Welcome to NAC Day!

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

Today's Agenda

- **9:00 to 9:45** **What is NAC?**
- **10:00 to 11:00** **Deploying NAC**
- **11:15 to 12:15** **Enforcement Options**
- **12:15 to 1:15** **Lunch**
- **1:15 to 2:15** **Extremely Real World NAC**
- **2:30 to 3:10** **Standards-based NAC**
- **3:25 to 4:15** **Hard Questions about NAC**

Network Access Control Part 1: What is NAC?

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

Agenda: Defining NAC

- **Why are we thinking about NAC?**
- **What is a definition of NAC?**
- **What are the four key components of NAC?**
- **What are the industry NAC architectures?**
- **Authentication, Environment, and Enforcement in Depth**

Security Management Is Moving Towards the End User

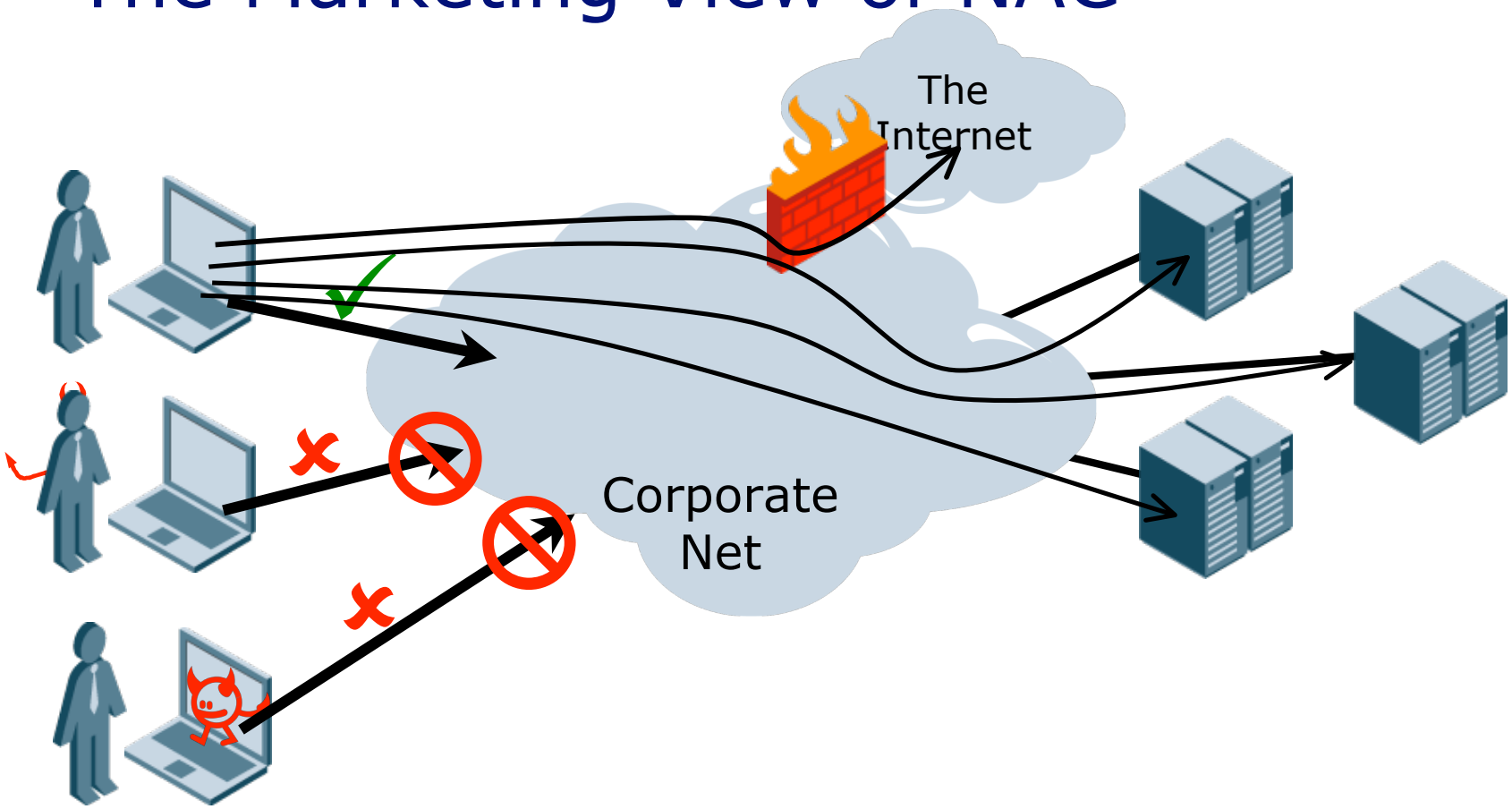
Last Year

- **Poke holes in the firewall for specific IP addresses and specific services**
- **Create IPsec remote access solutions that give broad network access**

Next Year

- **Determine security policy by *who is connecting* not where they are connecting from**
- **Create remote access solutions that *focus on the end-user*, not the network**

The Marketing View of NAC



Let's Define NAC: "Network Access Control"

NAC is | **user-focused,** | **network-based** | **access control** |

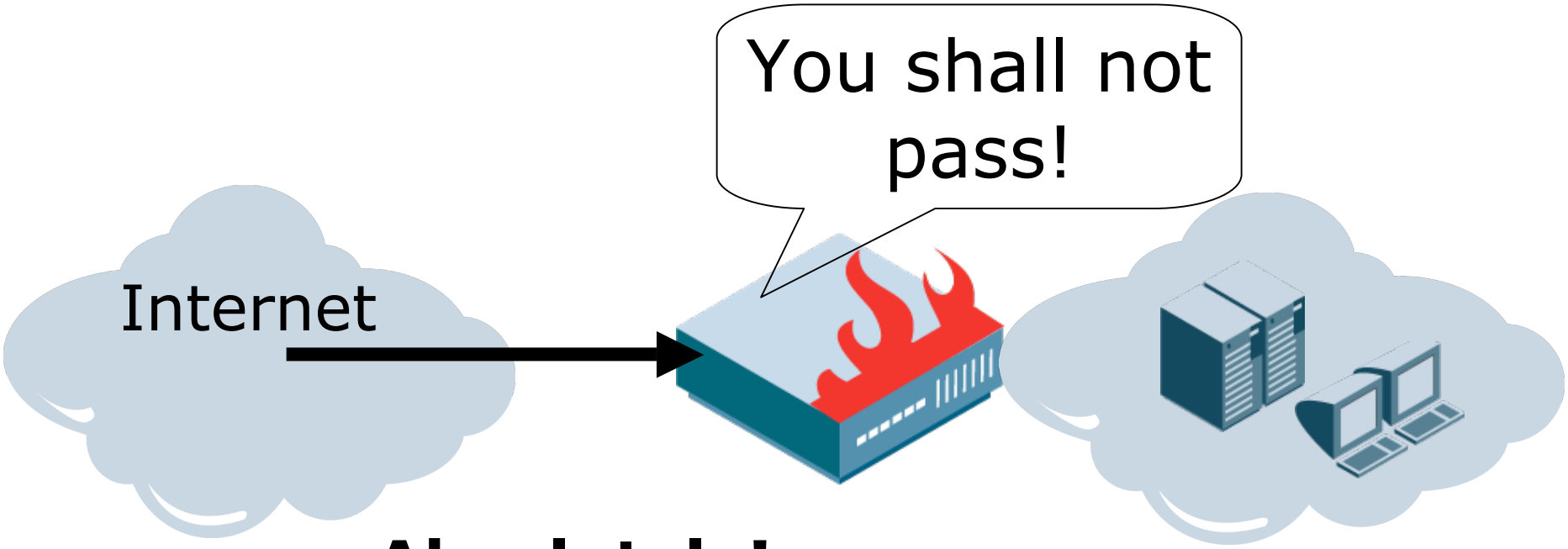
<u>Who you are:</u>
not your IP address, but your authenticated identity.

Also: your end-point security status, location, access type

<u>Something inside of the network:</u>
enforcement occurs in the network, not on the the end points

<u>Control:</u> limit access according to policy, where policy is based on the user

"OK, wait a second. Isn't Access Control what a firewall does?"



Absolutely!

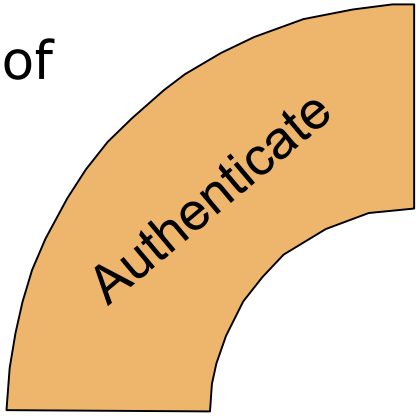
The difference is in the decision!

NAC Is Firewalling, but With a Difference

Common Firewall **Decision Elements**	Common NAC **Decision Elements**
Source IP and port Destination IP and port	Username and Group Access method and location End-point security status Destination IP and port
Position	**Position**
Between two networks	Between user and network

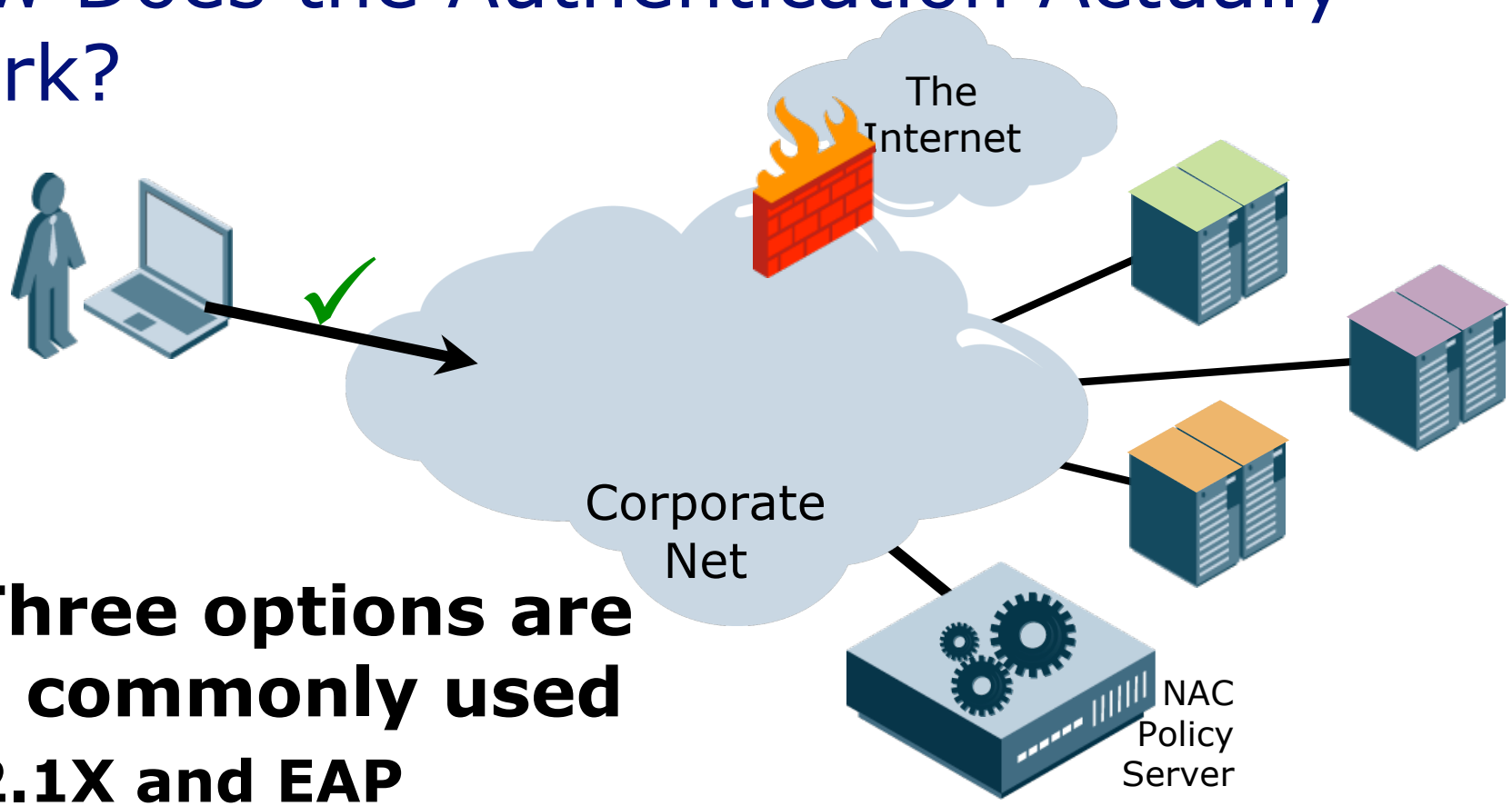
NAC Has Four Components

1. Authentication of the user



End users are authenticated before getting network access

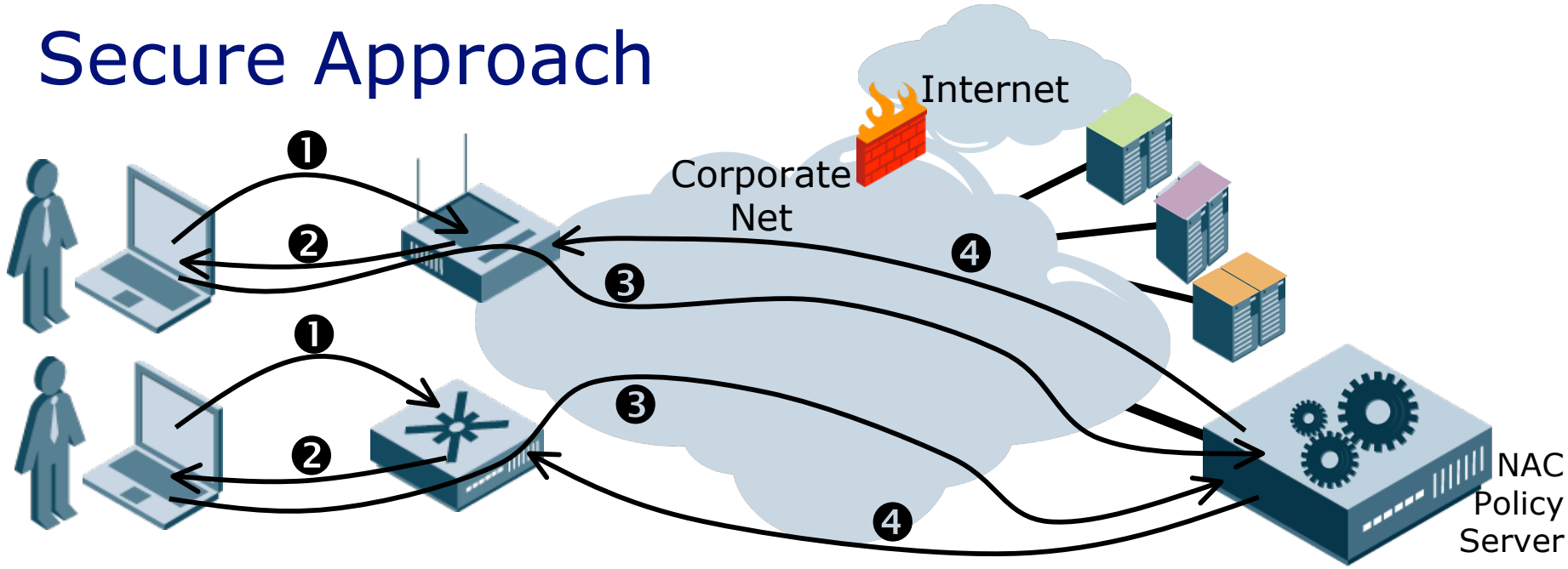
How Does the Authentication Actually Work?



Three options are commonly used

- **802.1X and EAP**
- **Web-based Authentication**
- **Proprietary Client**

802.1X is Preferred and the Most Secure Approach



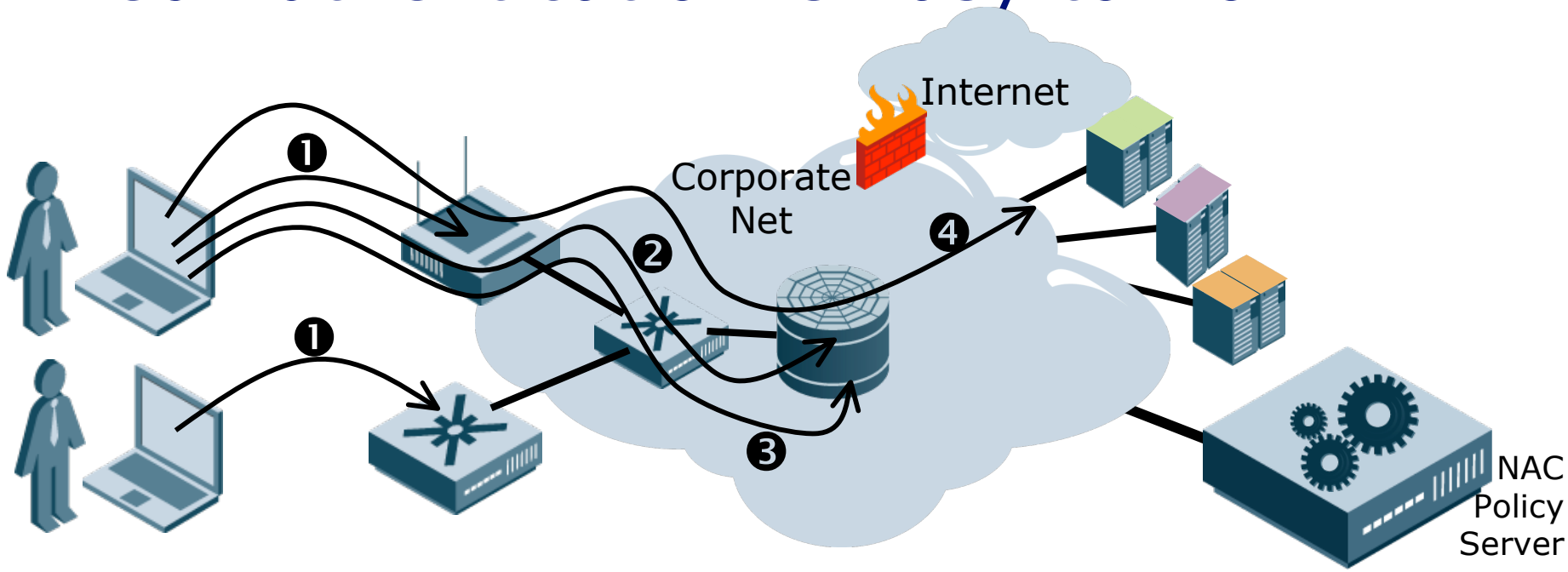
❶ User brings up link (or associates with AP)

❷ AP/Switch starts 802.1X (EAP) for authentication

❸ User authenticates to central policy server

❹ If authentication (and other stuff) is successful, policy server instructs edge device to grant appropriate access. User gets IP address.

Web Authentication is Easy to Do



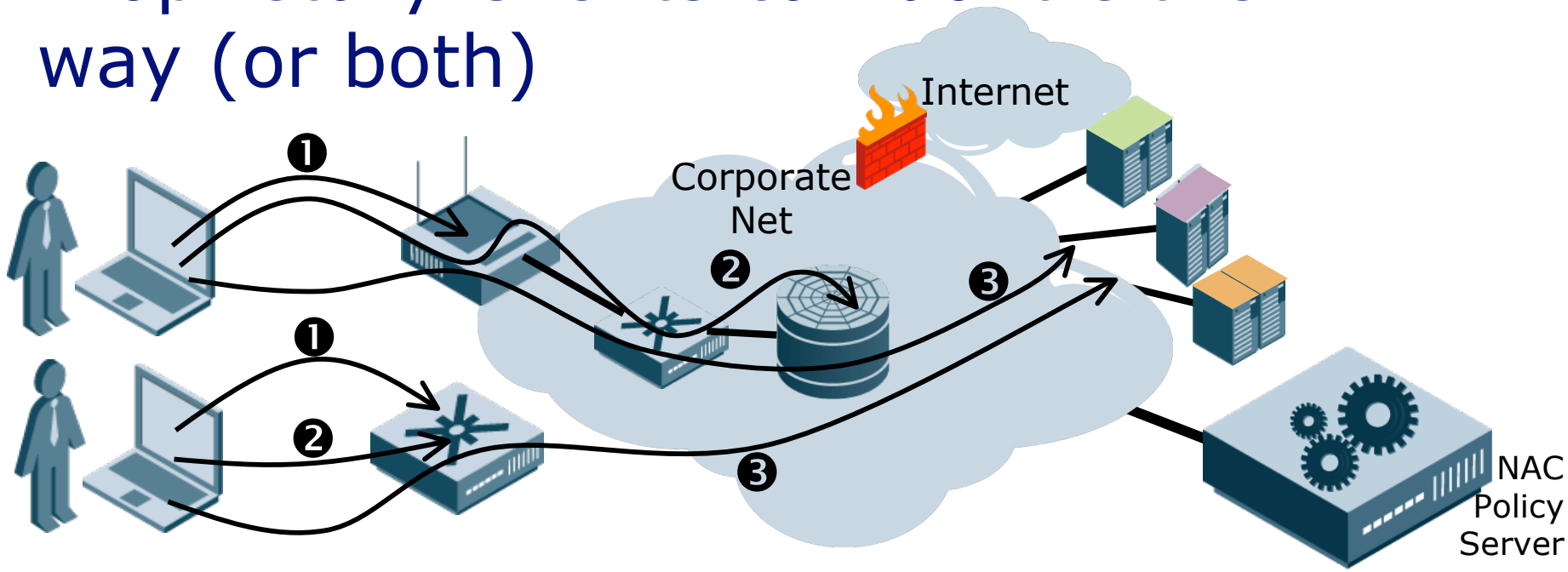
❶ User gets on network; gets IP address

❷ User opens web browser and is trapped by portal

❸ User authenticates to central policy server

❹ If authentication (and other stuff) is successful, portal lets traffic through or reconfigures network to get out of the way

Proprietary Clients can do it either way (or both)



❶ User connects and gets IP address

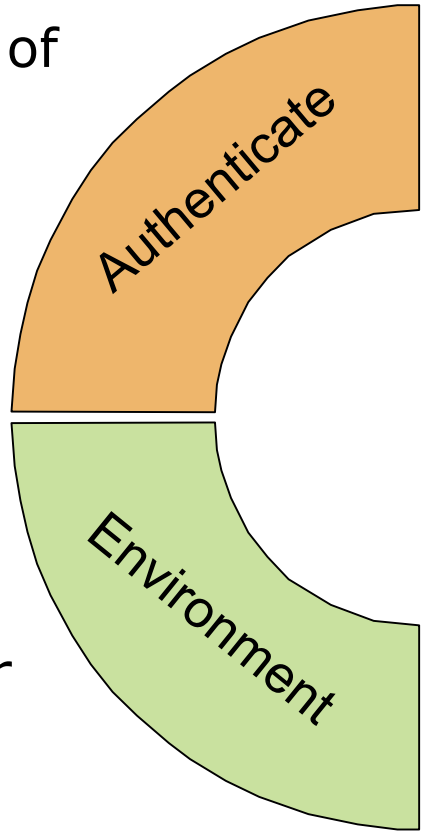
❷ Client magically authenticates to NAC device

❸ If authentication (and other stuff) is successful, user is allowed on network

Environmental Information Modifies Access or Causes Remediation

1. Authentication of the user

2. Use environmental information for continuous policy decision making



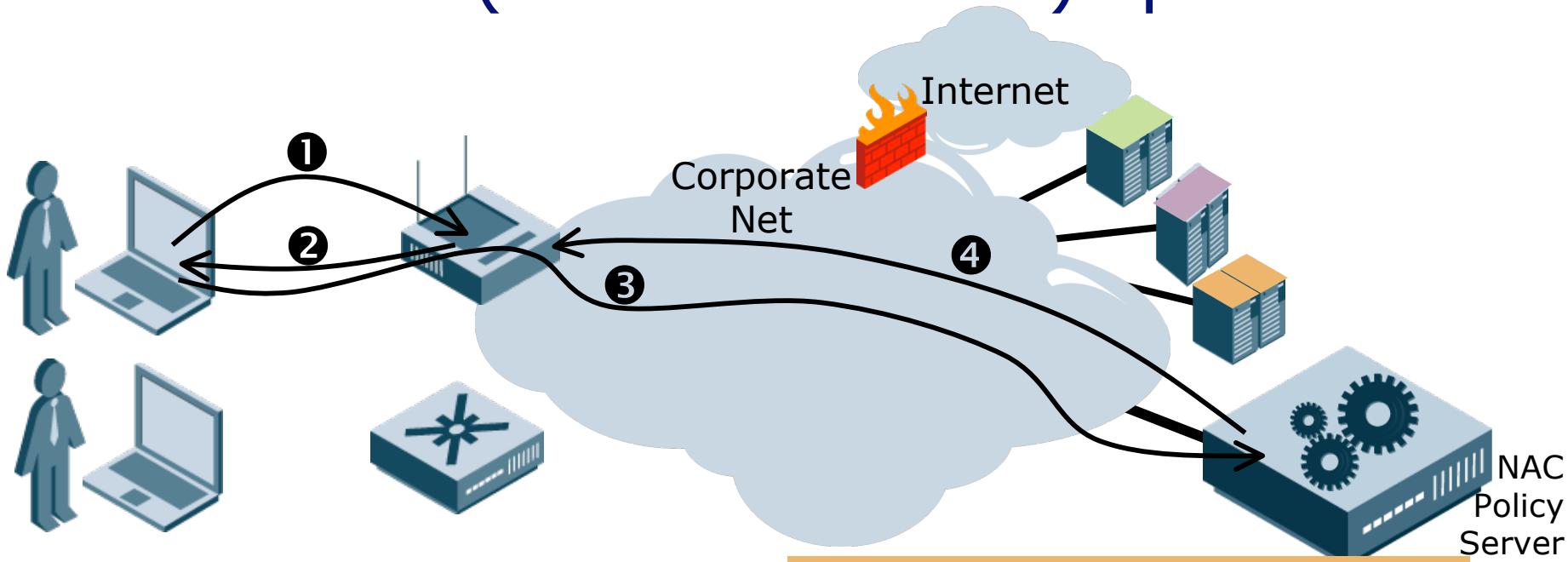
Where is the user coming from ?

When is the access request occurring?

What is the End Point Security posture of the end point? ("Pre-Connect")

What is our IPS/ NBA/SIM telling us about this user ("Post-Connect")?

This is the "(and other stuff)" part



❶ User associates with AP

❷ AP starts authentication

❸ User authenticates

❹ If authentication (and other stuff) is successful, user is given appropriate network access

For some, this is the main reason to want NAC!

Environmental Information Can Include Lots of Things

Pure Environment

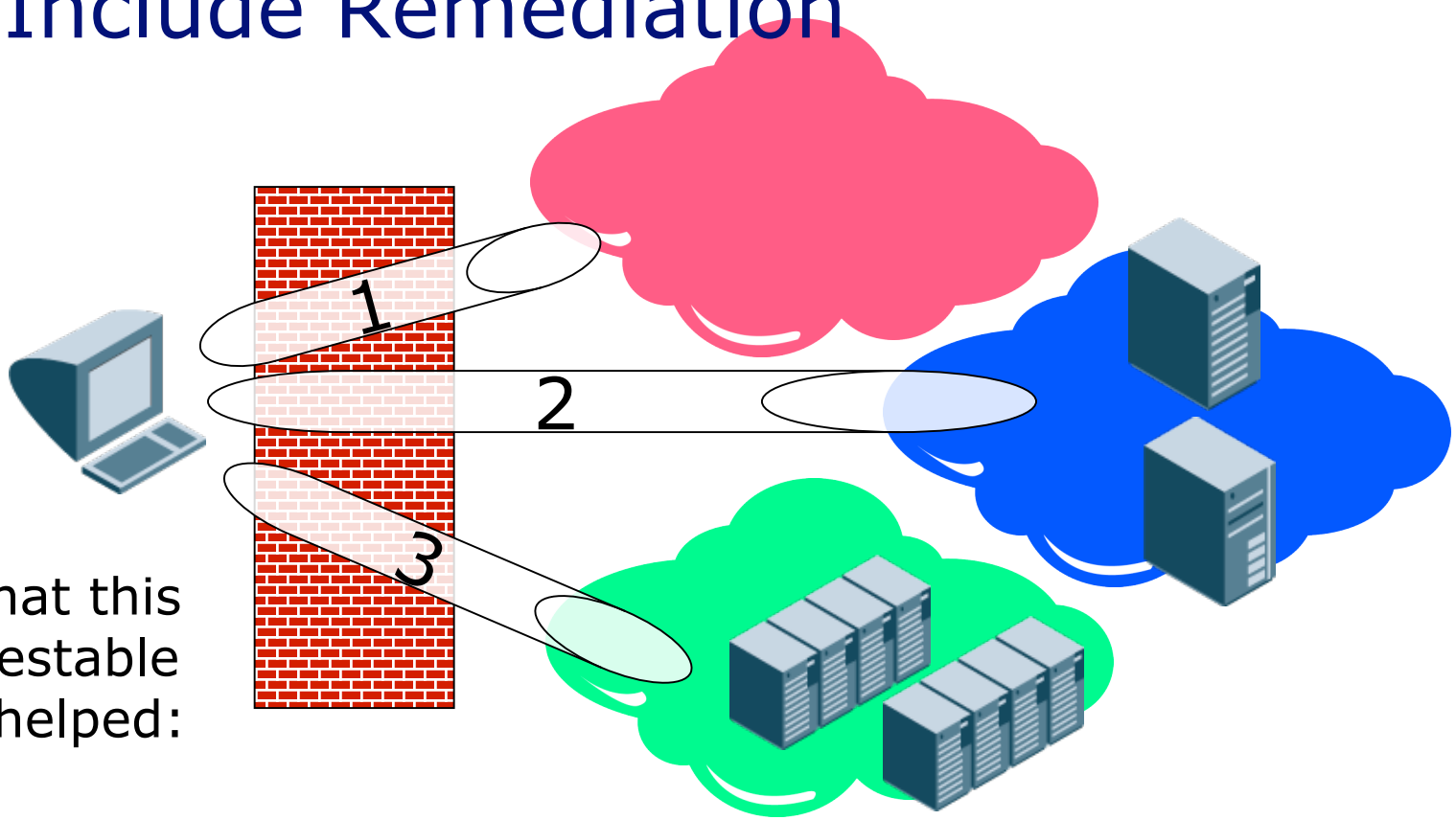
- Access Method (wired, wireless, VPN)
- Time of Day/Day of Week/Date within Limits
- Client Platform (Mac, Windows, *etc*.)
- Authentication Method (user/pass, MAC, *etc*.)
- Trusted Platform Module status

End Point Security

- Does the device comply to my policy regarding
  - **Security Tools (A/V, FW)**
  - **Applications (running/not)**
  - **Patch Level**
  - **Corporate "signature"**

Lots more about this in the next session!

Any End Point Security Test Should Include Remediation



1. EPS says that this system is untestable or cannot be helped: Internet only

2. System is non-compliant, but can be helped: Access to remediation network (or auto-remediate)

3. System complies with security policy: full access granted

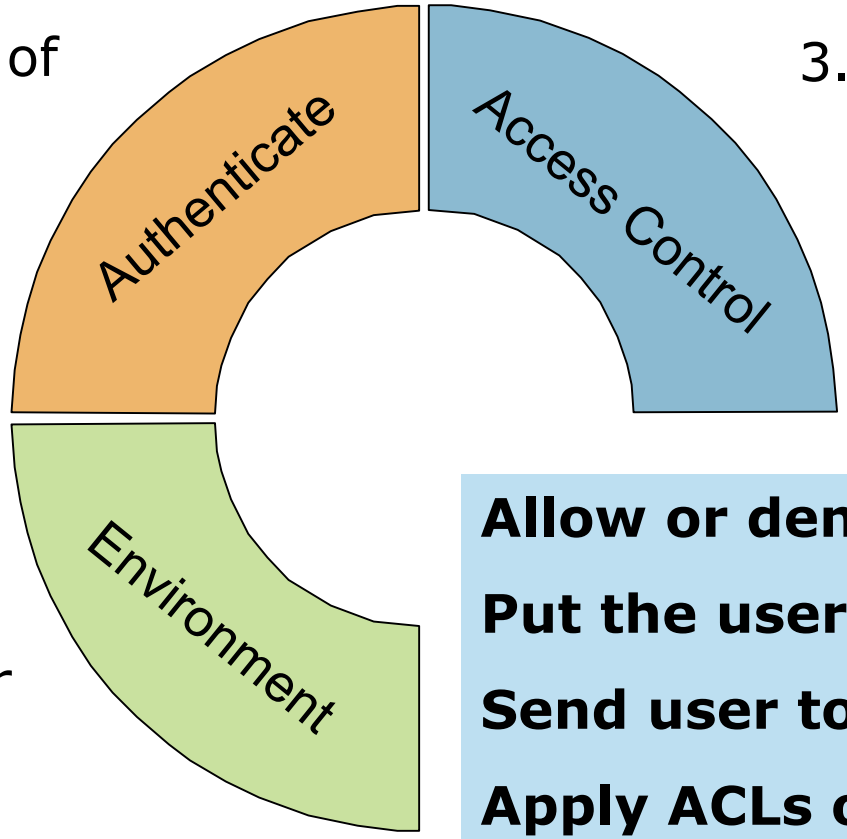
Key Concept: Access Is a Function of Authentication and Environment

What you can do = Who You Are + How Well You Comply with Policy + How Well You Behave On the Network

Darn… We just summarized NAC in one slide. What else is there to talk about?

Access Controls Define Capabilities and Restrict the User

1. Authentication of the user



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

2. Use environmental information for continuous policy decision making

Allow or deny access.

Put the user on a VLAN.

Send user to remediation.

Apply ACLs or firewall rules.

Access Control Enforcement Has Two Main Attributes to Understand

Control Granularity

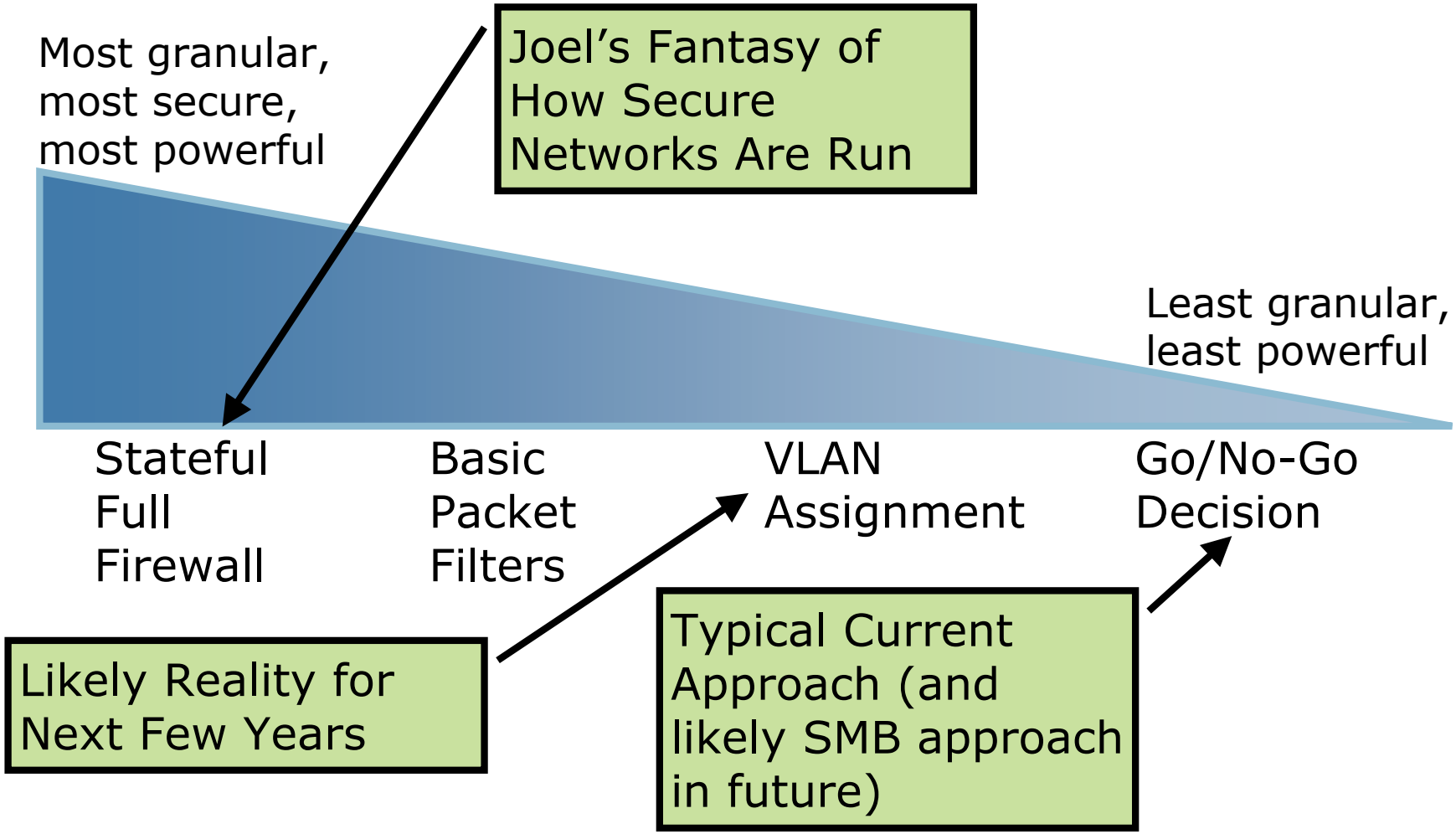
- **On/Off the network**
- **VLAN-level assignment**
- **Packet filters**
- **Stateful firewall**

Control Location

- **On the client itself**
- **At the edge of the network ("Edge Enforcement")**
- **A barrier between user and network ("Inline Enforcement")**
- **A hybrid of inline and edge**
- **Within the network protocols themselves**
- **At the server itself**

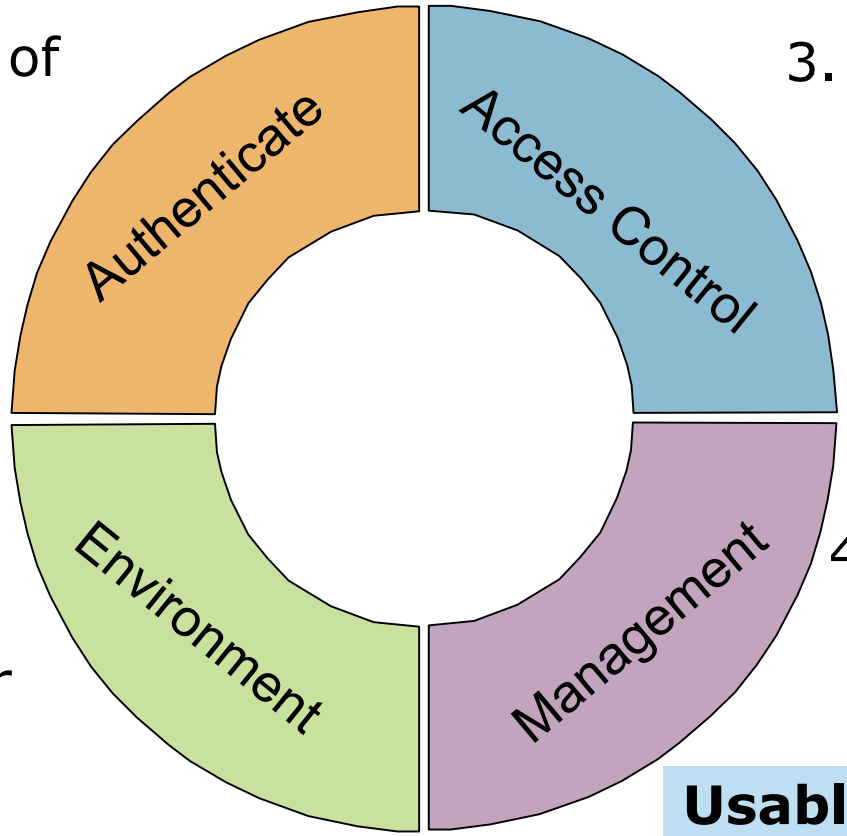
Lots more about this in the next session!

