End Point Security & Network Access Control

Presented by:
Jennifer Jabbusch - Carolina Advanced Digital Digital, Inc.
Alan Shimel - StillSecure
Darwin Socco - Bracewell & Giuliani LLP
Let’s Talk About…

- What NAC Does
- Key NAC Concepts
- Poor Man vs Rich Man’s NAC
- Your Thoughts?
What is NAC?

- Features depend on vendor and implementation choices.
- Why are some key features that NAC can provide?
What is NAC?

What ‘can’ NAC offer?

- Port security
- Network segregation
- User- or identity-based access control
- Endpoint integrity checking
- Guest access support
- Multiple user/device authentication
- Centralized management
Key NAC Concepts

- Where does it go?
- How does it work?
Key NAC Concepts

- Network based, host based
- Inline, out of band
- Managed and unmanaged
- Pre-connect, post-connect
- Remediation
- Identity based access control
- NAP, TCG, Cisco NAC framework
Key NAC Concepts

Network based, host based

- Authentication
- Network-Based
- Switch or AP
- Host-Based
- Endpoint

NAC
Key NAC Concepts

- Inline, out of band
Key NAC Concepts

Managed and unmanaged

Authentication

NAC

Switch or AP

Managed / Employee

Unmanaged / Guest

Endpoint

Endpoint
Key NAC Concepts

* Pre-connect, post-connect
Key NAC Concepts

- **Remediation**
  - Either automatically ‘fix’ what’s wrong on the endpoint, or provide access to remediation services on a quarantine network

- **Identity based access control**
  - Control what, when and how a user can connect and access resources based on their role or group
Key NAC Concepts

- NAP, TCG and Cisco NAC frameworks

**Microsoft**
- NAP = Microsoft’s Framework

**TRUSTED Computing Group**
- TNC = TCG Industry-approved framework by most vendors

**CISCO**
- Cisco NAC = Cisco proprietary framework
Why Do You Want NAC?

- Drivers for NAC in enterprises
- Drivers for NAC in the legal space
- What’s holding back NAC?
Importance of NAC in Legal IT

What are the drivers for NAC adoption in legal?
- Compliance
- Confidential information
- Guests on the network
- SOX and other compliance requirements

What are the factors slowing adoption?

What factors have driven adoption in existing firms?

Is there a competitive advantage to adopting NAC?
Poor Man vs Rich Man’s NAC

- Faceoff: NAC vs Not-NAC
- Getting NAC-ish features without NAC
Poor Man’s vs. Rich Man’s NAC

- Degrees of NAC adoption and mitigating your risk
- Reviewing some features of NAC?
  - Port security
  - Network segregation
  - User- or identity-based access control
  - Endpoint integrity checking
  - Guest access support
  - Multiple user/device authentication
  - Centralized management
✿ Practical Implementations (Wired or Wireless):
  ✿ Physical/Logical/Application

✿ Physical Approach:
  ✿ Create a stand-alone network ("The Starbucks Setup")
  ✿ Jack insert blocker/administratively shutdown data ports

✿ Logical Approach:
  ✿ VLAN segmentation with ACLs
  ✿ MAC address lockdown
  ✿ 802.1x Authentication (RADIUS)
Case Studies and Considerations for Selecting the Best NAC Solution (2)

Application Approach:

- Proactive OS patch/update management of endpoints
- Proactive AV push/updates
- Other company specific application updates
Poor Man’s vs. Rich Man’s NAC

**NAC**

- Port security with NAC
  (can be centrally managed)

- Network segmentation
  (can be globally configured by user or group and provisioned dynamically from ID mgmt)

**Not-NAC**

- Stand-alone 802.1X
  (must be managed on each switch manually or physical port control/jack covers)

- Dynamic or Static VLANs
  (manually configured per user-group from RADIUS or per-port on switches)
Poor Man’s vs. Rich Man’s NAC

NAC

- Identity-based access
  (centrally managed, based on users, groups or set of criteria)
- Endpoint integrity check
  (basic function of most NAC solutions)

Not-NAC

- Manual RADIUS groups
  (separate RADIUS group and policy manually created and configured for each unique access)
- Pro-active patching or NBAD
  (maintain patches and AV pro-actively or monitory with behavior anomaly detection)
Poor Man’s vs. Rich Man’s NAC

**NAC**

- **Guest access support**
  (centrally managed, based on user, endpoint type, presence of agent or other criteria)

- **Multiple user/device auth**
  (easily configured and centrally managed)

**Not-NAC**

- **Manual VLAN configuration**
  (manually configure VLANs per-port or per-SSID or use a vendor-specific solution)

- **Manual VLAN configuration**
  (same as above, must be manually configured, which makes multi-user/device auth difficult on shared resources)
Poor Man’s vs. Rich Man’s NAC

**NAC**
- Centralized management
  (centrally managed, based on user, endpoint type, presence of agent or other criteria)

**Not-NAC**
- Individual component config
  (each component, authentication servers, switches, access points and possibly endpoints will need to be configured manually individually or use a point solution per segment)
Case Studies and Considerations for Selecting the Best NAC Solution (3)

- Best of Breed Implementation
Your Thoughts?

- Why are you considering NAC?
- What’s keeping you from doing it?
- Do you need it?
Questions and Answers

Q&A

Jennifer Jabbusch
Carolina Advanced Digital, Inc.

Alan Shimel
Still Secure

Darwin Socco
Bracewell & Giuliani LLP