Securing Open Networks in Higher Education:
Protect Against New Threats in a Post-PC Era

What You Will Learn

Cyber security in higher education requires a fine balance because of the high value that colleges and universities place on open environments. If you allow all devices and traffic types, you need ways to protect campus networks, information, and reputation and to respond to requests to identify students engaged in illegal file-sharing activities.

This white paper, intended for leaders of college and university IT, cyber security, and compliance teams, explains proven approaches to solving higher education security challenges:

- Prevent malware when students bring their own devices to campus.
- Monitor usage of gaming consoles connecting to residence hall networks and limit their bandwidth consumption.
- Make sure you don't inadvertently become an outbound spam relay.
- Comply with subpoenas to identify students who are violating Higher Education Opportunity Act (HEOA) rules against peer-to-peer file sharing.
- Simplify wireless guest access.
- Block access for individual students when appropriate.

Block Malware in a BYOD World

Challenge: After vacation breaks, students flock back to campus bearing new devices such as smartphones, tablets, laptops, and gaming devices. These devices can become infected when students connect them to home or public networks, spreading malware when students next connect to the campus network. The old approach to malware protection—installing antivirus agents on endpoints—is not feasible when students own the endpoints. And even if it were, malware can still sneak onto networks between the time a new virus appears and the time the antivirus vendor updates its signature file.

Solution: The solution is to block malware at the network level, rather than on the device itself. The Cisco® security architecture provides multiple options to accomplish this:

- Cisco Identity Services Engine (ISE) recognizes user identity and the device profile.
- Cisco ASA CX Context-Aware Security provides full firewall capabilities and controls for web, Skype, peer-to-peer, and voice traffic.
- Cisco Web Security Appliance (WSA) protects against malware and also provides data loss prevention. For comprehensive, up-to-date threat information, the appliance connects to Cisco Security Intelligence Operations (SIO) (see sidebar).
- Cisco ScanSafe Web Security Service offers the same protection as Cisco WSA in the cloud, converting a capital expense for equipment and software to an operational expense.
- Botnet Traffic Filter, a feature of the Cisco ASA Adaptive Security Appliance, helps to identify and prevent botnets. Bots, surreptitiously installed on infected campus endpoints, send command-and-control traffic back to an attacker's host to exfiltrate data or launch denial-of-service attacks. The Botnet Traffic Filter monitors network ports to identify bots and uses information from Cisco ISO to accurately identify command-and-control hosts. One university uses this feature to identify compromised machines, providing a list to the campus security team, and also blocks the "phone-home" connections to command-and-control centers. This has enabled the university to increase its security posture without impinging on students' freedom to use the Internet; only the traffic to known command-and-control centers is blocked.

Protection from Even the Newest Malicious Websites

Cisco Security Intelligence Operations (SIO) protect colleges and universities from emerging threats that could take down the network or enable hackers to retrieve confidential information. Higher educational institutions benefit from the US$100 million Cisco has invested in the SIO:

- Cisco SensorBase is a threat-monitoring network that captures threat telemetry from more than 700,000 Cisco sensors deployed globally, monitoring 35 percent of the world's email and web traffic. This live data is combined with a historical database of more than 40,000 vulnerabilities.
- Cisco Threat Operations Center is staffed by 500 security analysts as well as automated systems. The analysts conduct research on emerging threats 24 hours a day, every day, from offices throughout the United States as well as Australia, China, India, Israel, Ukraine, and the United Kingdom.
- Dynamic updates are delivered to your Cisco security devices within a few minutes, often hours before other solutions, protecting the campus network against the latest threats.

 © 2013 Cisco and/or its affiliates. All rights reserved.

Manage Residence Hall Threats

Challenge: Gaming consoles are likely here to stay on residence hall networks (ResNets). Anecdotally, when one university tried to ban the consoles because of their susceptibility to malware, parents called the president to complain, citing the value of gaming for stress relief. Keeping track of gaming consoles presents a challenge for campus IT teams because they don't authenticate to the network as 802.1X supplicants. Campus IT teams also need a way to prevent consoles from consuming so much bandwidth that they degrade network performance for other dorm residents.

