

Never has the firewall been asked to do so much. Although firewalls have long offered extras, such as the ability to do VPN processing and content filtering, today vendors are throwing in the kitchen sink, including virus and spam filtering and even intrusion detection and prevention.

Putting all of these functions into one box and behind one management interface sounds like a winning idea, but what happens to firewall performance when you turn all of these services on? That was one question I wanted to answer when I tested two full-featured firewalls, Fortinet's FortiGate 800 and ServGate Technologies' EdgeForce Accel, at Spirent Communications' lab.

In addition to examining ease of setup, manageability, and security features, I used Spirent's Avalanche 5.2 and Reflector 5.2 test suites, running on Avalanche 2500 and Reflector 2500 hardware, to assess the performance of these gigabit-capable boxes. Avalanche and Reflector emulate multiprotocol traffic (namely HTTP, FTP, POP3, and SMTP) between a number of clients and servers, which allowed me to test performance under load with all features and filtering disabled, and when enabled, to determine the performance hit the device would take.

To assess firewall functionality, I emulated a Syn Flood, the only denial-of-service attack that phased participants in my previous test, and I created basic functionality tests to ensure that the Fortinet and ServGate firewalls handled an e-mailed virus and a forbidden URL Get request successfully.

Finally, to prove out VPN muscle, I used Spirent's TeraVPN 4.0 to test throughput for both 10 and 200 LAN-to-LAN tunnels. I verified data passage across all tunnels using six different payload sizes, from 64KB to 1350KB.

### Fortinet FortiGate 800

Since I tested the FortiGate 500, Fortinet has packed a full load of security services into its firewalls and given them a new, slicker front-end with the recent 2.8 release of the FortiOS operating system. Fortinet has beefed up the firewall's routing features by enhancing support for RIP (Routing Information Protocol) I and II and adding support for OSPF.

Firewall capabilities are also improved, through increased granularity of protection profiles and the ability to customize security features such as anti-virus, Web filtering, Web category (URL) filtering, anti-spam, intrusion prevention, and content logging. For example, the drop down window for intrusion prevention now has signature and anomaly subsections that give you up to eight action options.

The FortiGate's dashboard, or System Status page, is pretty cool. It gives you a quick overview of important information such as recent viruses, attack



**Firewalls:** Now featuring everything but the kitchen sink

detections, and the status of system resources. One of the handiest additions I found in FortiOS 2.8 is that command line access is now available with a single click from the main task bar icon. Other useful additions include a signature-based "grayware" malware category and a backup and restore feature, which should have been included sooner.

The FortiGate 800 turned in an excellent performance in my VPN throughput tests; firewall performance was also impressive. Although the maximum connections per second I achieved in the lab (3200) fell far short of the vendor's claim of 10,000, the maximum number of concurrent connections the box was able to handle (446,000) beat both Fortinet's spec and the ServGate box (131,000), the latter by a wide margin.

With all security features enabled, the FortiGate 800 took a significant hit in terms of its ability to serve new connections, achieving just 900 connections per second before choking, representing a 72 per cent drop in performance.

I was pleased with the FortiGate's VPN performance. The box arrived with VPNs preconfigured according to my test plan, using AES (Advanced Encryption Standard) 128-bit encryption, and I was able to pass data through the tunnels — in all six payload sizes — immediately. The box proved out at 544Mbps for the 10-tunnel test and 424Mbps for the 200-tunnel test, again exceeding Fortinet's marketing data.

The FortiGate also nailed my anti-virus and URL-filtering tests, stripping all of the infected files and blocking all of the verboten addresses I threw at it, while continuing to serve all legitimate requests. The denial of service attack test didn't go as smoothly, however. The Syn Flood caused the device to drop 36 per cent of legitimate traffic.

### ServGate EdgeForce Accel

Since my previous look at the EdgeForce Accel, ServGate has incorporated several important modifications and enhancements in its version 4 release of the ServGate OS. Like the FortiGate, the Accel combines firewall, VPN, anti-virus and anti-spam (both via McAfee), and URL and Web content filtering. It lacks intrusion detection and prevention; ServGate says this feature is on the product roadmap.

After firing up the box, the first change I noticed was a new dashboard that provides an at-a-glance view of major system summary info. More important changes lie beneath the surface, including a central management console that gives admins full control of remote devices, and a new wizard that speeds up

VPN configuration. Customisable security templates which you can push to multiple devices over a network, and policy-based filtering, which allows you to apply different firewall rules to different areas of your network, are now also part of the bargain.

Other enhancements include a Bayesian spam filter from McAfee and support for RIP I and II routing. ServGate OS 4.0 also delivers ICSA-certified VLAN pass-through, a full command line interface, and a boot-time feature that allows admins to revert to previous versions of the OS.

The EdgeForce Accel bested the FortiGate in tests of maximum connections per second, turning in 8,500 cps in my raw, sans-services baseline test and clocking 2,600 cps with all features and filtering enabled. That 70 per cent drop was nearly identical to the performance hit suffered by the FortiGate 800, showing that additional security services significantly hinder the firewall's ability to serve flows of new connections, such as when users log in to a network at the beginning of each day.

Like the FortiGate, the Accel also passed my URL and anti-virus filtering tests with flying colours. Unlike the FortiGate 800, it handled my denial of service attack successfully, continuing to serve legitimate traffic when fighting off the Syn Flood.

The ServGate did not keep pace with the FortiGate in my tests of maximum concurrent firewall connections and VPN throughput. Although perfectly acceptable, the EdgeForce Accel's concurrent connection figure of 131,000 fell far short of FortiGate's 446,000. And its 10-tunnel and 200-tunnel VPN throughput numbers of 196Mbps and 153Mbps represent just a fraction of what the FortiGate 800 achieved.

Which firewall to choose? If performance and scalability, or brawny VPN capabilities, are your chief considerations, then the FortiGate 800 has the edge. Overall, however, I'd give the nod to ServGate's EdgeForce Accel, due to its superior management capabilities, easy setup, and solid performance under attack. Whichever firewall you choose, keep in mind that those extra security features will cost you dearly in performance.

*Alyson Behr is an InfoWorld contributing editor.*

## Local information

**RRP:** Fortinet FortiGate 800 costs \$19,295. The product is distributed in Australia by Seccom Networks and Avante IT. For pricing details and a list of distributors in Asia/Pacific visit [www.servgate.com](http://www.servgate.com)