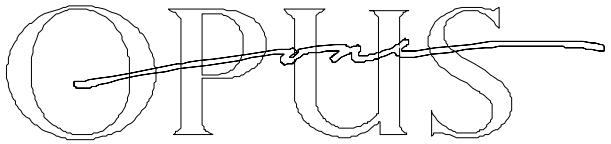
Answering The Hard

Joel M Snyder

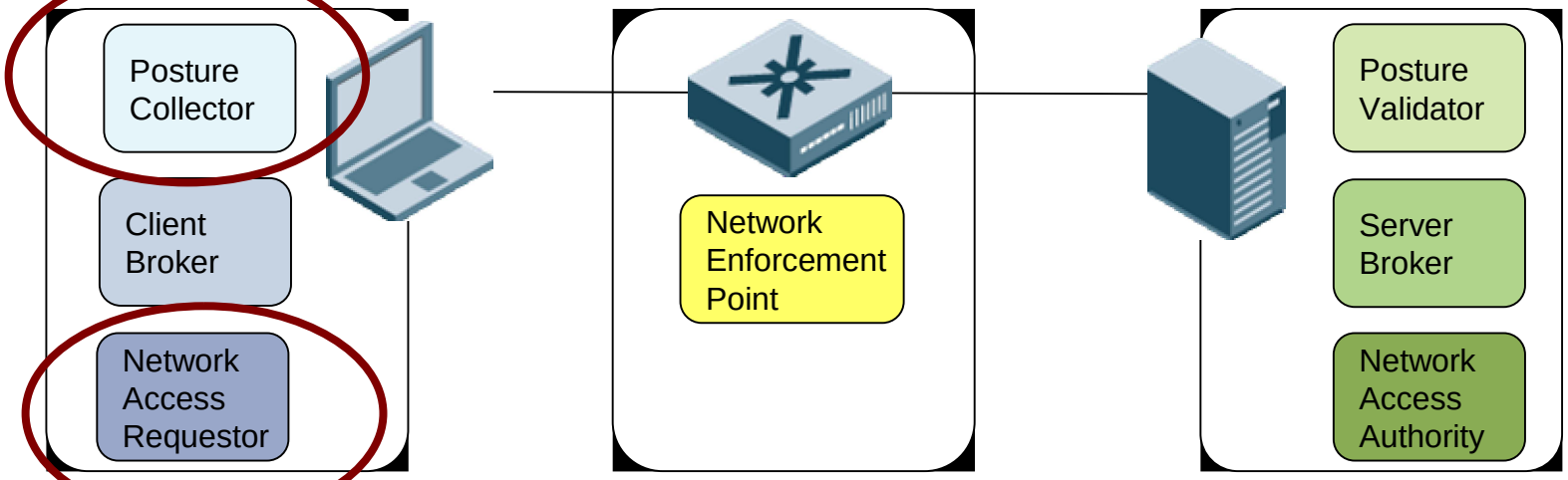
Senior Partner

Opus One

jms@opus1.com

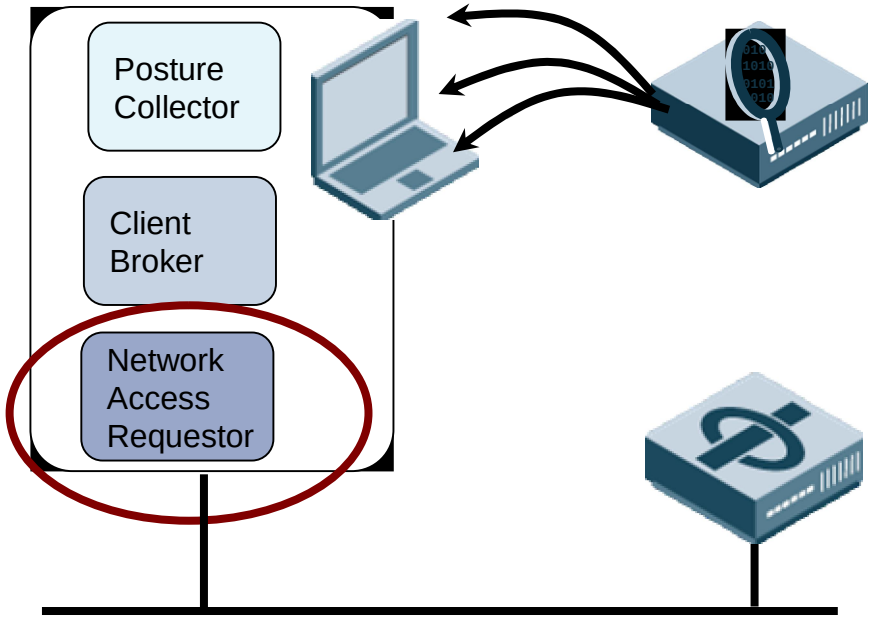


The NAC policy server gets its information from software running on the client



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

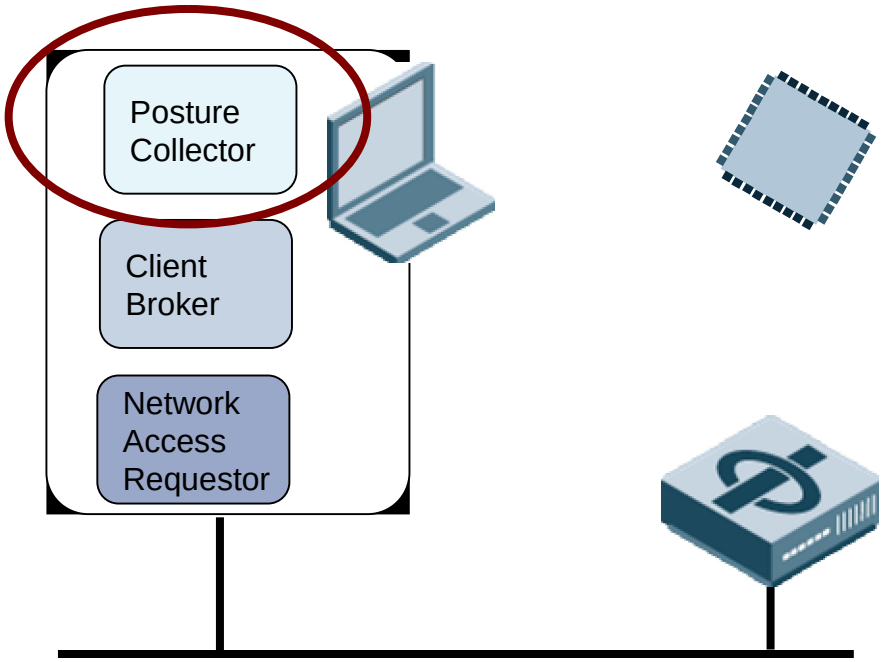
use MAC authentication for some devices



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



TCG/TNC has the TPM strategy to maximize “software trust”

