

Malicious persons can perform sophisticated attacks by breaking down their software and attempting to pass it through a firewall by making it appear as legitimate fragmented packets.

The CheckPoint stateful inspection engine inside the Celestix Orion will gather together all fragments until an entire packet is assembled, then inspect it to see if it conforms to the rules set by the user. It won't allow packet fragments through based on limited criteria, which is how blended threat viruses, such as Code Red and Nimda, sneak past certain commercially available firewalls. It also prevents legitimate fragmented packets from being dropped.

Even a reply from your computer saying, in effect, "I didn't request that" can contain enough information for a good cracker to determine your operating system, allowing the construction of a packet that looks like the answer to one of your legitimate requests. By performing stateful inspection, the second packet will be dropped.

Other firewalls offer stateful filtering, but stateful inspection was authored by CheckPoint back in 1993.

The rear panel of the Orion has five RJ-45 network jacks, four for network computers and one for either a broadband or WAN (wide area network) connection. The power jack and reset button are also on the rear panel. On the front are LED indicators. A legend for understanding the various colours and flashing is in the Getting Started Guide.

In our version of the guide, the order of the setup instructions was misleading. The best practice is to first connect the power supply and power the unit. When the LED stops flashing and turns steady, plug in the WAN cable to your DSL or cable modem or LAN, then connect a cable to your computer.

A Web browser is all you need to set up the Orion. By entering <http://my.firewall> into your PC's browser address box, the Setup Wizard for the Orion appears. Select a password, and the wizard walks you through the entire setup process. Choose your method of connection: LAN, DSL, or cable. Merely place a check in the box next to the services required: FTP, Telnet, POP3, SMTP, and others. The entire process is very simple. Online help files are available.

Knowledgeable and experienced users desiring more control can use Advanced Setup, with the option of customizing protection by adding rules based on protocols, port numbers, and IP addresses.

By default the firewall blocks one way, allowing everything outward. This can be changed in the management console by manually blocking protocols or IP addresses. A business could, for example, allow full or limited network, mail, and Internet access to some computers, while blocking all access to the systems in personnel and accounting.

The Orion will work with UNIX and Mac systems, as well as Windows. Because the software is installed on a Linux version inside the box, the user doesn't need to be familiar with that OS. With an online interface providing protection, it's possible for travelers to have full protection when using a broadband connection. The diminutive size of the appliance allows it to be stuffed into a laptop case. This unit is easy to use and convenient.

While visiting the Mississauga, Ont. office of CheckPoint Software, we were treated to a demonstration of the back-end management system available for the Orion. The level of control offered is astounding. If used on a business network, management can track what machines are active and connected, and include in the activity log information such as IP address, computer name, time, source, destination, protocol, and port number. Billing for connected time and service can be accomplished automatically. With such excellent central management capabilities, we're surprised ISPs and other managed service providers haven't bought these appliances by the truckload and distributed them to subscribers.

Celestix has engineered what is arguably the best available firewall software into a portable appliance with simple browser management interface.

By Dave Chappelle

Comments

There are currently 0 posted comments for this story.

trader
classified media

[about us](#)

[permissions](#)

[editorial policy](#)

[view our TV ad](#)

[HUB Pickup Locations!](#)