Granularity is a Spectrum Largely Determined by Hardware



Management of Policy is the Weak Link in most NAC Solutions

1. Authentication of the user



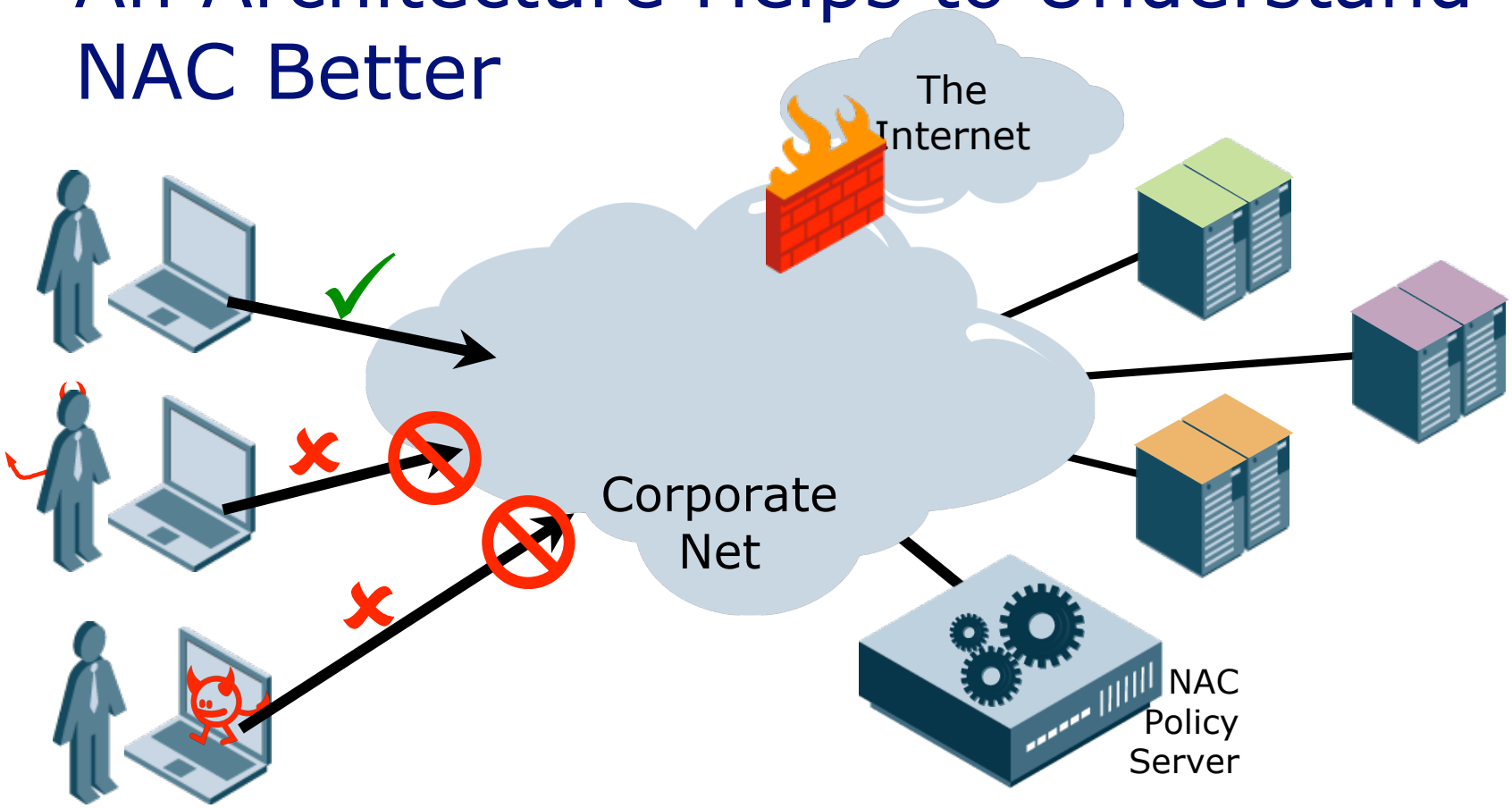
3. Control usage based on capabilities of hardware and security policy

2. Use environmental information for continuous policy decision making

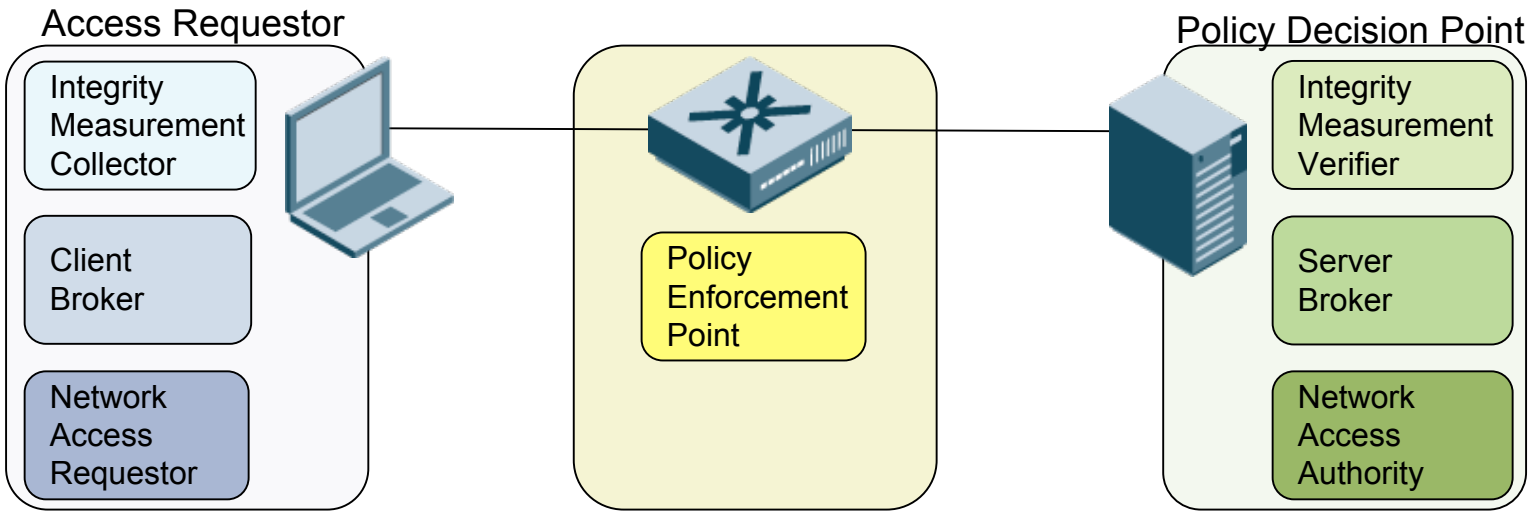
4. Manage it all

Usable management and cross-platform NAC normalization

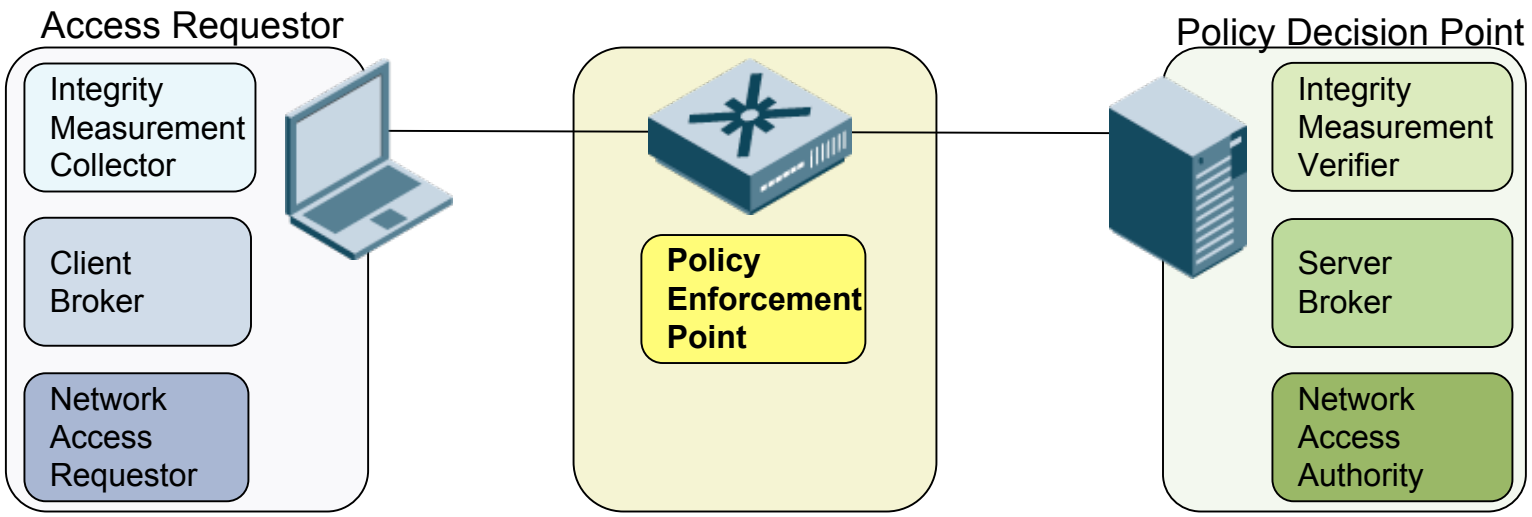
An Architecture Helps to Understand NAC Better



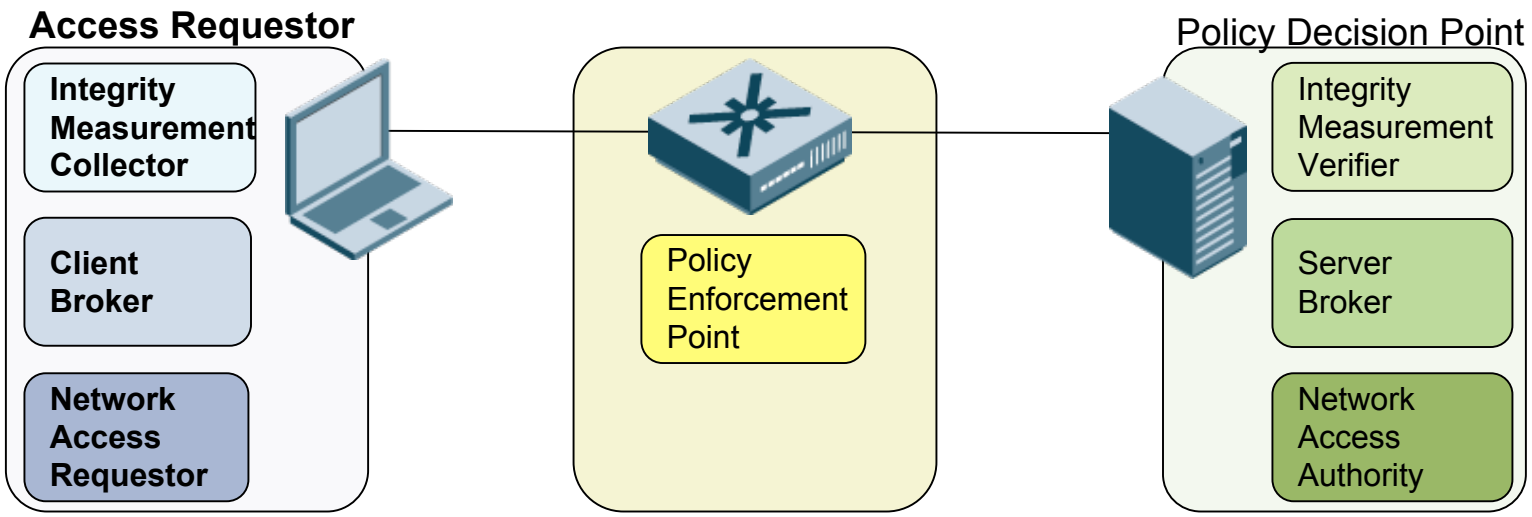
Lots of NAC Products… but Only a Few Good Architectures



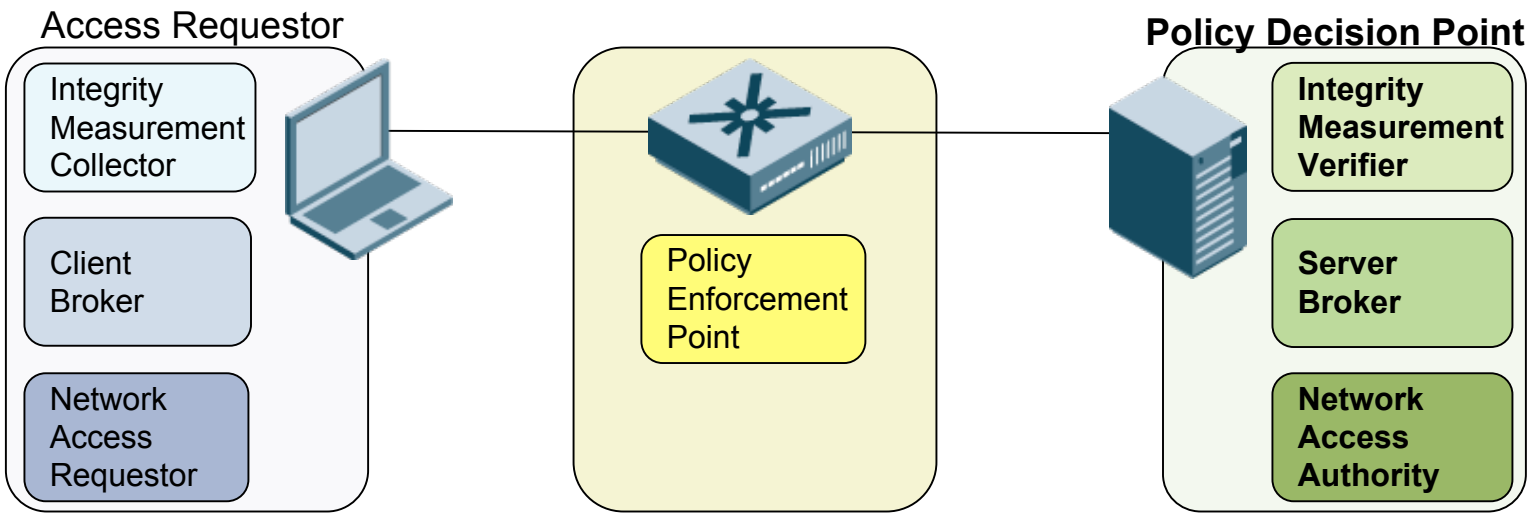
These are mostly TCG/TNC terms for each piece. IETF, Microsoft, and Cisco all have their own similar ones



What is it?	TCG TNC	Microsoft NAP	Cisco NAC
Policy Enforcement Point Component within the network that enforces policy, typically an 802.1X-capable switch or WLAN, VPN gateway, or firewall.	Policy Enforcement Point	NAP Enforcement Server	Network Access Device



What is it?	TCG TNC	Microsoft NAP	Cisco NAC
Integrity Measurement Collector Third-party software that runs on the client and collects information on security status and applications, such as 'is A/V enabled and up-to-date?'	Integrity Measurement Collector	System Health Agent	Posture Plug-in Apps
Client Broker "Middleware" that talks to the Posture Collectors, collecting their data, and passes it down to Posture Transport Client	TNC Client	NAP Agent	Cisco Trust Agent
Network Acces Requestor Connects the client to network, such as 802.1X supplicant. Authenticates the user, and acts as a conduit for Posture Collector data	Network Access Requestor	Enforcement Client	Cisco Trust Agent



What is it?	TCG TNC	Microsoft NAP	Cisco NAC
Integrity Measurement Verifier Receives status information from Posture Collectors then validates it against policy, returning a status to the Server Broker	Integrity Measurement Verifier	System Health Validator	Policy Vendor Server
Server Broker "Middleware" acting as an interface between multiple Posture Validators and the Posture Transport Server	TNC Server	NAP Administration Server	Access Control Server
Network Access Authority Validates authentication and posture, then passing policy to the Network Enforcement Point.	Network Access Authority	Network Policy Server	Access Control Server

http://www.networkworld.com/research/2006/040306-nac-overview.html

We've Just Grazed the Surface of NAC

- **NAC needs to be on your radar**
- **Tools like 802.1X should be part of your short and long range plans anyway**
- **Don't jump into a proprietary solution without considering the emerging standard architectures**

Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com

Network Access Control Part 2: Deploying NAC

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

How to Get a PDF of This Class

- **http://www.opus1.com/nac/**
  - **Piles of NAC resources and some pointers to other resource collections**

Agenda: Deploying NAC

- **Five Key Questions for NAC Deployment**
  - **Policy?**
  - **Authentication?**
  - **End Point Security?**
  - **Access Control**
  - **Integration**
- **Devil's Advocate View of NAC**

http://www.networkworld.com/research/2006/050106-ilabs-nac.html

Five Critical Questions for NAC

1) **What is your security policy? What are you trying to accomplish?**
2) **What authentication method will you use? How will you handle 'failure' cases?**
3) **What End Point Security (Posture Assessment) features do you want? What is the associated policy?**
4) **What enforcement strategy will you use? Where in the network will you enforce?**
5) **How is NAC going to integrate into your existing network smoothly and without unnecessary disruption?**

1) Policy

What Are Your Goals in Bringing NAC Into Your Network?

- **Normally, we add security to reduce risk.**

What Risk Are You Trying To Reduce?

You must decide early on why you are adding NAC to your network… because there are so many NAC vendors out there, you'll never get the right product if you don't know what you want

1) Policy

Questions, Questions, Questions

- **Are you trying to help honest people stay honest?**
- **Are you trying to keep hackers off your network?**
- **Are you trying to add greater control to the network?**
- **Are you trying to keep malware off your network?**
- **Are you trying to answer audit and compliance questions?**

1) Policy

Decide How Important Various Aspects of NAC Are to Your Deployment

User Authentication	End Point Security	Enforcement Granularity
Very Important — Not Very Important	Very Important — Not Very Important	Very Important — Not Very Important

Where will NAC apply?

VPN | WLAN | Guests | Desktops | Computer Room | Everywhere

2) Authentication

Each of the Authentication Methods Has Pros and Cons

	802.1X	**Web-based**	**Proprietary Client**
Pros	Highest security; standards-based; multi-protocol; most transparent; scales up	Very familiar model; broadest platform support; handles guest users best	Tight integration between client and security policy; broad range of topology support
Cons	802.1X supplicants have a "bad name;" weak guest support; poor support for non-mainstream platforms	Onerous and slow for local users; single protocol; requires web browser; security model weaker	Platform support not broad; vendor lock-in; weak guest support

2) Authentication

This Is Why Setting Policy in Step (1) Is So Critical!

- **Are you focused on enterprise users? Do you see this extending to desktops as well as "guest" areas? Is this for VPN access?**
- **Are you thinking about NAC largely for guest users or occasional staff use (conference rooms, for example)?**

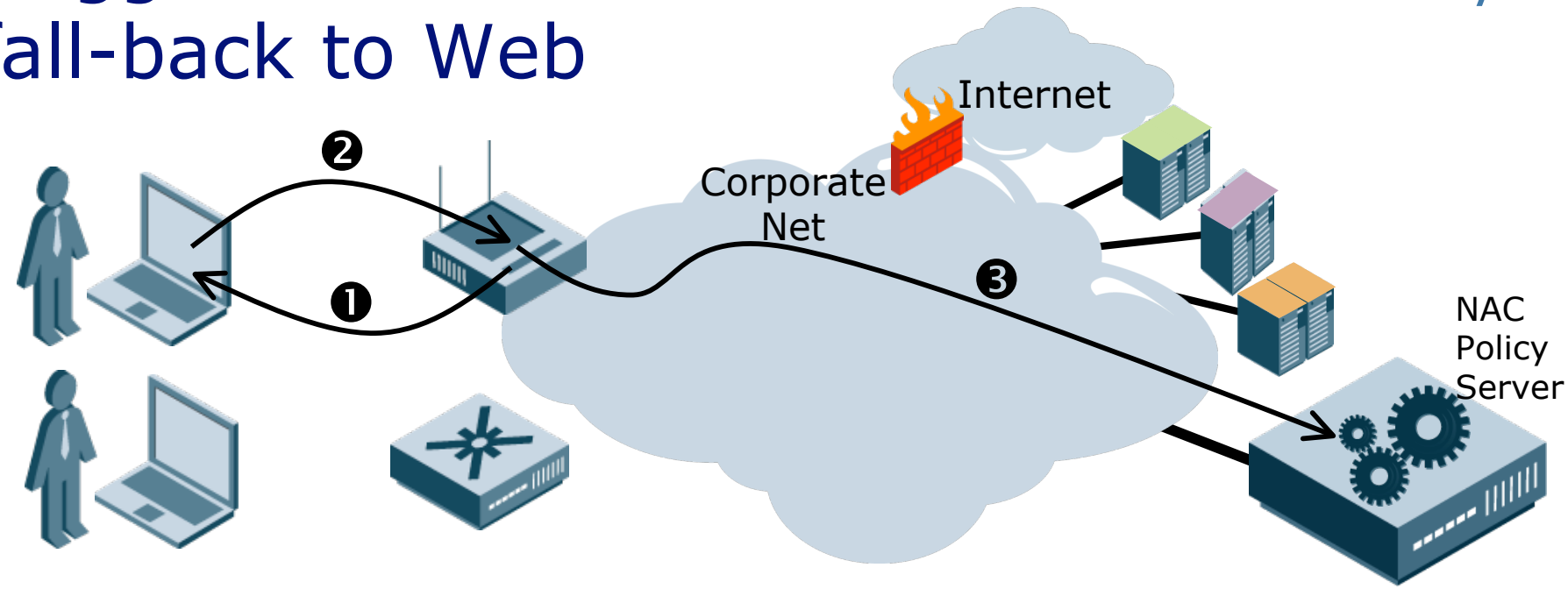
802.1X

Web

2) Authentication

Suggested Solution: 802.1X with fall-back to Web

1/2



❶ AP/Switch starts 802.1X (EAP) for authentication

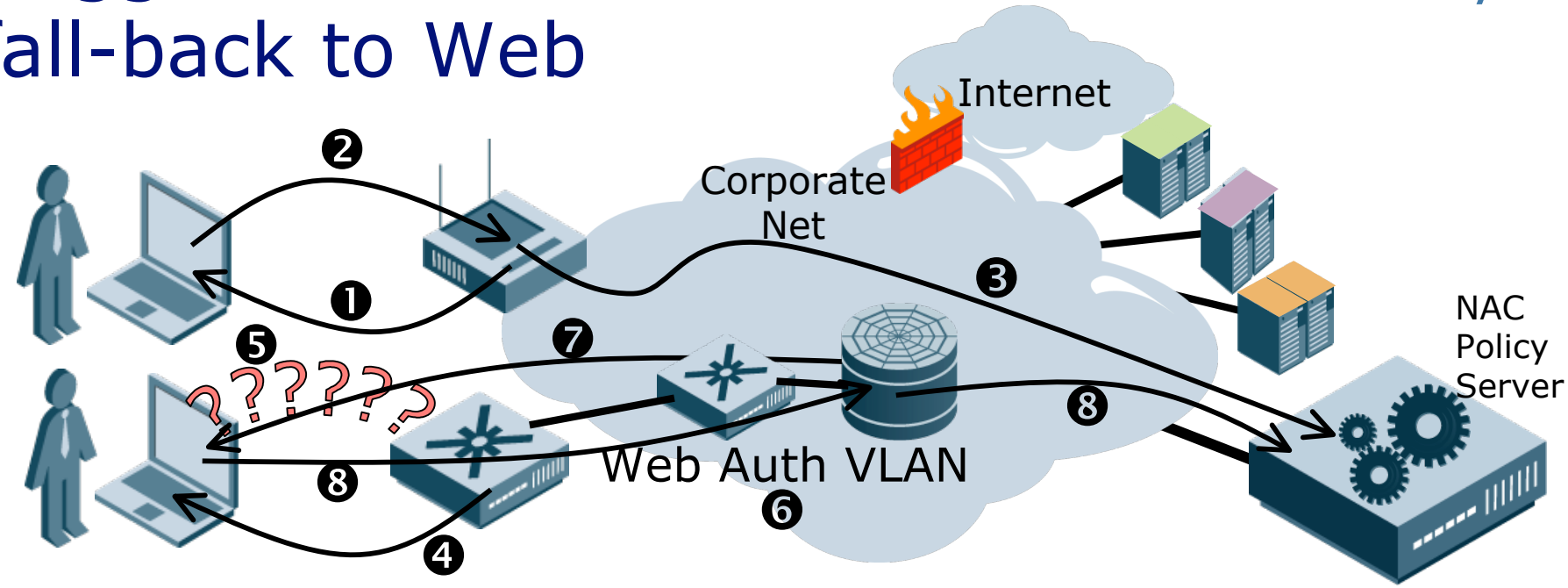
❷ Client knows 802.1X, and authenticates (and other stuff, don't forget) using 802.1X

❸ Authentication is passed to central policy server

2) Authentication

Suggested Solution: 802.1X with fall-back to Web

2/2



❹ AP/Switch starts 802.1X (EAP) for authentication

❺ Client doesn't know 802.1X; keeps DHCPing

❻ Switch puts user on Web Auth VLAN; user gets IP

❼ Eventually, user launches browser & hits captive portal

❽ User authenticates via web, passed to policy server

Two More Important Things To Remember

1. **Just because Snyder says you have to authenticate <u>doesn't mean</u> you have to authenticate**
   - Certain very large networking and O/S companies, for example, have NAC strategies that do not require authentication
2. **Lots of devices on your network will never run web browsers or 802.1X**
   - MAC-based authentication is common (with its drawbacks)
   - Backup MAC authentication with auditing/scanning if you can

3) End Point Security

End Point Security requires careful attention to policy

- **The hypothetical "Managed Desktop" (or Managed Laptop) is one important case**
- **The much-maligned guest user is the other significant case**

Managed vs. Unmanaged

Quarantine vs. Remediation

Guest Access vs. Network Access

Installed vs. "Dissolving"

3) End Point Security

Reduction in Risk Is Your Primary Driver When Defining Policy

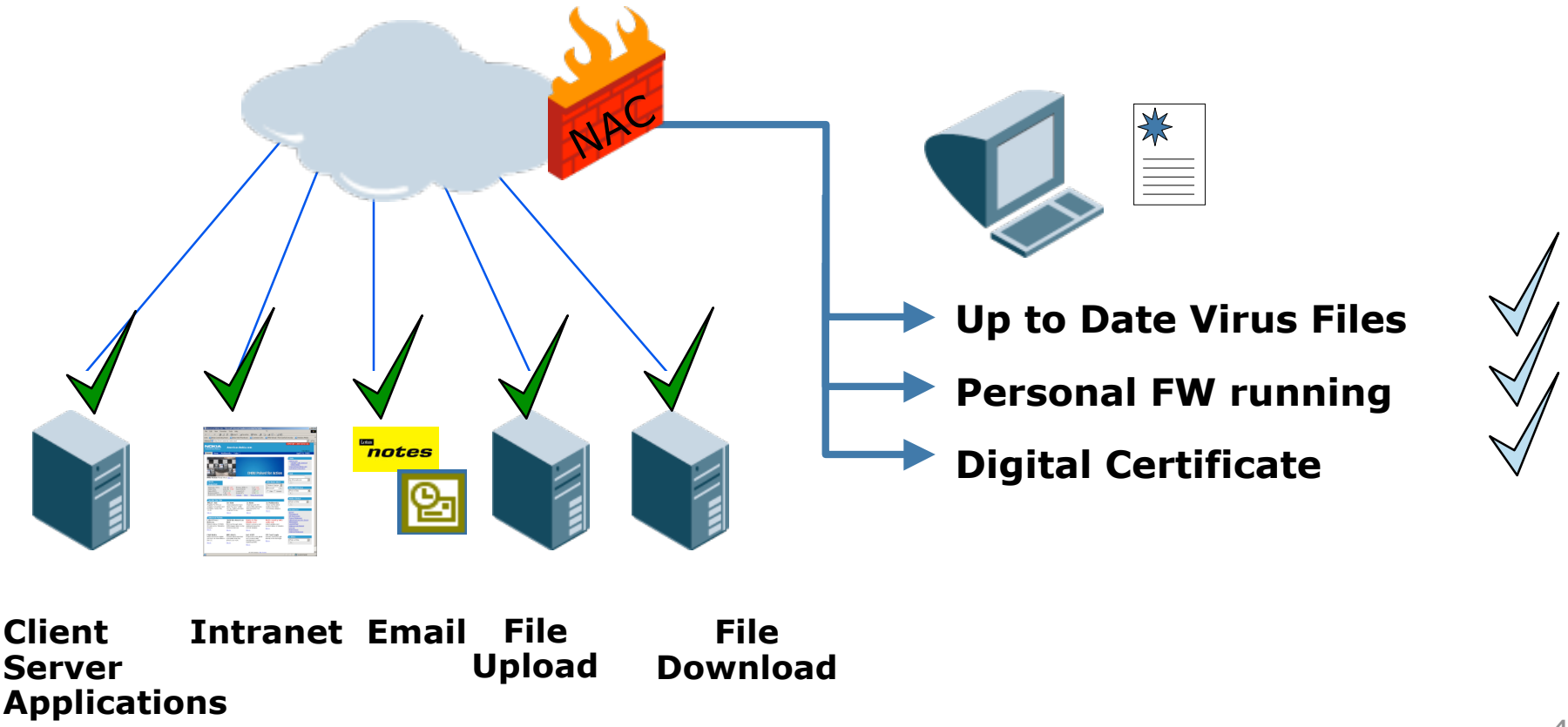
- **Doing stuff that doesn't <u>reduce your risk</u> is … a waste of time**
- **Doing stuff that doesn't <u>have value</u> is … a waste of money**
- **Doing stuff that has greater cost/aggravation/annoyance than value is … a good way to get to know Monster.COM**

Remember: Technologies are adopted to the extent that the pain they cause is less than the pain they relieve

3) End Point Security

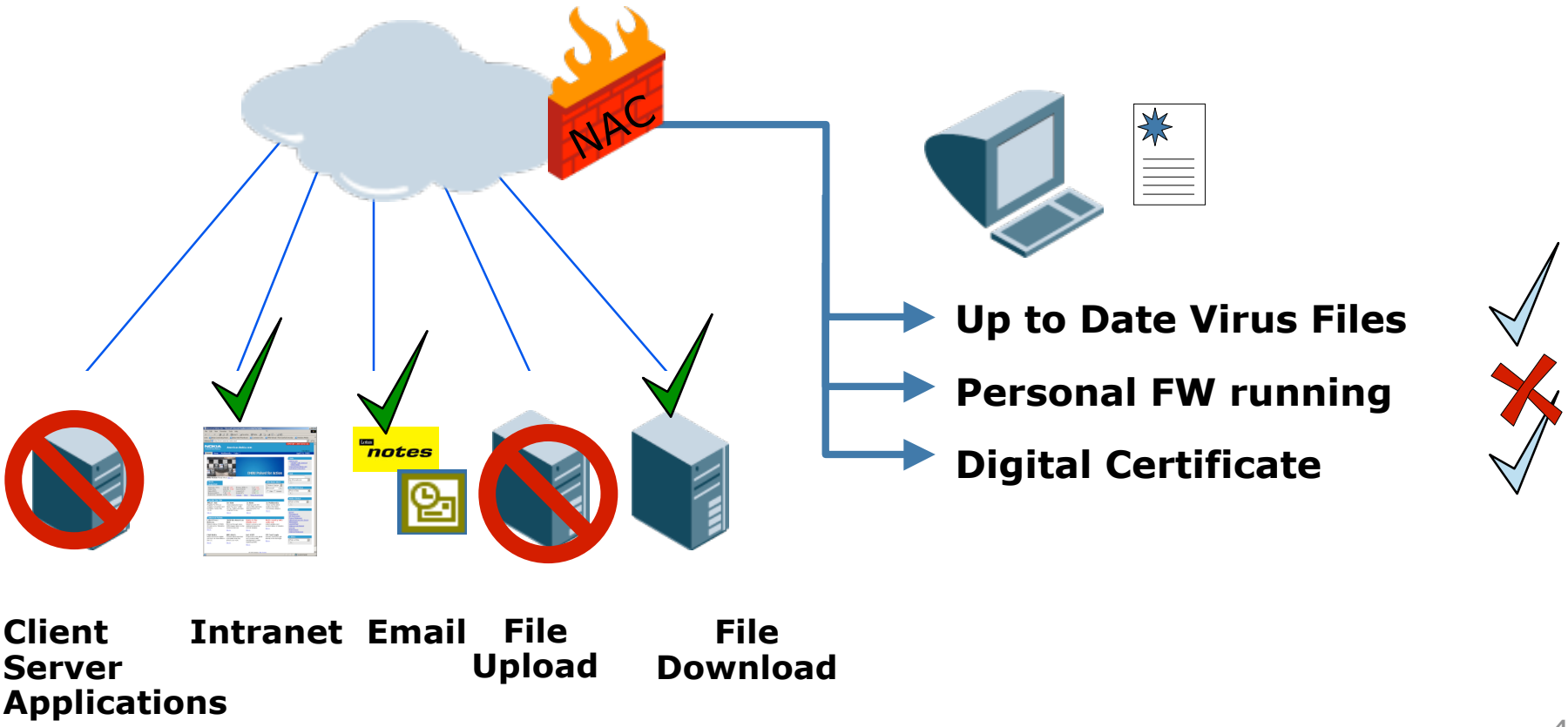
The Marketing View of End Point Security and NAC

Many NAC vendors are focusing on end-point security, quarantines, and remediation



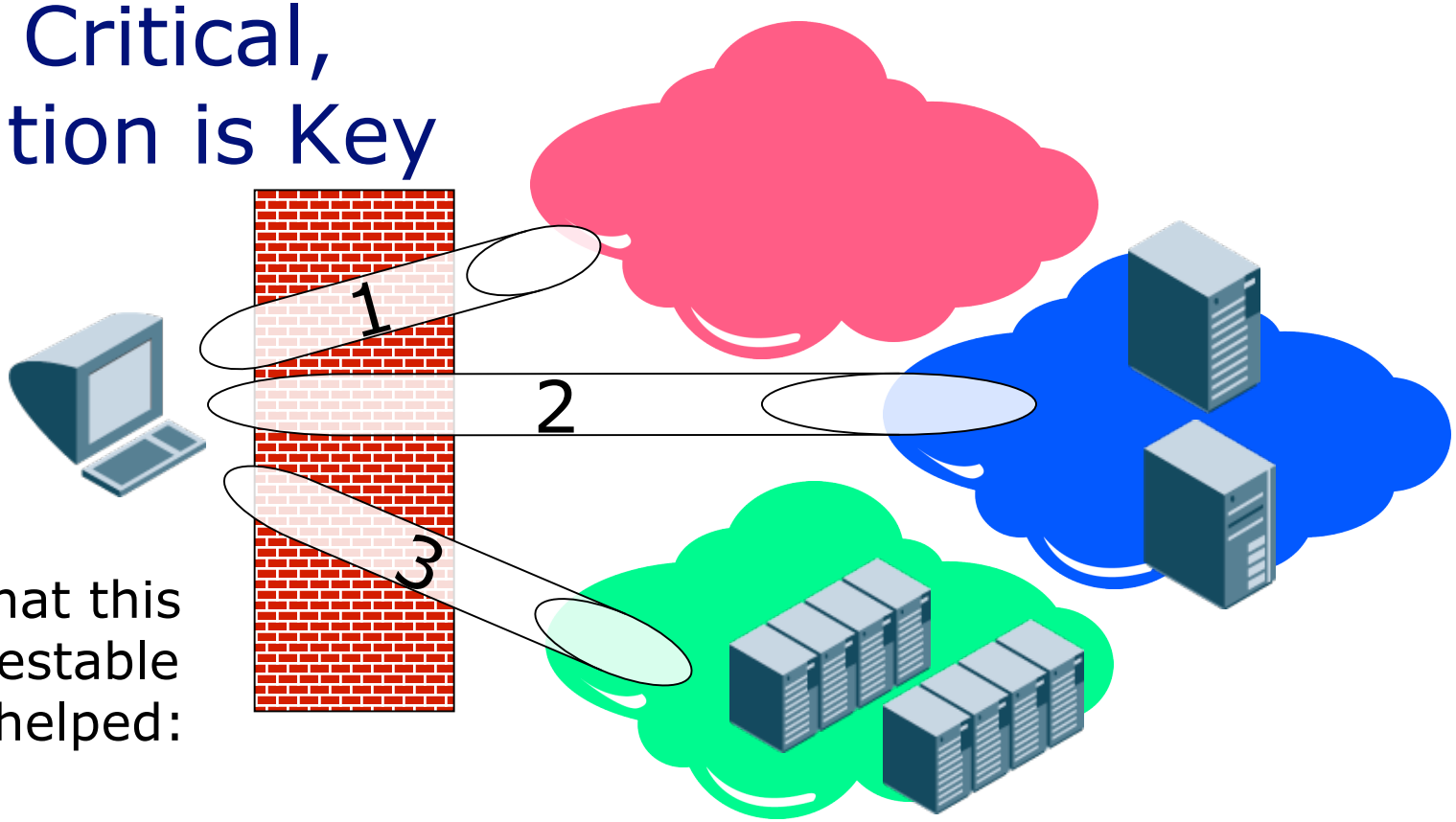
3) End Point Security

For systems which are not compliant, EPS could be very granular



3) End Point Security

If EPS is Critical, Remediation is Key



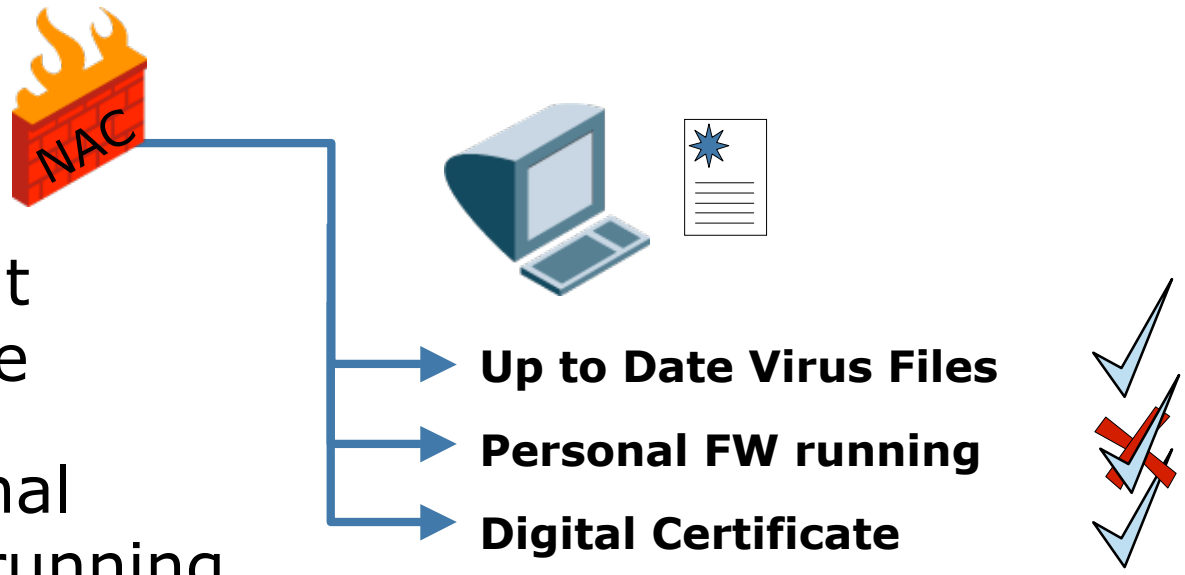
1. EPS says that this system is untestable or cannot be helped: Internet only

