

# InfoWorld

August 8, 2003 ■ ISSUE 31

GET TECHNOLOGY RIGHT

Low-cost appliances challenge pricey security platforms in our attack test

## Firewall

## Free-for-All

FOR BUSINESSES LARGE AND SMALL, firewalls mean more than network security, they also mean unknown amounts of network downtime during configuration and loads of extra expense for consultants and hardware fees. If you need more than traditional firewalling, such as the ability to secure IP telephony or protect application traffic, the solutions become even more expensive and difficult to configure.

Enter the firewall appliance. Previously, these machines represented basic firewall functionality with a concentration on increasing ease of use, thus allowing ordinary IT mortals — instead of expensive network security specialists — to configure and manage them. Now, along with offering straightforward setup, these devices have gotten smarter, incorporating the ability to defend against certain application-layer attacks,

BY OLIVER RIST AND WAYNE RASH ILLUSTRATION BY CHARLIE HILL

# As expected, the Enterasys security router blew the doors off the appliances in our performance tests.

and branching out into areas traditionally reserved for more advanced and resource-heavy security products.

How far have firewall appliances come? To find out, we tested three in this roundup — the low-cost Ingate Firewall 1400; the even more affordable Toshiba Magnia SG20, which runs Astaro Security Linux; and the pricier Nokia IP380, which incorporates Check Point's firewall and VPN software. To help flesh out the key differences between the appliance and the traditional firewall router, we also reviewed one of the latter, the Enterasys XSR-3250. The Enterasys promises tremendous power and flexibility, and like the Nokia, it has a price to match.

We tested our firewalls using Ixia Communications' Ixia 1600 traffic-generation chassis and WebLoad testing software. WebLoad not only establishes throughput baselines based on real-world traffic flows but also generates a variety of attack streams. We tested each firewall's performance and defense capabilities by generating stateful traffic, using a mix of protocols and seeing



Ingate Firewall 1400

how each responded to four application-layer attacks: the Ping of Death, Smurf, Syn, and Teardrop.

In addition to evaluating performance under load — how well the firewall continued to process legitimate traffic while under attack — we scored our four competitors on the basis of the total volume of traffic it could handle, the amount of effort and time required to configure the device, and the quality of the tools the vendor provided for long-term device management.

Among our appliance contenders, the Toshiba stood out in all categories, including performance, ease of use, and price. The Ingate performed adequately, but it was a step or two behind the Toshiba in performance, security, and manageability. The Nokia also performed well but not as well as expected,

considering its high-end Check Point software and high price tag, and the difficulty of configuring it without Check Point expertise. The Enterasys security router performed as expected; as is the Nokia, it's expensive and difficult to configure, but it blew the doors off the appliances in our performance tests.

## Firewall Phone Home

Ingate's Firewall 1400 is the company's midrange product aimed at medium to large networks. It performs all the standard firewall functions you'd expect. You can use it to deliver DHCP services, perform NAT, and support as many as 100 VPN tunnels. And of course, the Firewall 1400 also performs packet filtering and stateful inspection. Equally important in today's environment, the device is designed to handle DoS (denial of service) and DDoS (distributed denial of service) attacks by dropping the offending packets.

Configuring the Firewall 1400 is fairly simple, although it could be a little easier. Unlike the Toshiba appliance, in which setup is

**Enterasys XSR-3250 Security Router**  
Enterasys Networks  
[enterasys.com](http://enterasys.com)

<b>VERY GOOD</b>	<b>7.7</b>
Security (25%)	9
Management (20%)	8
Ease of Use (15%)	6
Scalability (15%)	9
Setup (15%)	6
Value (10%)	7

**COST:** \$9,995, base price; \$1,495, firewall feature set; \$5,495, VPN feature set

**BOTTOM LINE:** A classic security gateway combining firewall and WAN routing capabilities, the Enterasys XSR-3250 is both pricey and powerful. If you don't require appliance-like ease of configuration and management, this machine is definitely worth a look. Thanks to GbE capability, it easily led the field in our performance tests, including performance when under attack.

**Ingate Firewall 1400**  
Ingate Systems  
[ingate.com](http://ingate.com)

<b>VERY GOOD</b>	<b>7.1</b>
Security (25%)	7
Management (20%)	7
Ease of Use (15%)	8
Scalability (15%)	5
Setup (15%)	8
Value (10%)	8

**COST:** \$3,400

**BOTTOM LINE:** Ingate's firewall appliance features an easy-to-use Web-based management GUI that can control every aspect of the firewall's configuration and operation, although it's not quite as polished as Toshiba's interface. With performance typical of an appliance, the Ingate managed to defend against all four of our attack scenarios, but overall throughput was significantly hampered by two of them.