Behavioral analysis also works here

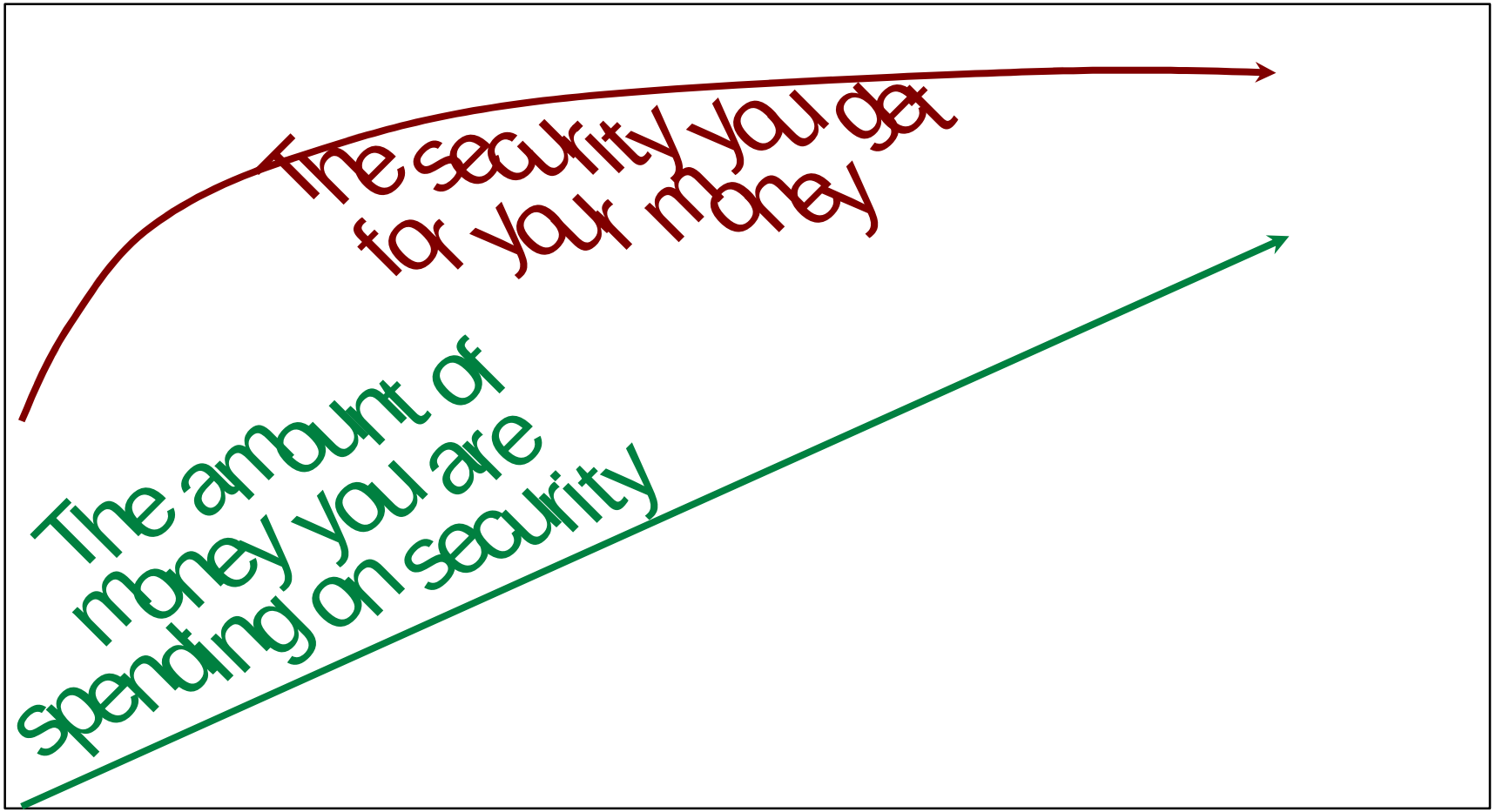
A sub-question: Do you care

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)

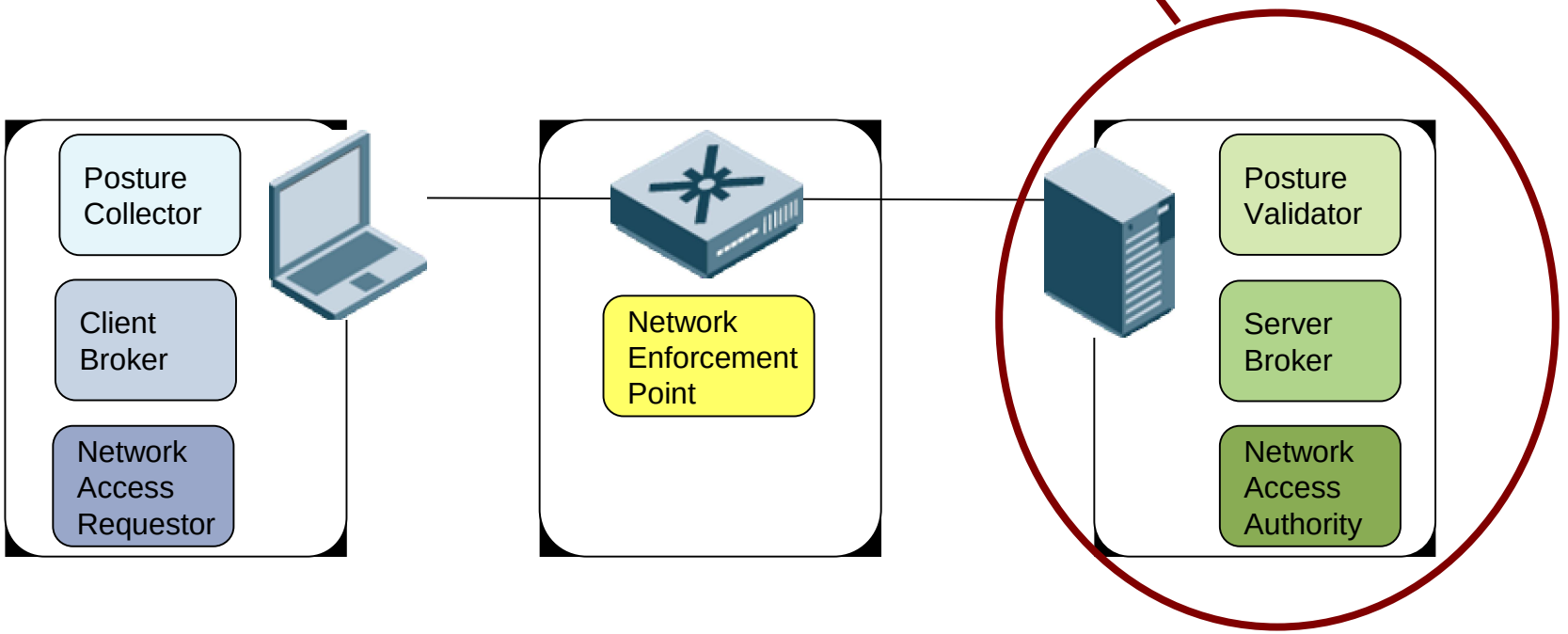
Beware perfect security



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

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

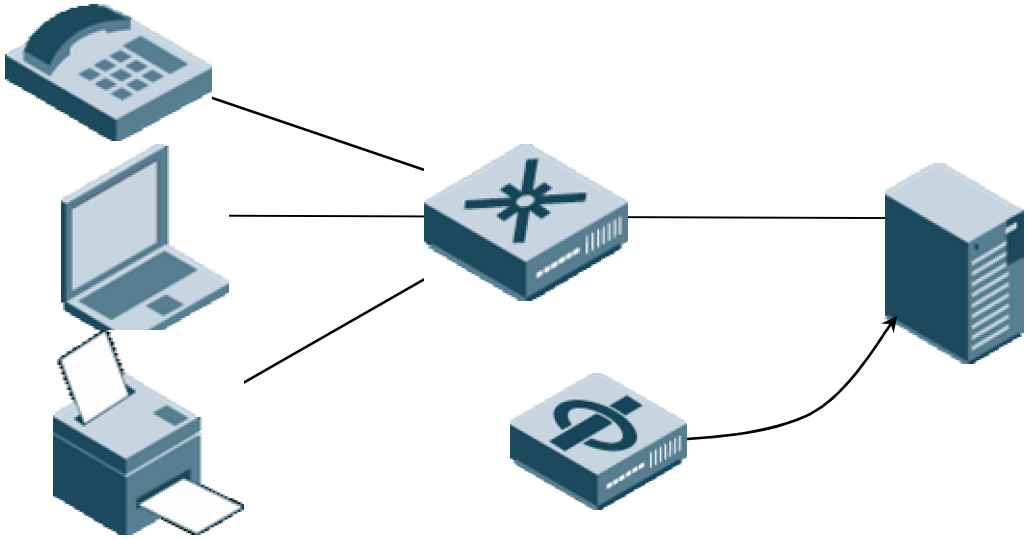


User thinks that they log in once per day

1000 users = .03 decision/second

MAC devices are re-authenticated every minute

1000 users = 30 decision/sec.



