

## Frequently Asked Questions about StoneGate IPS (March 2008)

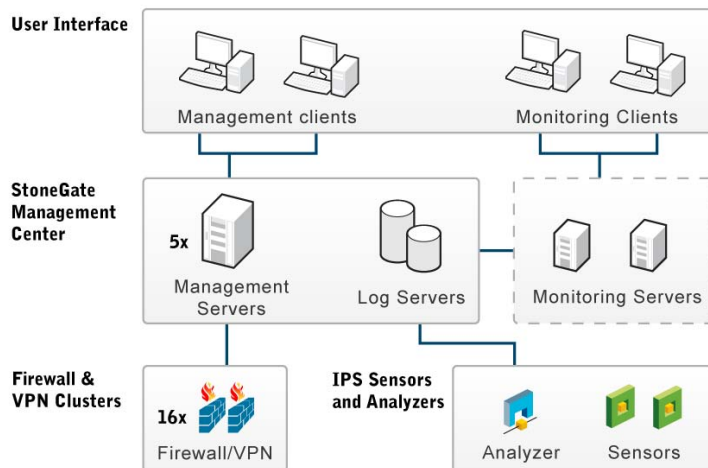
### Q: What are some of the main selection criteria for an intrusion prevention system?

A: While each organization may have their own unique requirements and priorities, some of the main elements that differentiate one intrusion prevention system over another include:

- **Management** – Reduces administration time for network security, incident and log management operations and extent of which it can integrate with other security components to enforce immediate threat mitigation policies or software updates
- **Performance** – Ensures optimal network performance based on elements such as wire speed operation and enabled features
- **Enforcement** – Enables different action such as proactively terminating attacks or just monitoring attacks, blacklisting, recording packets, alert management and what auditing tools such as policy snapshots for compliance records
- **Availability** – Ensures high availability and reduces downtime risks either in terms of it's design i.e. fail-open or clustering capabilities
- **Detection** – Utilizes multiple detection methods including protocol analysis, misuse detection, event correlation and behavioral analysis, and what level signatures can be customized
- **Architecture** – Provides deployment options such as where the device or devices can be placed, their integration with each other (if any) and whether or not there are limitations to different designs
- **Protection** – Provides options to protect vulnerable applications and operating systems from network attacks against server and client vulnerabilities. Protects services from Denial of Service (DoS) attacks and provides information of network activities and operation.
- **Access Control** – Provides flexible access control methods for easy network segmentation without need for costly routing changes. Is capable of transparently controlling network traffic access starting from Layer-2 like IPv4, IPv6, CDP up to Layer-7 protocols like HTTP(S), MSRPC, SIP.
- **Costs** – Delivers lower Total Cost of Ownership (TCO) both for hard capital and operational costs, but also soft costs of administration and training

### Q: What is the architecture of the StoneGate IPS?

A: StoneGate IPS is one part of the StoneGate Platform that integrates StoneGate Firewall, VPN, IPS and SSL VPN. The StoneGate IPS includes a StoneGate Sensor and StoneGate Analyzer. The StoneGate Sensor performs real-time analysis and enforcement of network traffic through protocol validation, misuse detection (signatures), DoS and scan detection. The StoneGate Analyzer analyses and filters the log events from the sensor(s) and sends the refined log data, including Event Correlation and Event Compression, to a Log Server. The smallest possible IPS system requires one Sensor, one Analyzer and one StoneGate Management Center. The Sensors and Analyzers can be combined into one appliance (combo appliance) and the Management Center contains a Management server and a Log server bundled together. The picture below shows how the events flow through the system components:



**Q: How should StoneGate IPS be used? Where should it be deployed and by whom?**

A: The StoneGate IPS protects vulnerable applications and operating systems from network threats against client and server vulnerabilities in the Intranet and DMZ. StoneGate IPS uses multiple analysis techniques to identify and prevent network traffic abuse, including (DoS) and communications from unwanted applications such as Peer-to-Peer and streaming media.

StoneGate IPS provides flexible deployment options in both inline IPS and IDS modes and is ideally suited for customers with consolidated and/or distributed security environments. With the Transparent Access Control (TAC) module, StoneGate IPS allows easy and cost-effective network segmentation and access control for internal networks. Medium- to large-sized organizations and managed service providers (MSPs) with high security standards benefit most from the StoneGate solutions.

