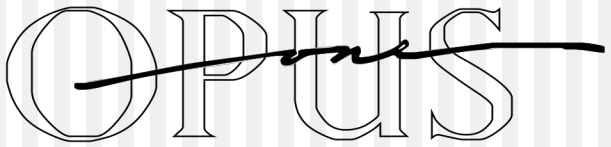
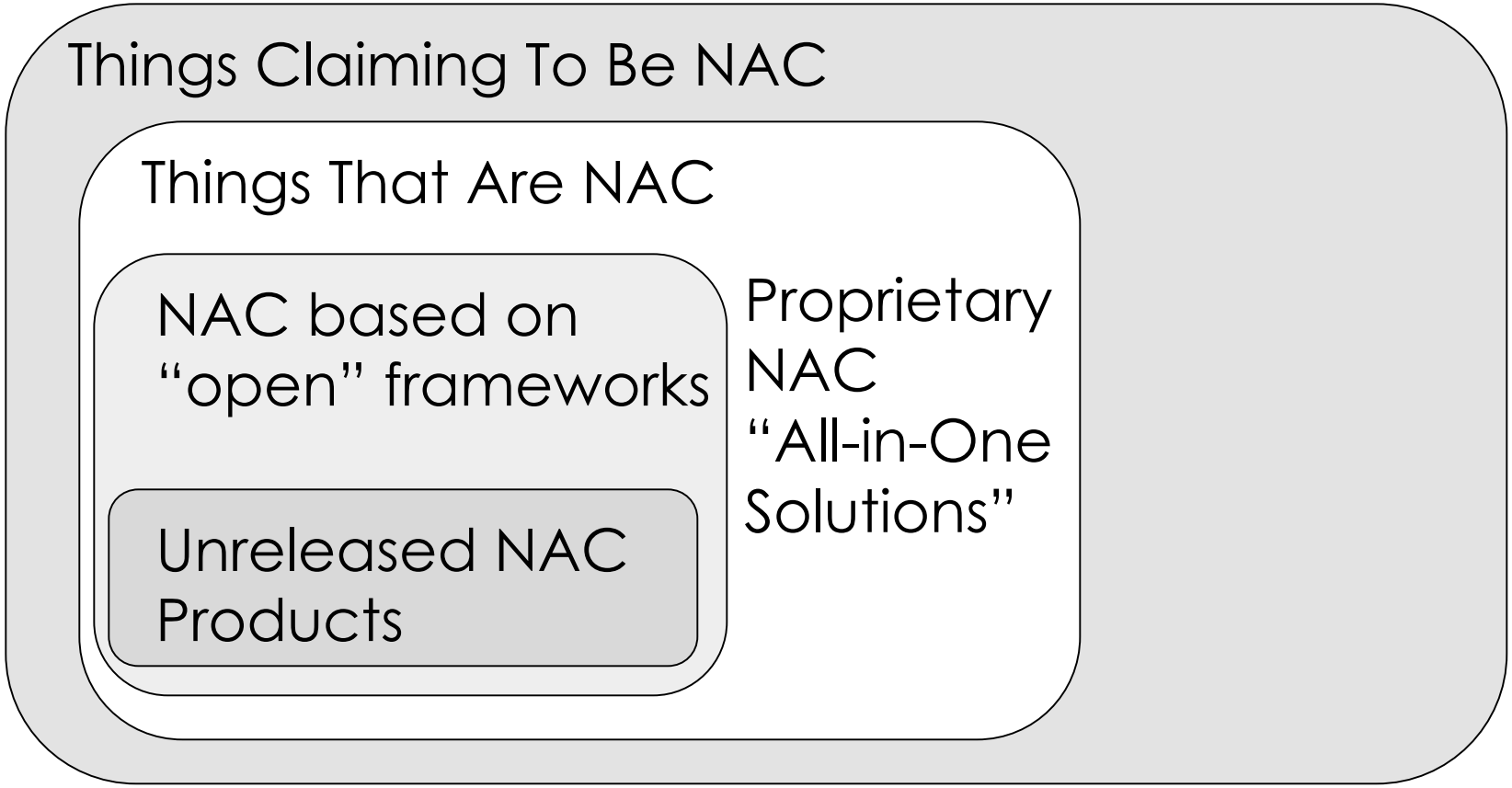
Lessons from the Lab: NAC Framework Testing

