

Feature Brief



RADIUS Authentication

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.

Introduction

There is a strong need to authenticate users, both internal users and external users, before they get access to network services. There are a number of different authentication methods that can accommodate this; Public Key Infrastructure (PKI), X.509, Pre-Shared Key (PSK), XAUTH and Remote Authentication Dial-in User Service (RADIUS). PKI and X.509 are common ways of authenticate users and firewalls, but XAUTH and RADIUS are gaining popularity, especially in large public networks, such as schools and municipal environments. One benefit with these protocols is that they do not need any configuration of the users device. This lowers administration cost and enables easier roll-out.

The RADIUS protocol is widely used for handling this approach. The protocol works on a client/server architecture. The Clavister Security Gateway acting as the clients of the RADIUS server, creates and sends 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. For more information on RADIUS accounting, see **Feature Brief: RADIUS Accounting**.

RADIUS Authentication

To authenticate a user using the RADIUS protocol, the Clavister Security Gateway act as a RADIUS proxy and communicates with configured RADIUS server. The Clavister Security Gateway is configured as a client towards the RADIUS server. They share a *shared secret* to prove the authenticity of the RADIUS requests and responses. The string can contain up to 100 characters and is case sensitive.

RADIUS uses PPP to transfer username/password requests between client and RADIUS server, as well as using PPP authentication schemes such as PAP and CHAP. RADIUS messages are sent as UDP messages via UDP port 1812.

These user authentication servers are connected to the organizations directory service, for example Microsoft Active Directory or Novell eDirectory. You then configure which users that must authenticate before they can gain access to specific internal services, such as mail or sales system.

In Figure 1 below you can see how a user can get different routing paths depending on type of authentication or type of device.

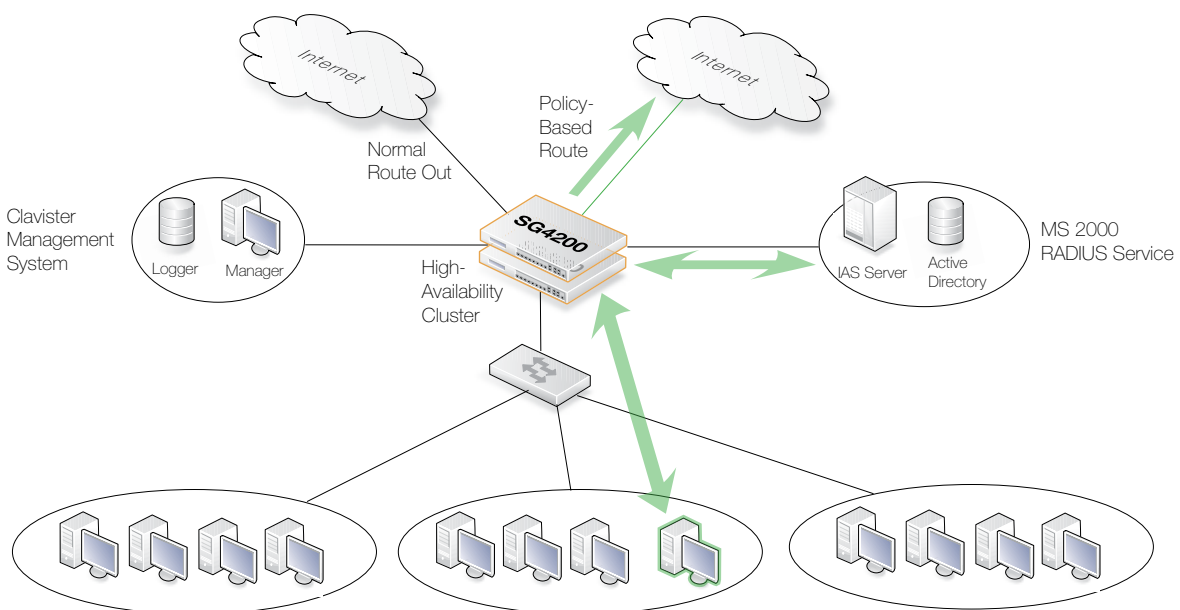


Figure 1: System Setup

Configuring an User Authentication Server

You configure an User Authentication Server in your Clavister Security Gateway by defining the following parameters:

- Name
The name of the server.
- Type
In this case it will be RADIUS.
- IP Address
The IP address for the RADIUS server.
- Port

For RADIUS it is port 1812.

