



ViPNet Connect Overview

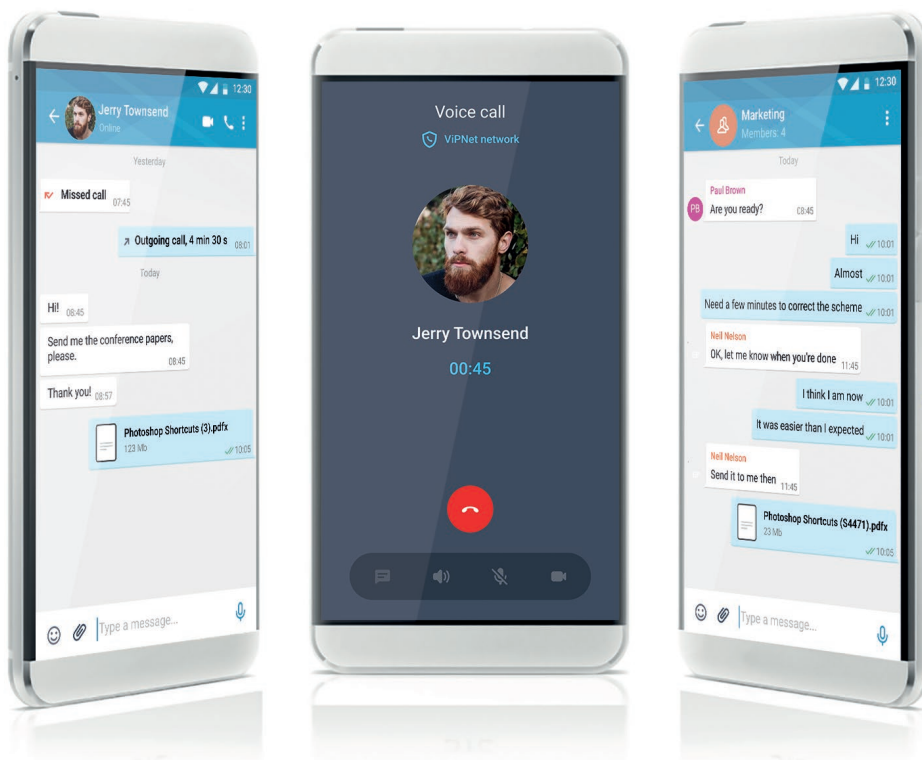

infotecs

In today's world, information is an essential asset that should be protected as a top priority.

Corporate communications are inherent in any operating company, but more and more companies tend to favor VoIP and mobile communications as these technologies allow them to reduce costs and ensure business continuity.

However, despite all the advantages and functional diversity, VoIP and mobile communications are rather vulnerable in terms of information security. Major threats include data interception and manipulation, user data spoofing and hacking, as well as denial of service (DoS) attacks.

Besides the primary function to provide telephone communications, modern mobile devices serve as mobile terminals to access the Internet and often corporate information resources. That is why information security presents even a more critical issue for mobile devices than for desktop computers.



The following considerations should be taken into account:

- 1 A strict information security policy should govern all corporate communications; the identification and authorization mechanisms should be in place; and, the infrastructure should be protected in general.
- 2 Mobile devices are so popular that their owners tend to use them all the time, namely, employees generally prefer using the same device both for business and personal matters. This leads up to insecure scenarios in the corporate environment; for example, untrusted applications in business processes and communications.

Driven by detailed research in the network protection field and comprehensive analysis of vulnerabilities in corporate IT infrastructures comprising remote and mobile users, as well as security issue investigations, Infotecs has developed the ViPNet Connect solution based on its own ViPNet technology.

SOLUTION CONCEPT

Employees are widely using WhatsApp, Viber, Telegram, Skype, and other publicly available services on their mobile devices within the corporate infrastructure, which poses serious information security risks.

ViPNet Connect is used to arrange secure communications between corporate users and allows security administrators to manage information security policies and infrastructure on their own. ViPNet Connect supports voice calls; texting; and, file sharing on IP phones, desktop computers, laptops, and mobile devices. ViPNet Connect users can communicate in private through secure point-to-point encrypted ViPNet network channels.

Since no routing server is required, there is no need to ensure a high-throughput channel for it.

