

STONESOFT

Whitepaper

Winning the Battle Against False Positives

Table of Contents

Executive Summary	1
State of Network Security	2
Introducing the StoneGate Platform	3
How a Modern IPS Meets Different Needs	4
Need for Accuracy	4
Need for Active Response	6
Need for Speed and Reliability	8
Need for Usability	8
Conclusion	9

Executive Summary

The number of network security incidents continues to grow fast. At the same time, the cost of network security is increasing, while business reality would call for a reduction in expenses. Different network security solutions, such as firewalls, network and host-based intrusion detection/protection systems, and anti-virus software, all contribute to enhanced network security. These components cover different areas of network security architecture, implementing a defense in depth. It is clear that no single device or method would soothe all network security concerns.

Intrusion detection plays an important part in the network security puzzle and is often called the “last line of defense” in the corporate network security arena. Intrusion Detection provides a warning or alarm that someone has managed to bypass all other security measures and is getting access to areas where are not permitted.

However, despite all the promises, the general view is that traditional Intrusion Detection Systems have failed to meet the expectations in many areas. Specifically, traditional IDS systems are:

- Inaccurate with a high noise-to-signal ratio
- Too passive-detection alone is no longer sufficient
- Unable to meet the throughput and reliability requirements of today’s networks
- Difficult and expensive to manage in distributed enterprise environments.

This white paper describes a solution to these problems. It introduces StoneGate Platform that combines StoneGate Firewall, StoneGate VPN, and StoneGate IPS-Intrusion Detection and Analysis for Active Response, under a common, centralized management system. Furthermore, it explains how StoneGate IPS solves the need for accuracy, active responses, speed, reliability, and usability.

Stonesoft has done extensive research to find a successful way to tackle the accuracy (false positive/false negative) problem. Our findings show that the best solution is a combination of multiple detection methods, granular and flexible configuration, and event correlation. Therefore, this is the approach taken in Stonesoft’s StoneGate IPS.

Automatic response mechanisms are an integrated part of StoneGate IPS. Although these systems can never prevent all security incidents, they can reduce the number of those incidents significantly, thus providing considerable cost savings. Incident handling is a taxing process, requiring time and dedicated resources. Avoiding this process is always a more cost-effective alternative than full-blown incident handling.

StoneGate IPS sensors are designed for Gigabit environments, and they meet the throughput requirements of the most demanding networks. Built-in clustering and high availability improve performance and reliability even further.

The underlying StoneGate Platform provides defense in depth without adding complexity to everyday network management. The StoneGate Management Center (SMC) achieves cost savings with reduced set-up times, reduced data and system maintenance efforts, lower training costs, and by more efficient daily operations. Our architecture is designed for distributed environments, where remote management, remote upgrades, and support for multiple administrators with different roles are mandatory requirements.

State of Network Security

Statistics from the CERT® Coordination Center (CERT/CC) show that the number of reported security incidents is increasing 50 - 100% a year. This number reflects, not just an increase in the number of found vulnerabilities, but also the easier access to a wide range of sophisticated, easy-to-use hacking tools. At the same time, real cyber crime is increasing as well as hacktivism and hacking just for fun. In today's environment, network security has become essential for ensuring business continuity.

As the number of incidents has increased, the need to cut down costs related to incidents continues to grow. This is where different security solutions get involve—all playing their own specific roles in different parts of the security model (see Figure 1).

The most effective way of dealing with incidents is to prevent them—after all, a prevented event does not cause any additional damage. Prevention covers any actions stated in a corporate security policy that prevents negative effects. Preventive actions range from physical access control measures to such technical solutions as perimeter firewalls. Another purpose for prevention is to increase the time and cost needed by attackers to penetrate the system, thus giving defenders more time to react.

Regardless of all the measures that have been taken, sometimes it is not possible to prevent incidents. Detection means that any undesired, abnormal, or plain malicious events are detected as soon as possible with the greatest amount of precision. The key here is timely detection. This is the area where traditional Intrusion Detection Systems have shone...and failed. The main problem with IDSs has been that they have produced a tremendous number of alerts—one IDS user reported having 1.8 million alerts monthly from their legacy system! Handling such a number of events is a problem by itself—not to mention the fact that real security incidents then get lost in the numbers. This scenario is called the noise-to-signal ratio.

