Application gateways are aware of the details of how various types of TCP/IP servers handle sequences of TCP/IP packets, so they can make more intelligent decisions about whether an incoming packet is legitimate or is part of an attack. As a result, application gateways are more secure than simple packet-filtering firewalls, which can deal with only one packet at a time.

The improved security of application gateways, however, comes at a price. Application gateways are more expensive than packet filters, both in terms of their purchase price and in the cost of configuring and maintaining them. In addition, application gateways slow down the network performance because they do more detailed checking of packets before allowing them to pass.

Next-generation firewall

Many modern firewalls use the term *next generation* to describe new types of advanced threat-protection intelligence that are designed to watch for types of packet behavior that indicates the likelihood of malicious attack. A firewall that includes these new protections is called a *next-generation firewall,* usually abbreviated *NGFW.*

A next generation firewall performs all the functions of a standard firewall and more. Using a technique called *deep packet inspection,* next-generation firewalls look beyond the surface of data packets as they enter your network to find threats that simpler types of firewalls would overlook. Next generation firewalls can often stop malware before it ever gets into your network.

Virus Protection

Viruses are one of the most misunderstood computer phenomena around these days. What is a virus? How does it work? How does it spread from computer to computer? I'm glad you asked.

What is a virus?

Make no mistake — viruses are real. Now that most people are connected to the Internet, viruses have really taken off. Every computer user is susceptible to attacks by computer viruses, and using a network increases your vulnerability because it exposes all network users to the risk of being infected by a virus that lands on any one network user's computer.