- **Shared Secret**
The shared secret that act as a level of trust between the Clavister Security Gateway and the RADIUS server. Note that you have to enter the shared secret twice for verification.
- **Routing Table**
You also specifies which routing table that should be used.

Configuring a User Authentication Rule

You need to configure user authentication rules for allow traffic to go through only when users are authenticated. Authentication rules are set up in a way that is similar to other Clavister CorePlus™ security policies, by specifying which traffic is to be subject to the rule. Authentication rules differs from other policies in that the destination network/interface is irrelevant, so only the source network/interface needs to be specified. An Authentication Rule has the following parameters:

- **Interface** - The source interface on which the connections to be authenticated will arrive.
- **Source IP** - The source network from which these connections will arrive.
- **Authentication Source** - This specifies that authentication is to be done against a local database defined within Clavister CorePlus™ or by using a RADIUS server. It is also possible to specify **Disallow**, which means that the rule is configured to never authenticate under these conditions. Sometimes it is convenient to say no one should be authenticated from a particular interface. It is usually used as the last rule in a list.
- **Agent** - The type of traffic being authenticated.

Agents can be on of the following types:

- **HTTP or HTTPS** - Web connections to be authenticated via a pre-defined or custom web page.
- **PPP - L2TP or PPP tunnel authentication.**
- **XAUTH** - IKE authentication, part of IPsec.

Connection Time-Outs

In the authentication rule you can also specify time-outs settings related to the users session:

- **Idle Time-out** - How long a connection is idle before being automatically terminated. 1800 seconds is set by default.
- **Session Time-out** - The maximum time that a connection can exist in seconds. No value is specified by default.

If an authentication server is being used, then the option **Use Timeouts Received From the Authentication Server** can be enabled to have these values set from the authentication server.

Multiple Login

An authentication rule can specify how multiple login are handled where more than one user from different source IP addresses try to login with the same username. The possible options are:

- Allow multiple login so that more than one client can use the same username/password combination.
- Allow only one login per username.
- Allow one login per username and logout an existing user with the same name if they have been idle for a specific length of time when the new login occurs.

Customizing Authentication HTML Pages

The local installation directory on the management workstation contains a folder called `HTTPAuth HTML Root`. This contains a subfolder called `samples` which contains the default HTML pages used for authentication. These files are also known as banner files. To customize these pages:

1. Create a new folder under `HTTPAuth HTML Root`. This folder can be given any name, in this description lets call it `CustomizedHTML`.
2. Make a copy in `CustomizedHTML` of all the default HTML files in `samples`.
3. Make the required changes to the files in `CustomizedHTML`. Only the presentation should be changed. No changes should be made to the variables names used in the files.
4. Start Clavister FineTune™. Go to Agent Options tab for the relevant Authentication Rule. It will now be possible to select `CustomizedHTML` from the HTML Directory dropdown options.
5. Upload the new banner files to the Clavister Security Gateway through the menu Action > Communication > Upload HTML Banner Files in Clavister FineTune™.
6. The final step is to issue a `configure` command from the remote console.

Operations

Clavister Security Gateway is set up for communication with an existing RADIUS server and will then generate RADIUS requests towards the configured RADIUS server, which, in response, will rely RADIUS responses from the directory services. If the users credentials match those stored in the directory service, the network traffic will be allowed in accordance with the user profile stored in the directory service.

User Login and Logout

When a user need to access a protected service, for example a mail server, the user enters the URL in a standard Web browser. Since the service is protected, the user is prompted with a HTML-page asking for the users credentials. Login out is equally simple; the users just click Logout from the same Web page.

Conclusion

This Feature Brief describes RADIUS Authentication 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 Authentication 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
- Customizable HTML pages for localized and branded login and logout pages

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_authentication](#) (0808)