Network Access Control: A Whirlwind Tour Through The Basics

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

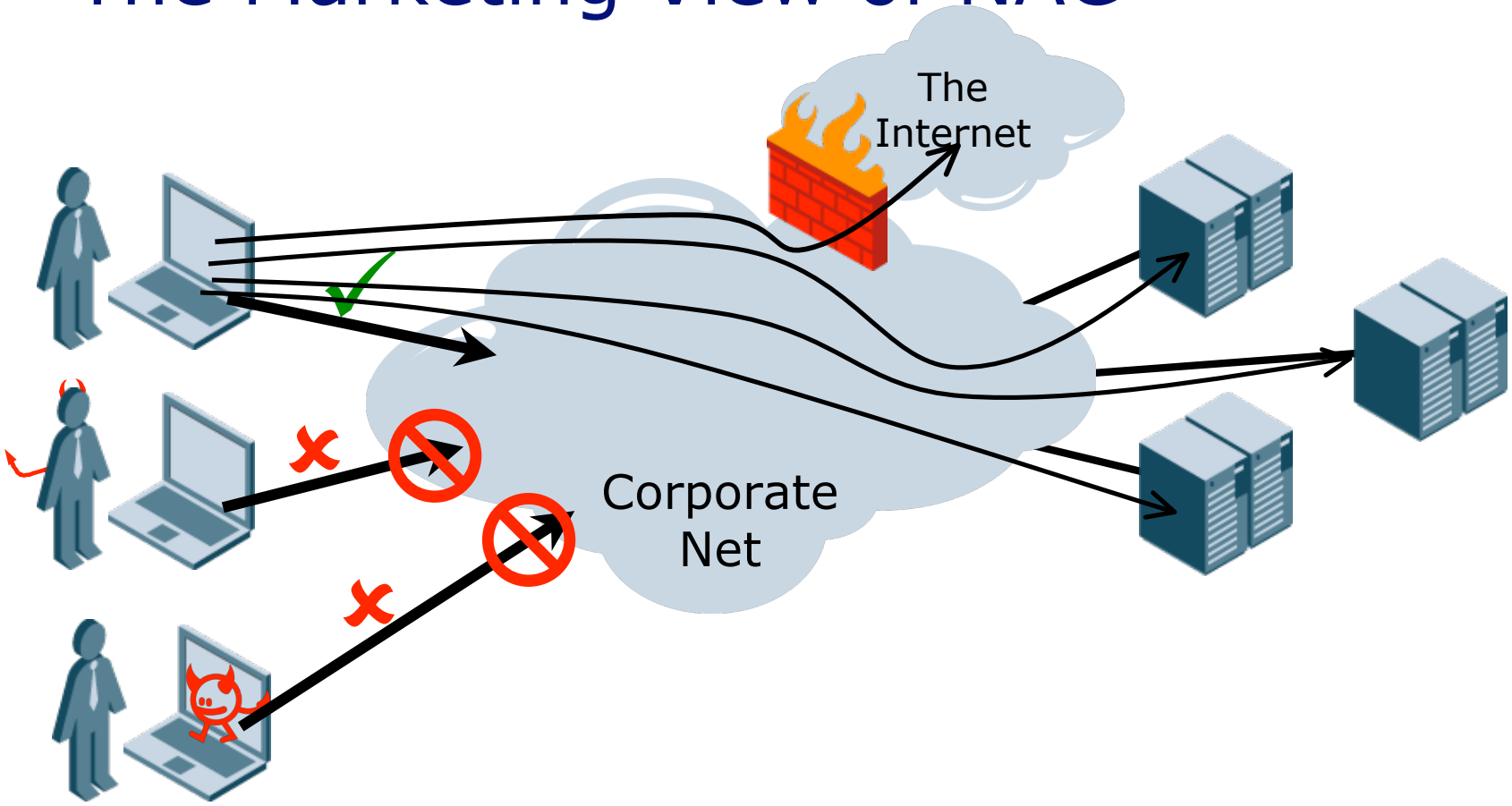
Last Year

- **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"

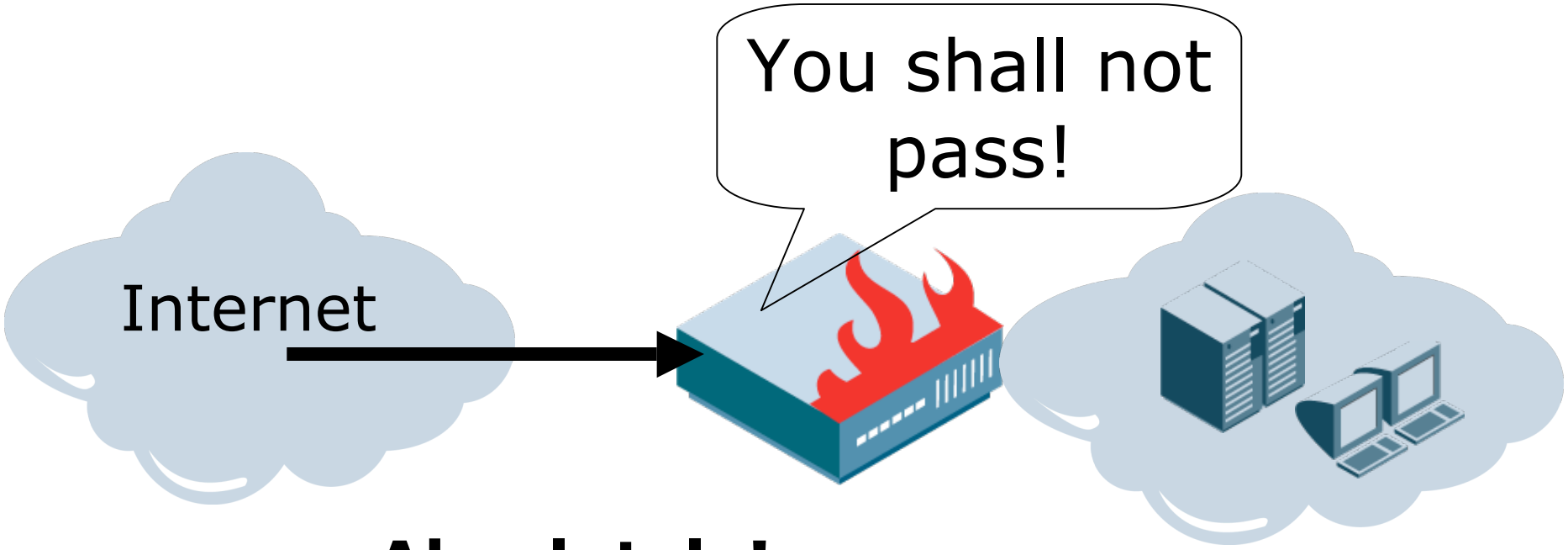
Who you are:
not your IP address, but your authenticated identity.

