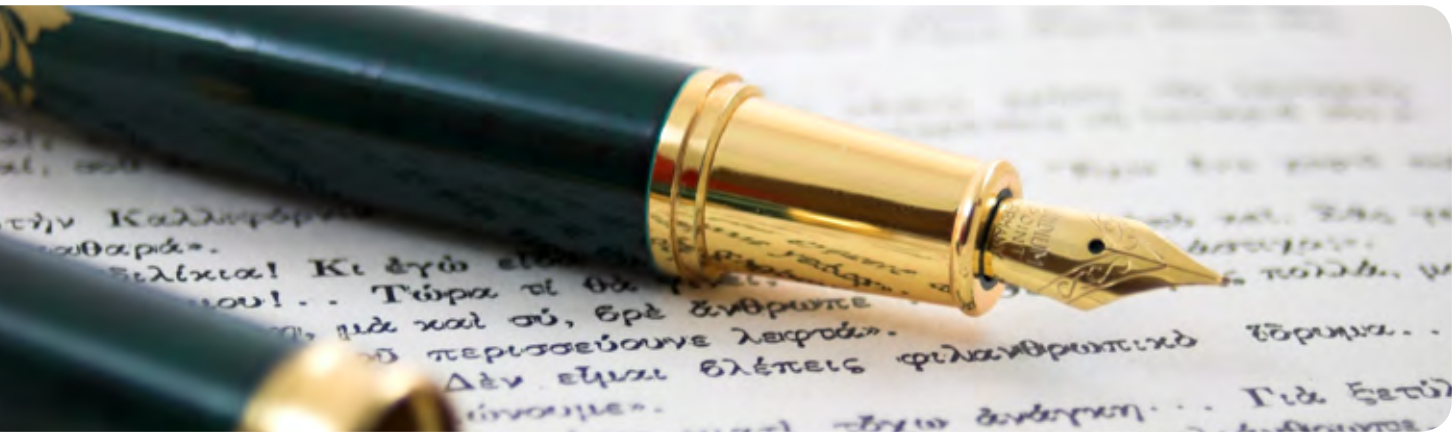

Intrusion Detection and Prevention

Clavister Technology Spotlight

Key Benefits

- **Protects the network against application-driven attacks that traditional firewall can not detect**
- **Increases productivity by blocking Peer-to-Peer (P2P) and Instant Messaging (IM) applications**
- **Decreases risk of information leakage through the use of P2P and IM applications**
- **Reduces the risk for copyrighted material being downloaded through P2P and IM applications**
- **Provides a robust and pro-active protection against zero-day attacks using component- based signatures**
- **Minimal latency and performance degradation thanks to the highly optimized Clavister engine**

Introducing

Organizations today are experiencing more intrusion attacks than ever. The attacks are more refined, more vicious and more organized then they where only two years ago. Not confined to the sole hacker anymore; these attacks are organized and coordinated like modern business organizations.

Organizations must trust their information security systems to protect their information from these serious threats. Failure could result in significant financial losses and in some cases, even bankruptcies. This makes the selection and implementation of security solutions that prevent intrusion attacks and malware threats a strategic requirement. This document is intended to assist you in understanding how Clavister Intrusion Detection & Prevention (IDP) works and the benefits it bring to your organization.

Every network has malicious traffic in it. This traffic could be generated by someone outside the organization trying to unlawfully gain information or it could be a disgruntled employee on the inside looking to cause havoc. Regardless who it is, you want to know and do something about it. This is where Clavister IDP comes in. The Clavister IDP solution will prevent the attack, collect data about the attack and inform you about the attack. This enables you to go back and do some forensic analysis using a Security Information Event Management (SIEM) solution.

Intrusion Detection and Prevention

Intrusions differ from viruses in that a virus is normally contained in a single file download and this is normally downloaded to a client system. An intrusion manifests itself as a malicious pattern of internet data aimed at bypassing server security mechanisms. Intrusions are not uncommon and they can constantly evolve as their creation can be automated by the attacker.

One of the critical aspects of an IDP solution is to differentiate between the regular or good network traffic and the malicious or bad network traffic in you network. The following network traffic scenarios can be identified in terms of IDP operations.