2. System is non-compliant, but can be helped: Remediation network access

3. System complies with security policy: full access granted

3) End Point Security

Some NAC Products Try to Self-Remediate



1. Check end point security posture
2. Discover Personal Firewall is not running
3. Turn on Personal Firewall (doh)

3) End Point Security

Two other wildcards in the EPS mix: auditing and continuous enforcement

Canine Acceptance Test

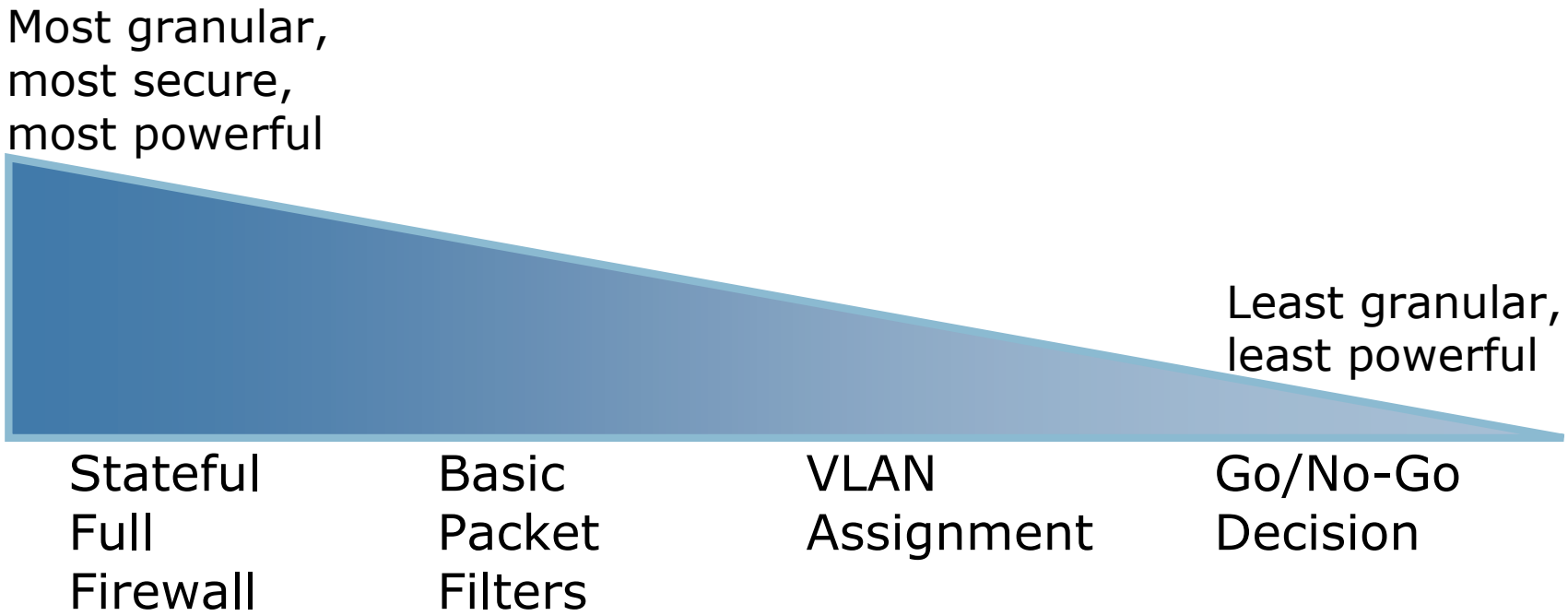
- **Auditing is often for guest users**
- **Auditing can help confirm ID of "non-authenticating" devices**

Continuous Enforcement

- **Obviously requires a continuously-present client (but does not have to be installed)**
- **"Are you keeping honest people honest?" or are you worried about deliberate deception?**

4) Enforcement

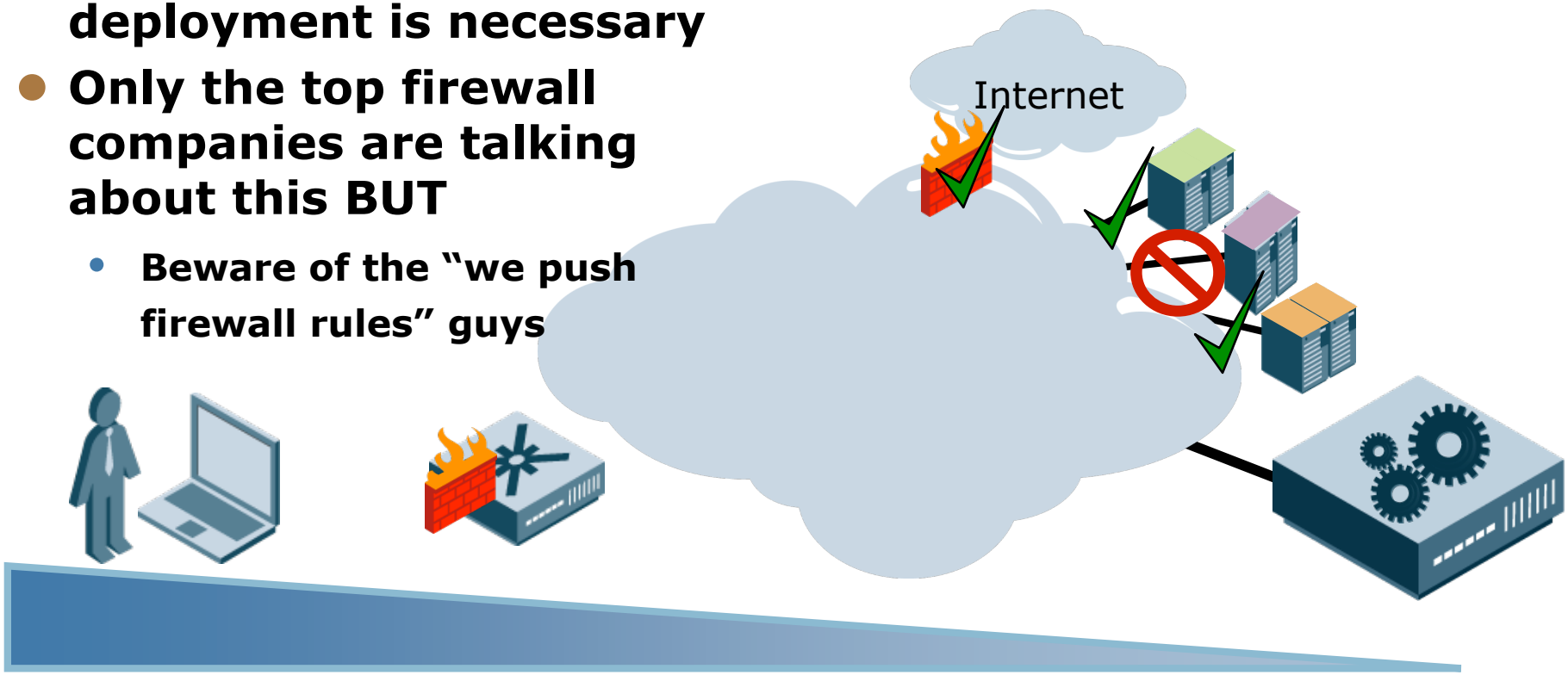
Enforcement and Hardware are Tied Together



4) Enforcement

Full True Firewalling is NAC Nirvana

- **You're on the cutting edge of technology here**
- **A v-e-r-y slow deployment is necessary**
- **Only the top firewall companies are talking about this BUT**
  - **Beware of the "we push firewall rules" guys**



Stateful Full Firewall | Basic Packet Filters | VLAN Assignment | Go/No-Go Decision

4) Enforcement

Basic Packet Filters Might Be As Good for Your Needs

- **Some devices require pre-generated ACLs**
  - **Dynamic multi-group membership may not be possible**
- **Some devices only have limited ACL capacity**

```
set policy profile 1 name "Quarantine"
set policy rule 1 udpdestport 53 mask 16 forward
set policy rule 1 udpdestport 67 mask 16 forward
set policy rule 1 tcpdestport 80 mask 16 forward
set policy rule 1 tcpdestport 443 mask 16 forward
set policy rule 1 tcpdestport 1723 mask 16 forward
set policy rule 1 ipproto 1  mask 8 drop
set policy rule 1 ipproto 6  mask 8 drop
set policy rule 1 ipproto 17  mask 8 drop
```

You can use packet filters and VLANs at the same time for higher security

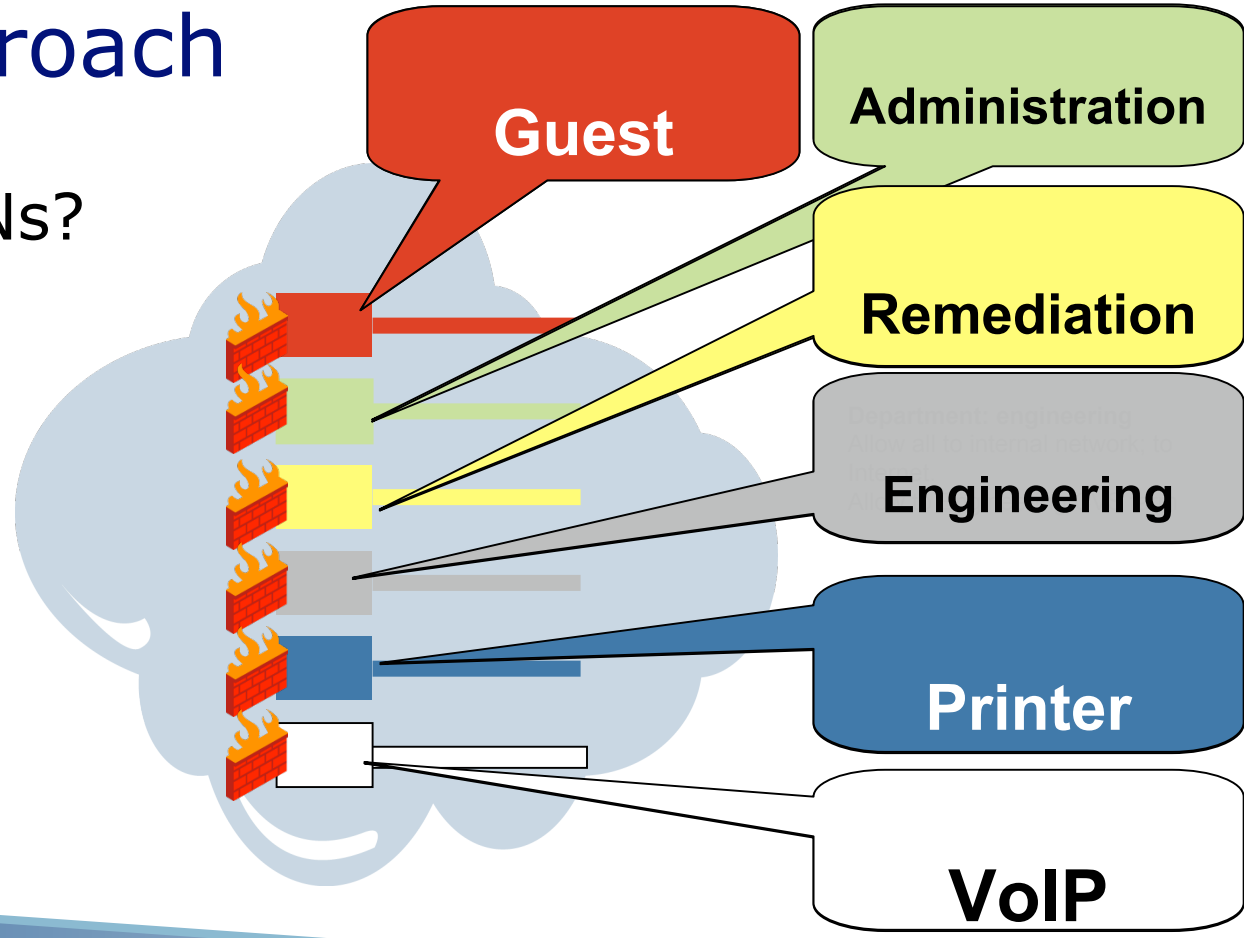
4) Enforcement

VLAN-based NAC is Probably the Most Common Approach

Q: How many VLANs?

A: A manageable number!

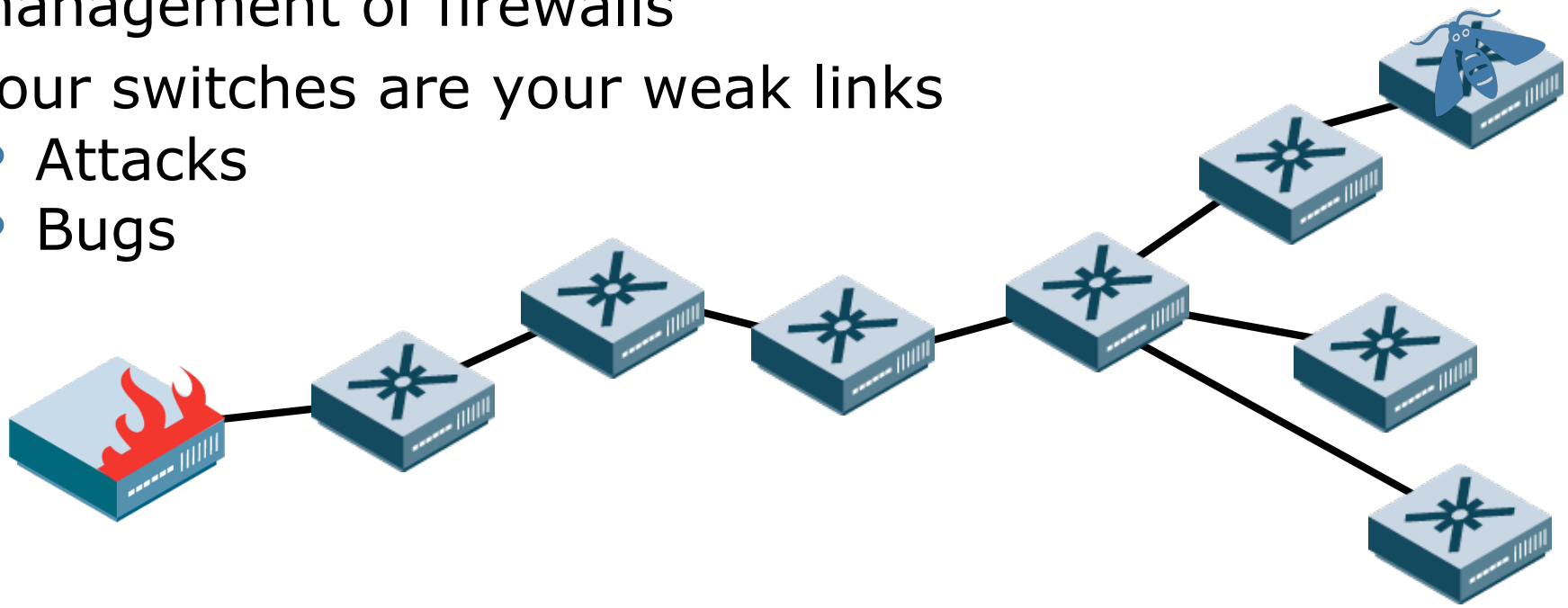
Firewalls must enforce policy between VLANs



4) Enforcement

Using VLANs for security has risks

- If packets jump from one VLAN to the other… the game is over
- Management of switching infrastructure is now as important as management of firewalls
- Your switches are your weak links
  - Attacks
  - Bugs



4) Enforcement

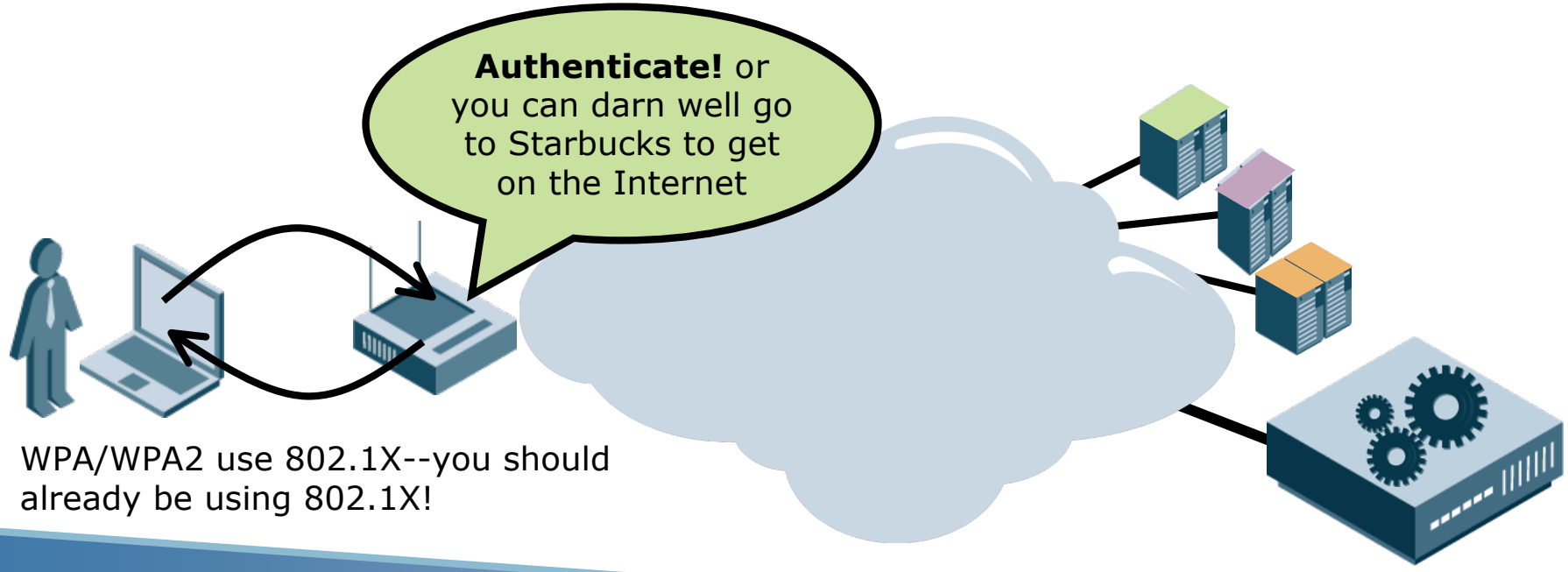
Switches need some minimum requirements for good NAC

Feature	Notes
Default VLAN	**Users who have no 802.1X client need to get put into captive portal-land (perhaps also have captive portal built into switch?)**
MAC Auth. Bypass	**Switch should try and authenticate user with MAC address for devices like printers**
Multi-Authentication	**Switch should deal with multiple MAC addresses on a port (even if it's not in the 802.1X standard to do so…)**
RFC 3580 VLAN Assignment	**Switch must accept VLANs in RADIUS attributes per RFC 3580**
"beyond VLAN" assignment	**Switch should have a way of receiving enforcement beyond VLANs, such as Filter-ID, (if the switch has enforcement capabilities)**

4) Enforcement

Go/No-Go Sounds Simple

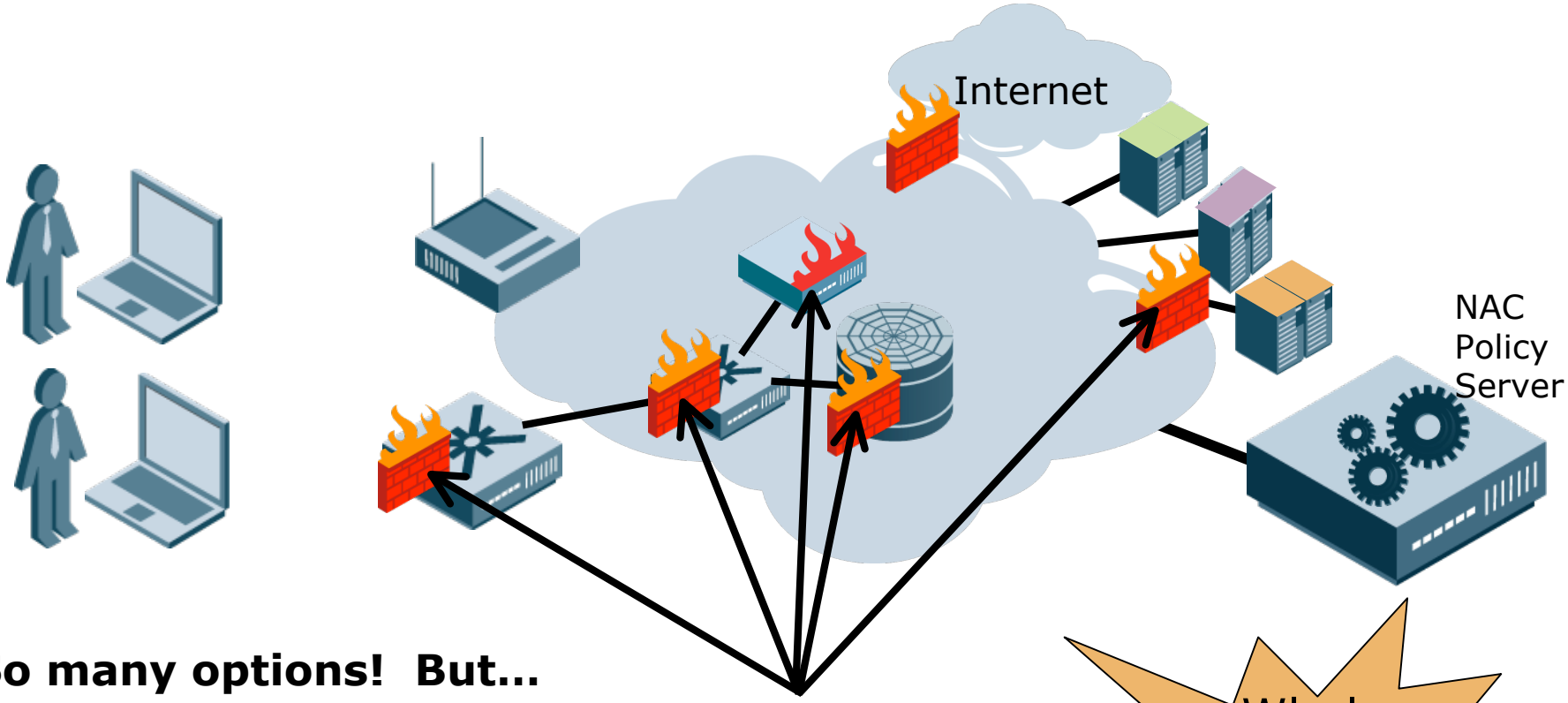
- **It is, but…**
  - **It's a good way to get your feet wet with underlying NAC technologies and concepts**



WPA/WPA2 use 802.1X--you should already be using 802.1X!

4) Enforcement

One Last Question: Where Is The Best Place for Enforcement?



So many options! But…
- the <u>closer to the user, the more secure</u>
- you will probably choose something that <u>works with your existing hardware</u> and not replace everything

Whole session on this later

5) Integration

Integration requires Multiple Teams

Network

Touch all hardware? Upgrade? New Firmware? Is your technology supported? Where will this go and not go? Wireless? Wired? Branches? HQ? And…?

Windows

Integrate client into desktop? Understand EPS implications? Work with remediation systems? And?

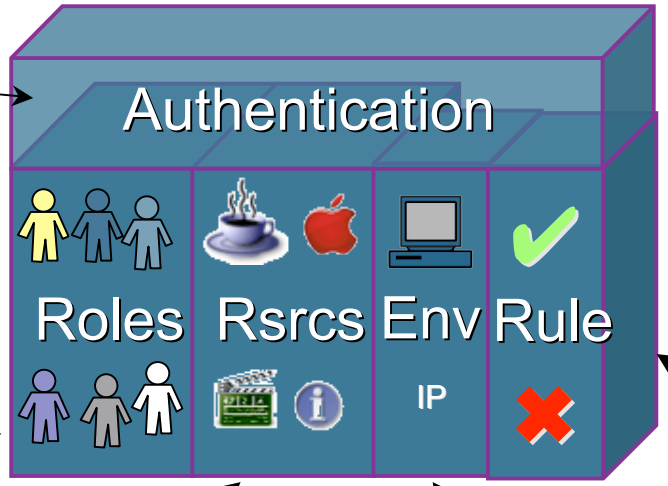
Security

Policy definition and maintenance? Integrate with authentication databases? Work with Ipsec/SSL VPN?

5) Integration

NAC brings together many different networking and security disciplines

First: authenticate. Then:



Roles: Who you are and what groups you are in

Rule: the Access Control decision

Resources: Systems, subnets, VLANs

Environmental information: End-point security posture, access method, *etc*.

5) Integration

It's early to define "best practices," but here are some starting points

- **Break down your deployment into tasks and subtasks**
  - **Don't NAC all access methods at once**
  - **Don't use all options at once**
- **Maximize your investment by extending NAC as far as you can**
- **Pay attention to edge cases and corner cases**
  - **PDAs**
  - **WiFi VoIP phones, printers**
  - **Staff-owned laptops/desktops**
  - **VPN access**
- **As with any technology, understand the failure points and build for availability**

The Devil's Advocate View of NAC

- **EPS checks work best when you need them least**
- **Generals---and NAC---always prepare to fight the last war**
- **ROI on NAC is a big unknown**
- **Too much information is just … too much information**
- **You can only control what you can see**

I'm not saying "don't do it." I'm saying "go in with your eyes open."

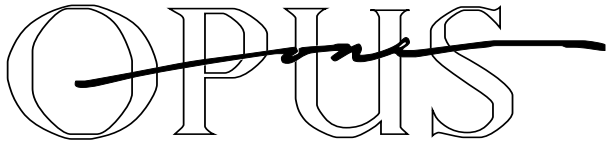
http://www.networkworld.com/columnists/2006/061206snyder.html

Thanks!

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

Network Access Control
Part 3: Enforcement Approaches

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



Agenda

- **What are the NAC enforcement approaches?**
- **How do these approaches compare?**

Access Control Enforcement Has Two Main Attributes to Understand

Control Granularity

- **On/Off the network**
- **VLAN-level assignment**
- **Packet filters**
- **Stateful firewall**

Control Location

- **On the client itself**
- **At the edge of the network ("Edge Enforcement")**
- **A barrier between user and network ("Inline Enforcement")**
- **A hybrid of inline and edge**
- **Within the network protocols themselves**
- **At the server itself**

This hour

Three Enforcement Locations Give Four Enforcement Strategies

Control Location

- On the client itself
- **At the edge of the network ("Edge Enforcement")**
- **A barrier between user and network ("Inline Enforcement")**
- **A hybrid of inline and edge**
- **Within the network protocols themselves**
- At the server itself

❶ Edge enforcement

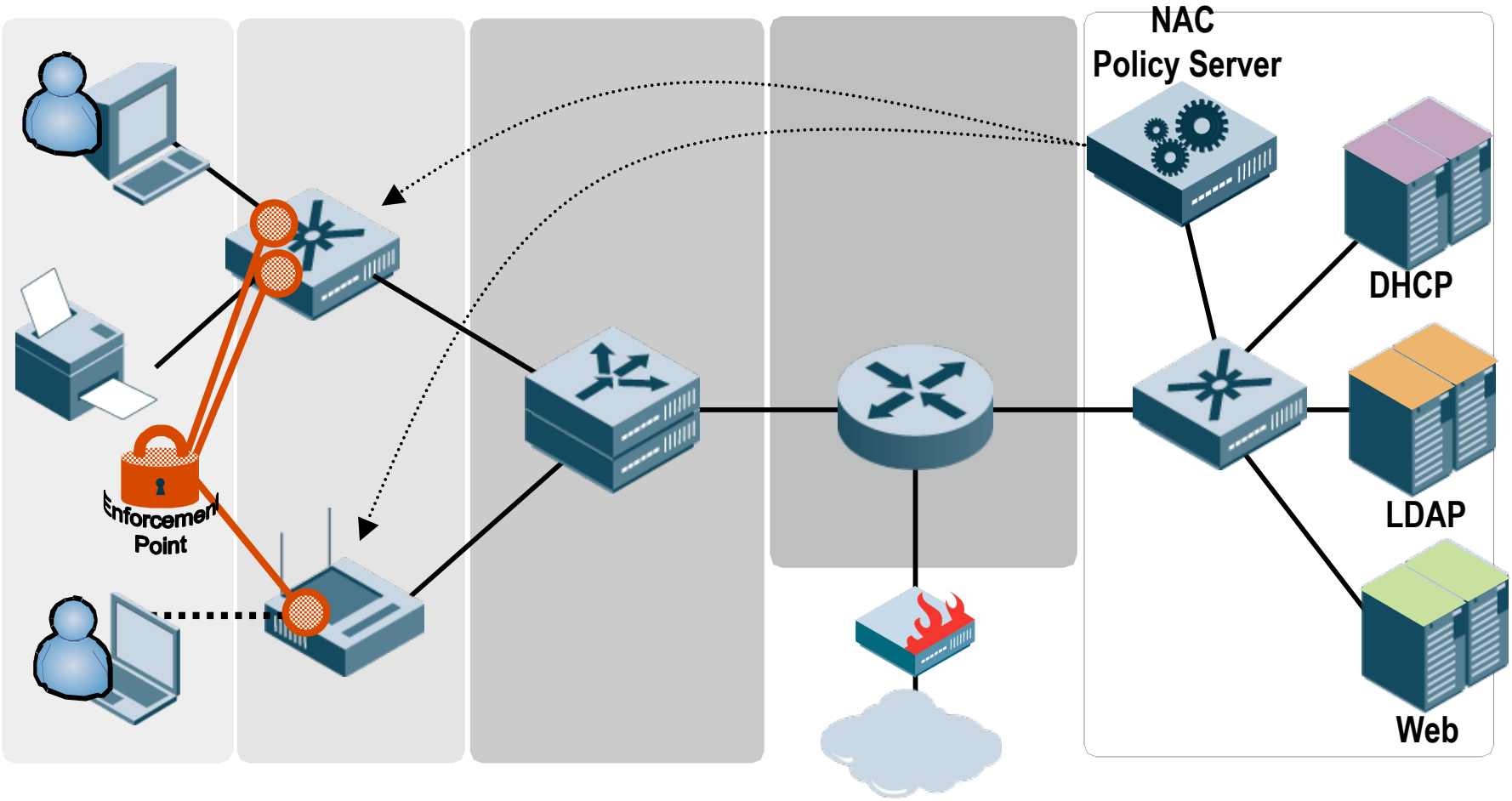
❷ In-line enforcement

❸ Hybrid enforcement, mixing in-line and edge

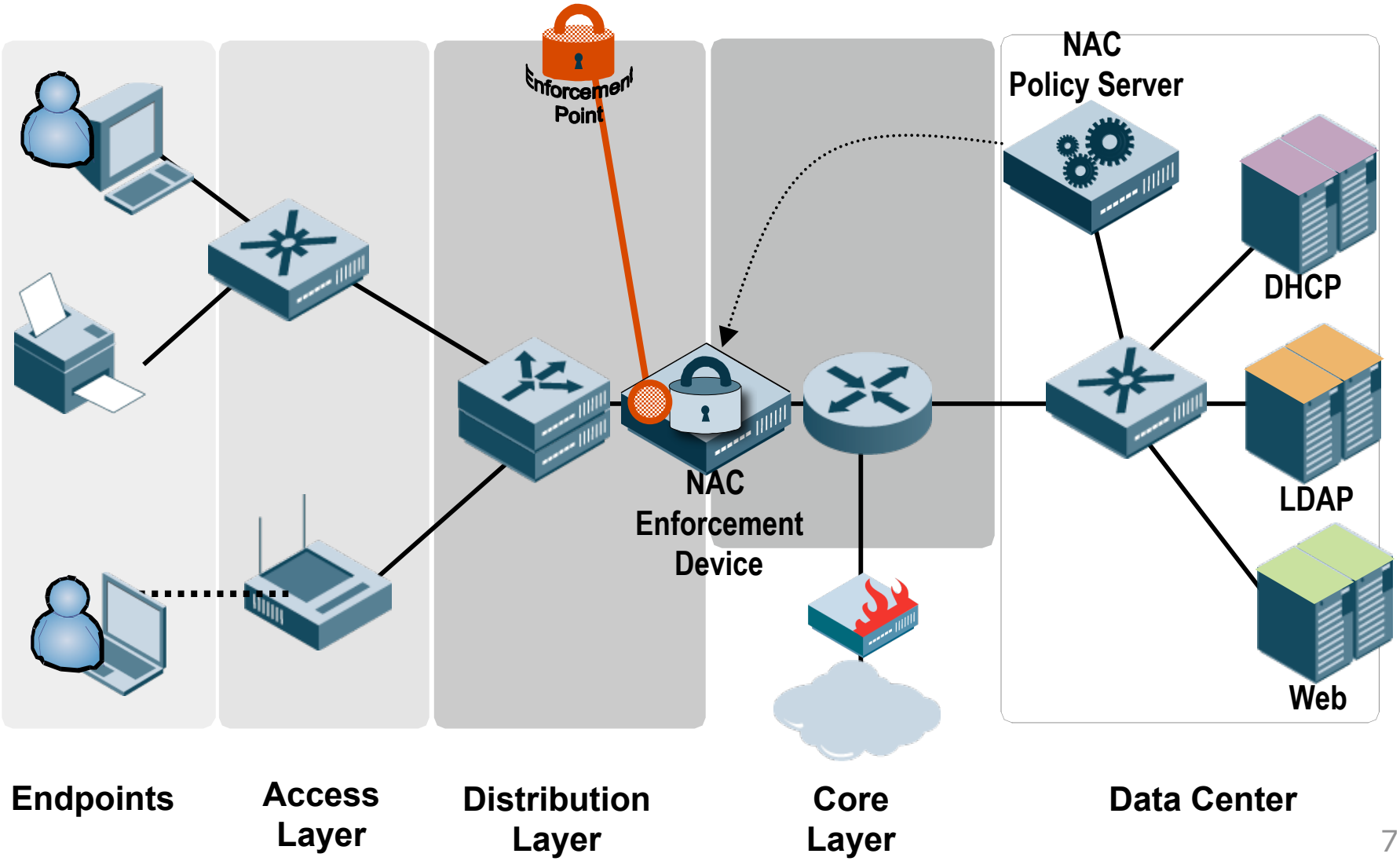
❹ Protocol-based enforcement

Not NAC, these are HAC (host-based access control)

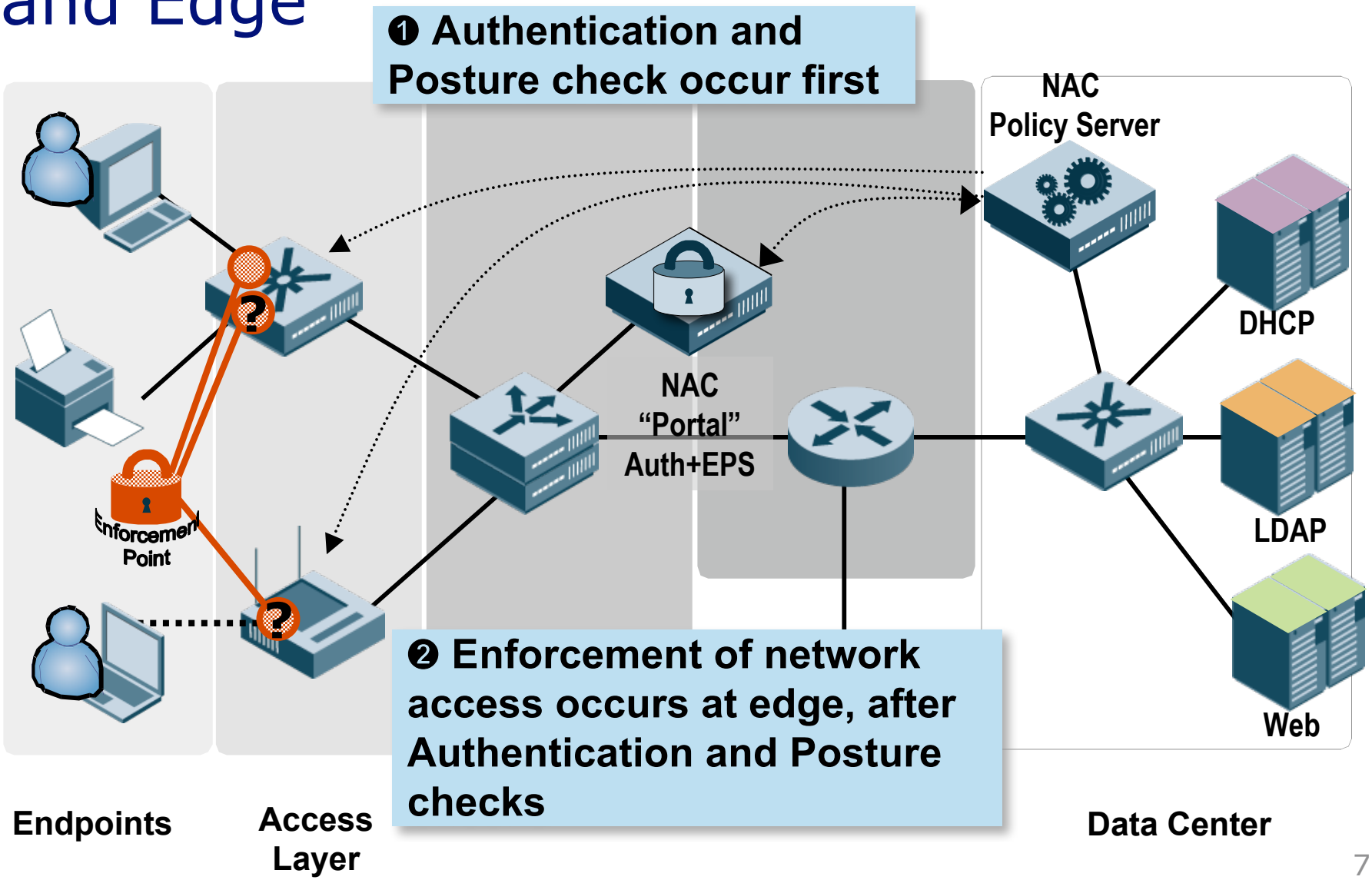
Edge Enforcement Occurs at the Point of Access to the Network