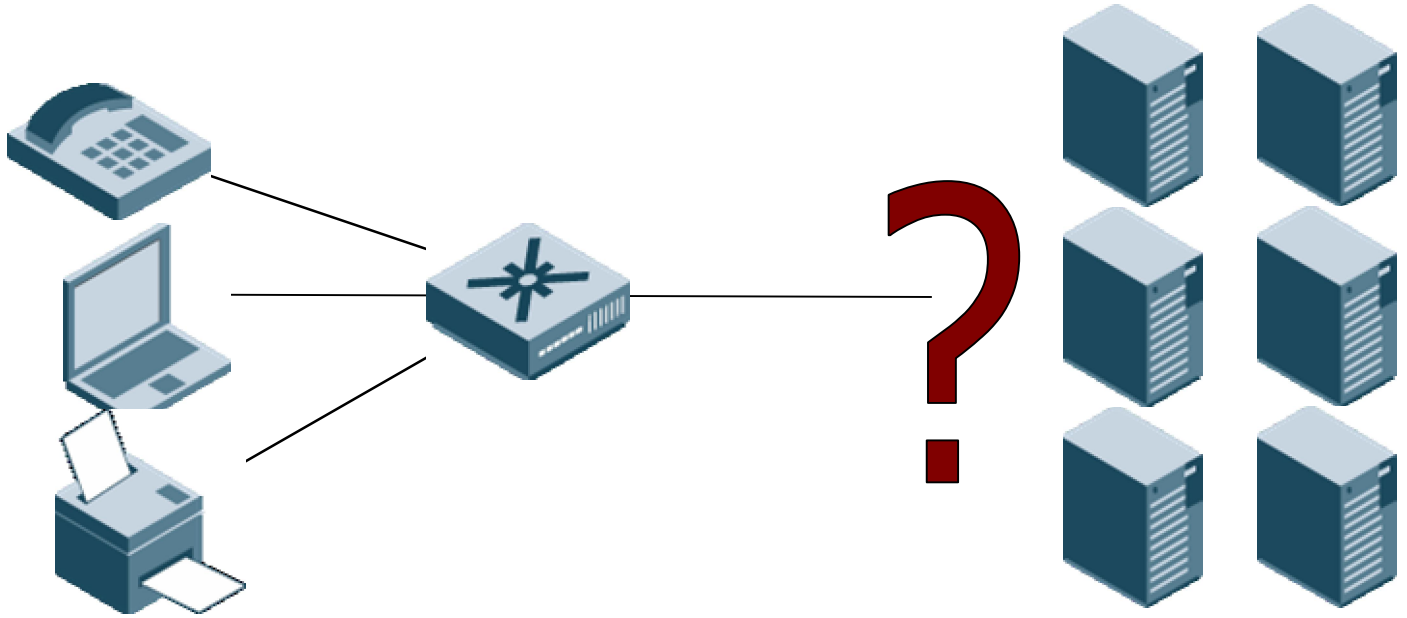
End-point security checks in every 15 minutes

1000 users = 1 decision/sec.

IDS+SIM+scanner generate 10 events a second

events = 10 decision/sec.

Policy servers need high availability



Can you build an active/active cluster?

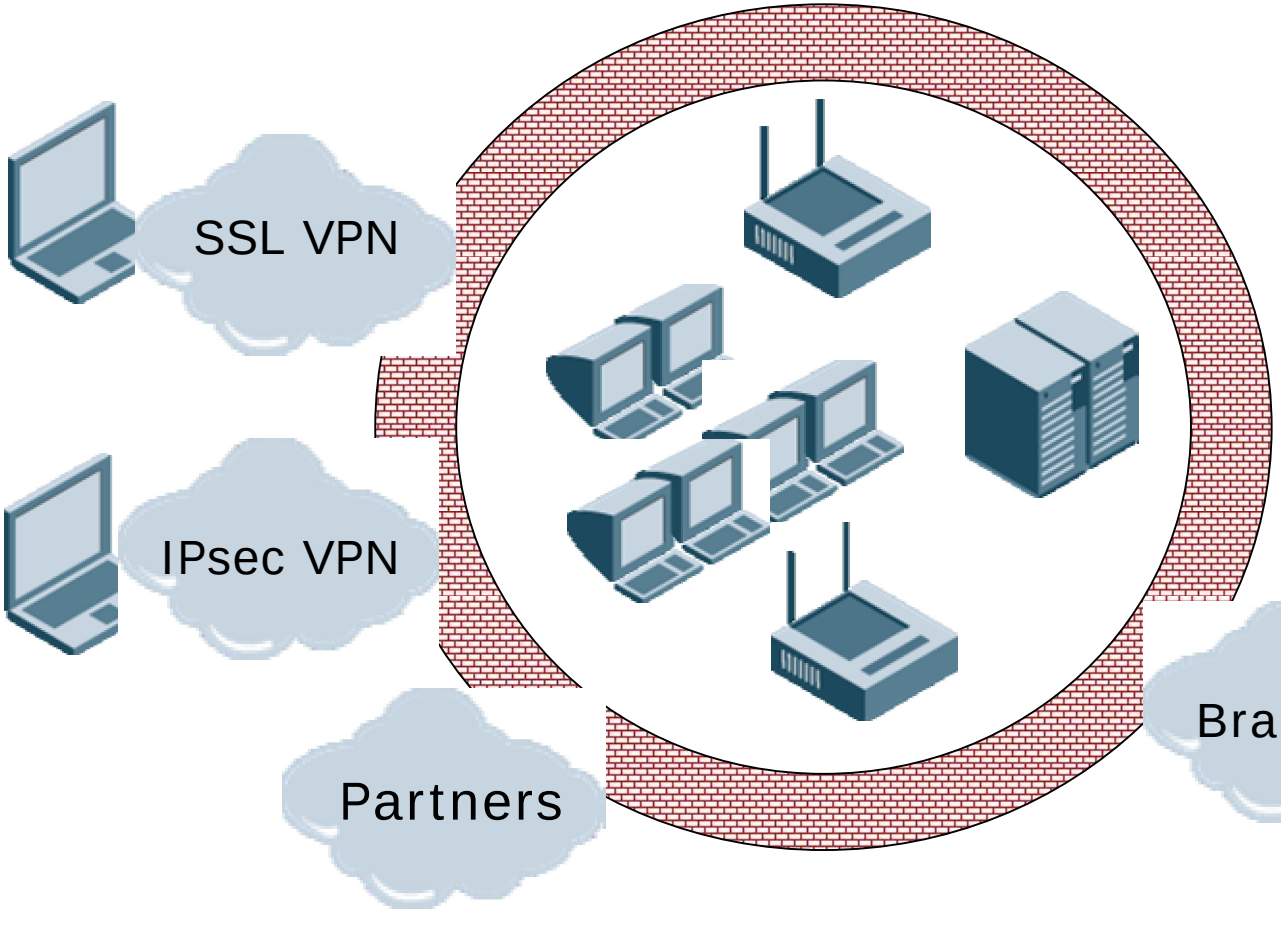
Are your decision points able to handle multiple locations?

Is the link to the backend database, such as Active Directory LDAP, properly provisioned for HA?

