

How We Tested IPSec-Compliant VPN Solutions

In our Syracuse University Real World Labs® we designed a test bed that reduced performance degradation, but was complex enough to offer some management challenges. At the center of our test network sat a Cisco AS4700 running IOS 11.2(P) with a six-port Ethernet module. Each vendor submitted four units to complete a fully redundant VPN. The four units from each vendor were connected directly to the 4700 Ethernet ports (see "IPSec-Compliant VPN Solution Setup" on the next page).

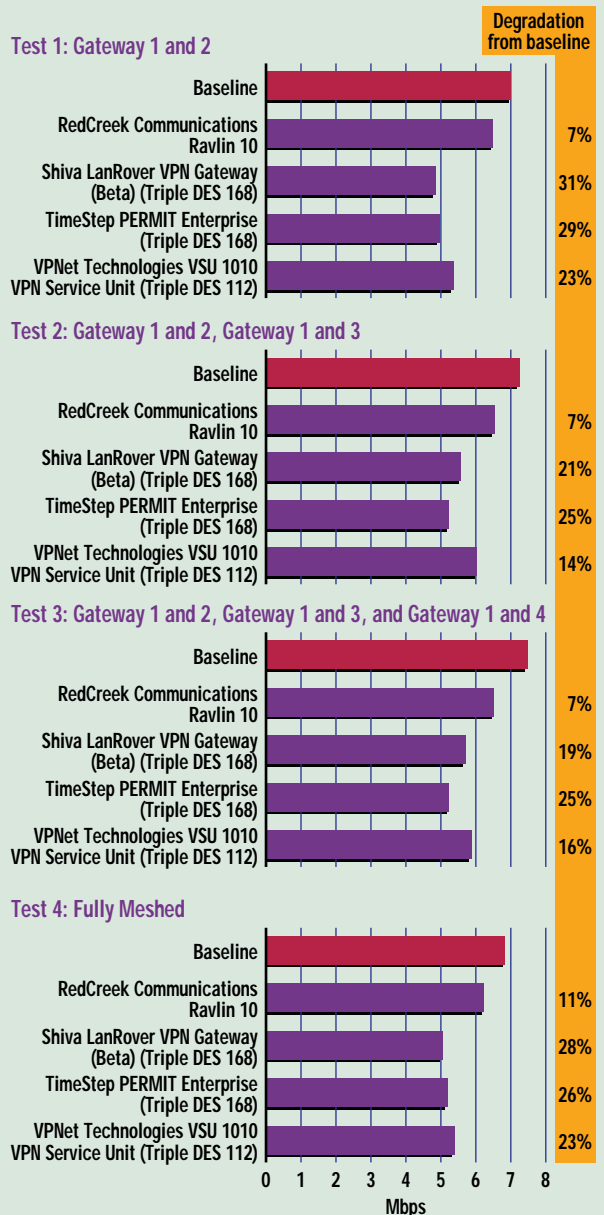
Each of the units tested was configured in IP bridge mode, with the exception of TimeStep's solution, which supports only routing. Attached via cross-over cables to Gateways 2, 3 and 4 were 233-MHz Pentium workstations running Ganymede Software's Chariot 2.1. Behind VPN Gateway 1 we placed several management consoles as well as our Chariot Console. Management stations were placed on another network segment, outside of our test VPN.

To gather performance data, we modified the Chariot Packet Blaster script to set the payload to 1,000 bytes. For each of our tests, we ran the script for 10 minutes with 15 individual TCP sessions. Testing was first run for each scenario without the gateways to gather baseline results. For Tests 1 through 4 we set up each IPSec tunnel using HMAC-MD5 for authentication and Triple DES 168 for encryption; throughput was tracked from the end point behind Gateway 1. We compared the tunneled performance data to the baseline data to measure tunnel degradation.

In our first test, we gathered performance data between Gateway 1 and 2. In our second test, we added a second tunnel between Gateway 1 and 3.

In our third test we added another tunnel between Gateway 1 and 4. Finally, we performed a fully meshed test: adding a tunnel between Gateways 2 and 3, 2 and 4, and between Gateways 3 and 4. In Tests 1 through 3, we split the 15 Chariot TCP sessions across all the gateways. The fully meshed test

IPSec-Compliant VPN Solution Performance



had six bi-directional tunnels, each carrying five Chariot TCP sessions.

Using a Network Associates Sniffer, we saw sustained utilization between 60 and 80 percent with collisions ranging from a low average of 6 percent to nearly 20 percent. In all, the test transferred approximately 550 MB of data in 10 minutes.

All of the devices we tested support IKE key management, but initial testing using longer time periods didn't show re-keying to alter performance significantly with our maximum of four tunnels. We did notice that, without exception, performance improved during Tests 2 and 3, while Tests 1 and 4 were very similar; indicating that performance depends on the ability of both ends of the VPN to encrypt and decrypt data. In Tests 2 and 3, the far gateways were doing less bulk encryption than in either Tests 1 or 4.

For the management testing, we looked at both the management station that was supplied with the hardware and with Castlerock's SNMPc 4.1n. All of the devices we tested allowed SNMP monitoring of the devices, though management outside of the vendor's management station was not possible, as expected.

