

Rollout: CP Secure's Content Security Gateway 2500

Shut the Gate on Malware

CP Secure scans traffic and blocks viruses, spyware, malware and spam before it gets to the desktop at a rate of 480 Mbps.

Oct 26, 2006 - By Howard Marks

The Upshot

CLAIM

CP Secure's CSG 2500 gateway appliance can block viruses, spyware and spam at a rate of 480 Mbps. Unlike proxy-based solutions, it's a transparent bridge. CP Secure's patent-pending stream-scanning technology vastly reduces latency.

CONTEXT

Desktop antivirus, anti-spyware and antispam solutions help combat the onslaught of malware, but require maintenance and are subject to the user's twiddling. A layered security model can keep malware off the network altogether, but must do so without significantly slowing the flow of data.

CREDIBILITY

The CSG 2500 deals with malware before it gets to the desktop. Compared with competing products from Barracuda Networks, Trend Micro and others, it's easy to install, transparent to users and adds minimal latency. The per-appliance pricing without per-user charges will be appealing to some organizations.

CP Secure's CSG 2500 gateway appliance

www.cpsecure.com

Some users just won't practice safe computing. Every downloaded smiley face screensaver and peer-to-peer sharing program can carry malware that breaches security and steals CPU cycles. Desktop anti-spyware and antivirus solutions require constant maintenance and are notoriously easy to bypass. Antispam gateways can help, but malware sneaks in from Hotmail accounts and other Web sites.

Adding a malware gateway can stop these invaders at the network's edge. CP Secure's Content Security Gateway CSG 2500 sits at your Internet entrance and scans HTTP, HTTPS, FTP, SMTP, POP and IMAP traffic. The device employs dual scan engines--its own and, for the first time, Kaspersky Lab's Anti-Virus scanner.

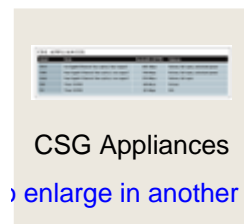
The CSG 2500 scans data for virus and malware signatures in near real time, unlike competing products from Barracuda Networks, eSoft, McAfee and TrendMicro. Those devices act as HTTP proxies and tend to introduce significant latency to the network. When we ran a series of 64-KB and 300-MB file downloads, we found no meaningful differences in download speeds with the CSG 2500 enabled or

disabled.

The CSG 2500 acts as a bridge for everything but HTTPS traffic. To scan HTTPS traffic, the CSG 2500 creates two SSL connections--one from the user's computer to the CSG, and a second from the CSG to the requested Web site. Data is decrypted and scanned for malware while inside the device--a brief exposure extra-cautious admins may not want.

Top Of The CSG Line

The vendor claims that the CSG 2500 can scan up to 480 Mbps of HTTP traffic--more than 2.5 million 15-KB SMTP messages per hour. This unit is the flagship of CP Secure's family of five malware filtering appliances. It retails for \$39,995, and would be appropriate for an organization that supports 10,000 users. All models run basically the same software, though only the larger models include failover and dual power supplies.



Installing the 2U CSG 2500 was a breeze. We ran a wizard to set the management IP address and plugged the appliance between our core router and firewall. The CSG 2500 has six Gigabit Ethernet interfaces, including two optical ones that accept standard SFP mini-GBICs.

Ports 5 and 6 are fail-open; they'll cross-connect and provide unprotected Internet access if the CSG 2500 crashes. You can also cross-connect two CSG 2500s in a failover cluster for even greater fault tolerance--a feature most vendors in this market don't support. Trend Micro's appliance is fail-open; Barracuda's has failover, and McAfee offers neither.

Management is similarly simple. The Web interface makes it easy to choose which protocols should be inspected and how infected files should be treated. The opening page shows how much traffic has been scanned and how much malware was discovered that day, though hour-by-hour graphs are missing.

You can set up the CGS 2500 to discard or quarantine infected files. The device also will strip forbidden e-mail attachments, block them, or delete whole messages. Quarantined files can be retrieved by an administrator, so if a critical file is corrupted, it can be recovered.

Keeps Malware Out

When we trolled for malware from a user workstation, the CSG 2500 stopped every attempt. The CSG 2500 did an equally good job when we attempted to download spyware vectors from the Internet. In some cases, we received error messages that indicated the files were blocked as malware; in others, we received browser error messages.

While the CSG 2500 does a good job stripping virus and spyware-infected attachments from e-mail, antispam features are basic: whitelisting, blacklisting and greylisting. You can use the device in addition to mail server antivirus solutions, such as Exchange's Intelligent Mail Filter, but it's not up to the standard of a dedicated antispam appliance.

The CSG 2500 also has basic reporting and logging. Within two hours of installing the device on a college network with 3,000 resident users' traffic passing through it, we were able to review logs and uncover a spyware-infected machine on the network that made more than 100 attempts to download more spyware.

Howard Marks is founder and chief scientist at Networks Are Our Lives, a network design and consulting firm in Hoboken N.J. Write to him at hmarks@naol.com.