**Q. How resource intensive is the StoneGate IPS to manage?**

A: At the core of the StoneGate Platform is the robust and versatile StoneGate Management Center that unifies Firewall, VPN, IPS and SSL VPN in a central GUI console that can automate and simplify tasks. Beyond just detecting attacks and creating alerts, StoneGate Analyzers correlate, compress and communicate to the StoneGate Management Center, which provides a variety of enterprise tools for visibility into the network with minimal resources. For example, the StoneGate Management Center's alert center manager allows you to create custom policies and thresholds that also follow an acknowledgement workflow providing relative alerts based on items such as type, time and severity of the attack, notifying only relevant resources in an efficient manner. Additionally, the rule sets apply to situations and severity levels according to source and destination addresses and services/protocols, so false positives can be reduced in this manner as well. All communication is TLS encrypted.

**Q. How does StoneGate IPS reduce and manage the amount of false positives and false negatives?**

A: StoneGate IPS is designed to provide efficient inspection and strong protection with minimal administration resources for threat management. The unique ideology of StoneGate IPS combines intelligent correlation with regular expressions that do not require individual alerts or signatures for every variant. Since we can look at the vulnerability, not just the exploit, this not only results in a more efficient solution and protects against variations, but also reduces the amount of signatures that are traditionally required. StoneGate IPS also combines inspection technology based on signatures with protocol analysis via regular expressions that can be defined specifically in the Sensor policy for context specific matching to further reduce the number of false alarms.

**Q: How does StoneGate IPS detect attacks?**

A: One of the main challenges many organizations have with IPS solutions is finding a solution that has the comprehensive functionality to effectively stop known and un-known attacks, that is also manageable. Unlike many other solutions, StoneGate IPS uses a unique approach that utilizes multiple inspection methods including protocol validation, misuse detection, DoS detection and scan detection, while our Analyzer uses intelligent event correlation to detect zero-day, or attacks spread over time. StoneGate IPS also provides the ability to modify or customize the detection methods according to the organization's needs, thus ensuring precise and accurate detection of organization or industry-specific threats. In addition, since StoneGate IPS reviews exploits, not just signatures or vulnerability, it offers efficient protection against slight variations of attacks as well.

**Q: What type of enforcement options does the StoneGate IPS include?**

A: StoneGate IPS is a true in-line solution that can terminate attacks proactively and with immediate effect, with no end user interaction. Beyond simply terminating attacks, when implemented as part of the StoneGate Platform, this information can be integrated into the StoneGate Firewall/VPN for comprehensive reporting, logging, auditing and enforcement. Actions also include blacklisting, terminating, packet recording and alerting. Our IPS can also uniquely act as a monitoring and/or prevention solution simultaneously on the same device.

**Q: Do IPS solutions have an impact on performance? How does StoneGate IPS address performance issues?**

A: Since the StoneGate IPS provides enterprise intrusion prevention, one of the main principles of its design has been to minimize the risk of performance degradation. StoneGate IPS addresses performance issues in several ways, including:

- **Clustering** – Stonesoft was the first to introduce clustering and high availability into the industry in the early 1990s. Along with this, StoneGate IPS can be clustered to help share processing connections to enhance performance and reduce downtime.
- **Deployment** – With the combination of the StoneGate Sensor and Analyzer, only relevant event data is compressed and forwarded to the Analyzer greatly reducing the volume of captured network traffic and providing better performance. Since this is a dedicated system, there also is no risk of performance degradation from other features that impact performance such as anti-virus and anti-spam.
- **Policy Processing** – Since StoneGate IPS uses a combination of protocol specific, context sensitive signatures and intelligent correlation, the system can process possible attacks much faster than ordinary systems that must review all signatures even if they are not related.

**Q: How is StoneGate IPS updated and how often are there new releases ?**

A: Through the StoneGate Management Center, Stonesoft provides automatic updates, upgrades and notifications for StoneGate IPS. These items can automatically download dynamic updates, refresh policies and install new engine upgrades, as well as test the latest content using *Passive Terminate* action. Dynamic update releases are published every second week or whenever needed.

**Q: How does StoneGate IPS address high availability?**

A: Stonesoft was the first to introduce high availability and active/active clustering to the network security industry. This experience and technology is also available with StoneGate IPS, whereby each appliance offers fail-open technology as well as inline serial clustering. In addition, inspection performance can be increased by adding multiple inline IPS engines together with Etherchannel or other link aggregation technologies. This results in reduced downtime and enhanced network performance.

**Q: What does intrusion detection do? How does it differ from intrusion prevention?**

A: StoneGate IPS can operate as an IDS and/or an IPS appliance. According to the definition by the SANS Institute, a network-based (IDS) monitors network traffic and responds with an alarm when it identifies malicious, inappropriate, incorrect, or otherwise abnormal activity. IPS products take IDS one step further: not only do they detect malicious activity, but they also block it, which requires a high level of detection accuracy. In essence, all the intrusion prevention products are also intrusion detection products, but not all intrusion detection products are intrusion prevention products. The difference lies in the response mechanisms that change the role of the IDS from a passive component to a proactive one.

