

Campus Case Study

Background

This case study deals with a large university campus in South Asia. The campus itself is spread over several hundred acres dotted with academic, residential and recreational buildings. The campus has been blanketed with WiFi coverage, used by students & faculty. Certain areas are also connected via Ethernet.

Quick facts:

- 10,000+ students
- Campus spread over hundreds of acres
- Network access provided to all, including campus visitors
- 2 x STM-1 (~300 Mbps) Internet connectivity from multiple service providers

Objectives

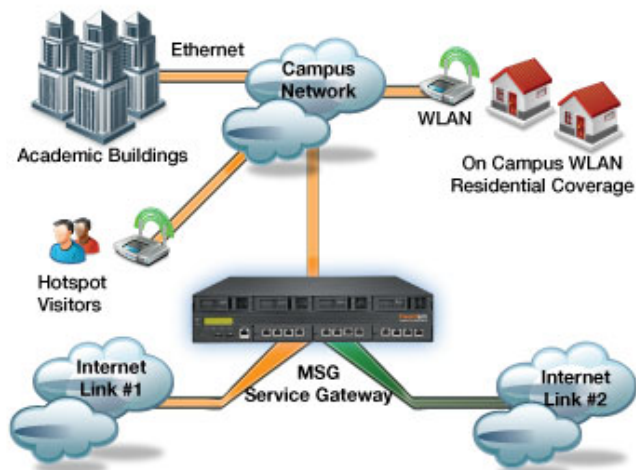
The university had the following key:

1. Authenticate, control and track every Internet session
2. Introduce billable Internet usage system for students
 - a. Reduce existing bandwidth spend through better control
 - b. Convert existing *operational cost* (bandwidth) into a revenue opportunity
 - c. Create logon schedules and assign monthly download limits/quotas for students, faculty and departments to check bandwidth abuse
3. Secure handling of visitor network access, typically single use
4. Traffic & Bandwidth Management
5. Firewall protection & filter unwanted websites
6. Lawful tracking of user sessions for various law enforcement agencies
7. Provide a highly reliable service using multiple ISP uplink providers

The Solution

Inventum proposed its MSG Multi Service Gateway 3000 as the ideal solution to address all the objectives laid out by the university.

The MSG ISP Edition gateway was installed at the central NOC of the university. Existing UTM appliances were removed from the network and all firewall features were also migrated over to the MSG.



Diagrammatic representation of customer deployment

Authentication & Control

The university was desirous of authenticating every user attempting to access the network. The primary form of authentication to be used was via a web portal page, similar to those implemented at hospitality locations worldwide.

The university already had all user credentials (usernames & passwords only) available on a central RADIUS¹ server. However, the university did not have any central policy store or directory such as LDAP to publish user specific policies. As a result, any authentication or network admission solution would have to devise a hybrid authentication system.

The MSG enabled the following:

- University was able to manage user accounts within the MSG subscriber database, complete with all policy information. The password lookup however was pointed to the external existing RADIUS of the university.
- Any new user session would first be sent to a portal logon page where the correct credentials would need to be entered.
 - The MSG made it possible to also tag user accounts with Ethernet MAC, VLAN & IP address information so that login passwords would work only from specified PCs, smart phones or other network devices.
 - For devices such as IP phones, which did not have a browser, the web login was replaced with a non-interactive or *silent login* using only the MAC & VLAN as credentials.
- Each session is now provisioned based on the stored network policy, which in turn could be linked to a bill plan and bandwidth rate limit. For example, it is possible to give *Student X*, 256kbps

¹ FreeRADIUS had been used to store credentials

during the day and 512kbps at night with access possible only on weekdays.

Billing for Bandwidth

Concerned with ever increasing bandwidth demand, the university had decided to convert Internet use on the campus into a profit center. Acting almost like an ISP/WISP, the university would provide students a monthly Internet plan with a download volume cap. The cost of this plan would be added in the tuition fee invoice itself. Should students exhaust their volume quota, they could purchase a *top-up* scratch card for a small reasonable fee.

The MSG enabled the following:

- Provided a point & click, web application to create and administer billable service plans.
- All plans could be linked to quotas, bandwidth rate-limits, logon schedules on a per student basis.
- Usage overages could be charged separately with support for top-up cards and one-time-passwords
- Provided a web browser based end user portal for students to monitor their accounts, raise trouble tickets, send administrators messages and even inspect individual session bandwidth graphs.

Secure Visitor WiFi

Be it visiting faculty or families of students, most visitors require WiFi access. The university required an easy way to provide a secure, traceable system to handle visitors who would stay from a few hours to a few days.

The MSG enabled the following:

- Use a hotspot style logon experience for visitors. Campus had the option to publish a second *Visitor SSID* on their WiFi access points, which were tagged to a different VLAN to ensure secure traffic separation at Layer 2.
- Creation of pre-pay, hotspot plans ranging from 30 minutes usage duration to a monthly pass.
- Once a visitor had selected the desired plan via the logon portal, the same would be activated using a one-time-password (OTP). The OTP would be generated and delivered via a mobile SMS.
- Visitors could also be acquired/authenticated using a credit card payment gateway hookup directly from the MSG.
- Once authenticated, the visitor's traffic would be logged against their identity for future analysis by lawful agencies or network administrators.
- The MSG being capable of hosting multiple routing tables and firewall rulesets made it possible for the university to handle

visitor traffic differently from internal WLAN users. It's worthwhile to mention that the MSG can tailor IP filtering & routing on a per user basis.

Traffic & Bandwidth Management

Class based bandwidth management enabled by the MSG helps the university prioritize certain users and improve QoS for latency sensitive, application traffic.

The MSG also manages bandwidth on a per user session basis including CIR/BIR, contention ratio management and more.

Firewall & Filtering

Prior to the MSG the campus had deployed a leading vendor UTM appliance primarily for handling IP filtering requirements.

Post MSG, the university was able to completely remove the existing UTM appliances while retaining the following key functions:

- Filter specific URLs
- Filter particular subnets
- Handle specific policy routes
- Block IP ports
- NAT & DNAT specific subnets and services
- Protect against denial-of-service attacks

Lawful Tracking

In compliance with local legislation, all WLAN users and visitors sessions must be logged. All activity of a given user can be summoned by lawful agencies up to three years.

The MSG met lawful requirements, logging session information to an external Syslog server.

Load Balancing

With thousands of concurrent Internet users and multiple Internet bandwidth providers, the university required the highest possible uptime with load balancing capabilities on Internet uplinks.

The MSG 3000 conformed to the high availability requirements:

- Dual redundant, hot-swappable power supply
- Redundant internal storage

- Front accessible, hot swappable network modules
- Capability to run second MSG in HA mode
- Multiple WAN link load balancing is provided to ensure policy based or load based optimal link usage

Conclusion

The MSG 3000 proved to be an ideal platform for the university to control their Internet usage. The university was able to derive immediate financial benefit from the reduction in bandwidth requirements owing to better management and no misuse by the student community.