

Feature Brief



PCAP Recording

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

Every network technician needs the ability to investigate and troubleshoot the network from time to time. You can either use it as a diagnostic tool to investigate problems, but it is also an excellent tool to use for investigating traffic in your network as an aid when writing rules.

Clavister security Gateway has a build-in tool for this purpose; the *pcapdump* console command tool. This command tool enables network technicians to capture and store network traffic to and from the Clavister Security Gateway, with support for filtering. It also supports the industry standard file format .cap so you can take the result to an external tool, such as Wireshark for further processing.

Using *pcapdump*

It is easy to use the *pcapdump* tool. You execute the commands from the Clavister Security Gateway console and the result is either shown in the console or capture to the specified disk file.

Configuring *pcapdump*

The *pcapdump* tool is configured from the console using a command-line interface (CLI). Table 1 below shows the available commands:

COMMAND	DESCRIPTION
-size <size>	The size of the buffer in kilobyte (kb) where the captured packets are stored in memory. The default value is 512 KB.
-s <snaplen>	The maximum length of each packet to capture expressed in bytes.
-c <count>	The number of packets to capture.
-o	Realtime packet brief dumped to the console.
-ou	Unbuffered realtime packet brief dumped to the console. Unbuffered packets are not stored in memory.
-p	Sets the interface in promiscuous mode. This allows a network device to intercept and read each network packet that arrives in its entirety.
[filterexpr]	Use the filter expression to filter traffic to and from the Clavister Security Gateway. For more information, see section Filtering below.
eth [addr]	Use this to filter on source or destination MAC address.
ethsrc [addr]	Use this to filter on a source MAC address only.
ethdest [addr]	Use this to filter on a destination MAC address only.
ip [addr]	Use this to filter on source and destination IP address.
ipsrc [addr]	Use this to filter on a source IP address only.
ipdest [addr]	Use this to filter on a destination IP address only.
port [num]	Use this to filter on source or destination port number.
srcport [num]	Use this to filter on a source port number only.
destport [num]	Use this to filter on a destination port number only.
proto [id]	Use this to filter on a specific protocol where id is a decimal protocol id number. It is also possible to use pre-defined alias for common protocol. The available aliases are: TCP, UDP and ICMP.
start [interface]	The start command starts the capturing on a specified interface [interface].
stop [interface]	The stop command stops the capturing on a specified interface [interface].
status	The status command show the capture status.
show [interface]	The show command shows the captured packets brief from the specified interface [interface].
write [interface] [filename]	The write command writes the captured packets from the specified interface [interface] to a specified file name [filename].
wipe	The wipe command removes all captured packets from memory.
cleanup	The cleanup command removes all captured packets from memory, releases the capture mode and delete all written capture files from the disk.

Table 1: *pcapdump* Commands

NOTE: File name must not exceed 8+3 characters and no spaces.

Filtering

A single Clavister Security Gateway can generate a lot of traffic which makes it harder to diagnose the captured result. But it is easy to set up filters to only capture traffic that are relevant to you. It is also possible to combine filters, for example if you are interested in traffic going to a particular destination port at a particular IP address. Note that the order of the filter expressions are not important.

Below are some examples of different filter expressions.

- This command starts the capturing on the int interface using a 1 MB buffer. The filter is set up to capture only traffic from IP source address 192.168.0.1.

```
> pcapdump -size 1024 ipsrc 192.168.0.1 start int
```

- This command is similar to the previous one, except it uses a combined filter to only capture TCP traffic from IP source address 192.168.0.1. Note that there is no need to use of filter expression keyword `proto` before the protocol ID number if you are using the built-in aliases; TCP, UDP and ICMP.

```
> pcapdump -size 1024 ipsrc 192.168.0.1 tcp start int
```

- This command extends the previous one by also capture traffic to IP destination address 192.168.0.1 and only traffic originating using protocol 103, which is Protocol Independent Multicast (PIM). Note the use of filter expression keyword `proto` before the protocol ID number.

```
> pcapdump -size 1024 ipsrc 192.168.0.1 ipdest 10.0.0.1 proto 103 start int
```

These examples gives you a glimpse on the how to set up your filtering to capture only the relevant traffic to make it easier to interpret the result.