Joel M Snyder
Opus One
jms@opus1.com



http://www.opus1.com/www/presentations/nac-testing-interoplv2007.pdf

Context: The World of NAC



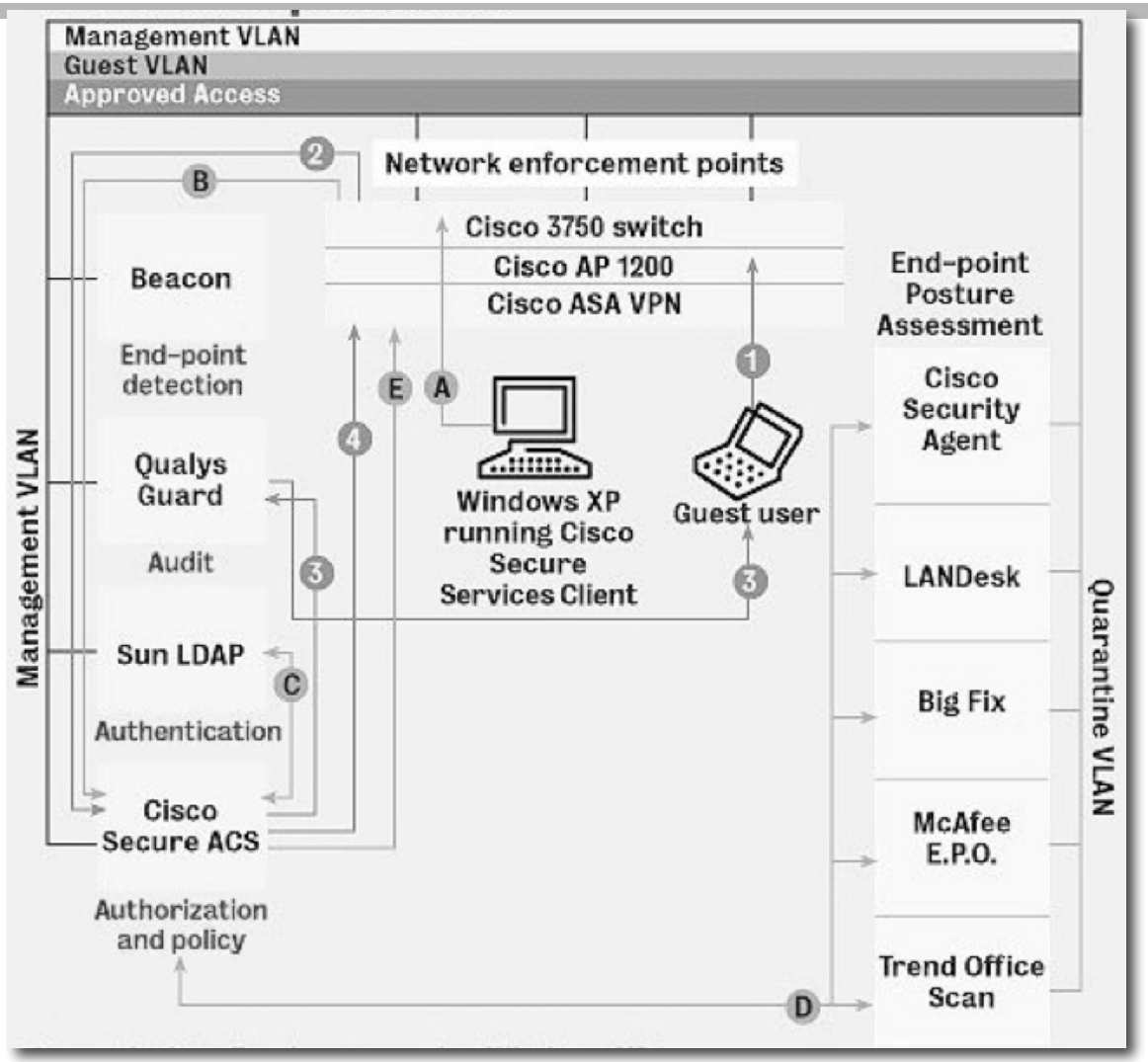
Context: Network World

- April 19, 2007 (first publication date)
- >30 products : 2 frameworks
- `http://www.networkworld.com/reviews/2007/041907-nac-intro.html`

Cisco Secure Access Control Server (ACS) v4.1
Cisco Catalyst 3750 Switch IOS v12.2
Cisco Adaptive Security Appliance ASA5510 V7.2
Cisco VoIP Phone model 7940
Grandstream VoIP Phone model GXP2000 v1.1.1.14
Cisco Aironet 1200 Access Point v12.3(8)
Trend Micro OfficeScan v7.3
Patchlink Update v6.2
LANDesk Systems and Security Management Solutions v8.7
Juniper Unified Access Controller IC-4000 v2.0r1
Juniper NetScreen-5GT v5.4.0
Juniper SSG20 v5.4.0
Vernier Networks EdgeWall 8800 v6
Vernier Networks Control Server CS8000 v6
HP ProCurve Switch 5406zl
Extreme Networks Summit X450a
Enterasys Networks Matrix C2 switch
BigFix Enterprise Suite v6
Qualys Qualysguard Scanner Appliance
McAfee ePolicy Orchestrator
Symantec AntiVirus
Great Bay Software Beacon Appliance v2.1.5
Q1 Labs QRadar v6.0
Cisco Security Agent v5.1
Aruba Networks Aruba 800 Mobility Controller (and access points)
Clients: Nokia E61 Smartphone R3, Palm TX Handheld, IBM/Lenovo Thinkpad X60s, Dell D600 Laptop