- **Malicious Network Traffic: IDP solution incorrectly identify malicious network traffic as regular network traffic**

  This is the worst thing that can happen with an IDP solution. It means that the IDP solution failed to do its job. Failure can be attributed to many things, such as inadequate or non-comprehensive IDP mechanisms.

clavister®

WE ARE NETWORK SECURITY

- **Malicious Network Traffic: IDP solution correctly identifies malicious network traffic**
  This is the first ideal result of an IDP solution. The ability to detect malicious network traffic with speed and reliability is referred to as intrusion detection accuracy. The more accurate the IDP solution is, the more you can trust its abilities. A system must have proven accuracy before you enable it to take the necessary actions in securing your network.
- **Regular Network Traffic: IDP solution incorrectly identifies regular network traffic as malicious network traffic**
  This is often referred to as a false alarm or a false positive. This is the most troublesome and time-consuming characteristic of an IDP solutions. What happens is that the IDP solution incorrectly identifies something in normal network traffic as being an attack. This scenario is detrimental because you still need to investigate the alarm to determine if it is in fact an attack and assess any damage. This can be both time consuming and laborious, and in the end it turns out to be a false positive. Nevertheless, you need to follow up on every generated alarm to make sure. You need to tweak your IDP solution to minimize false positives.
- **Regular Network Traffic: IDP solution correctly identifies the regular network traffic**
  This is the second ideal result of an IDP solution; identifying regular network traffic for what it is – just plain ol' regular network traffic.

Given these different scenarios, we are going to focus on how Clavister IDP works and how you can utilize its powerful features to secure your network traffic from malicious threats.

Clavister Extended Unified Threat Management

Clavister Intrusion Detection & Prevention (IDP) 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 Intrusion Detection & Prevention

Clavister Intrusion Detection & Prevention (IDP) is a Clavister CorePlus module that is designed to protect against intrusion attempts. The IDP module operates by monitoring network traffic as it passes through the Clavister Security Gateway, searching for patterns that indicate an intrusion is being attempted. Once detected, Clavister CorePlus IDP takes steps to neutralize both the intrusion attempt, as well as its source.

You need to ask yourself a couple of questions before engaging the Clavister IDP module. Answers to these questions will determine how you configure the IDP module.

- **Type of Traffic to Analyze**
  You need to determine which network traffic you want to analyze.
- **Data Traffic to Search**
  You also need to determine which type of data you want the search for in that network traffic.
- **Actions to Take**
  You need to determine what kind of action that Clavister IDP should take if an intrusion attempt is detected.

Performance Considerations

Intrusion Detection & Prevention (IDP) in general is a resource-intense task and therefore it is important not to create redundant overhead by checking for too many inapplicable signatures and signature groups. Do not use the entire signature database. In fact, you will get a warning if you try to configure the entire signature database. You should also avoid using signatures and signature groups unnecessarily. Instead, use only those signatures or groups applicable to the type of traffic you are trying to protect. For instance, using `IDS_WEB*`, `IPS_WEB*`, `IDS_HTTP*` and `IPS_HTTP*` groups would be appropriate for protecting an HTTP server.

Clavister IDP traffic scanning creates an additional load on the hardware. In most cases this should not noticeably degrade performance. However, using too many signatures during scanning can make the load on the hardware unnecessarily high, adversely effecting throughput.

Clavister IDP Signatures

Clavister IDP Signatures is brought to you as a service. By subscribing to this service you get access to latest Clavister IDP Signatures, including the highly unique component-based signatures. The signatures are provided automatically to your Clavister Security Gateway through the Clavister Service Provisioning Network (CSPN), which ensures the highest level of security and speed of delivery. Most competitors rely on either open-source signatures or by writing signatures by hand. This approach is highly cumbersome and laboriously, and also error prone. These competitors are reacting to publicly known attacks and focus mainly on exploits.

Clavister is focused on security threats and delivering signatures that can prevent intrusion threats. The advanced algorithms in use together with 'human-in-the-loop' analysts, enables us to be proactive and quickly produce high quality signatures that address multiple vectors of an attack, such as infection, payload, exploit, shellcode, etc.

Our highly accurate approach enables us to use auto-generate signatures with the capability to label multiple components of the attack. When a signature component is seen in other new or mutated attacks, Clavister already has a signature capable of blocking the attack in its database. This approach makes Clavister unique and strong on Zero Day Protection and mutated attacks.

Signature Service Updates and Coverage

With the speed of new attacks on the Internet, you need a combination of a wide vision and fast signature generation. The Clavister IDP Signature service generates an average of 20 signatures per week and the current list of signatures currently exceeds 22 000 signatures. Most competitors require days or weeks to write a new signature. The process behind our signature updates enables us to generate and release validated signatures in hours and includes complete coverage on complex attacks, such as the Metasploit and CA Brightstor attacks.

