Network Access Control: Hard Questions

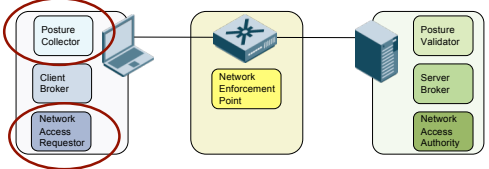
Joel M Snyder
Senior Partner
Opus One
jms@opus1.com

Agenda: Hard Questions about NAC

- **Questions you need to be able to answer about NAC regarding...**
  - **Lying clients**
  - **Denial of Service, MITM, and Eavesdropping Attacks**
  - **VPN, Branch, Remote Access, and Wireless**
  - **Interdependencies**
  - **Integrating NAC with other tools**
  - **Value of NAC to the organization**

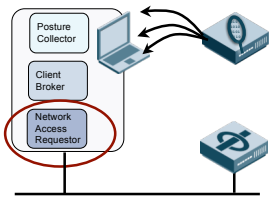
1. How will NAC deal with lying clients?

The NAC policy server gets its information from software running on the client



The Enforcement Point gets address information from software running on the client

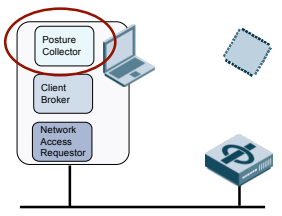
Most NAC deployments will have to use MAC authentication for some devices



You can use scanning of the end point to help confirm the type of device

You can use behavior analysis to detect when the device is behaving "uncharacteristically"

Posture assessment relies on the client to report the results



TCG/TNC has the TPM strategy to maximize "software trust"

Behavioral analysis also works here

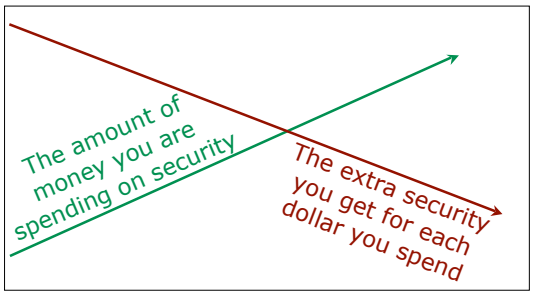
A sub-question: do you care about compliance, or infection?

Software on the PC can tell you whether the system complies with policy, but says nothing about whether the system is infected

External sensors can't tell you about policy compliance, but they are very good at detecting infections

(more about this later)

Beware trying to have perfect security unless you have infinite budget



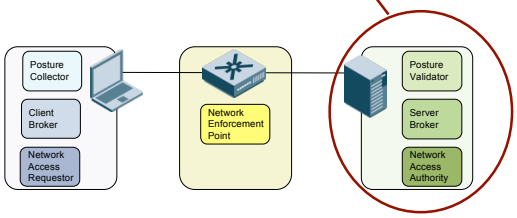
Action Items: Lying Clients

- **Seek out NAC solutions that can incorporate external scanning solutions and IDS/IPS data**
- **Identify holes in network security caused by MAC authentication, and document how you are plugging them**
- **Balance the cost of end-point security assessment with the benefits that it brings to the network**

2.

Are you ready to add another "P1" critical service?

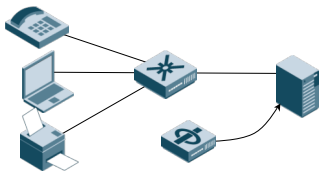
This Policy Decision Point is now critical to anyone connecting to the network



Policy servers need to be scalable

User thinks that they log in once per day
1000 users = .03 decision/second

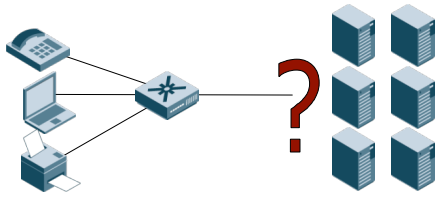
MAC devices are re-authenticated every minute
1000 users = 30 decision/second



End-point security checks in every 15 minutes
1000 users = 1 decision/second

IDS+SIM+scanner generate 10 events a second
events = 10 decision/second

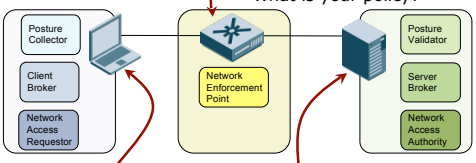
Policy servers need high availability



Can you build an active/active cluster?
Are your decision points able to handle multiple locations?
Is the link to the backend database, such as Active Directory LDAP, properly provisioned for HA?

Challenges to Reliability Require Broad Thinking

Can Enforcement Points survive loss of policy engine gracefully? What is your policy?



What happens if a misbehaving client thrashes the network with hundreds or thousands of authentications a second? Or spins its MAC address many times a second?