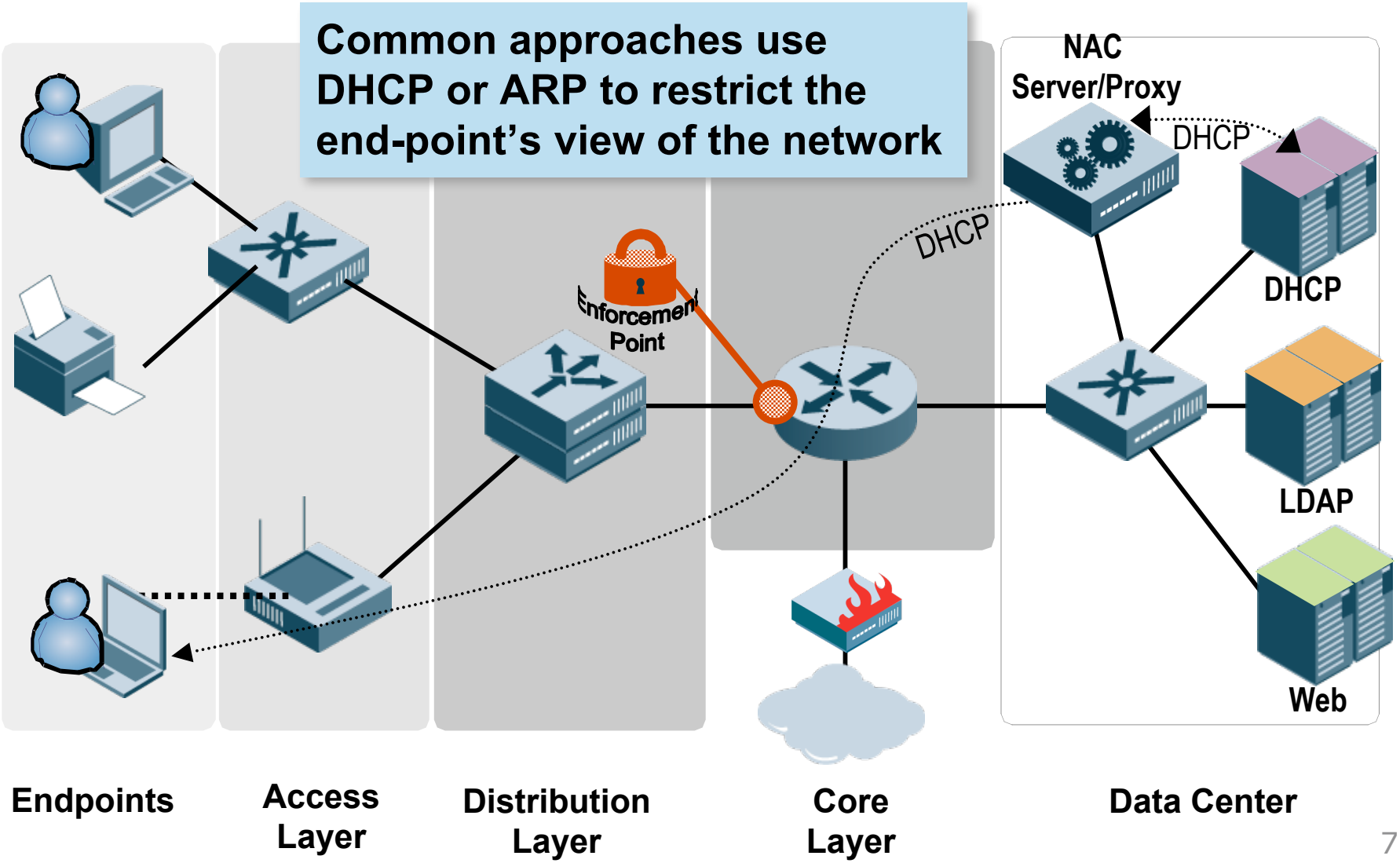
In-line Enforcement Occurs Deeper in the Network



Hybrid Enforcement combines In-Line and Edge



Protocol-based Enforcement Occurs at Layer Three

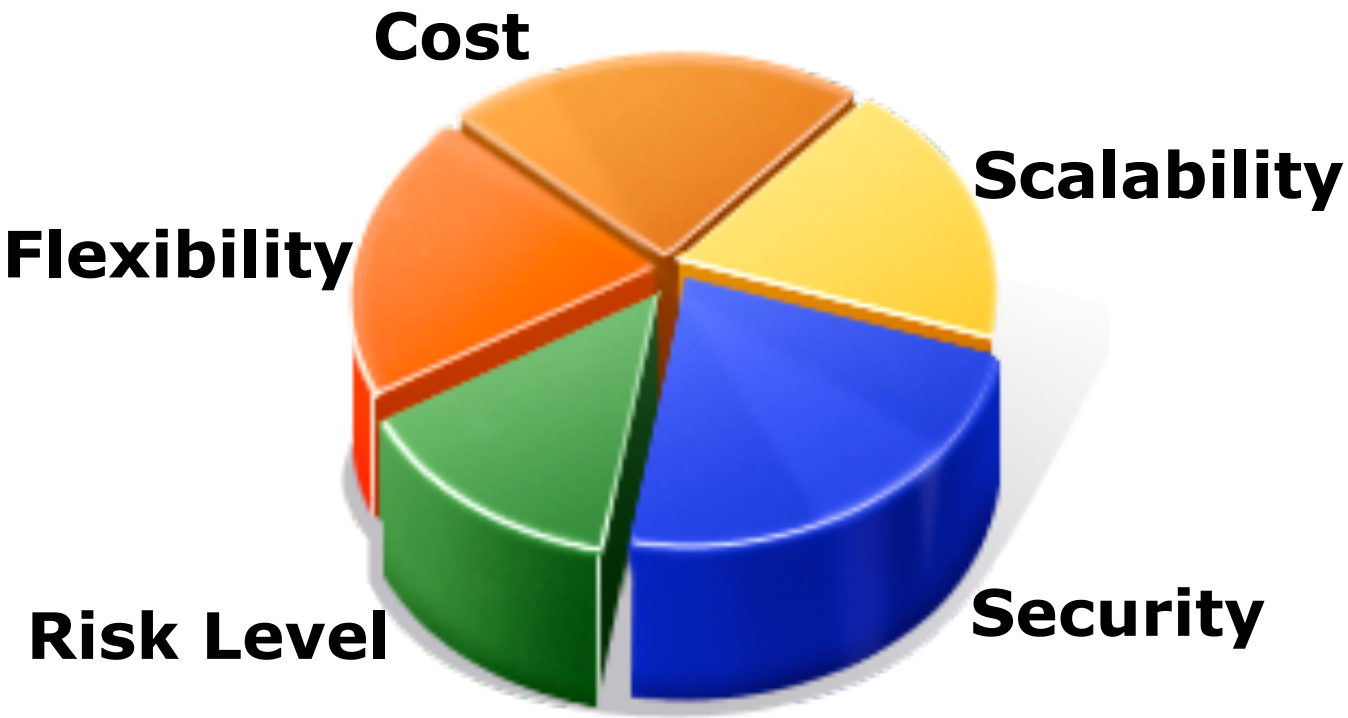


All Current NAC Products Use One Of These Four Enforcement Methods

- **So… Which Is Best?**

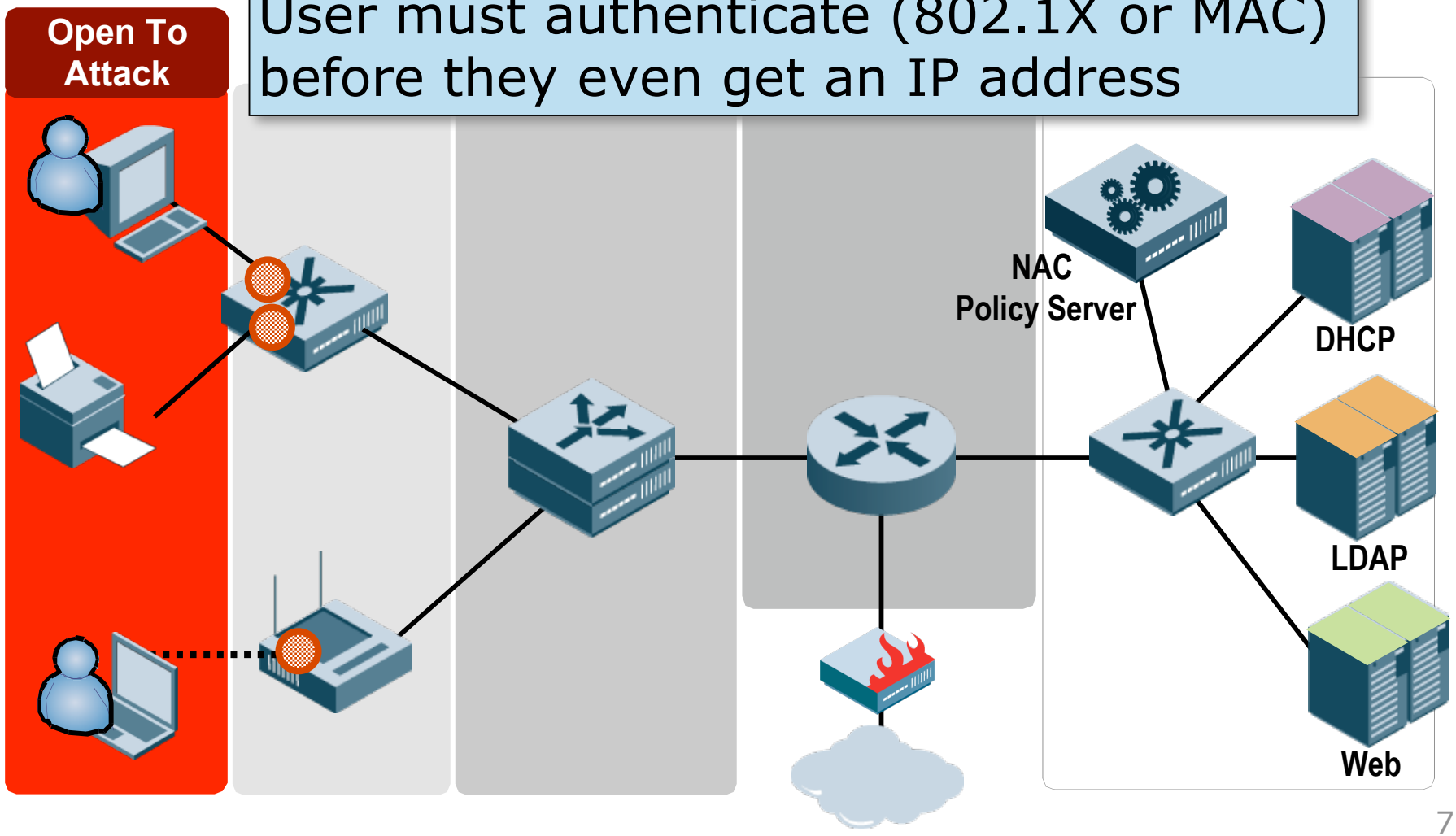
(That's Security Geek Code for "I Don't Know"… but there are significant differences which mean that one is probably "right" for you)

Five Criteria Can Help To Pick Right Enforcement Option For You

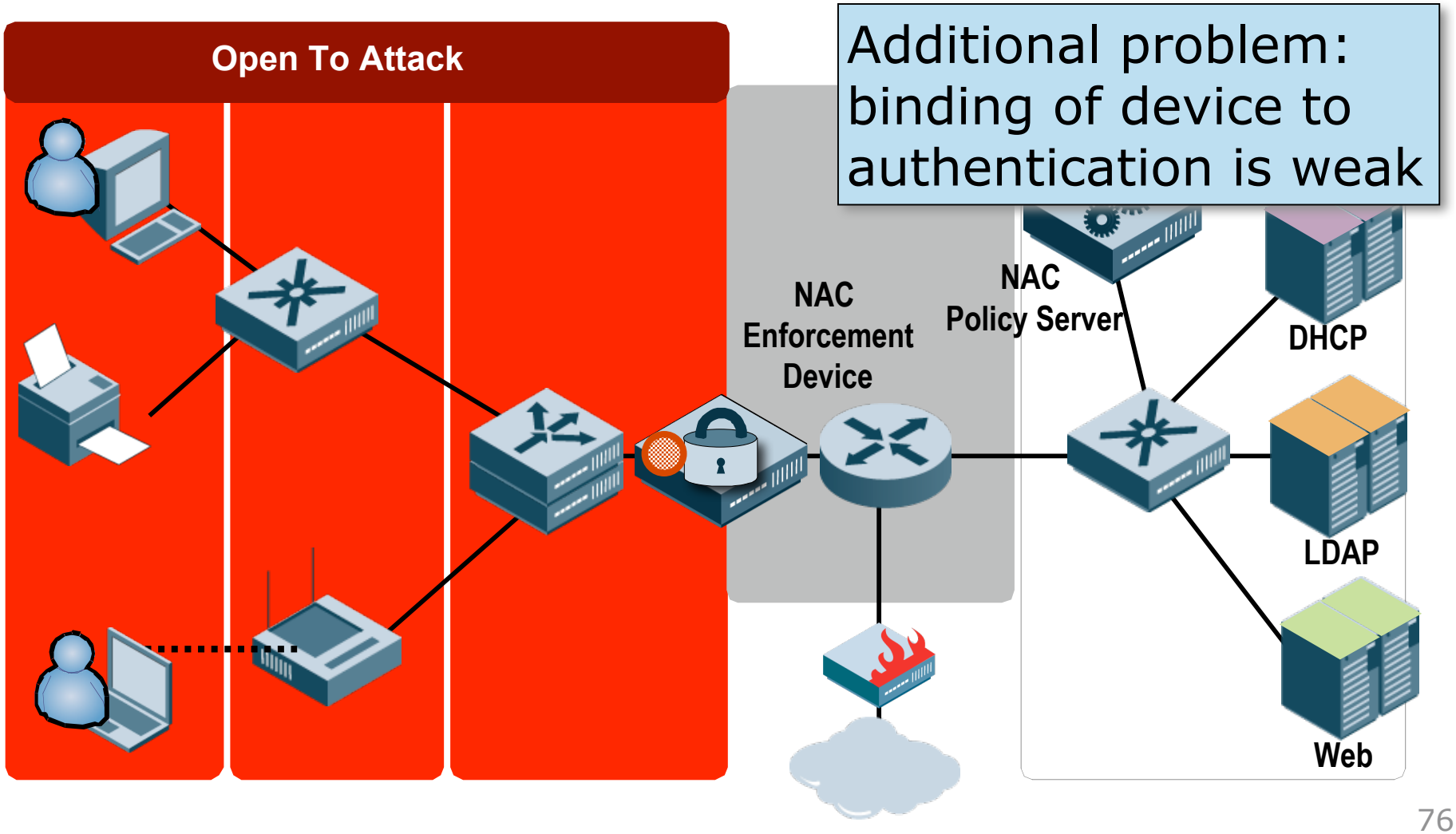


Edge Enforcement Reduces Attack Opportunities

User must authenticate (802.1X or MAC) before they even get an IP address

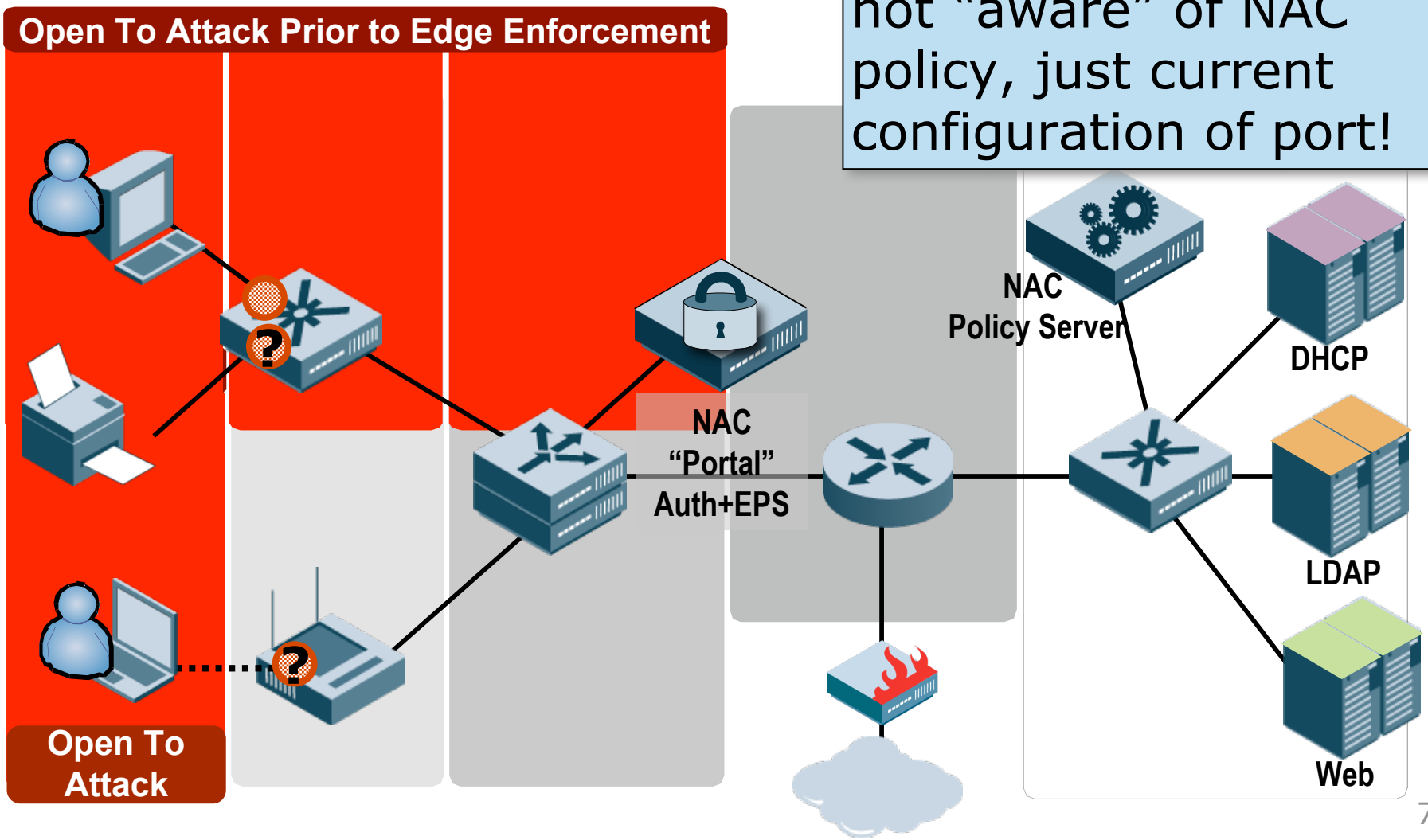


In-line Enforcement Allows Much Greater Monitoring and Attacking



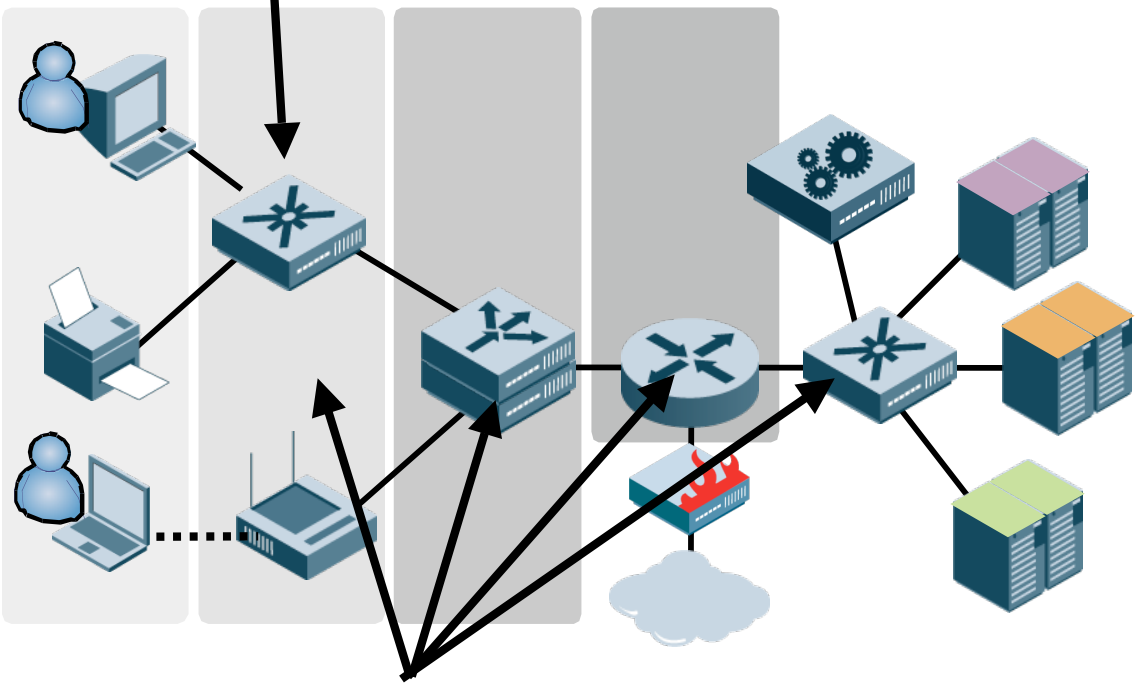
Hybrid Enforcement Starts Weak, but Strengthens

But: edge device is not "aware" of NAC policy, just current configuration of port!



Flexibility can be measured in several ways

How many different kinds of enforcement can I use here?

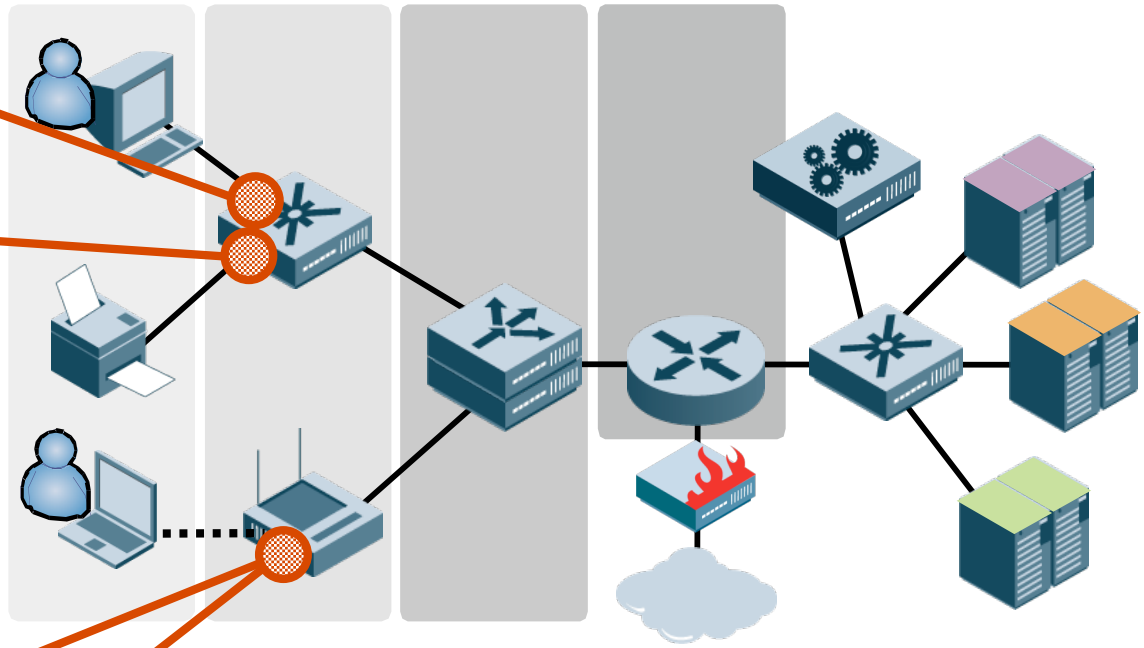


Where can I put the enforcement?

Different Kinds of Enforcement Solve Different Kinds of Problems

Go/No-Go You're either on, or you're not

VLAN Broad strokes access control: guest, employee, printer, etc.



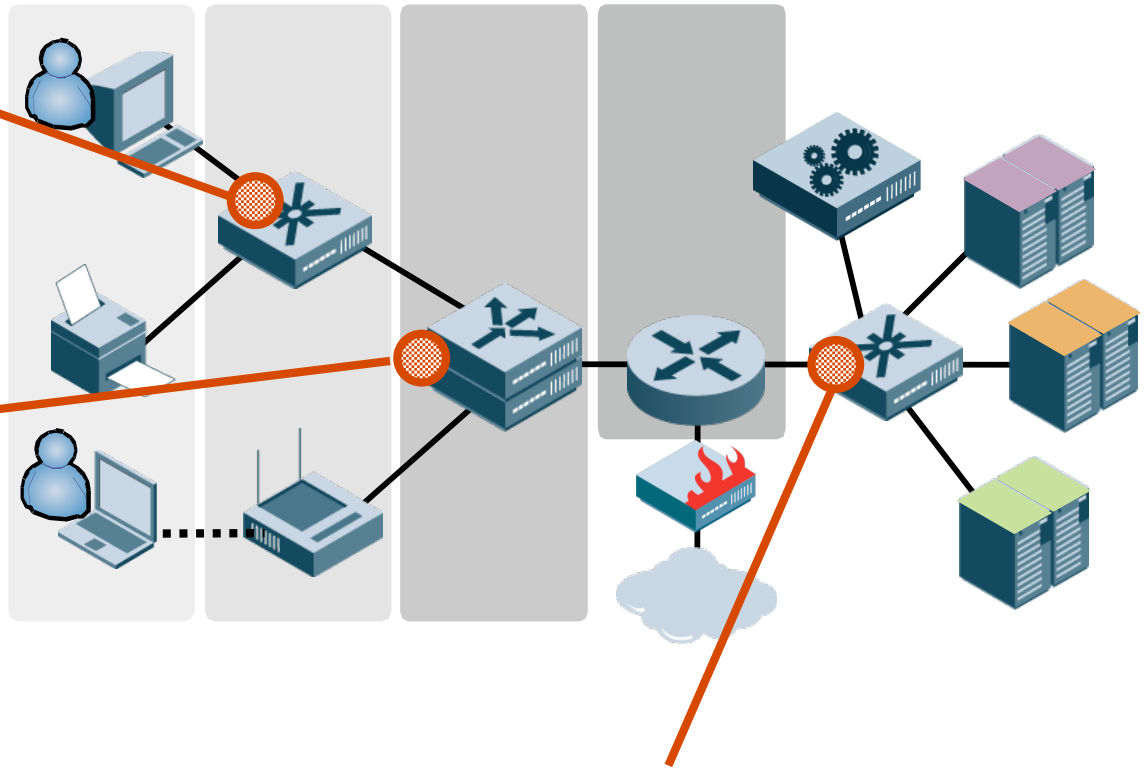
Stateless Packet Filter Fine-grained controls solve complex policy problems (or when VLANs won't work)

Firewall Very high level of security controls; very fine-grained policy

Different Enforcement Locations Focus Controls Where Needed

Enforce Here Users can't get anywhere at all unless allowed

Enforce Here Convenient if your switches are unmanaged or 'swampy'



Enforce Here Move enforcement to assets you really care about

Summarizing Flexibility

	Enforcement **Kind**	Enforcement **Location**
Edge Enforcement	Any, depending on equipment ✓✓	At edge
In-line Enforcement	ACL or FW (one type only)	At in-line server location
Hybrid Enforcement	Any, but most commonly VLAN ✓	Any point ✓
Protocol-based Enforcement	Protocol	At Layer 3 server location

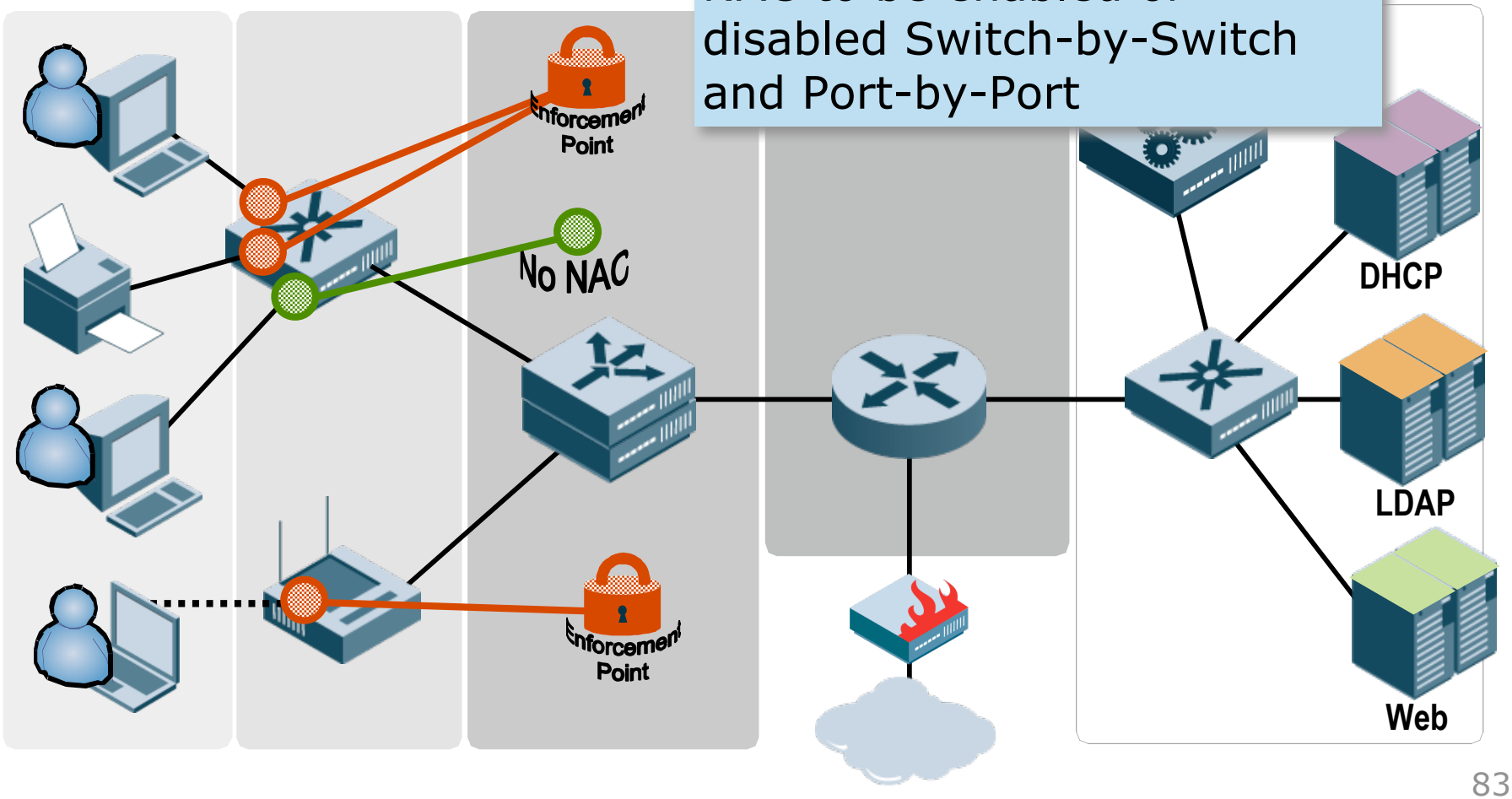
Simple Maxim: Risk is to be Avoided

- **Rules for a successful <X> Deployment:**
  1. **Step-by-step approach**
  2. **Refinement based on lessons learned**
  3. **Easy and inexpensive back-out plan**
  4. **Increase commitment to match comfort level with technology**

X = IPS, Web Proxy, Anti-Spam, *etc*.
And NAC!

