After struggling for more than a year to get Cisco Clean Access working, FSU got rid of it in favor of ConSentry switches. ConSentry's visibility capabilities, dissolvable EPV agent, and ability to protect all points of access into the network are major benefits for FSU, saving time and money, says Payman Damghani, network security analyst at FSU.

Fayetteville State University Standardizes on ConSentry Switches to Secure LAN Access

Given the objectives of higher education, it's no surprise that university students and faculty expect to go to any web site they want and download whatever they want – much to IT's dismay. "Our users aren't very security minded," notes Payman Damghani, network security analyst at Fayetteville State University (FSU). College campuses present unique security challenges because student laptops, which are the majority of devices connecting to the network, aren't under IT's control.

An arm of the University of North Carolina, FSU is the second-oldest public institution of higher education in the state. Founded in 1867, FSU today serves some 6,300 students with 2,000 faculty and staff. Because FSU is a public entity, Damghani and his team can go only so far in restricting access to university resources or the Internet. Consequently, "our biggest battle is malware outbreaks," Damghani says. ARP storms and denial of service (DoS) attacks from infected machines pose the biggest threats. He hoped to gain the upper hand by deploying network admission control (NAC).

However, several months after installing Cisco's Clean Access solution (now the Cisco NAC Appliance), Damghani had new headaches. The Cisco platform kept going down, students weren't properly downloading the desktop agent, and the IT team had no visibility into what was happening on the network. Damghani decided to investigate alternative LAN security solutions. His search led him to ConSentry Networks, which suggested a mix of LANShield Controllers and Switches that let him secure the network down to the port level, even in student dormitories.

LOOKING FOR A BETTER NAC SOLUTION

Damghani's experience with the Cisco product gave him a clearer idea of his LAN security requirements. First, he needed a solution that made it possible to check the endpoint status of machines without the need to download client software – the Cisco solution depended on Cisco desktop software to provide that endpoint verification. Not only was this cumbersome for FSU users, but it provided no protection against malware introduced by guests and other non-FSU users

About Fayetteville State University

Fayetteville State University is a constituent institution of the University of North Carolina and the second-oldest public institution of higher education in the state. Founded in 1867 as the Howard School for the education of African Americans, today FSU serves a growing student body of more than 6,300 students and ranks among the nation's most diverse campus communities.

The Challenge

Concerned about ARP storms and denial of service (DoS) attacks from infected machines, FSU installed Cisco's Clean Access solution (now the Cisco NAC Appliance). However the Cisco platform kept going down, students weren't properly downloading the desktop agent, and the IT team had no visibility into what was happening on the network. In the end, the Cisco solution caused more problems than it solved.

The ConSentry Solution

FSU's search for a better NAC solution led them to ConSentry Networks, where a combination of LANShield Controllers and Switches helped secure the network down to the port level, even in student dormitories.

who might connect to the network. Second, he needed a solution that was easy for IT to deploy and easy for students, faculty, and staff to use.

In addition to not serving guest machines, the Cisco Clean Access endpoint validation (EPV) also proved inadequate on the machines where it was running. Clean Access verifies whether users are running updated antivirus and anti-spyware software, but it doesn't scan users' computers for the actual presence of malware on that machine. "You could comply with the policy but still have an infected machine," notes Damghani. As a result, trojans, DoS attacks, and other malware regularly entered the FSU network and brought down the Linux-based Clean Access platform. In fact, bad traffic from users could hit the Clean Access server even if they had not authenticated or passed the EPV check, because that server was set up as the default gateway.

"A user can have up-to-date antivirus software on their laptop, but if its definitions aren't very good, the laptop can still be infected. We had that issue with a lot of students," says Damghani. "Three or four months after the semester began, the Clean Access server was getting pounded so hard it started losing its connection to the network. We'd get the flood of phone calls every morning around 8. Since Clean Access was the default gateway for the students, when it was down all traffic came to a stop. No one could get on the network. Even authenticated users were down," he notes. Tired of rebooting the server daily, Damghani wrote a script that automatically rebooted it every night.

A third drawback of the Cisco product was its reliance on a user-installed agent.

"Mass deployment of the Clean Access agent was another problem," Damghani says. "Getting students to download and install it was a huge headache for us. Students just want to run Internet Explorer and get on the network. They don't want to read instructions and install an agent."