Action Items: Critical Services

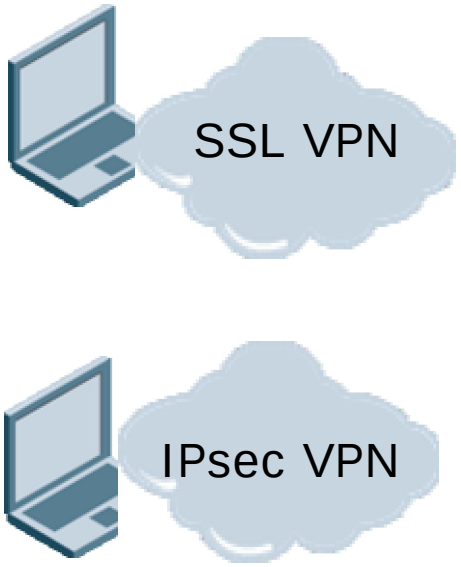
- Select NAC policy engine solutions that have:
  - Scalability, because you can't predict how many decisions/second you need
  - High availability, because the network can't stop working
- Review policy on enforcement points when contact is lost with the policy decision point
- Ensure that the link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

on identity and end-point posture



What works on the LAN should bring you value everywhere

SSL did NAC before NAC was even a buzzword

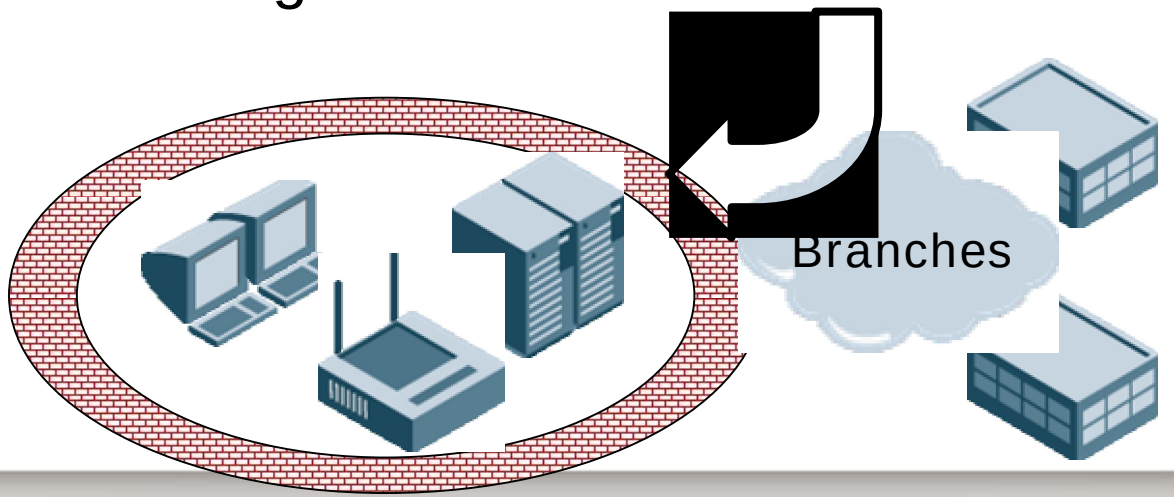


- SSL VPN vendors are ideally situated to be part of your NAC solution
- No SSL VPN vendor has yet integrated their policy engine with the NAC engine
- Obviously, you want to have fewer engines and fewer bits of software floating around

- 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"

L3 enforcement

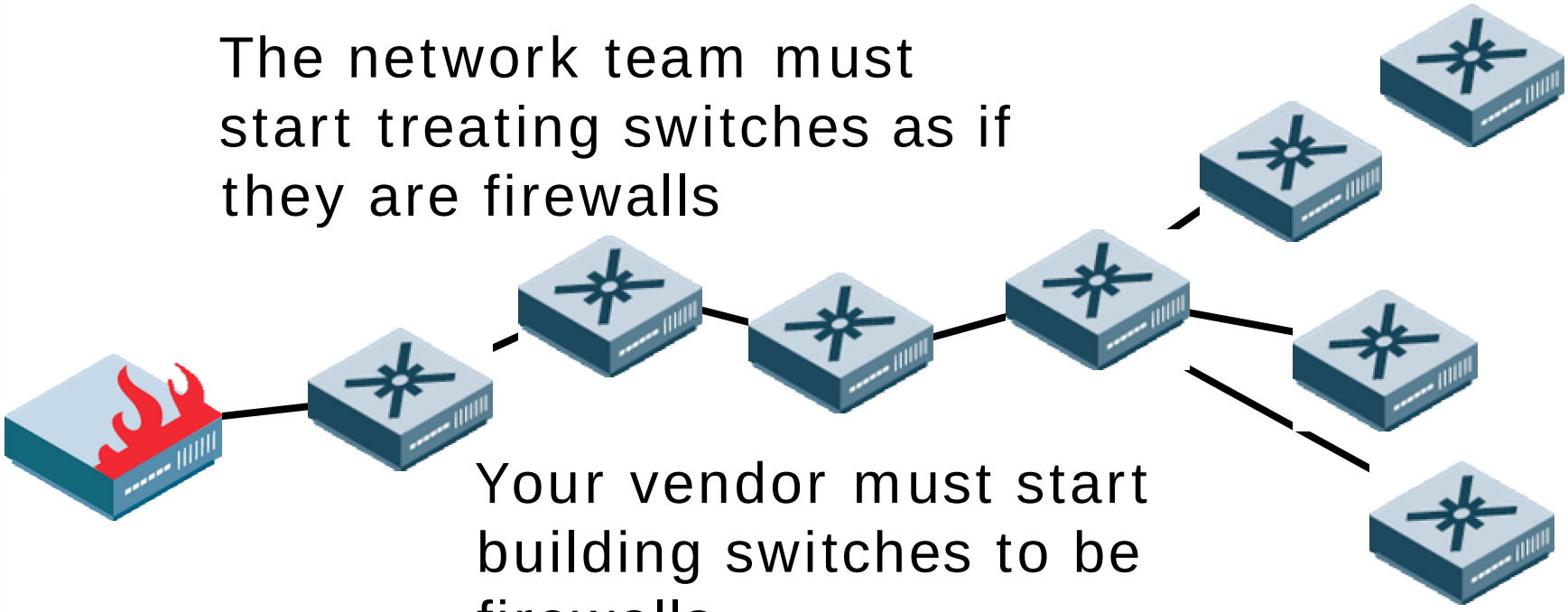


Wireless

- 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)
- vendors are “on board” with your NAC strategy

