Making a Mountain of a Molehill (all we wanted to do was automate eduroam installation)

Wil Daniels
ACU National

Questnet 2008

Introduction

The project team

Project Owner - Wil Daniels (National Infrastructure Manager)

Project Manager – Au Lai Wo (ITS - Infrastructure)

Technical Architect – Stephen Walsh (ITS - Infrastructure)

User Acceptance testing – Mark Laffan (ITS - Infrastructure)

Portal page design – Donna Laffan (Library)

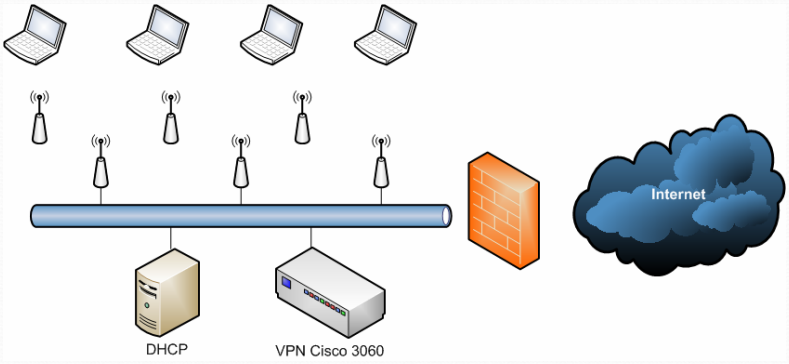
The Way it was...

- Wireless network in production for more then 3 years.
- Security based on VPN tunnelling via Cisco 3060
- Hardware components a mixture of Dlinks & Cisco Aironet 1200.
- Issues: Vista and mobile device support, lack of centralised network management.

The Way it was...

- Closed garden-style wireless network
- Different ESSID per campus (patwlan, msmwlan, etc)
- Router ACL to only allow traffic to VPN server
- Used standard Windows VPN software

The Way it was



The Way it was...

Pros

- Quick and simple to setup
- Easy to support (both locally and by service desk)
- VPN also allowed staff to connect back from other institutions
- Security was confirmed by the VPN tunnel itself

Cons

- User awareness of ESSID differences
- Required ACU user account
- Hard to diagnose faults or connection issues

Change is on the way...

In January 2006, ACU was one of the first Universities to deploy an eduroam wireless network. This moved the security from the VPN client to a two-stage security model;

WPA/TKIP provides security between the laptop and the AP

EAP/TTLS provides a second SSL-style tunnel between the laptop and the Radius Server down which the user authentication is passed.

Change is on the way...

Partial automation was provided by a Ghost AI package, but licensing limited what we could do, as we could not use this on student or private laptops.

There was marginal success with this method, but there was a continual need for different versions to be maintainted due to differences with patches on Windows XP.

Review what was...

An internal review of the network was undertaken in July 2007, and input was sought from both the end users and the Client Support/Service Desk areas.

All areas of the current wireless network were reviewed, from coverage to security, as well as ease of configuration and end user experience.

Reviewing what was

The end result of the review determined that;

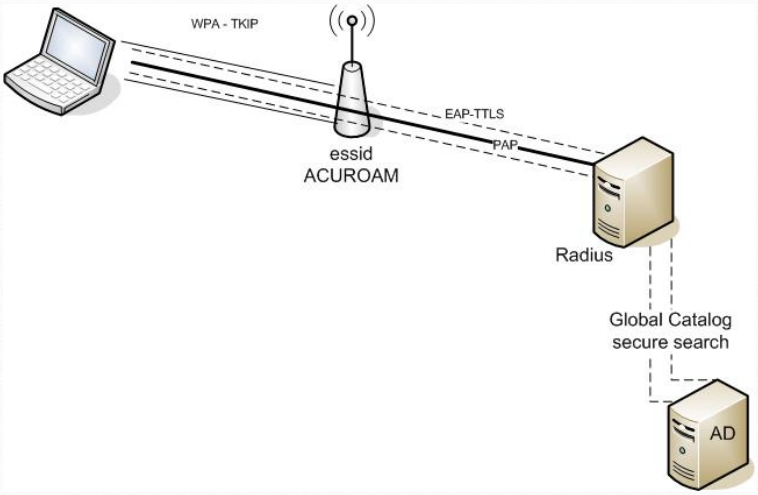
- The original closed garden wireless had been overtaken by new wireless security methods
- The usability of the eduroam network by university staff on campus was preferred over the original wireless service
- The difficulty with installing and configuring the SecureW2 client by support staff was highlighted

The change..

The solution reached was two fold;

- Replace the Closed garden wireless with a more secure wireless based on the WPA/TKIP and EAP/TTLS used in eduroam
- Find a way to automate the installation and configuration of the SecureW2 client needed for windows to connect to eduroam.

