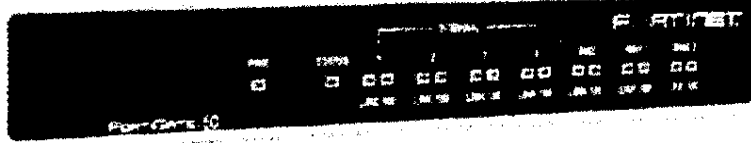


# LabReport



**The FortiGate-60: Its anti-virus engine supports common compression formats up to 12 layers deep and differentiates among file types.**

## Impressive anti-virus protection on the cheap

By EDZLYZAM  
tip@nstp.com.my

**FORTIGATE-60 (Anti-virus firewall)**  
 Manufacturer: Fortinet Inc  
 Enquiries: SIS Distribution (M) Sdn Bhd  
 (Tel: 03-79588330) and Ingram Micro  
 Malaysia Sdn Bhd (Tel: 03-79698913)  
 Price: RM4,180

SOME enterprises put firewall on one machine and other services on an all-in-one server that can take care of spam and virus blocking – this is precisely the market that Fortinet is targeting with its new FortiGate-60 device.

With firewall ruled out, the box has three remaining tasks – filtering spam, removing viruses and blocking inappropriate Web sites. These tasks are done with the device working like just another machine on the network, which means installation is simply a matter of plugging the device in.

Once you've adjusted our workstations' Internet protocol settings to that of the FortiGate-60, you can easily access the responsive and secure Web onfiguration interface. Onfiguring your firewall comes next.

The FortiGate-60's user interface is intuitive. A set-up wizard helps to configure basic features easily. Though the FortiGate-60 does not have a wizard for firewall rules and policies, the device is a breeze to set up, thanks to easy-to-follow menus.

FortiGate-60 Anti-virus firewalls are dedicated hardware-based units that

deliver real-time network protection services at the network edge. Based on Fortinet's FortiASIC content processor chip, the FortiGate platforms are the only systems that can detect and eliminate viruses, worms and other content-based threats without reducing network performance, even for real-time applications such as Web browsing.

Fortinet's anti-virus engine is impressive. Protection for file transfer protocol (FTP), hypertext transfer protocol (HTTP), Internet message access protocol (IMAP), post office protocol 3 (POP3) and simple mail transfer protocol (SMTP) traffic is ensured by examining the content stream based on virus signatures, file-size thresholds, and block patterns. The anti-virus engine supports common compression formats up to 12 layers deep and differentiates among file types.

Administrators can also set limits on the allowed file size for each type of traffic. The device lets you customise the notification

sent after a virus is detected, though it supports only "reject/notify sender" or "reject/notify receiver" when a virus is found.

Fortinet pushes updates for its anti-virus and attack definition databases out to its device – the only manufacturer to do so. All of the latest updates are installed without having to schedule updates when a new threat emerges.

Although Fortinet's anti-virus scans for only 3,100 viruses compared with 60,000 to 80,000 viruses by other devices, the large disparity has to do with Fortinet focusing on in-the-wild viruses. These are viruses that have been most recently seen in real-world networks and don't include viruses for older technologies such as Windows 3.1.

However, the Fortinet device did detect all 80 real-world viruses sent through and caught *MyDoom* within 24 hours of its release.

Fortinet has also added a convenient feature for developing firewall rules called Content Profiles. Using the profile settings, you can determine what level of scrutiny you want to apply to the traffic pass-

ing through the device.

Rather than inspecting incoming and outgoing mail based on the format or other characteristics that might identify the content as spam, Fortinet deploys several manual filtering mechanisms, including content block and block list.

With content block, administrators can manually create filters for keywords such as "chat", "war", etc, while block list can be used to match pre-defined strings against e-mail headers to identify spam based on sender or domain information.

The FortiGate-60 also provides a built-in four-port switch in addition to its two wide area network ports and DMZ port. This provides you with connectivity for servers or other network devices that you cannot place behind a firewall.

While the overall device and most of its components are fairly easy to deploy, its spam filtering can be time-consuming to configure, and the product generally lacks some of the flexibility found in competing products, the most critical being the ability to quarantine attachments or files. For small companies that can accept its required labour and limitations, the FortiGate-60 offers solid protection on the cheap.

## Beefing up

By AHMED KAMAL  
tip@nstp.com.my

HACKING has become more accessible in recent years, to the point that an average layman can load tools and tutorials that teach him how to hack – maybe one day you will see a "Hacking for Dummies" on the shelves of your local bookstore. An abundance of books have been written on the topic of network security, but few have taken a nice step-by-step approach to beef up the security of your network.

*Hardening Network Infrastructure* by William Noonan aims to help you increase network security by reducing risks. Instead of being theory-based, the book mostly offers practical methods and procedures that you can apply immediately, making it handy for the busy network security professional.

The book is divided into four parts. Part one describes solutions that can be applied immediately to your existing network, presumably because they are quick solutions to take effect. Part two is followed by the second part, which describes a systematic approach to hardening your network infrastructure. Writing about security policy, hardening your firewalls, routing switches, and implementing a secure perimeter are some of the topics covered.

I did find one amusing about the book on securing wireless networks – Noonan suggests that the best way to handle that issue is to only ban wireless access points, but also disallow employees who v