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

Something inside of the network:
enforcement occurs in the network, not on the the end points

Control: limit access according to policy, where policy is based on the user

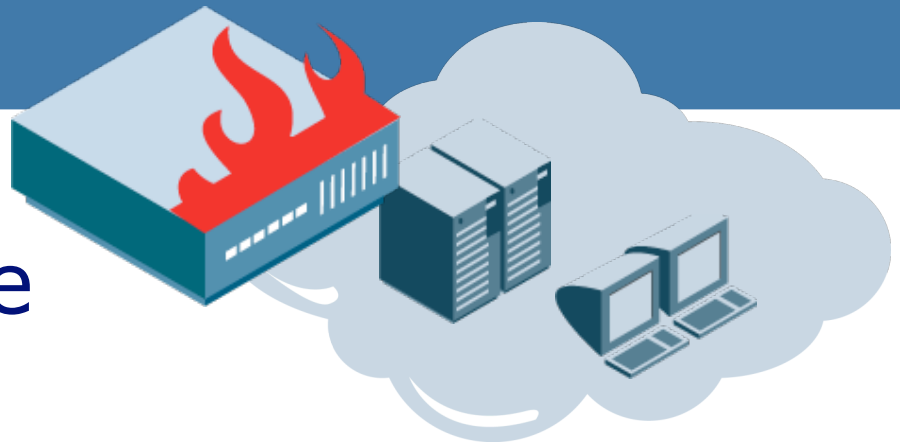
"OK, wait a second. Isn't Access Control what a firewall does?"



Absolutely!

The difference is in the decision!

NAC Is Firewalling, but With a Difference

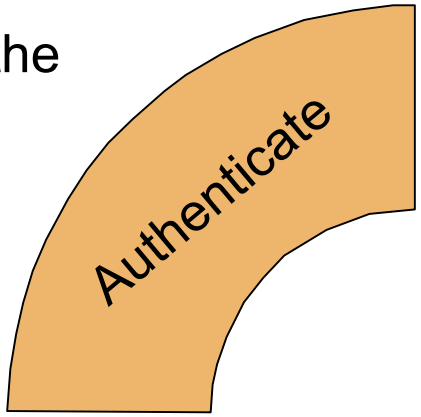


Common Firewall **Decision Elements**
Source IP and port Destination IP and port **Position** Between two networks

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

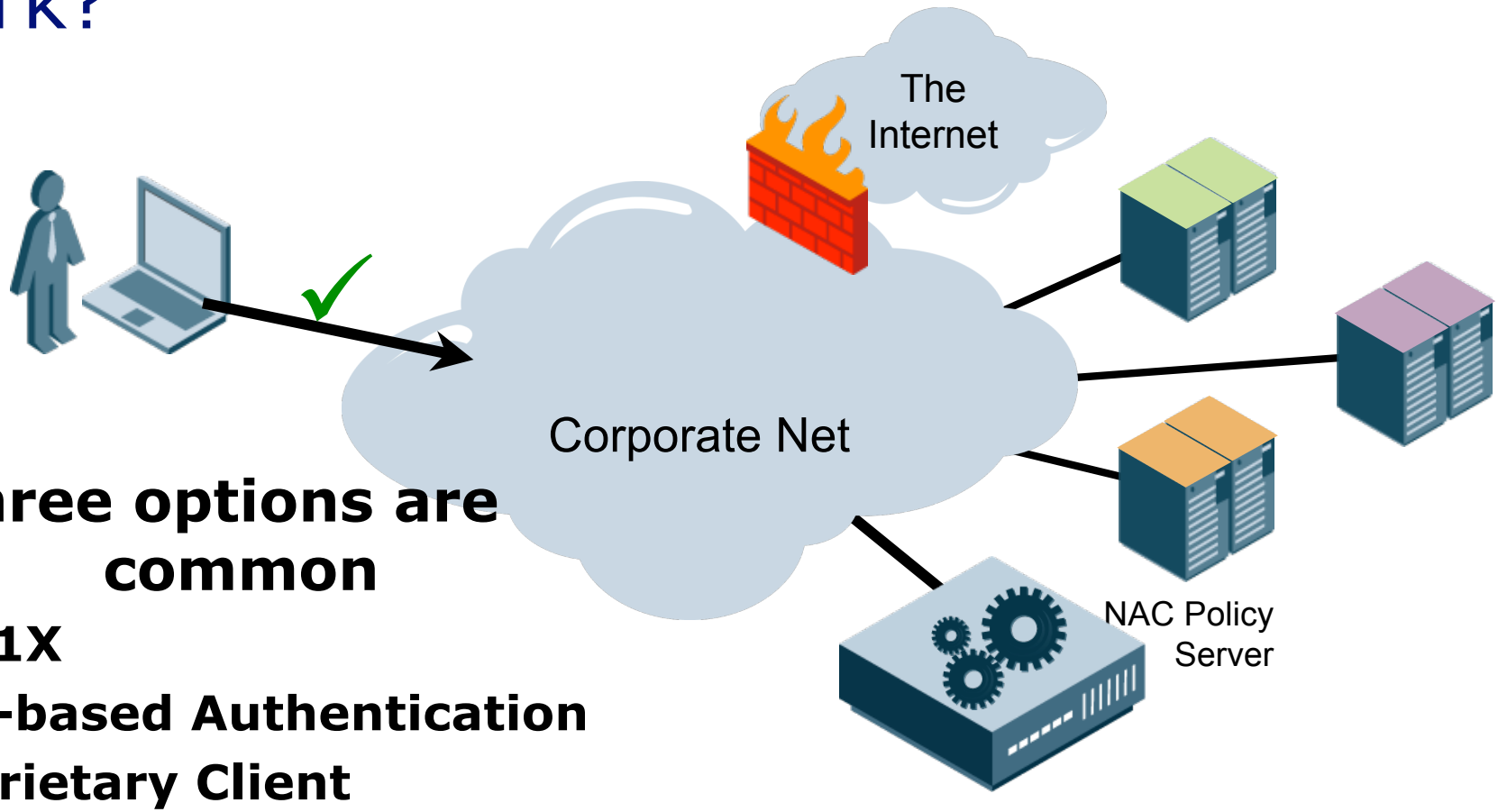
NAC Has Four Components

1. Authentication of the user



End users are authenticated before getting network access

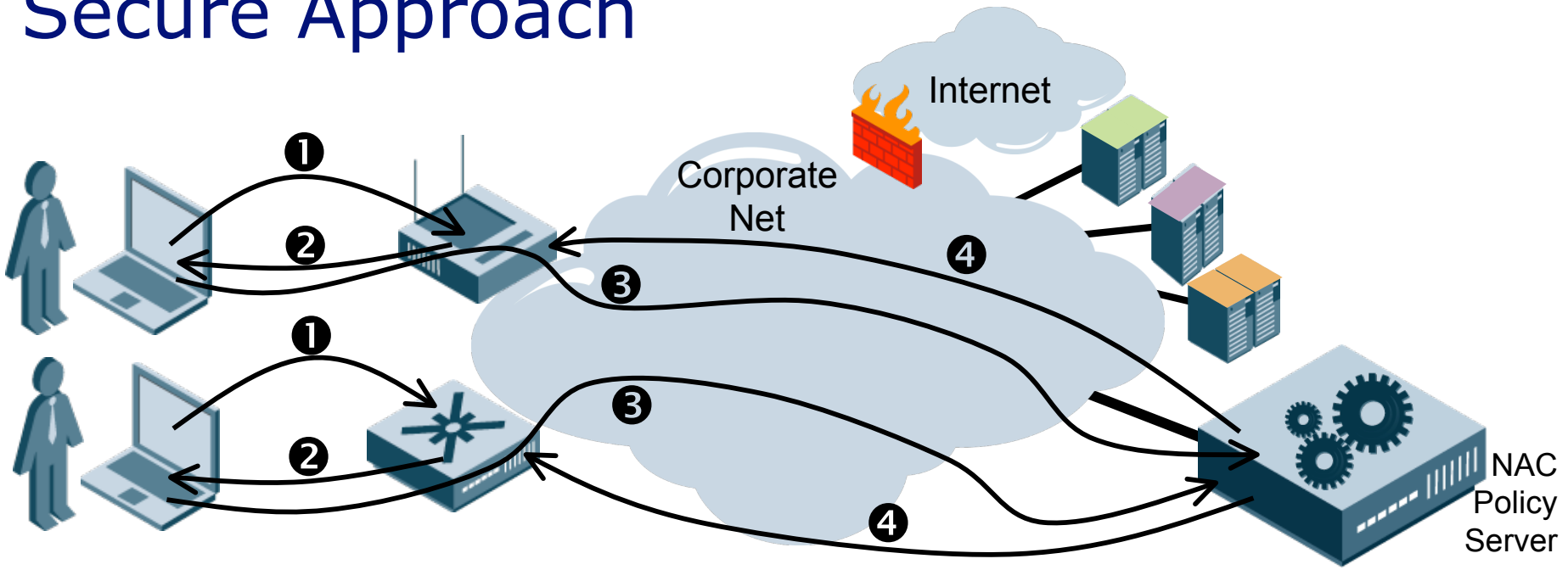
How Does the Authentication Actually Work?



