

Building a Secure, Reliable College Network Community

Mississippi State Board depends on a Cisco security solution to safeguard its network and extend access to students and staff.

EXECUTIVE SUMMARY
<p>Mississippi State Board for Community and Junior Colleges</p> <ul style="list-style-type: none"> • Higher Education • Jackson, MS • 32 employees <p>Business Challenge</p> <p>Safeguard critical student and administrative records while maximizing network reliability and accessibility.</p>
<p>Network Solution</p> <p>Intelligent firewall protection and support for both SSL and IPsec VPN connectivity</p>
<p>Business Results</p> <ul style="list-style-type: none"> • Network protected from denial of service attacks and other threats • Mobile and remote employees able to safely access applications and network resources over the Web • Students' learning experience improved through access to latest technology

Business Challenge

Making higher education opportunities accessible to all citizens is a top priority for the State of Mississippi. The state's 15 community and junior colleges are dedicated to providing affordable, diverse learning opportunities, and technology plays a key role in helping educators meet their objectives. The State Board for Community and Junior Colleges is responsible for technology initiatives to respond to the changing needs of the community. The Board also acts as the Internet Service Provider and supports the wide area network (WAN) for the state's community colleges.

"Our network enables communication between colleges, and provides access to the Internet," says Ray Smith, director of information services. "It also supports collaboration with other institutions and online education programs."

As an educational organization, the Board strives to facilitate the open exchange of information. Students, instructors, and librarians all need access to the Internet. However, at the same time, the Board has a responsibility to protect users from network threats, and keep the network up and running. A top security priority was to establish a private network to keep confidential information safe from unauthorized users, hackers, and other threats.

"Like any higher education entity, we have student records that contain a great deal of private information related to student loans, scholarships, and other data," says Smith. "We also have to safeguard our own business assets, administrative records, and financial information."

The Board needed a network security solution that could stop network attacks before they could harm network reliability and availability. Since staffers frequently travel outside the office, the solution would need to provide protection and secure access for remote users, as well as students and instructors on campus. At the same time, it would have to be flexible to meet changing needs.

Network Solution

After considering a variety of technology options, the Board chose Cisco® ASA 5500 Series Adaptive Security Appliances, which help the Board to keep its information and IT assets safe, while keeping deployment and operations costs under control.

“We chose a Cisco security solution because of Cisco’s strategy and architectural approach, they look beyond the network ‘plumbing,’ and enable us to focus on delivering the applications and services that we need.”

—Ray Smith, Director of Information Services

The Cisco ASA 5500 Series provides intelligent firewall services with identity-based access control, and protection from threats like denial of service (DoS) attacks. Two Cisco ASA 5550 appliances replaced the Board’s Cisco PIX 535 Security Appliances to provide redundant protection at the network perimeter.

The Board chose the Cisco ASA 5550 not simply for its advanced firewall capabilities, but because it also offered flexible virtual private network (VPN) services. SSL VPN technology allows a diverse group of the Board’s mobile and remote employees to safely access applications and network resources over the Web. The Cisco AnyConnect VPN Client provides the mobile workers transparent VPN connections and optimized support for latency-sensitive traffic.

“We are using SSL technology because we want to make network access available to them in the easiest sense possible,” says Smith. “Some of our staff work inside the state legislature, and during the budget season, they constantly need to access the network to update documents, look at spreadsheets, and work with colleagues—all from the capitol. The Cisco solution lets us get into our system securely and stay productive from wherever we are.”

Smith and his team are actively working with Cisco representatives to explore new options for the Cisco ASA 5500 Series appliances such as IPsec VPN technology, intrusion prevention (IPS), and protection for voice and video applications.

“The scalability and flexibility of the Cisco ASA Series were key reasons for the upgrade,” says Smith. “We used our Cisco PIX 535 primarily for Network Address Translation, but the Cisco ASA is completely different and offers a wide range of new features. We are highly motivated to learn more about it, so we can take full advantage of the solution.”

Deployment of the Cisco ASA Series and the transition to the new platform proceeded smoothly, since the solution was designed for ease of use.

“We had to perform the migration during the semester, which limited our ability to bring the network down,” says Smith. “We were able to accomplish the upgrade with very little downtime.”

Business Results

The Board's migration to the Cisco ASA has quickly unlocked several new benefits. By reducing network security risks, the Board can help ensure its network services are always available to students and staff.

"We support several online education initiatives, and our networks need to be up on a 24-hour basis," says Smith. "In the past, when we needed to upgrade firewall software, we had to bring down the network. Now, with the redundancy and failover provided by our dual Cisco ASA appliances, we can upgrade the devices without interrupting services."

By providing secure VPN access, the Cisco solution also helps staff stay productive when they are working outside the office. Employees use the Cisco AnyConnect VPN Client, which automatically adapts its tunneling to the most efficient method possible based on network constraints.

"With our new system we are able to utilize SSL VPN and come back through our ASAs and feel very secure about what we are doing," says Smith.

Managing the Board network has become easier, too, because IT staff can login securely anytime, from any location. If issues arise involving the network, Domain Name System (DNS) changes, or firewall modifications, staff can address them as soon as they occur.

"Our IT staff is very small, and even though supporting the network is mission critical, most of our work after business hours is done from home," says Smith. "Staff can work from home and have the feeling that they are sitting at their desk, which is great. And we save a considerable amount of time in not having to drive back to the office to modify the network."

Perhaps most importantly, by deploying the latest technology, the Board has helped Mississippi community colleges offer students a better learning experience.

"We want to make sure that when our students come in, they feel they have access to the same quality technology that they would if they went to other institutions," says Smith. "Most of our students have experienced high-speed Internet access at home or at school, and they expect it on a college campus. The Cisco solution was a real upgrade for us and enabled us to meet students' high expectations."

PRODUCT LIST

Security and VPN
Cisco ASA 5550 Series Adaptive Security Appliances, SSL/IPsec VPN Edition

Next Steps

Now that the Board has completed deployment of its ASA 5500 Series Adaptive Security Appliances, the organization plans to enhance its solution to tap its full potential. To provide a more personalized experience for

remote employees, Smith and his team are working to create customized portals for staff who connect to the Board network via SSL VPN.

The Board also hopes to improve management of its solution with the Cisco Security Monitoring, Analysis and Response System (MARS). Cisco Security MARS provides an end-to-end view of the network, and can help Smith and his team improve their threat mitigation.

"Because we share buildings with other agencies, we need to maintain a high level of security as we deploy wireless and other applications inside our offices," says Smith. "Cisco MARS can provide detailed reports and other tools that we have not had in the past, which will really enable us to have better insight into the state of the network."

For More Information

For more information, please visit <http://www.cisco.com/go/asa>.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc. Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)