aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

GRADUATE TO SECURE NETWORKS IN HIGHER EDUCATION

Securing the network amidst BYOD and IoT

EMERGING TRENDS, NEW CHALLENGES

Higher education has changed dramatically over the past ten years. With the proliferation of smart devices and Wi-Fi connectivity, the entire teaching and learning experience has been radically altered. As every user is now connecting wirelessly with multiple devices, student to educator and student to student collaboration have replaced the one-way lectures and physical pen on paper note taking of the past.

Studies show that 45% of students own three or more mobile devices[1], 78% of students use a smartphone, laptop, or tablet for learning[2], and 65% of student's report that when technology is used, they feel more connected to the course content, their instructor, and others in the class[3]. Given these statistics and the fact that devices such as AppleTVs are more common on the network, real-time collaborative teaching and learning is expected by teachers and students.

These changes go beyond the learning environment. With Internet of Things (IoT) devices being introduced at a rapid pace, departments responsible for running the campus now need to remotely monitor and manage various non-traditional endpoints such as temperature sensors, wireless surveillance cameras, door locks, and lightbulbs. The convergence of cloud, apps, and and a mixture of smartphones and IoT have moved into all aspects of campus operations and student life.

It's fascinating to think of the endless possibilities that a mobility powered network can provide, and with these advances, the upcoming challenges. The most obvious challenge is that of ensuring security and privacy. Network and security IT teams must collaborate to stay ahead of the curve, as they can easily lose control of their network, leaving students and staff vulnerable. According to Symantec's 2015 Internet Security Threat Report, education is the third most targeted vertical in terms of security breaches.

UNDERSTANDING TODAY'S CHALLENGES

It's one thing to have new technology create a richer and more flexible learning experience — but from IT's perspective, Pandora's Box has been opened to expose new security threats and privacy concerns. With users and BYOD potentially accessing questionable resources, and with outsiders potentially accessing sensitive student records, unmanaged and unknown devices bring a whole new host of problems for IT to consider.

Differentiated access – The roles of network users on campus need to be clearly defined. Whether it be an administrator, professor, guest, or student, each user should have clearly defined access to the network. Access control must be defined by user/role, devices, and from what location they are accessing resources. Policies can then be created that use this information to define access privileges.

As institutions have evolved and adopted new identities based on user needs, today's solutions must be able to leverage an active directory, LDAP, Google directory or endpoint database for user and device context. As BYOD and IoT devices may not be entered into an active directory, this is a looming challenge for higher education.

Managed BYOD – When dealing with large numbers of students on the campus, it's impossible for IT to know about and/or configure all of their personal devices. However, these unmanaged devices must have some level of control on them to access the campus network or internal resources. While visibility issues may be the same for professors, administrators, guests and staff, there are different concerns regarding access privileges.

Regardless of user type, IT can configure Aruba ClearPass to differentiate users based on role, device, and location. This contextual information can then be used in predefined policies that can enforce such things as who can onboard their BYOD devices and reach learning apps and who cannot, how many devices they can onboard, what type of device is allowed, and from what location they can access these apps.

ClearPass can also issue certificates to onboarded devices so that stronger authentication, easier revocation, and a simpler user experience is possible. Certificate based authentication relieves the user of manually typing in passwords on small smartphone screens and protects them from password loss. And when accessing specified applications, ClearPass can work with third party multi-factor authentication partners for an added level of security.

Internet of Things (IoT) – Headless IoT devices such as temperature controls, IP cameras, and game consoles have traditionally been a challenge to identify with standard fingerprinting tools. ClearPass has the ability to allow IT to custom define fingerprints for headless devices, categorizing them, for any device type that connects to wired or wireless networks. For example, a video conferencing device can be identified and put into a category that allows ClearPass to place it in a VLAN and grant its traffic priority access in the network for certain hours.

Streaming collaboration – Educators are using wireless streaming capabilities and tools like AirPlay and DLNA services to boost collaboration. Security is a problem though, as easy access to networks can allow anyone to connect to devices and printers that are not meant for them. Also, in education environments, where classrooms are just next door, it can be easy to accidentally connect to a networked device that sits in a neighboring classroom. Managing access within a group is important, as is restricting access to others outside the group. It is important for IT to easily create policies that manage and control access.

ARUBA CLEARPASS — KEEPING EDUCATION CONNECTED AND SECURE

With ClearPass, IT can replace legacy AAA solutions with mobility-centric policy management, profiling, reporting and management tools. The flexibility in managing BYOD, guest access, and device assessments allows IT to add onto a ClearPass deployment, as needed.

Per IT policy, ClearPass Onboard allows only users with permission to self-configure BYOD for use on a secure campus network.

Similarly, with ClearPass OnGuard, IT can ensure that any designated laptop is running current patches and hotfixes, anti-virus, and anti-spyware updates, relieving help desk calls and visits.

ClearPass Guest can grant Internet or internal access to any user via social login, usage agreements, or a completed form. Access can be restricted to certain network assets with auditable logs in lieu of simple Internet connectivity. Access periods can be enforced by length of visit, set amount of time, bandwidth used and more. Mac address caching allows for seamless connectivity each time the user connects to the network during a stay to eliminate the need to repeatedly login via the portal.

Because most learning institutions are multi-vendor environments, ClearPass works with any network infrastructure and communicates with any point security solution to bolster your existing network investments – which is included within our base product offering.

ClearPass is designed for the technology driven and mobile campus setting. To learn more about ClearPass Policy Manager and the Onboard, Guest, and OnGuard applications, click here (http://www.arubanetworks.com/solutions/adaptive-trust-defense/).

[1] Pearson Student Mobile Device Survey, conducted by Harris Poll, March 2014
[2] Students' Mobile Learning Practices in Higher Education: A Multi-Year Study, Educause Review, Baiyun Chen, Ryan Seilhamer, Luke Bennett and Sue Baue, June 2015
[3] ECAR Study of Undergraduate Students and Information Technology, Educause, 2014

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com