

John Brown University

Integrated Security For Campus Networks



iPolicy Networks' Intrusion Prevention Firewall equips John Brown University with an integrated security strategy to protect against current and emerging network security threats.

Case Study

EXECUTIVE SUMMARY

Industry:
Education

Environment:

John Brown University's IT department supports the computer and Internet usage of almost 2000 students. The campus runs 10/100 ethernet to desktops and all dorm rooms, supported by a gigabit fiber backbone. Internet connectivity is through a 9 Mbps ethernet (fiber) to the school's ISP.

Key Business Challenge:

- Did not have tools to fight worm propagation and upgrade
- Current firewall was not scalable for new security tools
- Budget extremely limited

Key Business Solution:

- Installed iPolicy's Intrusion Prevention Firewall with iPolicy Security Manager
- Solution included stateful firewall, Network Address Translation, IPS/IDS, and Content Filtering
- Comprehensive network protection at an affordable price

Key Business Benefit:

John Brown University was able to completely upgrade its network security to a fully comprehensive set of tools in one single, centrally managed platform. Now the campus network is armed with the tools to fight the threats of tomorrow, at a cost that is well within budget

Background

John Brown University has a remarkable history. Located in Siloam Springs, Arkansas, the school was founded in 1919, originally as a vocational technical school. Its namesake and founder was a visionary man who saw a cycle of poverty in the area, and felt people needed to be trained in basic skills. JBU's first students actually built the university.

Today, it's a fully accredited, private Christian university serving more than 1,900 undergraduates and graduates from around the world. The University has a state of the art computing infrastructure with more than 300 computers spread across 10 labs. In addition, there are 1300 office and student computers connecting into a gigabit fiber backbone through 100 Mbit wired LAN and a dozen WiFi Hotspots. JBU students enjoy this modern campus, along with access to campus-wide Internet service. Of course, the flip side of this benefit is students are constantly bringing in viruses, worms, and other malware from the Internet.

Challenge

JBU's Director of Technical Services, Ray West, Jr., was faced with the challenge that higher education IT departments everywhere are all too familiar with: how to fully protect the campus network against emerging threats. The University has a common infrastructure of multiple file, web, email, and database servers that are accessible to the student community, and as a result, constantly exposed to security threats.

JBU had a packet filtering firewall in place, of course. But it was not very scalable, which would eventually present a real problem as the campus network expanded in the coming years. They did not have an Intrusion Detection and Prevention System in place or the budget to cover one, either. The University was looking for a comprehensive and scalable network security solution, and needed a budget-friendly price.

"Bottom line, we wanted to arm ourselves against the threats of tomorrow and needed a firewall that would grow with us over the coming years. We felt really comfortable that iPolicy's firewall fit that bill."

Ray West, Jr., John Brown University, Director of Network Services

Existing & Emerging Issues

The increasing amount of malware that students picked up from the Internet had already caused several problematic events at JBU. In fall 2003, the network administrators were fighting a wild-fire when within a month, both the Blaster and Nachi worms hit the campus network by exploiting a common Windows vulnerability. In another instance, one student was alarmed when a worm selected a personal document in her hard drive, and proceeded to mail it as an infected attachment to every email address in her address book.

To prevent similar incidents from happening, JBU wanted to put in place a system that would make sure all student emails went only through the campus email server. But JBU's existing firewall was difficult to configure, and did not easily integrate with added technologies. In fact, implementing a network-based virus solution would require using a proxy, or redirecting the firewall.

Additionally, JBU did not have tools in place that, in the event of an attack, would stop worms from propagating and upgrading throughout the campus network. And existing security strategies were becoming obsolete as malicious threats increased in their sophistication.

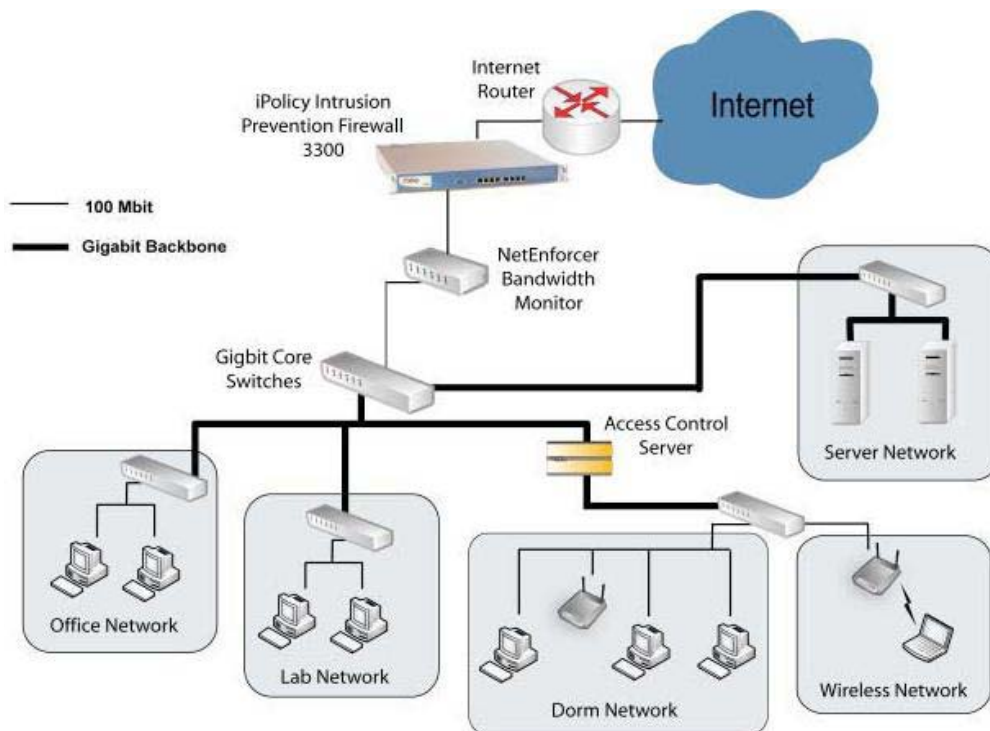
Solution

JBU evaluated iPolicy's products along with several others. iPolicy's Intrusion Prevention Firewall family was soon the first choice for numerous reasons.

"iPolicy offered an integrated solution that not only met our budget, but included more tools than we had before," said Ray. "We were able to replace our old firewall and content filtering service with iPolicy's Network Address Translation, Stateful Firewall, Intrusion Detection and Prevention, and Web Filtering at a very competitive price."

JBU particularly liked the fact that iPolicy provided comprehensive security in one easily managed platform. The campus network now had tools to detect and prevent threats, stop worms from attacking, and most importantly, these tools would continue to deliver superior performance as JBU's student body – and thus, Internet usage – grew in size.

Figure 1 - Network diagram showing deployment of iPolicy's Intrusion Prevention Firewall 3300



Summary

With the iPolicy solution, JBU has a security infrastructure that keeps its backbone and servers free of worms and malware, allowing students to better utilize the University's technology resources. The upgraded network security includes comprehensive firewall and content filtering, while offering a high performance intrusion detection and prevention solution.

It's now easy to take care of behavior anomalies, such as infected client machines generating SMTP traffic. And the iPolicy scalable management platform means more firewalls can be added and centrally managed. As the campus has multiple sites, this is a likely need the future.

JBU has essentially replaced individually managed security components with one centralized platform that saves IT administrators time, and sets the stage for easily upgrading and adding security tools as the University's security needs grow.