Anti-Virus

Clavister Technology Spotlight

Key Benefits

- Multi-layered security
- Stream-based anti-virus scanning, eliminating the need for full file proxying
- No size limitation of files being scanned
- Virtually no limitation in number of simultaneous files being scanned
- High-speed throughput
- Efficient perimeter defense against the most dangerous virus outbreaks

Introducing

Computer viruses are one of the most publicized and feared network attacks an organization can encounter. In matter of seconds, an organizations network can be infected and brought to a standstill. The cost for an infected organization runs in the millions of dollars and possible lost of both customers and goodwill. For this reason it is vital to have an ironclad antivirus solution that deters any attempts before it gets a change to spread.

Two common methods are used to detect viruses. The first, and by far the most common method of virus detection, is using a list of virus signature definitions. The disadvantage of this detection method is that users are only protected from viruses that pre-date their last virus definition update. The second method uses a heuristic algorithm to find viruses based on common behaviors. This method has the ability to detect viruses that anti-virus security firms' have yet to create a signature for.

Clavister Extended Unified Threat Management

Clavister Anti-Virus is part of the Clavister Extended Unified Threat Management (xUTM) solution that provides best-in-breed Intrusion Detection & Prevention (IDP), Web Content Filtering (WCF), Anti-Virus and Anti-Phishing. The converged security solution provides your IT department with a comprehensive toolbox which is easy to use, low on maintenance and scales as you grow. All components in the Clavister xUTM solution are built to lower your maintenance as it increases the productivity within your company.

Clavister Service Provisioning Network

The Clavister Service Provisioning Network (CSPN) is a global network of secure and high performance servers managed by Clavister that ensures fast, accurate and safe delivery of Intrusion Detection & Prevention (IDP) and Clavister Anti-Virus signatures, as well as classification databases for the managed Web Content Filtering (WCF) services. The CSPN is the backbone in Clavister Zero-Day Protection (CZDP).

Clavister Anti-Virus

Clavister Anti-Virus protects against malicious code carried in file downloads, unlike Intrusion Detection & Prevention (IDP), which is primarily directed at attacks against servers. Files may be downloaded as part of a Web page in an HTTP transfer, in an FTP download, or as an attachment to an email delivered through SMTP. Malicious code in such downloads can have different intents ranging from programs that merely cause annoyance to more sinister aims such as sending back passwords, credit card numbers and other sensitive information. The term "virus" is used here as a generic description for all forms of malicious code carried in files, including Trojans, worms and other malware .

Clavister Anti-Virus supports a unique stream-based anti-virus feature that is able to keep you protected against "in-the-wild" viruses by scanning files regardless of file sizes and supports thousands of concurrent downloads. Virus definition files from Kaspersky Lab are automatically provided by the Clavister Service Provisioning Network (CSPN). With this service you get access to the latest Clavister Anti-Virus Safestream Signatures. The signatures are then provided automatically to your Clavister Security Gateway to ensure the highest level of security and speed of delivery.

Subscribing to the Clavister Anti-Virus Service

The Clavister Anti-Virus feature is purchased as a renewable subscription. The Clavister Anti-Virus subscription includes regular updates of the virus signature database during the subscription period with signatures of the latest virus threats.

To subscribe to the Clavister Anti-Virus service, please contact your local Clavister Sales Representative, or visit us at: www.clavister.com for more information.

Real-Time, Stream-Based Anti-Virus

Clavister Anti-Virus Signatures are designed to detect the most dangerous viruses at wire speed, with only a minimal latency. Also, there is basically no limitation to the number of files that can be scanned or the size of the files being scanned. This stream-based approach is very different from the solutions where the entire file first need to be downloaded before it is being scanned. Non-stream-based solutions are often very limited and often a majority of the files are not scanned or even worse, the entire anti-virus functionality is turned off because of user complaints.

The Clavister Anti-Virus also supports the Clavister xPerformance Cards. This hardware acceleration gives the stream-based scanning ultimate performance where traditional anti-virus software is not able to perform due to limitations in architecture, processing power or memory.

NOTE: Anti-Virus scanning performance, like IDP scanning performance, can be increased with an optional hardware acceleration upgrade on the SG50, SG4200 and SG4400 Security Gateways. Multiple streams are accelerated asynchronously in this optional hardware to boost overall throughput. The console command `hwaccel` can be used to check if acceleration is installed.