**Nokia IP380**  
Nokia Americas  
[nokia.com](http://nokia.com)

<b>VERY GOOD</b>	<b>7.3</b>
Security (25%)	8
Management (20%)	8
Ease of Use (15%)	6
Scalability (15%)	8
Setup (15%)	6
Value (10%)	7

**COST:** \$9,995, base price; \$9,450, unlimited Check Point Firewall-1/VPN-1 license

**BOTTOM LINE:** Nokia's IP380 may not be an appliance, but it still represents a robust firewall and VPN concentrator solution for high-end businesses. Its dependence on Check Point's Firewall-1/VPN-1 platform means not only additional licensing costs, but also that a skilled Check Point administrator is required to configure it. Nevertheless, this security platform can protect anything from a small business to a large enterprise network.

**Toshiba Magnia SG20**  
Toshiba America Information Systems  
[shoptoshiba.com](http://shoptoshiba.com)

<b>EXCELLENT</b>	<b>8.6</b>
Security (25%)	8
Management (20%)	9
Ease of Use (15%)	9
Scalability (15%)	8
Setup (15%)	9
Value (10%)	9

**COST:** \$2,295, base price

**BOTTOM LINE:** Toshiba and Astaro have teamed to provide an exceptionally polished and extremely robust security gateway for a very reasonable price. Combining Toshiba's well-muscled hardware platform and Astaro's secure Linux distribution, this product not only surprised us in benchmark testing, but also had the most polished and easy to use Web-based management system we've seen to date.

## Sizing Up Firewalls

Easy-to-configure appliances such as the Ingate and Toshiba are beginning to challenge their higher-end brethren in features and defense capabilities, if not performance.

	OPERATING SYSTEM	RACK-MOUNTABLE	STANDARD PORTS	OPTIONAL PORTS	WEB MANAGEMENT	EVENT ALERTING	SYSLOG	STATEFUL INSPECTION	PACKET FILTERING	CONTENT FILTERING	VIRUS PROTECTION	SPAM FILTERING
<b>Enterasys XSR-3250 Security Router</b>	EOS	yes	three 10/100/1000	six additional network interface slots	no	yes	yes	yes	yes	no	no	no
<b>Ingate Firewall 1400</b>	Linux 2.4	no	four 10/100	none	yes (console required)	no	no	yes	yes	no	no	no
<b>Nokia IP380</b>	Nokia IPSO / Check Point Firewall-1/VPN-1	yes	four 10/100	eight 10/100; V.35/X.21; ISDN-BRI	no (console and GUI combination)	yes	yes	yes	yes	yes	no	no
<b>Toshiba Magnia SG20</b>	Astaro Security Linux	no	eight 10/100	None	yes	yes	yes	yes	yes	yes	yes	yes

accomplished entirely from the supplied Web browser interface, Ingate forces you to first access the box via a console cable to set basic IP addressing and password information at the command line. After basic setup, further configuration and management is handled by an easy-to-use Web-based GUI. This isn't the sexiest GUI on the planet; using it feels a lot like filling out tax forms on the Web. But it's functional, intuitive, and complete.

Ingate's Web GUI makes it easy to select the basic features you need, including DHCP, NAT, and encryption. Inspection rules are configured via an extended, list-oriented interface that allows administrators to configure both predefined inspection rules and custom rules. Nokia and Enterasys provide more flexible rules definition, but for small- and midsize business requirements, the Ingate's capabilities should more than suffice.

What takes the Firewall 1400 beyond the ordinary is its capability of functioning as a SIP (Session Initiation Protocol) proxy, and directing SIP traffic to the right destination by using its internal NAT tables. Managing SIP traffic is relatively new for firewalls and aimed strictly at organizations that want to run VoIP (voice over IP) outside the firewall. The Ingate firewall not only protects VoIP streams, which are vulnerable to a variety of hacking techniques as soon as they leave your network, but also aids in their performance and hence the quality of VoIP communications.

In our performance and attack testing, the Firewall 1400 did quite well, although we do consider it the least muscular of all our entries. In our baseline throughput tests, for example, it came in slightly behind the Toshiba and Nokia entries, and well behind

the Enterasys machine. It managed to defend against all four of our attack sequences, but its overall throughput was significantly hampered by both the Syn and Smurf attacks.

Finally, we had some trouble getting the Ingate box to recognize our initial addressing scheme; a quick reconfiguration took care of that. Overall, the Ingate represents a solid value for midsize networks, especially those looking to take advantage of secure VoIP systems.