NETWORKWORLD

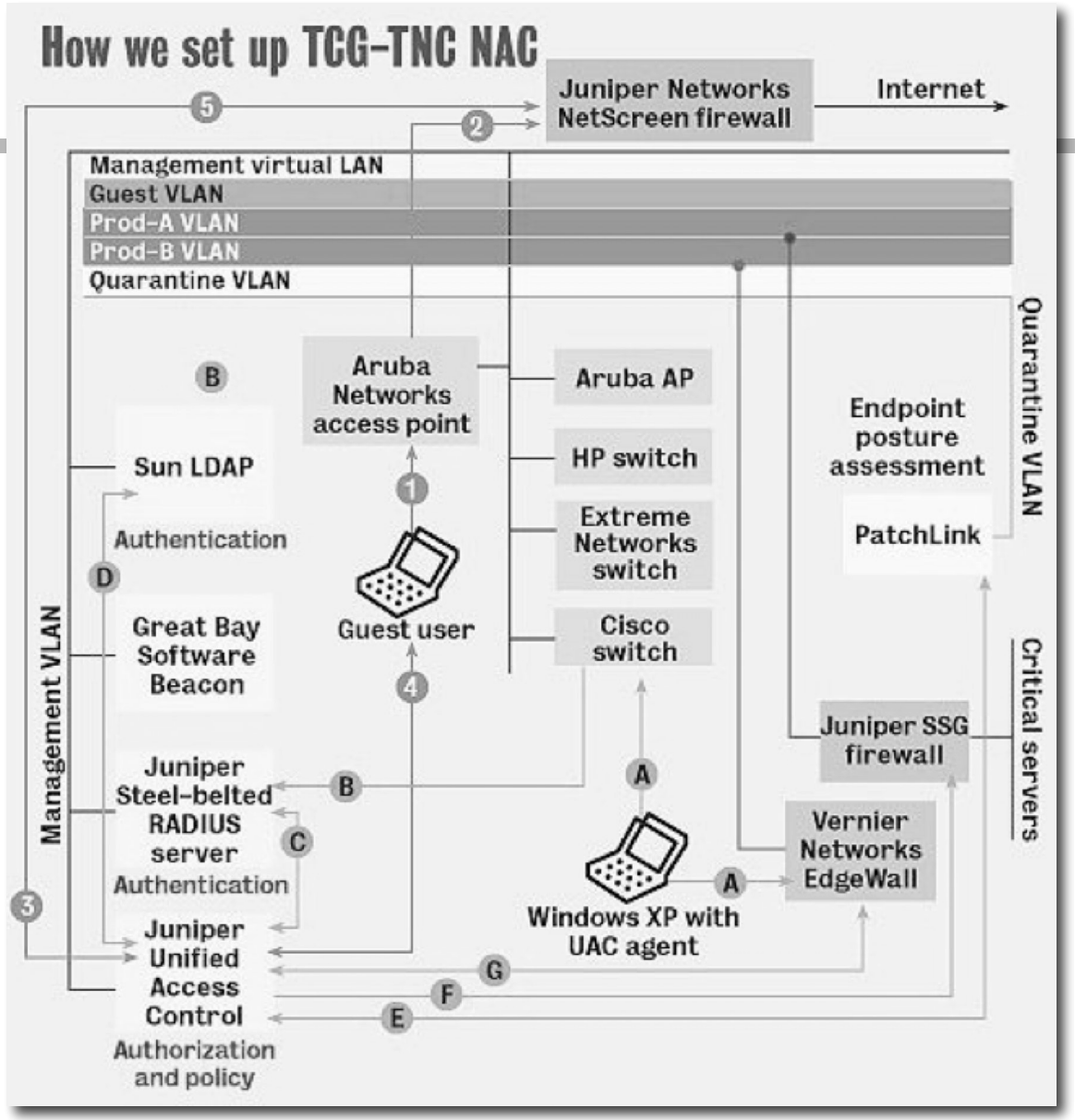
Cisco CNAC Topology Overview



Not all devices and configuration are shown, but you get the general idea

(Numbers & Letters represent different scenarios)

TCG/TNC Topology Overview



Not all devices and configuration are shown, but you get the general idea

(Numbers & Letters represent different scenarios)

So, How Do You Evaluate NAC?

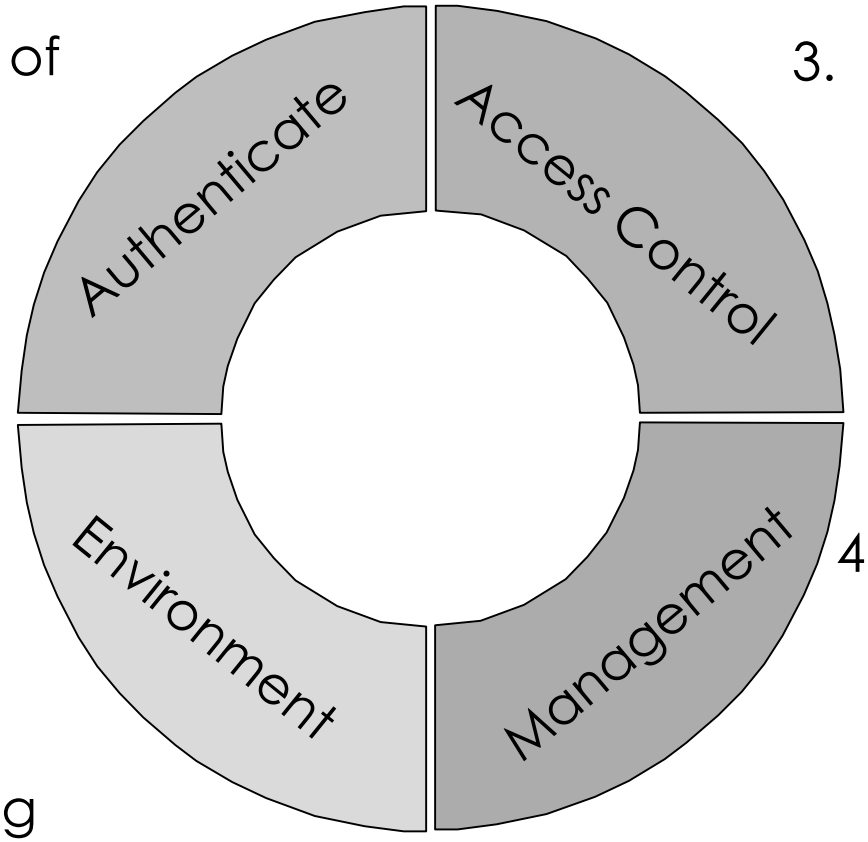
- Answer: You look at the requirements for NAC
- Answer: You evaluate frameworks the same way as All-in-One products…
  - Except it's a lot harder