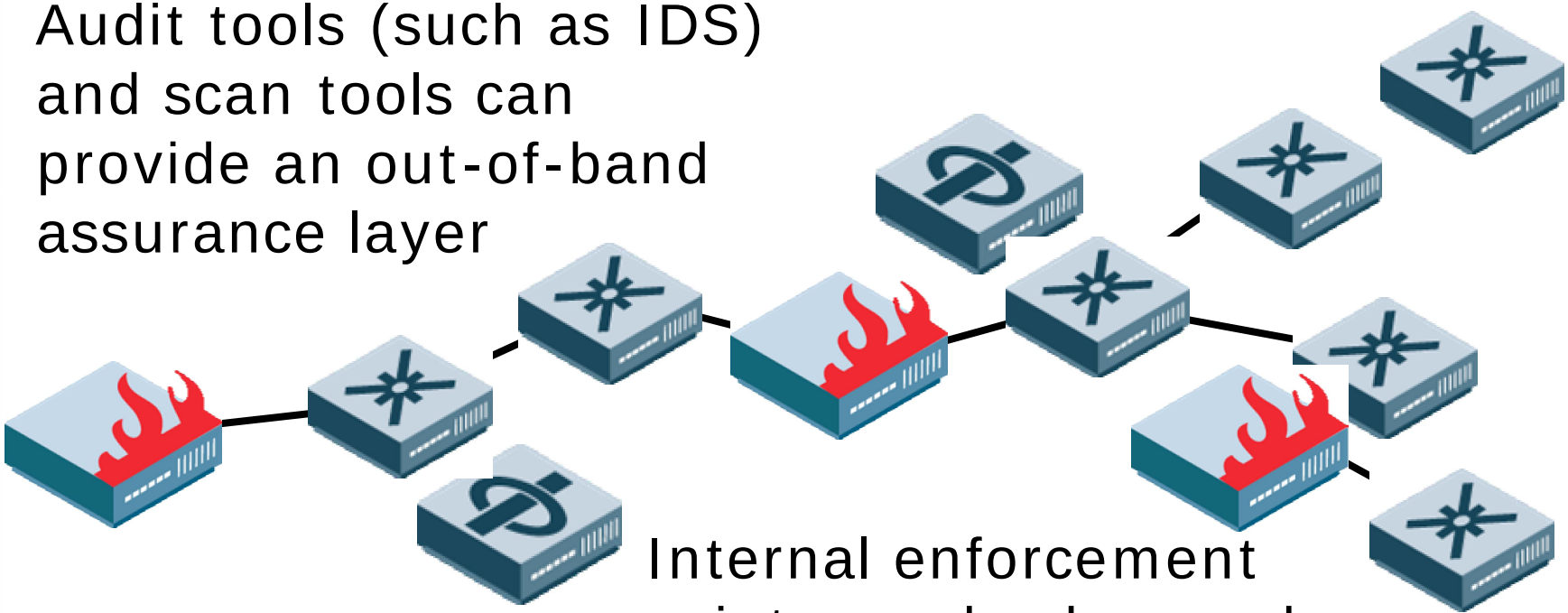
network, the network must be secure

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



Your vendor must start building switches to be firewalls

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

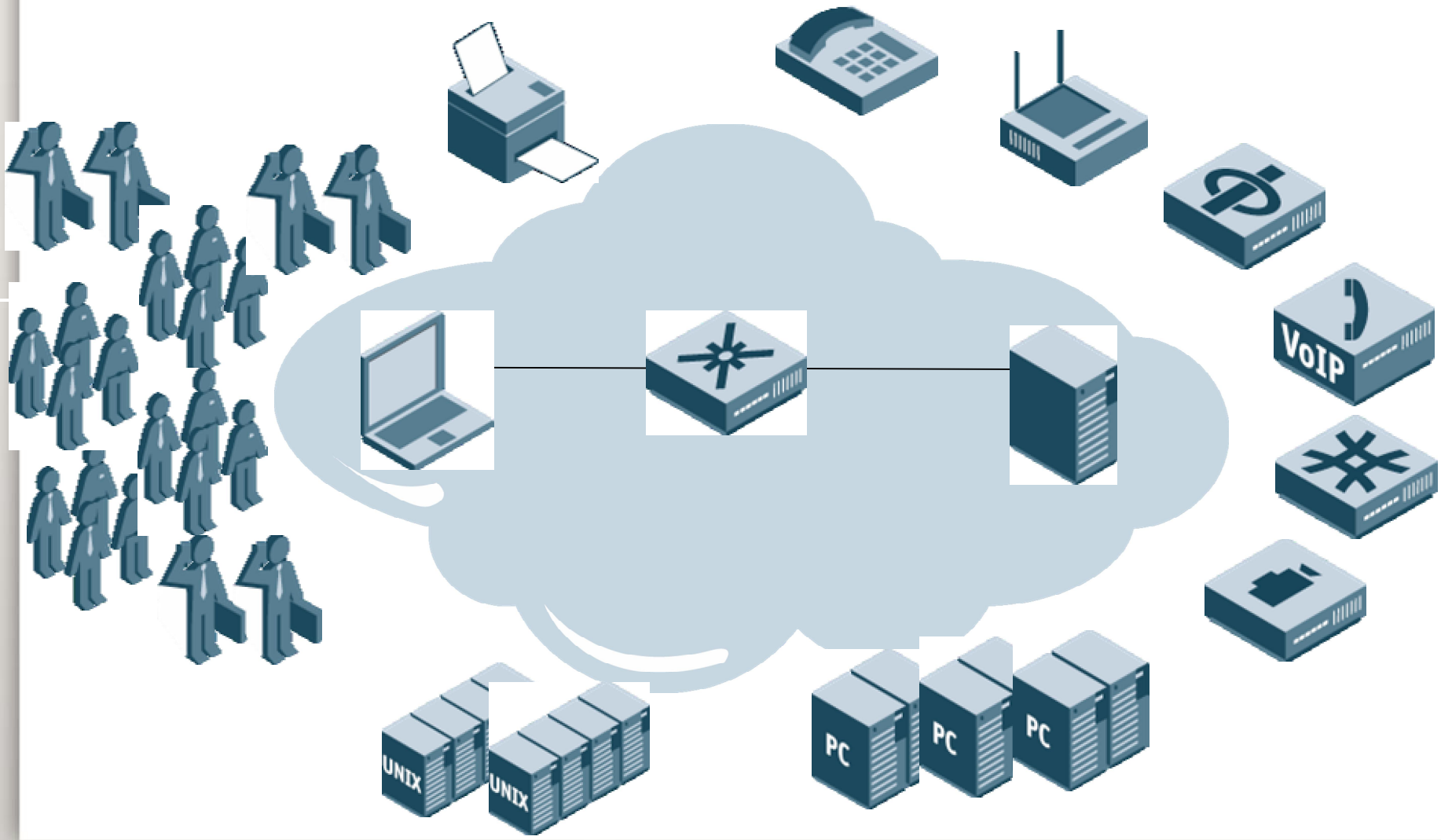


Internal enforcement points can backup and extend switch enforcement

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
-
  firewall
- Evaluate whether your infrastructure is ready to transition from “connection utility” to “enforcement point”

“ ”


VoIP
UNIX
UNIX
PC
PC
PC

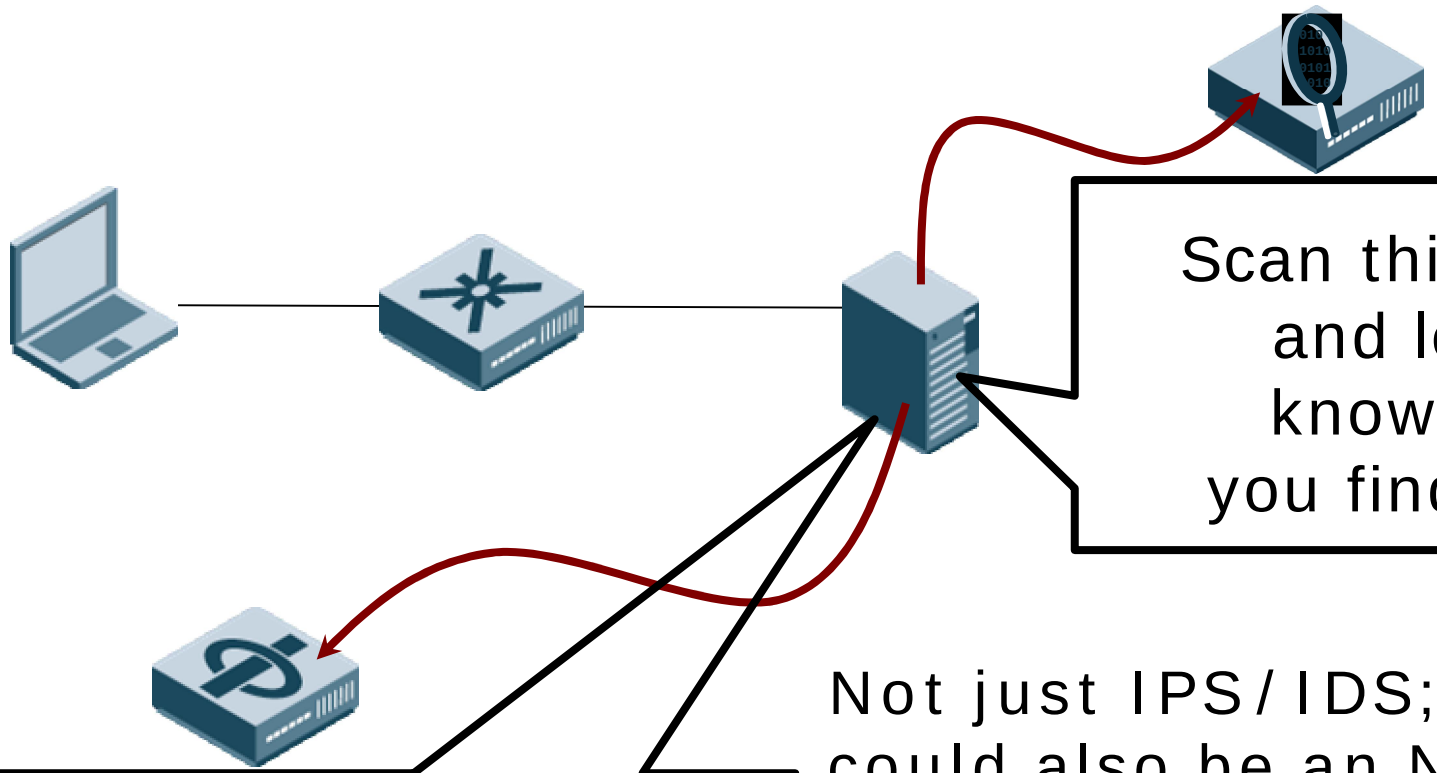
You need to consider NAC's interaction with the rest of the world

