



Protecting your wireless network with **Network Admission Control**

Justin Rowling – Systems Engineer

What is NAC ?

Gives differentiated access to the network based on

- Who you are (staff, student, visitor etc)
- What you have (Platform/OS, patch level, AV status etc)

Why do you want NAC

- Major threat is still malware on Windows 2K upwards
- Primary motivation is fear or 'mass outbreak'
- Also reducing helpdesk/support workload
- Also makes ports/SSIDs 'dynamic'
 - access/acl's vary by user/group

NAC on Wireless LANs

- WLAN users are more likely to
 - Have been off the network for periods of time
 - Have been on another network
 - Be non-standard
 - Be new (to you)
 - Need an authentication system*

- All of these increase the risks and/or support overhead

Key Requirements of NAC Solution

- Securely identify users
- Enforce policy specific to type of users
- Quarantine and Remediate
- Be easy to set up and keep up to date
- Play nicely with network operating systems

Securely identify users

- Check username and password directly or
- Trust some other authentication like 802.1x, Windows domain, VPN concentrator etc
- Should use existing directory structure LDAP, Radius etc
- Use this information to get group/role of user e.g staff, student, contractor etc.

Enforce policy specific to type of users

- Staff – policy might be very prescriptive:
 - specify the allowed types of OS, one AV agent, required software etc, but then allow unrestricted access
- Students – policy may be more flexible
 - allow any AV, any OS, but restrict access to finance and admin networks
- Guests – policy may be light touch
 - may warn about OS health (patch levels) but not enforce, and allow access to anything but local IP addresses

Quarantine and Remediate

“as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know.”

Donald Rumsfeld

Quarantine and Remediate

- Protect the network from unknown users
- Protect unknown users from each other
- Give users who do not comply with policy enough access to self help
- Guide these users through the steps they have to take
- Take steps to prevent abuse

Be easy to set up and keep up to date

- Ideally turn written policy in to NAC configuration in easy steps
- If the system is not kept up to date its value diminishes
- If remediation is not straightforward users are more likely to phone/queue up at help-desk

Play nicely with Network OS

NAC solutions may restrict or change network access during boot up and log on process

Boot scripts, network drives, Group Policy objects may suffer

It's important to understand what the impact of a NAC deployment would be, and work around or fix these issues

Side benefits of NAC

Also works on Wired network ! (simplify)

Can also be used to check for required/undesirable s/w

Generates a wealth of information about clients

Can make ports/networks multi-use

Can present an AUP for regular acceptance

Summary

- NAC tailors network access to different user types
- NAC enforces your policy (good or bad)
- NAC can update/reconfigure users who don't comply
- NAC can reduce your exposure to 'mass outbreaks'
- NAC need to work with network OS for prime-time