The Signature Database

Clavister Anti-Virus uses the "SafeStream" virus signature database, which is created and maintained by Kaspersky Labs, a world leader in the field of virus detection. The signature database includes records for malicious code that is known to currently propagate over networks or that is active "in-the-wild". The list of malicious programs is continuously updated based on data gathered by Kaspersky Lab network sensors and the Kaspersky Virus Lab. The database is also thoroughly tested to provide near-zero false positives, e.g. wrongly classifying an innocuous file as a virus.

Database Updates

The virus signature database is updated on a daily basis with new virus signatures. Older signatures are seldom retired but instead are replaced with more generic signatures covering several viruses. The local Clavister CorePlus™ copy of the virus signature database should therefore be updated regularly and this updating service is enabled as part of the subscription to the Clavister Anti-Virus subscription.

Thanks to the highly unique combination of component-based signatures and the CSPN provisioning network, you are protected against new and unknown attacks. More importantly, it is also capable of blocking variations of existing attacks without introducing false positives.

Combining with Client Anti-Virus Scanning

Clavister Anti-Virus scanning is designed to be a compliment to the standard virus scanning normally carried out locally by specialized software installed on client computers.

Clavister Anti-Virus at Work

Association with an ALG

Activation of Clavister Anti-Virus scanning is achieved through an Application Layer Gateway (ALG) associated with the targeted protocol. For example, if you create an HTTP ALG and enable Clavister Anti-Virus, you will be able to scan HTTP downloads. The ALG must then be associated with a given Service which in turn is used by a particular rule defined in the IP Rule Set.

Creating Anti-Virus Policies

Since IP Rule Set rules are the means by which the Clavister Anti-Virus feature is deployed, the deployment can be policy-based. IP rules can specify that the ALG and its associated Clavister Anti-Virus scanning can be applied to traffic going in a given direction and between specific source and destination IP addresses and/or networks. It is also possible to set up scheduled virus scanning that take place only at specific times.

Streaming and Inspecting

When a file, which can be documents, images, videos, scripts and similar, is transferred through the Clavister Security Gateway, the Clavister Anti-Virus will scan the data stream for the presence of viruses. Since files are being streamed and not read completely into memory, a minimum amount of gateway memory is required and there is minimal effect on overall throughput.

The inspection process is based on pattern matching against the virus signature database of known virus patterns. The Clavister Anti-Virus can determine if a virus is in the process of being downloaded to a user. Once a virus is recognized, the download is terminated before it is completed.

Types of Files Scanned

The Clavister Anti-Virus is able to scan the following types of downloads:

- HTTP, FTP or SMTP file downloads
- Any uncompressed file type transferred through these protocols
- ZIP, Deflate and GZIP compressed file types transferred through these protocols

The administrator has the option to always drop specific files as well as the option to specify a size limit on scanned files. If no size limit is specified then there is no default upper limit on file sizes.

When scanning compressed files, Clavister Anti-Virus must apply decompression to examine the file's contents. Some types of data can result in very high compression ratios where the compressed file is a small fraction of the original uncompressed file size. This can mean that a comparatively small compressed file attachment might need to be uncompressed into a much larger file which can place an excessive load on resources and noticeably slowdown throughput.

To prevent this situation, the administrator could specify a Compression Ratio Limit. Setting this limit to 10 means that if the uncompressed file expands beyond 10 times than the compressed file a specified Action should be taken. The configurable Action's can be one of:

- Allow - The file is allowed through without virus scanning
- Scan - Scan the file for viruses as normal
- Drop - Drop the file

In all three of the above cases the event is logged.

Certain file types can also be explicitly excluded from scanning if so desired. This can increase overall throughput if an excluded file type is a type which is commonly encountered in a particular scenario. For example, a file might be identified as being of type .gif and therefore should contain image data of that type. However, some viruses can try to hide inside files by using a misleading file type. A file might pretend to be a .gif file but the file's data will not match that type's data pattern because it is infected with a virus. Clavister Anti-Virus can check that the file's content matches the MIME type it claims to be. Enabling MIME type checking is strongly advised.

Simultaneous Scans

There is no fixed limit on how many Clavister Anti-Virus scans can take place simultaneously on a single Clavister Security Gateway. However, the available free memory can place a limit on the number of concurrent scans that can be initiated. The administrator can increase the default amount of free memory made available to the Clavister Anti-Virus scanning through changing the parameter `AVSE _ MAXMEMORY` in Clavister FineTune Advanced Setting. This setting specifies what percentage of total memory is to be used for the Clavister Anti-Virus scanning.