Ultimately, FSU sought an alternative. "We got very frustrated so we decided to look around to see if we could find a better solution," says Damghani. When he began researching LAN security products, he knew he wanted a NAC solution that:

- didn't require users to install a desktop agent;
- could identify and limit access for any user's machine, regardless of whether it's under IT's control or belongs to students, university personnel, guests, or contractors;
- authenticates users regardless of how or where they log onto the network;
- provides EPV for managed as well as unmanaged PCs; and
- provides virus and spyware scanning as part of EPV.

The FSU team installed a ConSentry test platform and quickly made up their minds. "We saw how it performs and were sold on it."

Payman Damghani,
Network Security Analyst

REQUIREMENTS BEYOND NAC

With malware so prevalent, Damghani wanted additional layers of protection beyond EPV. For instance, he wanted the ability to identify and isolate anomalous traffic. Above all, he wanted to see what was happening on the network.

"If a student got infected and was causing a broadcast storm, our resources were very limited in finding that student and stopping the broadcasts," Damghani says. Lack of visibility into network traffic "adds a layer of complexity to your troubleshooting," he notes. "We could see Clean Access going down but we didn't know what was taking it down."

The IT team also wanted visibility into user activity so they could enforce network usage policies; for example, to ensure staff and faculty weren't accessing inappropriate web content and students weren't downloading music, videos, or other copyrighted material. Likewise, IT wanted a way to quickly identify bandwidth hogs and other resource abusers.

In addition to seeing traffic, IT also wanted a way to control it. At a high level, IT needed the ability to differentiate among users, so that students, faculty, staff, guests, and other groups of users could be given appropriate access to the Internet and university resources.

As Damghani and his team began researching security alternatives, their requirements list grew to include:

- malware control;
- traffic visibility down to the user level;
- identity-based post-admission controls;
- transparency to end users;
- ease of deployment; and
- stable, high-performance operation.

"From a legal standpoint, ConSentry's visibility is very helpful. If a faculty, staff member or student is doing something that's against our user policy, we have proof of them doing it, and that's very important."

Payman Damghani,
Network Security Analyst

THE CONSENTRY SOLUTION

The FSU team contacted several vendors, including ConSentry, for more information about their products. "Except for ConSentry, all the vendors had server-based solutions that operated out-of-band and didn't have the visibility capability we wanted," Damghani says. The ConSentry LANShield platform became the leading candidate. The FSU team installed a test platform and quickly made up their minds. "We saw how it performs and were sold on it," Damghani says.

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 a server-based system would."

FSU's initial plan was to deploy LANShield Controllers in key areas of the campus, such as the administration building. The Controller is easily installed between the wiring closet and network core and requires no changes to an organization's existing IT infrastructure or to desktops. As the evaluation progressed and the IT team discussed the upcoming refresh of the university's 50+ wiring closet switches, the decision was made to replace all these with LANShield Switches, which provide full per-port security control in a gigabit Ethernet wiring-closet switch.

Installing LANShield switches is straightforward. "It's just like any other switch," Damghani says. "You configure the management interfaces and the VLANs and rack it up. There's nothing special to it."

"ConSentry's malware heuristics is another great feature that's going to help us tremendously."

Payman Damghani,
Network Security Analyst

ADDRESSING FSU REQUIREMENTS

ConSentry was able to meet the full list of FSU's security needs, including the requirement for transparency. A key feature was ConSentry's authentication and posture check. The ConSentry system supports passive and active authentication as well as a method for performing host posture check that is much easier for users. With passive authentication, the platform watches users authenticate to back-end identity stores such as RADIUS and Active Directory, verifying that users have authenticated successfully. FSU faculty and staff use this type of authentication, which ties directly into the university's Active Directory implementation.

ConSentry also offers active authentication, in which the LANShield platform actively challenges a user for authentication information via a browser-based captive portal. This capability allows IT to extend admission control to users not in the identity store. FSU plans to use active authentication for students, guests, and other non-employees.

Damghani was particularly pleased with ConSentry's posture check, which uses a dissolvable agent in the form of an Active X or Java applet to perform a complete compliance check on hosts. "The dissolvable agent was one of the selling points for the ConSentry solution," Damghani says. "The fact that a student doesn't have to go through the process of downloading software and running the installation is a big relief for everyone. With ConSentry, students don't have to read any instructions. After they've authenticated, ConSentry's EPV does its thing. They only know it's there if they need to install or update antivirus or anti-spyware software. Then it tells them what to do."

