

Jin Wen Institute of Technology

Dealing with security challenges from P2P networks

Situation

Located in picturesque Taipei County, Jin Wen Institute of Technology is composed of 4 schools and 16 departments, offering courses in computer science, business administration, international trade and travel management. The institute was founded in 1986 as a leading private college offering junior college programs to vocational school graduates. It was recently promoted within the Taiwan education system, to an institute of higher learning in technology. The school has grown rapidly since its humble beginnings, and currently has an enrolment of over 12,000 students.

In recent months, the rising popularity of peer-to-peer (P2P) networks and applications, such as Kazaa, eDonkey, and the proliferation of instant messaging (IM) applications, posed a new set of challenges for the technology team at Jin Wen.

"We were concerned about the viruses and threats that could spread via these new networks and client applications," said Dr. Steven K.C. Lo, Information Center Director at Jin Wen Institute of Technology. "Infected programs or malicious software masquerading as innocent files on P2P networks can easily find their way past the firewall and infiltrate the network. IM applications are similarly vulnerable as binary files can be sent directly from person to person, in addition to simple text messages."

Although computer users have largely learned to recognize bogus emails containing attachments with a virus or Trojan payload, they may not expect a binary attachment in IM applications to be infected because it appears to come from a trusted source - a friend or colleague, or worse, a superior or faculty member.

Jin Wen's technology team quickly understood that addressing these issues would be challenging. Banning P2P networks would be difficult to enforce because some P2P services do not depend on a central server, so simply blocking a particular IP address would not be possible. There were similar difficulties with instant messaging, which has an essentially decentralized mode of operation. This is further complicated by the rising importance of IM for communications, which means banning it would be unproductive.

Solution

Jin Wen decided on a plan that addresses these new challenges in two ways: first, the technology team evaluated solutions from vendors such as Cisco, Netscreen and Fortinet for features that would help them deal with threats from IM and P2P networks; second, they decided that if an outbreak did occur, that the part of the network that was affected could be isolated from the rest of the campus network.



"We are the first tertiary institution in Taiwan to use the FortiGate-5020. We had a good experience with the FortiGate-5020: it deployed very easily, and is very easy to manage, just like our FortiGate-3000. The FortiGate-5020 really simplified threat management significantly for my team."

- Dr. Steven K.C. Lo,
Jin Wen Institute of Technology
Information Center

FortiGate-5020

Industry: Higher Education

Jin Wen Institute of Technology

Dealing with security challenges from P2P networks

Jin Wen eventually decided on Fortinet's FortiGate-5020 solution. The FortiGate-5020 is a carrier-class antivirus firewall platform

Dr. Lo explains: "We were impressed by the integrated threat management features, high scalability and flexibility of the FortiGate-5020 - and the fact that the FortiGate-5020 is ICSA-certified, and features 4 Gigabit ports per blade with support for fibre channel and RJ-45 connections really made us look at Fortinet's solution favorably."

Content-based attacks, through IM or through email, were already competently addressed in the FortiGate-5020's feature-set. Even recent vulnerabilities in Skype were addressed in specific threat signatures within the FortiGate product itself. As for threats originating from P2P networks, Dr. Lo was similarly impressed that the new FortiOS 2.8 version on the FortiGate-5020 featured blocking of all or selected P2P traffic through its IPS module.

"The FortiGate-5020 really simplified threat management significantly for my team."

- Dr. Steven K.C. Lo,
Jin Wen Institute

"We are the first tertiary institution in Taiwan to use the FortiGate-5020," said Dr. Lo. "We are actually no strangers to Fortinet's products. We have successfully deployed and operated a FortiGate-3000 for two years now. It sits on the edge of our network and has so far kept viruses, Trojans and worms at bay. We had a similarly good experience with the FortiGate-5020: it deployed very easily, and is very easy to manage, just like our FortiGate-3000. The FortiGate-5020 really simplified threat management significantly for my team."

"Protecting the network from internal threats is much more difficult than protecting from external threats, but with the combination of the FortiGate-3000 and FortiGate-5020 devices, and automatic push updates, we have "360-degree" all-round protection."

Success

The FortiGate-5020 was shipped to Jin Wen in July, and has already been successfully installed and is currently running. With this new addition, Jin Wen now has the capability to quarantine parts of the network which are infected, thus restricting potential damage. Jin Wen plans to expand on this deployment by adding a customized software package called SimCommander to provide additional reporting facilities.

Learn More at Fortinet.com

Fortinet.com/contact

Tel: +1-408-235-7700 - Sales: +1-866-868-3678 - Tech Support: +1-866-648-4638

* 2005 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiGuard, FortiManager, FortiProtect are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. CAS1430511