User Directories and Campus Network Authentication - A Wireless Case Study

Sean Convery
Identity Engines

Kevin Jones
Metropolitan Community College
Agenda

- Role-based Access Control
- About MCC
- Wireless project Goals
- Wireless Hardware
- Authentication Setup
- Future Plans
A History Lesson

Expanded threat profile leads to more security devices (IDS, VPN, Basic Host Controls). Legacy RADIUS serves authentication requests but lacks richness for authorization policy. Most access IP rather than user based.

Distribution of security continues, with authorization tied closely to enforcement. Lack of flexibility of legacy AAA leads to multiple discreet RADIUS stores and local users configured in enforcement devices.

The goal:
1. Centralize user authentication through flexible next-generation AAA services.
2. Centralize key elements of the authorization policy creating centralized audit and control.

IdM Phase 2

IdM Phase 1

Centralized

Distributed
Network Security Evolved

Traditional device-centric IP-based security techniques are inadequate to meet this new reality
- Role of the traditional inline security gateway is diminishing

Organizations are turning to role-based access control (RBAC) as the new unified network security approach
- Supports multiple user types with multiple access profiles
- Addresses compliance requirements
- Leverages identity to integrate with the network infrastructure directly

IT departments are now required to support more kinds of users, with more types of devices, connecting to a wider variety of network access points – all while being exposed to an unprecedented degree of regulatory and audit oversight
Role Based Access Control

- **Client** - Device / user attempting to access the network
- **Policy Enforcement Point (PEP)** - network device that brokers access request and enforces policy result (i.e. WLAN AP, Firewall, VPN gateway, Ethernet switch)
- **Policy Decision Point (PDP)** - network device that decides policy for client based on PEP and PIP interaction
- **Policy Information Point (PIP)** - a source of information in setting policy (i.e. user directory, asset management system)
- **Accounting** - Audit destination for client access and network usage

Production Network
RBAC Example - Secure Wireless

- All WLAN Access is authenticated enabling user audit and differentiated access
- Dynamic VLAN assignment segments the traffic with enforcement via ACLs
- Guests can be forced to the Internet only, contractors can be given restricted internal access, privileged employees can see sensitive areas
- *Guest access is fully audited rather than open*
Secure WLAN, 802.1X, and RBAC

RBAC via 802.1X is the core component of secure WLAN

There is more to 802.1X than basic RADIUS

- **Policy Server** – need to support rich policies and heterogeneous network gear
- **Directory Connectivity** – must leverage LDAP for user accounts *and* groups/attributes
- **Supplicant Management** – 802.1X client configuration requires automation to ensure a supportable infrastructure
- **Legacy Support** – portal solutions for outdated portions of the network and for guest access
• Seven Campuses serving the greater Kansas City area.
• Our database contains over 123,000 users.
• For the fall 2007 semester we have 18,124 active credit students.*
• Add non-credit classes and MCC has over 43,000 students each year.**

*http://www.mcckc.edu/research/factbooks/MCC_Fall_Factbook.pdf
Our Locations

Seven Campuses located around the greater Kansas City area.
• Consisted of SOHO wireless routers spread throughout the district. Mainly just covering the libraries and cafeterias
• Each one had to be managed individually
• Open access (no security)
• Unreliable
New Wireless Goals

- Expand coverage
- Improve Reliability and Security
- Easier to manage
- Authentication to Novell eDirectory
- Provide Wireless Internet without compromising the normal network
- Did not want to load any software onto Students or Guest computers
- Needed and easy way to create and manage guest users that was separate from Novell eDirectory
Wireless Hardware

- Cisco Wireless Control System
- One Wireless Control Server for the district
- One Wireless LAN Controller for each location (6 total)
- As many lightweight access points needed to cover the needed areas
- Each campus has a fire-walled private network dedicated for wireless
- The WCS system can use access-lists, but by itself can only assign an access-list per SSID
Cisco WCS Hierarchy

**WCS Server:**
- Central Management
- Templates and Policies

**Ignition Server:**
- Authentication

**Wireless Controllers:**
- Manages Lightweight Access points
- DHCP for local private network
- Where the Access List is applied to the wireless user
- Rouge Detection