How will the policy engine behave while under a DoS attack?

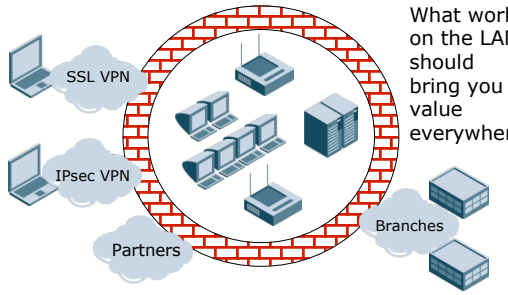
Action Items: Critical Services

- **Select NAC policy engine solutions that have:**
  - **Scalability, because you can't predict how many decisions/second you need**
  - **High availability, because the network can't stop working**
- **Review policy on enforcement points when contact is lost with the policy decision point**
- **Ensure that the link between enforcement point, policy decision point, and backend authentication database, cleanly survives failures and "scale up" events**

3.

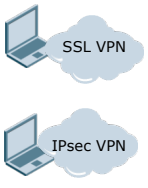
How will NAC extend to remote access, branch, and wireless environments?

NAC defines access controls based on identity and end-point posture



What works on the LAN should bring you value everywhere

SSL VPNs did NAC before NAC was even a buzzword



- **SSL VPN vendors are ideally situated to be part of your NAC solution**
- **No SSL VPN vendor has yet integrated their policy engine with the NAC engine**
- **Obviously, you want to have fewer engines and fewer bits of software floating around**

IPsec VPNs will either have proprietary or IKE v2-based solutions

Proprietary is easy if your NAC vendor is your IPsec vendor…

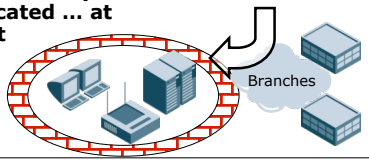
… and of course you can use L3 enforcement

The most interesting future solutions build on EAP being used in 802.1X (most current NAC solutions) and in IPsec when IKE v2 is finally available

Branch Offices need NAC even more than HQ, but have challenges

- **VLANs can't easily be propagated to branches, and may have different meanings**
- **Remediation services and policy engines may have to be replicated … at higher cost**

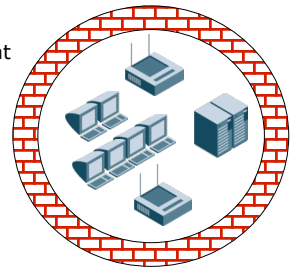
Consider pushing NAC "brains" towards HQ or using L3 enforcement



Wireless almost always implies guest access of some sort

802.1X is a great strategy for LAN and WLAN…

but guests will want captive portal



Action Items: Branch, VPN, Wireless

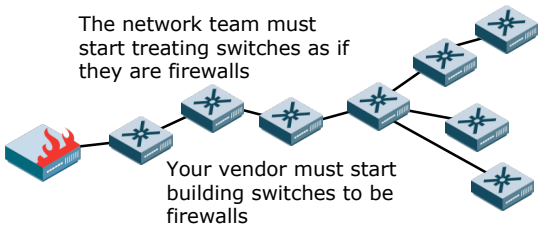
- **Aim to reduce number of policy engines and posture checkers you need to manage; look forward to extend NAC capabilities outside of the LAN and WLAN environments**
- **Consider different strategies for enforcement at branches (while preserving same policy engine)**
- **Make sure your IPsec and SSL VPN solution vendors are "on board" with your NAC strategy**

4.

How much does NAC depend on the security of your infrastructure?

When you push security into the network, the network must be secure

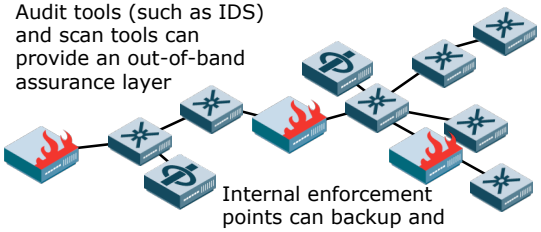
The network team must start treating switches as if they are firewalls



Your vendor must start building switches to be firewalls

Many NAC solutions can help work around infrastructure

Audit tools (such as IDS) and scan tools can provide an out-of-band assurance layer



Internal enforcement points can backup and extend switch enforcement

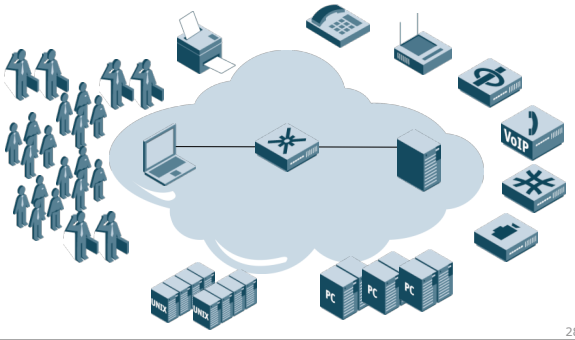
Action Items: Infrastructure Security

- **Bring together the network operations team and NAC teams to resolve "infrastructure" issues early**
  - **Password management**
  - **Bug fixes and software version updating**
  - **Change control and access rights**
- **Deliver the key message: Every switch is a firewall**
- **Evaluate whether your infrastructure is ready to transition from "connection utility" to "enforcement point"**

5.

