Technology Overview
Intrusion Detection and Prevention

IPS in Kerio Control

Kerio Control, a Unified Threat Management solution, incorporates a signature based packet analysis architecture known as Intrusion Detection and Prevention (IPS), which transparently monitors inbound and outbound network communication to identify suspicious activity. Depending on the severity of the activity, Kerio Control can log and block the communication. New signatures are regularly added to the rules database to defend against emerging threats.

The system is designed to protect servers behind the firewall from unauthorized connections, typically originated by an Internet bot or hacker trying to exploit an available service. The IPS is also designed to protect network users from unknowingly downloading malicious content or malware, or to mitigate the effects of a compromised system.

Server Security

In many deployments, servers are placed behind the firewall, and only those services being hosted can receive connections. Depending on the type of service hosted (e.g. SQL server) the firewall may not have the ability to inspect the actual conversation taking place between a client and the server. The firewall is primarily responsible for ensuring that the connection is established, without allowing any other type of backdoor access to other services available on the server. What this type of configuration does not address is the potential threat of a request or command that exploits a vulnerability in the server software.

Perhaps the best-known incidence of this type of attack occurred in 2001, where a worm was developed to attack systems running the web server software, Microsoft Internet and Information Server. Labeled "Code Red", the worm was programmed to send a series of commands through the HTTP service that would cause a buffer overflow in the memory space of the server software. This allowed the attacker to inject and execute arbitrary code on the server. Part of this code included the ability to rapidly redistribute itself by affecting other servers running the Microsoft IIS software. This specific attack resulted in a denial of service to the affected server.

Adding the IPS layer

Keeping server software updated is critical to protecting server applications from this type of threat. Application vendors regularly update their software to patch security vulnerabilities. In some cases however, it may not be possible to update to the latest version of the software or the vendor may not yet have a fix for an emerging threat. Adding an Intrusion Prevention System provides an extra layer of security to protect against threats such as the Code Red worm.

The IPS maintains a local database of signatures, which it uses to identify known types of attacks. Without interpreting the communication between a client and server, an IPS system can generate a signature of the network connection, and search for this signature in its local database. This type of architecture is highly effective at combating the threat of a worm or other server based attack.

Other types of server attacks include password guessing or brute force, distributed denial of service, port scans or session hijacking. These types of attacks generally involve attempts to obtain information about the server software, such as the version and developer. With this information, the attacker can research vulnerabilities in the server software and attempt to gain unauthorized access to the system, or perform malicious actions to prevent the server from properly functioning. In all of these cases, the IPS will notify the administrator of this suspicious activity, and block any communication if it is known to cause harm to those servers protected by the firewall.

Mitigating the effects of Trojans, Worms, Spyware and other Malware

Aside from the exploitation of available services to vulnerable applications, there are other ways to exploit an operating system. One of the more common approaches used by an attacker is to piggyback an application on top of free software. The user is deceived into installing malware through the installation of another application, or by simply accessing a website which runs a client side script to install the malware. These types of applications may not be apparent to the user, but can be programmed to expose sensitive corporate information found on the infected computer. They can also degrade the performance of a computer, or cause other applications to fail. As these programs may appear to be legitimately installed, they may not be identified by Anti-Virus software.

An Intrusion Prevention System is instrumental in identifying systems that are infected by these types of applications. The IPS can identify that the user is inadvertently attempting to download an unwanted application and can close the connection, preventing the file from successfully reaching the end user's computer. In case a previously infected computer is brought onto the network, the IPS can also identify and block the activity of the installed malware. The IPS in Kerio Control thus works in tandem with the firewall and content filtering capabilities to prevent the spread of malware on the network.

Architecture

(1) Location. Typically, an Intrusion Detection System resides at the location of the network that receives a broadcast of all network activity. The IPS **must reside on a gateway router or firewall**, which is responsible for the transport of IP traffic between different network segments and the Internet. As a perimeter based firewall, Kerio Control implements "network-based" Intrusion Prevention. In other words, any traffic routed through the firewall, between the protected networks and the Internet, will be protected by Kerio Control's IPS.

(2) Packet Analysis. At the core of its scanning technology, Kerio Control integrates a packet analyzer based on **Snort**. Snort is an open source IDS/IPS system that transparently scans all network communication, and provides a framework for incorporating custom rules. More information is available at www.snort.org.