Examples

The following is an example on how to use *pcapdump* to examine packets going to and from your Clavister Security Gateway. In this example we specifies a 2 MB buffer and start the capturing on interface int. We then issue the stop command on interface int, and with the show command we dump the captured data to the console. This is displayed in summarized form. The same data is then written to the specified file, which we named `capture.cap`. We then clean up after us with the clean command. This command frees our allocated memory buffer, release the capture mode and deletes all capture files from the disk.

```
> pcapdump -size 2048 start int
> pcapdump stop int
> pcapdump show
> pcapdump write int capture.cap
> pcapdump clean
```

NOTE: Remember to save your capture files to you local workstation before issuing the `clean` command. For more information on how to save your capture files, see section [Download Capture Files](#)

The example shows how configure *pcapdump* to set the Clavister Security Gateway in promiscuous mode, capture 20 packets from IP source 192.168.0.1 and IP destination 10.0.0.1 and only protocol 103. When start the capturing on interface int. The size of the buffer is not defined so *pcapdump* will use the default 512 KB. We then stop the capturing on interface int and dump the captured 20 packets to the console. We then clear up the buffer using the wipe command.

```
> pcapdump -p -c 20 ipsrc 192.168.0.1 ipdest 10.0.0.1 proto 103 start int
> pcapdump stop int
> pcapdump show
> pcapdump wipe
```

Packet Sizes

By using the `-s <snaplen>` switch it is possible to specify how much of the packet you are going to capture. If you are only interested in the first 64 bytes of a packet, it is a waste of buffer memory to capture the whole packet. By specifying the packet capture length you will only get the first 64 bytes of each packet. In the following example we specify that we only like to capture the first 64 bytes of TCP traffic.

```
> pcapdump -s 64 ipsrc 192.168.0.1 ipdest 10.0.0.1 tcp start int
> pcapdump stop int
> pcapdump show
> pcapdump wipe
```

Troubleshooting Network Traffic

It is also possible to use the `pcapdump` command to aid in the creation of new, more specific security policies. Lets say that you have a user that is trying to print a document on a printer located in the Sales department. The user is located on the internal network, but the printer in the Sales department is located on another interface in the Clavister Security Gateway. Here is an excellent opportunity to use `pcapdump`. Ask the user to try to print the document again and this time you set up `pcapdump` to record the traffic. Save the traffic data and analyze it. Based on the information from the recording, you can now construct a correct and exact security policy. Without `pcapdump` you would have had to resort to tedious trail-and-error tests or even worse, create a very broad security policy that allow far more traffic than you want to between the different departments.

This shows the benefits of using `pcapdump` to identify troublesome traffic or traffic that does not get through, and it also show how to make exact and "narrow" security policies that serves its purpose without opening up more than you need.

Hopefully these examples have shown a bit of what you can do with `pcapdump` and how you can use it to investigate and troubleshoot your network.

Download Capture Files

Once the captured data has been written to a file on the Clavister Security Gateway and before you execute the `pcapdump cleanup` command, you should download the capture file to a local workstation. Use the console command-line tool `fwctl` to download the file.

```
> fwctl --filedownload <source_filename> <destination_filename> <gateway>
```

The `<source_filename>` parameter is the name of the capture file specified in the `pcapdump` command. It should use the `.cap` file extension. The `<destination_filename>` parameter is the name of the destination file on the local disk. The `<gateway>` parameter identifies a specific Clavister Security Gateway from which to download the capture file. The parameter is specified as `<data-source:gateway-name>`, which is required to uniquely identify which Clavister Security Gateway to download from.

The following example show how to download the file `remote.cap` to the file `local.cap` from a Clavister Security Gateway identified as `mydatasource:mygateway`.

```
> fwctl --filedownload remote.cap local.cap mydatasource:mygateway
```

More information about the `fwctl` console command can be found in Appendix C - `fwctl` Command Options in the Clavister CorePlus™ Administration Manual.

Further Explorations

The industry standard file format `.cap` is used by `pcapdump`. This makes it easy to use external tools to further examine the captured data. For example, you can open your saved capture files using Wireshark (née Ethereal) and do some more elaborate examinations. You can find out more about Wireshark at www.wireshark.org.

Conclusion

This Feature Brief describes how to use `pcapdump` to troubleshoot your network 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.

pcapdump Key Benefits

- Excellent aid in both investigating network traffic when writing rules and for troubleshooting network problems.
- Filtering on source and destination addresses, ports and protocols makes it easier to capture relevant data.
- Industry standard output file format, `.cap` makes it easy to use external tools for further processing.

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-pcap_recording (0801)