

# ONE-STOP SECURITY

ALL-IN-ONE APPLIANCES UNLEASH MULTIPLE FORMS OF THREAT PROTECTION FOR YOUR NETWORK, SIMPLY AND INEXPENSIVELY

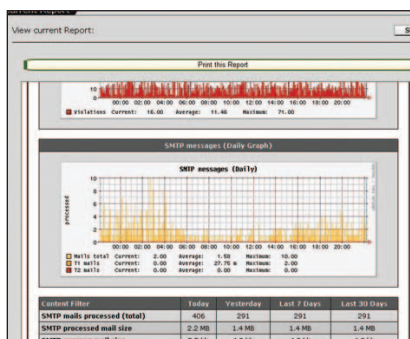
## Astaro Security Gateway 220

\$4,035 direct. Astaro Corp., www.astaro.com.



The Security Gateway 220 is an impressive, medium-size appliance that has no user license limit and integrates an updated version of Astaro's stellar threat-management software, Astaro Security Linux (ASL). The software won our Editors' Choice last November, and the Gateway 220 earns our award in this roundup.

The Astaro 220 supports up to 280 Mbps throughput on the firewall, more than any other appliance here, and up to 105 Mbps throughput for the VPN. It also



ASTARO'S Daily Executive Report can be viewed in a browser, printed, or automatically e-mailed to the administrator.

comes with eight 100-Mbps Ethernet ports, plus a 1.2-GHz Pentium III processor, 512MB of RAM, and a 40GB hard drive.

This should offer plenty of space for all log file and reporting data.

The ASL software impresses us with its ease of use and attention to detail. In fact, it has satisfactorily addressed many of the gripes we had with the multi-function security appliances in our March 2003 roundup, such as quarantine queues that cannot be sorted or searched, or units that lacked IDS (Intrusion Detection).

Built on a mix of open-source and commercial components, the firmware provides six pillars of security for the network: a firewall, antivirus (Kaspersky Labs' engine), intrusion protection, content filtering, spam protection and a VPN gateway. The full-featured firewall supports Network Address Translation (NAT), including source/destination NAT, IP

## SCORECARD

The rating for **setup and deployment** reflects all the steps needed to integrate each appliance into an existing or new network infrastructure. For **versatility and features**, we look at the feature set and options that allow for a flexible deployment in advanced networks, including gateway functions, available network topologies, and remote VPN connectivity. For **management interface**, we analyze each device's interface and how easily specific tasks can be completed. **Firewall, VPN, antispam, antivirus, and intrusion**



**detection** ratings reflect the implementation, quality, usability, and effectiveness of each respective feature. For **ongoing management**, we evaluate how easy it is to perform necessary, recurring maintenance tasks. The **logging and reporting** rating reflects the facilities the appliance provides to inform the administrator of system status, alerts, user activity, and common and hostile traffic patterns. Finally, the **overall** rating is not an average, but an aggregate based on analysis by PC Magazine Labs staff.

	Setup and deployment	Versatility and features	Management interface	Firewall	VPN	Antispam	Antivirus	Intrusion detection	Ongoing management	Logging and reporting	OVERALL
<b>Astaro Security Gateway 220</b>	●●●●	●●●●●	●●●●●	●●●●●	●●●●●	●●●●●	●●●●	●●●●●	●●●●	●●●●●	●●●●●
Fortinet FortiGate 200A	●●●●	●●●●	●●●●	●●●●●	●●●●	●●	●●●●	●●●●●	●●●●	●●●●	●●●●
ServGate EdgeForce	●●●●●	●●●●	●●●●	●●●●●	●●●●	●●●●	●●●●	●●●●●	●●●●	●●●●	●●●●
SonicWALL Pro 2040	●●●●	●●●●	●●●	●●●●●	●●●●	●●●	●●●●	●●●●	●●●	●●●	●●●●

RED denotes Editors' Choice.

- - EXCELLENT
- - VERY GOOD
- - GOOD
- - FAIR
- - POOR

masquerading, and load balancing. It provides very granular intrusion detection, with the ability to block suspect traffic. We like that the 2,000-plus rules are grouped in service categories, and that administrators can observe which rules are being triggered by violations—very helpful in troubleshooting bad traffic. The firmware includes several proxy servers—an HTTP cache proxy, a SOCKS proxy, and an SMTP relay with antispam and AV, just to name a few.