Three options are common

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

802.1X is Preferred and the Most Secure Approach



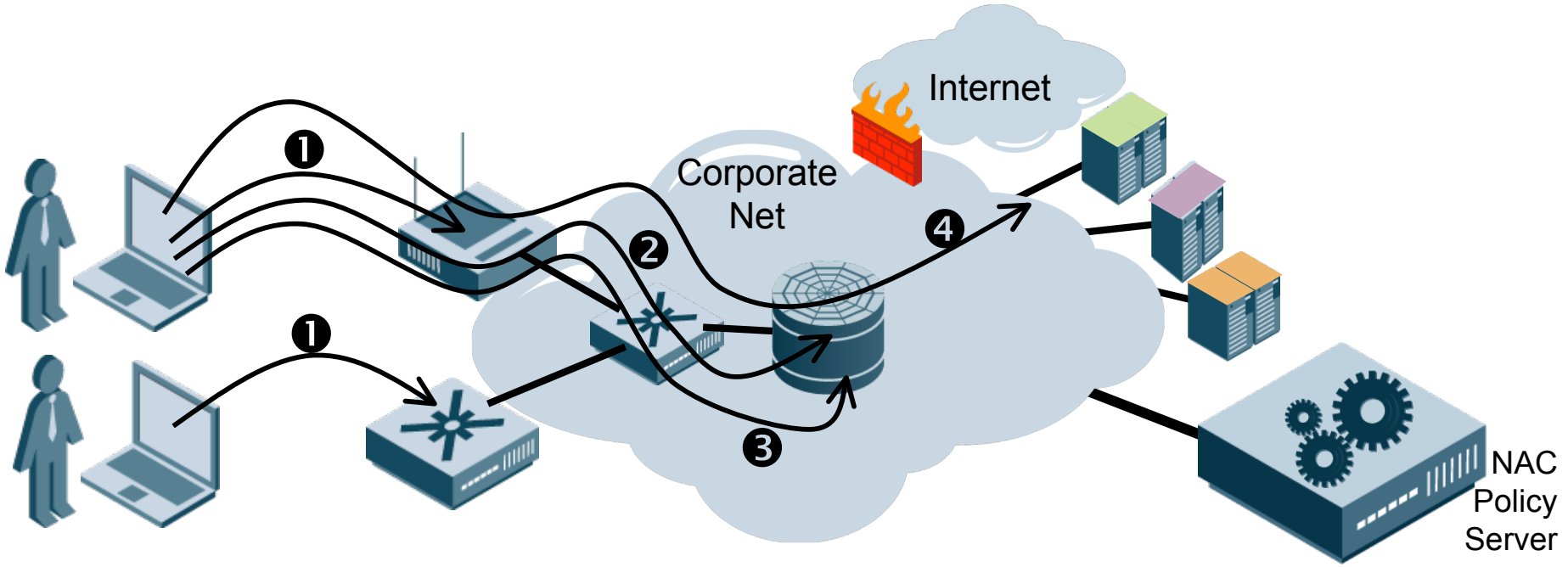
❶ User brings up link (or associates with AP)

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

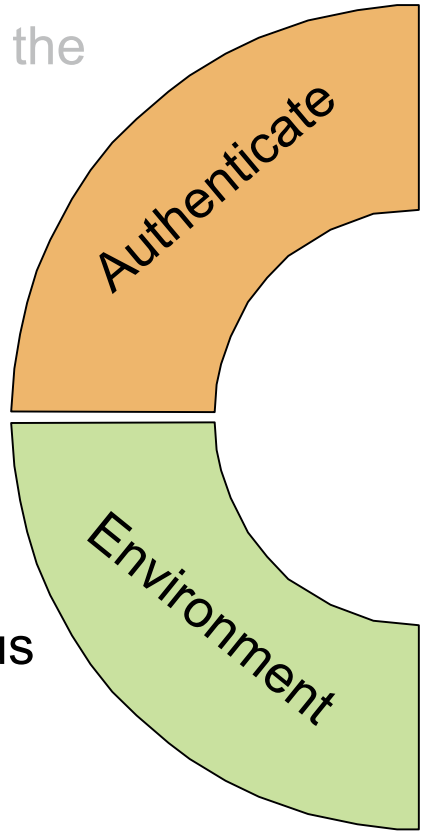


❶ User gets on network; gets IP address
❷ User opens web browser and is trapped by in-line portal
❸ User authenticates to central policy server
❹ If authentication (and other stuff) is successful, portal lets traffic through or reconfigures network to get out of the way