How well does NAC interact with the world around it?

"No NAC is an Island"



You need to consider NAC's interaction with the rest of the world

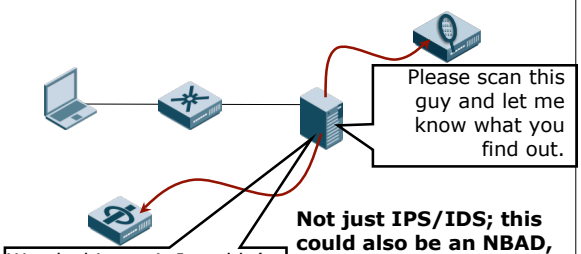
Layers 8, 9, and 10

- **The all-important religious, political, and economic layers of the OSI model**
- **(see next hard question)**

Layers 3 through 7

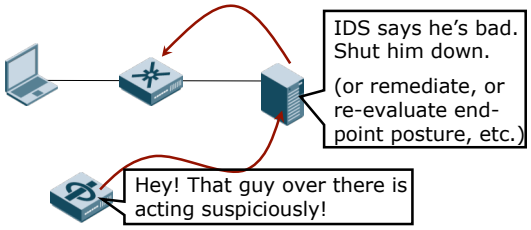
- **NAC is already linked to end-point security tools**
- **What about data sources such as IDS and IPS events?**
- **What about data streams from SIMs?**

NAC can talk to IPS



Not just IPS/IDS; this could also be an NBAD, SIM, or vulnerability analyzer, or other device with relevant knowledge

IPS (and IDS) could talk to NAC

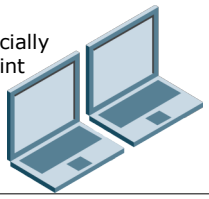


Subtle Problem: "Change of Authorization" is not within existing protocols, so this is a work in progress for open frameworks

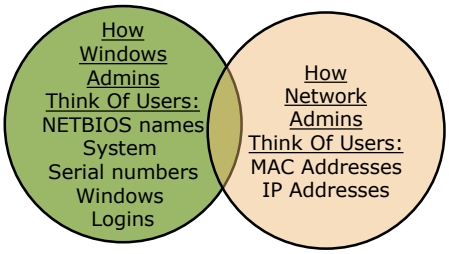
NAC integration with external devices is an evolving story

Howard's Observation: "NAC is the bouncer at the door. We need more bouncers inside of the bar."

This integration is especially critical to you if end-point security is one of your driving factors for NAC.



Other complexities will confound the process



Action Items: NAC Communications

- **Identify your "security sensors" such as IDS, IPS, SIM, Vulnerability Analyzers, and even NetFlow data.**
  - **This will probably overlap in some ways with the information provided by end-point management tools (Patchlink, BigFix, Altiris, *etc.*)**
- **Determine where NAC can make use of this data and how well your vendor supports it**
- **Look at how NAC can make your network security tools "smarter" by sharing information about network users**

6.

How does NAC change how everyone thinks about the network?

NAC Fundamentally Changes the Way You Think About the Network

Before:
Switching Infrastructure

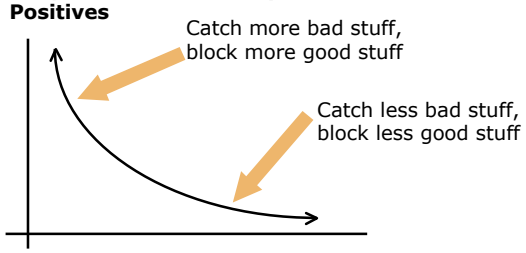
- **You plug things in, and they work**

After:
Policy Enforcement Infrastructure

- **You plug things in, and maybe they work**

Dealing with a fundamental change requires layer 8, 9, and 10 support

- **Simple Fact: All Security Creates False Positives**



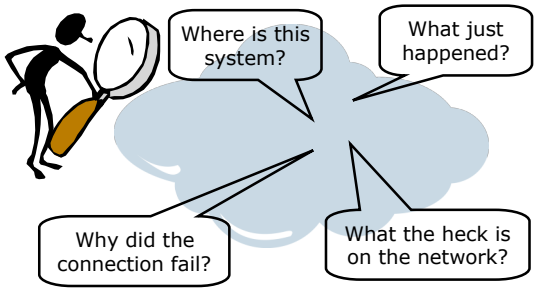
Keep In Mind The Guiding Principle of NAC

The Goal of NAC Is to Allow Devices to Connect to the Network.