Protocol Specific Behavior

Since the Clavister Anti-Virus scanning is implemented through an Application Level Gateway (ALG), specific protocol specific features are implemented in Clavister CorePlus™. For example, FTP scanning is aware of the dual control and data transfer channels that are opened and can send a request via the control connection to stop a download if a virus in the download is detected.

Example: Enabling Anti-Virus Scanning

In this example we want to setup an Anti-Virus scanning policy for HTTP traffic from `lannet` to `all-nets`. We will assume there is already a NAT rule defined in the IP rule set to handle this type of traffic. Please follow the instructions below to complete this example.

1. Start your Clavister FineTune application, if it is not already started, and select the Security Editor from the Tools menu.
2. Right-click on the Security Gateway you want to edit. This will bring up the contextual menu. Select Version Control > Check Out. You can also select the Security Gateway and use Ctrl-O.
3. Expand the Security Gateway by clicking on the + (plus) sign. Expand the Local Object folder by clicking on the + (plus) sign.
4. Right-click on the Application Layer Gateways icon to bring up the contextual menu and select New Application Layer Gateway.... You can also select the Application Layer Gateways icon and use Ctrl-N.
5. The Application Layer Gateway Properties dialog is shown. Select the Application Layer Gateway tab and enter the following information:

```
Name: anti _ virus
Type: HTTP
```

6. Click the Parameters button to bring up the HTTP Application Layer Gateway Properties. Select the Antivirus tab and enter the following information:

```
Mode: Enabled
```

7. Click OK twice to accept all changes.
8. Next you need to create a Service object using the newly created HTTP ALG. Make sure the Local Objects folder is expanded. Right-click on the Services icon to bring up the contextual menu and select New Service.... You can also select the Service icon and use Ctrl-N.
9. The Service Properties dialog is shown. Select the Service tab and enter the following information:

```
Name: http _ anti _ virus
Type: TCP
ALG: anti _ virus
```

10. Select the TCP/UDP Parameters tab and enter the following information:

```
Destination Port: 80
```

11. Click OK to accept all changes.
12. Finally, you need to modify the NAT rule to use the newly created Service. Select the Rules icon to show all defined rules. Double-click the NAT rule handling the HTTP traffic between `lannet` and `all-nets`.

NOTE: If you do not see any rules labeled `lannet` and `all-nets`, do worry. This is just an example. If you do not have rules you can create a dummy rule just to complete this example.

13. The Rules Properties dialog is shown. Select the Service tab and click on the Pre-defined radio button to enable the dropdown list. Select the newly created pre-defined service:

```
Pre-defined: http _ anti _ virus
```

14. Click OK to accept all changes.

Clavister Anti-Virus scanning is now activated for all Web traffic from `lannet` to `all-nets`.

Clavister xUTM Licensing

All Clavister xUTM services, including Anti-Virus are licensed on a per Clavister Security Gateway basis. This means that you buy one license per Clavister Security Gateway regardless of how many connections or users that use the service. This makes it easy to budget and monitor costs compared to some vendors who prefer to license comparable service on a per user basis.

Conclusion

This Feature Brief describes Clavister Anti-Virus and how to use them with your Clavister SSP™ installation. Below are some key customer benefits:

Clavister Anti-Virus Key Benefits

- Multi-layered security
- Stream-based anti-virus scanning, with no requirement for full file proxying
- No limitation in the size of the files being scanned
- Virtually no limitation in the number of simultaneous files being scanned
- High-speed throughput
- Compatible with the Clavister xPerformance accelerator cards
- Efficient perimeter defense against the most dangerous virus outbreaks

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

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.

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.

About Clavister

For over a decade, Clavister has been delivering leading network security solutions, providing commercial advantage to businesses worldwide. The Clavister family of Carrier Telecom Security Systems, unified threat management (UTM) appliances and remote access solutions provide innovative and flexible network security with world-class management and control. Clavister is a recognized pioneer in virtualization and cloud security. This compliments its portfolio of hardware appliances delivering customers the ultimate choice of network security products. Clavister products are backed by Clavister's award-winning support, maintenance and training program. Clavister boasts an unprecedented track record in pioneering network security solutions including the two largest deployments of Virtual Security Gateways in the world to date.

Clavister's solutions are sold through International sales offices, distributors, and resellers throughout EMEA and Asia.

To learn more, visit www.clavister.com.

Clavister Contact Information

Sales Offices
www.clavister.com/about-us/contact-us/worldwide-offices

General Contact Form
www.clavister.com/about-us/contact-us/contact-form

CID: clavister-tns-anti-virus (2011/02)

WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com