

Feature Brief



Securing VoIP using SIP

Clavister SSP™ Security Services Platform

firewall • VPN termination • intrusion prevention • anti-virus
anti-spam • content filtering • traffic shaping • authentication

CLAVISTER®

Protecting Values

Introduction

Clavister Security Services Platform (SSP™) is our proven, feature-rich, service-oriented framework for providing best-in-class security solutions. Clavister SSP™ consists of **Clavister Network Security Elements**, **Clavister Lifecycle Systems**, and **Clavister Lifecycle Services**. Clavister SSP™ combines precise control, fine-granular administration, and seamless scalability making it easy to provision the perfect solution for any customer; be it a small organization, a large Internet Service Provider, a Managed Security Service Provider, or a multimedia-ready telecommunication operator.

Clavister Network Security Elements

These are the physical building blocks that you install in your network. Clavister SSP™ currently offers two network security elements; Clavister Security Gateway Series and Clavister Secure Access Gateway. The Clavister Security Gateway is available both as a pre-packaged turnkey appliance solution for fast and easy deployment or as a distributed software-only solution for your preferred hardware platform. The Clavister Secure Access Gateway Series is available as a pre-package turnkey appliance solution only and offers SSL VPN, Single Sign-On (SSO) and multi-factor authentication (MFA).

Clavister Lifecycle Systems

The Clavister Lifecycle Systems is a set of software components enabling true network security management throughout the entire lifecycle, including deployment, monitoring and reporting, configuration and integration, as well as analysis, optimization and troubleshooting. Clavister FineTune™ and the Web-based administration user interface enable you to manage a large set of Clavister Network Security Elements. Clavister InSight™ is our premium Security Event and Information Management (SEIM) system, which does not only support Clavister security network elements, but also a majority of other network devices. By correlating data from all network elements, you get a complete log of all activities in your network. Clavister PinPoint™ completes the Clavister Lifecycle Systems suite with accurate and precise real-time information packaged in a convenient dashboard-style application.

Clavister Lifecycle Services

The Clavister Lifecycle Services empowers you and your products with tools, services, and resources that help maximize benefits and eliminate problems, including planning, deployment, optimization, operations and maintenance. The Clavister Lifecycle Services include the Clavister Service Provisioning Network (CSPN) for automated signature updates, the Clavister xPansion Lines™ license upgrade framework and Clavister's award-winning Technical Support.

The Clavister SSP™ service-oriented framework provides you with a secure environment for your business; either as a service provided to you by a Managed Security Service Provider (MSSP) or as systems and services integrated in your own network.

For more information about Clavister products and services, please visit us at: www.clavister.com.

Overview

Voice over IP (VoIP) has finally arrived as a mainstream application. IP-based PBX equipment sales topped \$1 billion in 2005, for the first time outselling traditional TDM PBXs, according to Dell' Oro Group. Other analysts predict that IP PBXs will account for more than 90% of the market by 2009. VoIP and IP telephony are becoming increasingly popular with large organizations, but also with regular consumers. Internet Protocol (IP) is increasingly viewed as more than just a way to transport data, but also as a tool that simplifies and streamlines a wide range of business applications. Telephony is the most obvious example. VoIP is also the foundation for more advanced unified communications applications that can have a huge impact on the way we do business. But before deploying VoIP, you need to be aware of the security risks and the countermeasures that you can take.

Security is important in every context, but especially when you are replacing the world's largest, oldest and most durable and available communications network. While no individual security measure will eliminate attacks against VoIP deployments entirely, a layered approach can meaningfully reduce the probability that attacks will succeed.

VoIP Terms and Technology

Before we go into the risks associated with VoIP it is important to understand the terms used and it is also a first step toward learning the potential of this technology:

- VoIP refers to a way to carry phone calls over an IP data network, whether on the Internet or your own internal network. Although not the only attraction of using VoIP is its ability to help reduce cost because telephone calls travel over the data network rather than the phone company's network.
- IP telephony encompasses the full suite of VoIP enabled services including the interconnection of phones for communications; related services, such as billing and dialing plans; and basic features such as conferencing, transfer, forward, and hold. These services might previously have been provided by a PBX.
- IP communications includes business applications that enhance communications by enabling features such as integrated contact centers, unified messaging, and rich-media conferences with voice, data, and video.
- Unified communications takes IP communications a step further by using such technologies as Session Initiation Protocol (SIP) and presence along with mobility solutions to unify and simplify all forms of communications, independent of location, time, or device.