Environmental Information Modifies Access or Causes Remediation

1. Authentication of the user

2. Use environmental information as part of 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”)?

Environmental Information Can Include Lots of Things

This is the "(and other stuff)" part

Pure Environment

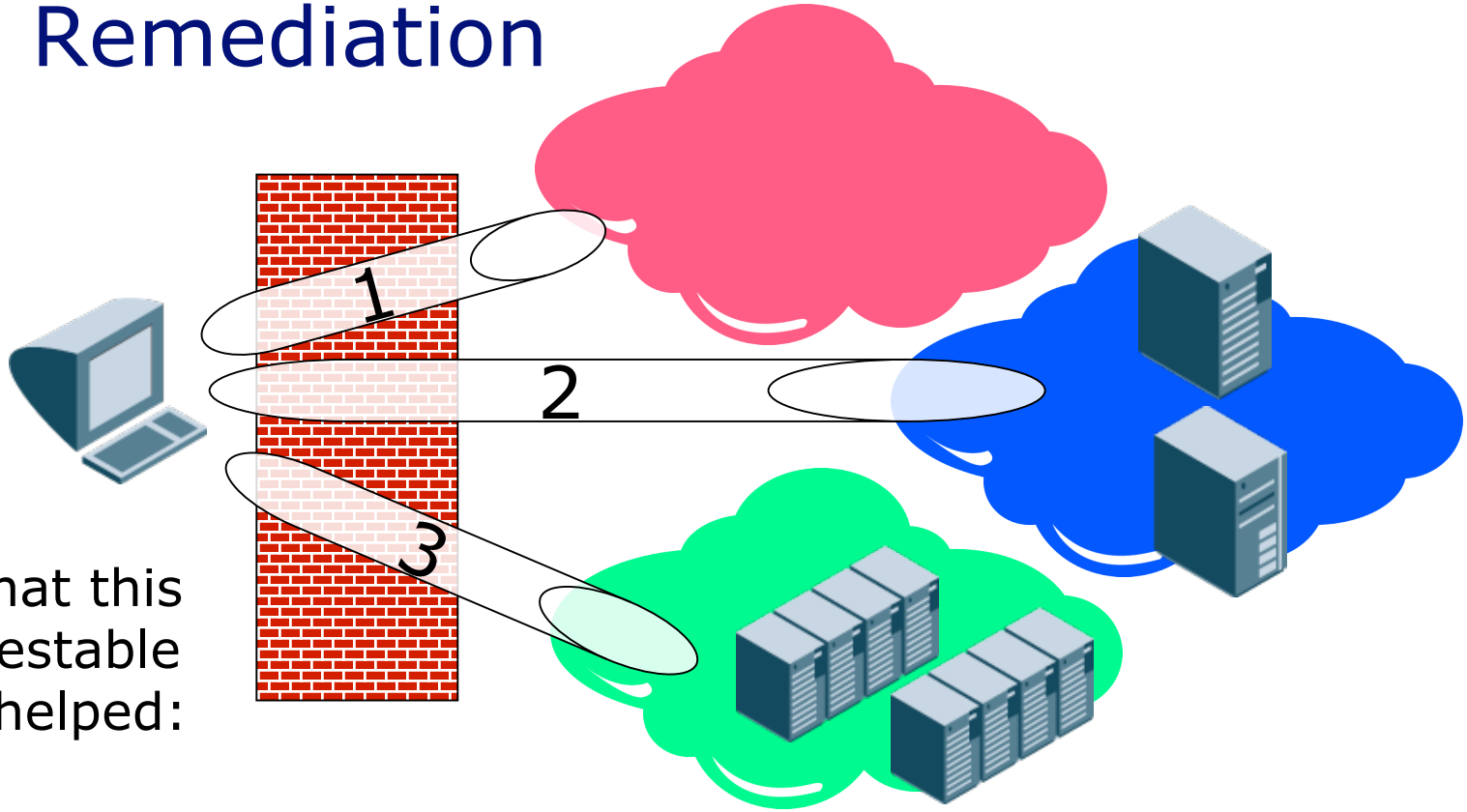
- Access Method (wired, wireless, VPN)
- Time of Day/Day of Week/Date within Limits
- Client Platform (Mac, Windows, *etc*.)
- Authentication Method (user/pass, MAC, *etc*.)

