



StoneGate™ Virtual IPS: In-depth inspection of network traffic in VMware environments

IPS has become an indispensable security tool for detecting malicious traffic. For this purpose, Stonesoft provides StoneGate Virtual IPS, an intrusion detection and prevention system that determines the appropriate response. This solution is the only way to ensure full visibility and protection of communications between all virtual machines.

The StoneGate Virtual IPS (Intrusion Prevention System) appliance has all the functionalities of a traditional IPS appliance along with the possibility to filter and report on all traffic within a virtual infrastructure between virtual machines and exiting the VMware ESX server.



The integrated management tool – StoneGate Management Center (SMC) – provides the tools for monitoring, analysis, and reporting needed to ensure the compliance of virtual environments.

This gives the administrator real-time visibility over all traffic events between various systems, in the form of clear and precise audit logs.

Real-time visibility and control

Traditional administration consoles are not designed to monitor network traffic between virtual machines or alert administrators about availability or security problems. Through its unified management center, StoneGate allows administrators to combine all security policies, giving them complete control over all traffic across virtual environments.



The SMC offers improved auditing capabilities for virtual environments through its sophisticated log filtering and management system, advanced monitoring tools, and customizable integrated reports. This makes it possible for administrators to identify and isolate traffic between virtual machines based on source or destination IP address, protocols, applications, time of day, and numerous other criteria.

STONESOFT

Secure Information Flow

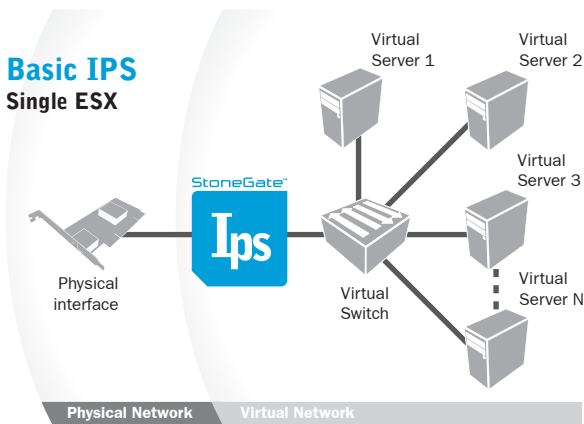
StoneGate Virtual IPS for in-depth security

StoneGate Virtual IPS detects and blocks attacks in real time on traffic that has already passed perimeter firewalls. It also reveals the presence of worms, spyware, and peer-to-peer (P2P) applications in the network.

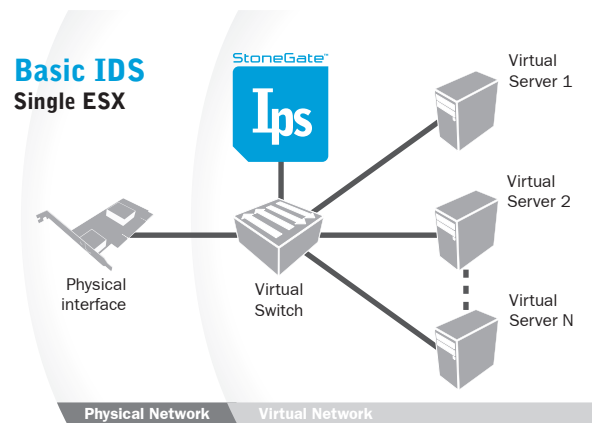
The exclusive StoneGate Virtual IPS technology allows very accurate detection and prevention. It is based on multiple contextual methods:

- Vulnerability centric protection signatures (customizable logical expressions)
- Zero day vulnerability protection, protection against new attack variant or vulnerability without software vendor patch
- Network application identification (for example, P2P inside HTTP)
- Advanced reconnaissance detection.

StoneGate Virtual IPS can be installed in the virtual architecture in traffic inline mode and/or in capture mode.



In inline mode, an attack is blocked instantly before it can reach its target by simply placing StoneGate Virtual IPS in front of the virtual machines.

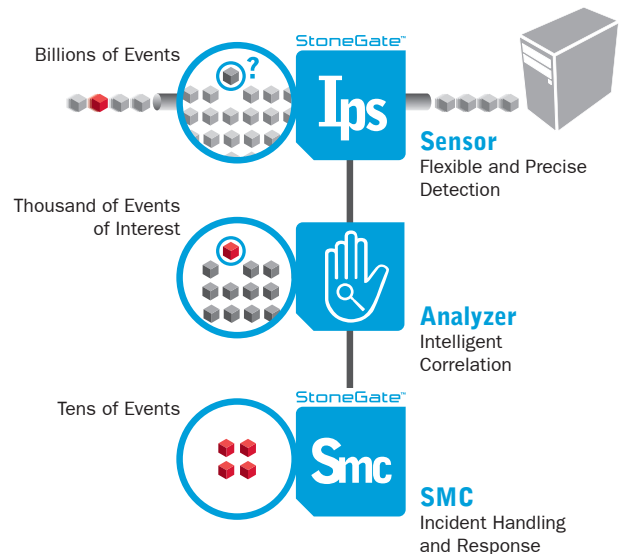


In capture/capturing mode, all traffic is analyzed on a virtual switch by the port mirroring functionality. This switch can also block traffic by delegating this task to another StoneGate IPS and/ or FW engine.

StoneGate Virtual IPS also supports Transparent Access Control (TAC), which is used to set up level 2 to 7 access rules in addition to the IPS functions. This feature makes it easy to segment a network efficiently by implementing StoneGate firewall rules. It also prevents unauthorized access between various zones, virtual or physical, with different security levels.

Functionality at a glance

- Protects vulnerable applications against network attacks, including client and server vulnerability on Windows, Linux/Unix and, other operating systems.
- Detects spyware, denial-of-service (DoS) attacks (rate and non-rate-based DoS), port scans, Trojan horses, worms, protocol anomalies, and network transactions.
- Includes diverse range of inspection methods, such as protocol validation, malicious activity detection, generic and contextual signatures, denial-of-service detection, scan detection, and event correlation over time and space for detected events.
- Thousands of signatures for more than 160 protocols - HTTP, DNS, IMAP, SMB, MSRPC, MYSQL, Oracle, POP3, and many others.
- Accommodates for user-definable signatures that use regular expression syntax to ensure greater protection against vulnerability.
- Provides an intelligent event correlation mechanism to reduce false positives.
- Allows advanced blacklisting and whitelisting in conjunction with other StoneGate virtual and/or physical appliances.
- Allows implementation of inline mode and/or sensor mode within the same virtual appliance.
- In inline mode, allows automatic and immediate blocking of detected anomalies or attacks.
- Vulnerability centric protection and virtual patching ensures regulatory compliance.



This offer is available on an annual fee basis, thus providing all the flexibility expected in this type of environment (please note that the service can be started or discontinued upon request):

	Basic 8/5	Premium 24/7
StoneGate Virtual IPS	995 €	1,495 €
StoneGate Virtual FW	599 €	799 €

The prices include the StoneGate Management Center (SMC).