

FIREWALL

StoneGate SG-4000

Stonesoft's StoneGate SG-4000's high availability, and networking and performance features make it a good fit for large enterprises.

Stonesoft, www.stonesoft.com

Price: Starts at \$36,500

Large enterprises that value performance and availability as much as data integrity and confidentiality will find Stonesoft's StoneGate SG-4000 network firewall's high availability, scalability and low maintenance requirements hard to beat.

SG-4000's impressive networking capabilities offer significant value. Its multilink technology provides uninterrupted availability for Internet and VPN traffic without the cost of redundant routers and switches, or configuring routing protocols such as BGP. Clustering for up to 16 nodes and load balancing for each connection eliminate the need for third-party devices.

The 3U hardened Linux appliance is the biggest and strongest of the StoneGate line, with 22 copper interfaces for scalability in complex, high-performance network environments. Stonesoft rates it for 3.1-Gbps firewall throughput and 500 Mbps for VPN for up to 500,000 concurrent sessions.

Stonesoft's multilayer inspection engine can act as a packet filter, stateful inspection or application firewall, using the appropriate method for the type of traffic and the rule it's matched against.

There's little need to touch the appliances after initial configuration; the Management Center is used for just about every administrative and maintenance task. In our lab, we installed its components—management server, client, log server and monitoring server—on a single Windows 2003 Server (Linux and Solaris are supported) to manage two clustered SG-4000s.

With great features comes complexity. It might take a while and a few reads of the administrator's guide to get accustomed to the GUI because of the many configuration options and features.

The Management Center streamlines administration through the use of a base template, inherited rules,



Hotpick

and a straightforward drag-and-drop interface for adding rules and configuring routing, among other things. Default templates include basic rules governing communication to and from the firewall units, and a deny-all statement, which forces administrators to explicitly allow permitted traffic.

Inherited rules greatly facilitate managing multiple firewalls, each with its own rules to protect its network. The first rule base created inherits all the rules in the default template. Managers can then use this rule base, say, for North America, to create a rule base for New York by adding rules that apply specifically to that network.

While this can save a lot of time and effort for large enterprises, the inherited rules in the branch firewall can't be modified, making creation and removal of exceptions difficult.

Other administrative tasks are a snap. It takes only two mouse clicks to back up the configuration and rule sets of clustered SG-4000s, or restore the system from a backup.

Remote software upgrades are simple and can be scheduled. The rollback feature is invaluable for testing connections before committing to an upgrade.

Although SG-4000 is expensive, it's a great value, providing enterprise-level performance and high availability and load balancing, without the expense of additional devices and the staff required to manage them. •

—PHORAM MEHTA

Test Notes

↑	HA, load balancing
↑	Inherited rules
↑	Easy backup/restore
↑	Upgrade rollback

Reprinted with permission from Information Security Magazine, February 2006.
All Rights Reserved. FosteReprints: 1-866-879-9144

STONESOFT

Stonesoft Inc.

info.americas@stonesoft.com