Advantages



SECURE DATA EXCHANGE

ViPNet Connect users exchange traffic directly between devices; there are no servers to decrypt data at intermediate stages. This ensures the protection of the transmitted data against decryption even by an insider



SECURE CONTACT LIST

In ViPNet Connect, the contact list is formed by the ViPNet network administrator centrally and is isolated from the device's contact list. The administrator controls the list of contacts a user can communicate with in a secure way



COMPREHENSIVE

ViPNet Connect is intended to unify all the corporate communications



RELIABLE

ViPNet Client encrypts and protects all the data (including traffic in a local network)



EASY TO USE

A modern and intuitive UI design does not require any special skills from users. ViPNet Connect contact list contains only user names, which is enough to make phone calls and chats



FEATURES

ViPNet Connect has all the most popular features of publicly available messengers:

PRIVATE CHATS

ViPNet Connect allows you to create individual point-to-point chats without storing the transmitted data on any intermediate servers. The solution features include formatting the message text, quoting and forwarding messages, mentioning users in messages, editing the message text within 10 minutes after it was sent, deleting messages automatically based on a timer, etc.

GROUP CHAT

ViPNet Connect allows you to create group chats, choose a name for your group chat and manage it by adding users to it. All information is stored on the ViPNet Connect server and is reliably protected.

BROADCASTS

ViPNet Connect allows you to create broadcasts to notify your organization's employees about significant events. A messaging list is a one-way notification mechanism in which users cannot communicate with each other within the mailing group.

AUDIO CALLS

With ViPNet Connect, not only can you send messages, but also call a user in the point-to-point mode. All conversations are encrypted with symmetric 256-bit keys over the communication channel using ViPNet Client. ViPNet technology ensures high-quality voice communications even on poor and unstable communication channels.

VOICE MESSAGES

ViPNet Connect allows you to send voice messages up to 10 minutes long, which is convenient when a user cannot type text on the keyboard.

INTEGRATION WITH MDM SYSTEMS

ViPNet Connect is compatible with MDM systems in regards to remote connection use cases and software distribution.

DATA BACKUP, RESTORATION, AND DELETION

ViPNet Connect allows you to save and later restore a backup copy of chats and message history. If necessary, you can use the emergency data deletion option, in which case the solution will delete the data and also overwrite the memory areas where the chats and message history were previously stored.

INTEGRATION WITH SIP TELEPHONY

ViPNet Connect can be integrated with SIP telephony systems and connect to the customer's existing SIP servers as a SIP client. With such an integration option, all the communications within the customer's organization can be centered on ViPNet Connect, which creates a unified communication space. If the company is connected to the city phone landline, you can make calls from ViPNet Connect to the city landline phone numbers due to the SIP integration.

VIDEO CALLS

In addition to audio calls, you can also arrange video calls, using either the front camera or the main camera on your smartphone. During a video call, you can share your screen, for example, to demonstrate a slideshow, work on a document or provide technical support for another user.

INTEGRATION WITH VIDEO CONFERENCING SYSTEMS

ViPNet Connect can be integrated with video conferencing systems, which allows you to organize video conferences from both desktop computers and mobile devices.

PROTECTION OF VIPNET CONNECT CORRESPONDENCE ON YOUR DEVICE.

ViPNet Connect allows you to prevent access to your correspondence and contact list by protecting them with a password, a PIN code, or a user's biometric data, such as FaceID or fingerprints.

SAMSUNG DEX SUPPORT

ViPNet Connect supports DeX mode on Samsung devices, which allows you to work on your mobile device and use an external monitor and keyboard/mouse at the same time.

SAMSUNG KNOX SUPPORT

ViPNet Connect supports Samsung Knox technology and can function inside the Knox container. Your data is double protected by both the ViPNet Connect and Samsung Knox security mechanisms.

FILE SHARING

ViPNet Connect allows you to share files and send attachments without any size limitations both in individual and group chats and messaging lists. You can send graphic files without changing their quality, which is especially important for corporate communications.



VIPNET CONNECT IP PHONE

A special device that ensures protection of business communications due to the secure VoIP technology.



SOLUTION ADVANTAGES

- Provides an easy to use, user-friendly, and intuitive UI without tricky buttons and complex algorithms for finding and calling another subscriber
- Encrypts and filters the signaling and voice traffic for all parties in the VoIP network
- Ensures that the VoIP traffic passes through NAT devices smoothly
- Supports virtual addresses, particularly for SIP, H.323, and Cisco SCCP (Skinny Client Control Protocol) protocols, thus solving the issue of conflicting IP addresses for remote offices



SPECIFICATIONS

- 10.1" HD sensor display with an intuitive UI
- Wireless/wire* phone, left or right handed holder design
- Built-in high-definition camera (720p)
- Built-in Wi-Fi client
- 2-port Gigabit Ethernet (10/100/1000) switch
- Integrated PoE

