

Business Plus Article – Oct 2004 Security

So you've installed your antivirus software and setup your firewall. You could be forgiven for thinking you were now safe from the perils of the Internet; you could be wrong! Not unlike airport baggage screeners, firewalls and antivirus software might catch most, but not all security threats. Opening the item for closer inspection may be required to catch the less obvious threats. To achieve this, you will need conscientious baggage inspection staff or, in the case of firewall security, an application layer firewall.

To understand what an application layer firewall can do for us, we must differentiate it from the more traditional network layer firewall. Consider the baggage screening scenario; it would be perhaps unwise to allow or block baggage based purely on where it came from or where it is going. This is effectively how a network layer firewall treats its traffic. A baggage handler who takes the time to open the suitcase and inspect the contents would be a far more effective security measure. In the world of Internet security, this conscientious baggage handler would be the application layer firewall, opening and examining all network traffic before allowing it through.

The latest generation of firewall packages use Deep Packet Inspection (DPI) technology. This is the capability to open and dissect network packets with some intelligence. By doing this, the firewall can decipher what to let in and what not to let in based on the *content* of the packets, not just the source or destination address. Because application layer firewalls view the information as a data stream, not just a series of packets, they have the ability to make these intelligent decisions based on a pre-defined or custom rule set. A network layer firewall would simply look at the header information, which contains information such as where the packet came from and where it's going, and then make such a decision. More and more, header checking or "stateful inspection" is failing to protect networks from malicious content. The infamous Code Red exploit of a couple of years ago managed to elude many a corporate firewall and wreak havoc on its victims. Had application layer firewalls been installed and configured correctly, it might have been a blip rather than a crisis.

Microsoft's latest generation firewall software, Internet and Acceleration Server (ISA) 2004 is a multilayer firewall Web-cache server. This means that it can minutely examine all data that enters your network via the firewall for any malicious content at several different layers - packet, circuit and application layers to be precise - whilst offering the performance benefits of intelligent Web caching (Frequently visited Web pages are stored in a quick access cache database so they can be delivered more efficiently thereby reducing the load on the firewall itself.) Importantly, alongside numerous predefined filters, ISA also includes the ability to customize and create custom filters for just about any application behind the firewall.

So far we've talked exclusively about threats from outside the network perimeter. It is important, however, to be aware that for an organization's network to be protected fully, the network administrator must also address threats from within the network perimeter. ISA answers this call in many ways including allowing network administrators the ability block users from downloading potentially harmful content from the web or to make sure critical or confidential data cannot leave the network via email.

Application layer firewalls are undoubtedly the future of network security; and whilst such a firewall is clearly a step in the right direction, it must be remembered that any firewall is only as strong as the policy enforcement. With ISA, Microsoft has pushed the boundaries of the application layer firewall. Its intuitive graphical user interface and advanced dynamic filtering capabilities mean it will play an important role in securing organizations of all sizes.

Matthew Smith
Raven Computers Ltd