OK, so what are the requirements for NAC?

Network Access Control has four components

1. Authentication of the user

2. Use environmental information as part of policy decision making

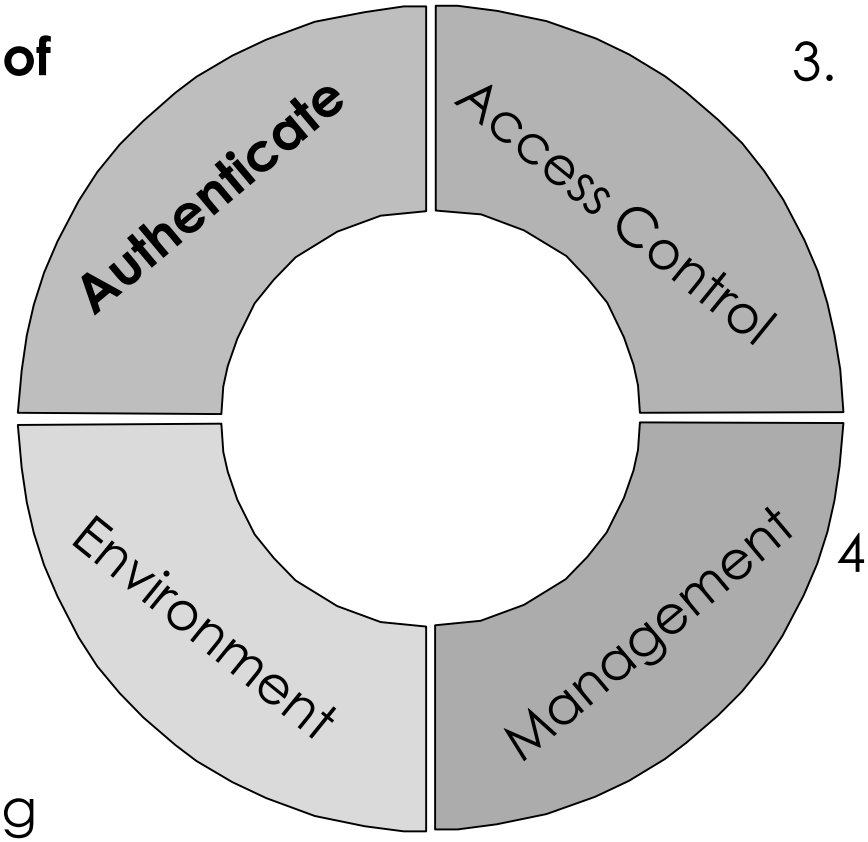


3. Control usage based on capabilities of hardware and security policy

4. Manage it all

What Did We Learn About Authentication?

1. **Authentication of the user**



3. Control usage based on capabilities of hardware and security policy

2. Use environmental information as part of policy decision making

4. Manage it all

Authentication Lesson #1:

Mainstream in Great Shape

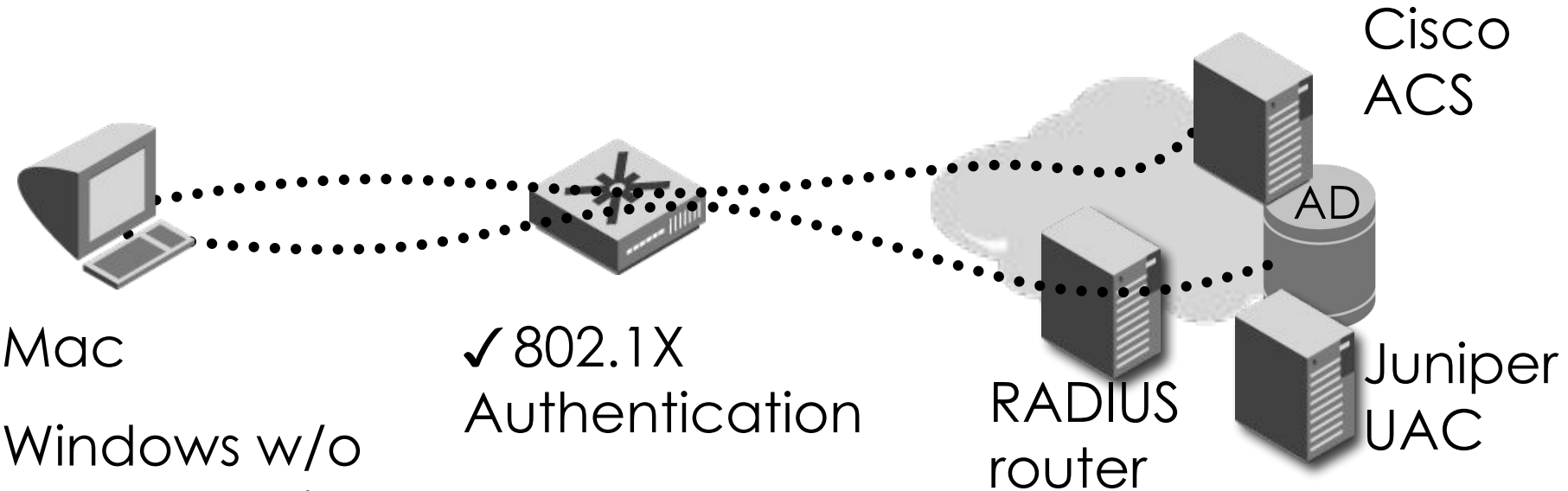
- ✓ Windows XP
- ✓ Windows 2000
- ✗ Windows Vista