* Depends on the modification

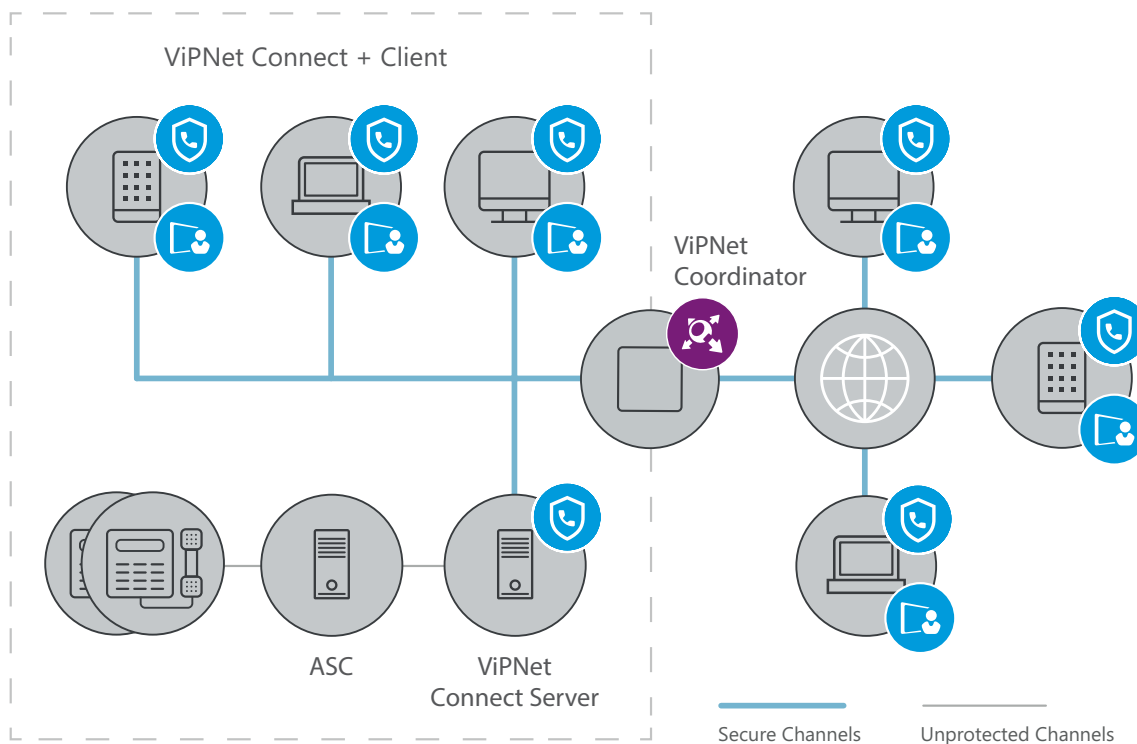
VIPNET CONNECT INFRASTRUCTURE

ViPNet Connect requires a ViPNet network infrastructure with ViPNet Connect Server deployed.

ViPNet Connect Server powers the group chat feature in ViPNet Connect applications and allows you to create and manage group chats, as well as stores the message history in group chats.

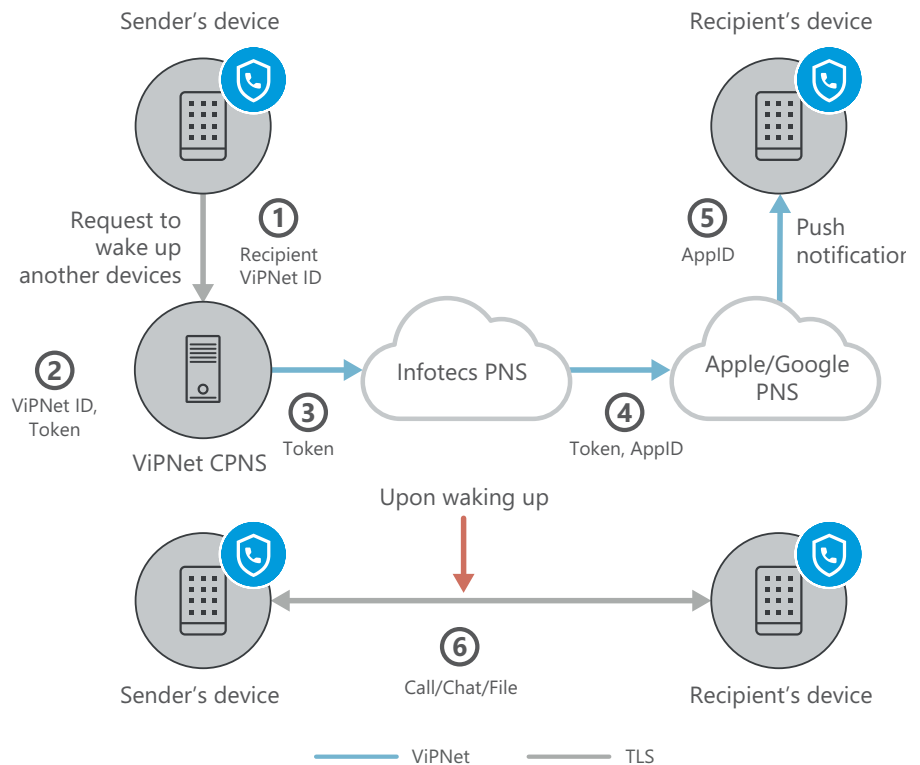
ViPNet Connect Server includes ViPNet Customer Push Notification Server (ViPNet CPNS), a component that allows making calls and exchanging messages and files between sleeping mobile devices with ViPNet Connect installed. This software transfers the push notifications to a mobile device, awakening it from sleep mode. As a result, ViPNet Connect installed on a device can accept incoming messages and calls.