Security against attacks



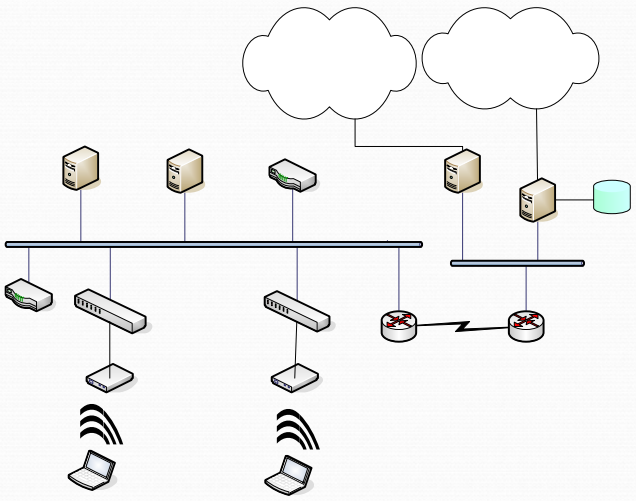
The Secure Wireless network

Once the technology was decided the architecture was simple;

- Clone the eduroam freeradius config
- Remove the parts that proxy users to the AARNET NRPE servers
- Use it as the backend to the new wireless network called “ACUroam”

The Secure Wireless network

- Coverage = equipment
- Original service was hotspot orientated
- Hotspot != coverage



The problem remains..

This still left us with the problem of how to automate the installation of Eduroam. Our previous attempt had shown us the problems of trying to “overlay” a config onto a machine, and that SecureW2 had to be installed for optimum results.

The Solution appears

This solved the automation problem, but still left us with the problem of deploying the installer.

The Solution

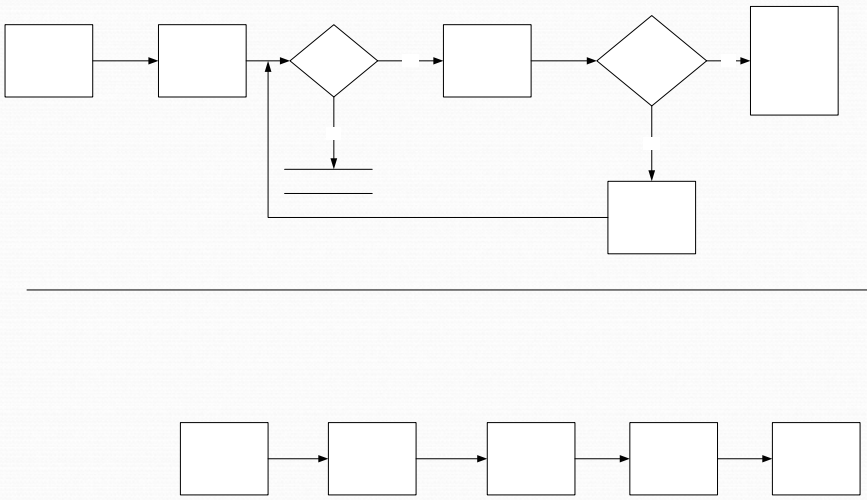
We eventually decided on a “pull” model, where students could go to a web portal page and download the installer, but that introduced a chicken-and-egg problem.

The open wireless network

From this, ACUwifi was born. It was an open, unsecured wireless network, that would redirect all web traffic to a webpage, portal.acu.edu.au, and download the installer.

Plan 'B'

“Plan B” consisted of a linux box on each campus, acting as a NAT gateway and firewall, between the open wifi network, and the ACU Internal network.



The Configuration juicy bits

Iptables;

iptables -t nat -A PREROUTING -i etho -p tcp --dport 80 -j REDIRECT --to-port 3128

Squid.conf;

url_rewrite_program /usr/local/sbin/rewrite.pl

Configuration

rewrite.pl

```
$|=1
while (<>) {
    @X = split;
    $url = $X[0];
   //check the URL, if it matches, allow it through
   if ($url =~ m[^http://portal\.acu\.edu\.au]) {
            print "\n";
    }
   //otherwise send them to the portal
           else {
   print "302:http:\/\/portal.acu.edu.au\n";
     }
}
```

Even Plan 'B' has scope creep

User feed back on the new wireless network was extremely positive. Initial responses indicated that whilst acuwifi was filling it's role perfectly, there were still students using the web kiosks to check enrollments, webct, view the corporate and intranet sites, etc.

URL inspection in Perl

```
$|=1;
while (<>) {
   @X = split;
   $url = $X[0];
   print LOG "got URL $url, ";
        //check the URL matches what's allowed
   if ($url =~ m[^http://(webct|my|www|inet|portal)\.acu\.edu\.au]) {
      print "\n";
      }
        //else send it to the portal page
    else {
      print "302:http:\/\/portal.acu.edu.au\n";
         }
}
```

Flexibility is key..

The flexibility of the system was key to it's acceptance by the end users.

The results

Although the design of the network has been proven a success by it's security and flexibility, the end results, which was to simply and automate the installation of the Eduroam connection software, we are in the same position we were when we started, where the end user prefers social interaction to have their device configured.

Stats

In the first week of operation, over 1400 successful unique logons where made to the new system.

Since it was launched into production on the 6th September 2007, the portal website has had 160,000 hits, with over 1000 downloads of the self service installer, and over 3000 walk in requests for assistance with the installer.

Not everyone wants selfservice

Investigations into the disparity between self service downloads and requested assistance showed that even with the simplification of the installation process of the SecureW2 client, where the client has prompted to enter their username, accept a AUP, then reboot, they still preferred to have someone else do it for them.

Budget

• Linux based routers and radius server:	$12.5k
• Cisco WLC (11x):	$55k
• Lightweight AP (100):	$55k
• Network Cabling :	$28 k
• Contingency :	$4.5 k
TOTAL	$155k

QUESTIONS?

- Acknowledgements

  Stephen Walsh

  Mark Laffan