Clearing Up Some Popular Misconceptions Involving Firewalls

by Scott Borg
with extensive editing and rewrite suggestions by Austen Borg

The most common of these tools for filtering transmissions between computers are called “firewalls.” Unfortunately, this term has caused many misconceptions, especially among television scriptwriters and viewers whose understanding of cyber security comes from television. Television writers have often imagined that firewalls are like heat shields or other physical barriers with protective layers. They have described “brute force” attacks burning or pounding away at firewalls. They have imagined that if the attackers direct enough fire at a given firewall, they will gradually wear it down, blast away the layers of protection, and finally break through. Some scriptwriters have even dramatized the progress of this activity, so that their characters could announce that the attackers were now “sixty percent” of the way through the firewall or, to make it really exciting, “ninety-eight percent” of the way through. Some television writers have also described stored information as being surrounded by many layers of firewalls inside the computer that is storing it. If they want to emphasize how well protected the information is, television writers will sometimes say that it is surrounded by several firewalls. They will then describe the hackers as digging or blasting away at the firewalls inside the computer to get to the information hidden inside them.

This is nothing like the way firewalls actually work. A firewall is simply a program or device that receives packets of instructions from one system and forwards them to another system. It forwards packets with features it has been programmed to send on and drops packets with features it has been programmed to block. The only thing that reaches the firewall itself over the computer network are the individual packets of instructions. The packets can arrive very rapidly, but they always arrive one by one. It is just as easy for a firewall to drop a packet as to send one on. If a cyber attacker directs packets at a firewall of the sort that the firewall will drop, this does not damage the firewall or reduce its effectiveness at all. If more packets are sent to the firewall than the firewall can handle, these packets will simply be processed more slowly than they arrive or, if the volume is too great, not be processed at all. Bombarding a firewall with more packets does not increase the likelihood of any given packet being forwarded. It does not wear down the firewall or make the firewall in any way less effective. In fact, it does not have any lasting effects at all. If something gets through a firewall, this does not make it easier for subsequent things to get through, at least not in any direct way. An attack on a firewall cannot succeed gradually or in stages. A firewall either forwards an individual packet or it doesn’t. Like most things computers do, the choice a firewall makes is always either/or at the level where it is operating. There is nothing gradual about it.

To decide whether to forward a packet, a firewall usually just reads some of the packet’s headers. It sends the packet through if the headers are on the firewall’s list of headers to send through. It blocks the packet if the headers are on its list of headers to block. A firewall, for example, might send through packets using certain port numbers and application protocols, while blocking packets using other port numbers and application protocols. More advanced firewalls keep track of what kinds of communication sessions are in progress and only forward packets with headers appropriate to those sessions. But these firewalls still determine what packets to send through based on a few labels in the packet headers.

Several firewalls do not protect an information system any better than a single firewall. If a second firewall is blocking a different type of packet than the first firewall,

then that type of packet can be added to the list of packet types that the first firewall is instructed to block, and the second firewall can be eliminated. The only effect of running multiple firewalls, instead of loading their instructions into a single firewall, is to slow down communications.