Reaction refers to the actions taken once a security breach is detected. The purpose of swift reaction is to limit the potential damage to a minimum. A reaction can be an automated response from an IDS, or it may be any other action taken by a system administrator to confine the effects of the event.

Recovery includes all the steps taken after an incident. Once a security violation occurs, it is crucial to determine the damage done in order to restore systems back to their normal state, and to prevent further incidents. This is an area where network security solutions can help to determine the needed actions by pinpointing who did what, where, and—maybe the most difficult one—why.

It seems clear that there is no single device or method will solve all the network security concerns. A proper solution is to implement defense-in-depth, which means adding layers of defense to your network covering all the different sectors in the presented security model. Besides firewalls, network and host-based intrusion detection/protection, as well as anti-virus software all contribute to enhanced network security. Despite all the promises however, the general view

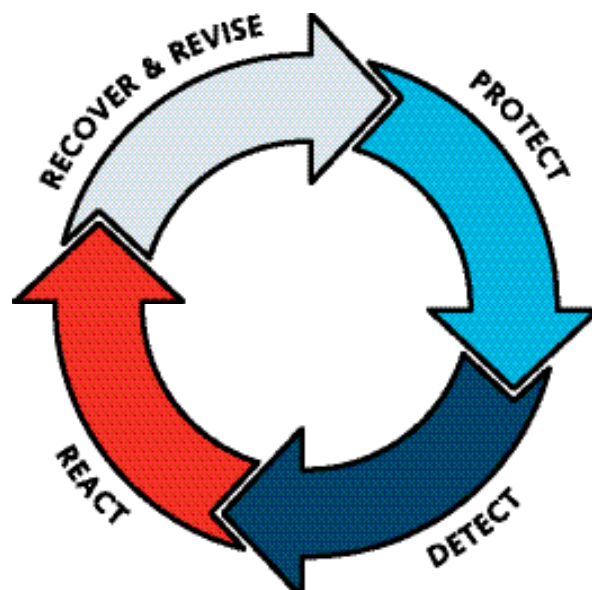


Figure 1: Security Model

is that the traditional Intrusion Detection Systems have failed to meet expectations in many areas. More specifically, the traditional IDS systems are:

- Inaccurate with a high noise-to-signal ratio
- Too passive-detection alone is no longer sufficient
- Unable to meet the throughput and reliability requirements of today's networks
- Difficult and expensive to manage in distributed enterprise environments.

There is no doubt that Intrusion Detection Systems are an important element of network security and that they bring value. At the same time, in order to survive, IDS systems need to meet the challenges outlined above—otherwise this vital technology faces death due to operations becoming too expensive in return for the benefit they provide.

Introducing the StoneGate Platform

StoneGate Platform is designed to meet real world business security demands and business continuity goals as well as designed to create cost savings. This is achieved by excelling in manageability, scalability, availability, and security.

The key element in StoneGate Platform is the StoneGate Management Center (SMC), which provides a unified management interface for Stone-Gate Firewall, StoneGate VPN, and StoneGate IPS products. The SMC is designed around Stonesoft's vision to build a centralized, scalable management system providing in-depth defense. StoneGate's distributed security architecture allows effective deployment of system components in different network environments. With a single user interface, the whole StoneGate system can be easily and comprehensively managed, regardless of the number or physical location of the sensors, analyzers, FW/VPN engines, or the management system. StoneGate's layered StoneGate architecture is illustrated in Figure 2 on page 9, where the GUI client is in communication with the StoneGate Management Center and the StoneGate Management Center is in turn in communication with the Sensors, Analyzers, and FW/ VPN engines. StoneGate Platform consists of the following main components:

- IPS Sensor nodes capture network traffic and make the initial analysis.
- IPS Analyzers correlate and manipulate event information received from the sensors and possibly from other analyzers or syslog compliant devices.
- Firewall/VPN Engines implement access control, Multi-Layer Inspection, NAT, VPN, authentication, monitoring, and logging.

