There is a wide variety of network traffic. Servers can be using different operating systems, an FTP server application used in the demilitarized zone (DMZ) can be different from the one used in the corporate intranet, the SSH server in the partner DMZ might be running on a non-standard port, and so on. Successful intrusion detection requires both a granular and a flexible configuration as to what type of traffic is inspected, and how it is inspected.

The Stealth IPS sensor policy is defined in a sensor rule base. The rule base defines the order in which traffic is inspected by an individual inspection agent. All the inspection in the sensor is done by inspection agents.

An inspection agent is a way to customize the protocol handling for a specific application by changing the parameter settings. In addition to customized parameters, an inspection agent may include its own set of context-sensitive fingerprints for detecting application-specific attacks. This will further reduce the number of false positives.

For example, a first-generation IDS evaluates all network traffic in the same way, not differentiating between protocols. A more advanced IDS evaluates each network traffic differently depending on the protocol. With Stealth IPS sensor policy, a step further is taken with inspection agents having a look at traffic on each layer of the protocol stack. That traffic can then be handled differently based on such things as its destination, source, or service. Thus network traffic on port 80 can be inspected differently based on its destination as well as *what* is at the destination, such as a server using Microsoft's Internet Information Server (IIS) or Apache.

Responses can be defined for each inspection agent. This means that it is possible to define different responses for different servers and applicationsŠand even a different response based on where the attack is coming from. An attack attempt using Nimda from the external network should not cause any actions, but the same attack from an internal network should

generate an alert.

Sensor Modules

Stealth IPS sensor has two kinds of inspection modules: protocol-specific inspection modules such as the HTTP module and generic inspection modules such as the TCP fingerprint module. A inspection module with a configuration is called an inspection agent. A protocol-specific inspection module can decode the protocol and validate it if the protocol usage complies with the specification.

The protocols should be well defined, thus permitting deviations from the standard usage to be detected with good accuracy. However, as the actual implementation and use of protocols varies quite significantly in real life, Stealth IPS offers administrators a variety of ways to define what is considered a protocol violation in their network. By using different inspection agents, each with a unique parameter setting, it is possible to validate real-life protocols accurately without false positives.

Sometimes a malicious attack does not violate the actual protocol, but it breaks the application that has implemented the protocol by providing unexpected data that the application designers didn't anticipate. These kinds of anomalies are possible to detect by configuring a custom inspection agent to detect the abnormal data.

All fingerprinting is done by inspection agents. The protocol-specific inspection agent evaluate their fingerprints only in the right context, thus significantly reducing the number of false positives. As it is possible to have different fingerprints on different inspection agents, using IIS-specific fingerprints on an IIS inspection agent and not on an Apache inspection agent can further reduce false positives.

If there is no protocol-specific inspection agent available for a protocol, fingerprinting is done by using a generic inspection agent. In a generic inspection agent, fingerprints are evaluated with regards to the direction of the traffic

flow. It is possible to group fingerprints related to a specific protocol into a new inspection agent, which gives an opportunity to use them in the rule base and to decrease the number of false positives even further.

Stealth IPS comes with a set of protocol-specific inspection modules. To fine-tune the system for different environments, Stonesoft provides system inspection agents for most typical applications such as HTTP-specific system inspection agent for Microsoft IIS and Apache. Moreover, Stonesoft provides inspection module updates whenever protocols are changed, or new ones become standardized.

Fingerprints

Context sensitive fingerprints in Stealth IPS are defined using regular expression strings. Using regular expressions allows the necessary flexibility in fingerprint definition. At the same time context sensitivity in the inspection agents decreases the number of false positives as the fingerprint pattern matching is made in the right context.

The Stealth IPS contains plenty of system fingerprints for known vulnerabilities and exploits. The user can freely group them, and then select which to use for matching specific types of traffic. All system fingerprints are open, so if needed they can be fully evaluated and used as templates for custom fingerprints. The custom fingerprints are created using Stealth IPS Fingerprint Editor. Stonesoft regularly provides fingerprint updates to ensure that the system stays up to date.

Event Correlation (Analyzer)

The Stealth IPS Analyzer opens a totally new level of detection possibilities. Most traffic analyzed by sensors does not violate corporate security policy (being valid business traffic), so only some statistical information is generated from it. On the other hand some traffic is immediately identified as malicious, and a corresponding event is generated (which may result in an active response). There is, however, a set of events that are at best interesting–or even suspicious.

Traditional IDS products would have passed all this information to the administrator for manual analysis. The Stealth IPS Analyzer automates this task by correlating and manipulating event information received from various sources. Events typically come from the sensors, but they can also originate from other analyzers. Moreover, the Analyzer can also process events originating from syslog compliant devices. The Analyzer examines suspicious events in-depth, correlates events with one another to detect trends and determine their significance, and drops irrelevant events. All this improves the quality of event information and reduces the need for time-consuming manual analysis.

Stealth IPS comes with a predefined Analyzer system policy. If needed, the Analyzer policy can be configured using a graphical user interface (GUI). The configuration connects the input events to a set of analyzing modules through matching filters and finally to the response modules. The settings of the analyzing modules are also configurable.

Statistics

Stealth IPS detects anomalous traffic based on traffic statistics that match the defined rules. The data is collected by sensors and examined in the Analyzer. Statistics provide information for detecting events such as unknown attacks, slow scans, unusual number of connections, and so on. Stealth IPS can analyze statistical data with:

- ***Connection Statistics*** where a counter is used for detecting certain types of traffic connections. When the counter hits a user-defined limit, a specified response or alert is triggered.
- ***Timeslot Statistics*** where connection data is collected over a specified time window. If a user-defined limit for all traffic is exceeded within this sliding window, a specified response or alert is triggered.

For example, connection statistics can be used to detect, for example, anomalous traffic originating from a server that should not normally initiate any outgoing connections. If such traffic is observed, it can be held as a sign of a Trojan horse or a successful intrusion.

Timeslot statistics, on the other hand, can be used to detect port scans.

Stealth IPS false Positive

Need for Active Response

A successful attack results in a cumbersome and time-consuming incident handling process. Repairing the damage, investigating the cause of the incident, and preventing further damage is costly, and typically ties up many key resources. The ideal way to avoid all this is to stop an incident before it occurs. When a Stealth IPS detects and identifies an attack attempt, it should stop it by using a predefined automatic response.

The usefulness of automatic responses depends mainly on their detection accuracy. If it is possible to identify an attack attempt without the possibility of false positives, an active response mechanism should be used to automatically defend against the attack. On the other hand, if detection cannot be made with 100% accuracy, a more conservative approach is advisable.

Despite all the efforts made in a sensor to accurately identify attacks, some events remain suspicious on their own. These events require further analysis and correlation with the Analyzer. The Analyzer is able to use its own set of automatic responses either to prevent further attempts from the same source, or to collect evidence for forensic analysis.

Passive responses are the basis for successful intrusion handling. Without data on the various events related to an incident, determining the cause and symptoms of the incident can take much longer and require more resources. Your ability to improve your defenses, and to remove the cause of the incident, might be limited until it is determined what exactly happened and why.

Automatic alert handling, escalation, and acknowledgement are defined in the Alert Center of the Stealth Management Center. This allows yet another way to automate responses to various events.

Log Message X X

Connection Recording X

IP Blacklisting X X

TCP Connection Termination X

Stealth IPS false Positive

Packet & Connection Drop Version 2

Alert X X

E-mail X

SMS X

Pager X

SNMP Trap X

Console Message X