Toshiba Magnia SG20

### Secured by Linux

For our money, we found that Toshiba's Magnia SG20 provided the best balance between appliance-style ease of use and advanced security technology in this roundup. The combination of Toshiba hardware and Astaro Security Linux software arrives as a preinstalled security gateway that literally covers all the bases.

You'll not only find a highly configurable stateful inspection and packet-level firewall but also built-in virus protection, content filtering, and optional e-mail-oriented virus and spam protection. Application-level security is also addressed using DNS, HTTP, POP3, SMTP, and SOCKS proxies. And as do most firewall appliances these days, the Toshiba device can also function as an IPsec-based VPN concentrator, creating and handling encryption for remote user and site-to-site VPN tunnels. You even get a choice of

supported encryption schemes, as Astaro can handle AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard), Blowfish, or Twofish.

But what really sets Toshiba's box apart is Astaro's user interface. It's clear from the get-go that Astaro has gone all out with the fit and finish of the WebAdmin browser-based management tool. "Slick" only begins to describe WebAdmin in terms of both flexibility and ease of use. Whereas we were able to configure the Ingate in less than two hours (great for a firewall), the Toshiba box was fully functional in less than 45 minutes, including setting up the addressing, 20 inspection rules, and full VPN functionality.

Astaro also does a nice job of leveraging the underlying Linux OS for management purposes. Obviously, it's a hardened version of the OS, but it allows you to leverage its management capabilities via SNMP or Syslog. Astaro also offers an online updating service that can automatically update the OS and its security gateway against the latest security threats.

On the hardware side, Toshiba's Magnia SG20 hardware provides a surprising amount of processing muscle and plenty of connectivity, including a single 10/100 interface for public access and seven 10/100 interfaces for the private LAN side. A single 10/100 port is designated as an uplink port for expansion purposes.

Our testing showed the Toshiba/Astaro solution on par with the big boys. Raw HTTP-based throughput tests proved it to be faster than the Nokia appliance, and it performed better than the Nokia under the Ping of Death, Syn, and Teardrop attack sequences. For the most part, the product seemed almost

# Toshiba's Magnia SG20 provided the best balance between appliance-style ease of use and advanced security.

unaffected by our attacks, yet it suffered a slight throughput hit during the Syn attack and a heavy hit during the Smurf attack.

Nevertheless, despite generally high latency numbers and succumbing to the Smurf attack, we liked the Toshiba/Astaro combo very much. For sheer price/performance and true appliance-style ease of use, the Toshiba Magnia SG20 is the box to beat.

## Check Point Inside

The Nokia IP380 is a robust box carrying four integrated 10/100 ports (expandable to eight) and rated at a maximum of 600Mbps of secured firewall throughput. According to Nokia, it's also capable of 90Mbps of 3DES VPN-based throughput and 130Mbps via an optional accelerator card. (We didn't test our firewalls' VPN capabilities.) Additional features or memory expansion can be accomplished via a proprietary slide-out expansion tray.

Inside, the Nokia runs two software applications: Check Point's Firewall-1/VPN-1 NG and Nokia's own Voyager package for device management. That's where our trouble began: Despite Nokia's claims for appliance-like ease of setup, we found that you've really got to be an expert Check Point user to get the Nokia IP380 running. Without this knowledge, it's extremely difficult to tell where to configure each of the box's capabilities — Voyager or Check Point.

Although Voyager shows granular aspects of the IP380's security configuration, it's really just for local hardware and network management. This gets configured first. Then you proceed to Check Point — not via its GUI but via the command line — to configure all basic firewall settings, including rules and VPN tunneling. When these settings are configured, you can manage and modify them via the Check Point GUI.

On the upside, the Nokia device offers all the power and cutting-edge flexibility that users expect from a Check Point product. But it's not what you'd expect from an appliance; appliance-like ease-of-use simply isn't a feature of the IP380. This is a high-end firewall and VPN aggregator aimed at high-end needs and high-end budgets.



Nokia IP380

With a base price of \$9,995, plus Check Point licensing fees, we expected the Nokia IP380 to place either first or second in our firewall and attack sequence benchmarks. Instead, it placed a close third behind the Toshiba appliance, not only in raw throughput but also under three of the four attack sequences (the Smurf attack was the exception). Although it was slightly slower than the Toshiba entry, the IP380 was also steadier, and it produced better latency numbers. Where the Astaro doubled over and whimpered under Smurf, the Nokia merely grunted, losing a significant but not crippling number of packets, and kept on chugging.

For power and flexibility, we think the Nokia IP380 has a definite place in large enterprises with large IT budgets and qualified Check Point administrators on hand. If the company's VPN claims are true, the box could be a definite boon in large networks with lots of remote connections. For smaller businesses, however, and especially those looking to implement security via an easy appliance-style management interface, this product doesn't hit the mark.