- ✓ 802.1X Authentication
- ✓ Vendor-supplied Client

- ✓ Juniper UAC & Cisco ACS using AD via LDAP

Authentication Lesson #2:

802.1X-only, Cisco is Easier



✓ Mac

✓ Windows w/o vendor-supplied client

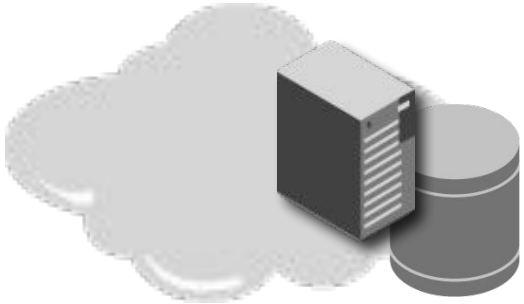
✓ Vista

✓ 802.1X Authentication

Authentication Lesson #3:

Sometimes, it's not framework: It's all about the switch/AP

These guys don't have NAC or 802.1X clients…



…so switches and APs have to deal with it

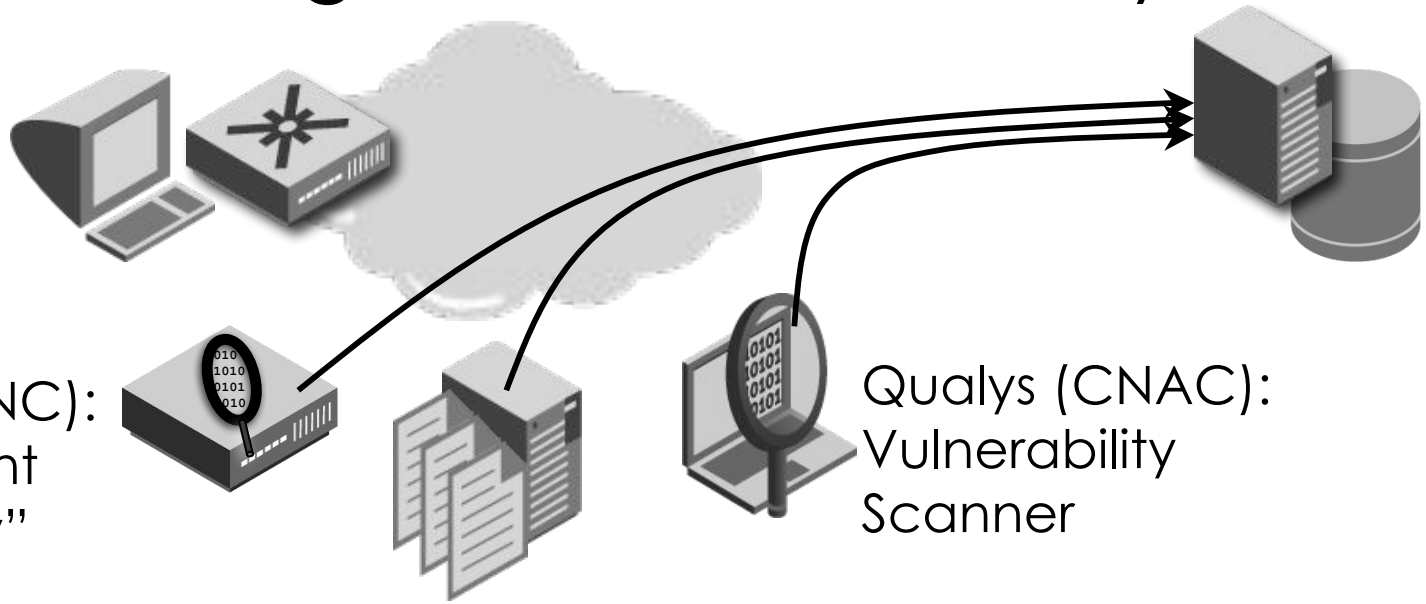
Option A: MAC authentication bypass

Option B: Guest Captive Portal

Authentication Lesson #4:

"Trust But Verify"