Additionally, Clavister IDP Signatures cover the following categories of attacks:

- Root Level Exploit
- User Level Exploit
- Back Door Activity
- Exploit Check
- Worms & Virus'
- Back Door Check
- Denial of Service
- Policy
- Discovery
- Suspicious
- Component

Clavister IDP Components

There are several components that together form the Clavister IDP service. This section will explain each component and how they work. But first, we need to establish how packets are processed:

Initial Packet Processing

The initial order of packet processing when Clavister IDP is configured is as follows:

1. A packet arrives at the Clavister Security Gateway and Clavister CorePlus performs normal verification. If the packet is part of a new connection then it is checked against the IP rule set before being passed to the IDP module. If the packet is part of an existing connection it is passed straight to the IDP module. If the packet is not part of an existing connection or is rejected by the IP rule set, it is dropped.
2. The source and destination information of the packet is compared to the set of IDP rules defined by the administrator. If a match is found, it is passed on to the next level of IDP processing, which is pattern matching (see below). If there is no match against an IDP rule then the packet is accepted and the IDP module takes no further actions, although further actions defined in the IP rule set can be applied, for example, address translation and logging.

The following sections will explain in detail what IDP rules are and how IDP pattern matching works.

IDP Rules

An IDP rule defines what kind of traffic, or service, that the IDP module should analyze. An IDP rule is similar to an IP rule and the IDP rule is constructed like other security policy rules in Clavister CorePlus. An IDP rule specifies a given combination of source/destination and interfaces/addresses. It is also associated with a Service object, which defines which protocols to scan. But most importantly, an IDP rule specifies what type of Action to take when detecting an intrusion attempt in the traffic targeted by the IDP rule.

Insertion/Evasion Attack Prevention

Overview

When defining an IDP rule, the administrator has the option to enable or disable the ability to **Protect Against Insertion/Evasion Attack**. These forms of attacks are specifically targeting IDP systems. They exploit the fact that in a TCP/IP data transfer, the data stream must often be reassembled from smaller pieces of data because the individual pieces either arrive in the wrong order or are fragmented in some way. Insertion/Evasion attacks are designed to exploit this reassembly process.

Insertion Attacks

An insertion attack consists of inserting data into a stream so that the resulting sequence of data packets is accepted by the IDP system, but will be rejected by the targeted application. This result is two different streams of data.

For example, consider a data stream broken up into 4 packets: P1, P2, P3 and P4. The attacker might first send packets P1 and P4 to the targeted application. These will be held by both the IDP system and the application until packets P2 and P3 arrive so that reassembly process can be done. The attacker now deliberately sends two packets, P2' and P3', which will be rejected by the application but accepted by the IDP system. The IDP system is

now able to complete the reassembly process of the packets and believes it has the full data stream. The attacker now sends two further packets, P2 and P3, which will be accepted by the application which can now complete its reassembly process. This results in different data stream than that seen by the IDP system.

Clavister CorePlus automatically corrects the data stream by removing the extraneous data associated with the attack when you enable the **Protect Against Insertion/Evasion Attack** option.

Evasion Attacks

An evasion attack has a similar end-result to the insertion attack in that it also generates two different data streams, one that the IDP system sees and one that the target application sees, but it is achieved in the reverse way. It consists of sending data packets that are rejected by the IDP system but are accepted by the target application. The end result is the same; two different data streams.

Clavister CorePlus automatically corrects the data stream by removing the extraneous data associated with the attack when you enable the **Protect Against Insertion/Evasion Attack** option.

Insertion/Evasion Log Events

Insertion/Evasion attacks can generate two types of log message:

- An **Attack Detected** log message indicates that an attack has been identified and prevented.
- An **Unable to Detect** log message when Clavister CorePlus has been unable to identify a potential attack when reassembling a TCP/IP stream, although such an attack may have been present. This condition is usually caused by infrequent and unusually complex patterns of data in the stream.

Recommended Configuration

By default, insertion/evasion protection is enabled for all IDP rules and this is the recommended setting for most configurations. There are two motivations for disabling this option:

- Increasing throughput – Where the highest throughout possible is desirable, then turning the option off, can provide a slight increase in processing speed.
- Excessive False Positives – If there is evidence of an unusually high level of insertion/evasion false positives then disabling the option may be prudent while the false positive causes are investigated.

IDP Pattern Matching

Signatures

In order for the IDP module to correctly identify an attack, it uses a profile of indicators, or pattern, associated with different types of attack. These pre-defined patterns, also known as signatures, are stored in a local Clavister CorePlus database and are used by the IDP module to analyze traffic for attack patterns. Each IDP signature is designated by a unique number.

Consider the following simple attack example involving an exchange with an FTP server. An intruder might try to retrieve the password file `passwd` from an FTP server using the FTP command `RETR passwd`. A signature looking for the ASCII text strings `RETR` and `passwd` would find a match in this case, indicating a possible attack. In this example, the pattern is found in plaintext but pattern matching is done in the same way on pure binary data.