(3) Database. Kerio Control implements a set of rules maintained by a community sponsored project called **Emerging Threats**. Each rule is digitally signed to ensure the authenticity of updates, preventing any type of tampering. The rules are based on many years of contributions from industry professionals, and are continuously updated. More information is available at www.emergingthreats.net.

Kerio Control's Intrusion Prevention System offers three different actions, depending on the severity of the potential attack:

- Low severity intrusions: (no action)
- Medium Severity: (log only)
- High Severity: (log and drop)

These are the default settings, however the action may be adjusted according to the needs of the organization. Severity is based on qualifications built into the rule. High severity rules have the greatest probability of being an actual attack on the network. An example would be the detection of network activity from a Trojan application. Medium category events are defined as suspicious and potentially harmful, but have a possibility of being legitimate activity, for example, a connection over a standard port, using a non standard protocol. A low severity threat may be considered suspicious activity that does not pose any immediate harm, for example, a network port scan.

IP Blacklisting

In addition to a rules database comprised of network behavior signatures, Kerio Control maintains a database of IP Addresses, which are explicitly denied any type of access through the firewall. The IP Addresses included in this database are known to be the origin of some form of attack. In many cases, these IP Addresses were assigned to legitimate companies, but have become repurposed for illegitimate activities, such as spam distribution. This database of IP Addresses is pulled from various Internet sources, and managed by organizations such as Dshield and Spamhaus. These lists are stored locally and updated automatically.

False positives and exceptions

Intrusion Detection technology is not foolproof. Similar to Anti-Spam, it is normal to encounter a small percentage of false positives. In other words, legitimate network communication that matches the signatures of suspicious activity can be misidentified. It is therefore necessary to provide a simple method for making exceptions to the signature database.

How to fine-tune the IPS

(1) Review the Security log. Any communication blocked by the IPS engine is reported to the "Security" log. The details of each event, including the "rule ID" are provided in the log. If a user reports a connection problem in a specific application that uses a permitted protocol, it is worth reviewing the security log for the potentially misidentified intrusion.

(2) Verify that the application is not compromised. If the communication of an application is blocked by the IPS, the application should be examined to ensure it has not become compromised and it is in fact behaving legitimately.

(**3) Create exceptions**. If an exception should be made to the signature database, the rule ID taken from the log event can be added to the "Ignored Signatures" dialog in the advanced settings of the IPS management interface.

Update management

Just like viruses, new threats are identified daily. It is therefore necessary to ensure that the signature database is updated regularly. Kerio Control's IPS engine checks for updates once every day, but also can be set to check hourly.

The community surrounding emergingthreats.net contributes newly added rules, or signatures. Kerio contributes to the ongoing maintenance of these signatures, while encouraging administrators using the IPS in Kerio Control to participate in the community effort to identify new attacks and assist in the development of new rules. More information can be found at www.emergingthreats.net.

Inherent IPS rules

The built-in deep packet inspection of Kerio Control acts as an additional layer of defense by transparently monitoring specific protocols to ensure the communication does not violate the specification. It also filters malicious content that may not be recognized by the signature database. In addition to the blacklists and signature databases, Kerio Control combines a number of automatic features to fortify its intrusion prevention capabilities:

- Peer-to-peer blocker. When enabled, the firewall will monitor connections over certain ports to identify and block activity of known P2P applications, which heavily contribute to the spread of malware.
- Blocking illegal binary data in HTTP. As part of its packet inspection, the firewall will prevent the illegal use of binary data in HTTP connections.
- GDI+JPEG vulnerability filter. A specifically designed JPEG image file can cause a buffer overflow in un-patched Windows Operating Systems, allowing the execution of arbitrary code (MS04-028). Kerio Control identifies and blocks the transfer of this specific file through Email and Web protocols.
- Ongoing ICSA Labs certification testing. As part of ICSA (International Computer Security Association) Labs certification, Kerio Control must continuously pass a number of security audits, such as TCP syn flooding, FTP bounce, Man-in-the-middle attacks, and other evolving threats.

Summary

Intrusion Prevention is a highly sophisticated technology, based on a large set of varying rules. Every network is unique, and a so-called "intrusion" may be subject to interpretation. The IPS built into Kerio Control is designed to identify and block attacks as accurately as possible, while maintaining an optimal level of network performance.

Brian Carmichael
Sales Engineer
Kerio Technologies Inc.

Copyright © 2010 Kerio Technologies Inc. All rights reserved.
Published in April 2010.