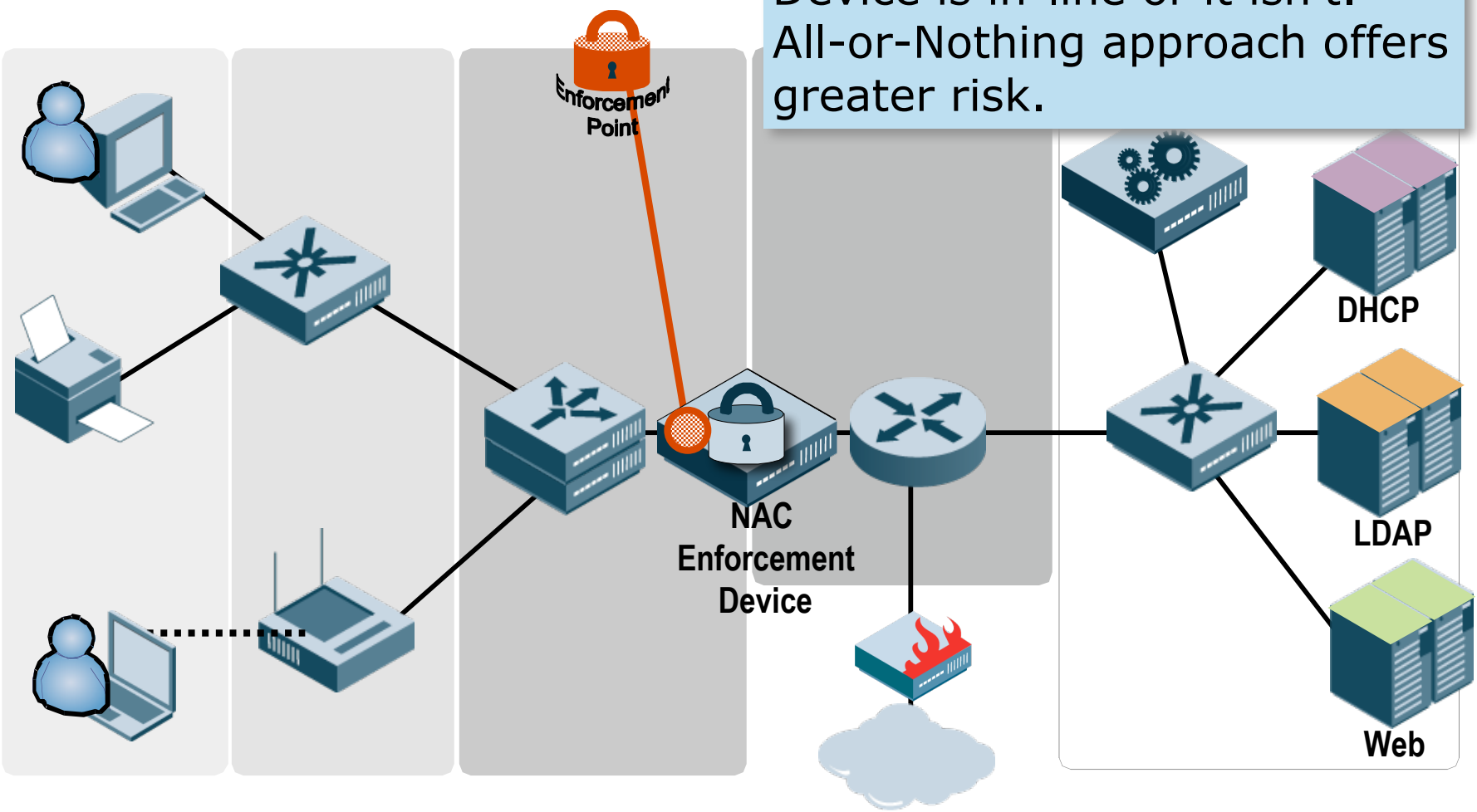
Edge Enforcement Reduces Risk with Port-by-Port deployment

Edge Enforcement allows NAC to be enabled or disabled Switch-by-Switch and Port-by-Port

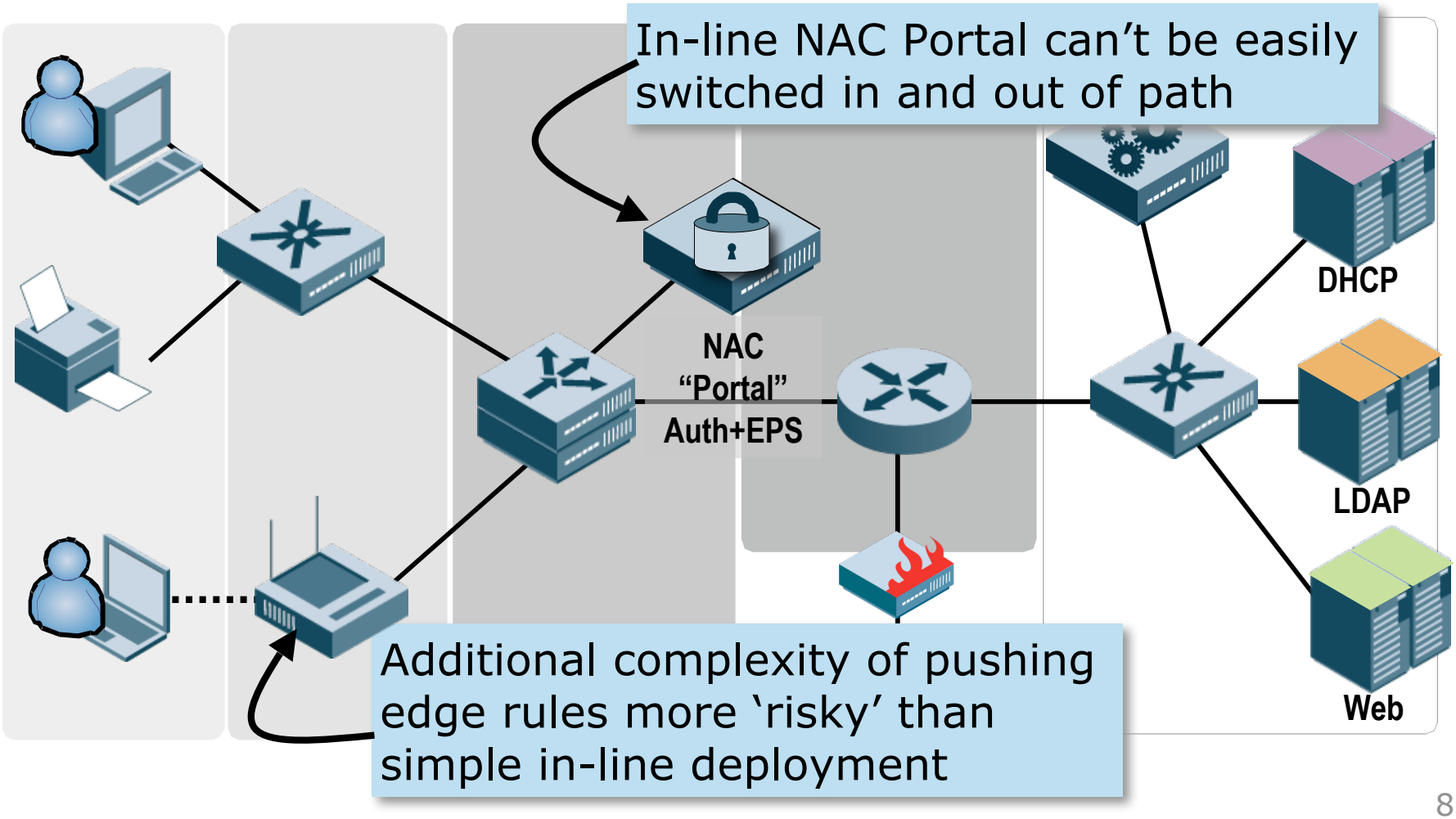


In-line Enforcement Requires Disruptive Changes

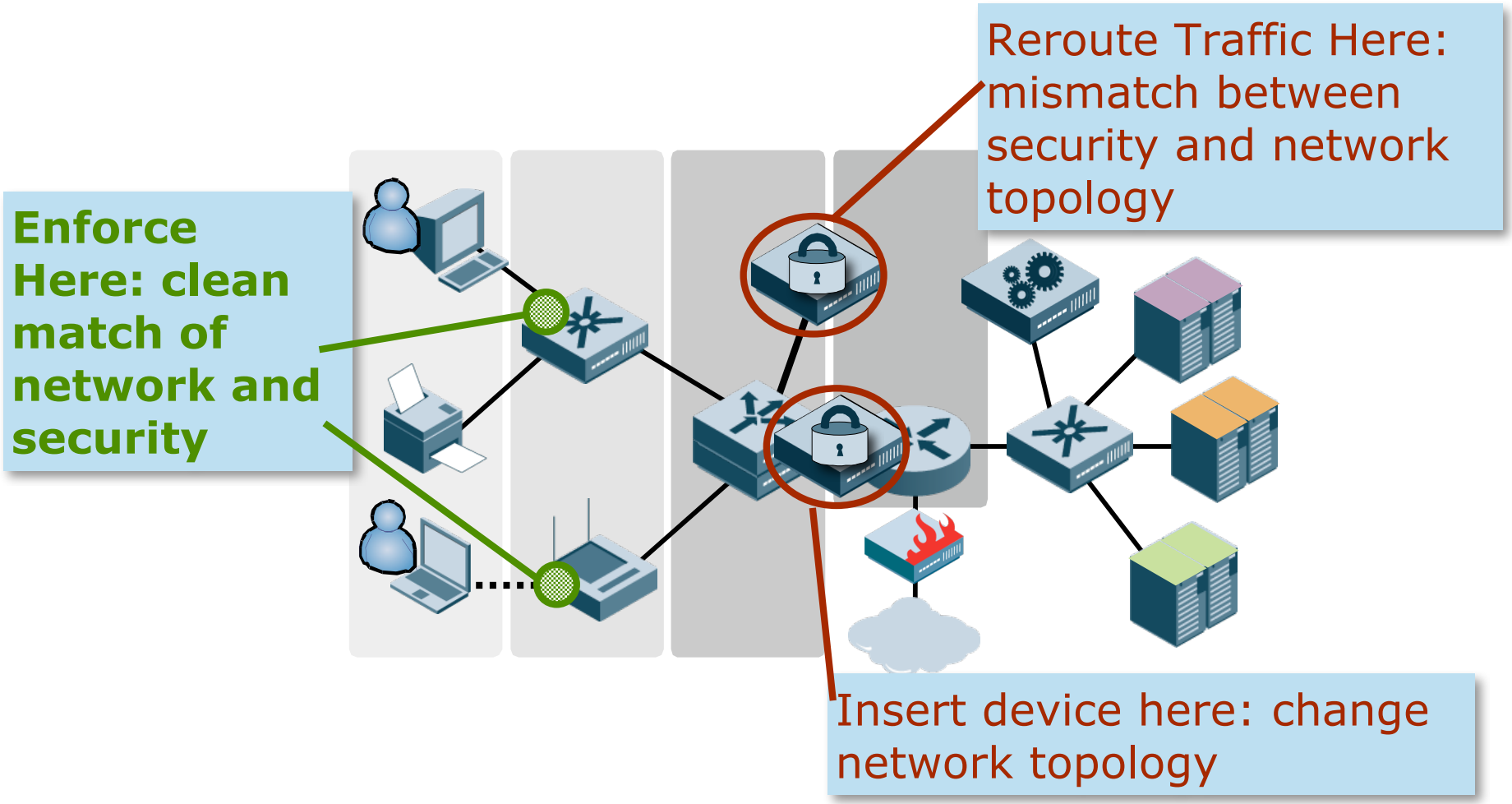
Either the NAC Enforcement Device is in-line or it isn't. All-or-Nothing approach offers greater risk.



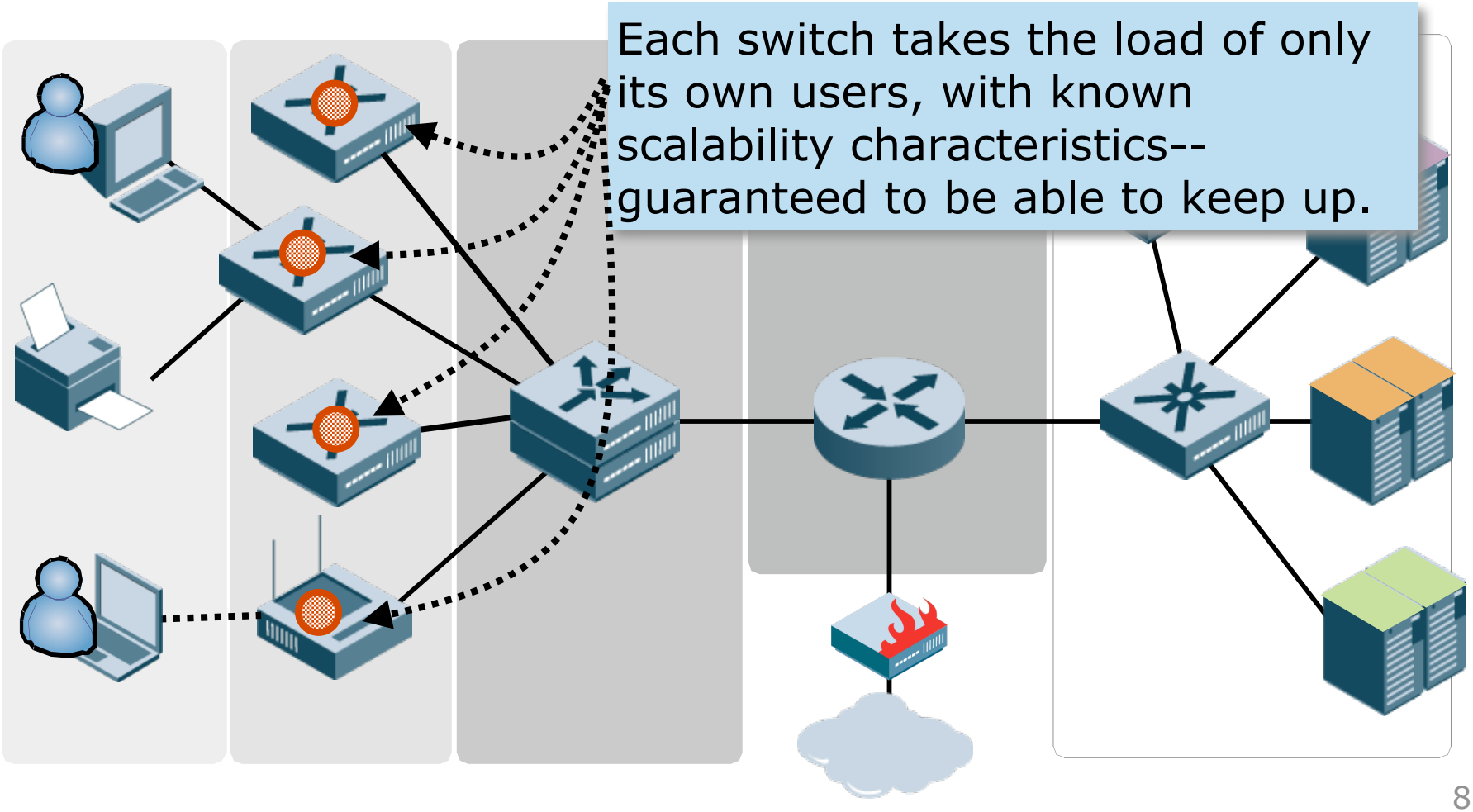
Hybrid Enforcement Methods Combine Drawbacks of In-Line and Edge



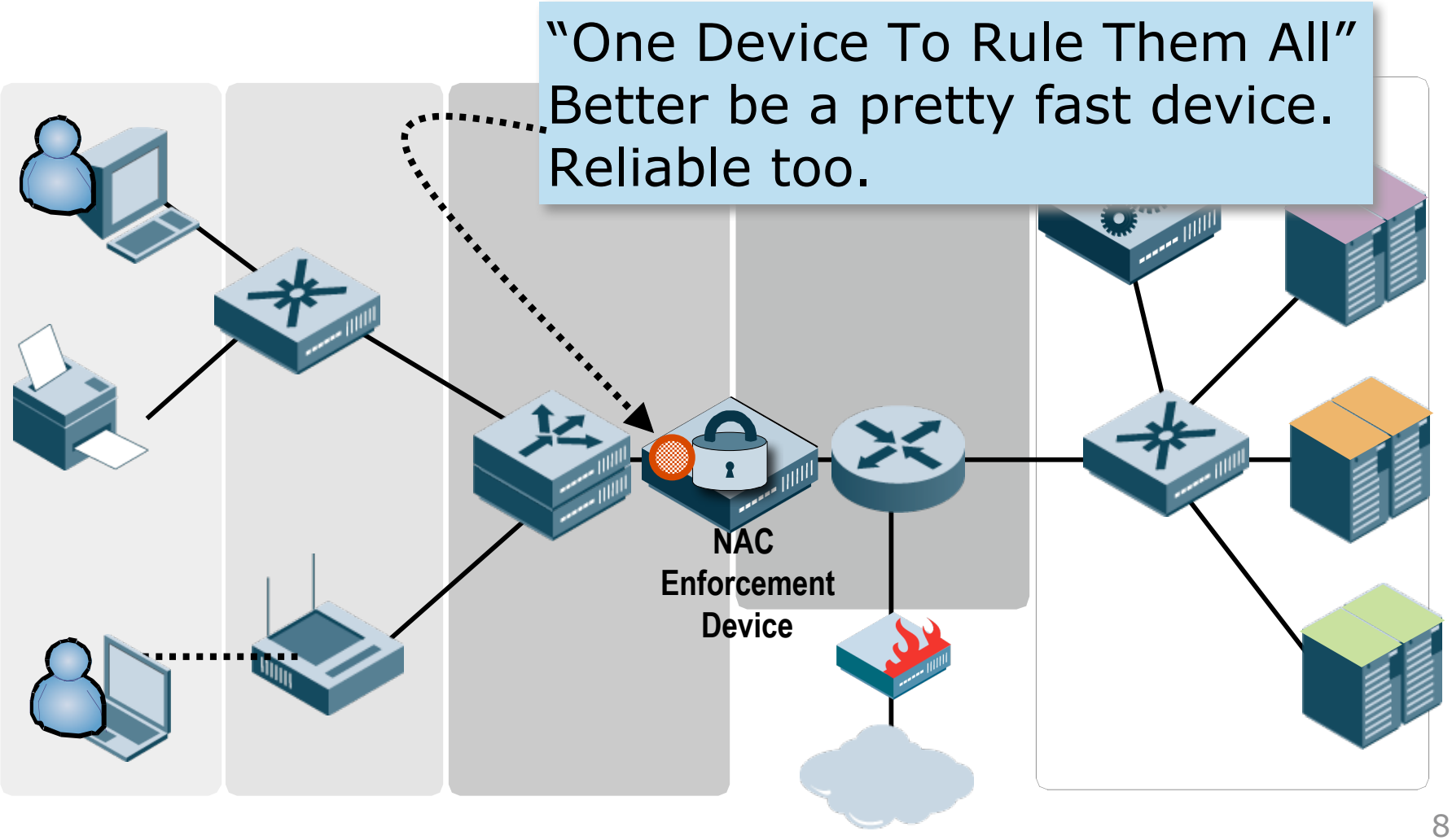
A Pragmatic View Matches Security Topology to Network Topology



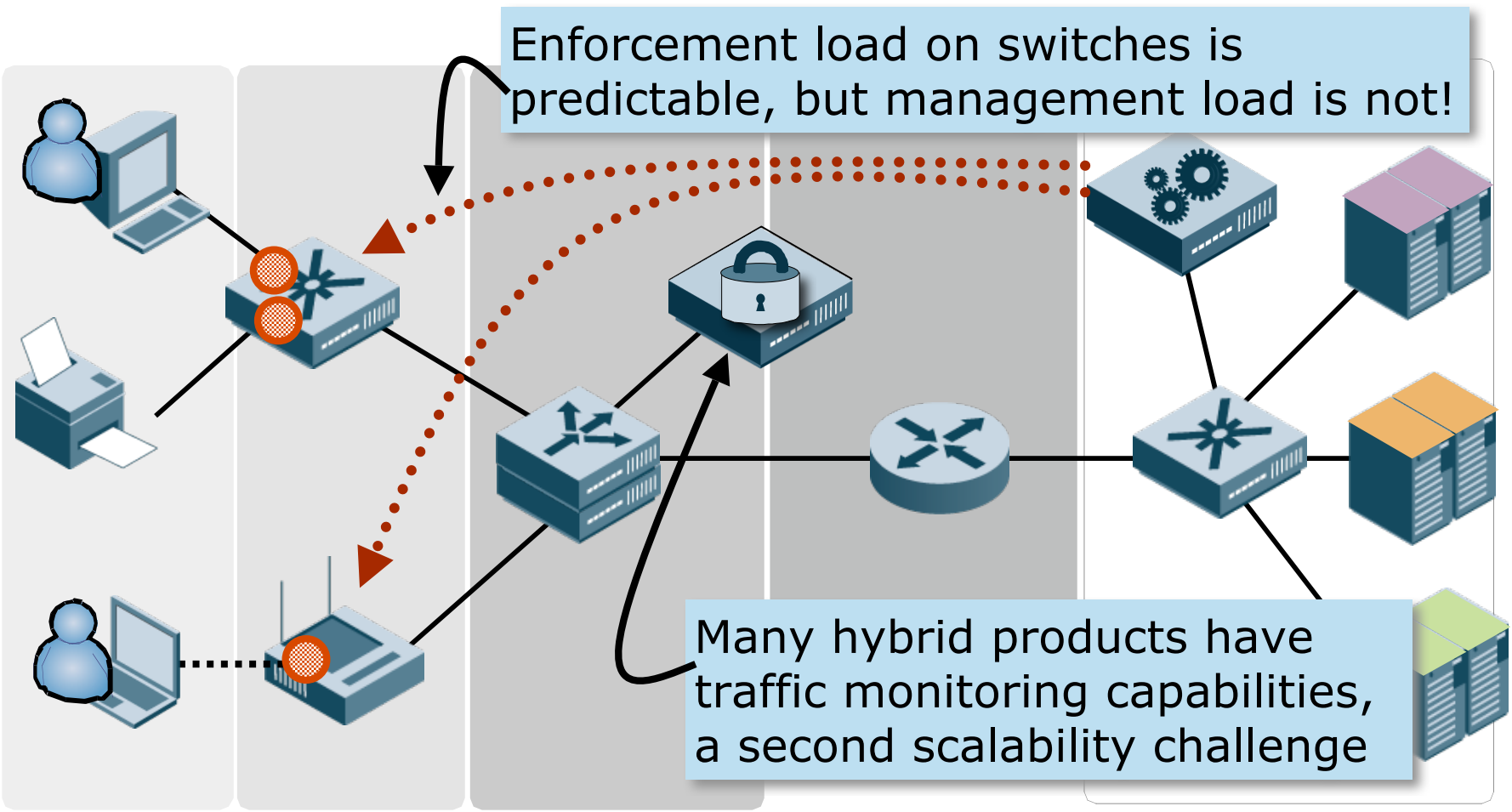
Edge Enforcement Scales Naturally By Distributing Loads



In-line Enforcement Has Obvious Scalability Challenges



Hybrid Enforcement Stresses Switches and NAC Servers Much Harder



Obvious Truism: Less Expensive is Better

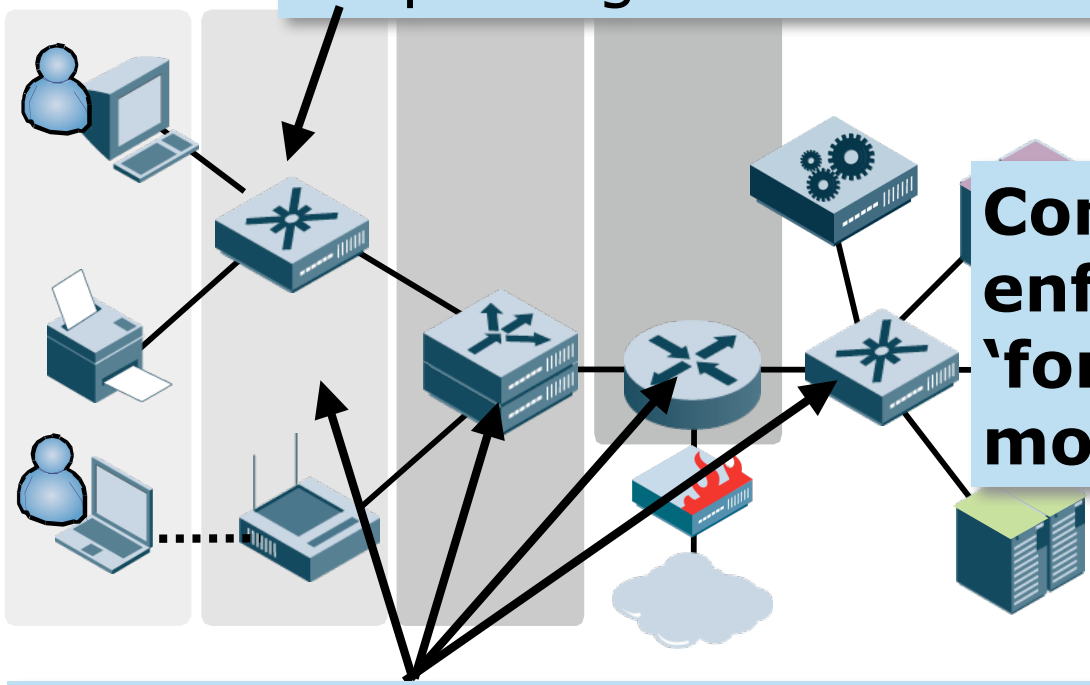
How can you build good NAC solutions that cost less?

❶ Leverage the products you already own, paid for, and are happy with.

❷ Let other people do the heavy lifting

Edge Enforcement uses existing hardware and vendor relationships

Your post-2002 managed switches already support simple edge enforcement

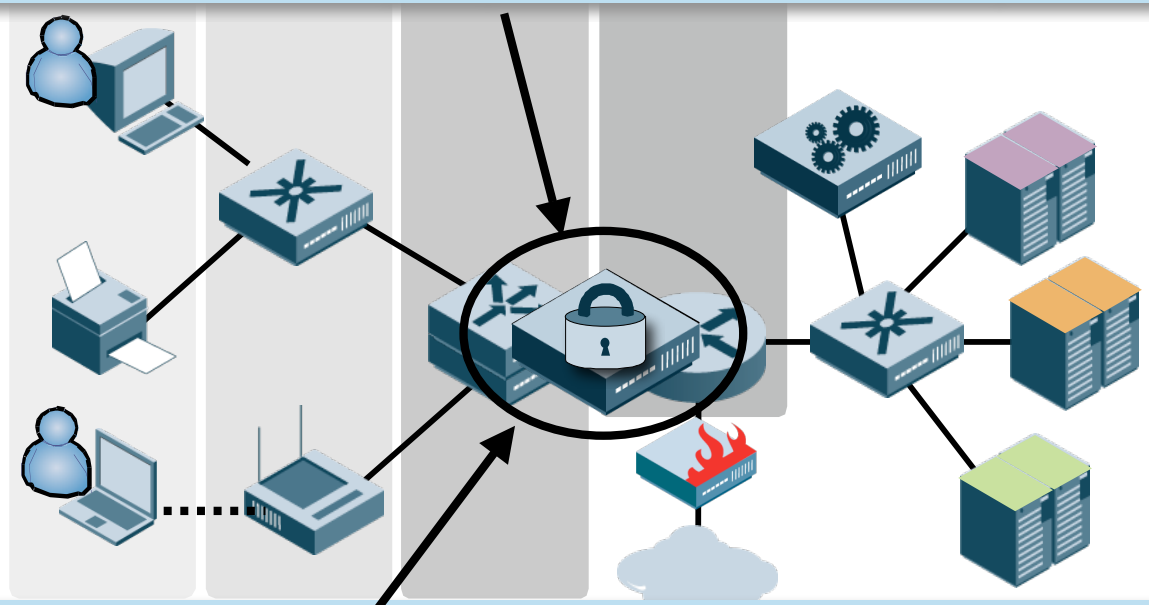


Conclusion: Edge enforcement is <u>not</u> a 'forklift upgrade' for most enterprises

Your switch vendor is improving the security capabilities of their equipment

In-line Enforcement Has Obvious and Not-So-Obvious Costs

You have to buy this multi-gigabit, scalable and highly reliable NAC system



Operational expenses are also increased: this "bump in the wire" requires more training and increased problem resolution time

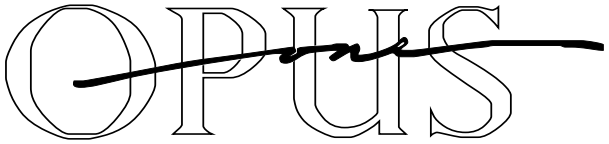
Consider Five Criteria When Evaluating NAC Enforcement

- **<u>Security</u> How "secure" is each option? How well do they meet your security needs?**
- **<u>Flexibility</u> How much flexibility does each approach offer you?**
- **<u>Risk</u> Which approach reduces your risk in deploying new NAC technology?**
- **<u>Scalability</u> What are your performance needs now and in the future?**
- **<u>Cost</u> What are the capital and operational expenses for each option in your network?**

Enforce NAC at:	Edge	Inline	Hybrid (Edge + Inline)	Layer 3 (Protocol)
Security	Greatest level of security; enforce at point of access;tied to authentication	Progressively less security; enforcement occurs deeper in the network with inline/protocol; authentication "far" from device; leaves more areas vulnerable/uncontrolled.		
Flexibility	Greatest flexibility; protocol independent	Progressively less flexible enforcement method; dependent on behavior of a single protocol (*e.g.*, DHCP or IPv4 only)		
Risk	Least intrusive; granular deployment lowers risk of network disruption	Changes to network topology and/or protocols are more risky and intrusive with limited back-out capability (usually "all or nothing") which increases potential for network disruption or failure		
Scalability	Most scalable; load of enforcement is spread across network fabric for highest performance	Inline nature of enforcement reduces scalability and has significant impact on cost of equipment and performance bottlenecks		"Dual subnet" complexity reduces scalability by requiring full overlay network
Cost	Very cost-effective; leverages security functions of existing infrastructure to reduce capital and operational expenses	Inline enforcement has highest capital cost by requiring high-end custom hardware; operational costs higher because of troubleshooting issues		Capital cost low, but potential for higher operational expenses for debugging and troubleshooting; fails to leverage existing infrastructure

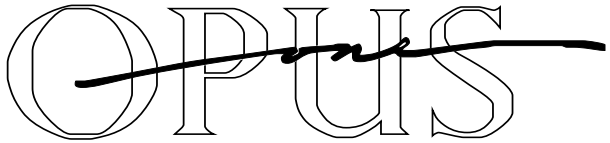
Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com



Network Access Control Part 4: Extremely Real World NAC

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

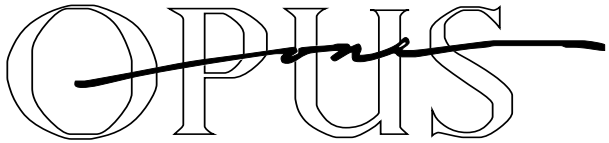


Our Embattled NAC Veterans Are…

- **Brendan O'Connell (Cisco)**
- **Chester Wisniewski (Sophos)**
- **Denzil Wessels (Juniper)**
- **Manlio Vecchiet (Microsoft)**
- **Steve Hanna (TCG)**

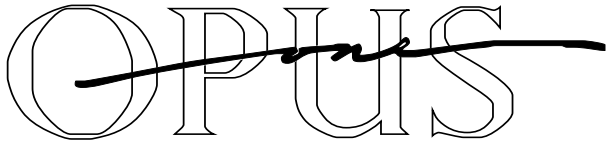
Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com



Network Access Control
Part 5: Standards-based NAC

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



For more information on CNAC & TNC Testing done by Opus One

NETWORKWORLD

Search / DocFinder

GET UP TO SPEED FAST ON
Network Access Control

HOME
RESEARCH CENTERS
Security
Anti-Virus
Firewalls / VPN / Intrusion
Spam / Phishing
Wireless Security
+ LANs & Routers
+ VoIP & Convergence
+ Network Management
+ Wireless & Mobile
+ Operating Systems
+ Servers & Data Center
+ Applications
+ Storage
+ Wide Area Network
+ Small Business Networking
Cisco Subnet
Microsoft Subnet
EVENTS

Security
NAC Cram Session | Anti-Virus | Firewalls / VPN / Intrusion | Spam / Phishing | Wirele

NAC passes basic tests

NETWORKWORLD CLEAR CHOICE

Cisco, TCG schemes work for simple deployments, but complex scenarios are another story

- Authentication: A snap with XP
- End point security: Cisco TCG deliver
- Enforcement: Tools fall short
- Management: Can be a headache

STATUS

What can NAC do for you now?

Test of 30 products shows benefits, limitations of existing Cisco- and standards-based NAC schemes

Clear Choice Tests By *Joel Snyder*, *Network World, 04/19/07*

With a virtual lock on the Ethernet switching market, any enterprise IT manager has to consider Cisco's product line as at least one network-access control option.

But how does a Cisco-controlled NAC deployment hold up against the more industry standards-based one offered up by the Trusted Network Connect (TNC) working group of the Trusted Computing Group (TCG) and backed by Cisco competitor Juniper Networks?

Other stories on this topic

CLEAR CHOICE TEST

Does a good SSL VPN provide good NAC?

Why Vista is missing from NAC landscape?

NAC all-in-one test on the

http://www.networkworld.com/reviews/2007/041907-nac-intro.html

Same method of testing: different products

NETWORKWORLD

Search / DocFinder

Security

Whitepapers | Guides and Reports | Webcasts | Videos | Buyer's Guide

Read your issue online

HOME

RESEARCH CENTERS

Security
- Anti-Virus / Spyware / Spam
- Compliance & Regulation
- Firewalls / VPN / Intrusion
- NAC
- Services
- Cisco Security Watch
- Microsoft Security Watch

+ LANs & WANs
+ VoIP & Convergence
+ Network Management
+ Wireless & Mobile
+ Software
+ Data Center

CLEAR CHOICE TEST: NAC

NAC alternatives hit the mark | NetResults | Test archive

Inside this test package

13 product summaries Jump to a summary

Main story links Jump to a link

NAC alternatives hit the mark

Symantec tops Juniper, Cisco and Check Point in test of 13 NAC point products

Clear Choice Tests *By Mandy Andress, Network World, 07/30/07*

Comments (8) Print article

Network-access control is a buzzword of epic proportion. And as is the case with much of larger-than-life industry vernacular, products with even the slightest aspect of access control are being pitched by their makers as integral components of the NAC fray.

http://www.networkworld.com/reviews/2007/073007-test-nac-main.html

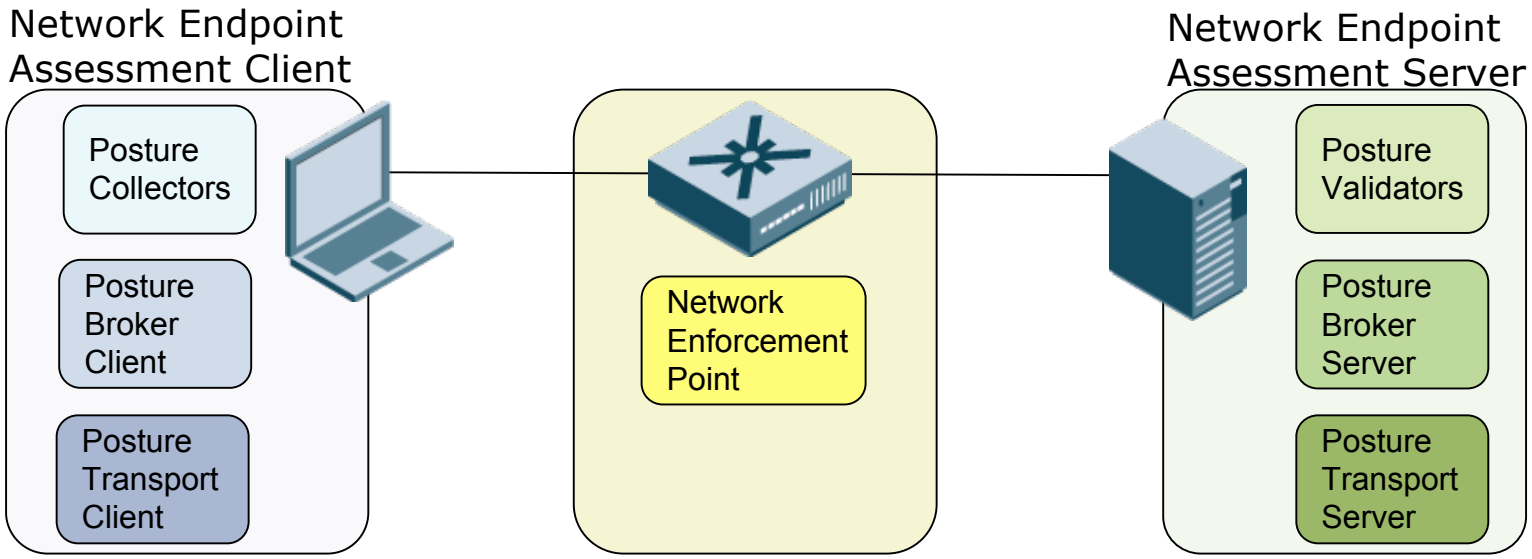
Disclaimer!

- **I don't work for <u>any</u> of the companies involved, so**
  - **I am solely responsible for any errors of any kind**
  - **None of this represents the official position of anyone**
- **Slides are selected from company decks, so**
  - **When value statements are made, that's the company talking, not me**
- **This material is all <u>public</u> and <u>released</u>**
  - **No NDA material from you to me, or from me to you**

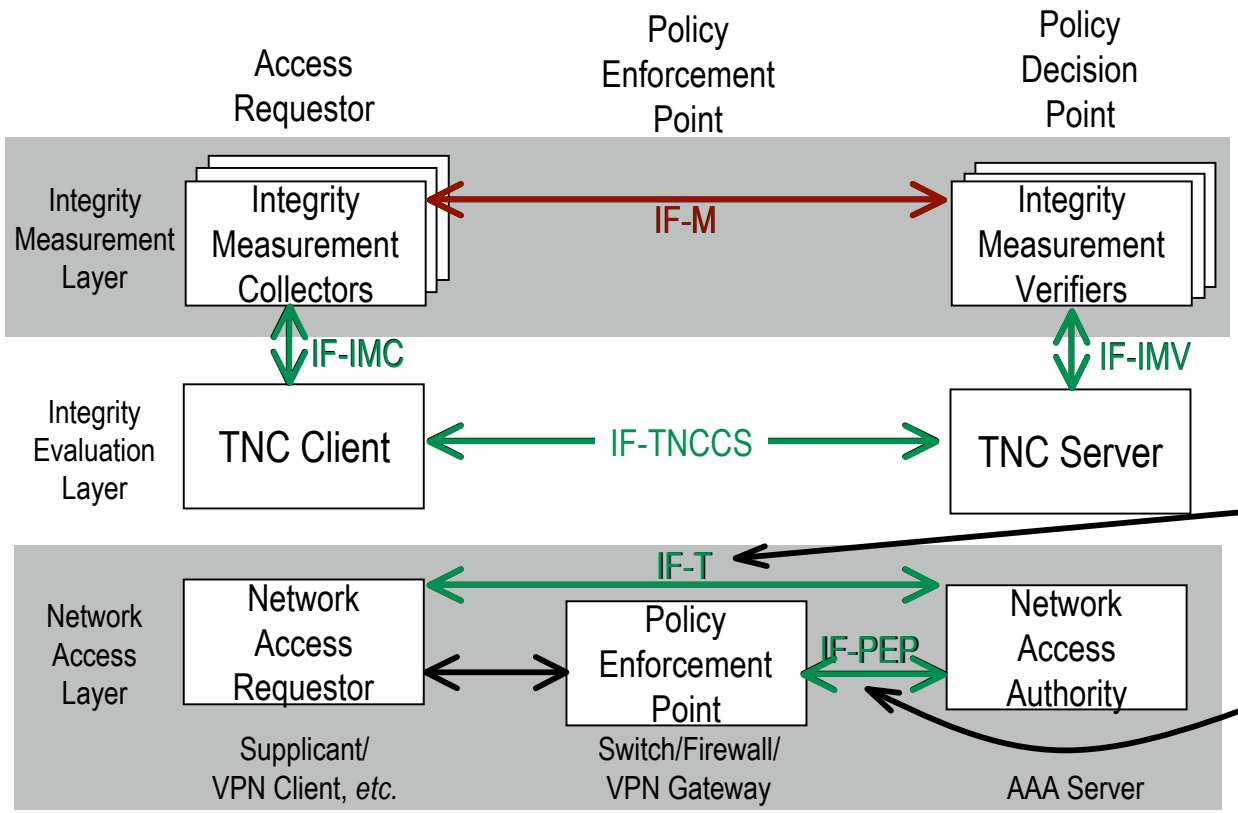
Trusted Computing Group offers a standards-based alternative

- **The politics of it all are breathtaking**
- **Cisco's refusal to play nice with everyone else (TCG and Microsoft) is doing more harm to NAC by failure to cooperate …**
  - **…than even the most senior Gartner analyst**

With TNC, the question is… what do we have today?