Public Internet phone calling uses the Internet for connecting phone calls, especially for consumers. But most businesses are using IP telephony across their own managed private networks because it allows them to better handle security and service quality. Using their own networks, companies have more control in ensuring that voice quality is as good as, if not better than, the services they would have previously experienced with their traditional phone system.

Session Initiation Protocol (SIP)

VoIP uses the IETF Session Initiation Protocol (SIP) and the Real-time Transport Protocol (RTP) for call signaling and voice-message delivery. SIP is an ASCII (UTF-8) text-based signaling protocol, much like H.323. In fact, the underlying packet handling in both SIP and H.323 is the same. Where the two protocols diverge is in the call signaling, which influences the call set up and breakdown, call control, and delivering advanced communications features. The SIP protocol and RTP protocol together with complementing session description and RTP control protocols (SDP, RTCP) do not provide adequate call-party authentication, end-to-end integrity protection and confidentiality measures on call signaling and call data (such as media streams containing compressed and encoded speech).

SIP is modeled upon other Internet protocols, such as Simple Mail Transfer Protocol (SMTP) and Hypertext Transfer Protocol (HTTP) using a request-response model. It is responsible for establishing, changing and terminating sessions between one or more users in an IP-based network. These sessions include Internet multimedia conferences, Internet or any IP network telephone calls and multimedia distribution. Members in a session can communicate via multicast or via a mesh of unicast relations, or via a combination of these

Today, SIP and RTP protocols do not encrypt call-signaling packets and voice streams, so identities, credentials and SIP Uniform Resource Identifiers (phone numbers) of callers can be captured using LAN and wireless LAN (WLAN) traffic-collection tools (sniffers). Until these security features are implemented and put into service, attackers have many vectors to exploit.

The Clavister Security Gateway have support for both SIP and H.323, which makes it an ideal solution for securing any type of IP communication, be it video or voice, for any set of diverse end-points. This feature brief will focus on SIP and the SIP Application Layer Gateway (ALG).

SIP Components

The SIP protocol is made up of a number of components that interact to bring forth the SIP service. The following three important aspects need to be clarified before going deeper into the subject.

- User Agents
A user agent is the end-point or peer that participates in the peer-to-peer communication. This can be a workstation or a telephone device used in a telephony conversation.

- Proxy Servers
A proxy server acts as a router in the SIP protocol. When receiving peer requests, it functions both as peer and server. Proxy servers forward requests to a peer's current location and manage authentication and authorization access to services.
- Registers
A registrar is a server that handles the actual SIP REGISTER requests. Its main function is to locate the host where the other peer is reachable.

NOTE: The Registrar and the Proxy Server are both logical entities and may reside on the same physical server.

VoIP Threats and Vulnerabilities

Enterprise VoIP customers and service providers are vulnerable to many of the same impersonation-based attacks "phreakers" attempt against traditional telephone and cellular services. The attacker's goals are the same; identity and information theft and toll fraud.

Many attacks focus on VoIP end-points. The operating systems, Internet protocols, applications and management interfaces of VoIP hard phones and computers running softphones are all vulnerable to unauthorized access, viruses and worms, and many denial-of-service (DoS) attacks that exploit common Internet protocols and VoIP protocols themselves.

Impersonation Attacks

An attacker can use captured account information to impersonate a user to a customer representative or self-service portal, where he can change the calling plan to permit calls to toll-free numbers or to blocked international numbers. He also can access voice mail or change a call forwarding number. Impersonation attacks commonly are used to perpetrate toll fraud, but financially motivated attackers also can capture voice conversations and later replay them to obtain sensitive business or personal information.

Man-in-the-Middle Attacks

VoIP is vulnerable to man-in-the-middle attacks, where the attacker intercepts SIP call-signaling traffic and masquerades as the calling party to the called party, or as the called party to the calling party. Once the attacker has gained this man-in-the-middle position, he can hijack calls via a redirection server.

DoS Attacks

Flooding VoIP targets with SIP call-signaling messages, for example `Invite`, `Register`, `Bye` or RTP media stream packets, which can degrade service, force calls to be dropped prematurely and render certain VoIP equipment incapable of processing calls entirely. VoIP equipment also may be vulnerable to DoS attacks against such Internet protocols as TCP SYN, ping of death and the recent DNS distributed DoS amplification attacks.

Media Attacks

VoIP systems also can be disrupted by media-specific attacks, such as Ethernet broadcast storms and Wi-Fi radio jamming. Operating systems and TCP/IP stacks used in new VoIP hardware may be susceptible to implementation-specific attacks that exploit programming flaws. This can cause the system to cease operating or provide the attacker with remote administrative control of the system.

