

Feature Brief



RADIUS Accounting

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.

RADIUS Accounting

Clavister Security Gateway with the integrated support for RADIUS accounting is a unique high-availability, intelligent security device capable of enforce authentication and deliver accounting information to RADIUS compatible systems.

Within a network environment containing large numbers of users, it is favorable to have one central server or a cluster of central servers to maintain user account information, and to be responsible for authentication and authorization tasks. The central database resided in the dedicated server or servers contains all the user's credentials and details of connections that helps to significantly reduce the administration work for configuring the information in multiple and distributed Clavister Security Gateways.

The RADIUS protocol is widely used for handling this approach. The protocol works on a client/server architecture. The gateway acting as the clients of the RADIUS server, create and send authentication requests to the dedicated server or servers. The server receives the requests, verifies the user's information by consulting its database, and returns either an `ACCEPT` or `REJECT` decision to the requested client. This method is extended in RFC2866 to cope with the delivery of accounting information. The benefits of having centralized configuration and control is thus extended to user's connection accounting and monitoring, though it is

not necessary to have the same server work for both authentication and accounting tasks. This makes it more convenient for an administrator to gather user statistics and/or create billing information.

RADIUS accounting is similar to RADIUS authentication in the sense that it is working on a client/server basis. In this case the Clavister Security Gateway acts as a Network Access Server (NAS), which is the client responsible for generating and sending RADIUS accounting requests and receiving the responses from the RADIUS server. The designated RADIUS accounting server is responsible for receiving the accounting request, recording accounting updates in its database, and returning a response to the client indicating that it has successfully received the request.

When a session is started by a user's connection, the NAS, in this case the Clavister Security Gateway, will send an `AccountingRequest Start` packet to the RADIUS server, describing the beginning of a user's service, and the user's account information is delivered as well. The server will send back an `AccountingResponse` to the NAS acknowledging that the request packet has been received. At the end of each session, the NAS sends an `AccountingRequest Stop` packet, optionally containing statistics such as the number of packets sent/received and the lifetime of the session to the server.

This flow of communication is shown in Figure 1.

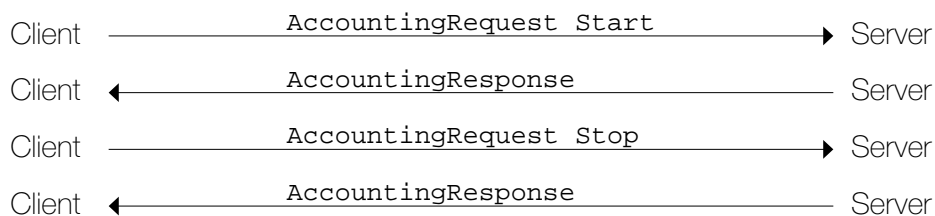


Figure 1: RADIUS Communication Flow

For security considerations all communication between the Clavister Security Gateway and the server is protected by the use of a shared secret, which is never sent over the network. From this secret, appended with the packet information, an `Authenticator` is calculated through a one-way MD5 hash function in order to authenticate accounting messages. The message is sent via UDP and the officially assigned port number is 1813.

RADIUS Accounting in Clavister Security Gateway

Clavister Security Gateway is capable of operating as a Network Access Server, being responsible for delivery of accounting transactions.

RADIUS authentication and RADIUS Accounting can be implemented on one single server or separate servers. Clavister Security Gateway support both a local user database and an external user database on one or several RADIUS servers as authentication sources. If RADIUS accounting is enabled in the Clavister Security Gateway, as soon as the Clavister Security Gateway authenticates a user via an authentication source, an `AccountingRequest Start` packet will be sent to the configured RADIUS accounting server. Alternative RADIUS servers can be configured in the Clavister Security Gateway to deal with the event when the primary server is unreachable.

When the user is no longer authenticated, for example, the user logs out or the session time expires, an `AccountingRequest Stop` packet will be sent by the Clavister Security Gateway, containing session statistics. The information included in the statistics is user configurable. Available options are the number of bytes sent/received, the number of packets sent/received, and the number of seconds the user's session lasted.

RADIUS Interim Accounting

The Clavister Security Gateway can periodically send interim accounting messages, to update the accounting server of the current status of an authenticated user. An interim accounting message can be seen as a snapshot of the network resources that the authenticated user has used up until now. It is for example possible to see how many bytes and packet an authenticated user has send and received up until this moment.

An interim accounting message contains the current values of the statistics for an authenticated user. It contains more or less the same parameters as found in an `AccountingRequest Stop` message, except that the disconnect-reason is not included (as the user has not disconnected yet).

The interval in which to send interim accounting messages can be specified either on the authentication server, or on the Clavister Security Gateway. A setting on the Clavister Security Gateway will override a setting on the accounting server.