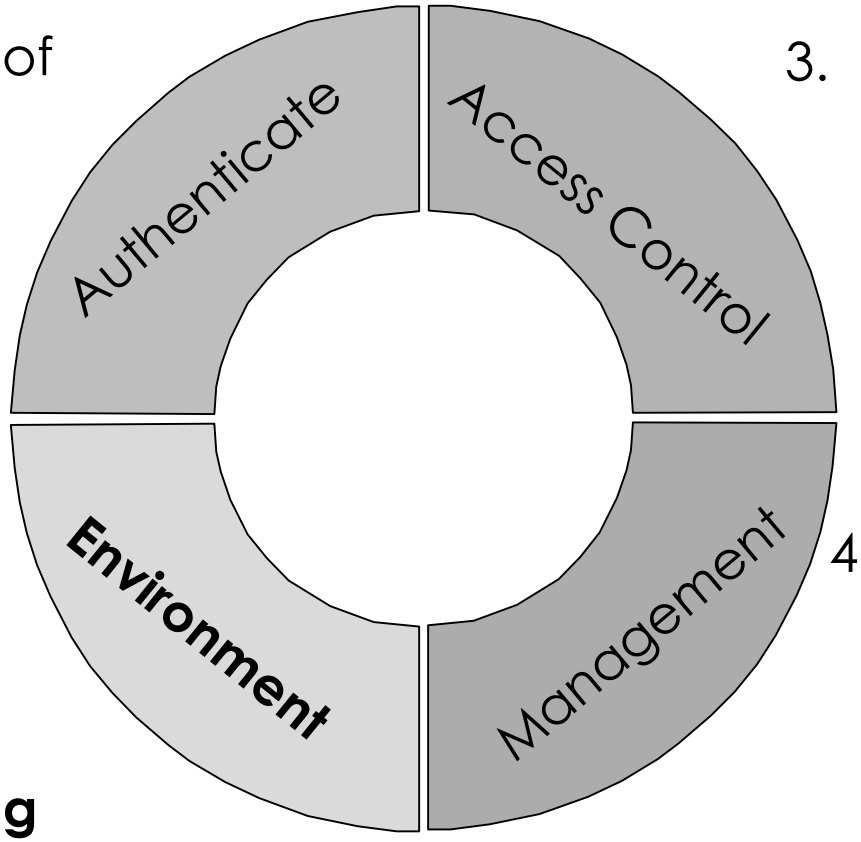
It worked for Reagan; it can work for you



But: Integration at this stage was weak

What did we learn about environment?

1. Authentication of the user



3. Control usage based on capabilities of hardware and security policy

2. **Use environmental information as part of policy decision making**

4. Manage it all

Environment Lesson #1:

The Big Boys Work Fine

- BigFix (CNAC) and PatchLink (TNC) do what they say they do

- We were able to mesh remediation strategy and NAC framework easily

But: Using the "built-in" validator for each NAC framework gave us a weaker solution. Don't be tempted.

Environment Lesson #2:

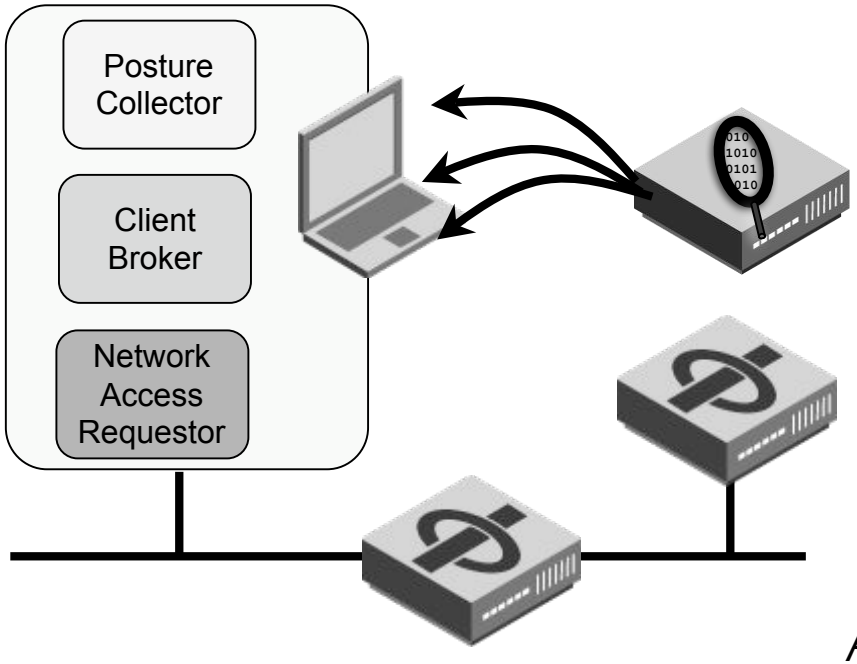
Cisco Has A Lot Of Muscle

- Cisco has attracted more partners to the CNAC framework
- However, it's w*aaaa*y better to link your NAC to patch management than simply check for A/V software

Environment Lesson #3:

Guest Users Are Hard

- Only liars and idiots say they can determine the posture of guest users
  - Pushing software at users doesn't work