Trusted Computing Group's Trusted Network Connect Status



✓ **Done**

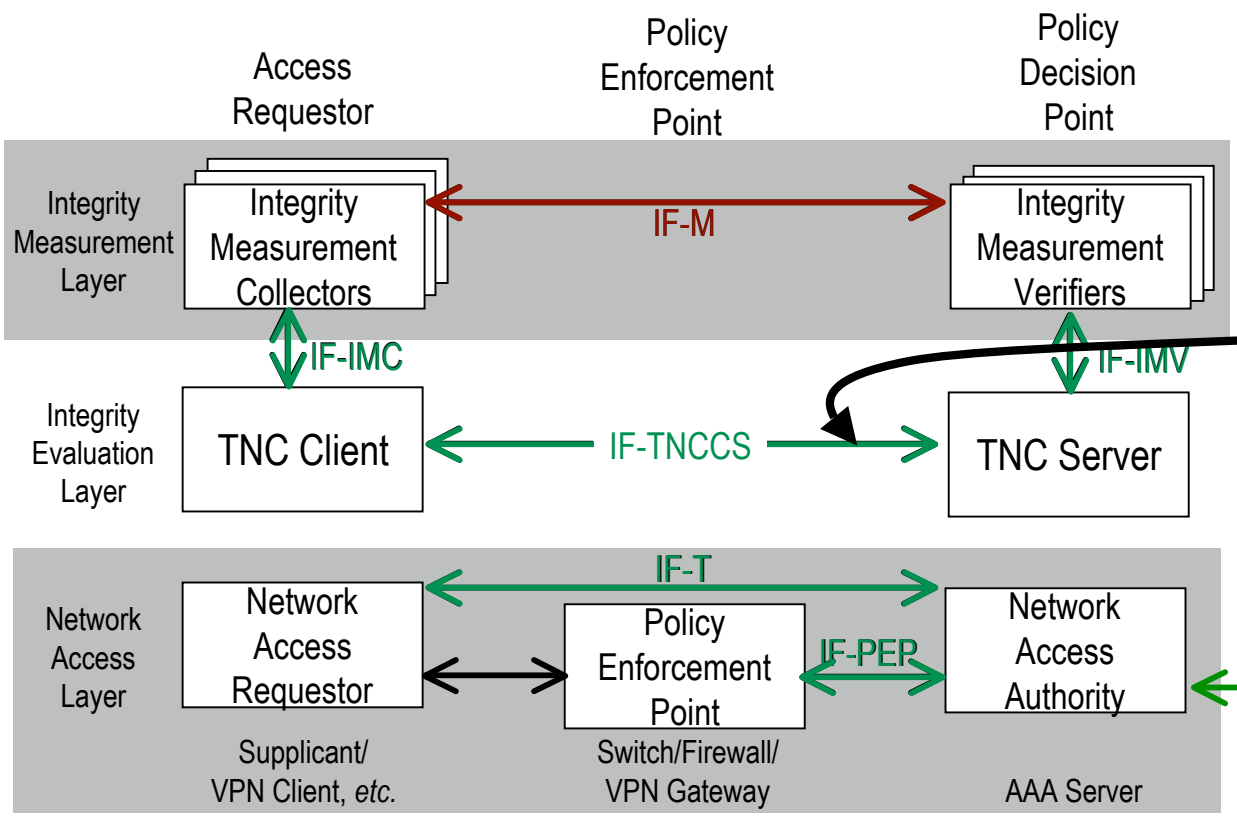
✗ **Not Done**

Defined for Tunneled EAP

Defined for RADIUS with 3 enforcement models (go/no-go, VLAN, ACL)

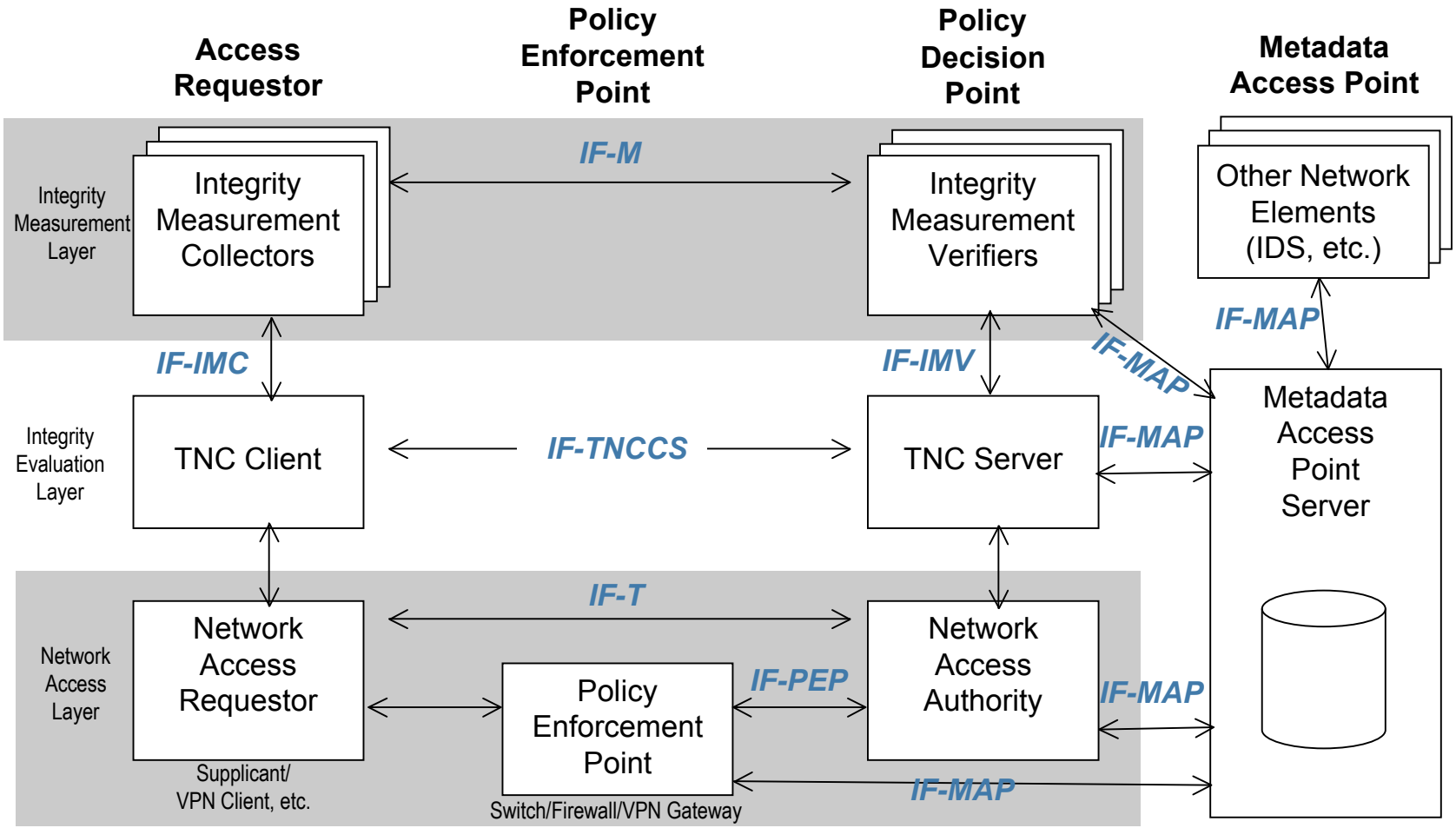
Developments in the TCG front are very interesting…

Vista's *Statement of Health* protocol is added as a TNC-allowed TNCCS protocol (which also will extend to XP)

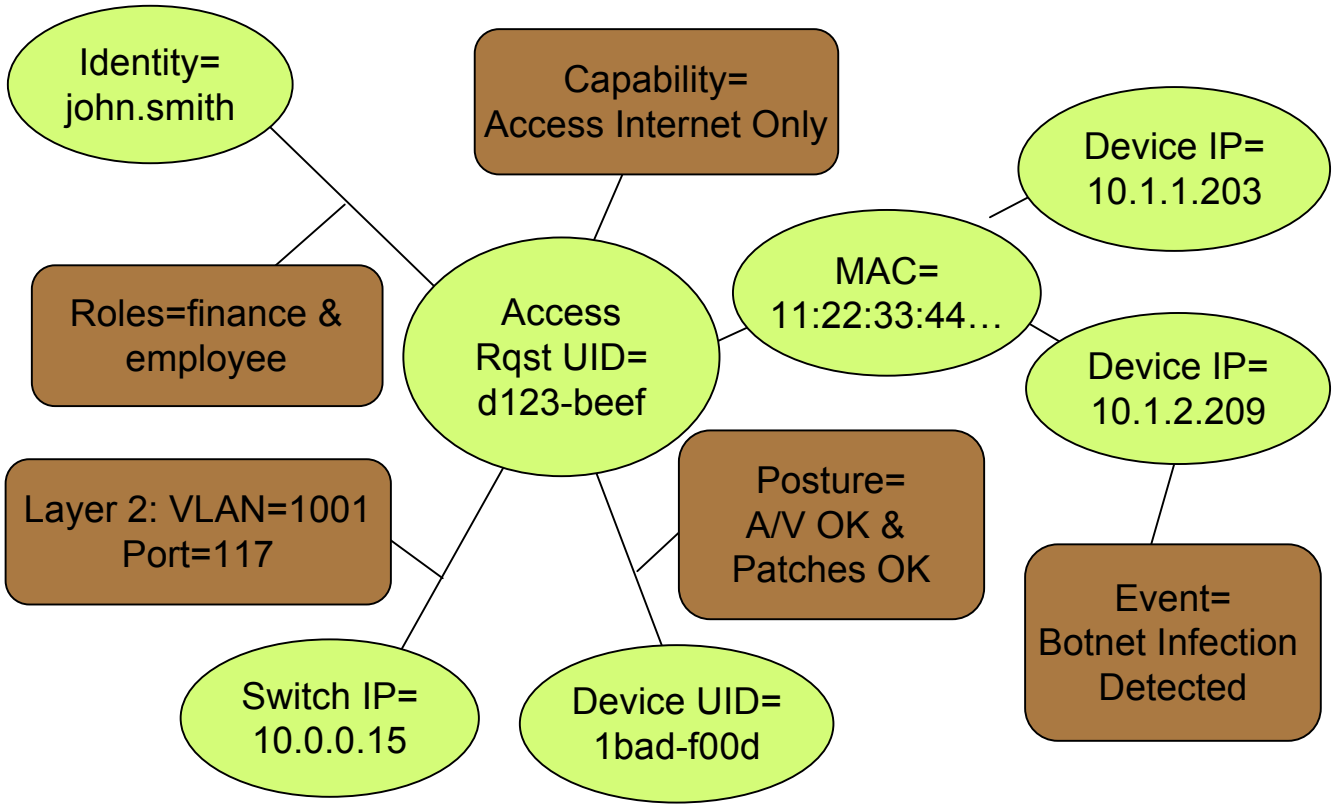


IF-MAP allows external devices (think SIM and IPS) to talk to the policy decision point

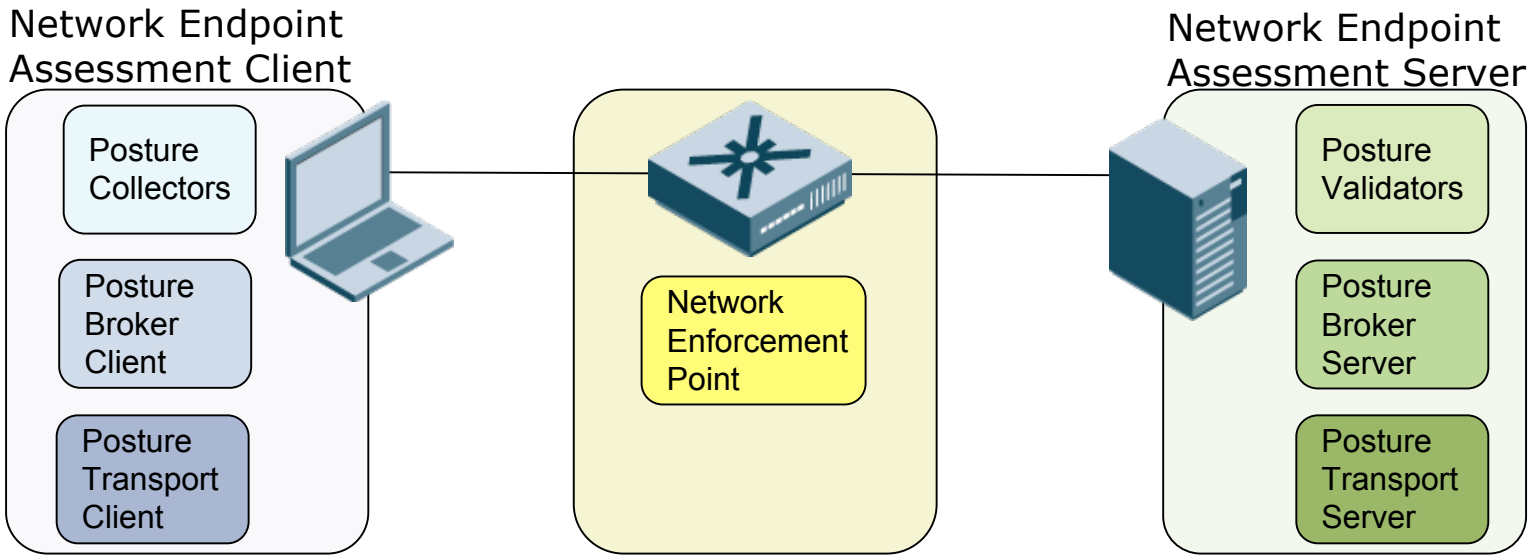
IF-MAP is announced today!



What Might Metadata Look Like?



With TCG, vendor ecosystem talking about products is fragile (or is it robust?)

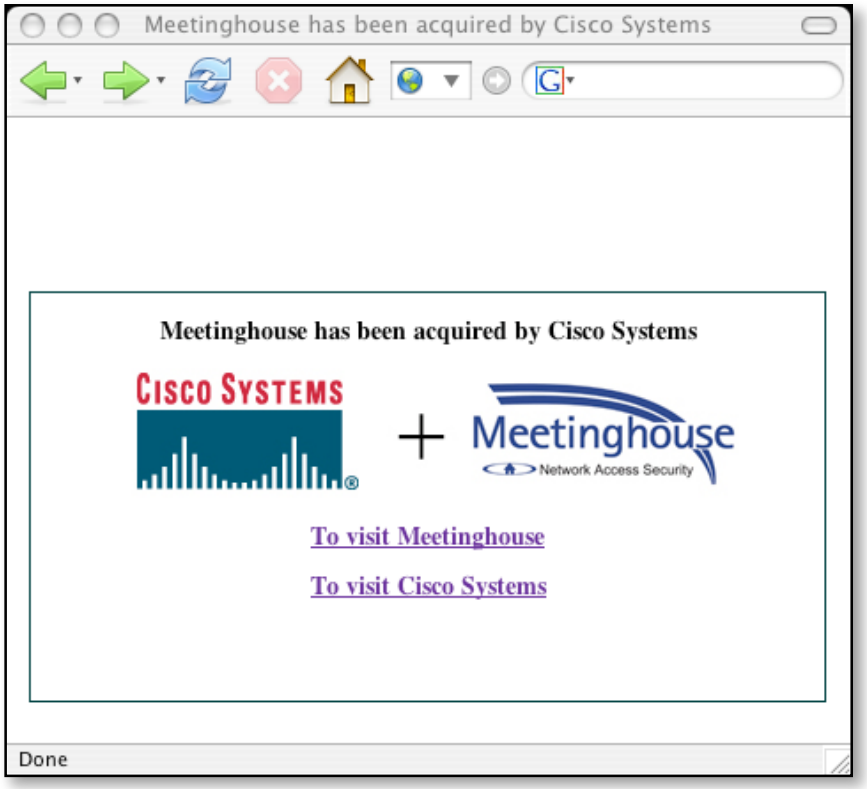


Symantec, McAfee, IBM, Wave, Juniper, Patchlink, OpenSEA, Microsoft, Q1 Labs, ID Engines, Avenda

Everybody on Earth (Aruba, Cisco, Extreme, Enterasys, HP, Consentry, Nevis, Nortel, Trapeze, etc.)

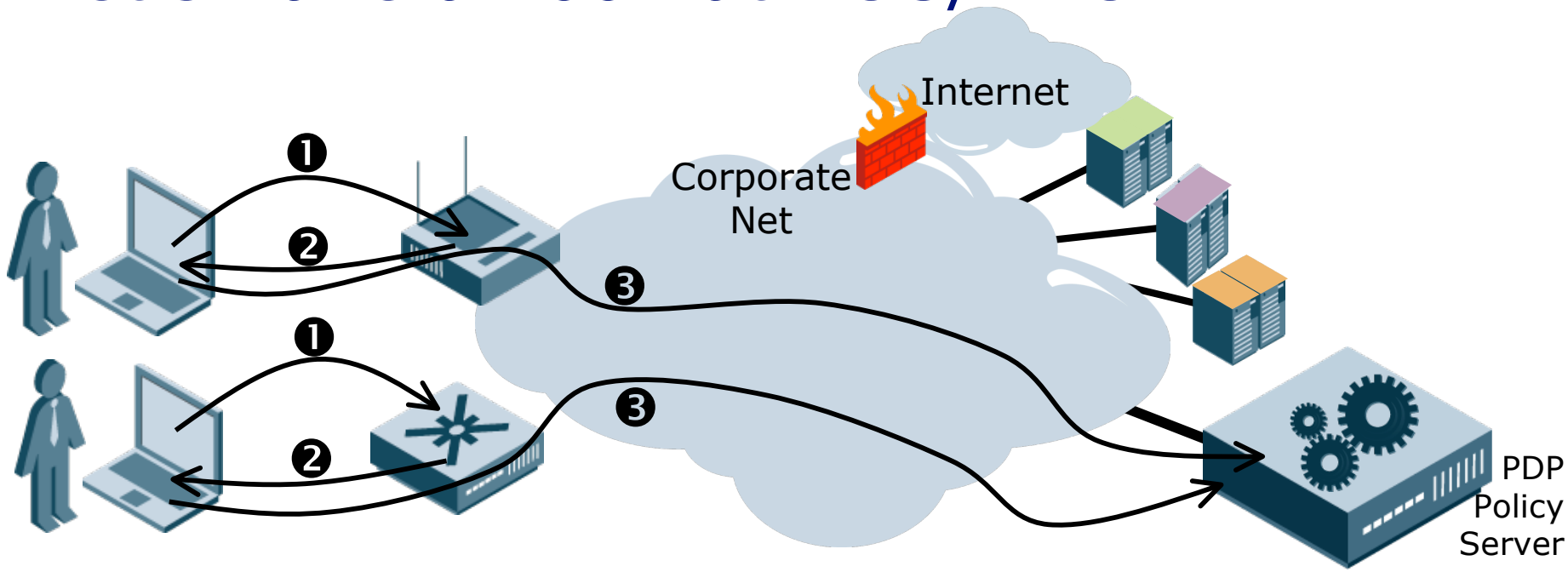
Juniper, OSC Radiator, Microsoft, ID Engines, Avenda

Wait… Didn't Meetinghouse Data Communications get bought?



- Q. Will the Cisco Secure Services Client become a part of the Trusted Computing Group (TCG) Trusted Network Connect (TNC) working group?
- A. Cisco continues to have no plans to join the TCG, which is a requirement to participate in the TNC working group. However, relative to "industry initiatives," Cisco remains focused on addressing customer requirements. Cisco monitors closely the activities of industry groups and actively participates in those groups that will bring the greatest benefits to customers.

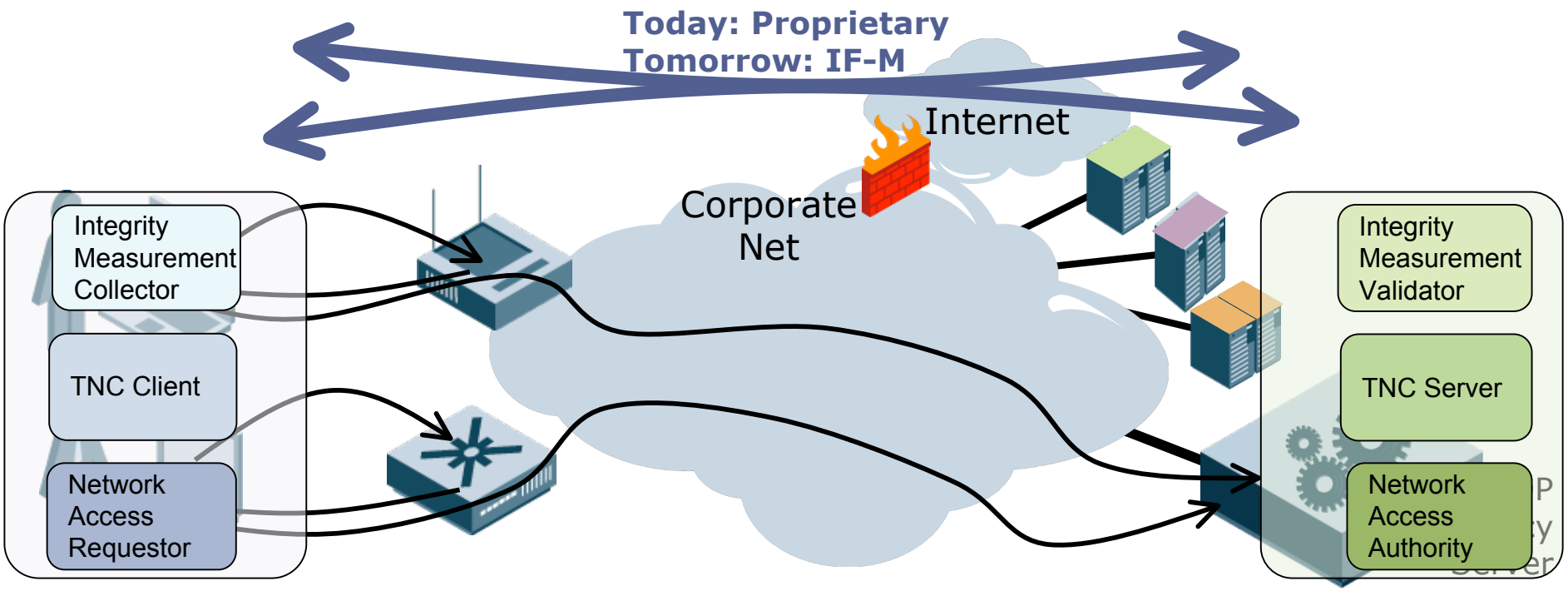
Let's Take a Look at TCG/TNC



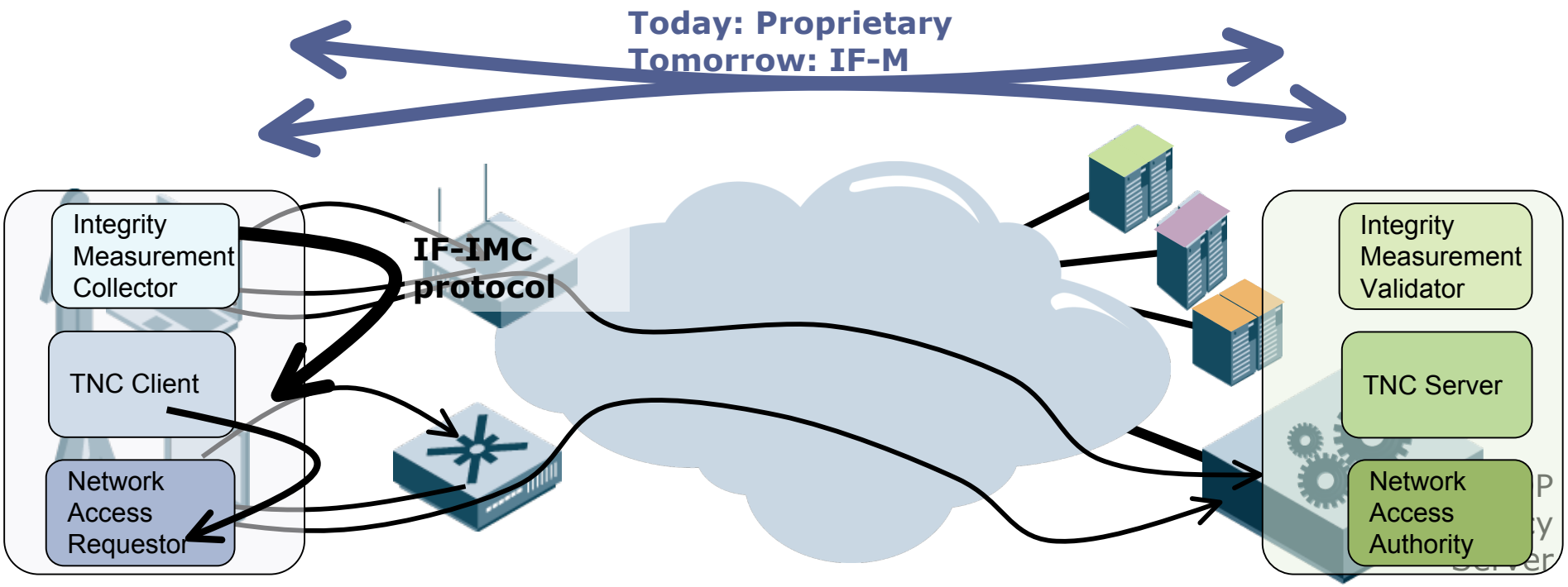
❶ User brings up link (or associates with AP)

❷ AP/Switch starts 802.1X (EAP) for authentication

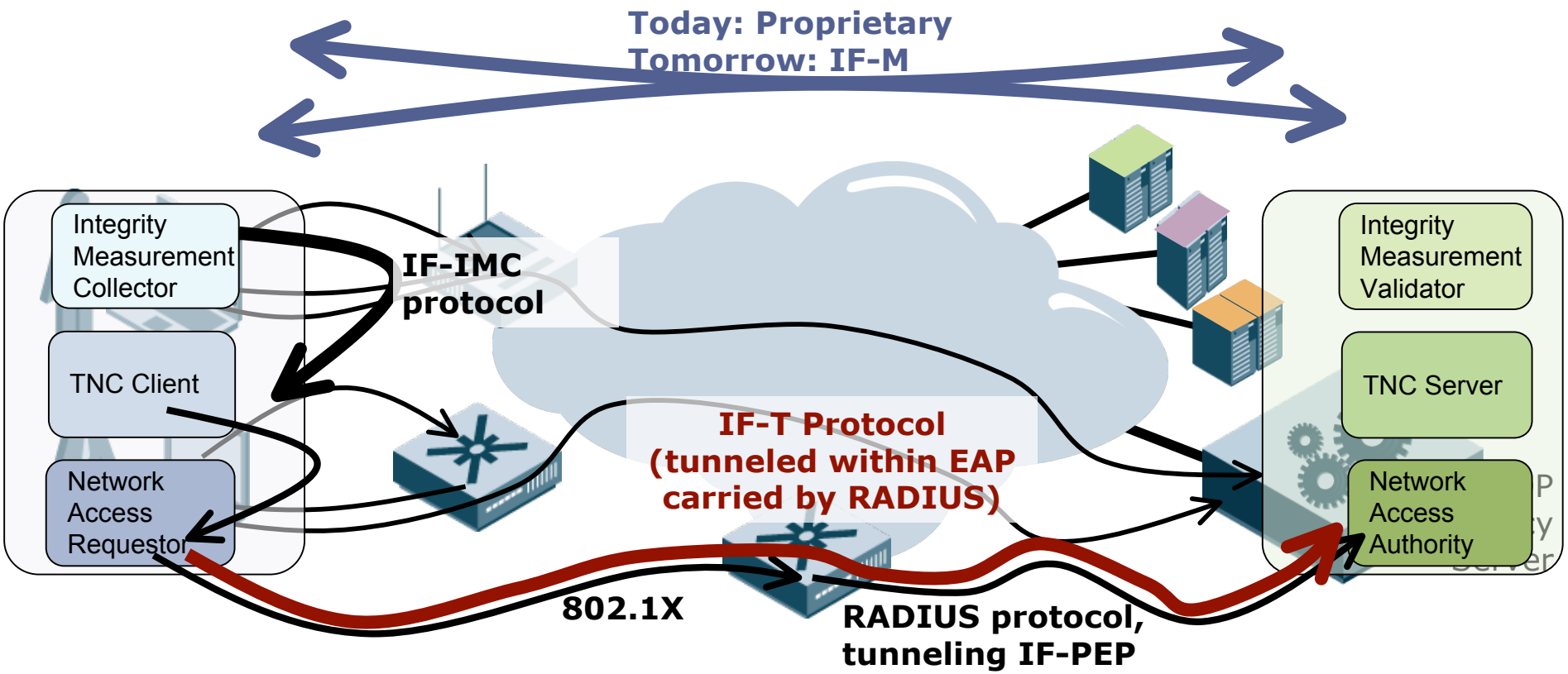
❸ Network Access Requestor (802.1X) client "connects" over 802.1X/EAP tunnel to PDP



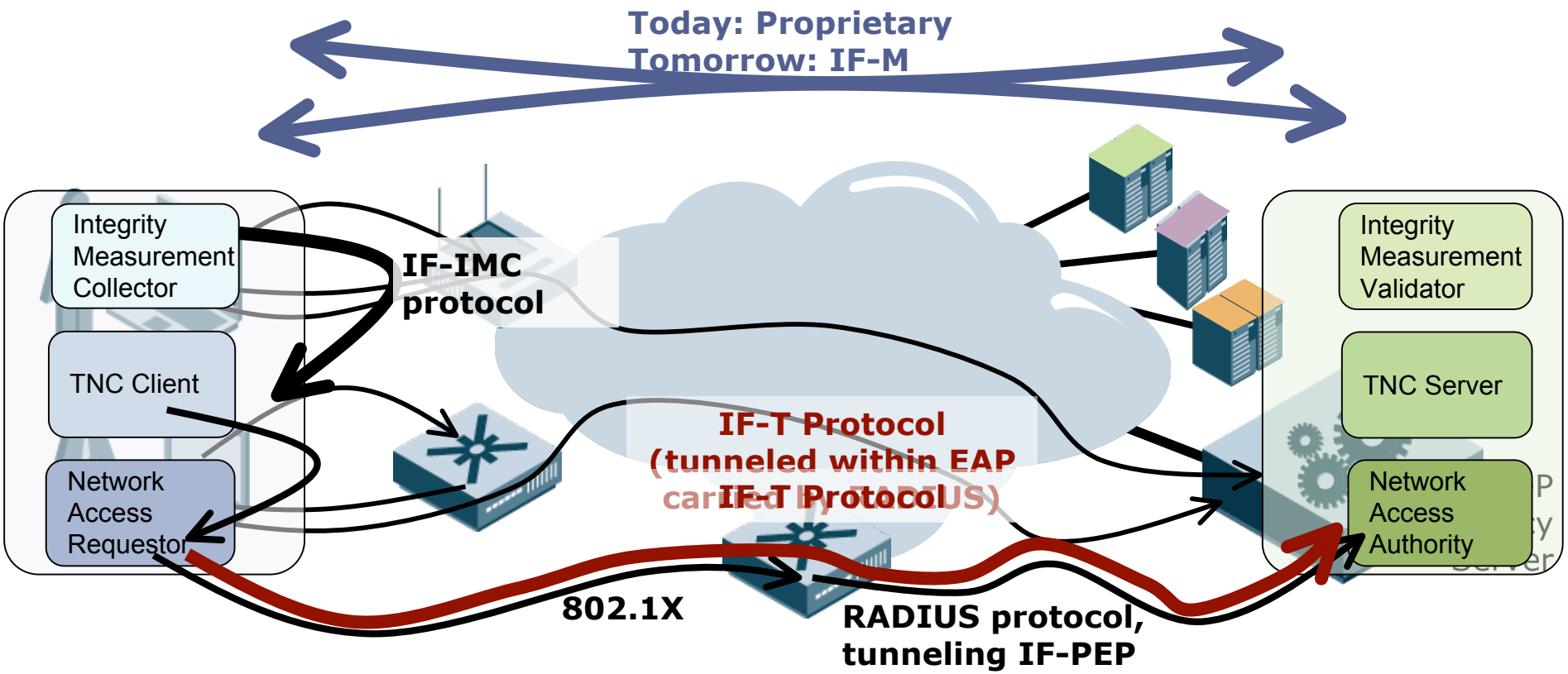
- Integrity Measurement Collectors are on the client; Integrity Measurement Verifiers are within (virtually) the Policy Decision Point.
- IMVs talk to IMCs using a proprietary protocol… but they don't talk to each other directly.

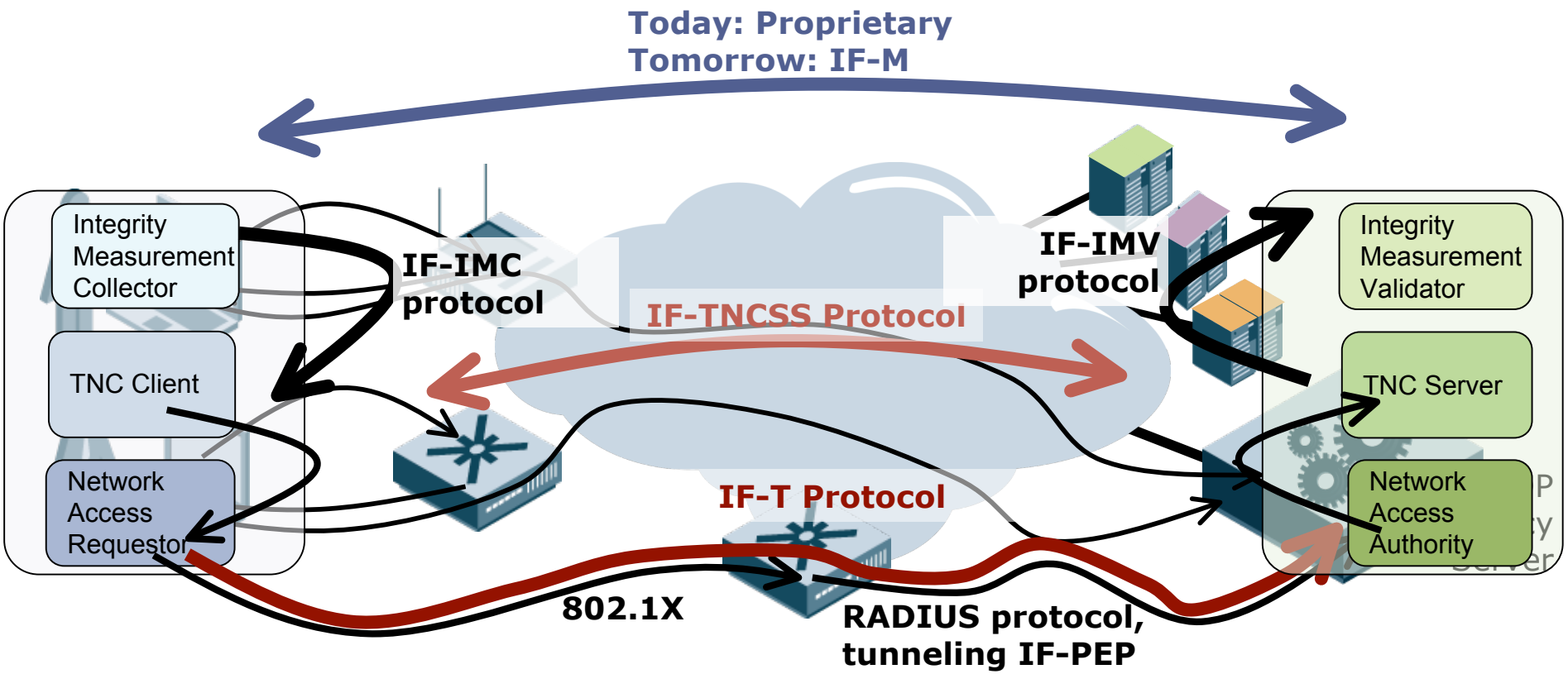


- TNC clients ("brokers" is a better word) collect IMC data using IF-IMC API
- TNC Clients generally have their own 802.1X "NAR" included, although this is not required

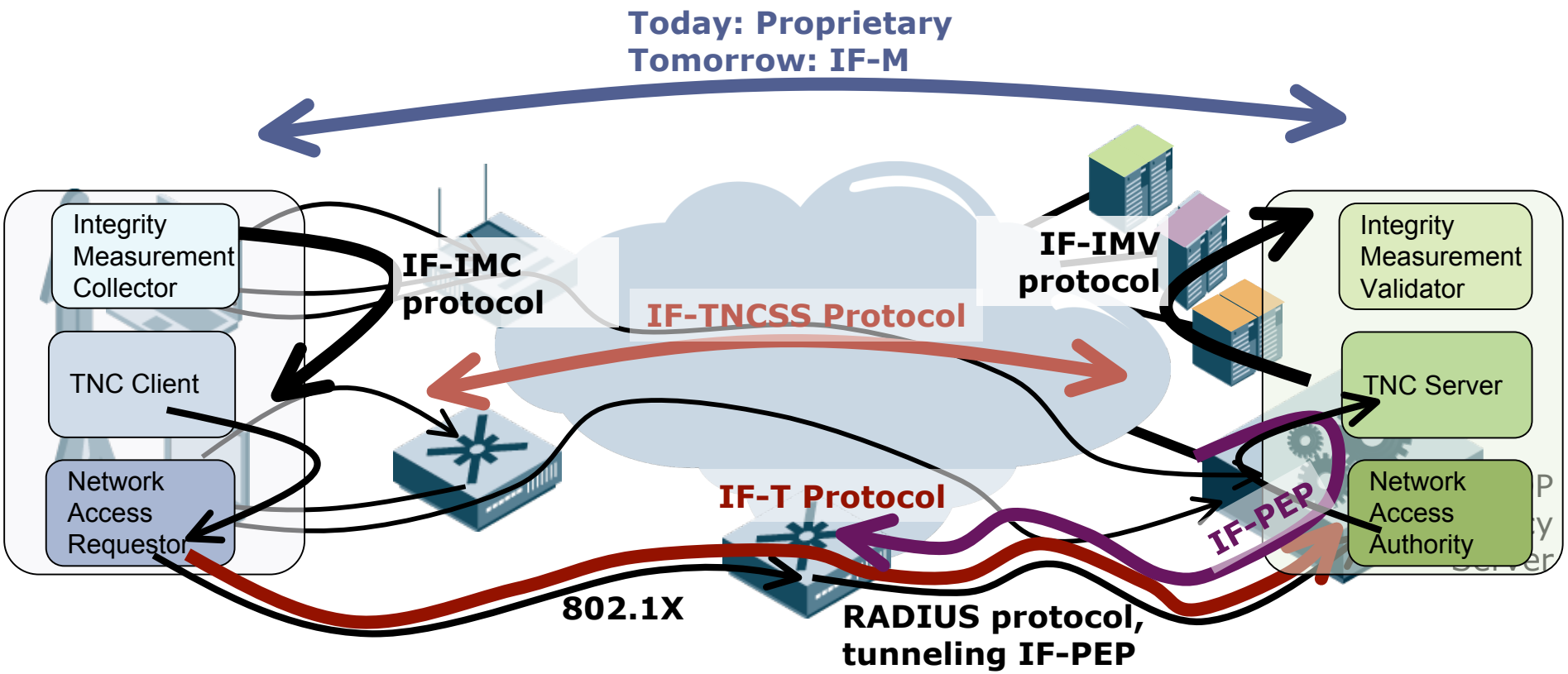


- 802.1X (or IPSec IKEv2) from client to edge
- RADIUS from edge to Policy Decision Point
- IF-T from end-to-end tunneled and secured by EAP, carried by RADIUS, gets the IMC talking to the IMV

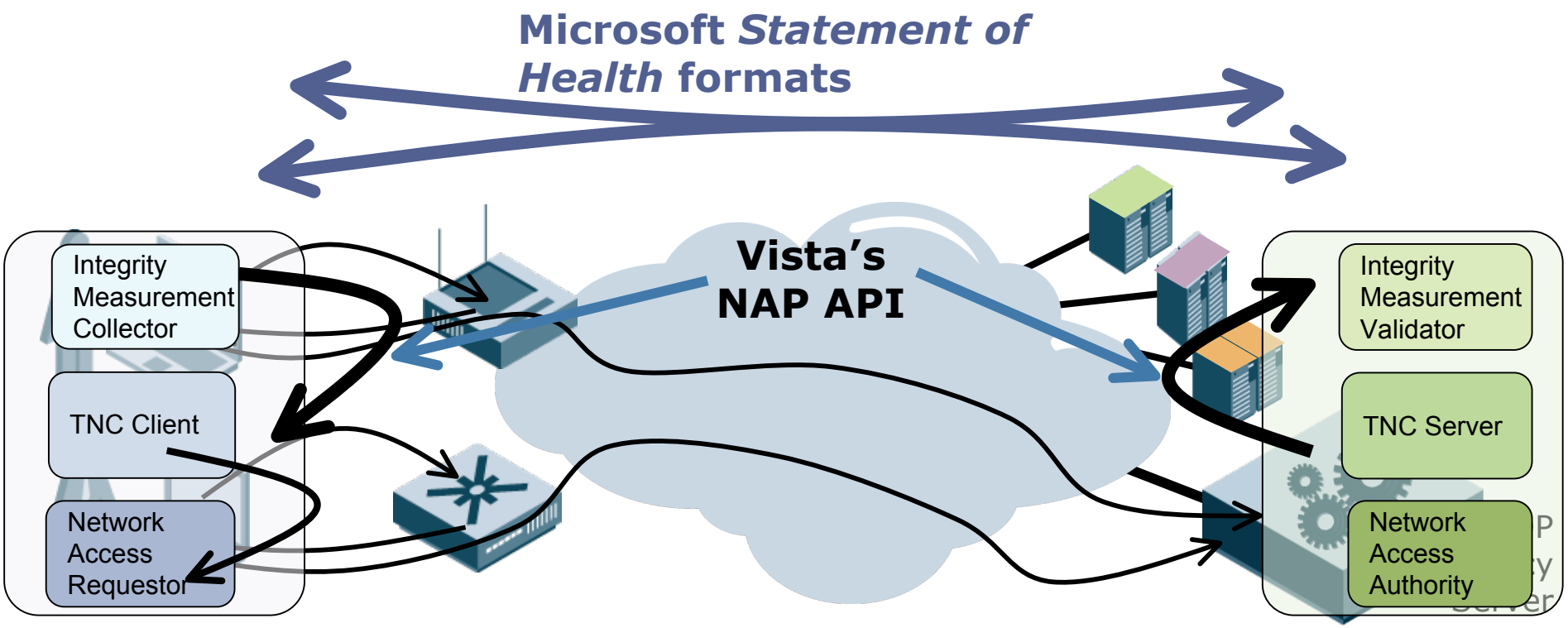

Today: Proprietary
Tomorrow: IF-M
Integrity Measurement Collector
TNC Client
Network Access Requestor
IF-IMC protocol
IF-T Protocol
(tunneled within EAP carried by RADIUS)
IF-T Protocol
802.1X
RADIUS protocol, tunneling IF-PEP
Integrity Measurement Validator
TNC Server
Network Access Authority



- RADIUS servers include TNC Server (broker) in PDP
- The TNC brokers use IF-TNCSS (tunneled in EAP) to tunnel IMV to IMC communications
- IF-IMV completes the chain from IMC to IMV via …

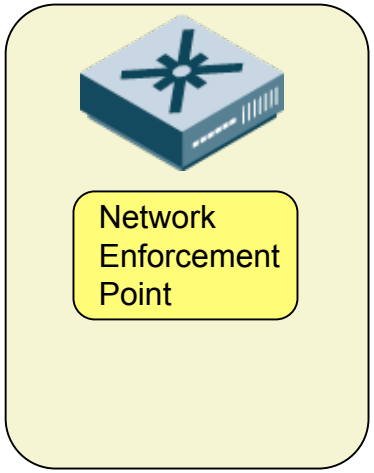


- When the policy decision is made, the RADIUS server (NAA) communicates policy to enforcement point



- With Vista/XPsp3 and built-in NAP, the Microsoft protocols will run above the NAR/NAA (an alternative IF-TNCCS and the basis of future protocol work in TNC).
- Vista has its own 802.1X wired/wireless supplicant, so the NAR is included (using PEAPv0 for encapsulation)

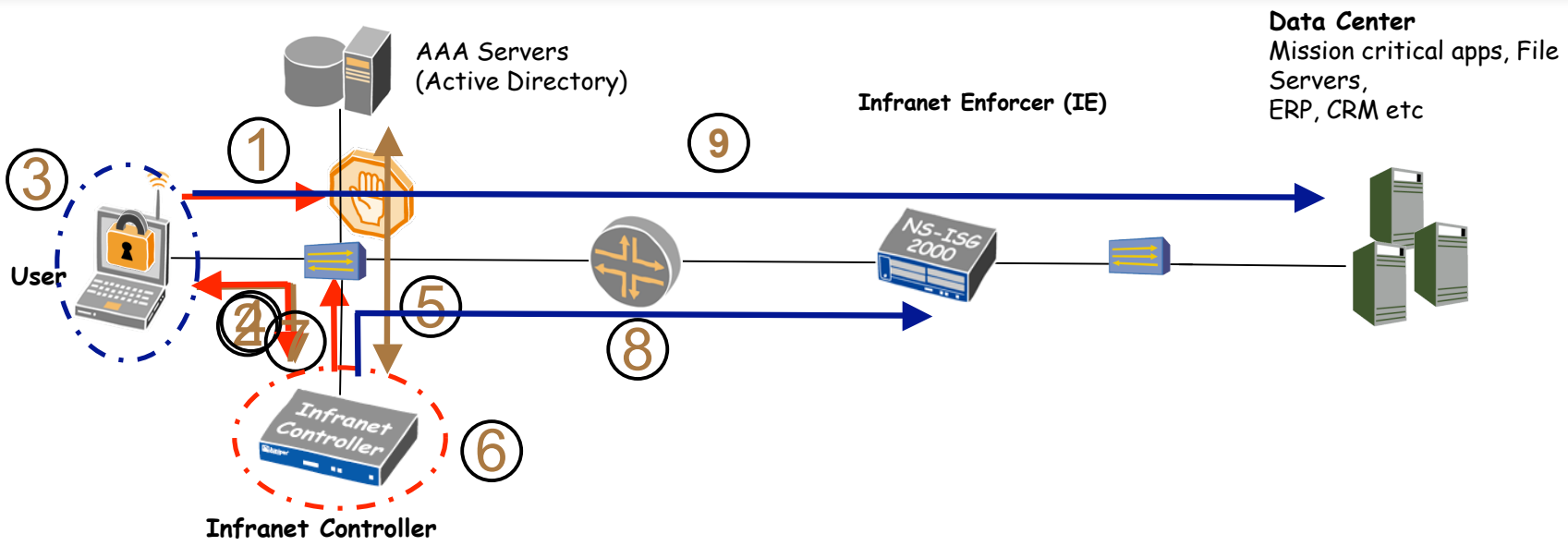
So, what kind of policy are we talking about?