Recognizing Unknown Threats

Attackers who build new intrusions often re-use older code. This means their new attacks can appear "in-the-wild" quickly. To counter this, Clavister IDP uses an approach where the module scans for these reusable components, with pattern matching looking for building blocks rather than the entire complete code patterns. This means that "known" threats as well as new, recently released, "unknown" threats, built with re-used software components, can be protected against.

Signature Advisories

A signature advisory is an explanatory textual description of a signature. Reading a signature's advisory will help explain what the signature will search for. Due to the changing nature of the signature database, advisories are not included in Clavister documentation but instead, are available on the Clavister Web site at: www.clavister.com/securityportal/advisories/.

IDP Signature Group Types

IDP offers three types of signatures groups; each offering different levels of certainty with regard to threats:

- Intrusion Protection Signatures (IPS) – are highly accurate and a match is almost certainly an indicator of a threat. Using the **Protect** action is recommended. These signatures can detect administrative actions and security scanners.
- Intrusion Detection Signatures (IDS) – can detect events that may be intrusions. They have lower accuracy than IPS and may give some false positives. It is recommended to use the **Audit** action initially before deciding to use the **Protect** action.
- Policy Signatures – detect different types of application traffic. They can be used to block certain applications such as file sharing applications and instant messaging applications.

IDP Signature Groups

Using Groups

Usually, several lines of attacks exist for a specific protocol, and it is best to search for all of them at the same time when analyzing network traffic. To do this, signatures related to a particular protocol are grouped together. For example, all signatures that refer to the FTP protocol form a group. It is best to specify a group that relates to the traffic being searched than be concerned about individual signatures. For performance purposes, the aim should be to have Clavister CorePlus search data using the least possible number of signatures.

1. Signature Group Type

   The signature group type is one of the previously mentioned IDS, IPS or Policy Signatures.

2. Signature Group Category

   This second level of naming describes the type of application or protocol. For examples: BACKUP, DB, DNS, FTP and HTTP.

3. Signature Group Sub-Category

   The third level of naming further specifies the target of the group. This often specifies an application, for example MSSQL. The sub-category may not be necessary if the signature group type and signature group category are sufficient to specify the target, for example APP_ITUNES.

A listing of all supported IDP groupings can be found in **Clavister CorePlus Administration Manual**.

Administrating Groups

Administrating IDP signature groups is done through selecting appropriate signatures from a hierarchical tree view displaying all available signatures. This enables you to drill-down into the appropriate group sub-categories and select or deselect just the right types of signatures. First you select the IDP type, IDS, IPS or Policy Signatures. Secondly you select the category followed by the sub-category. Going down further into the tree-view will show the individual signatures in a group. These individual signatures can be turned off or on if desired so that a signature group can be changed to contain only those signatures you are interested in.

Actions

Action Options

If pattern matching recognizes an intrusion in the network traffic subject to an IDP rule, the Action associated with that rule is triggered. The administrator can associate one of three action options with an IDP rule:

- Ignore - Do nothing if an intrusion is detected and allow the connection to stay open.
- Audit - Allow the connection to stay open but log the event.
- Protect - This option drops the connection and logs the event. There is also an additional option to blacklist the source of the connection as described below.

Processing Multiple Actions

For any IDP rule, it is possible to specify multiple actions and an action type, such as **Protect** can be repeated. Each action will then have one or more signatures or signature groups associated with it. When signature matching occurs it is done in a top-down fashion, with matching for the signatures for the first action specified being done first.

IDP Blacklisting

The **Protect** option includes the option that the particular host or network that triggers the IDP rule can be added to a Blacklist of offending traffic sources. This means that all subsequent traffic coming from a blacklisted source will be automatically dropped by Clavister CorePlus.

Clavister UTM Licensing

All Clavister UTM services, including Intrusion Detection and Prevention 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 Intrusion Detection and Prevention (IDP) and how to use it to help you with your Clavister Security Gateway installation. Below are some key customer benefits.

Intrusion Detection and Prevention Key Benefits

- Protects the network against application-driven attacks that traditional firewall can not detect
- Increases productivity by being able to block applications, for example Peer-to-Peer (P2P) and Instant Messaging (IM)
- Decreases risk of information leakage through the use of P2P and IM applications
- Reduces the risk for copyrighted material being downloaded through P2P and IM applications

- Provides a robust and pro-active protection against zero-day attacks through the use of the highly unique component- based signatures
- Helps to enforce the organizations security policies by offering signatures that blocks the use of specific protocols or application functions
- Lowers the Total Cost of Ownership (TCO) by integrating best-of-breed IDP functionality in a converged and multi-purpose security gateway
- Minimal latency and performance degradation thanks to the highly optimized Clavister engine

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.

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-intrusion-detection-and-prevention (2011/09)

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