**Q: Does StoneGate IPS protect against viruses?**

A: By definition IPS products do not protect against viruses, but they can protect against worms. In computer security technology, a virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Viruses are one of the several types of malicious software or malware. In common parlance, the term virus is often extended to refer to worms, Trojan horses, and other sorts of malware. A computer worm is a self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers.

**Q: How does StoneGate IPS differ from already existing IDS/IPS solutions?**

A: StoneGate IPS differs from the other products in several ways:

- Since its inception, StoneGate IPS has been part of the StoneGate Platform that was designed to blend firewall, VPN and IPS into a centrally managed system.
- StoneGate IPS is managed through the centralized StoneGate Management Center that provides a single system for centralized remote upgrades, incident handling, back-up and restore actions and reporting for all StoneGate devices within a matter of minutes. The StoneGate Management Center even utilizes the same objects and has the same approach for creating policies for both the StoneGate Firewall/VPN and the StoneGate IPS.
- StoneGate IPS's intelligent correlation and architecture of Analyzers and Sensors not only provides a unique approach to detect attacks, but also drastically reduces false positives with minimal impact on performance.

**Q: Do I have to buy StoneGate Firewall and VPN in order to use StoneGate IPS?**

A: No. StoneGate IPS is fully functional without StoneGate Firewall and VPN. While the StoneGate Firewall has several built-in features that can mitigate attacks (including automatic anti-spoofing), ensuring protocol compliance, preventing application-layer attacks and discarding illegitimate packets, the StoneGate IPS has the ability to detect and stop a much more complex variety of attacks. They both share the same centralized management. You can later add the StoneGate Firewall and VPN component to the StoneGate Platform.

**Q: What is the benefit of having both StoneGate Firewall/VPN and IPS?**

A: By integrating the StoneGate Platform, this provides not only enhanced protection and seamless integration, but also a lower TCO since you can manage both solutions from the same centralized management, therefore enabling more efficient reporting and auditing to help reduce administration time and operational costs. For example, all logs are visible from the same place, while incident handling becomes faster and more accurate when you can follow the attackers' trail from several devices e.g., the IPS can communicate to the firewall and vice versa. Reports for items such as compliance and troubleshooting can be produced from the same central location and even scheduled automatically, saving additional time.

System backups are also easily created or can be scheduled to backup and restore your complete configuration for all elements for Firewall, VPN and IPS into a single file. By utilizing the seamless integration you will benefit from more secure and efficient threat mitigation process.

**Q: What is the best place to deploy StoneGate IPS?**

A: Normally customers deploy StoneGate IPS in the network segments where they have business-critical servers or where the network traffic or computers enter the corporate network. For example, typical places are internal network segments, the DMZ, and the extranet and branch office network segments. The StoneGate IPS Analyzer and Sensors allow a variety of flexible deployment options to meet specific needs and reduce performance issues.

**Q: Does StoneGate IPS provide any Network Access Control (NAC)?**

A: Stonesoft has a partnership with several technology vendors, including Bradford Networks for NAC. When StoneGate IPS detects that a user has violated the network security policy, it sends alert data to NAC Director/Campus Manager, which can take appropriate action and disconnect the user or the IP address from the network.

**Q: Why do you place StoneGate IPS behind the firewall and not outside?**

A: The network(s) inside the firewall (LAN) have much less “noise.” “Noise” in this case refers to random activity, usually in the form of scans or probes, on the Internet or WAN side of the firewall. This extraneous activity can complicate the actual security picture, and a well-configured firewall will block activity of this nature. If you place the IPS behind the firewall, it can verify that the firewall is functioning correctly and presents a clearer picture of the security posture.

**Q: Is StoneGate IPS available as both software and as an appliance-based solution?**

A: As with StoneGate Firewall and StoneGate VPN, StoneGate IPS is available either as an appliance, providing a single point of contact for hardware and software issues and reducing compatibility risks, or software allowing you to capitalize on previous hardware investments. Each appliance has the exact same features. The only difference is the performance and number of interfaces. The software engines are the same for both options, and the engines have an integrated OS.

**Q: How much will the StoneGate IPS solution cost? What is the basis for the pricing (e.g., IP-based or throughput-based license)?**

A: The total cost of the StoneGate IPS solution depends on several issues including the number of sensors and analyzers needed, throughput needed on sensors as well as on the number of the appliances under the management. Pricing options are available for small and medium organizations, from entry-level devices supporting 100 Mbps up to devices for large organizations requiring 10 Gbps.

**Q: Where can I find more technical info about StoneGate IPS?**

A: Follow this link <http://my.stonesoft.com/support/search.do?product=StoneGate>