A new firmware addition with Version 5.2 is spyware protection, which blocks incoming spyware and adware and prevents malicious programs from sending confidential information outside of your network. The full-featured VPN endpoint allows for in-depth configuration and complete control over policies.

The Astaro 220's logging and reporting sections are equally outstanding: They offer querying, searching, sorting, and live log views. We especially like that the proxy queue, which holds questionable e-mails, can be searched by the sender, the receiver, or other free-form configurable strings to track down a message that might have been caught erroneously. In addition, the administrator can configure the system to send a daily spam digest to all users with valid e-mail addresses.

The appliance can send encrypted backups of its configuration files to the administrator on a set schedule. It also supports remote syslog and accounting. Remote management and user authentication against AD, LDAP, RADIUS, or SAM are further indications that the Astaro Security Gateway 220 is an extremely well-rounded, capable, and powerful product.



Toll-Free: 1-877-427-8276  
 Americas: salesus@astaro.com  
 EMEA: info@astaro.com  
 APAC: salesasia@astaro.com

## Astaro Security Gateway 220



All the products in this roundup offer a strong set of features and are of high quality, but the Astaro Security Gateway 220 is our top choice among them: It has an extremely well-rounded set of features, the best-designed interface, and the most valuable reporting for the administrator. Daily executive reports, searchable logs, live logs, daily spam digests for each individual user, and a fully featured SMTP proxy gateway are among the unique features that impressed us.

Trailing close behind the Astaro were the appliances from Fortinet and ServGate. The ServGate, however, fell short in its logging and reporting features, and the Fortinet's lack of a spam quarantine hurt its overall rating. We believe that catching spam at the gateway is a more desirable option than tagging it and funneling it through your mail server to the individual user.

The Fortinet and ServGate appliances are both quite capable and would serve businesses well, but the Astaro Security Gateway 220 simply offers the most complete package, the most flexibility, and the best bang for the buck.

### SUMMARY OF FEATURES

## Security Appliances

Download this table at  
[www.pcmag.com](http://www.pcmag.com)

	Astaro Security Gateway 220	Fortinet FortiGate 200A	ServGate EdgeForce	SonicWALL Pro 2040
Price for unit, including antispam and antivirus for 50 users	\$4,035 direct	\$3,495 direct	\$3,300 street	\$2,995 direct
<b>GENERAL</b>				
Routeable network port count	8	8	3	4
Unit can be configured for failover	■	■	■	■
<b>MANAGEMENT AND INTERFACE</b>				
Management access via HTTPS/SSH/local	■■■	■■■	■■■	■□■
User authentication through local/RADIUS/LDAP	■■■	■■■	■■■	■■■
System configuration can be downloaded/restored	■■	■■	■■	■■
<b>SPAM FILTERING</b>				
SMTP/POP3	■■	■■	■■	■□*
Message format/header analysis	■■	■■	■■	□□
Whitelist for e-mail domain/IP address	■■	■■	■■	□□
RBLs/reverse DNS lookup	■■	■■	■■	■□
<b>SPAM HANDLING</b>				
Message can be quarantined/blocked/marked	■■■	□■■	■■■	□■□
Quarantined messages can be forwarded to recipient	■	N/A	■	N/A
Notification to recipient/daily digest	■■	■□	■□	□□
<b>ANTIVIRUS</b>				
SMTP/POP3	■■	■■	■■	■■
FTP/HTTP	■■	■■	■■	■■
Virus can be cleaned/deleted/quarantined	■■■	■■■	■■■	□■□
Quarantined content can be forwarded to recipient	■	■	■	N/A
Notification to recipient	■	□	■	■
<b>FIREWALL</b>				
NAT route mode/bridge mode	■□	■■	■■	■□
NAT modes: One-to-One/One-to-Many/Many-to-One	■■■	■■■	■■■	■■■
Max throughput (in Mbps)	280	150	150**	200
<b>VPN</b>				
IPSec L2TP/PPTP	■■	■■	□■	■■
Max simultaneous tunnels/throughput (in Mbps)	500/105	200/70	500/30**	50/50
<b>LOGGING AND REPORTING</b>				
Logs activity for AV/Spam/VPN	■■■	■■■	■■■	■■■
Live logs available/Logs are searchable	■■	□■	□■	□□
Executive report summary	■	□	□	□
<small>RED denotes Editors' Choice.          N/A—Not applicable: The product does not have this feature. * Provides only RBL blocking. ** With optional performance module.</small>				