Intrusion Prevention System

Background

Process Software is excited to introduce the Intrusion Prevention System (IPS) feature in the latest release of MultiNet. This feature will also be added to the next release of TCPware. IPS is a highly flexible and customizable security feature that allows for both MultiNet and user applications to detect and defeat potential security threat events in real-time. IPS is being used to protect OpenVMS systems across the globe today. This case study provides three examples of how it has been implemented to protect mission-critical systems from the threat of an attack. Process Software uses IPS to protect development systems in multiple sites; VSM Software Services uses IPS in their Internet service to protect customers using their web services in Australia; and The Hebrew University of Jerusalem uses IPS to protect the academic staff's system in Israel.

> ***"IPS is one of the most interesting new features in MultiNet v5.3. It has proven to be effective at limiting intrusion activity and I hope that others are encouraged to make use of MultiNet's Intrusion Prevention System to improve security."***
>
> Jeremy Begg
> Managing Director of
> VSM Software Services

How it Works

The IPS feature monitors network and/or system activities for malicious or unwanted behavior and can react in real-time to block or prevent those threats. MultiNet SSH, FTP, SNMP, TELNET, IMAP, SMTP, and POP3 have been instrumented with IPS to report suspicious activity to a highly flexible and customized central filter server. The filter server will then use pre-configured rules to determine if it should block an intruder's IP address from accessing the system and/or if it should prevent an intruder from accessing a specific application. For example, it can detect when a bogus username or invalid password is being used in an attempt to access a system. The time period that the filter is in place is configurable. An API is provided so that customers can incorporate the IPS functionality into their applications. Process Software has also incorporated IPS to protect PMDF.

Preventing Dictionary Attacks and Denial-of-Service Attacks

Examples of malicious or unwanted behavior include dictionary attacks and denial-of-service attacks. A dictionary attack is a brute force attack that uses common words as possible passwords or decryption keys and provides a more efficient way of discovering a user's code. A denial-of service attack is an attack that floods the system with repeated attempts using the same bogus name. By flooding the server with too much traffic, the server cannot maintain acceptable responsiveness. The system is then vulnerable to malicious behavior and at risk of being attacked. By incorporating the IPS functionality into your application, you can combat these security threats by blocking and preventing the attacks.

IPS in Action

Process Software

In today's business world, it is essential that systems have services available through the Internet. Process Software has remote software developers whose systems have FTP, SSH, and POP available via the Internet. The engineering department decided to put their code to good use and configured the remote systems to use IPS to secure their valuable source code.

In one month, IPS stopped an average of nearly two attacks per day on one system, with a high of 8 attacks stopped on one particular day. The attacks were primarily on SSH and FTP, but there were also attacks on the

POP3 server. The attacks were typically dictionary-style attacks, but there were also denial-of-service attacks. The nature of the attacks was studied and actions were taken. Geoff Bryant, vice president of engineering, describes how these attacks were defeated. “We made adjustments to the filter events, time and duration configuration parameters for FTP and SSH to fit the attack profiles being seen. These adjustments and configurations further weakened the impact of the attacks by making IPS respond more aggressively. This IPS packet filter stopped 28,000 attempts.” Mr. Bryant points out that “A packet dropped or stopped by a filter could represent a correct password guess from reading the target application. It certainly minimizes the performance impact by stopping the attack at the lowest possible level of the IP stack.”

Mr. Bryant cites a second instance in which an IPS filter caught thousands of packets. “The attempted attack involved one of our FTP and web servers. This particular system is used for customers to access product releases, eco kits, and Process Technical Support pages. It is Internet facing and IPS is configured to protect FTP and SSH intrusions. We were observing the FTP system being attacked once per day. Similar to the attacks on the developer’s system, these have been dictionary attacks trying to log into the non-existent accounts such as ADMINISTRATOR and ACCOUNTING. This system has debugging enabled and can log the attack events to the operator console.” Mr. Bryant notes “One day, while an administrator was working on the console, an attack was seen. It began with several OPCOM messages being logged for FTP login failures. This interrupted the administrator’s work on the console. After a few messages were logged for the failures, a filter was put in place automatically. The attack was stopped and that allowed the administrator to continue working. When the filter expired, the attack began again. The filter was configured in such a way that it once again prevented another attack automatically.”

VSM Software Services

Jeremy Begg, managing director of VSM Software Services, notes that “The IPS security mechanism is one of the most interesting new features in MultiNet v 5.3 because it provides an additional level of security in an automated way.” VSM Software Services runs an Alpha server to provide services to customers on the Internet including DNS, web serving and email. VSM Software Services also allows incoming FTP and SSH access for server management and customer website maintenance. Mr. Begg notes that “In operating these services, they regularly see VMS break-in events logged by MultiNet’s SSH and FTP servers and by PMDF’s POP3, IMAP, and SMTP servers.”

Until IPS, all of the methods that VSM Software Services used to control these threats relied upon manual observation of an attack and manual updating of a configuration file. Mr. Begg now utilizes MultiNet IPS to automatically update the MultiNet packetfilter mechanism. He notes that IPS has “Proven to be effective at limiting intrusion activity and hopes that others are encouraged to make use of MultiNet’s Intrusion Prevention System to improve security.”

The Hebrew University of Jerusalem

The Hebrew University of Jerusalem has an academic staff utilizing a system that serves TELNET, SSH, POP and IMAP available via the Internet. Yehavi Bourvine, the Chief Technical Officer of the University, finds that “Dictionary attacks are the most common threat and they tend to occur nearly five times per day. On occasion, I have seen rare peeks in the hundreds! MultiNet’s IPS has been installed and aggressively configured. We are now seeing IPS at work, blocking these attacks. We have had no complaints from the users and our system is not filled with thousands of lines in our audit logs.”

ADDED SECURITY AND INCREASED PRODUCTIVITY

With the flexibility of IPS, you can determine how this added layer of protection will best serve your systems and your company’s needs. As described in this case study, IPS can be customized to combat security threats to your mission-critical OpenVMS systems.

ABOUT PROCESS SOFTWARE

Process Software is a premier supplier of communications software solutions to mission critical environments since 1984. With a loyal customer base of over 3,000 organizations, including Global 2000 and Fortune 1000 companies, Process Software has earned a strong reputation for meeting the stringent reliability and performance requirements of enterprise networks.

Process Software
959 Concord Street
Framingham, MA 01701

Telephone:

U.S./Canada	(800)722-7770
International	(508)879-6994
Fax:	(508)879-0042
Web:	www.process.com
Email:	info@process.com

The information contained in this document is subject to change without notice. Process Software assumes no responsibility for any errors that may appear in this document. **N-OPVMSEC-01** 0609