- **TNC suggests Go/No-Go, VLANs, and ACLs**
- **This is great, because now (almost) every 802.1X switch (even Cisco switches!) is part of a standards-based NAC solution**
- **Assuming you wanted VLANs**

TCG/TNC vendors can still differentiate

Juniper Slide



1. User connects to network through standard 802.1X infrastructure, is blocked at switch
2. Juniper TCG "client" network access requestor (Odyssey Access Client) starts 802.1X with switch and builds EAP tunnel to Policy Decision Point (Juniper Infranet Controller)
3. Infranet Agent profiles the endpoint using Collectors.
4. Profile and Authentication information is passed to the Infranet Controller
5. Infranet Controller authenticates user against AAA servers. (AD, LDAP, etc.)
6. Infranet Controller determines users access policy.
7. Infranet Controller pushes VLAN or ACL information to switch
8. Infranet Controller provisions user access on the Infranet Enforcer
9. User connects to network, controlled both by switch and Infranet Enforcer

Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com

Network Access Control Part 6: Hard Questions

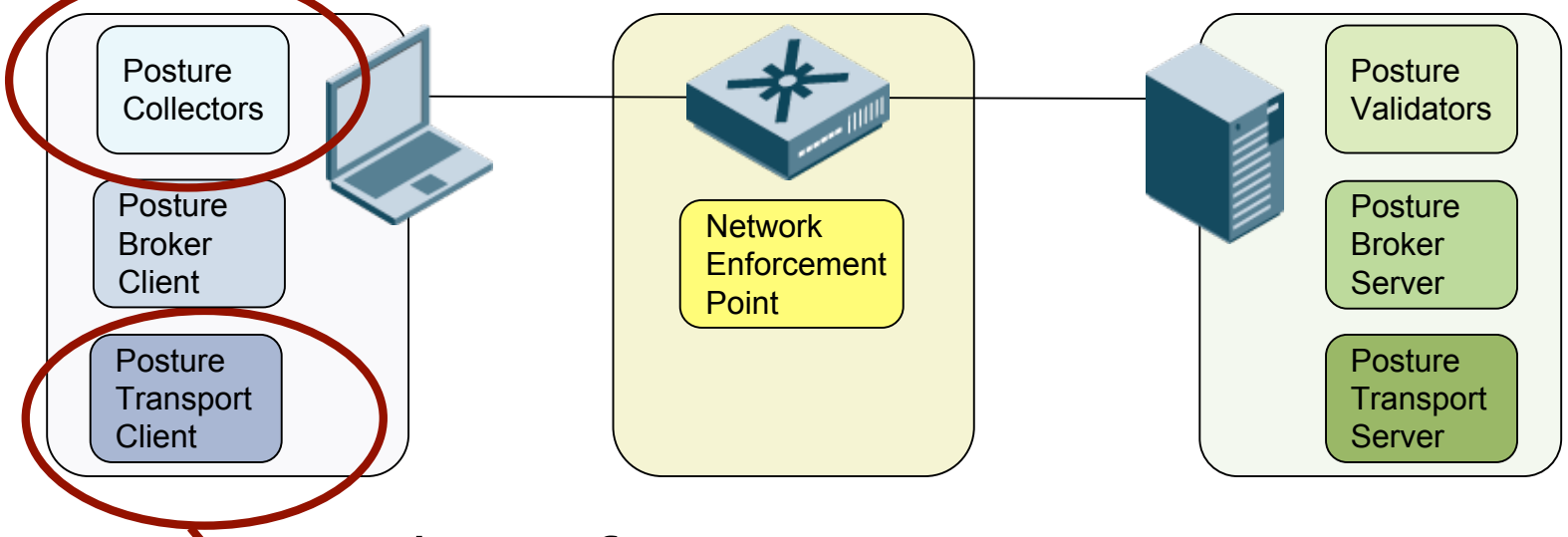
Joel M Snyder
Senior Partner
Opus One
jms@opus1.com

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**

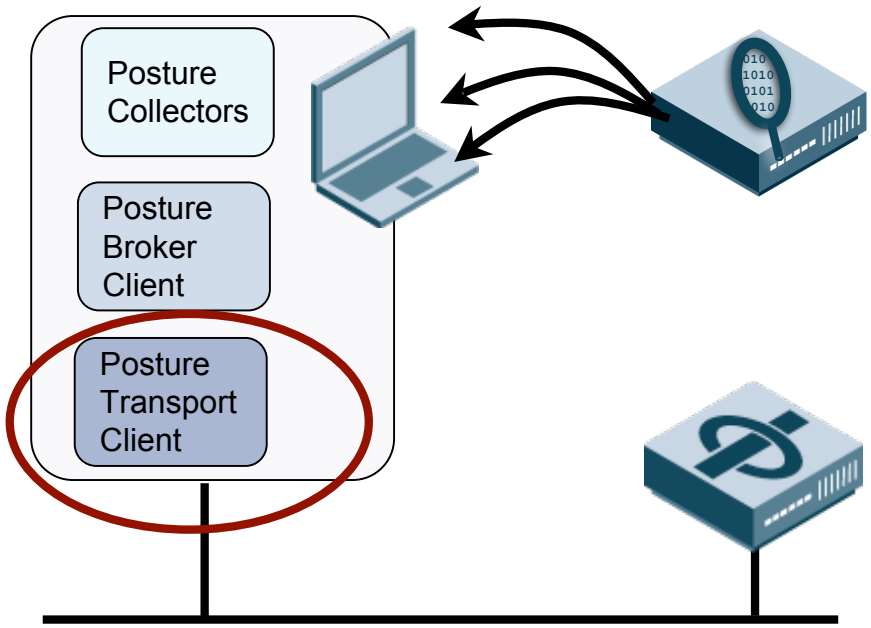
1.
How will NAC deal with lying clients?

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

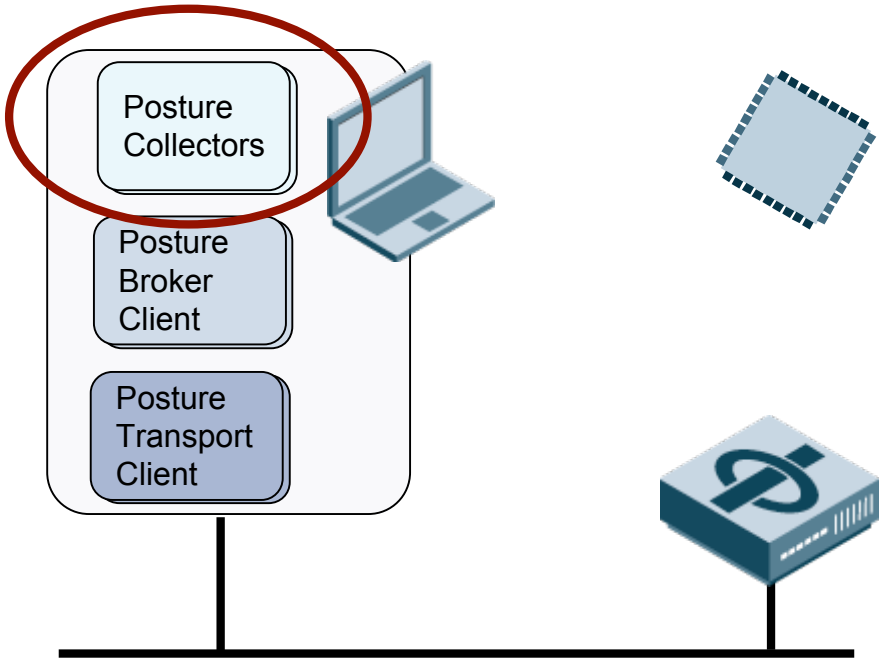
Most NAC deployments will have to use MAC authentication for some devices



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

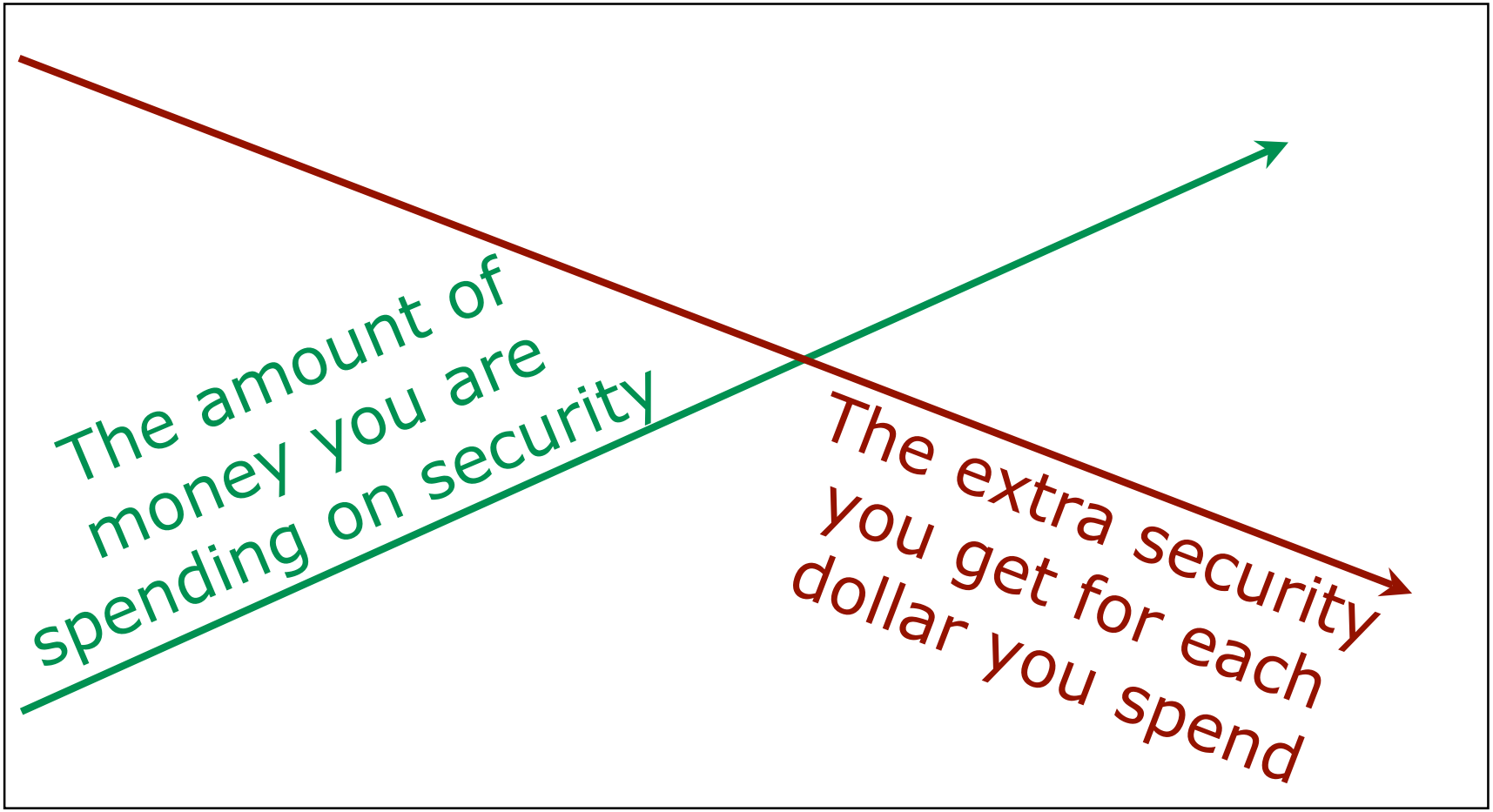
A sub-question: do you care about compliance, or infection?

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



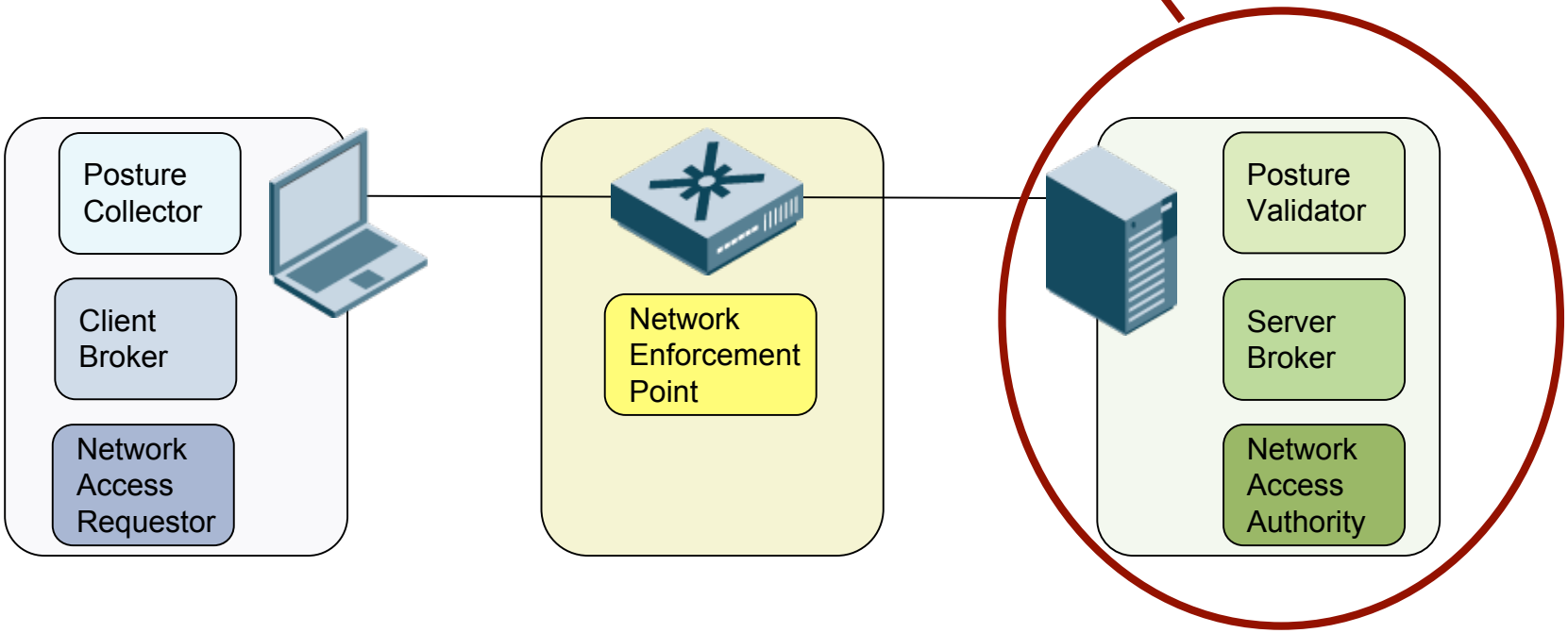
Action Items: Lying Clients

- **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



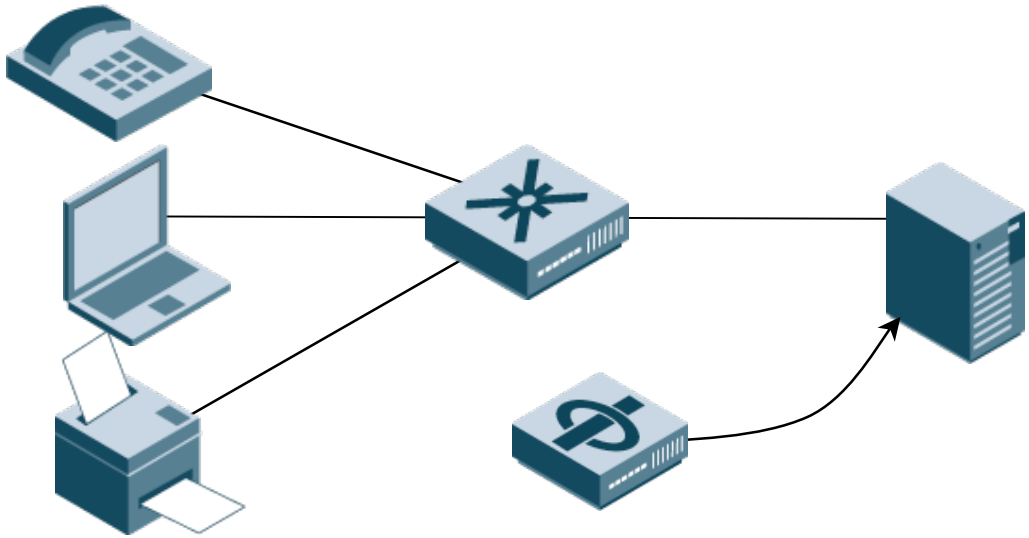
Policy servers need to be scalable

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



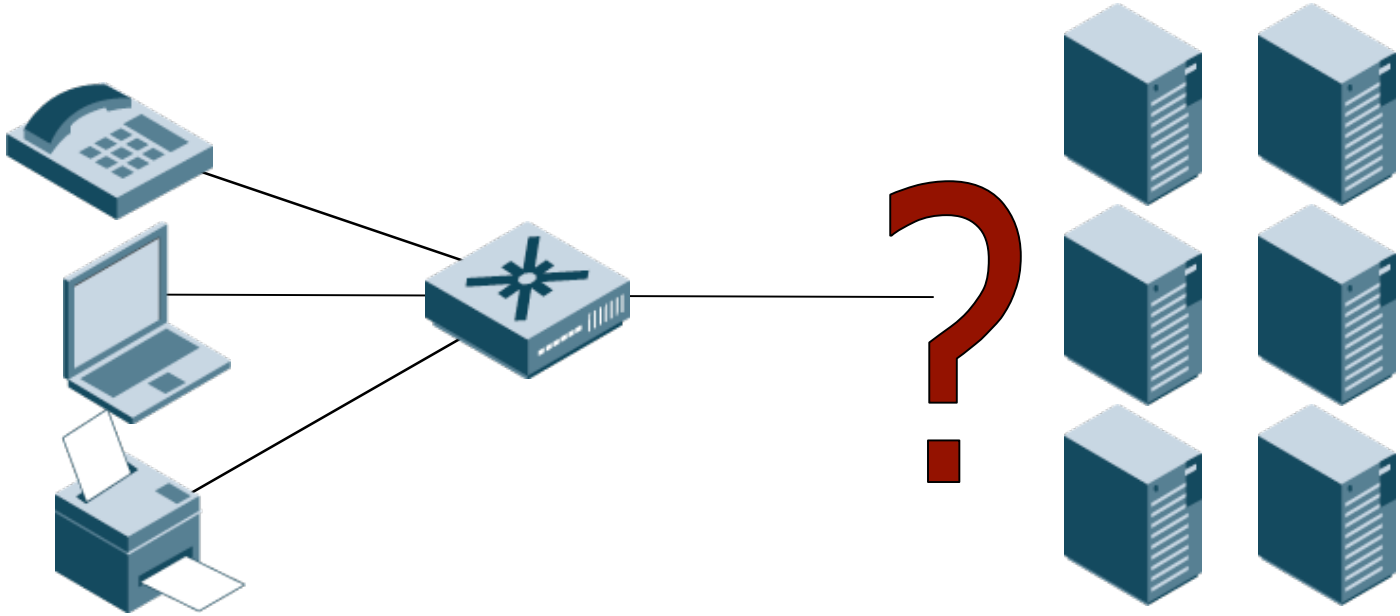
End-point security checks in every 15 minutes

1000 users = 1 decision/second

IDS+SIM+scanner generate 10 events a second

events = 10 decision/second

Policy servers need high availability



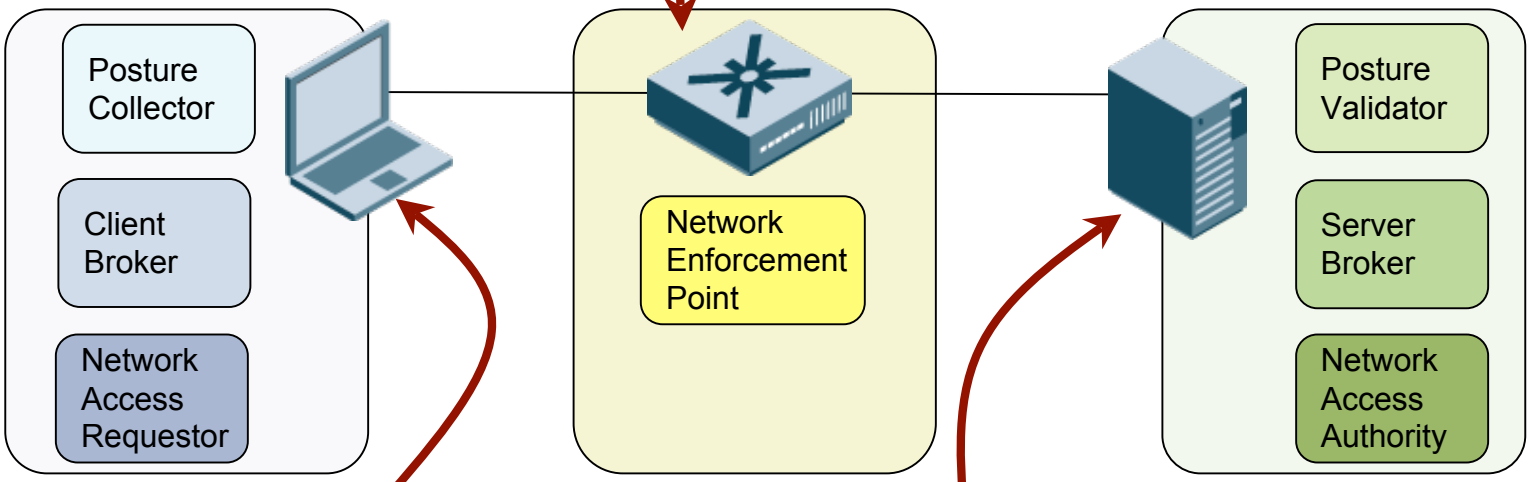
Can you build an active/active cluster?

Are your decision points able to handle multiple locations?

Is the link to the backend database, such as Active Directory or 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?

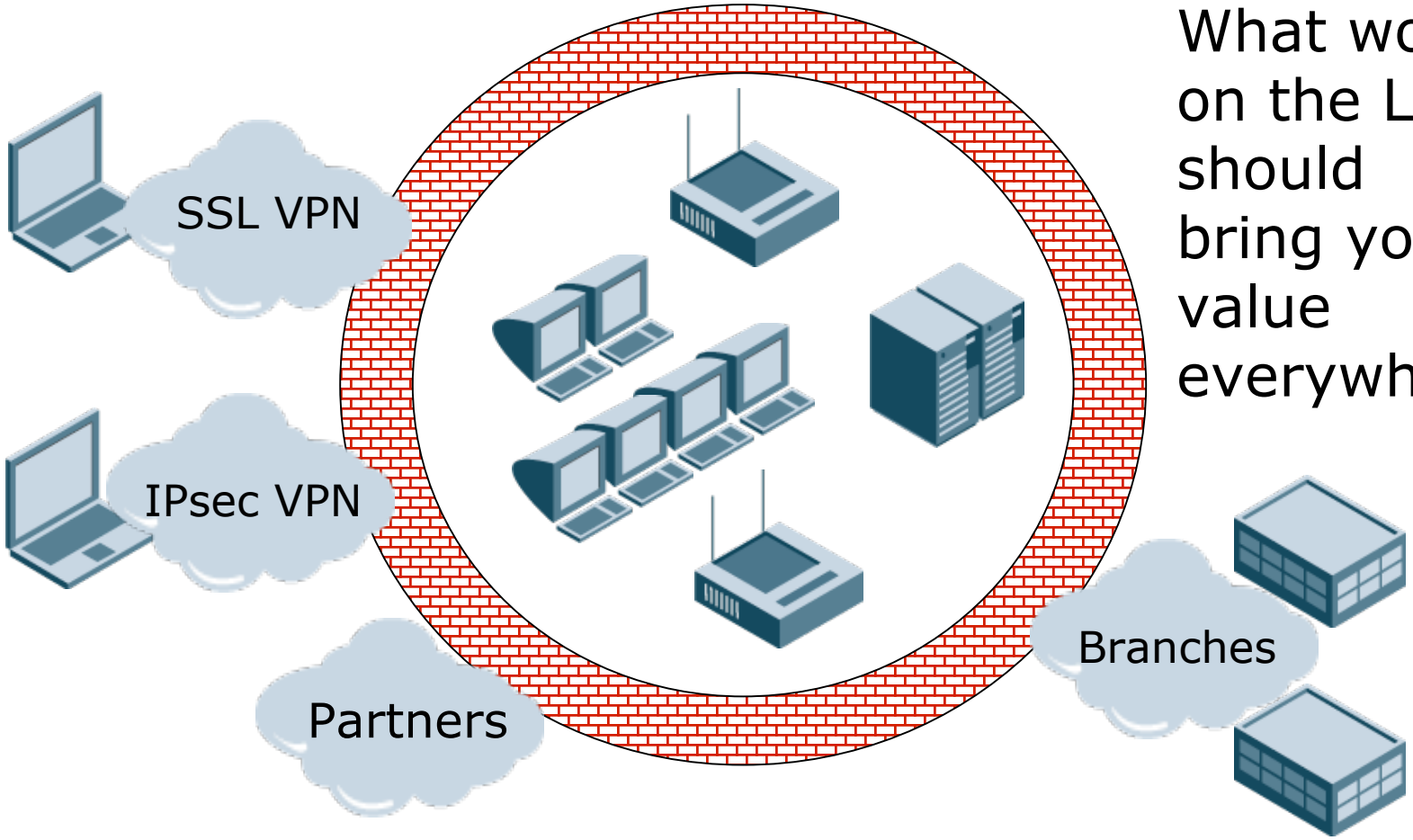
How will the policy engine behave while under a DoS attack?

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

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…

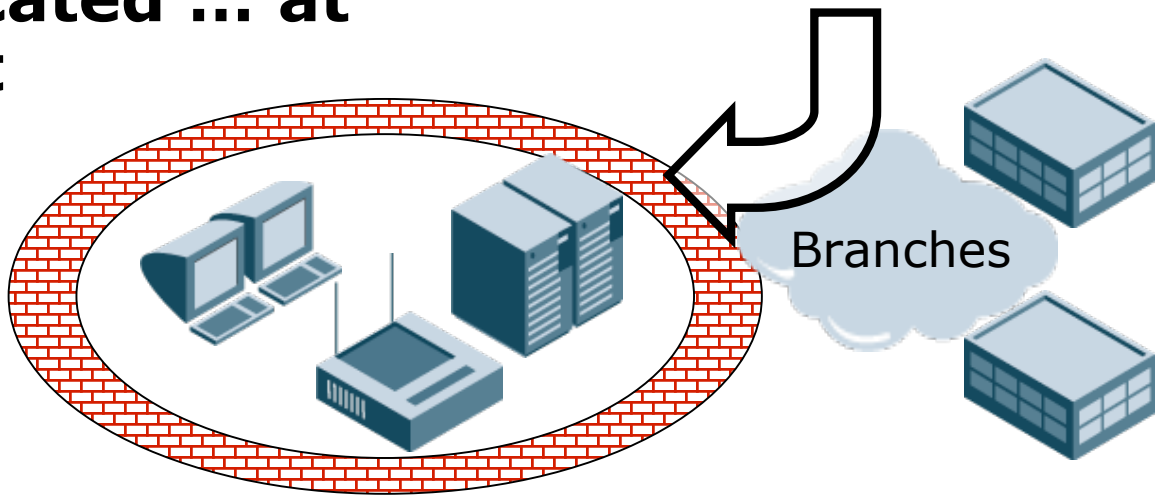
… and of course you can use L3 enforcement

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**

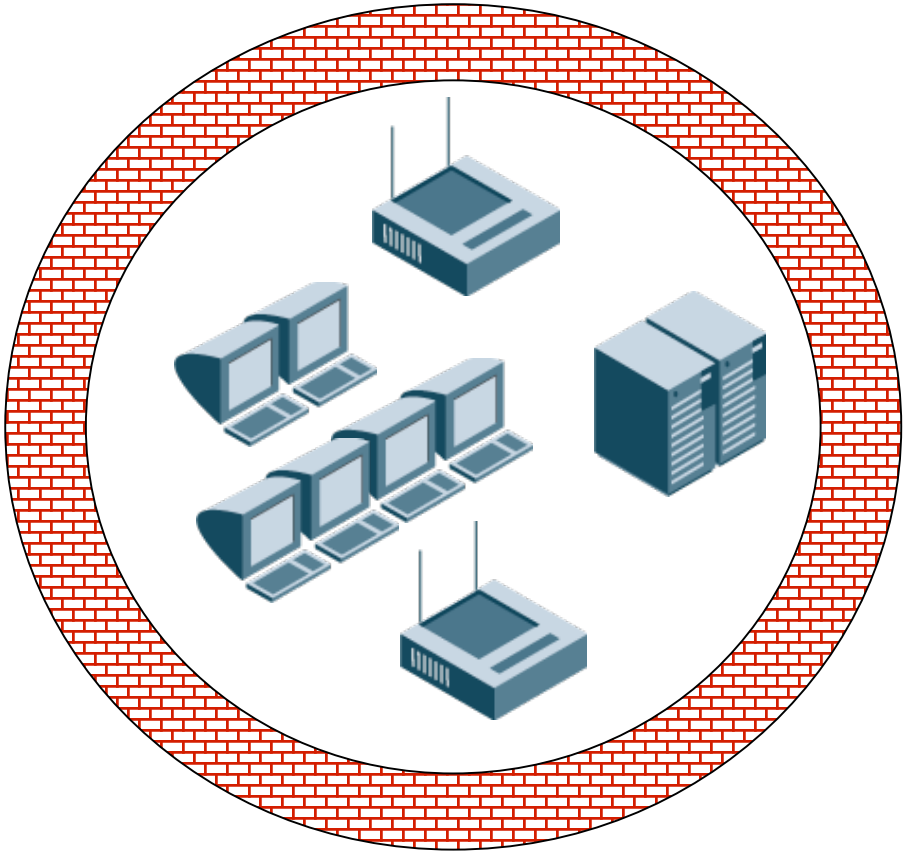
Consider pushing NAC "brains" towards HQ or using L3 enforcement



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

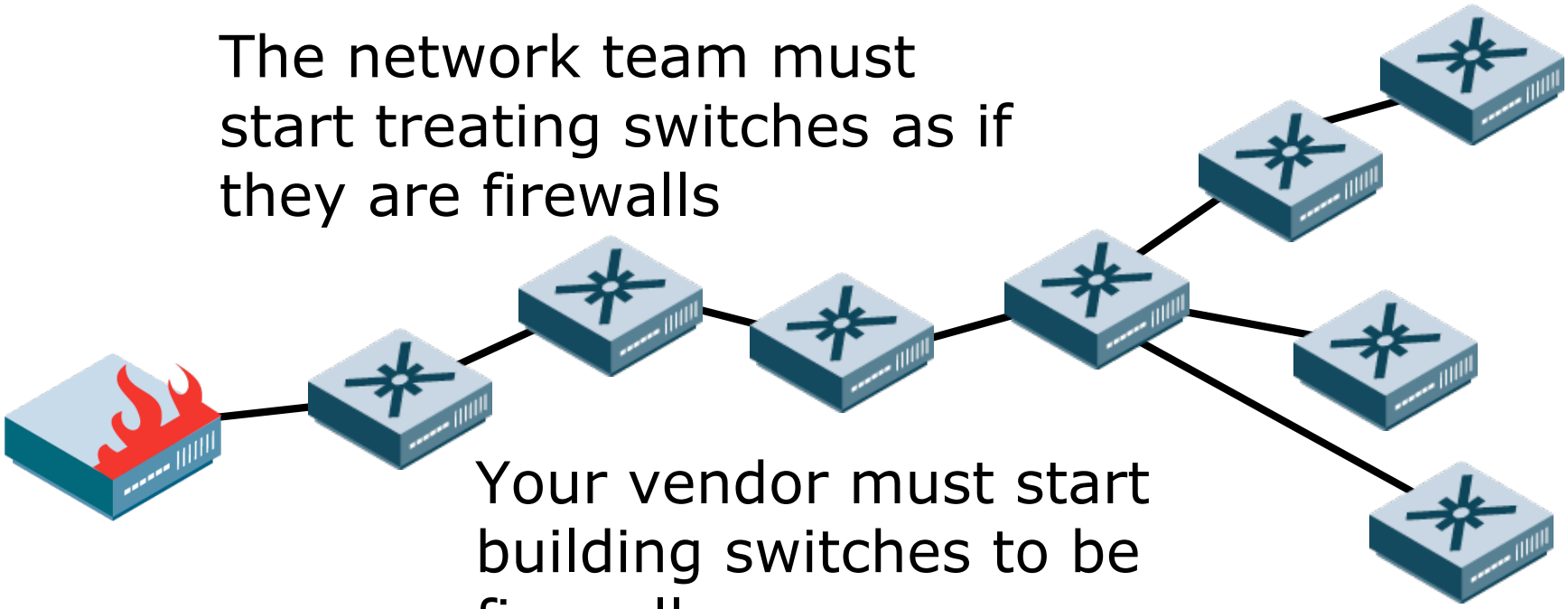
- **Aim to reduce number of policy engines and posture checkers you need to manage; look forward to extend NAC capabilities outside of the LAN and WLAN environments**
- **Consider different strategies for enforcement at branches (while preserving same policy engine)**
- **Make sure your IPsec and SSL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

4.