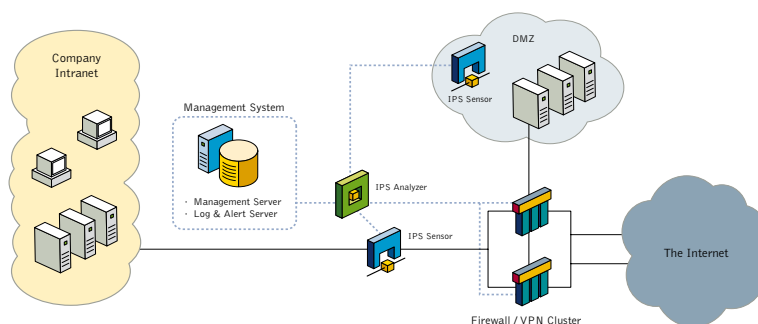


Figure 2: StoneGate Security Solution

- VPN Engines implements VPN, authentication, monitoring and logging
- StoneGate Management Center, which consists of:
 - Management Server controls the StoneGate system
 - Alert/Log Server stores the event information received from the analyzer(s) and alerts the administrators when critical events occur.
 - One or more management GUI clients manages and monitors the whole StoneGate system.

For more information on this technology, please see the white papers "The Secret to Simplified Firewall & VPN Technology" and "StoneGate Multi-Link Technology" available from: <http://www.stonesoft.com>.

How a Modern IPS Meets Different Needs

Need for Accuracy

The rate of false positives and false negatives compared to actual attacks—the noise-to-signal ratio—should be very low. False positives are false alarms; alarms that are set off even when there is no attack. If the number of false positives is very high, the produced information becomes unreliable, and real incidents might go undetected. False positives are typically generated by systems that rely on a single detection method, and by ones that cannot be configured at different levels to fit into the operational environment. An additional reason for false positives is that the first-generation intrusion detection products do not offer any means of correlating events. False negatives, on the other hand, are missed attacks. The IPS needs to be able to detect each and every real attack.

StoneGate IPS tackles the problem through a combination of powerful detection methods that are applied according to administrator-defined rules, and by introducing intelligent event correlation. In addition, there are several improvements in the detection methods themselves, such as context-sensitive, regular expression-based fingerprints, and configurable protocol inspection modules. This way, real threats are acted upon more readily, and less manual work is wasted on analyzing false alarms.

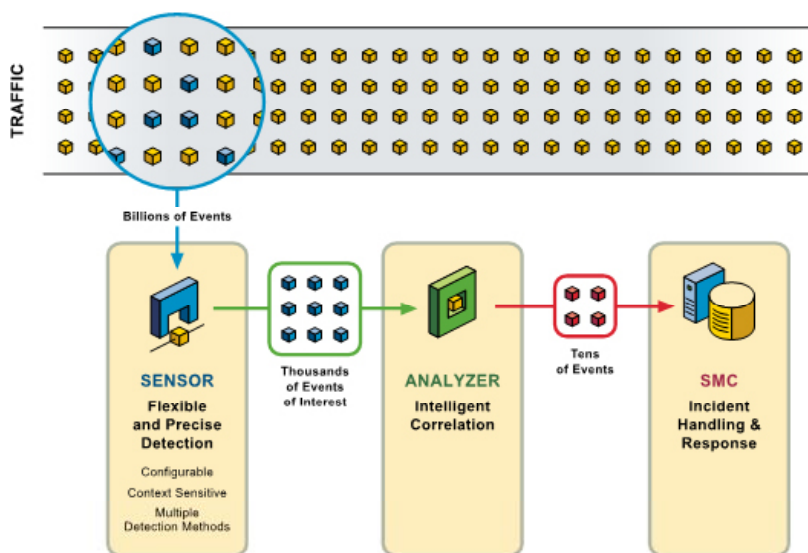


Figure 3. Incident Handling in StoneGate IPS

StoneGate IPS Sensor Policy

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 StoneGate 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 StoneGate 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 applications—and 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

StoneGate 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, StoneGate 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.

StoneGate 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 StoneGate 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 StoneGate 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 StoneGate IPS Fingerprint Editor. Stonesoft regularly provides fingerprint updates to ensure that the system stays up to date.

Event Correlation (Analyzer)

The StoneGate 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 im-

mediately 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 StoneGate 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. StoneGate 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

StoneGate 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. StoneGate 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.

