

Steelcape Pushes Network Envelope

Unique Tunneling Technology Helps To Secure, Optimize Network Traffic

June 8, 2007 • Vol.29 Issue 23

by Christian Perry

Interesting Fact: Claims to be the only company with technology that can send information without opening ports.

Despite its power and seemingly unending flexibility, TCP/IP (Transmission Control Protocol/Internet Protocol) continues to display an inherent lack of security, an aspect that leaves plenty of industry room for improvement and innovation. One company that's taking advantage of this opportunity to ramp up network security is Steelcape, which has developed an alternative to TCP/IP.

"The general security industry has lacked innovation," says Dean Norman, vice president of sales for Steelcape. "We made the decision to take a different approach, instead of focusing on the weaknesses of TCP/IP and how to fix it, firewall protection, port scanning, etc."

Instead of trying to fit a bandage on the popular protocol, Steelcape set out to build a secure communication model that isn't hampered by the limitations or shortfalls of TCP/IP. Enterprises can use the Steelcape protocol library to replace elements of their existing TCP/IP protocol stacks or even supplement their existing stacks.

Sturdy Security

Thanks to a blend of computing algorithms and packet manipulation, the Steelcape solution can set and change protocol ports on a firewall without actually opening those ports. In fact, enterprises using the technology can eliminate the TCP/UDP (Transmission Control Protocol/User Datagram Protocol) transport layer altogether, which the company says can decrease CPU cycles by an estimated 25% and improve network performance up to 40%.

"Our communication protocol travels unhindered by the firewall; thus, it is extremely secure—so secure that our initial early clients requested an enhanced version to offer reports, or goggles that can see the invisible man, if you will," Norman says. "Besides reporting, the Enterprise Server is needed to configure our Agents to decrypt the data and build segregation zones."

The Steelcape Enterprise Server provides complete administration of the protected network, including control and monitoring of Steelcape components, such as Agents. The server also gathers and reports critical data, including the time at which the connection is established; identities or addresses of the computers establishing the connection; the number of connection attempts; the time at which the connection is closed; and the amount of data transacted.

These Agents work to improve network communications performance and security and can be installed on desktop systems/ servers, application servers, and database servers. Because the Agents function independently, secure data flow can be accomplished without requiring the Steelcape Enterprise Server at all times.

"We have software-based Agents, an Applet version for e-commerce, and an external hardware appliance. Almost 50% of our clients prefer an external hardware appliance, and the others prefer software inside the servers or client," Norman says.

Another element is the Steelcape Gateway, an appliance that works in tandem with security and business apps and data storage devices to boost performance and security. Also available is the Steelcape Embedded Library, which facilitates a session between software applications or hardware devices, such as NAS/SAN appliances that need built-in, comprehensive security.

Flexible Deployments

According to the company, the Steelcape solution can work in any environment but has particular appeal in VPN and VLAN architectures, where it can be deployed without modifying existing equipment.

“We are a perfect replacement for VPN, as we provide a more robust ‘tunnel,’” Norman notes. “In addition, there are no pesky authentication keys to manage—which is a headache.”

Once in place, Steelcape products allow operation of the VPN or VLAN with no open ports and provide continuous authentication of source and destination clients. In addition to these environments, the company’s technology can be applied to other point-to-point communications, such as FTP, SSL (secure sockets layer), Telnet, and MIME (multipurpose Internet mail extensions).

The Steelcape communications protocol is compatible with TCP/IP and creates a direct tunnel between components. The result is not only increased security but also accelerated traffic aided by the removal of redundant TCP processing, maximized bandwidth utilization, and packet compression. However, Norman notes that the performance improvements are a byproduct of the technology because the company continues to focus on security.

In a typical Steelcape communications session, an Agent detects a Steelcape-enabled communication request, prompting the Agent to connect and authenticate to the Enterprise Server to request a connection to the destination Agent. The Server checks that the source and destination Agents are configured to communicate and asks for authentication from the destination Agent. After authentication, the Server issues routing information to both Agents, which establish a unique connection and begin communicating.

Looking Ahead

In the future, Steelcape will be introducing a rack-mounted, high-volume unit for large financial transactions. Also, Steelcape is looking toward the realm of digital content delivery, which Norman notes is growing in priority but faces challenges when using standard protocols.

“Currently, using TCP/IP is like pushing a watermelon through a garden hose,” he says. “We have the ability of using all of the bandwidth—in a sense, turning a garden hose into a walk-in tunnel.”

