



CASE STUDY

Anchiva Systems Stops Viral, Spyware Infections for University

Northwestern Polytechnic University (NPU), located in Fremont, California, offers undergraduate and graduate-level education for adult students, from as many as 30 different countries worldwide, in the engineering, computer and business disciplines. Many faculty members have active careers in Silicon Valley industries such as electronics, computer engineering, information technology and global business development.

“Our faculty and students reflect the fast-paced culture of Silicon Valley. They depend on mobile devices whether they are at work or at school. We needed to provide a security defense system that would protect our digital campus from the possibility of unprotected or infected mobile devices,” said David Lee, IT network administrator, Northwestern Polytechnic University.

Solution Details

Key Benefits

- **No viral or spyware infections**
- **Secures university’s email system and wireless network**
- **No performance degradation at the Internet gateway**
- **Easily configured and installed**

Product: Anchiva-1000X

The Challenge: In-Depth Protection at the Gateway without Compromising Performance

It wasn’t too long ago that students relied on the university’s bank of networked computers for Internet access and to log onto the NPU Online Service Center, a Web access for grade look-ups and other self-service applications. Each of the desktops was protected with anti-viral software. Now, the majority of students bring their own laptops on campus and the university’s IT group focuses on providing a network and Internet access for the students.

“When the students’ behavior shifted to bringing their own laptops, and spyware and spam became a bigger problem, we had to expand our content security strategy,” said Lee. “We needed complete protection against all malware to adequately protect the students’ data, the university’s data and the school’s reputation. Security at the gateway was the answer, because we could no longer control the security of student-owned laptops and mobile devices.”

With hundreds of students plus faculty and staff using a single network, NPU found that some of the students were using the Internet access to download videos and share music files from the school's network. To protect the bandwidth requirements for official school business, NPU established a separate, wireless network on campus specifically for the students' use. No longer could the security focus on protecting individual laptops, but the focus needed to be securing Internet traffic through the Internet gateway.

“We wanted a gateway device that was straightforward to use and flexible enough to protect both our email system and the Internet wireless network,” said Lee.

Another important requirement for the university was protection from spyware, spam and viruses without compromising network performance. “NPU is expanding its day-time schedule for younger, full time students,” commented Lee. “With more students, naturally, Internet traffic will increase on the wireless network.”

The Anchiva Systems Content Security Management Appliance

The university was drawn to Anchiva Systems' integrated design, the all-in-one protection, against all types of malware. A single appliance requires fewer hours of management than updating and revising multiple software or multiple hardware devices.

The Anchiva content security management system, the industry's first solution that accelerates all malware protection at network speeds. With its ASIC design, the Anchiva system can maintain its high speeds by scanning for all malware in a single pass. “We have experienced no performance degradation with the Anchiva device at the Internet gateway,” said Lee.

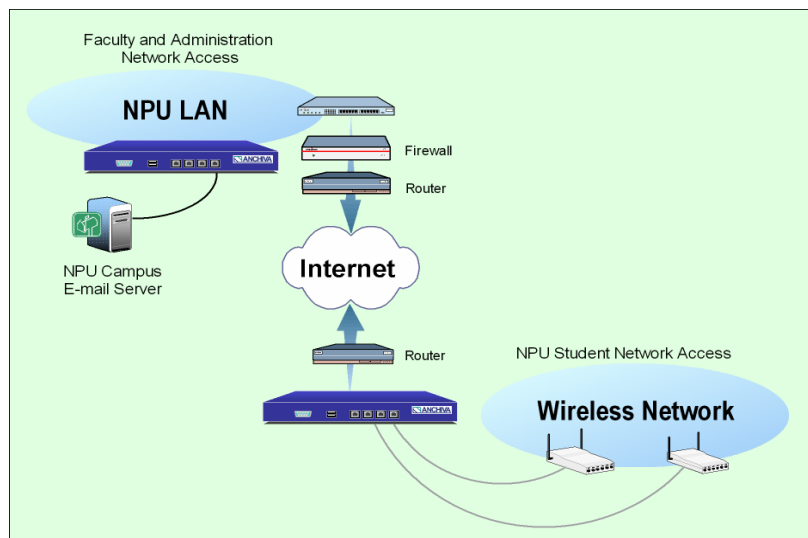


Figure 1. NPU network topology

The Anchiva staff also made the decision easy. “They provided a system to troubleshoot and test in our own environment at our convenience,” said Lee. “The Anchiva appliance

delivered immediate results. We could see from the Anchiva reporting system that it was capturing malware within hours of installation. Also, the Anchiva staff members were attentive and responded quickly.”

No Viral or Spyware Outbreaks Since Installation

Satisfied with the performance and protection from the Anchiva Systems appliance, NPU deployed the content security management devices on its email servers and on the students’ Internet wireless network as well. The Anchiva system is deployed on the network inspecting all emails for virus, spyware and spam content. For its campus-wide wireless network, the Anchiva 1000X is deployed at the Internet gateway securing all Internet traffic, including web mail access, from virus, spyware and phishing attacks.

