



FAYETTEVILLE STATE UNIVERSITY STANDARDIZES ON CONSENTRY SWITCHES FOR ROLE-BASED LAN SEGMENTATION AND ACCESS CONTROL

ConSentry Solution Enables University to Control Access for Students and Faculty and Audit all User Activity; Switch Deployment Simplifies Security

Milpitas, CA – October 8, 2007 – ConSentry Networks, the leader in secure switching, announced today that Fayetteville State University (FSU), a constituent institution of the University of North Carolina system, has selected ConSentry's LANShield Switch and LANShield Controller to provide secure switching for user segmentation and access control. The ConSentry solution provides malware control, increases IT's visibility into what users are doing on the university's LAN, enables IT to restrict LAN access to only authorized users, and records a full audit trail of all user activity.

The university LAN serves about 6,300 students and 2,000 faculty and staff, as well as vendors, contractors, and auditors, across 37 buildings. As a public entity, FSU must balance access control with the rights of users to access any Internet and most university resources.

The university's biggest problems were the continual exposure to malware and the lack of visibility into what users were doing on the LAN. Student-owned PCs, for example, would frequently release trojans, spyware, denial of service (DoS) attacks, and address resolution protocol (ARP) storms. The FSU IT team also struggled to enable open access to the Internet without leaving the university vulnerable if users downloaded copyrighted material or did other illegal activities.

Looking for a Better NAC Solution

FSU had implemented Clean Access in an effort to address these security needs but after a year found the solution too unreliable and limited in features. Since student machines could always reach the Clean Access server, infected devices bombarded it with so much malware that it went down every night. In addition, the solution relied on students properly installing the Clean Access Agent on their laptops, which presented recurring helpdesk issues. The need for this agent also meant the university had no means for scanning the laptops of visitors to the campus.

Ultimately, FSU sought an alternative, and the IT team's research led them to ConSentry. The ability to perform posture check without pre-installed software, to fully log all user activity, and to control access to resources based on roles within Active Directory drove the decision to deploy ConSentry, and an evaluation validated the inline performance the university needed to keep up with LAN traffic.

"We talked to other vendors, but they couldn't provide the visibility or control we needed," said Payman Damghani, network security analyst at FSU. "When we got the ConSentry demo gear and saw how it performs, we were sold on it. And having all that security available in a switch allowed us to blanket our campus and put controls right next to the users. It was a much stronger security architecture for our needs."

Why ConSentry – Pervasive Deployment in a Switch

Available as an appliance or wiring closet switch, ConSentry's LANShield platform delivers a suite of security services encompassing NAC, traffic visibility, identity-based post-admission control, and threat control, including anomaly detection and malware containment. Both the LANShield Controller

and Switch are purpose-built devices based on custom silicon, including a 128-core processor and two programmable ASICs. The hardware performs deep packet inspection while maintaining 10 Gbps forwarding rates, enabling the LANShield platforms to identify and provide access control on every flow.

“The fact that these are ASIC-based devices was important to us,” notes Damghani. “These aren’t servers, so I don’t have to worry about them getting flooded and going down like the server would.”

When the IT team learned that ConSentry’s secure switching capabilities were available in both the LANShield Controller and the LANShield Switch, they decided the switch provided the easiest means for extending security pervasively across the campus. They purchased more than 50 LANShield Switches to support student dormitories. Several LANShield Controllers are controlling staff and faculty within administrative buildings.

“The university’s embrace of a pervasive secure-switch deployment highlights the growing trend for NAC and other security features to be built directly into access switches,” said Dan Leary, vice president of product management and marketing for ConSentry. “The simplicity of our all-in-one platform makes both installation and ongoing operations that much easier.”

About ConSentry Networks

ConSentry Networks delivers secure switching, enabling enterprises to control every user and secure every port on the LAN through its LANShield product family—the LANShield™ Switch, LANShield Controller, and InSight™ Command Center. More than 150 enterprises today rely on ConSentry’s award-winning secure-switching platforms to protect their corporate assets, ensure continuity of operations, and dramatically reduce the risk of security breaches. ConSentry is backed by blue-chip venture capital firms Accel Partners, DAG Ventures, INVESCO Private Capital, and Sequoia Capital; and is headquartered in Milpitas, California.

ConSentry Networks, the ConSentry Networks logo, LANShield, and "Control every user. Secure every port." are trademarks of ConSentry Networks Inc., for use in the United States and other countries. All other product and company names herein may be trademarks of their respective holders.

Media Contacts:

Michelle McLean
ConSentry Networks
(408) 956-2100
mmclean@consentry.com

Shannon Malliet
Engage PR for ConSentry Networks
(510) 748-8200 x309
smalliet@engagepr.com