Beyond verifying that users' PCs are in compliance, ConSentry's EPV scans hosts for trojans, viruses, and other malware. If anything malicious is detected, the user is blocked from accessing the network and sent to remediation. For FSU, this capability "is a big thing," Damghani says. "With ConSentry's EPV, you're not relying on the antivirus software alone. It's an extra level of protection."

In addition, through ConSentry's threat control capability, the LANShield platforms protect against known and unknown threats, including worms and zero-hour attacks. Both the Controller and Switch can correlate all traffic from a single user and employ ConSentry-developed algorithms to detect anomalous behavior. In addition to detection, the LANShield platforms provide containment, allowing IT to stop traffic on a per-user or per-application basis if malware is detected. "ConSentry's malware heuristics is another great feature that's going to help us tremendously," says Damghani.

USER VISIBILITY AND CONTROL

ConSentry's ability to provide visibility into network traffic down to the user level was another major selling point for FSU. The LANShield platforms' visibility feature provides real-time and historical views of all LAN traffic, giving IT a clear picture of traffic on the network at all times, including who is accessing what resources. LANShield platforms perform Layer 2-7 deep packet inspection and full Layer 7 application decode, enabling them to identify and control network traffic at a granular level.

"If I see a student violating copyright policy or using up all our bandwidth downloading the latest movie, I can cut off his network access for a week."

Payman Damghani,
Network Security Analyst

And the ConSentry platforms tie all LAN activity back to a username, making it easy to define and implement identity-based access controls. The LANShield platforms automatically learn a user's identity by watching users authenticate to back-end identity stores such as Active Directory and RADIUS. Usernames are bound to an IP and MAC address, making it possible to track and control individual user's application flows, files opened and closed, and the use of printers, VoIP phones, and other resources.

Initially, Damghani envisions defining two broad users groups – students and FSU employees. All student resources will be accessible via a captive portal web page. "If a student plugs into a network port or sits at a hot spot, they're going to have restrictions because they're authenticating to the captive portal," he says. Faculty and staff, on the other hand, need direct access to servers. They'll use the standard Microsoft login and gain access to the network once they're authenticated. "The domain-joined machines are going to have broader access," he notes.

Damghani also chose the ConSentry platform because of the visibility and control enabled by ConSentry's InSight Command Center. It gives IT the means to capture and view network traffic data and to create and distribute policies. It aggregates all captured data and presents IT with actionable information, showing key security incidents in at-a-glance summaries and drill-down, detailed views. InSight also enables rapid forensic troubleshooting, auditing, and reporting.

"From a legal standpoint, the visibility is very helpful," notes Damghani. "If a faculty or staff member is doing something that's against our user policy, we have proof of them doing it, and that's very important. The same goes for students. We're not allowed to block a user's traffic. But if I see a student violating copyright policy or using up all our bandwidth downloading the latest movie, I can cut

off his network access for a week and he can't complain to me. I can point to his account and the whole history is all right there."

And because the LANShield platform ties all LAN activity to users, access control is applied to users regardless of how they connect to the network, whether they're attaching locally via a wired or wireless connection or connecting remotely via a VPN. With this feature, FSU no longer has to worry about unprotected ports. "If someone's who's not a student, faculty, or staff member wanders into a building and plugs into a port, they still have to authenticate through captive portal to get on the network," Damghani says.

CONSENTRY: LESS PAIN, MORE GAIN

FSU's IT team focused on installing the LANShield Switches first, as these serve student areas. "It's important to get the students up and running and to get the EPV and posture check going in the dorms because that's usually where the problem areas are. Next, we're going to install the Controllers in the administration buildings," says Damghani.

ConSentry's visibility capabilities, dissolvable EPV agent, and ability to protect all points of access into the network are major benefits for FSU, he says. And with malware being isolated, client services will have fewer infected desktops to clean, saving time and money. For Damghani, the bottom line is: "ConSentry has saved me a lot of headache and frustration."

"ConSentry has saved me a lot of headache and frustration."

Payman Damghani,
Network Security Analyst

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 100 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. www.consentry.com

Corporate Headquarters
ConSentry Networks
1690 McCandless Drive
Milpitas CA 95035
Phone 408.956.2100
Fax 408.956.2199
Toll-Free 866.841.9100
Email info@consentry.com
www.consentry.com

Worldwide Locations
London, United Kingdom
Phone +44 (0) 00870 351 9494

Frankfurt, Germany
Phone +49 69677 33 4

Tokyo, Japan
Phone +813 5532 7630

For a complete listing of all our office locations go to:
www.consentry.com/company.html

100907 CON-DS-1006

CONSENTRY NETWORKS