Layers 8, 9, and 10

- The all-important religious, political, and economic
- (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?

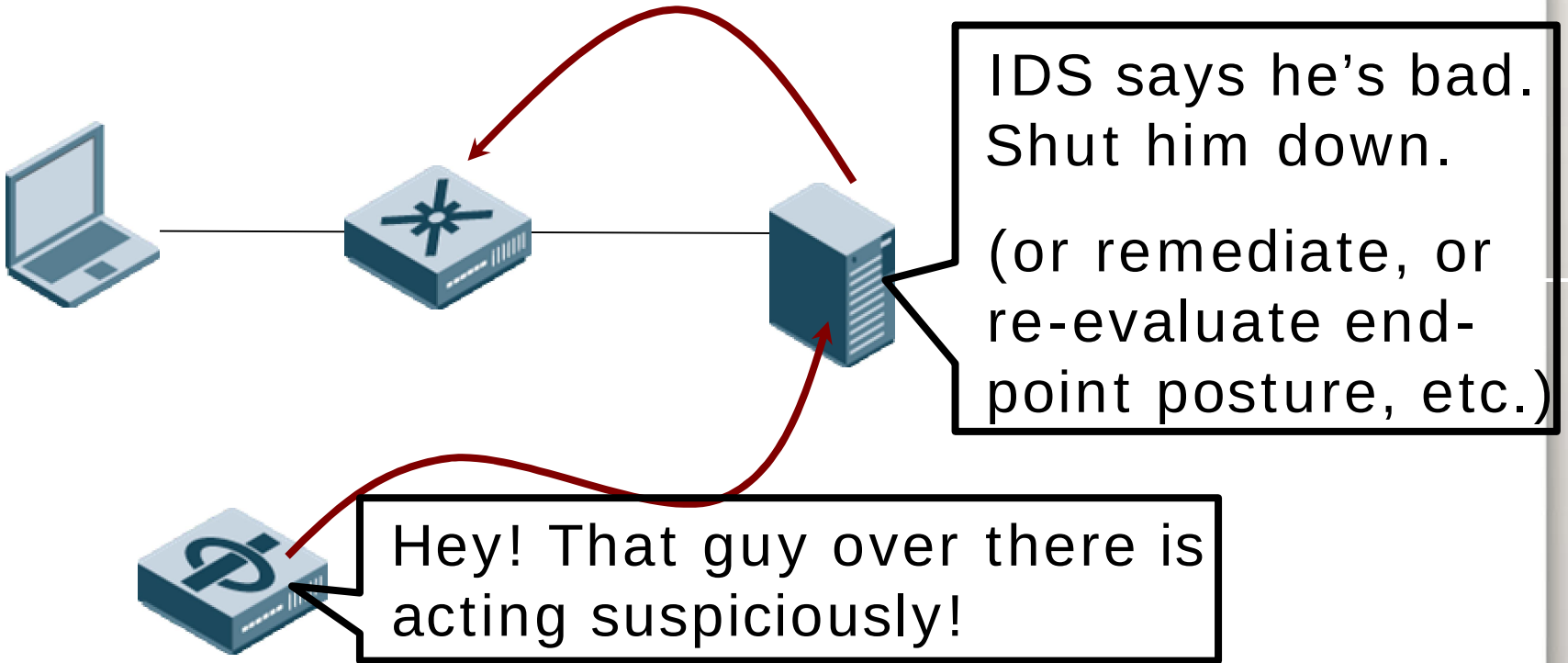


Scan this guy and let me know what you find out.

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

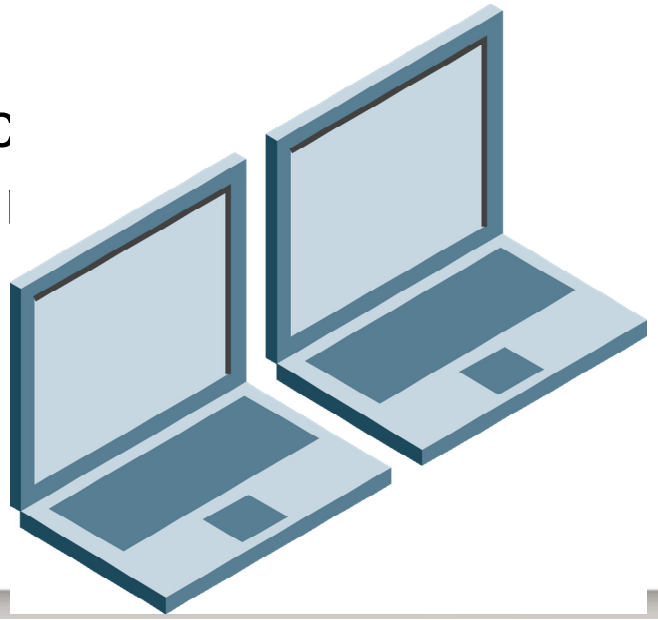
IPS (and IDS) could talk to NAC



devices is an evolving story

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

This integration is espec
critical to you if end-poi
security is one of your
driving factors for 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

