

School Gives Students Secure Web Access to Needed Applications



EXECUTIVE SUMMARY

Customer Name: PDM Group of Institutions

Industry: Education

Location: Bahadurgarh, India

Faculty/Students: 1200 faculty; 15,000 students

Business Challenge

- Control access to network, applications, and websites
- Help ensure adequate network bandwidth for growing student population spread across five campuses
- Simplify network and security operations

Security Solution

- Cisco Web Security Appliance
- Cisco ASA 5520 Adaptive Security Appliance

Business Results

- Enables students to access sites they need for digital learning without degrading network bandwidth
- Provides granular control of URL filtering and applications
- Simplifies security management and operations, while leaving room for future growth

PDM Group of Institutions uses Cisco Web Security Appliance to manage network bandwidth for rapidly growing student body.

Business Challenge

The PDM Group of Institutions (PDM), located in Bahadurgarh, near Delhi, India, provides primary, secondary education as well as higher education and operates 14 different institutions that offer high-quality technical, business, engineering, and medical education. The main, 95-acre campus is home to more than 15,000 students and 1200 faculty members. The institution's mission is to contribute to society through the pursuit of education, learning, and research at the highest level of excellence – and that excellence is driven by technology.

Chitresh Lather, CEO of the PDM Group of Institutions, has seen many changes in the past 19 years that PDM has operated. A long-time Cisco customer, PDM built its organization using Cisco® networking technology across its campuses. PDM also provides its students with the opportunity to remain connected to the outside world via its unified wireless communication network. With over 100 access points providing uninterrupted wireless Internet connectivity, the campus is one of India's most advanced technical campuses.

“Our different institutions are covered by 10 gigabits of fiber-optic cable, which connects Cisco switches, routers, LAN controllers, and firewalls. It's a lot of bandwidth – which is required for the digital learning that goes on today,” said Lather. “Both teachers and students use iPads in the classroom for teaching.”

In addition, PDM has a bring-your-own-device (BYOD) policy that allows faculty and students to connect personal PCs, tablets, and smartphones to the network. This policy means IT needed to be able to control access and web filtering so that the PDM network could handle the additional traffic.

“With the application control built into the WSA, we have very good control and network-related help desk calls have dropped between 75 and 80 percent.”

Saurabh Seth

Senior Network Administrator
PDM Group of Institutions

Security Solution

In 2013, PDM implemented the Cisco Web Security Appliance (WSA). The WSA combines Advanced Malware Protection, application visibility and control, acceptable-use policies, insightful reporting, and highly secure mobility on a single platform.

“With more than 10,000 students accessing the network each day, we needed a deep level of granular control,” says Saurabh Seth, network administrator. “There were many students who wanted to access social media – which is, of course, acceptable. However, we didn’t want them using our bandwidth to play Internet games,” says Seth.

Seth continues, “The granularity of the URL filtering makes our job easier. For instance, we give our students the ability to access educational videos on YouTube, but not the capability to comment on those videos. It’s a simple option like this that helps us keep bandwidth in check.”

Like students everywhere, the students in the college of engineering and computer science are naturally curious and had found ways around earlier security protocols. And BYOD only exacerbated that. “The WSA has transfer and redirection, which allows us to decide which files should be blocked, which should be allowed, and where traffic should redirect to,” says Seth. “It also has very good control around encrypted traffic.”

Seth cites the WSA’s ability to control encrypted traffic. This can be a blind spot for IT, and with thousands of students accessing the network each day, the potential for subverting both security and performance is a real concern. “The WSA has good control around encrypted traffic, and it doesn’t impede bandwidth.”

In addition, the WSA allows the IT staff at the PDM Group of Institutions to set restrictions on file size. “This is really helpful to us,” says Seth. “It saves our network bandwidth, because we can restrict downloads to 100 MB or even 80 MB.”

The IT team at PDM appreciates the real-time threat intelligence embedded in the WSA. The Security Intelligence Operations (SIO) team at Cisco delivers early-warning insights and vulnerability analysis with some of the industry’s largest collection of real-time threat intelligence: 100 terabytes of security data daily, 13 billion daily web requests, 150 million endpoints, and 1.6 million deployed security devices.

“The SIO team is constantly updating our web appliance. It protects us completely and offers us very good control over malware and security issues,” says Seth.

The Cisco Wireless LAN Controller also helps PDM control its network performance. “If we let them, students might connect three or even four devices to the network at one time – PC, iPad, smartphone, tablet. But with the Wireless LAN Controller, says Seth, “it’s easy to set policy and allow the students to connect only one device at a time, saving network performance. It’s an unnecessary connection, really. At a single time, a person can really only operate one device, so it’s not a hardship.”

Business Results

Before implementing the WSA, network bandwidth was constrained. “Students would eat up bandwidth watching entire movies, for instance. Now with the application control built into the WSA, we have very good control, and network-related help desk calls have dropped between 75 and 80 percent,” says Seth.

And with the granular control provided by the Cisco WSA, giving students access to social media isn't a problem. "We give them access to what they need, while we have the control we need," says Seth. "For instance, Facebook is accessible, but students can't comment or 'like' a post. This type of granularity wasn't available in other products that we looked at. It also helps our faculty. For example, if they want the students to have access to a particularly large video on YouTube, we can permit that."

While other solutions require complex multi-device deployments, the Cisco WSA operates as a standalone solution, deployed alone or integrated with the existing infrastructure. Seth and the IT team at PDM Group of Institutions cite the tight integration as a major benefit. "It integrates with Active Directory and allows us to set user-based policies quickly and easily."

Seth added a final thought about the results PDM has achieved with the Cisco WSA. "Before implementing the WSA, we were managing everything manually, so we have seen a significant time and cost savings. As well, the controls are helping keep our growth on track."

Next Steps

Today, in addition to the Cisco Web Security Appliance, PDM is using the Cisco ASA 5520 Adaptive Security Appliance firewall for additional network protection. However, as the student population continues to grow, the organization is actively considering the ASA 5500-X Series Next-Generation Firewall.

"The included features and on-board granularity of the next generation firewall is really fabulous. It's definitely something we're considering, and I imagine we'll upgrade sometime in the next year," says Seth. "We'll also consider the Identity Services Engine at that time to further help us support our BYOD policy."

For More Information

To find out more about the Cisco Web Security Appliance, go to:

<http://www.cisco.com/go/wsa>.

PRODUCT LIST

Security

- Cisco Web Security Appliance
- Cisco ASA 5520 Adaptive Security Appliance

Routers and Switches

- Cisco Catalyst 4507 Switches
- Cisco Catalyst 2960 Series Switches

Wireless

- Cisco 5508 Wireless Controller
- Cisco Aironet 1100, 2200 Series Access Points



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)