End Point Security

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

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

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 & user-focused Environment

What you can do =

Who You Are

+

How Well You Comply with Policy

+

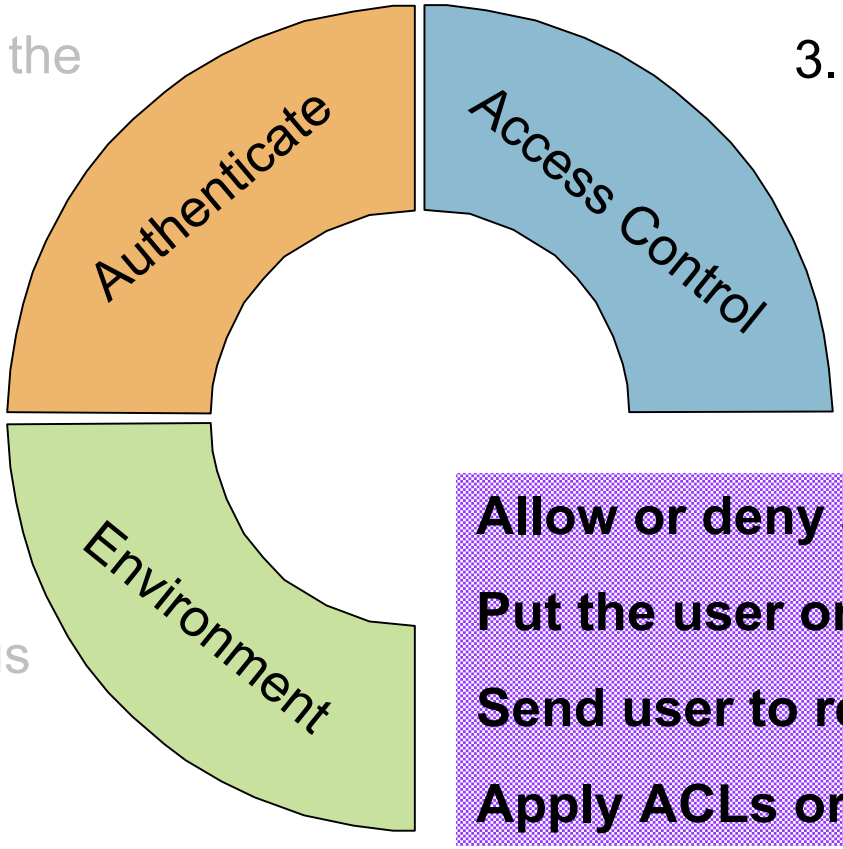
How You Behave On The Network

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

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



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

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

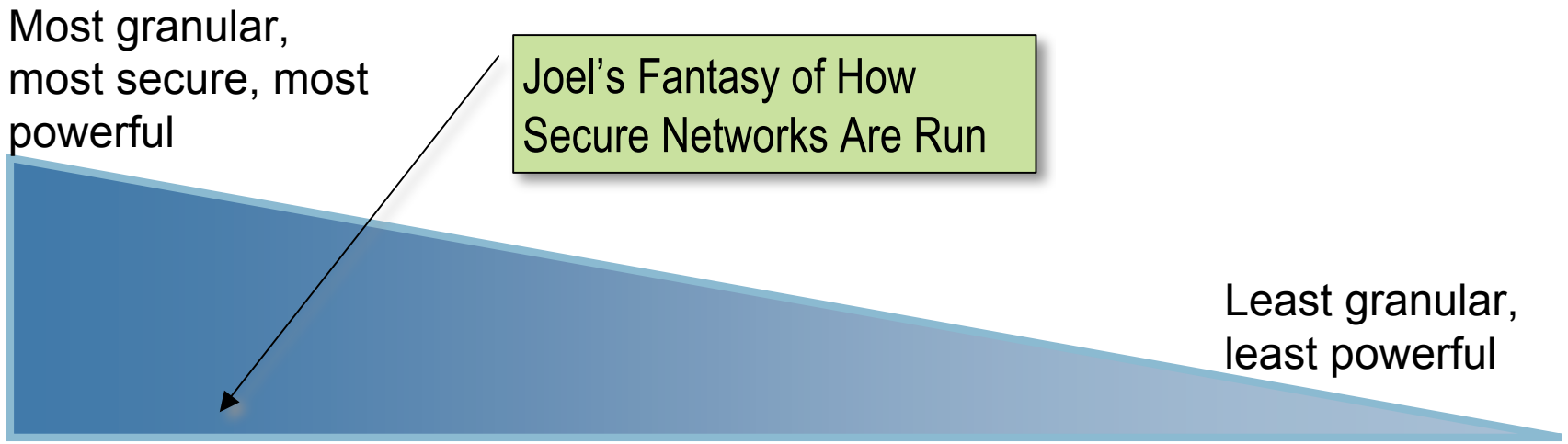
Control Granularity

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

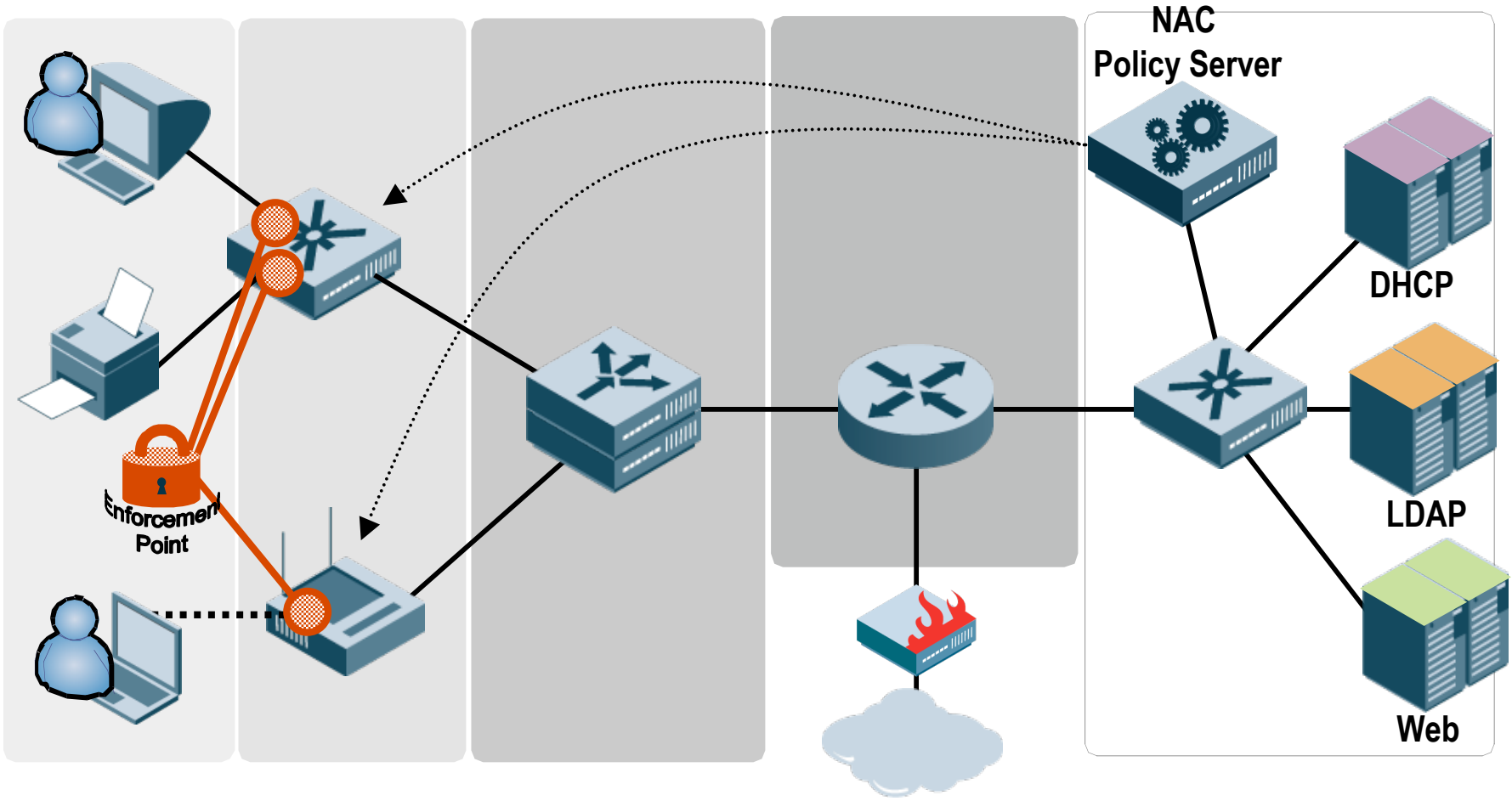
Control Location

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

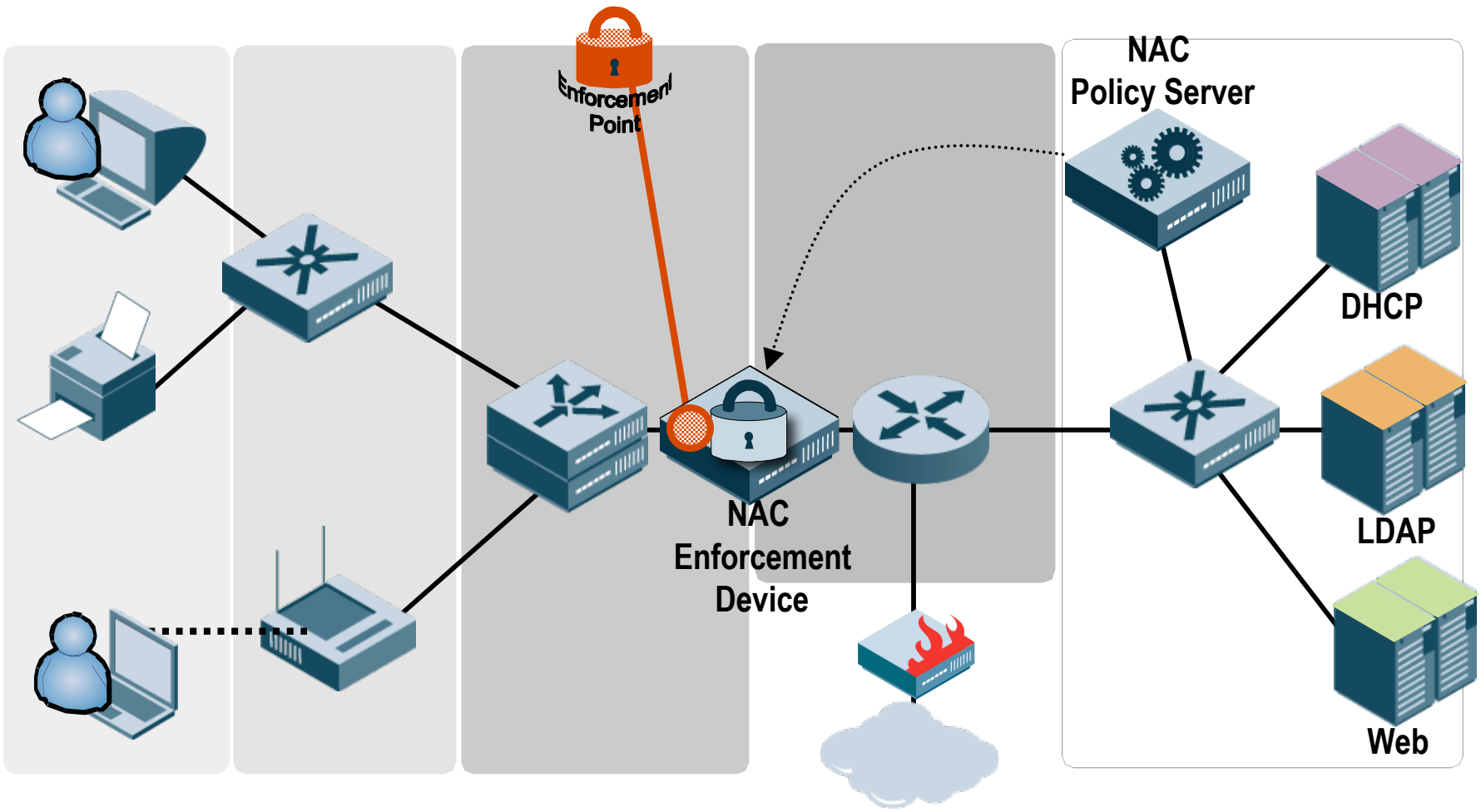
Granularity is a Spectrum Largely Determined by Hardware