Interim accounting is a very useful way of ensuring that accounting information is provided continuously to the service provider whose customers might be connected over an extensive period of time.

RADIUS Accounting Scenario

This scenario demonstrates how the Clavister Security Gateway could be used by an Internet Service Provider (ISP) to deliver secure and reliable internet access without having to add separate authentication or accounting gateways.

In this case the Clavister Security Gateway is place centrally in the network between the wireless access points and the internet connection.

The user in this case login to the network by entering his account information found on a voucher into the HTTP/HTTPS login interface provided by the Clavister Security Gateway. The login data is then passed from the Clavister Security Gateway to the RADIUS authentication and accounting server which responds by sending back a permit or deny message to the Clavister Security Gateway.

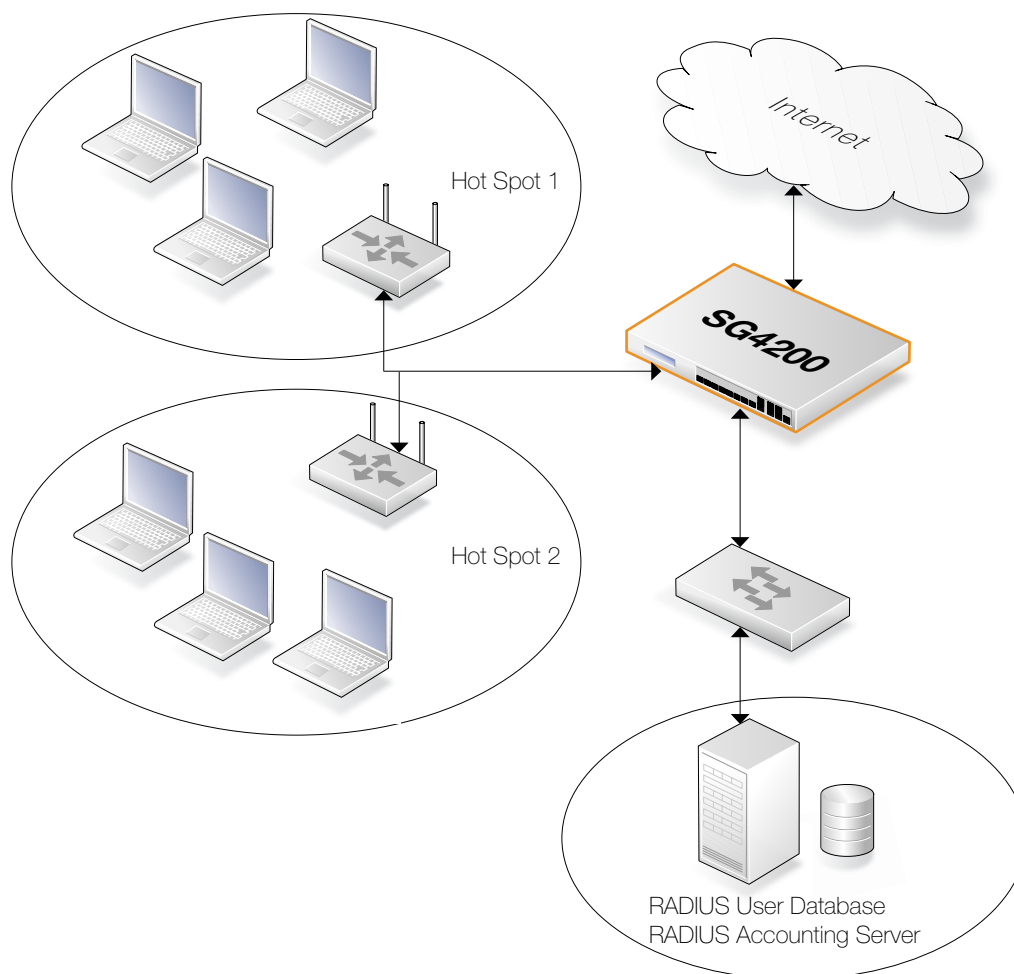


Figure 2: RADIUS Accounting Example

Once the client is authenticated, the client's traffic is allowed to pass through the Clavister Security Gateway based on the security policies configured.

When the client chooses to log out or if the session time expires, the Clavister Security Gateway sends, to the RADIUS accounting server, an `AccountingRequest Stop` packet which includes statistical information such as bytes and packets sent/received and session time.

The statistical information sent to the RADIUS accounting server can then be used for billing or statistical purposes.

Conclusion

This Feature Brief describes RADIUS Accounting 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.

RADIUS Accounting Key Benefits

- Efficient integration into existing RADIUS infrastructure
- No need for additional access control equipment
- Centralized enforcement of access control, accounting data and security policies
- Tested and proven interoperability with leading billing systems ensures rapid deployment and reliable service

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 Örnköldsvik 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-radius_accounting \(0801\)](#)