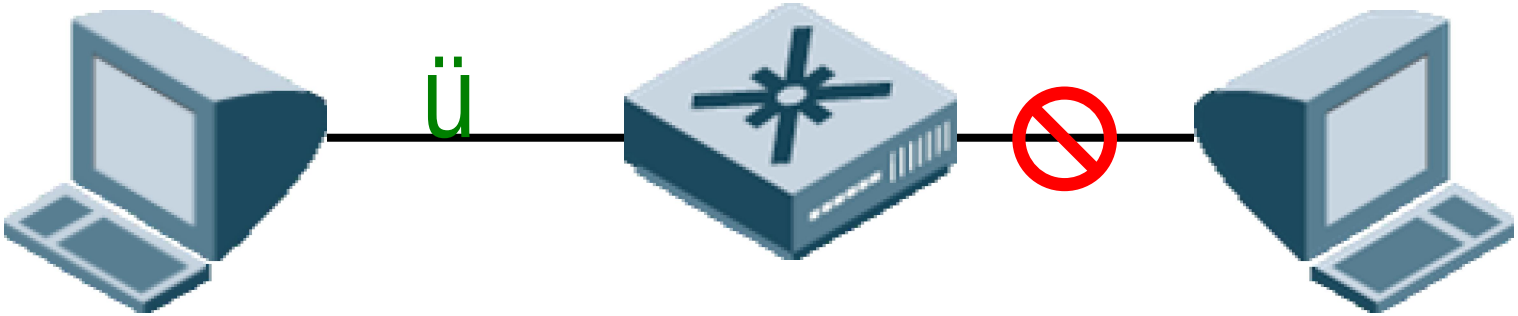
NAC Fundamentally Changes the

Before:
Switching Infrastructure

- You plug things in, and they work

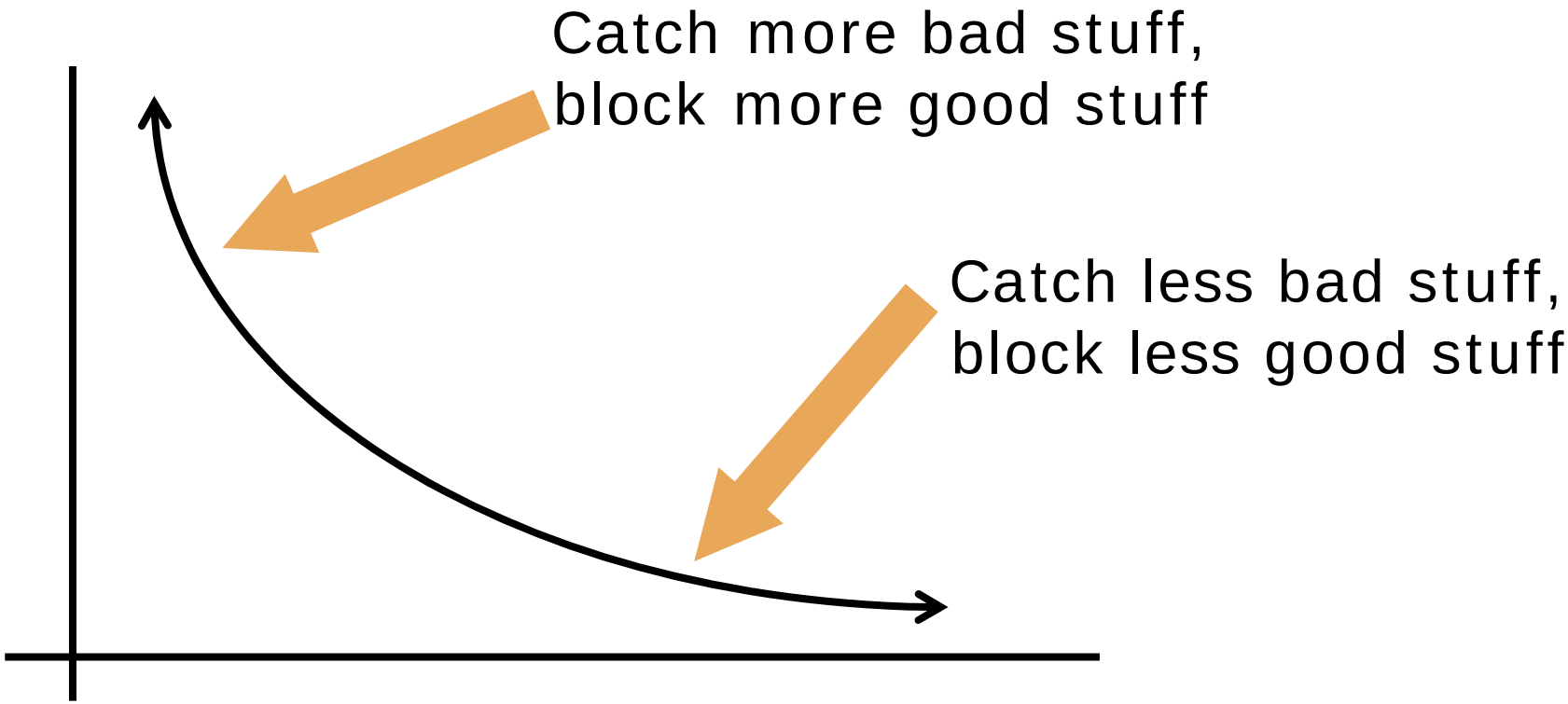
After:
Policy Enforcement Infrastructure

- You plug things in, and maybe they work



Dealing with a fundamental change

- Simple Fact: All Security Creates False Positives

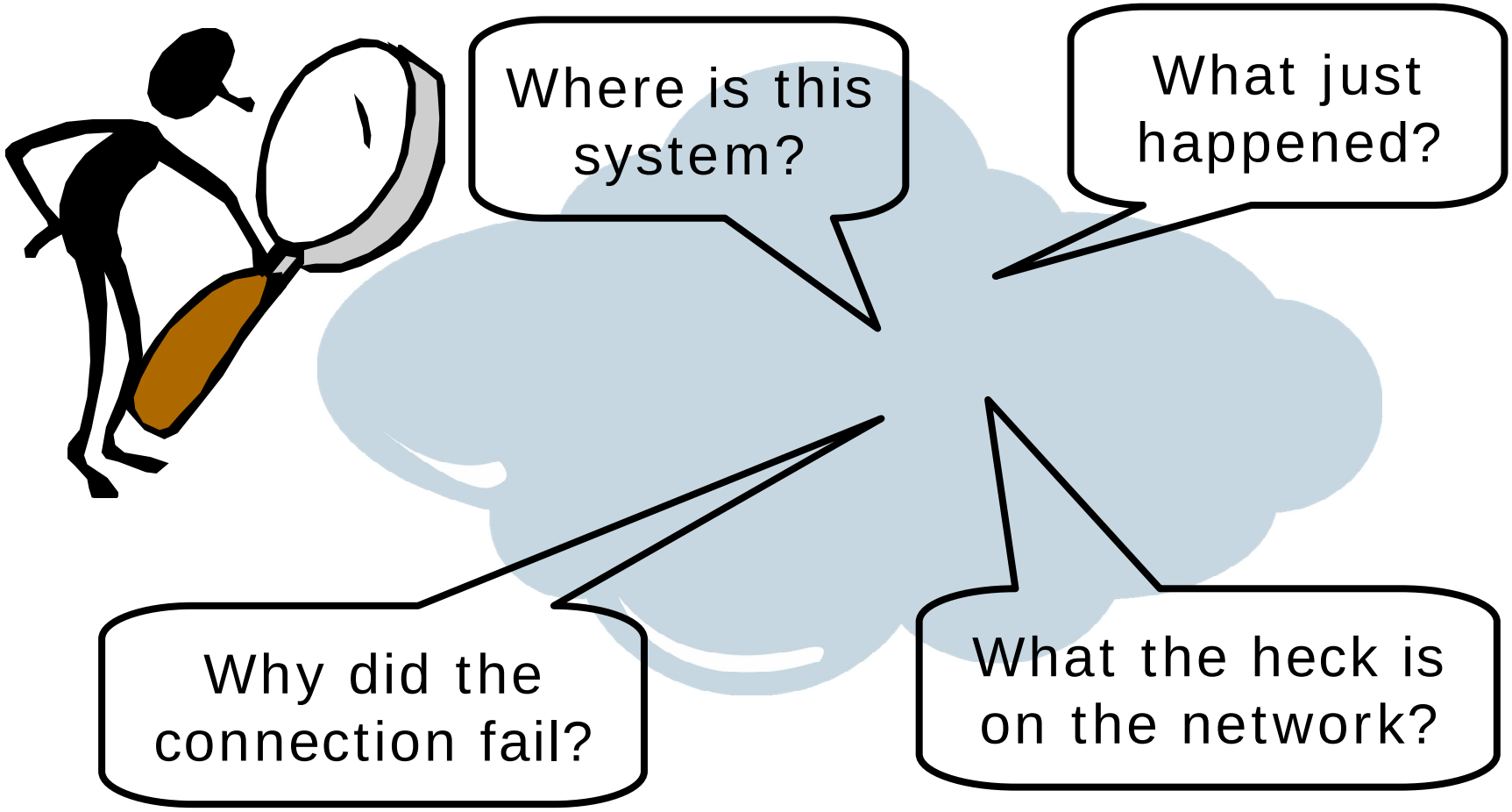


Principle of NAC

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

(Not to Keep Devices off of the Network)