**Lightweight Access Points and Clients:**
- Completely dependent on the controller
WCS Campus Level

Firewall

Wireless Controller

Access Points

Clients PEAP/MSCHAPv2

Internet
Authentication Goals

• Needed to use LDAP to connect to the Novell eDirectory for user authentication

• Needed to give different levels of access to different groups

• Certain staff and faculty need full network access, while students and guests should only get basic Internet
• We were committed to using Cisco wireless hardware and Novell’s Identity Manager
  • We just needed to get them to work together
• Tried Cisco’s Access Control Server (ACS)
• Tried FreeRadius
• Finally ended up using Identity Engines’ Ignition Server 3000E
Identity Engines Advantages

- Easiest to connect to Novell Identity Manager
- Easy to setup initially
- Could tell the Cisco System which ACL at the user level
- Provides many other options we may use in the future
- We felt it was a RADIUS solution that could meet all of our needs
Identity Engines Setup

- First create your service categories
- Next create any outbound values you need
- Lastly create policies
Creating an Outbound Value
Triggering an ACL
After you have your service categories and attributes setup you can set up your groups.

These are just the groups from the Identity Engines embedded database not the Novell Identity Manager groups.
Once you have your attributes and groups set up you can then create your policies.
Authorization Rules
Once your policies are set you need to set up the Authenticators.

The Authenticator is the actual device making the radius request. At MCC the authenticators are the Cisco Wireless Controllers.
• There is an explicit deny rule that will automatically block anything not permitted by a rule.
• In this way we manually create an rule for permitted traffic and everything else is automatically blocked.
• We can have as many access lists as we need and each group can have their own unique access list.
• We rely on the Ignition Server to tell the wireless controllers which access list to use for each authenticated user.
Guests

- Guests are managed separately from Novell Identity Manager
- We use Identity Engines Guest Manager software for all Non-MCC users
- Guest Manager is a software suite that integrates with Ignition Server
- It even allows different levels of access to Provisioners.
  - Different Provisioners can grant different levels of access to the guest users they create
This image shows the options available when creating a provisioner.

The Access Types are equivalent to the groups and policies you created for them on the Ignition Server.
Adding a Guest User
Client Setup - WinXP

1. Network name (SSID): MCC-Wireless

2. Wireless network key
   - Network Authentication: WPA2
   - Data encryption: AES

3. EAP type: Protected EAP (PEAP)

4. Enable IEEE 802.1x authentication for this network

5. 1 - Select PEAP
6. 2 - No Check marks
7. 3 - click here

- This is a computer-to-computer (ad hoc) network; wireless access points are not used
- The key is provided for me automatically
- The key is provided for me automatically
- This is a computer-to-computer (ad hoc) network; wireless access points are not used
Client Setup - Mac

The selected AirPort network requires a password to join.

**Wireless Security:** WPA Enterprise
**User Name:** S012345678
**Password:** ********
**802.1X Configuration:** Automatic
**TLS Certificate:** pistos

- [ ] Remember password in my keychain

- [ ] Always trust these certificates

The server certificate could not be validated because the root certificate is missing.

- [ ] Show Certificate
- [ ] Cancel
- [ ] Continue

*DefaultProtocol*
Issued by: www.idengines.com
Expires: Wednesday, December 31, 2025 12:32:42 PM US/Central

- [ ] Details
- [ ] Trust Settings

This certificate was signed by an unknown authority.

- [ ] Hide Certificate
- [ ] Cancel
- [ ] Continue
Issues

• At first could not get Vista to authenticate
  • IDE updated the software on the Ignition server to accommodate Vista

• Older hardware/software combinations may not support WPA and RADIUS
Future Projects

• Now that the Ignition Server is in place and connected to Novell eDirectory we can use it for all of our future RADIUS needs
  • VPN
  • Wired 802.1X: Some wired ports are in public areas. We plan on implementing 802.1X so that we can leave them active and control access to the normal wired network.
Summary

- Wireless users of Metropolitan Community College authenticate to Novell Identity Manager and Identity Engines Ignition Server in order to be granted access to a secure Cisco Wireless system.
- The Students love having wireless district wide.
- The Feedback has been overwhelmingly positive.
- Both speed and reliability has been greatly improved.
- Netflow reports show an almost complete drop in unwanted traffic.