External scanning of the end point can help detect device configuration

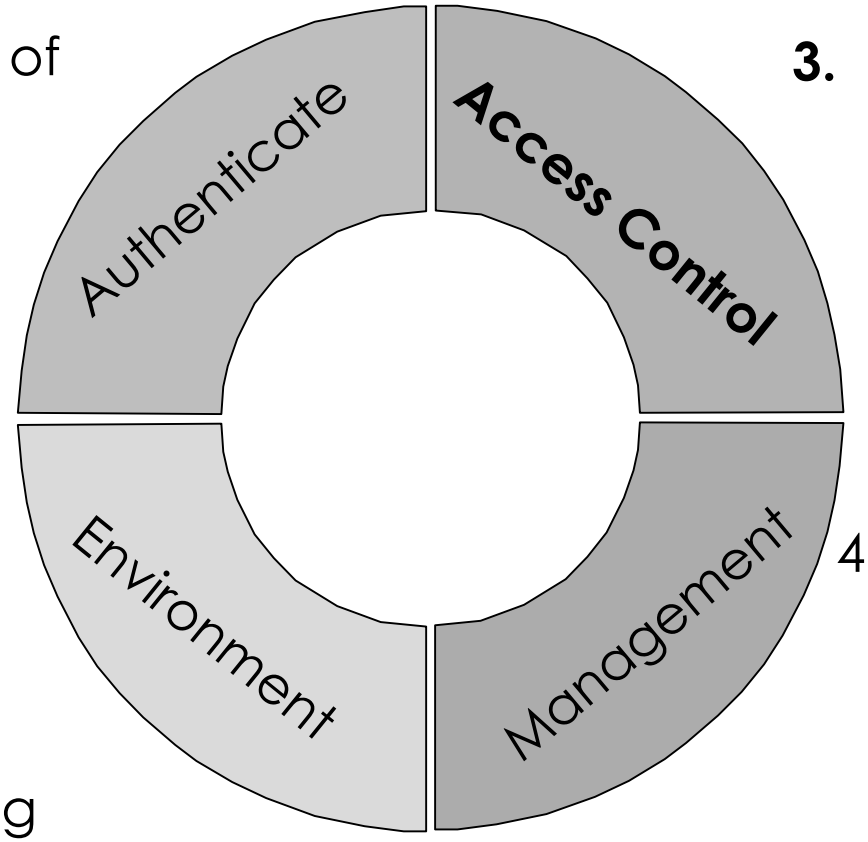
You should use IPS to protect yourself
You should use IDS to detect bad behavior

A necessary layer within the framework!

What did we learn about Access Control?

1. Authentication of the user

2. Use environmental information as part of policy decision making



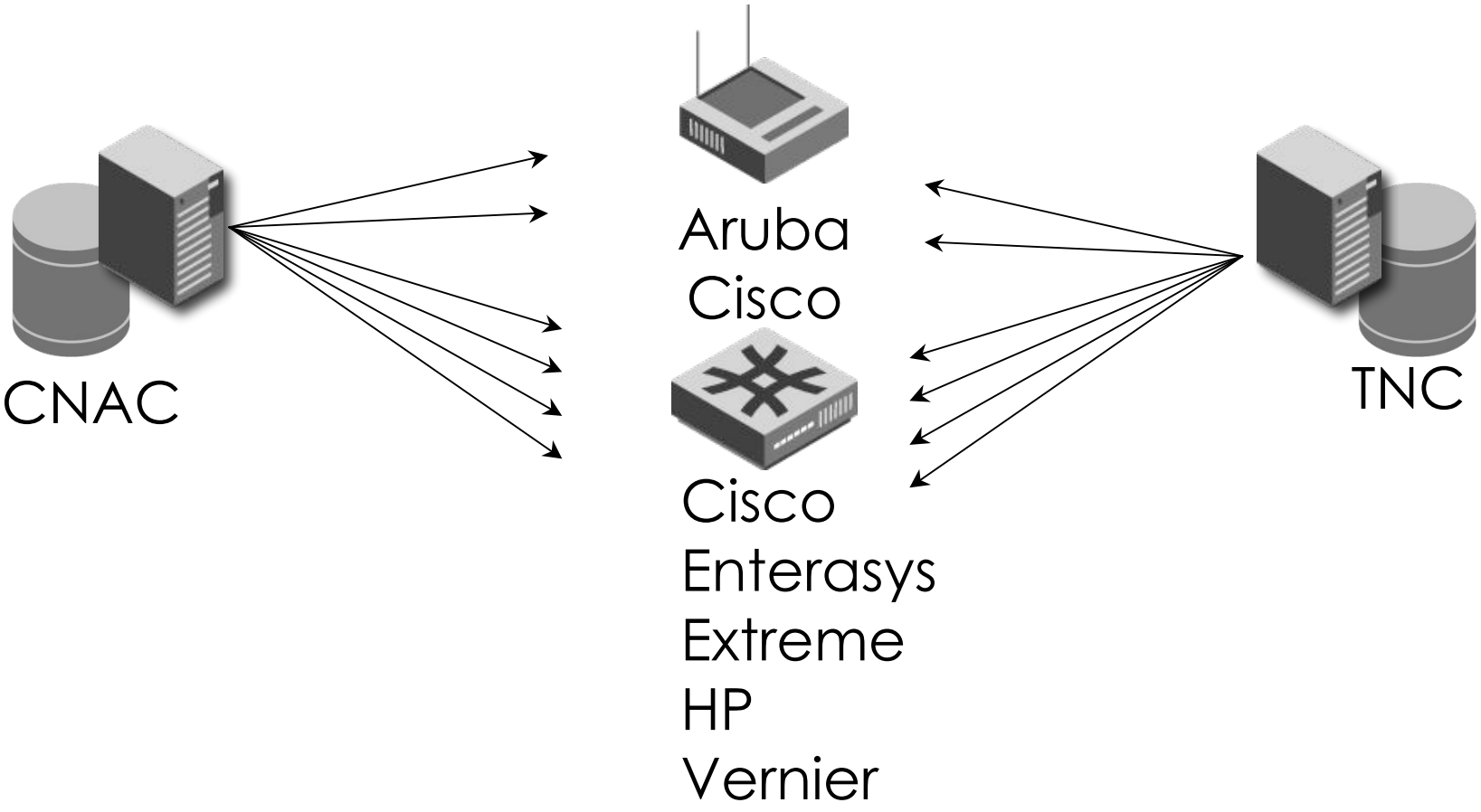
3. **Control usage based on capabilities of hardware and security policy**