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 StoneGate 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 StoneGate Management Center. This allows yet another way to automate responses to various events.

	Sensor	Analyzer	Alert Center
Log Message	x	x	
Connection Recording	x		
IP Blacklisting	x	x	
TCP Connection Termination	x		
Packet & Connection Drop	version 2		
Alert	x	x	
Email			x
SMS			x
Pager			x
SNMP Trap			x
Console Message			x

Table 1. Alert Center

Different Response Mechanisms

Log Message

A log message stores the basic event information on the Log Server. The information is valuable for forensics analysis, as it gives an overview to what has happened.

Connection Recording

StoneGate IPS sensor is able to record all packets—both the header and payload—related to a connection. The recording is done in a proprietary format. Conversion tools are available for changing the recording into tcpdump format. The recorded packets can be used to reconstruct an attack, and they can be analyzed in detail to gain additional information.

IP Blacklisting

Integration of the StoneGate IPS and the StoneGate Firewall enables IP blacklisting, making it possible to change the firewall policy dynamically for a predefined time period so that the source of the detected anomalous traffic is already blocked at the firewall. IP whitelisting on StoneGate Firewall then protects the legitimate pre-existing connections against spoofed attacks that could result in denial-of-service attacks against important connections. IP blacklisting is an effective way to block various attacks that require a valid IP address to work, however, this feature should always be used with care due to the possibility of IP address spoofing.

TCP Connection Termination

TCP connection termination means disconnecting a TCP connection by sending a TCP reset packet to both ends of the connection—a simple way to stop TCP-based attacks. This response requires that an interface other than the listening interface be available to the sensor for sending the packet. The main limitation with TCP connection termination is that it works only with TCP—not with any connectionless protocols like UDP or ICMP. Additionally, TCP reset packets may reveal the existence of an IPS to attackers.

Packet and Connection Drop

StoneGate IPS version 2 will introduce an additional deployment mode: inline mode. In this mode, the IPS is on the traffic path and every packet passes through the system. The inline mode allows implementation of an additional response mechanism: packet and connection drop. This response means that the IPS sensor drops offending packets (or all the packets related to an offending connection), thus preventing them from reaching their final destination and causing damage. This method requires that we are able to be 100% accurate in our attack detection, based on the information available from a single packet or connection.

Alert

Alert is a notification to the Alert Server that it should handle alert information based on the configuration in the alert rule base and in the alert chains. Notification methods that are available to the Alert Center are e-mail, SMS, Pager, SNMP trap, and console messages.

Need for Speed and Reliability

Intrusion detection systems must keep up with increasing bandwidth. Even though Internet connections in the enterprises are still typically well below the gigabit level, the traffic volume in the internal networks can be much higher. In a typical location, the aggregated traffic on a switch's span port can nearly be a gigabit. Systems that cannot handle such traffic volumes start to lose packets. This in turn may result in false negatives; in other words, some attacks could go unnoticed only because the IPS could not process all of the traffic on the wire. Respectively, the system may produce excess false positives as protocol violations are incorrectly observed.

StoneGate IPS sensors have an integrated operating system and internal architecture with high performance and robustness as their design principles. Parallel fingerprint evaluation and context sensitiveness are just a few examples of how sensor performance has been optimized.

StoneGate IPS introduces built-in sensor clustering and load balancing as ways to improve the throughput and high availability of the sensor nodes in the most demanding customer environments. By clustering the sensor nodes, a single sensor doesn't have to process all the traffic as the traffic load is distributed between the nodes in the cluster.

Need for Usability

As more and more network security devices are added to networks, the benefits of centralized management become clear. Managing the firewall, IPS, and VPN all from a single, centralized management system can produce significant savings in operating, maintenance, and training costs. This also eliminates potential incompatibility problems between different systems. One issue that has hampered the deployment of IPSs is the lack of usability. Running a system in complex environments is difficult. Systems are not designed to cope with the need to store large amounts of information and they do not support well enough the real-life complexity of the today's distributed enterprise.

Everyday Management

In large scale, possibly transnational, environments, system manageability becomes crucial. With StoneGate's flexible architecture, management system components can be distributed physically while simultaneously be managed through a single GUI client over the network.