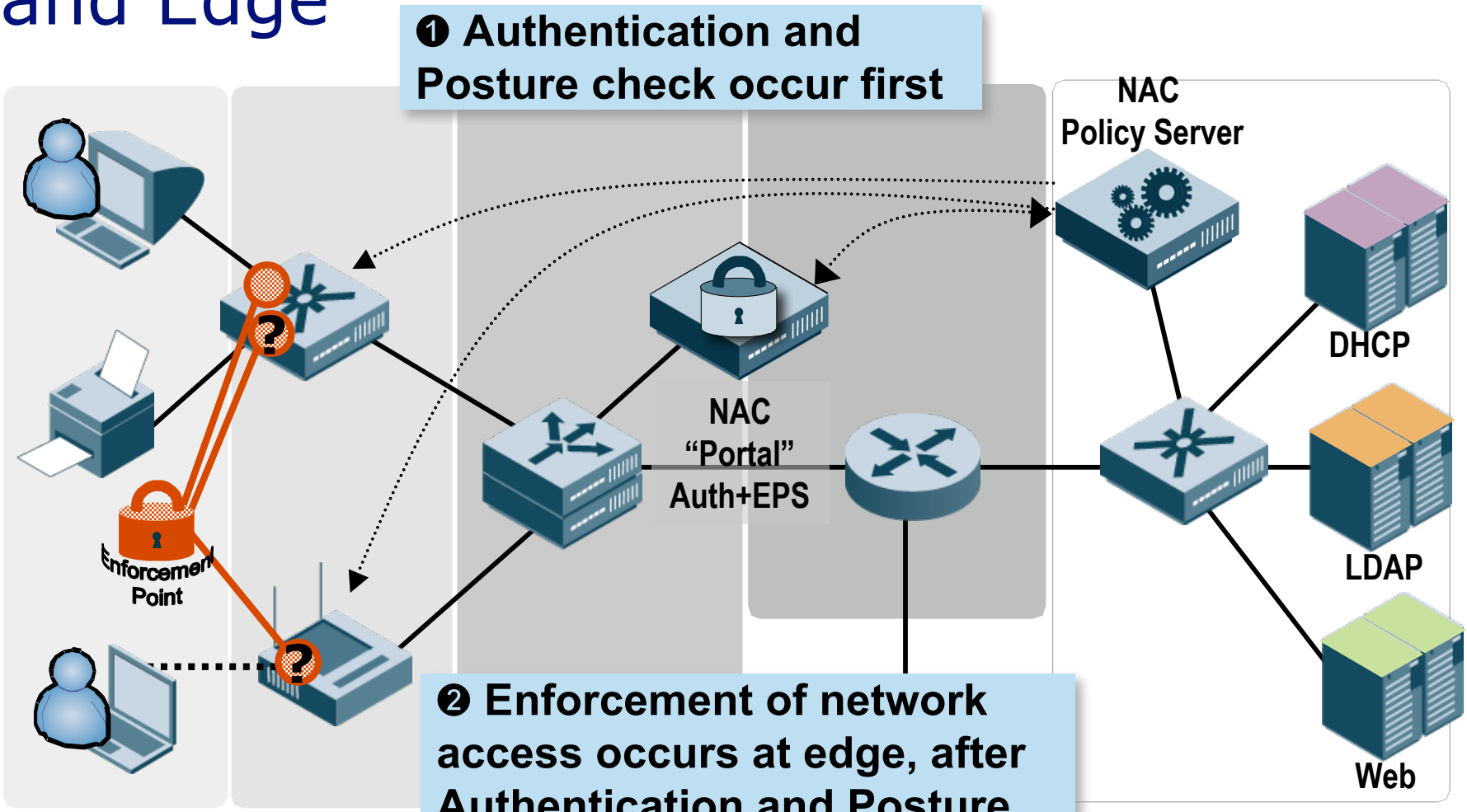
Edge Enforcement Occurs at the Point of Access to the Network



In-line Enforcement Occurs Deeper in the Network



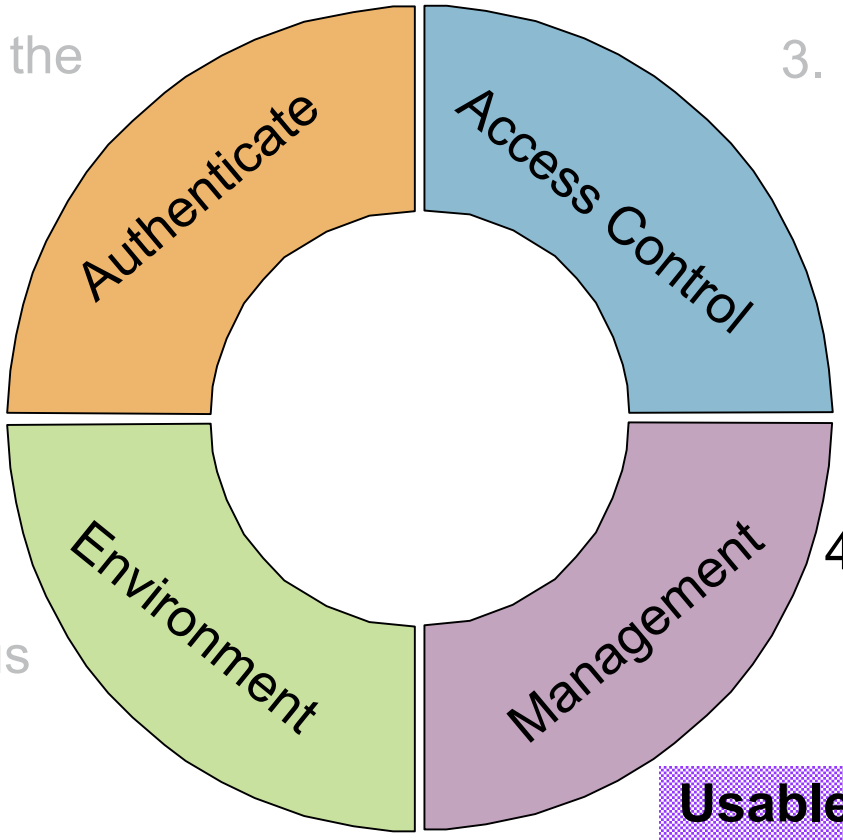
Hybrid Enforcement combines In-Line and Edge



