

TCP/IP Revamped

Steelcape Overcomes Security Weaknesses

TCP/IP (Transmission Control Protocol/Internet Protocol) were the first two networking protocols defined. This duo is still the protocol of choice, but is it the best choice? TCP/IP was not built for security. What if you could send secure data without opening ports in the firewall and send it much faster?

Big Problems

“Last March 2007, TJ Maxx reported that 45.7 million credit and debit cards’ information was stolen by hackers who accessed TJ Maxx’s customer database, resulting in the largest security breach to date,” says Dean Norman, vice president of sales at Steelcape (www.Processor.com/Steelcape-Inc). “TJ Maxx more than likely had millions in their security budget, and they still got hacked. Maybe we should be looking at the real culprit and focus on TCP/IP itself.”

In addition to a host of security issues, TCP/IP’s other disadvantages include higher configuration costs, administration of dual protocol stacks, and the dwindling supply of IP addresses; it’s also slow and cumbersome.

Steelcape, which deploys next-generation network security solutions for the Internet/network community but specializes in the financial services, entertainment, and banking markets, has new patent-pending technologies that are 100% compatible with TCP/IP, 50% faster, and more secure because they do not open ports to communicate point to point.

Steelcape has developed a unique technology to overcome inherent security weaknesses and operational inefficiencies in network communications, adds Norman. Steelcape’s network communications technology operates within the standard OSI network model at Levels 3 and 4.

A Steelcape deployment bypasses the TCP/UDP transport layer and decreases network overhead by up to 80%, with typical improvements in the 30 to 40% range, Norman says. Steelcape uses patent-pending technology for packet transport, enabling packets to travel point-to-point on a network without open ports, making them immune from current and emerging TCP/IP threats.

A well-known film production company needed to send its digital media from various on-location sites back to its head office for processing, notes Norman. Pirated content was their primary concern, but transfer speed was also an issue. “The solution to the film production company’s problem . . . was Steelcape,” says Norman. “Agents installed at the company’s head office and remote locations eliminated open ports. In addition to radically tougher security and increased network performance, the transfer speed doubled, decreasing transfer time from one hour to 35 minutes, per one hour of film.”

R&D

The core developers/founders set out to make TCP/IP faster and more secure, originally for the gaming industry. Because this protocol had to be fast, the developers wrote more efficient code, which, in some cases, was faster than TCP/IP by 70%. This was accomplished by condensing the packets and making every element of the protocol as efficient as technically possible. The developers designed the protocol to specifically eliminate the need to pass through a firewall and the open ports. The resulting products are 100% compatible with TCP/IP and 50% faster and more secure.

“It took almost three years to develop this unique way of securing data,” says Norman. “We released the core product two months ago with clients now deployed. Now we’re working to deliver mobile versions and small Applet versions that can be temporarily downloaded for one-time-only secure communications. We have doubled our R&D efforts since announcing the first product, which was a hardware appliance. We still offer software versions in most of the common platforms, but we also sell the hardware appliance because some customers don’t want agents installed on their servers.”

How It Works

Steelcape can be applied to current security or communication solutions to improve security and performance and to close open ports. A Steelcape deployment enables clients to segregate their networks into zones for increased control of data flow. Zones are logical perimeters encompassing one or more LANs, each with its own Steelcape gateway, says Norman. All hosts within a given zone can transact data. Hosts in separate zones cannot communicate. However, clients can configure a Steelcape gateway to operate within “overlapping” zones, relaying data transactions between select segregated hosts.

As an added security measure, Steelcape gateways themselves do not recognize or understand zones, notes Norman, and their administration is a function of the enterprise server. When one gateway attempts to talk to another gateway, the destination gateway consults information provided by the enterprise server to determine whether the gateway attempting to communicate is in the same or an overlapping zone. If so, communication proceeds. If not, the destination gateway simply ignores the communication request. For example, a popular online health-care distributor needed to increase the security of its interoffice communications, as well as with its customers. So it turned to Steelcape to provide a solution that could supplement its existing architecture. Steelcape agents were added to the company’s five locations under a zero-tolerance hacking policy.

“We take securing patient records seriously,” says Scott Webster, COO/CFO at SEALS Healthcare. “Steelcape gave us the confidence to finally feel we were secure—open ports are the real problem in securing organizations.”

Target Market

“Our market focus is financial, healthcare, and entertainment. Both financial and healthcare have enormous amounts of regulations around privacy and, if public, have to disclose breaches, which can cost big,” says Norman. These organizations have been spending millions on security, only to see it fail. Entertainment, under the digital content category, must cope with a security challenge but also faces a throughput hurdle. Financial and healthcare have a host of other issues that also require special attention, but Steelcape caters to all sizes of enterprises, both public and private.

Future Plans

“Future plans include version 3, which has been road mapped, and it’s confidential, but our enterprise server, over the next couple of months, will have extensive reporting capabilities, as we are providing a stealth, secure environment. Our customers have asked us to keep track of what is coming and going, so we are committed to improving those reporting capabilities, in addition to maintaining user-friendliness in all areas of our products,” says Norman. “For example, all installation and configuration is accomplished through a Web-based interface connected to the enterprise server, plus Steelcape has a compact footprint and broad platform support—it’s easy and efficient.”

by Julie Sartain
Processor.com