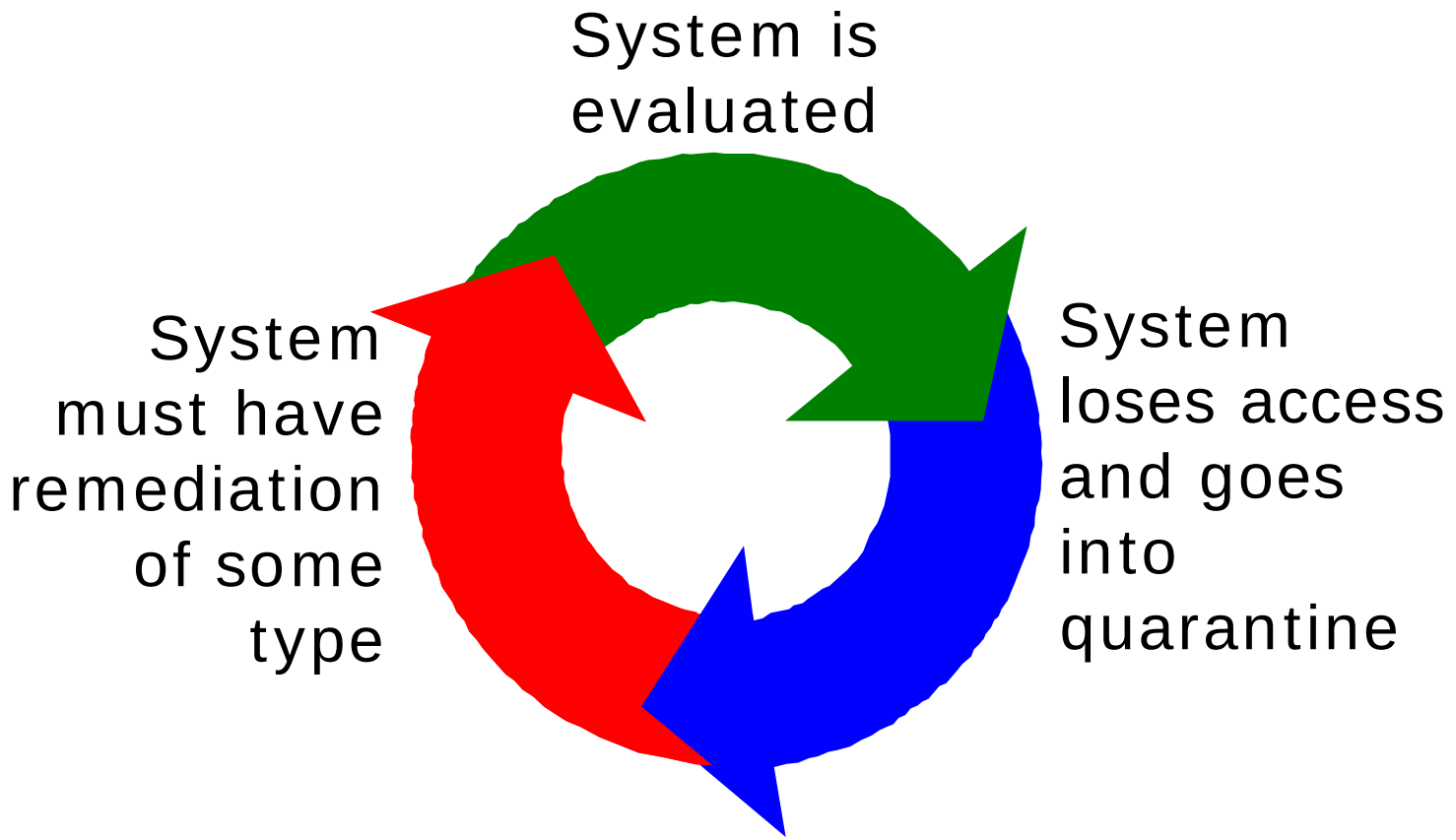
Visibility gives you the best opportunity to avoid problems



Action Items: Change in Thinking

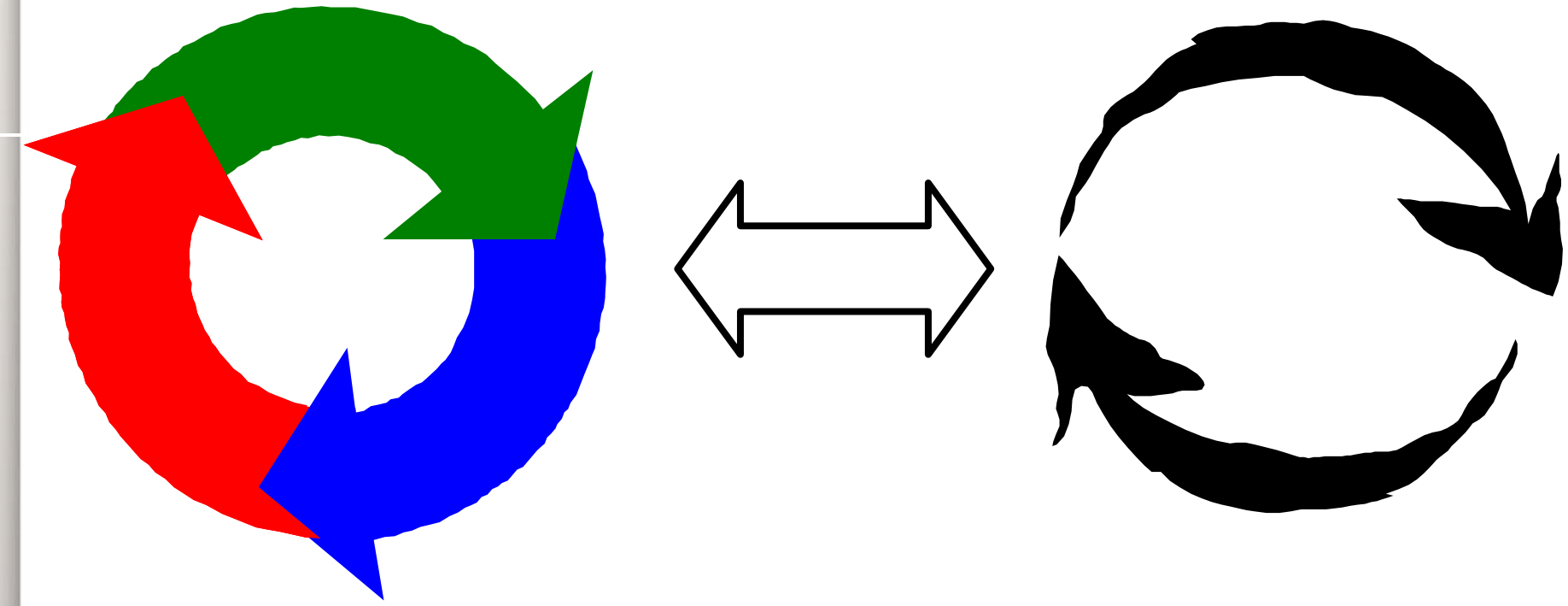
-
  you run into problems and before they start affecting network usage
- Become “forearmed” by making use of existing tools for network discovery and visibility as part of your NAC plans
- Where appropriate, add new visibility tools to your network to support NAC help desk as well as audit and trust-but-verify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

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



INFORMATION SECURITY | SearchSecurity.com | INFORMATION SECURITY DECISIONS

NAC end-point strategy must ’s strategy



. Detect . Remediate . Quarantine . Allow .

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

- 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

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

- But here are some things people have said

- è Reduced help-desk calls (after initial spike)
- è Reduced cost of RIAA subpoena answers
- è Better ability to answer compliance requirements
- è Reduced cost on Moves/Adds/Changes by making the network more dynamic
- è Reduced load on "high cost" staff by allowing "lower cost" staff to grant access

Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com