Management of Policy is the Weak Link in most NAC Solutions

1. Authentication of the user

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

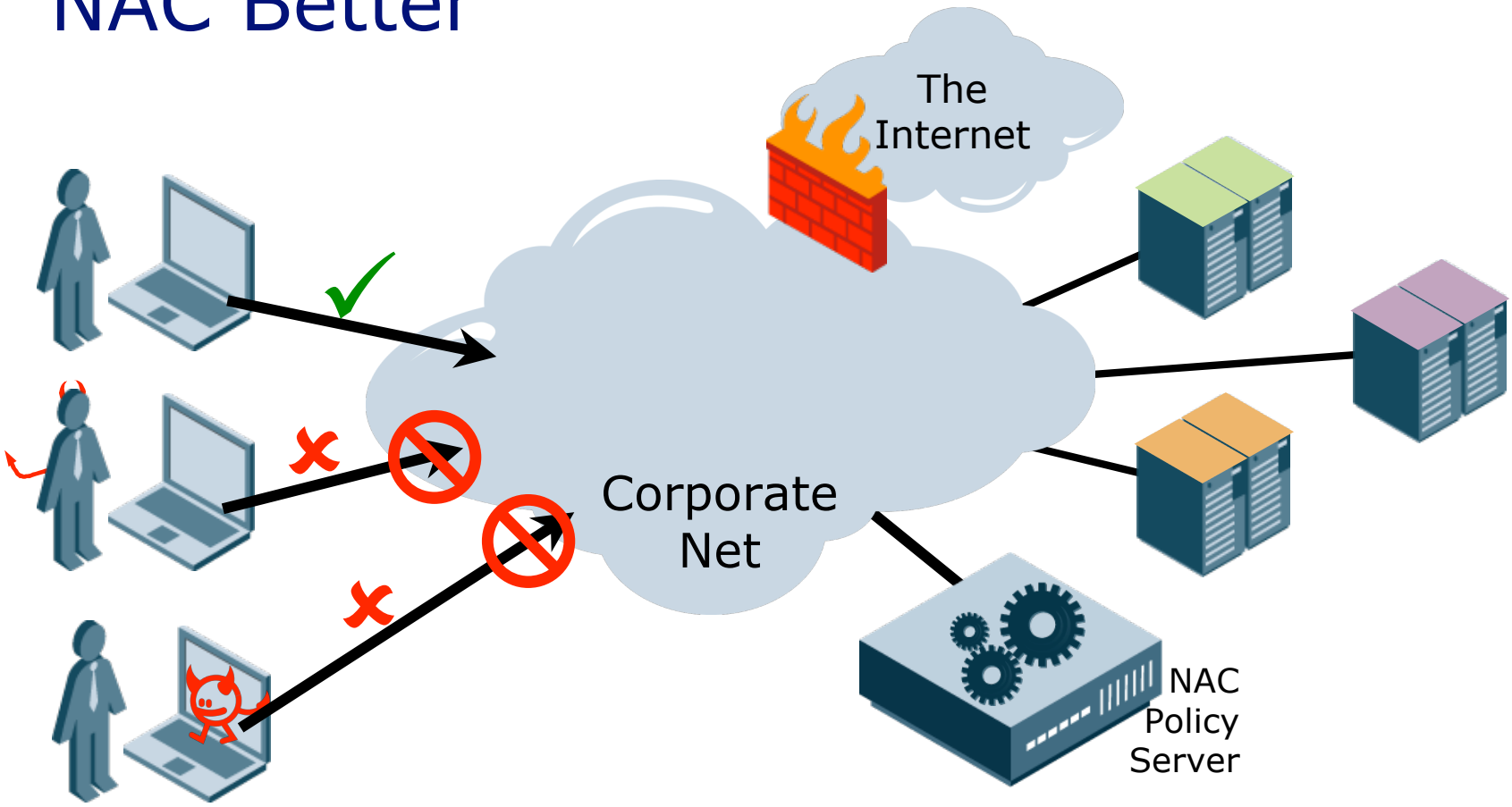


3. Control usage based on capabilities of hardware and security policy

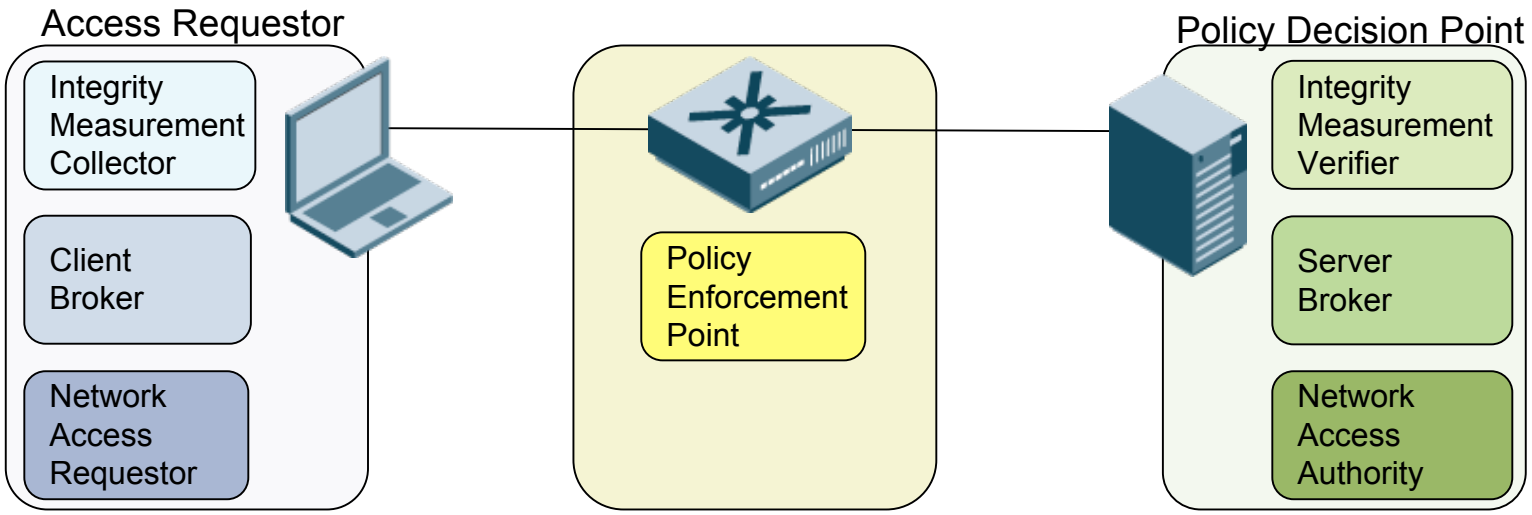
4. Manage it all

Usable management and cross-platform NAC normalization

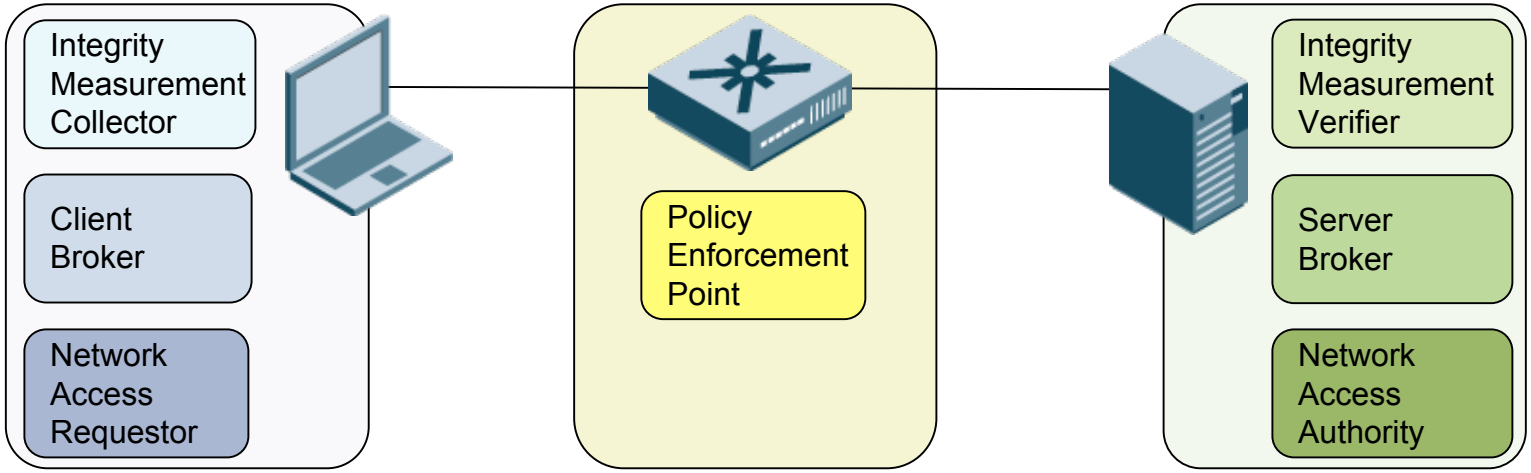
An Architecture Helps to Understand NAC Better



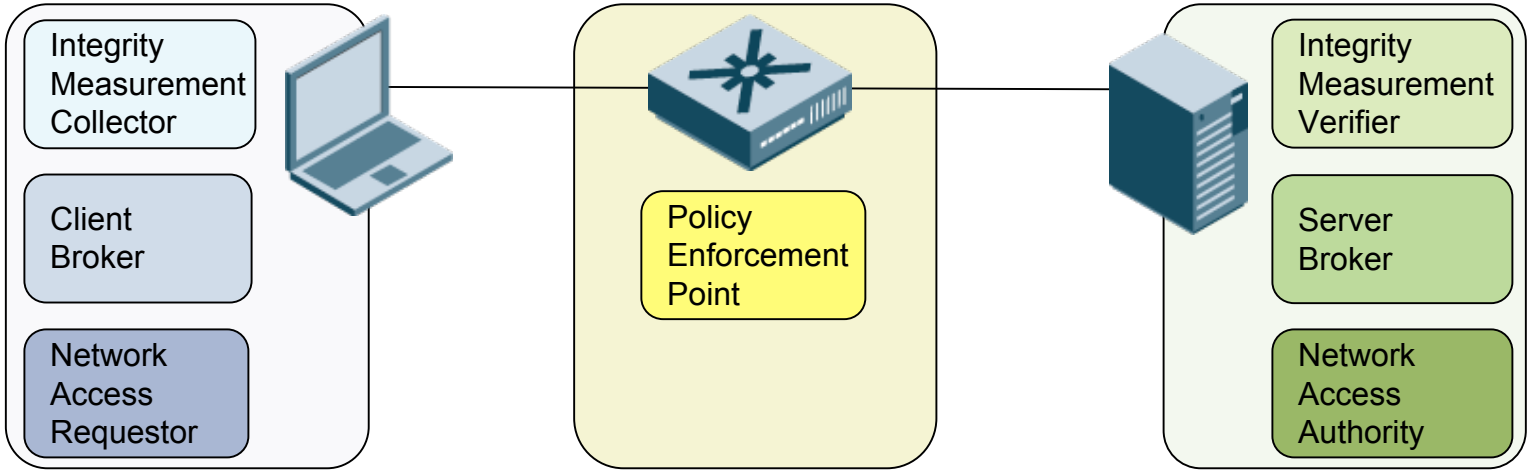
Lots of NAC Products… but Only a Few Good Architectures



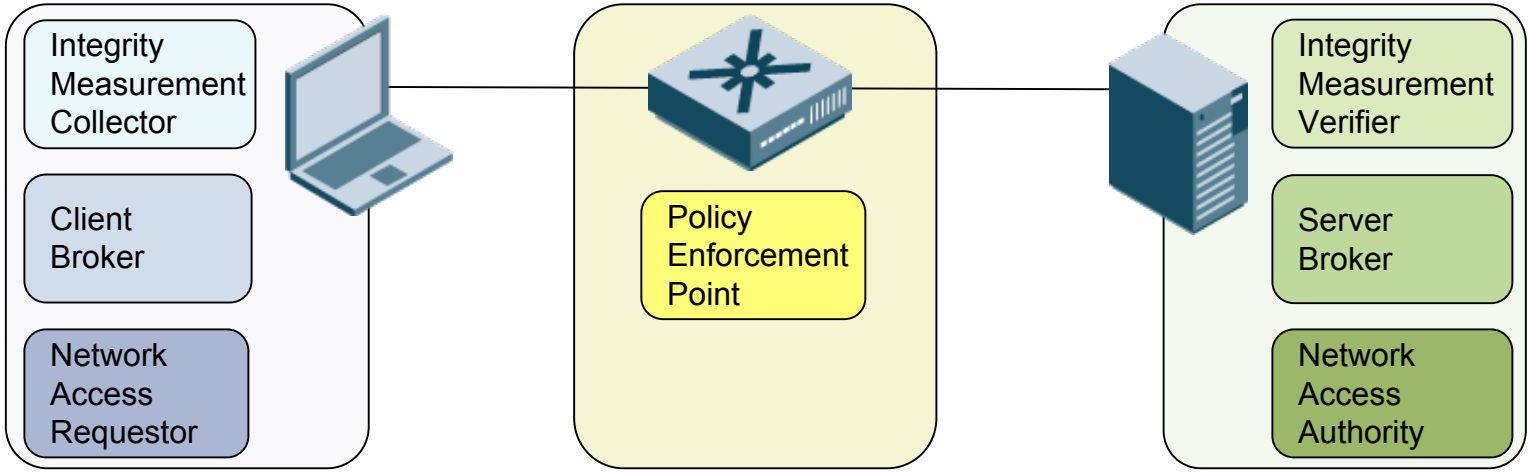
These are the TCG/TNC terms for each piece. IETF, Microsoft, and Cisco all have their own similar ones



What is it?	IETF NEA	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.	Network Enforcement Point	NAP Enforcement Server	Network Access Device



What is it?	IETF NEA	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?'	Posture Collector	System Health Agent	Posture Plug-in Apps
TNC Client Broker "Middleware" that talks to the Posture Collectors, collecting their data, and passes it down to Network Access Requestor	Posture Broker Client	NAP Agent	Cisco Trust Agent
Network Access Requestor Connects the client to network, such as 802.1X supplicant. Authenticates the user, and acts as a conduit for Posture Collector data	Posture Transport Client	NAP Enforcement Client	Cisco Trust Agent



What is it?	IETF NEA	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	Posture Validator	System Health Validator	Policy Vendor Server
TNC Server Broker "Middleware" acting as an interface between multiple Posture Validators and the Network Access Authority	Posture Broker Server	NAP Administration Server	Access Control Server
Network Access Authority Validates authentication and posture, then passing policy to the Network Enforcement Point.	Posture Transport Server	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