(Not to Keep Devices off of the Network)

J-P's Principle of NACology:
Forewarned is Forearmed

Visibility gives you the best opportunity to avoid problems



Gaining visibility is good network discipline anyway

Network Management Tools with Discovery: IPMonitor, What'sUp

Vulnerability Scanners and Mappers: Nessus, nmap, Sourcefire RNA, Tenable PVS

3rd Party NAC Add-ons for Inventory: Great Bay, ID Engines

IDS using Signatures and NBAD techniques: Mazu, Lancope, & the usual suspects

Action Items: Change in Thinking

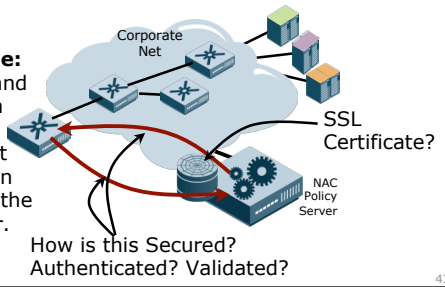
- **Socialize the changes that NAC will bring before you run into problems and before they start affecting network usage**
- **Become "forearmed" by making use of existing tools for network discovery and visibility as part of your NAC plans**
- **Where appropriate, add new visibility tools to your network to support NAC help desk as well as audit and trust-but-verify functions**

7.

How will you resolve NAC susceptibility to security attacks?

All Security Systems Have Vulnerabilities You Must Understand

For Example: An out-of-band NAC solution requires management links between devices and the policy server.



Complex and Cross-Platform Solutions Need Extra Care

Areas of Concern	Potential Issues
Command-Line Management Links	**CLI passwords; clear-text management; credential management; change control**
SNMP Tools	**Lack of SNMP authentication in devices; clear-text passwords; UDP lossage; change control**
Client APIs	**Registration and impersonation vulnerabilities**
SSL; RADIUS	**Certificates and Trusted Roots; Protection of private keys; Renewals**
Data Feeds	**Impersonation; Loss; Privacy of Information**

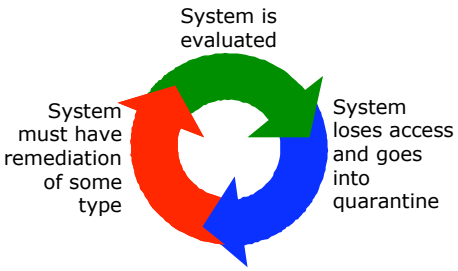
Action Items: Security Vulnerabilities

- **Work with your vendor to identify areas of "linkage" between components where you need to be concerned**
- **Identify specific training issues for end-users related to potential vulnerabilities (such as SSL certificates)**
- **Get outside help to review security vulnerabilities and identify areas for increased vigilance**

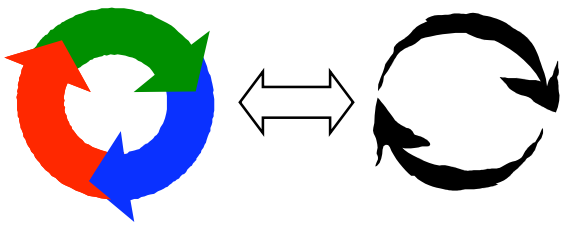
8.

How will NAC's lifecycle and your Organization's lifecycles mesh?

End-Point Security Assessment isn't a "yes/no" answer



NAC end-point strategy must match the organization's strategy



. Detect . Remediate . Quarantine . Allow .

Key Advice: Know When To Throw the Ball to the Other Team

- The Organization must have infrastructure in place before you can even start down the NAC path.
- Take a lifecycle view of end-points.
- Don't fixate on just one aspect of the cycle (such as evaluation)

Integration of Network Team and Desktop Team is Required ... and Hard

Action Items: Lifecycle

- Have your end-system lifecycle already implemented and running before you add NAC to the picture
- Ensure that your NAC solution will fully support the lifecycle the desktop team has endorsed
- Build management bridges carefully to keep desktop and network people out of each other's hair

9. What value does NAC bring to the Organization?

This one, you're going to have to answer for yourself

- But here are some things people have said they used to build ROI case for NAC
  - → Reduced help-desk calls (after initial spike)
  - → Reduced cost of RIAA subpoena answers
  - → Better ability to answer compliance requirements
  - → Reduced cost on Moves/Adds/Changes by making the network more dynamic
  - → Reduced load on "high cost" staff by allowing "lower cost" staff to grant access

Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com

OPUS