination equipment.

When dealing with a **Private Branch Exchange** (**PBX**), trunk lines are the phone lines coming into the PBX from the telephone provider. This differentiates these incoming lines from **extension** lines that connect the PBX to (usually) individual phone sets.

Caveat

The figures in this document are solely for illustrative purposes. They give you an idea about the essential information you are supposed to see on the screen while executing the test cases. However the layout of the screen and the details of the information may be changed in subsequent revisions of the software and these modifications are not obligatory reflected in this document. When considering whether a test case passed or not, you should relay only on the textual description of the test case.

1. Installation