On the other hand, large enterprise networks require features for delegating administrative tasks. StoneGate Management Center divides administrator accounts into different levels, permitting task delegation according to individual administrator's authority. The system supports several administrators connecting to the management system simultaneously, allowing concurrent work from multiple locations—a typical situation in an enterprise that has several physical locations.

Handling alerts is one of an administrator's daily tasks. StoneGate Management Center includes a new Alert Center that automates the alert handling and escalation. The alert rule base allows routing alerts to alert chains based on the alert origin, type, and time. Each alert chain consists of an alerting method, target, possible thresholds for overload situation, and a delay on how long the system will wait for the acknowledgement before escalating the alert to the next level in the alert chain. See Figure 4 for more information on this.

Upgrading the software in all locations of an enterprise with

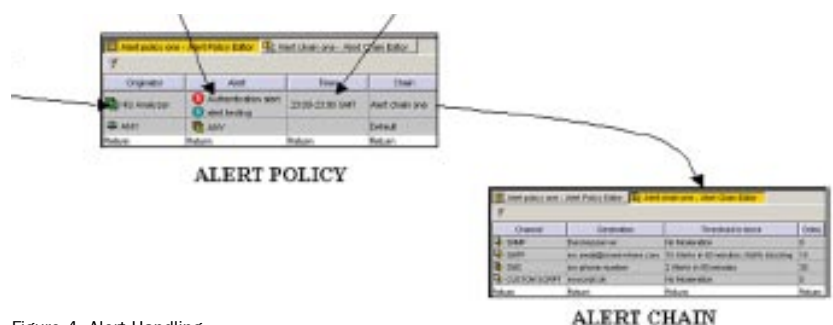


Figure 4. Alert Handling

multiple remote offices can be costly and time consuming, especially if on-site visits are required. StoneGate Management Center allows upgrading remote nodes from the Management Server by selecting the sensor or the analyzer to upgrade, selecting the installation package from a list of available packages, and giving the upgrade command. The upgrade process is quick and fail-safe. A more frequent task is the need to update the security-related data. Dynamic updates—containing new fingerprints, inspection module updates, templates, and documentation—are downloaded to the management system, and they are available for policy definitions and updates immediately after the import.

Integration with StoneGate Firewall and VPN StoneGate IPS

Integration with StoneGate Firewall and VPN StoneGate IPS is not just an “Intrusion Detection and Analysis for Active Response”. Rather it is part of a larger combination. The seamless unification of the StoneGate Firewall and StoneGate VPN solution together with the StoneGate IPS make the combination a very powerful network security solution. The common management system with its unified concepts and notions and secured inter-system communication ensure efficient and secure integration of the system components. Although the parts of the system operate independently of each other, the full power of the Stone-Gate Platform is available when they are used together.

Conclusion

StoneGate IPS is a modern Intrusion Detection and Response System with Intelligent Analysis that meets the challenges that traditional intrusion detection systems failed to meet:

- need for accuracy
- need for active responses
- need for speed and reliability
- need for usability

Together with the StoneGate Firewall and VPN, StoneGate IPS forms an ideal solution for enterprises looking for an easy to manage, secure, reliable, and scalable network security solution under the StoneGate Management Center.

If your network security is still missing the last line of defense, or if you have faced the challenges of the traditional Intrusion Detection Systems, it might be time to evaluate what StoneGate IPS could do for your network.

STONESOFT

Stonesoft Corp.

Itälahdenkatu 22 A
00210 Helsinki
Finland
tel. +358 9 476 711
fax. +358 9 476 712 34

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338, USA
tel. +1 770 6681 125
fax. +1 770 6681 131

Stonesoft Corp.

90 Cecil Street
#13-01 Carlton Building
Singapore 069531
tel. +65 6325 1390
fax. +65 6325 1399

Copyright 2006 Stonesoft Corp. All rights reserved. Registered or unregistered trademarks in this document are property of their respective owners. The products described in this document are protected by one or more of U.S. patents and European patents: U.S. Patent No. 6,650,621, European Patents No. 1065844, 1289202, and may be protected by other U.S. patents, foreign patents, or pending applications. Specifications subject to change without notice.