

Chung Hua University wanted to protect its network but not cramp its style, and found just the firewall to do it.

by Jeffrey Lim

Fortifying an Open Community

Established in 1990, Chung Hua University in Hsinchu city is one of the youngest universities in Taiwan. Like many other universities, it has a network that supports an "open community", allowing easy access and exchange of information among its 10,000 students, faculty and staff.

With 5000 access nodes connected to more than 100 IBM, Sun, HP and Dell servers running Windows NT, Solaris and AIX through Enterasys core switches and Cisco edge switches, Chung Hua wanted to protect its critical data, such as student research, academic records and faculty data, while still maintaining its "open community" with its easy access and information exchange.

While they already had Cisco PIX 535 firewall and NetScreen 100 security appliance to protect their network, and Norton Antivirus to safeguard the client end, Chung Hua found that with the increasing DDoS and ICMP attacks, as well as the increasing number of e-mail and network viruses they were facing, a re-look at their network defence strategy was in order.

LOOKING INTO THE PROBLEM

According to Michael Jiang, Chung Hua University Computer Centre's network administrator and lecturer, not only were the frequency of attacks increasing, but at times they caused the whole network to freeze. "The network could be inaccessible



Chung Hua University, Hsinchu city.

for 10 to 20 minutes if such attacks occurred during office hours as our staff could attend to the problem immediately, but outside of office hours, the problem could take as long as half a day to resolve," recalls Jiang.

Chung Hua decided on a defence-in-depth strategy, and looked at solutions that would not only plug any existing gaps but also beef up their existing defences. A few options were considered including solutions from NetScreen and BroadWeb, but they eventually settled on Fortinet's FortiGate 4000 antivirus firewall solution, at a contract value of around US\$100,000. According to Jiang, the key deciding factors were its all-in-one multi-functionality, as well as high performance and stability.

While the evaluation took 6 months to

complete, implementation, once they had decided, was swift, taking 2 weeks in July 2004. This was aided by the fact that their requirements became a lot clearer during the evaluation period, says Jiang, with issues like where to install and what needed to be done also crystallising then.

THE FULL SETUP

The installation, consisting of a FortiGate 4000 base system with 2 blades for High Availability (HA) connected to the campus backbone and the Internet via a 1Gbps fibre link, was uneventful apart from some problems with the HA configuration, which was resolved with help from Fortinet's technical consultant.

Once installed and properly configured, Chung Hua found, to their delight, that e-mail viruses were reduced to near zero, to the extent that Jiang now boasts of having 100% antivirus protection. DDoS and ICMP attacks have also been drastically reduced, with almost all such attacks being blocked.

Jiang is also pleased with how easy it is to configure the FortiGate 4000, as well as its good management capabilities and performance. Reflecting Chung Hua's satisfaction with the upgraded network security, Jiang remarked that they have no plans at the moment to further secure their network, other than to add more blades to the FortiGate 4000 as network traffic increases. *