



Security with Your business in mind

White Paper

Secure VoIP for optimal business communication

Learn how to create a secure environment for real-time audio, video and data communication over IP based networks.

Andreas Åsander
Manager, Product Marketing

Introduction

Effective information flows has become a strategic resource for all organizations as they face increased market competition, restricted budgets and limited resources. Therefore most large and modern organizations need a secure and reliable way of sharing business critical information with its customer, employees and partners across widely dispersed geographical areas.

To supplement the perimeter security the modern organizations also need a platform that provide them with value adding functionality such as secure VPN, VoIP capabilities, User Authentication, Traffic Shaping, Content Filtering and Centralized Management.

As Clavister focus on providing security with Your business in mind, we see that today security is just as much about reaping the benefits from improved information flows as the security itself.

In short: the safe exchange of intellectual property and confidential information is a top-line business enabler.

In this document you will learn how to create a secure and reliable environment for real-time audio, video and data communication over IP based networks such as Internet and Virtual Private Networks.

Background

Telephony is in a transitional stage where the traditional Private Automatic Branch Exchange (PBX) systems are replaced by, or upgraded into, new and highly efficient IP based solutions.

VoIP is voice delivered over IP (Internet Protocol) and is transported on the same network as data, thus avoiding the costs from telephone services that comes with the Public Switched Telephone Network (PSTN)

VoIP has in a short period of time become one of the largest growing technologies within the communication area and is driven by a desire to profit from the cost-efficiency that these systems carry. Today some analysts predict that IP based telephony will become a 15\$ billion market and that there will be more than 2 million companies benefiting from it.

As VoIP is gaining momentum and becoming a valuable resource for enterprises all over the world there are still critical concerns that holding the companies back from a large scale VoIP operation. One of those concerns is the threat of security breaches.

Most equipment in a VoIP infrastructure, no matter if it is an IP based telephone with embedded systems or standard VoIP Gateway servers running commercial Operating Systems like Windows or Linux, they are addressable and thereby exposed for security threats.

Clavister Security Gateway with a full-scale support for secure VoIP via H.323 is available in a variety of models suitable for branch offices to models capable of managing even the largest Service Providers and Telecom Operators.

Network Solution

H.323 Standard Overview

H.323 is a standard approved by the International Telecommunication Union to promote compatibility in videoconference transmissions over IP networks. H.323 is considered to be the standard for interoperability in audio, video and data transmissions as well as Internet phone and voice-over-IP (VoIP).

H.323 Components

The H.323 standard consists of these four main components:

- Terminals
- Gateways
- Gatekeepers
- MCUs (Multipoint Control Units)

Terminals

A H.323 terminal is a device that is used for audio and optionally video or data communication. For example phones, conferencing units or “software phones” (for example: NetMeeting®) running on standard PCs.

Gateway's

A gateway acts like an interface and connects two dissimilar networks and translates traffic between them. A H.323 gateway provides connectivity between H.323 networks and non-H.323 networks such as public switched telephone networks (PSTN). The gateway takes care of translating protocols and converting media between the different networks. A gateway is not required for communication between two H.323 terminals.

Gatekeepers

The Gatekeeper is the core application in the H.323 system and it is used for addressing, authorization and authentication of terminals and gateways. It can also take care of things like bandwidth management, accounting, billing and charging. The gatekeeper may allow calls to be placed directly between endpoints, or it may route the call signaling through itself to perform functions such as follow-me/find-me, forward on busy, etc. A gatekeeper is always needed when there is more than one H.323 terminal behind a NATing firewall with only one public IP. One could say that the Gatekeeper is a database that keeps track of all users and its role in a H.323 network is very similar to the role of a switchboard in a traditional PSTN system. Usually you will find the Gatekeeper as a software or appliance product installed on a standardized Operating System such as Windows or Unix.

MCUs (Multipoint Control Units)

MCUs provide support for conferences of three or more H.323 terminals. All H.323 terminals participating in the conference call have to establish a connection with the MCU. The MCU then manages the calls, resources, video and audio codecs used in the call.

H.323 Application Layer Gateway (ALG) in Clavister Security Gateway

The H.323 ALG is a flexible application layer gateway that allows H.323 devices such as H.323 phones and applications to make and receive calls between each other while connected to private networks secured by Clavister Security Gateways.