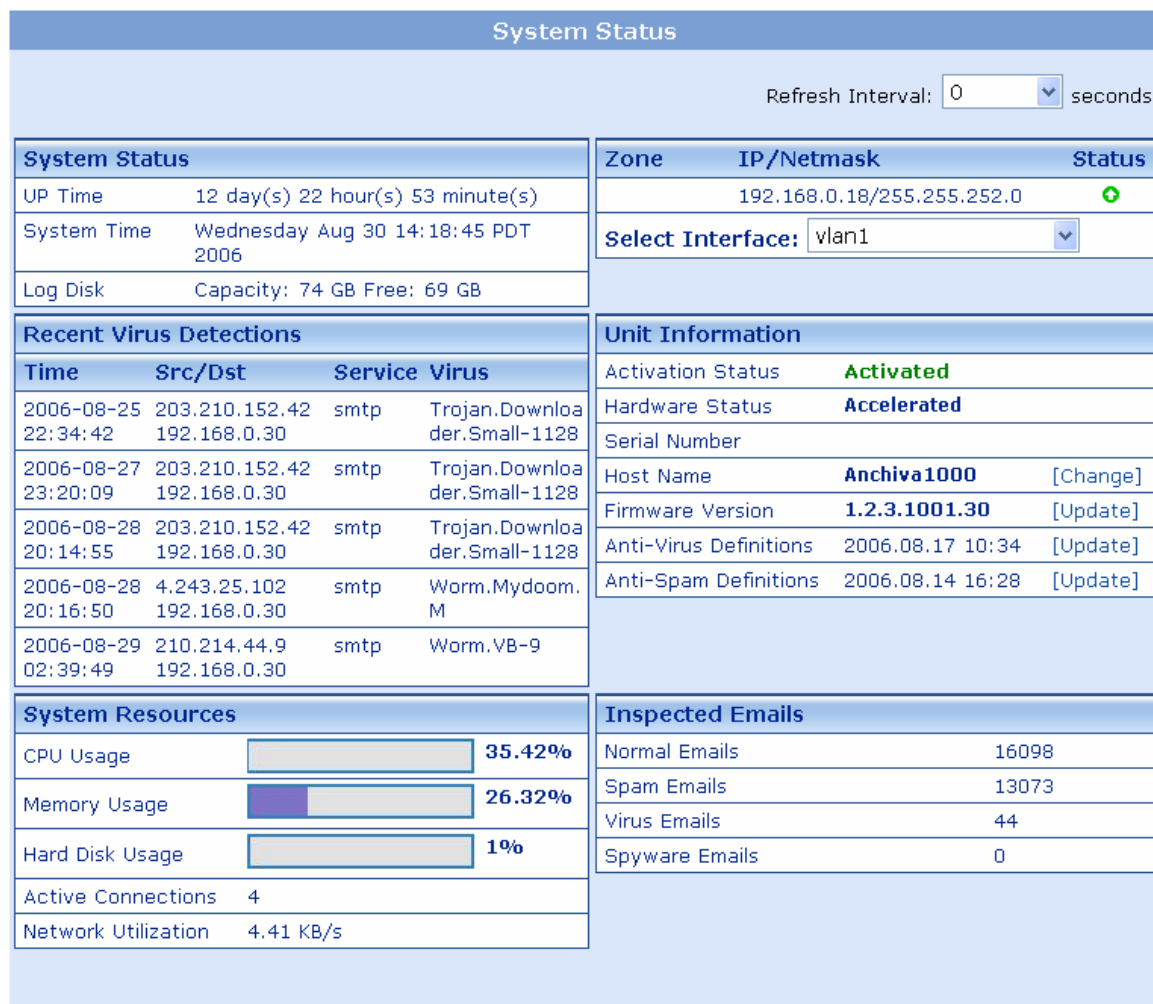


Figure 2. Anchiva Web virus report

“We were impressed that the configuration and installation took little time,” said Lee. “Installation was especially easy when we used the transparent mode, a network-savvy feature that prevents conflicts with other network devices. Another feature that saves time is the automatic updates.

Anchiva systematically downloads new malware signatures directly to the appliance, which reduces the amount of time to manage the appliance ourselves.”

Not only was the Anchiva content security management system easy to install, but it has lowered operational costs related to the after effects of malware. “Honestly, we haven’t measured how much time it takes to clean up after an outbreak, but every time the Anchiva captures and isolates viruses or worms, we breathe a sigh of relief,” said Lee. “Since we installed the Anchiva system, we haven’t had any viral or worm outbreaks. The Anchiva System has minimized the malware issue for us.”

About Anchiva Systems

Anchiva Systems is a fast-growing network security company that manufactures content inspection systems for enterprises and service providers. Faced with the onslaught of spyware, viruses and spam, enterprise businesses are in a state of siege from malicious content. To solve this problem, Anchiva Systems has introduced a line of high speed, content inspection systems that can remove harmful content in real-time before it enters or leaves a network. The Anchiva solution combines a dedicated platform with optimized pattern-matching algorithms, ASIC acceleration and a high-speed memory bus to combat malicious Internet traffic. The Anchiva solution offers enterprise and service providers increased levels of security at the gateway and key points throughout their infrastructure.

Anchiva Systems' core competency is its patentable and optimally implemented content inspection, scanning algorithms and its proprietary hardware-acceleration technologies, which delivers scalability in terms of high speed performance and extensive number of database signatures.

To support its next-generation security solution, Anchiva has assembled a team of world class researchers at its RapidRx Labs. This team, led by industry veteran Samuel Chen, is dedicated to capturing the latest malicious content, generating automatic updates and ensuring that customers are always protected from the latest threat.



Anchiva Systems, Inc.
3255 Scott Blvd., Suite 4-105
Santa Clara, CA 95054
Phone: 408-492-9712
Fax: 408-492-9732

www.anchiva.com

Copyright ©2006 Anchiva Systems, Inc. All rights reserved. AnchivaOS, RapidRX and Anchiva are trademarks of Anchiva Systems, Inc. All other names and/or trademarks shown are the property of the entities listed.