Push notifications contain no meaningful data, which completely eliminates the risk of data leakage to Apple and Google servers.



How push notifications work

As you lock your mobile device, it stops accepting any messages, except for push notifications and cellular data. The ViPNet CPNS server can wake up your mobile device from sleep mode using push notifications. Sleeping devices with the installed ViPNet Connect software exchange push notifications as illustrated in the diagram below.



Here is an overview of how push notifications are transferred:

- As soon as you send a message or make a call via ViPNet Connect, ViPNet CPNS receives a request to send a push notification. This request contains:
 - ViPNet identifier of the recipient's device
 - Notification type (a call or a message)
- ViPNet CPNS scans the table with the details of the ViPNet hosts registered on ViPNet CPNS. When scanning, ViPNet CPNS compares the token issued by Apple or Google PNS (Google Firebase) with the ViPNet identifier of the recipient's device (depending on the device type, iOS or Apple). The recipient's device token does not contain a ViPNet identifier, therefore, you cannot find out the sender's or recipient's names. ViPNet identifier is stored only on ViPNet CPNS.
- ViPNet CPNS sends a push notification request to Infotecs Push Notification Server, IPNS. This request contains:
 - Recipient's device token
 - Recipient's device type (iOS or Android)
 - Notification type (a call or a message)
- IPNS sends a request to Apple or Google PNS (Google Firebase) depending on the recipient's device type. This request contains:
 - Recipient's device token
 - App ID for ViPNet Connect (to find out where to send a push notification)
 - Notification type (a call or a message)
- A sleeping recipient's device with ViPNet Connect installed receives a push notification from Apple or Google PNS. The device wakes up, and the traffic transfer resumes. A push notification contains:
 - App ID for ViPNet Connect
 - Notification type (a call or a message)
- The woken up recipient's device exchanges data directly over the secure ViPNet connection.

Thus, the push notifications mechanism is completely secure to use and entails no risks of data leakage.

System requirements

ViPNet Connect supports several popular operating systems and corresponding devices, namely, Android version 6 and later, iOS version 11 and later, Windows 8 and later, Linux, macOS.


Minimum requirements to the virtual machine with ViPNet Connect Server:

4 CPUs	Free disk space: at least 100 GB
RAM: at least 10 GB	Guest OS: Linux Debian (64-bit)


Remote deployment and distribution scheme

ViPNet Connect can be deployed remotely and licensed on a SaaS model, which reduces the capital expenditures on the product and allows you to manage the number of product copies in use flexibly. ViPNet Connect can be fully deployed on the customer's infrastructure, ensuring control over all the components of the solution.



 Infotecs GmbH, Germany
Potsdamer Strasse 182, D-10783 Berlin

 info@infotecs.de

 +49 30 206 43 66-0

 www.infotecs.de



© Infotecs GmbH («Infotecs»). All rights reserved. Disclaimer. The information contained herein has been prepared solely for the purpose of providing general information about Infotecs and its products. Infotecs has taken care in the preparation of the content of these materials. Such information presented is believed to be reliable but is subject to change at any time without notice. Infotecs disclaims all warranties, express and implied, with respect to such content. Infotecs does not represent that the information contained herein is accurate or comprehensive and shall accept no liability for the information contained herein or for any reliance placed by any person on the information. All brands and product names that are trademarks or registered trademarks are the property of their owners. The TM and ® symbols are omitted in this document.