The H.323 specification was not originally designed to handle NAT, as IP addresses and ports are sent in the payload of H.323 messages. The H.323 ALG modifies and translates H.323 messages to make sure that H.323 messages will be routed to the correct destination and allowed through the firewall.

The Clavister H.323 ALG has the following features:

- H.323 version 5 (H.225.0 v5, H.245 v10)
- Application sharing (T.120)
- Gatekeeper support
- NAT, SAT

The Clavister H.323 ALG supports version 5 of the H.323 specification. This specification is built upon H.225.0 v5 and H.245 v10. In addition to support voice and video calls, the H.323 ALG supports application sharing over the T.120 protocol. T.120 uses TCP to transport data while voice and video is transported over UDP.

To support gatekeepers, the ALG makes sure to monitor RAS traffic between H.323 endpoints and the gatekeeper, in order to configure the firewall to let calls through.

NAT and SAT rules are supported, allowing clients and gatekeepers to use private IP addresses on a network behind the firewall, thus minimizing the risk of exposure to threats.

Threat Defense

Voice over IP face the same security risks as legacy telephony system but it also has the inherited characteristics of IP communication. One example of security risks that comes inherited from IP based communication is the risk for Denial of Service attacks. Clavister Security Gateway is purpose built for securing IP based communication and includes an extensive set of features designed for protection against denial of service attacks as well as other IP and / or application layer based attacks.

By using the strong encryption algorithms in the Clavister Security Gateway it is also possible to ensure secure and private connections, thus making VoIP an alternative even for the most sensitive and confidential phone or video conferences.

Redundancy and Reliability

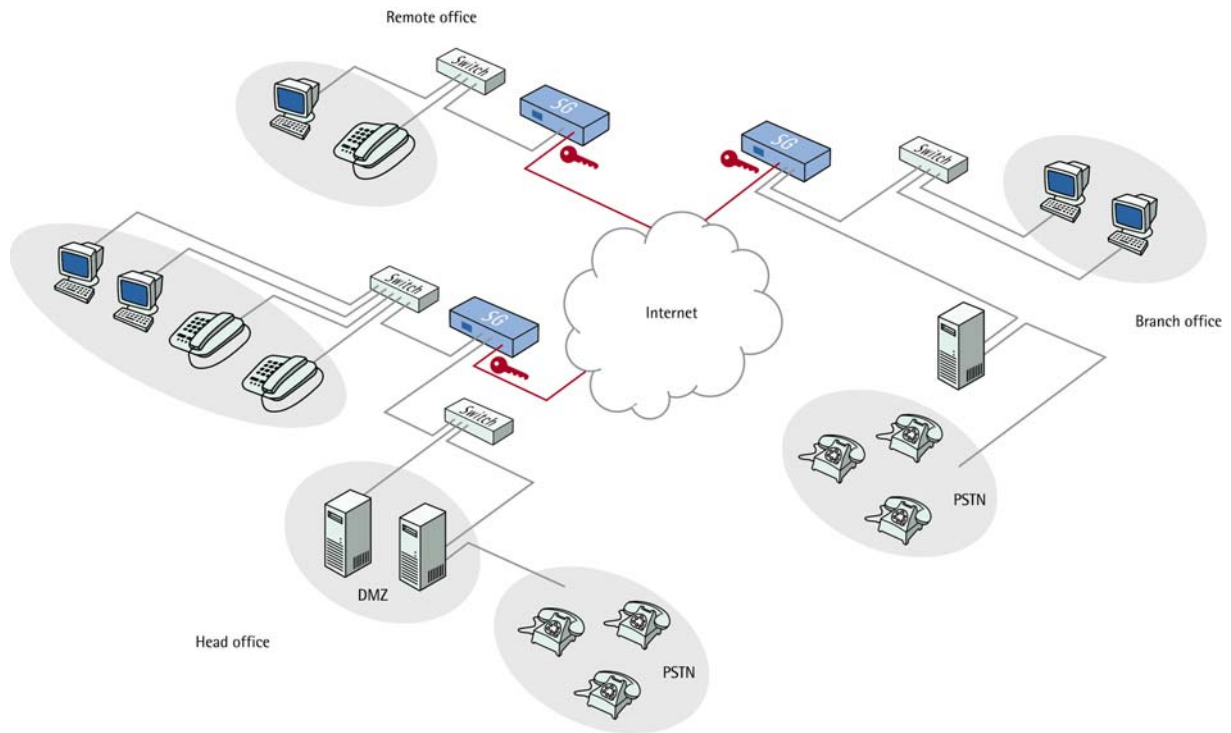
Transitioning from a traditional PBX system to a VoIP system might be a hairy task with reliability claims that could scare of even the most hardened telephony or IT manager.