Softphones

VoIP softphones pose a unique problem. Softphone applications run on user systems (PCs, PDAs) and thus are vulnerable to malicious code attacks against data and voice applications. IT administrators must consider the possibility that an attacker may try to evade conventional PC malware protection by injecting malicious code via a VoIP softphone application.

Spam

Spam often harbors spyware and remote administration tools. Spam over Internet telephony can carry unsolicited sales calls and other nuisance messages, and programs downloaded to softphones could include hidden malware.

Call Tampering

The attacker can tamper with calls in progress; for example, he could impair the quality of the call by interjecting noise in the RTP protocol stream, or by withholding delivery of RTP packets so that conversation elements are lost. He could also delay delivery so participants encounter long periods of silence during the call.

Even this partial list of possible threats should cause IT managers to assess the risk of introducing VoIP, and to develop a policy and an implementation plan to reduce the risks using security technology at hand. With the Clavister SIP Application Layer Gateway (ALG) it is possible to curb a number of these threats.

Security and Clavister SIP Application Layer Gateway

The SIP protocol has some security issues that should be taken into consideration before implementing a VoIP solution. There are three types of security issues that the Clavister SIP Application Gateway (ALG) is addressing: Malformed SIP/SDP Message Attacks, Buffer Overflow Attacks, and Registration Hijacking Attacks. Apart from these types of attacks, the Clavister SIP ALG also supports a number of security measures that will help you make a better and more secure VoIP installation, such as Topology Hiding, Network Segmentation and Protocol Inspection.

Malformed SIP/SDP Message Attacks

The Clavister SIP ALG provides protection from malformed SIP/SDP messages, such as duplicate From and To headers or malformed Uniform Resource Identifiers (URI). In addition, the Clavister SIP ALG provides further protection by validating the parsed SIP packet. For example, the SIP ALG can validate username parameters, Fully Qualified Domain Names (FQDN), IP addresses, ports, etc. There are also controls that validate the maximum value for the MAX-FORWARD header is not compromised, that the Expires header is not invalid, etc. When detecting a malformed SIP message, the Clavister Security Gateway will inform the user sending the malformed SIP message by sending a `400 BAD Request Error` response.

Buffer Overflow Attacks

A buffer overflow is an exploit that takes advantage of a program that is waiting on a user's input. For example, suppose a program is waiting for a user to enter his or her name. Rather than enter the name, the hacker would enter an executable command that exceeds the allocated memory for the stack where the user's input will be stored. The command is usually something short. In a Linux environment, for instance, the command is typically `EXEC("sh")`, which tells the system to open a command prompt window, known as a root shell in Linux circles. Generally speaking, this often means that the attacker will gain full control of the operating system.

It is vital from a security standpoint to protect against possible buffer overflow attacks. To curb these types of attacks, the Clavister SIP ALG allocates only the required memory size and restricts each parameter to 1024 bytes. The whole size of the SIP message is also restricted to 6048 bytes and the SDP size is restricted to 4000 bytes. For this type of violation, the Clavister Security Gateway will inform the user sending the malformed SIP message by sending a `400 BAD Request Error` response.

Registration Hijacking

The type of attack known as registration hijack tries to guess the password for a valid `userid`. The Clavister SIP ALG counts the number of failure attempts for the `REGISTER` request for each user. Once the failure count reaches the maximum value, the following `REGISTER` request will be dropped and blacklisted for a period of time. This will stop anyone from trying to guess the password for a valid `userid`.

DoS Protection

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by:

- forcing the targeted computer or computers to reset, or consume its resources such that it can no longer provide its intended service; and/or,
- obstructing the communication media between the intended users and the victim so that they can no longer communicate in an adequate way.

The Clavister Security Gateway supports a number of different strategies to avoid DoS attacks and also Distributed versions, so called DDoS attacks.

Topology Hiding

Another important security aspect is topology hiding. The Clavister SIP ALG provides the ability to do this through Network Address Translation (NAT). The SIP protocol contains a lot of information about the application layer, such as IP addresses and ports. This type of information is best to keep safe.

Network Segmentation

As the VoIP network becomes a crucial part of an organization's infrastructure it is advisable to build a separate network for VoIP traffic. By using Virtual LANs (VLAN) the same segmentation can be achieved without having to build a completely new physical network. Clavister has extensive support for VLANs and offer the same functionality for these interfaces as for physical interfaces, which makes administration more easy and streamlined.