## Firewall Meets Router

The Enterasys XSR-3250 is one of the larger members of the Enterasys XSR security router family, which attempts to combine security considerations and WAN routing tasks into a single chassis. Although it's not an appliance by any means, its dual nature might still be attractive to midsize businesses as an all-in-one security gateway and especially to large enterprises requiring more muscle in their remote sites than an appliance can provide.

The XSR-3250 carries six network interface module slots configurable with a variety of LAN and WAN ports. It was the only device in the roundup capable of 10/100/1000 connectivity on the LAN side, and it can handle

site-to-site as well as single-user remote-access VPN connectivity at as many as 3,000 simultaneous tunnels (as many as 5,000 tunnels via hardware upgrade). And of course, it also features a policy-managed stateful inspection firewall and full WAN routing capabilities.

Configuration is a bit of a problem if you're expecting an appliance-style Web browser-based interface; setup is via command line only. Enterasys' OS appears at first to be a Cisco IOS (Internetwork Operating System) clone, but close inspection reveals any number of small syntax and process differences that prevented our Cisco-educated lab tester from getting the device running with our full suite of traffic rules installed and configured.

Only after we enlisted the services of an Enterasys-trained network manager did the security router come fully to life. The good news here is that when this machine is humming, it's really humming. Gigabit networking capability on the LAN side easily assured the XSR-3250 first place in our performance tests by a wide margin. And although this was a given from the start (considering its additional bandwidth), the Enterasys showed careful engineering here as well.

Impressively, the Enterasys was almost completely impervious to all four of our attack sequences. The Ping of Death and Teardrop attacks had virtually no impact on performance, and the Enterasys only barely registered any additional load when hit with either Syn or Smurf. Even the second-fastest box, Toshiba's Magnia SG20, was noticeably affected by more than one attack form. The XSR, however, simply grinned and bore it.

Obviously, neither the XSR's pricing (\$11,490, not including VPN capabilities) nor its management interface orient it toward the appliance arena. But if you're willing to spend some extra money and time, the XSR-3250 is an outstanding example of what you give up when you only concentrate on ease of use.

## Rise of the Appliance

Firewall appliances have come a long way since their inception. The standout product here was definitely the Toshiba/Astaro combination.

## The only area where a router-based product has an advantage over appliances anymore is performance.

This device not only led the Ingate appliance in ease of use and price, it also came in second overall in our performance test, a black eye to the much more expensive Nokia IP380. The Toshiba also demonstrates the new trend in appliance flexibility.

Previously, appliances were limited in their capability of incorporating new functionality through firmware upgrades, making it difficult to keep pace with a quickly changing attack landscape. Router-based OS approaches were more difficult to configure, but they provided much more flexibility in responding to new threats. They also allowed you to install new security applications on top of existing configurations. The Check Point Firewall-1/VPN-1 platform, for example, can incorporate




Enterasys XSR-3250 Security Router

Check Point's application layer firewall product, SmartDefense, as an additional software layer.

Toshiba's use of Astaro's Security Linux distribution, however, puts a dent in that strategy. Linux is more robust than most router OSes, and it can be made to accept any new third-party security application, although few have been developed. This means that a low-cost appliance such as the Toshiba Magnia SG20 could provide

long-term protection equal to the Enterasys and Check Point platforms. The only area where a router-based product has an advantage anymore is performance — witness the Enterasys, which more than doubled the Toshiba in most of our performance scores.

Still, the Toshiba Magnia SG20 costs a fraction of the Enterasys XSR-3250, and it can be clustered and even load-balanced with additional options. For cost-effective protection, the Toshiba/Astaro product and devices similar to it can make a real difference in the purchasing patterns of midsize businesses, which may need all the flexibility but not necessarily all the horsepower that a router approach has previously offered. 

# TOSHIBA

Toshiba America Information Systems, Inc.  
Computer Systems Group  
9740 Irvine Boulevard, Irvine, CA 92618-1697, USA  
Tel: 1-800-TOSHIBA  
www.solutions.toshiba.com • magnia@tais.toshiba.com



Astaro Corporation, 67 S. Bedford St., Suite 400W  
Burlington, MA 01803, USA  
Tel: +1 781 229 5880 • Fax: +1 781 359 1802  
www.astaro.com • salesus@astaro.com

Astaro AG, Pfingsttalstrasse 90, 76227 Karlsruhe, Germany  
Tel: +49 721 490 0690 • Fax: +49 721 490 069 55  
www.astaro.com • sales@astaro.com