Telephony is a crucial part of the business operations and it is expected to work at all times. No interruptions at all are tolerated.

Clavister Security Gateway that easily combines H.323 VoIP features with High Availability, Bandwidth Management, Quality Of Service and Enterprise Management makes the transition a lot more convenient and less complex.

Combining proven industry-standards with purpose-built features provides the enterprise with a central, easy-to-use and reliable solution eliminates most of the concerns threatening the transition into a new era of communication.

The Enterprise VoIP Network



The diagram above demonstrates a typical VoIP network scenario and how the Clavister Security Gateway with the VoIP Application Layer Gateway can be deployed in a corporate environment. At the head office DMZ a H.323 Gatekeeper is placed that can handle all H.323 clients in the head-, branch- and remote offices. This will allow the whole corporation to use the network for both voice communication and application sharing.

Imagine an environment where the entire company safely can take part of the highly cost efficient communication capabilities that voice, video and conferencing over an IP based networks provide.

With VoIP and real-time video conferencing you will not only earn money on the elimination of telephone service rates, you will create new business by becoming more available and improve collaboration with employees, partners and customers.

Conclusion

Key Customer Benefits

- **Robust Security**
The purpose-built security products from Clavister provides a complete set of security features including SPI Firewalling with DoS and DDoS protection, VPN with strong encryption and User Authentication.
- **Secure VoIP with DoS & DDoS protection**
Avoid costly service interruptions by limiting call setup from un-known sources and number of requests sent over UDP.
- **Lowered costs for telephone service rates**
Large cost reductions by utilization of existing, flat-rated, IP based connections for the telephone infrastructure.
- **Increase Security and Flexibility with NAT for H.323**
Clavister Security Gateway supports NAT for H.323 which makes it possible to avoid exposure of internal network addresses.

Several thousands of IP-Based telephones can be secured behind a Clavister Security Gateway with one single exposed public IP-address.

Clavister's integration of NAT for H.323 also makes it possible to use VoIP via less expensive ADSL connections where only one public address is available.
- **Rapid Deployment**
The Clavister Security Gateway provides effortless and rapid deployment. A trained technician can easily deploy and configure a new device within minutes, even across continents.
- **Lowered costs for administration**
The powerful Enterprise Management system that comes included in all Clavister Security Gateway products enables organizations to lower the costs for administration through centralized management. The Enterprise Management makes it possible to deploy and configure all devices across the network, no matter if they are located in the server hall next-door or ten thousand kilometers away.
- **High Performance**
Scalable performance with unsurpassed maximum bandwidth, concurrent connections and simultaneous VPN tunnels makes the Clavister Security Gateway the ideal choice even in the most demanding environments like Service Provider Networks and Data Centers.
- **Low TCO**
Clavister's goal is to provide complete security solutions more cost efficient than any competitor. Clavister Security Gateway with it's unique combination of integrated features and Enterprise Management System provides the lowest TCO and the best price / performance ratio possible

About Clavister

Clavister is a leading developer of high-performance IT/IP security. The products, based on unique technology, include carrier-class firewalls and VPN solutions. They have been awarded preferred choice by international press and are in use today by thousands of satisfied customers. In short; In a world where people depend on information, Clavister provides complete security solutions more cost-efficient than any competitor, always with Your business in mind.

Clavister was founded 1997 in Sweden. Its R&D and headquarters is situated in Örnköldsvik, Sweden and its solutions are marketed and sold through sales offices, distributors and resellers in Europe and Asia. Clavister also offers its technology to OEM manufacturers.

Limitation of Responsibilities

The information in this document represents the current view of Clavister AB on the issues discussed as of the date of publication. Because Clavister must respond to changing conditions, it should not be considered to be a commitment for Clavister, and Clavister cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. CLAVISTER MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the written permission of Clavister. Clavister may have trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Clavister, the furnishing of this document does not give you any license to these trademarks, copyrights, or other intellectual property.

© 2005 Clavister AB. All rights reserved.