Protocol Analysis

The firewall module in the Clavister Security Gateway monitors the network level security aspects; who are communicating, from where are the data packets coming and what ports are being used. This is a very efficient perimeter defense mechanism, but the Clavister SIP ALG can do even better. Using full protocol analysis the SIP ALG can analyze the data streams for any anomalies and take action on the result.

Working with Clavister SIP Application Layer Gateway

The following section will illustrate how to configure the Clavister SIP ALG for protection against various types of threats.

The SIP ALG supports the following usage scenarios:

1. **Internal to External**
The SIP session is between a peer on the protected side of a Clavister Security Gateway and a peer which is on the external, unprotected side. Communication typically takes place across the public internet.
2. **Same Network**
A refinement of the previous scenario where two peers in a session reside on the same network.

In these scenarios the proxy server is assumed to be on the unprotected side of the Clavister Security Gateway.

SIP ALG Options

The SIP ALG comes with several options allowing you to configure it for both security, as well as easy maintenance. Table 1 below outlines the main set of options for the SIP ALG.

PARAMETER	DESCRIPTION
Maximum Session per ID	The number of simultaneous sessions that a single peer can be involved with is restricted by this value. The default number is 5.
Maximum Registration Time	The maximum time for registration with a SIP Registrar. The default value is 3600 seconds.
SIP Request-Response Timeout	The maximum time allowed for responses to SIP requests. A time-out condition occurs after this wait. The default is 180 seconds.
SIP Signal Timeout	The maximum time allowed for SIP sessions. The default value is 43200 seconds.
Data Channel Timeout	The maximum time allowed for periods with no traffic in a SIP session. A time-out condition occurs if this value is exceeded. The default value is 120 seconds.

Table 1: SIP ALG Options

For setup we will assume a scenario where there is an office with VOIP users on a private internal network and the network's topology will be hidden using NAT. This scenario is illustrated below.

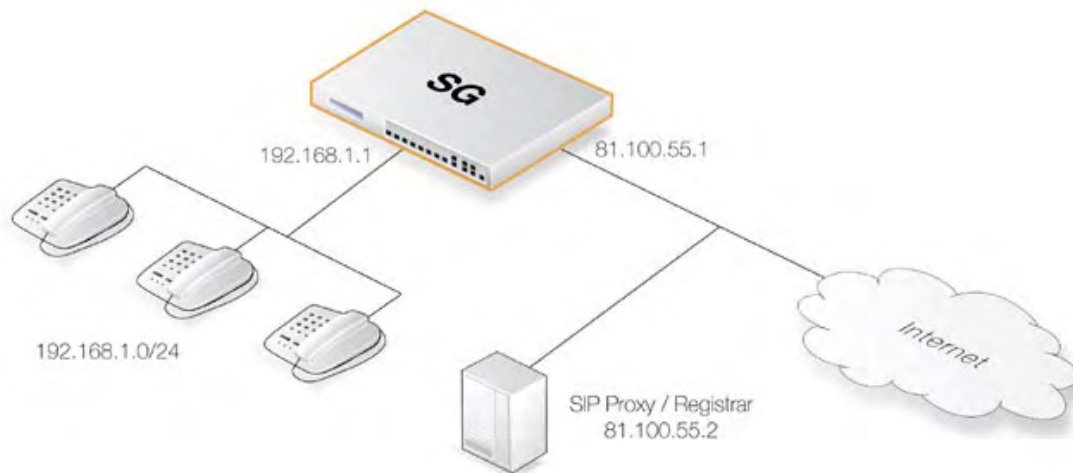


Figure 1: A Typical VoIP Setup

The SIP proxy in the above diagram could alternatively be located remotely across the Internet. The SIP proxy server should be configured with the feature Record-Route Enabled to insure all SIP traffic to and from the office peers will be sent through the SIP Proxy. This is recommended since the attack surface is minimized by allowing only SIP signaling from the SIP Proxy to enter the local network. To configure this scenario, follow these steps:

1. Define a SIP ALG object using the options described above.
2. A Service object is used for the ALG which has the above SIP ALG associated with it. The Service should have:
 - Destination Port set to 5060
 - Type set to UDP
3. Define two rules in the IP rule set:

- A NAT rule for outbound traffic from user agents on the internal network to the SIP Proxy Server located externally. The SIP ALG will take care of all address translation needed by the NAT rule. This translation will occur both on the IP level and the application level. Neither the user agents nor the proxies need to be aware that the local users are being NATed.
- An Allow rule for inbound SIP traffic from the SIP proxy to the IP of the Clavister Security Gateway. This rule will use core (in other words CorePlus itself) as the destination interface. The reason for this is due to the NAT rule above. When an incoming call is received, CorePlus will automatically locate the local receiver, perform address translation and forward SIP messages to the receiver. This will be executed based on the ALGs internal state.