4. Manage it all

Enforcement Lesson #1:

VLANs aren't hard

- RFC3580 VLAN assigment works



Enforcement Lesson #2:

Everything Else is Hard

- Cisco ACS policy definition is miserably bad
- Juniper UAC policy definition is very good
  - But it doesn't talk to anyone but their firewalls
  - We only used 10% of our Vernier box

Enforcement Lesson #3:

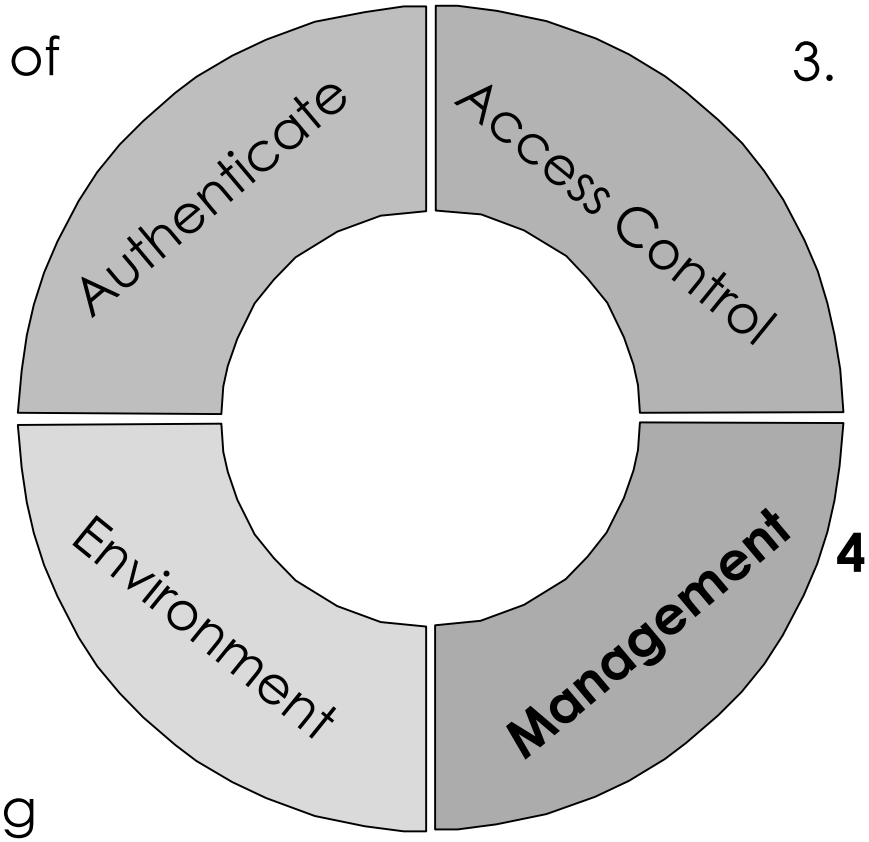
Flexible Cisco = No Auth.

- Cisco has this wonderfully wide range of enforcement options
- Everything but the 802.1X option loses authentication

What did we learn about Management?

1. Authentication of the user

2. Use environmental information as part of policy decision making



3. Control usage based on capabilities of hardware and security policy

4. **Manage it all**

Management Lesson #1:

Drawing a Line is Important

- Both CNAC and TNC draw a clear line in the sand between Network/Security and Desktop
- CNAC has way more options
- But CNAC requires ACS, which is … suboptimal as a NAC policy engine

Management Lesson #2:

Defining Policy is Important

- Cisco ACS (CNAC) doesn't define policy; it sends down RADIUS options
- Juniper UAC (TNC) does define policy

- Both of these are implementation issues, and are not really specific to the framework

Conclusions?

- Frameworks are a great way to build NAC deployments
- TNC needs more partners (but Monday's news should change that)
- Cisco needs to replace ACS with something else
  - Or simply join the New World Order of NAC and let other people be good at other things

Lessons from the Lab: NAC Framework Testing

Joel M Snyder
Opus One
jms@opus1.com