Solution: Monitor and control gaming console usage using the Cisco ISE, which can identify gaming consoles in addition to printers, fax machines, laptops, and so on. Cisco ISE recognizes when a new gaming console is attempting to connect to the ResNet and can present a web page for the student to register the device. You can limit the number of consoles per student.

Cisco ISE shows whether each device is on or off. If you see that one IP address is generating excessive traffic, you can tell whether it is a Blu-ray player, PlayStation, and so on and then look at the self-service registration information to see who owns that device. Then you can either ask the student to curtail usage or simply take the console off the network. Cisco ISE trending reports help to prevent future problems. If you see from a report that the ResNet connects 250 gaming consoles that are consuming 10 percent of bandwidth, for example, you can use Cisco ISE in conjunction with a third-party tool to apply rate limiting.

Don't Become a Spammer

Challenge: Infected devices owned by current and former students can become outbound relays for spam. If this occurs, your service provider might block outbound email from university addresses, interrupting operations and compromising the institution's reputation. Uncontrolled high-volume email delivery can also overwhelm recipient domains, including other campuses in the system.

Solution: Cisco Email Security Appliance provides two ways to prevent outbound spam and maintain a healthy reputation score:

- Turning on the Virus Outbreak Filter.
- Using the Destination Controls feature to set up rate limiting. You can specify the maximum number of concurrent connections, number of messages that can be sent to each destination domain, and number of recipients.

Simplify Guest Access

Challenge: Campus IT teams often need to provide guest access during events such as Homecoming Week, when hordes of parents and alumni arrive on campus. A common approach is to create hundreds of guest accounts, one by one, before the event, which is a time-consuming chore.

Solution: Cisco ISE can automatically register guests as they attempt to connect, restricting traffic to a guest VLAN that provides Internet access only. This relieves the campus IT team from having to issue passwords.

Comply with Subpoena Requests Relating to Illegal Peer-to-Peer File Sharing

Challenge: The Higher Education Opportunity Act (HEOA) includes provisions that are designed to reduce the illegal exchange of copyrighted works through peer-to-peer file sharing. But some students violate the law. Therefore, campus compliance teams need an easy way to comply with subpoenas to identify the campus user associated with an IP address associated with illegal file-sharing activities. The difficulty is that IP addresses change frequently, making it difficult to find out which student had which IP address on a particular date. Also, savvy students engaged in illegal file sharing might use proxy anonymizers.

Solution: One option is to control peer-to-peer applications such as Tor and BitTorrent and control or block proxy anonymizers. You can accomplish this using Cisco ASA CX Context-Aware Security. Or, if your college or university prefers to not block any type of traffic, on principle, you can comply with subpoenas more easily by using Cisco ASA CX to correlate traffic with a username instead of an IP address.

Limit Internet Access for Specific Students

Challenge: Colleges and universities sometimes need creative ways to get the attention of students who owe fines or who repeatedly violate restrictions on peer-to-peer file sharing.

Solution: An effective attention-getting method for today's students is to interrupt their Internet access. You can accomplish this by integrating Cisco ISE with Microsoft Active Directory. If a student has multiple outstanding parking tickets, for example, the campus safety team or IT team can select a checkbox in the student's Active Directory account. The next time the student attempts to connect, Cisco ISE sees the attribute and then presents a webpage explaining that Internet access will be restored when the student pays the fines. Then Cisco ISE can even redirect the connection to a webpage where the student can pay.

 © 2013 Cisco and/or its affiliates. All rights reserved.

Conclusion

In the post-PC era, colleges and universities face a new set of cyber security challenges. Implementing point solutions for each challenge is an unsustainable approach and leaves the campus in a vulnerable position when new types of threats emerge. The more cost-effective and simpler approach is to implement a security architecture that addresses the full spectrum of cyber security challenges, including malware blocking, registering of new devices such as gaming consoles, preventing outbound spam, and guest access.

The Cisco security architecture addresses all of these security requirements, helping colleges and universities maintain their commitment to an open environment without compromising campus information and networks.

For More Information

To learn more about Cisco security solutions for higher education, visit **www.cisco.com/go/edumobilitywireless**.

To learn more about Cisco solutions for education, visit **www.cisco.com/go/education**.

 © 2013 Cisco and/or its affiliates. All rights reserved.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1007R) C36-641137-00 9/11