A SAT rule is not needed since the ALG takes care of the mapping of the individual user IP address behind the gateway to the public internet address. When a user behind a Clavister Security Gateway registers with a SIP proxy it sends its SIP URI (to uniquely identify it) to the gateway's public IP address. When an external user then initiates a call, the SIP traffic arrives at the public IP address and the ALG performs the necessary translation to the user's internal IP address.

4. Ensure the peers are correctly configured. The SIP Proxy Server plays a key role in locating the current location of the other peer for the session. The proxy's IP address is not specified directly in the ALG. Instead its location is either entered directly into the client software used by the peer or in some cases the peer will have a way of retrieving the proxy's IP address automatically such as through DHCP.

Handling Data Traffic

The setup steps above take care of the SIP communication for establishing peer-to-peer communications. The two IP rules are always needed so that peers can access the SIP proxy but no rules are needed to handle the actual data traffic involved in, for example, a VoIP call. The SIP ALG automatically takes care of establishing the necessary objects required for allowing the data traffic to traverse the Clavister Security Gateway and these are invisible to the administrator.

Depending on the SIP environment, the Clavister SIP ALG can operate in hidden-topology environments with private IP addresses, as well as open environments with public IP addresses. SIP is a highly configurable protocol and the following describes the configuration required.

Conclusion

This Feature Brief describes how you can use the SIP Application Layer Gateway (ALG) to secure your VoIP telephony installation and how to use it with your Clavister SSP™ installation. Below are some key customer benefits:

Clavister SSP™ Key Benefits

- **Robust Security**
The purpose-built security offering from Clavister provides a complete set of security features, including Stateful Packet Inspection (SPI) firewall with DoS and DDoS protection, VPN with strong encryption, and User Authentication.
- **Rapid Deployment**
The Clavister Security Gateway provides effortless and rapid deployment. A trained technician can easily deploy and configure new network security elements within minutes, even across continents.
- **Flexible Traffic Control**
The highly sophisticated bandwidth management capabilities in the Clavister Security Gateway make it possible to not only guarantee bandwidth for business critical applications or server, but also to optimize the entire traffic flow in your network and avoid inefficient bandwidth usage.
- **Lowered Costs for Administration**
The powerful administration system that comes with Clavister Security Gateway enables organizations to lower the costs for administration through centralized management. The administration system makes it possible to deploy and configure all devices across the network, no matter if they are located next door or across the globe.
- **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 Internet Service Provider Networks, Data Centers, and telecom operators.

- Low Total Cost of Ownership (TCO)

Clavister's goal is to provide complete security solutions more cost efficiently than any competitor. Clavister SSP™ with its unique combination of integrated features, world-class service and support, and powerful administration system provide the lowest TCO and the best price/performance ratio possible.

SIP Key Benefits

- SIP ALG greatly improves the security imposed by the SIP protocol, with less risk of security breaches and attacks
- No additional hardware required since everything is included in the Clavister Security Gateway, which means lowered costs and fewer licenses

Feedback

Clavister Product Marketing is always interested in feedback from our readers. Please direct suggestions, comments or questions regarding this document to product-marketing@clavister.com. Please include the title of the document in your email.

About Clavister

Clavister - a Swedish privately owned company developing IT security products, including its award-winning Clavister Security Services Platform (SSP™). This service-oriented framework enables organizations to monitor network traffic, protecting critical business assets and blocking undesirable surfing. It will also protect you against intrusion, viruses, worms, Trojans, and overload attacks. It requires minimal servicing, with central administration, and has exceptionally flexible configuration possibilities. Its seamless scalability makes it easy to provision the perfect solution for any customer; be it small organizations, large Internet Service Providers, Managed Security Service Providers, or multimedia-ready telecom operators.

Clavister was founded 1997 in Sweden, with R&D and headquarters based in Örnsköldsvik and Sales and Marketing based in Stockholm. Its solutions are marketed and sold through International sales offices, distributors, and resellers throughout EMEA and Asia. Clavister also offers its technology to OEM manufacturers.

For more information, please visit us at www.clavister.com.

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 document 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.

Part Number: [clavister-fbr-securing_voip_using_sip](#) (0801)