How much does NAC depend on the security of your

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

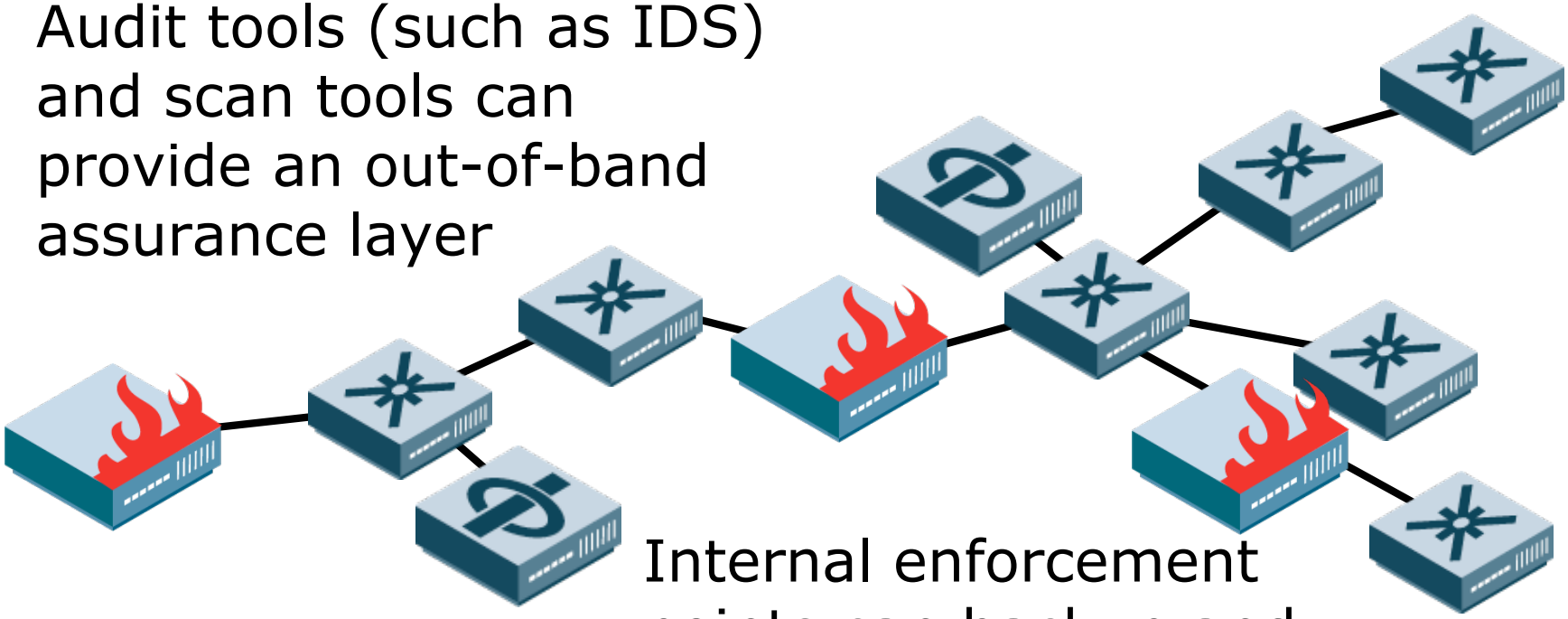
The network team must start treating switches as if they are firewalls



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



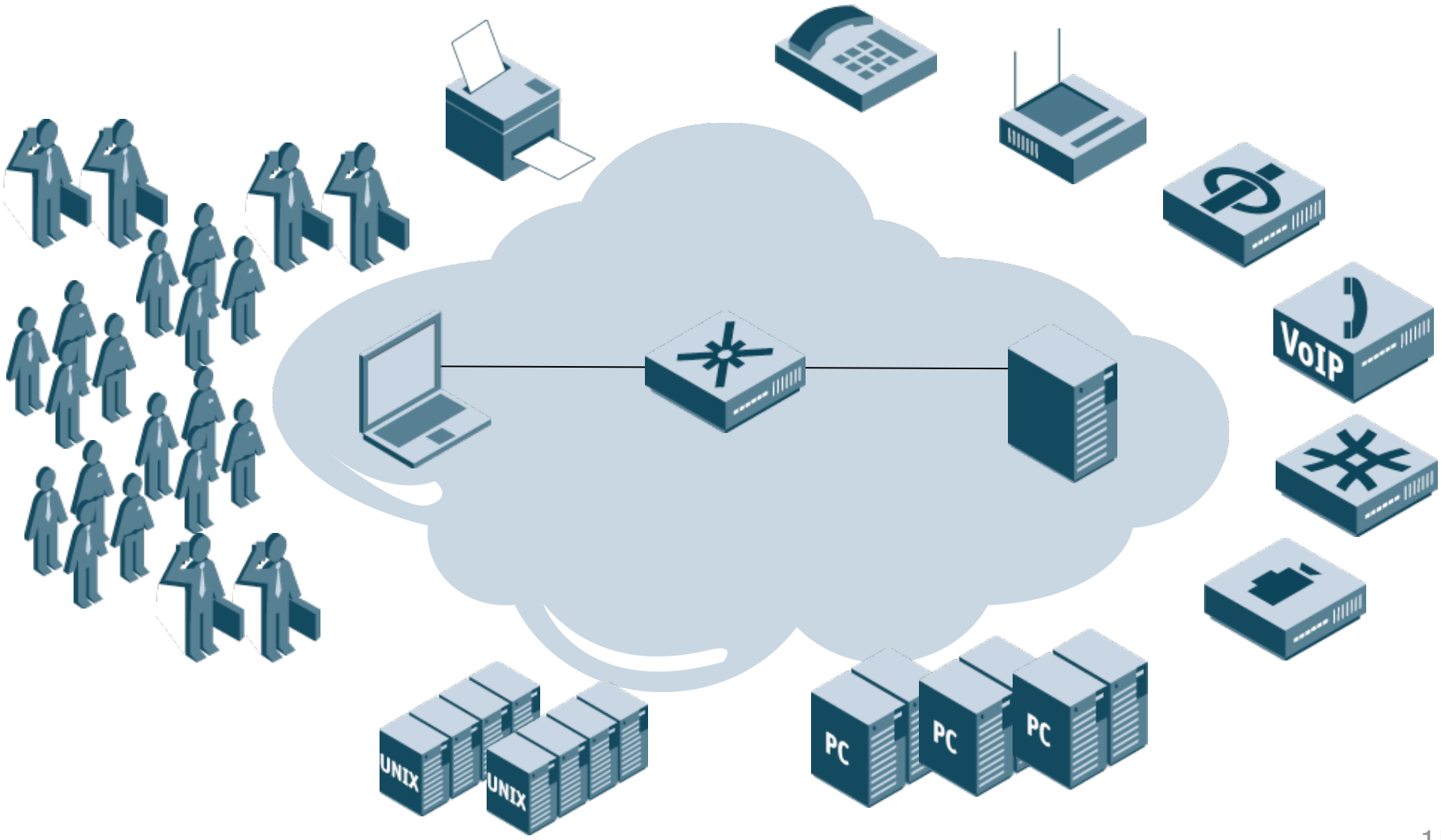
Internal enforcement points can backup and extend switch enforcement

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

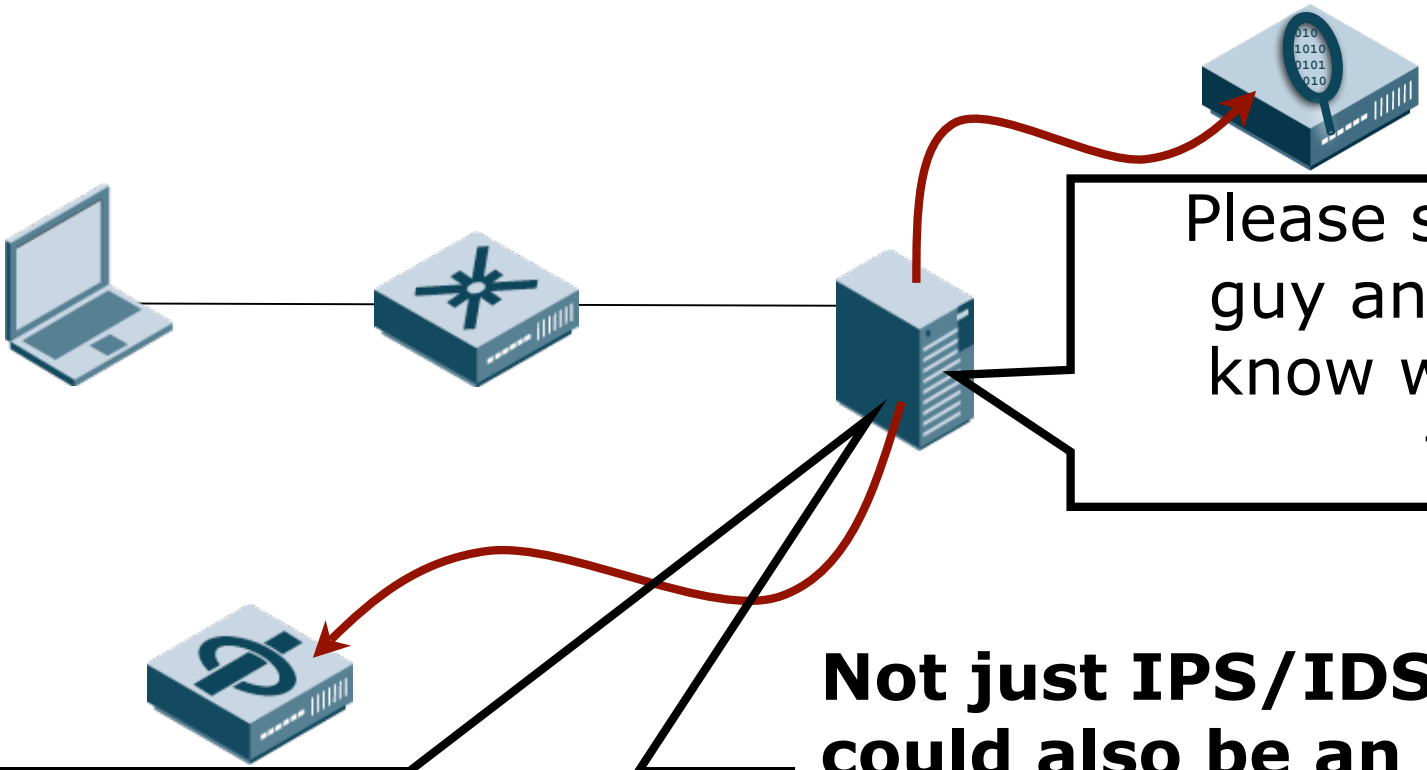
Layers 8, 9, and 10

- **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

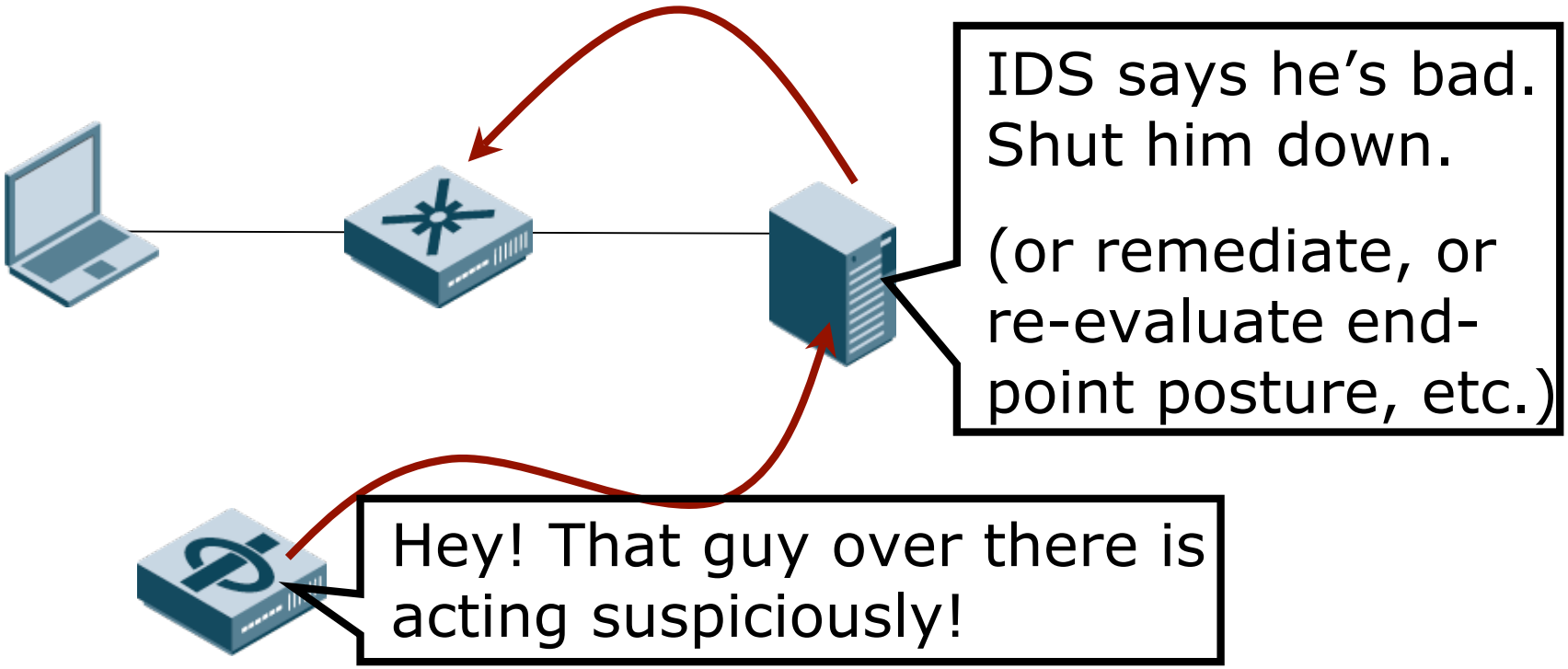


Please scan this guy and let me know what you find out.

Watch this one! I couldn't check end-point security and they're a "guest" user.

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

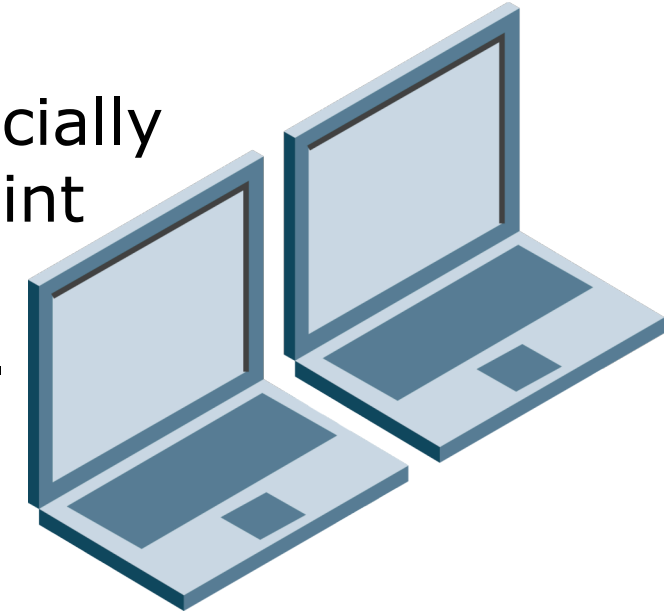


Subtle Problem: "Change of Authorization" is not within existing products, so this is a work in progress for open frameworks

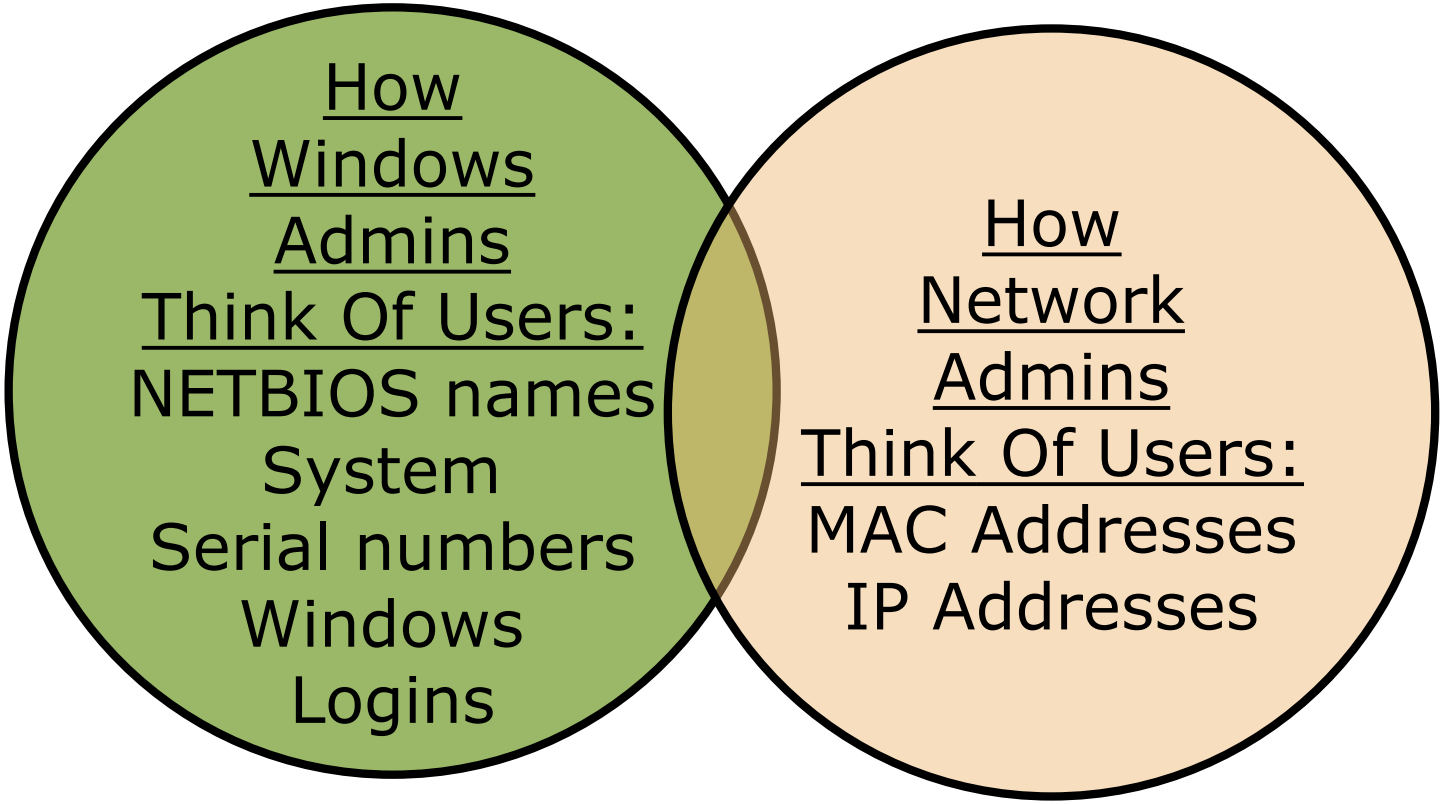
NAC integration with external devices is an evolving story

<u>Howard's Observation</u>: "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

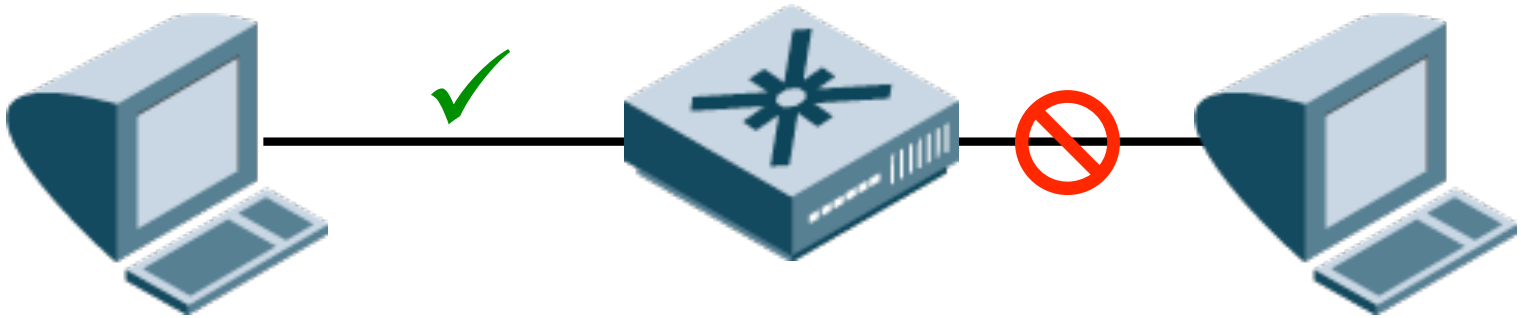
NAC Fundamentally Changes the Way You Think About the Network

Before:
Switching Infrastructure

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

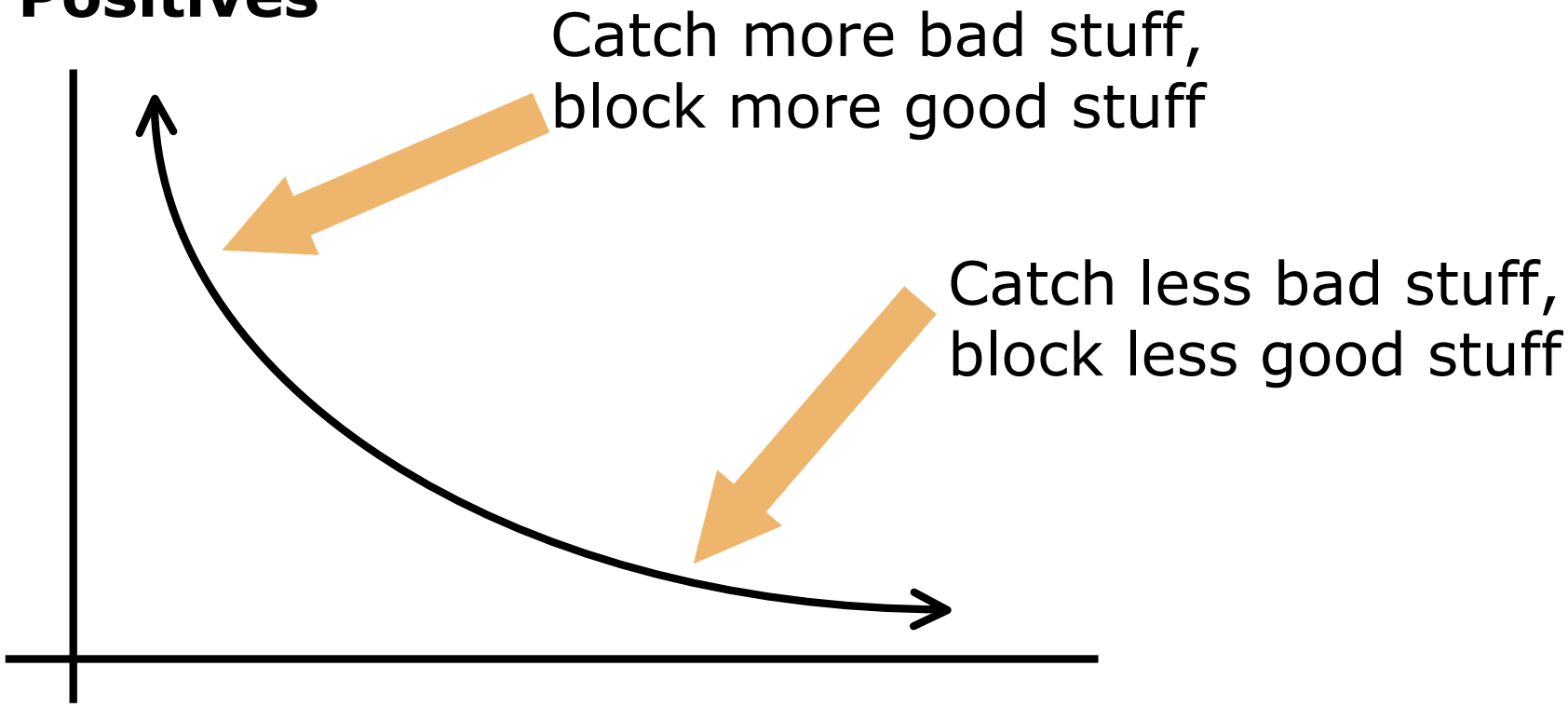
After:
Policy Enforcement Infrastructure

- **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**



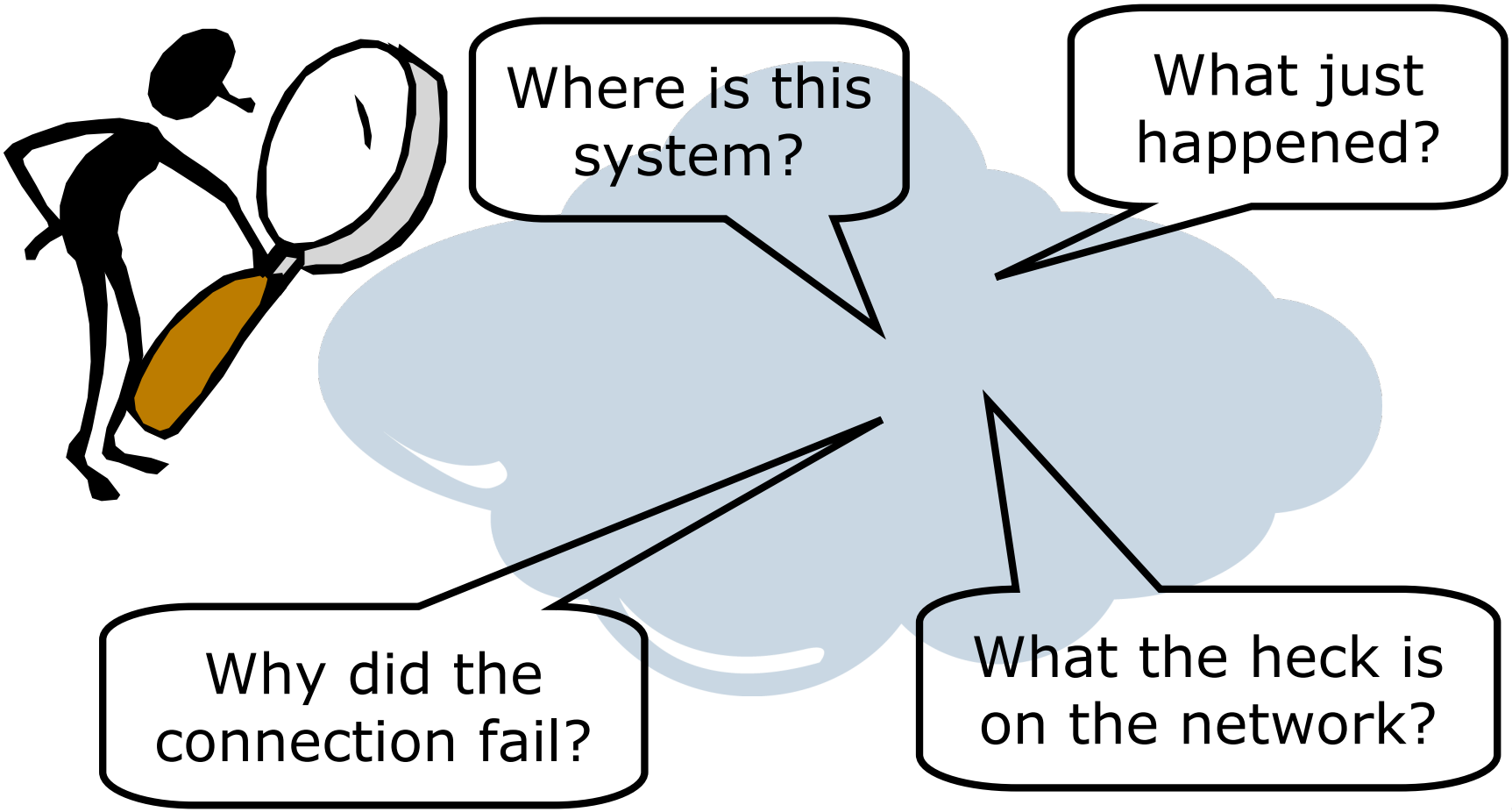
Keep In Mind The Guiding Principle of NAC

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

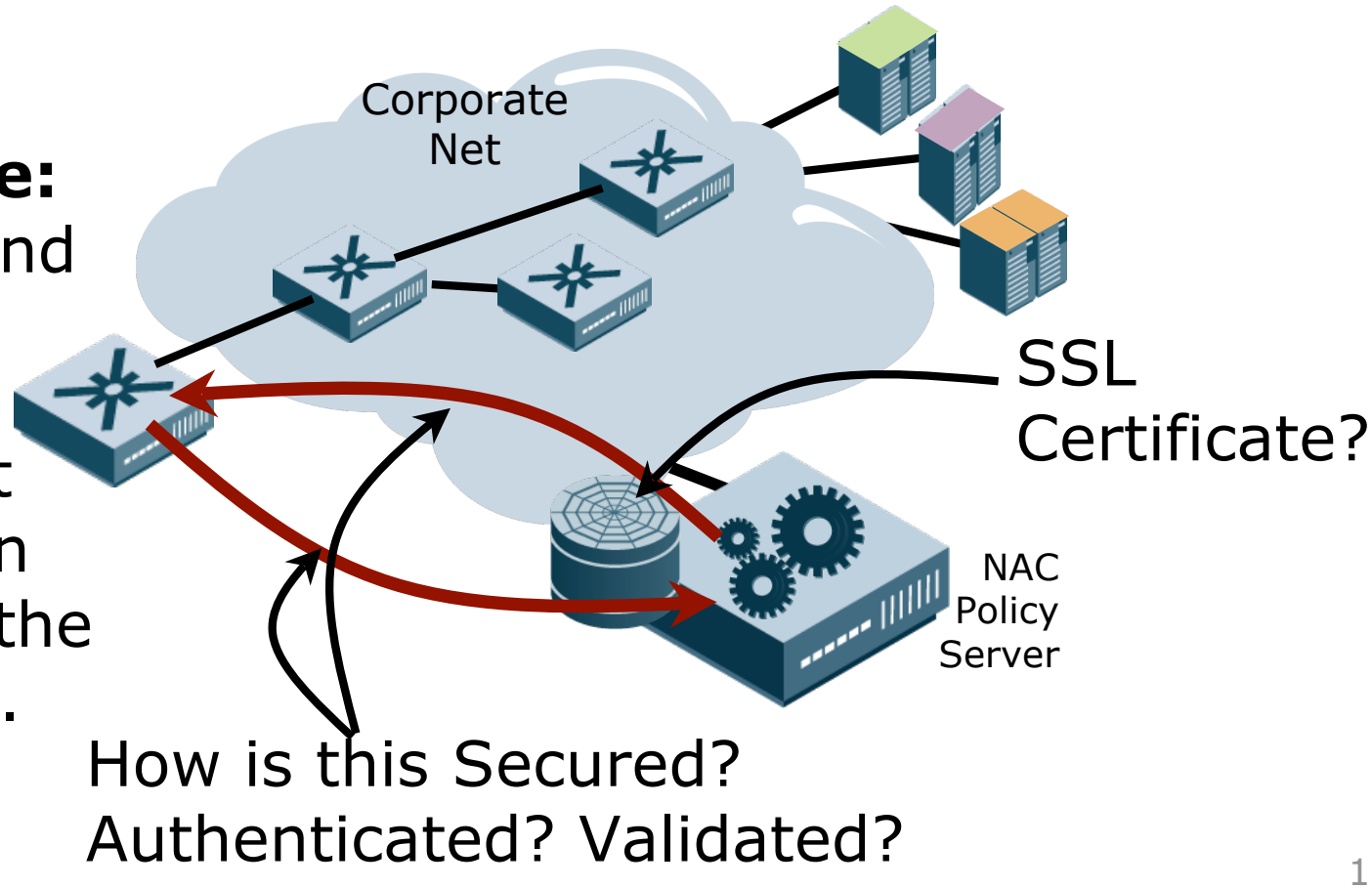
Action Items: Change in Thinking

- **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

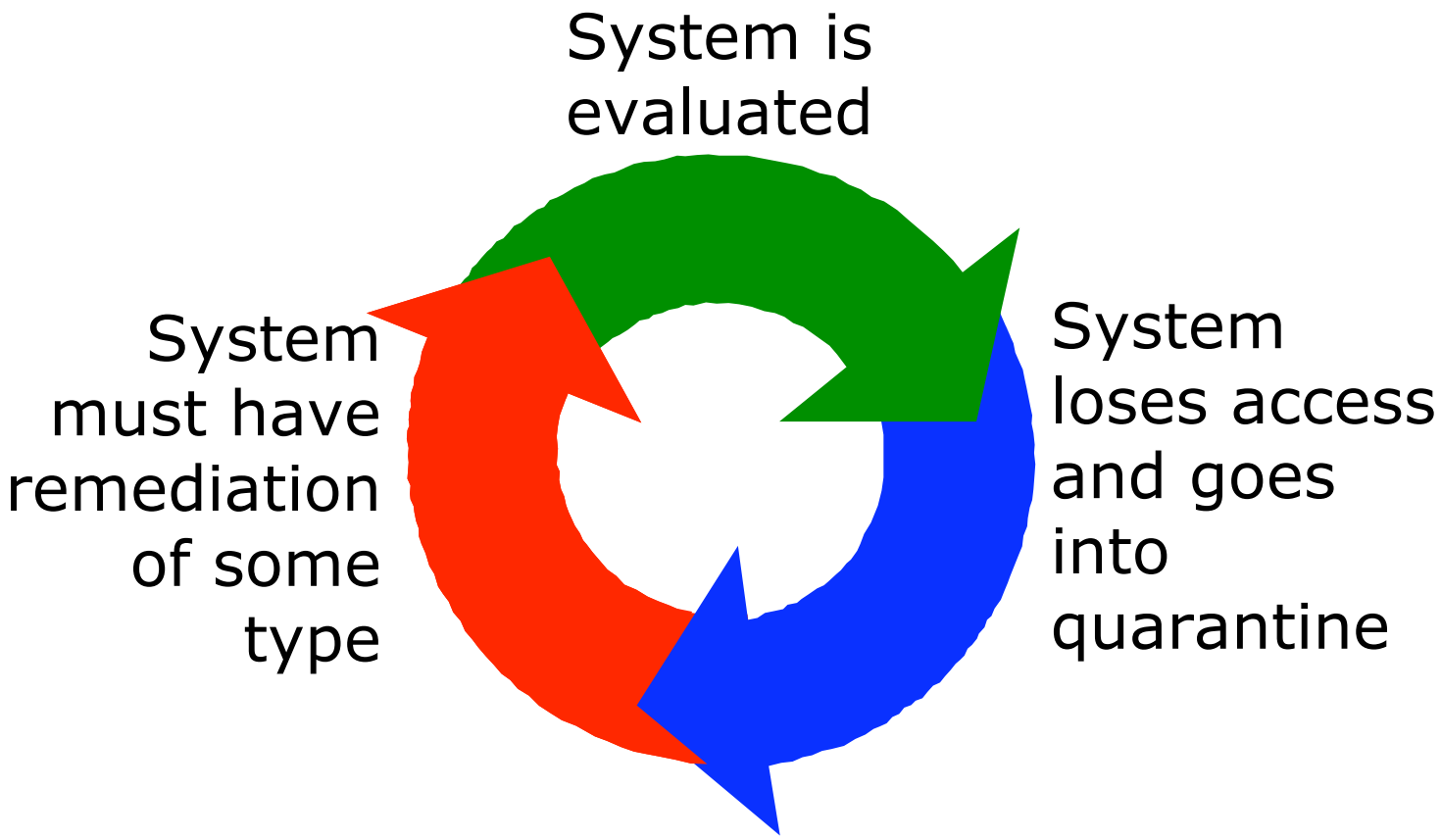
Areas of Concern	Potential Issues
Command-Line Management Links	**CLI passwords; clear-text management; credential management; change control**
SNMP Tools	**Lack of SNMP authentication in devices; clear-text passwords; UDP lossage; change control**
Client APIs	**Registration and impersonation vulnerabilities**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

Action Items: Security Vulnerabilities

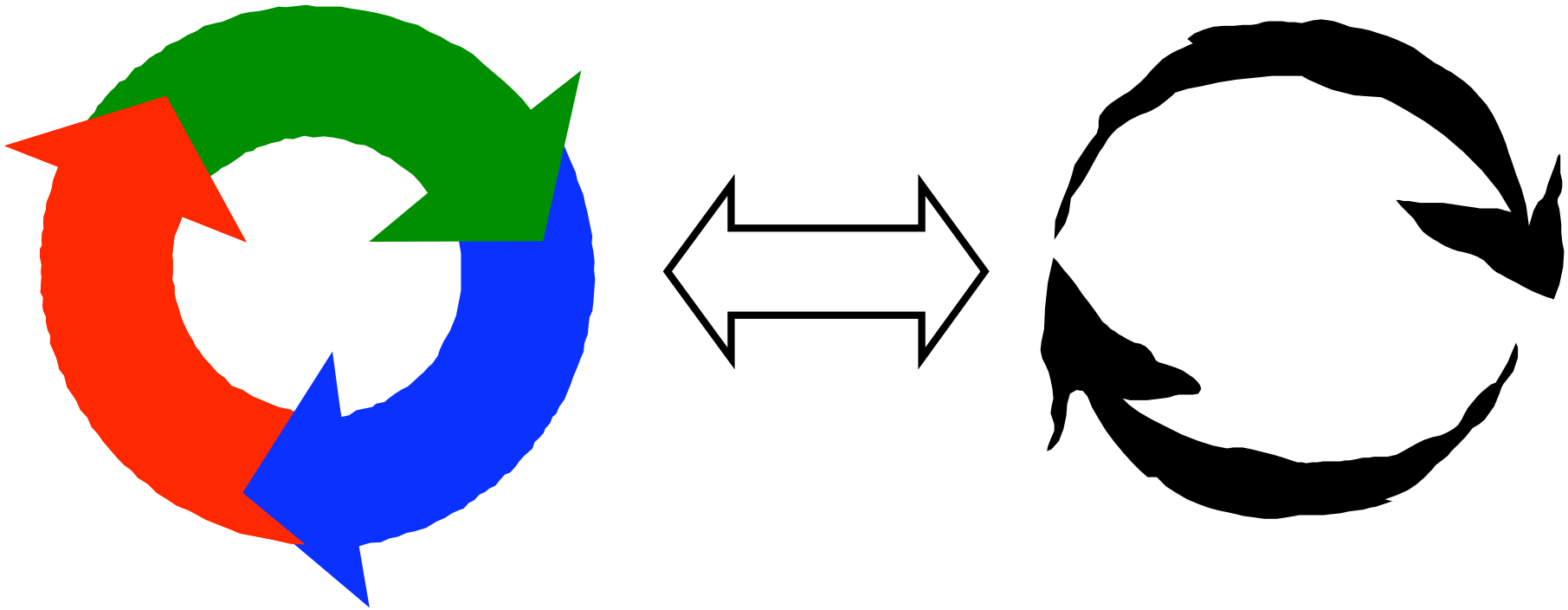
- **Work with your vendor to identify areas of "linkage" between components where you need to be concerned**
- **Identify specific training issues for end-users related to potential vulnerabilities (such as SSL/TLS certificates)**
- **Get outside help to review security vulnerabilities and identify areas 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 <u>lifecycle</u> view of end-points.**
- **Don't fixate on just one aspect of the cycle (such as evaluation)**

Interaction 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