Identity-centric NAC

Sean Convery, CTO
Identity Engines
sconvery@idengines.com
Network Access Control
NAC Applications

Networks and Applications
- Role-based Segmentation
- Guest Management
- WLAN Security
- Network Node Validation

Identity Management

Security
Point Solutions

- Role-based Segmentation
  - VMPS
  - URT
  - 802.1X
  - MAC-Auth

- Guest Management
  - Web-Auth
  - Captive Portal
  - Overlay Network

- WLAN Security
  - WPA
  - VPN
  - MAC-Filter

- Network Node Validation
  - TNC
  - NAP
  - CCA
But...

What happens when you want to get a guest user on the Internet, via a wireless network, and check their laptop’s software?
Enter Complexity...

- Pre-NAC Network Troubleshooting
  - Physical Layer Problems
  - Network Congestion
  - Host TCP/IP Errors
  - Router / switch errors

- NAC Network Troubleshooting
  - Everything in the other column
  - Host 802.1X supplicant errors
  - Certificate issues
  - Availability of AAA server
  - Availability of NNV server
  - Misconfiguration of NNV rules
  - Device ID not in database
  - Username / password issues
  - EAP-type / crypto mismatch
  - VLAN / DHCP release - renew
  - Port ACL misconfiguration
  - SNMP drops / errors
A Lack of Standards...

- Trusted Computing Group / Trusted Network Connect
  - Juniper is the only shipping “solution”
  - Cisco pulled out Meetinghouse

- IETF Network Endpoint Assessment (NEA)
  - Two BoFs, One year of a mailing list, Cisco and Juniper participation.... No WG even created yet.

- Microsoft NAP
  - Vista is a requirement to begin

- Cisco NAC
  - Cisco is pushing their appliance not the framework
A Gaggle of Vendors
And What do You Get?
Instead, be Identity-centric

- Authenticating users before network access is not bleeding edge (dial-up, VPN, wireless, firewalls)
- Standards do exist for this (RADIUS, EAP, 802.1X, PPP)
- Compelling business benefits:
  - Centralized audit for all network access
  - Short-term access solution
  - WLAN Security
  - Role-based Segmentation
  - User Traceback
- Force guests to partitioned access and use standard host controls on endpoint devices
Go back to the basics

- Identity-centric NAC, and indeed all NAC means your AAA is now mission critical
- Mission critical functions in networking today include:
  - DNS
  - DHCP
  - Routing Protocols
  - Spanning Tree
- Consider how you deploy those technologies today vs. how you deploy AAA
Tame that pesky directory

- Multiple instances of Microsoft AD, LDAP, and other directories is the norm
- Virtual / meta directory projects take time
- Network operations guys aren’t fans of LDAP schemas
- Yet the business needs remain
The Identity Foundation

- **Goals**
  - Support all common network enforcement points
  - Support all common user directories
  - Enable rich standard policies based on network and directory context
  - Non-stop availability

- **Standards**
  - 802.1X
  - EAP
  - RADIUS
  - LDAP
  - XACML
  - SOAP
  - VRRP
Build for the Future

• The future of networking is mobile, user-centric, and secure
• User directories are a rich repository of user attributes, enabling this future to see reality
• Network enforcement devices will soon support a common base set of controls
• The key is to bridge the directory and networking worlds with a highly-available and user-centric policy decision service for NAC
  • As standards emerge to extend this policy layer they can be easily added
  • However significant business benefit is there now
For More Information

- Identity Engines: www.idengines.com
- Sean’s Blog: www.seanconvery.com/weblog
- Email: sconvery@idengines.com