Improving Your Network Defense

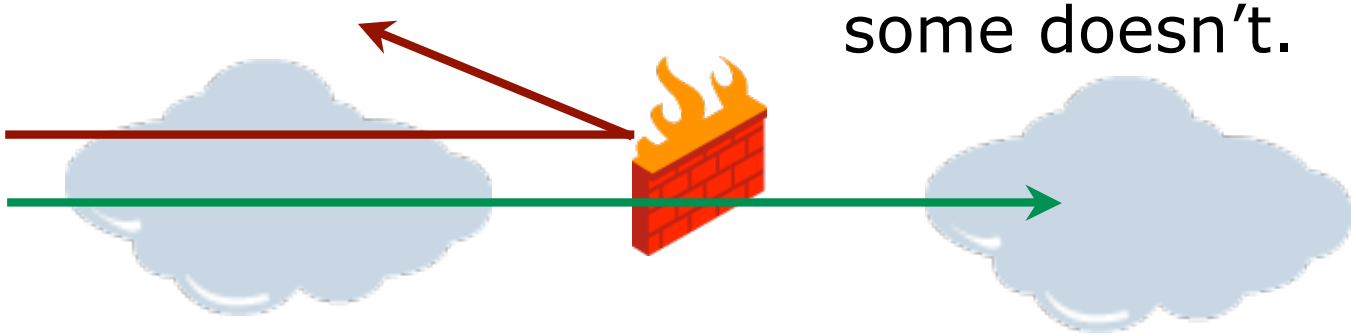
Joel M Snyder
Senior Partner
Opus One
jms@opus1.com

Agenda: Improving Your Network Defense

- **What's the Thesis?**
- **Intrusion Detection**
- **Collecting Information**
- **Enabling Features**
- **Vulnerability Analysis**
- **Network Access Control**

A Firewall Blocks Traffic, but…

- **A firewall cannot tell you how your network is operating**
- **A firewall cannot tell you whether your network is secure**



Some traffic gets through; some doesn't.

What do you know about the traffic that got through?

Improve Network Security with Visibility and with Control

Visibility

- **Means: Knowing what is happening on the network from a SECURITY point of view**
- **Also may mean: Knowing what is happening on the network from a NETWORK point of view**
- **(these "points of view" are not that far off)**

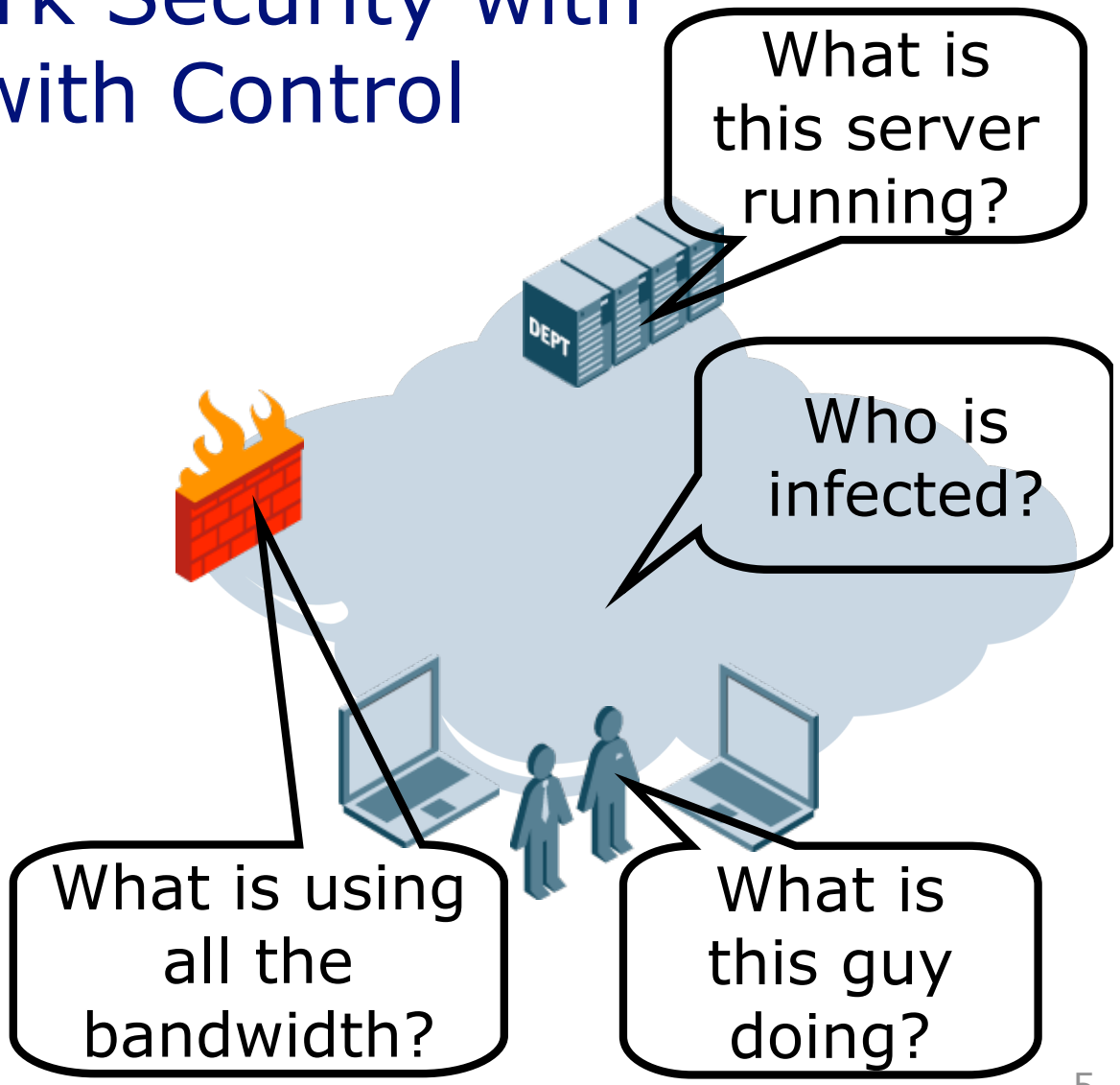
Control

- **Means: Enabling control points on your network to direct and manage traffic**
- **Means: Changing the network to be a secure asset rather than an anything-goes utility**

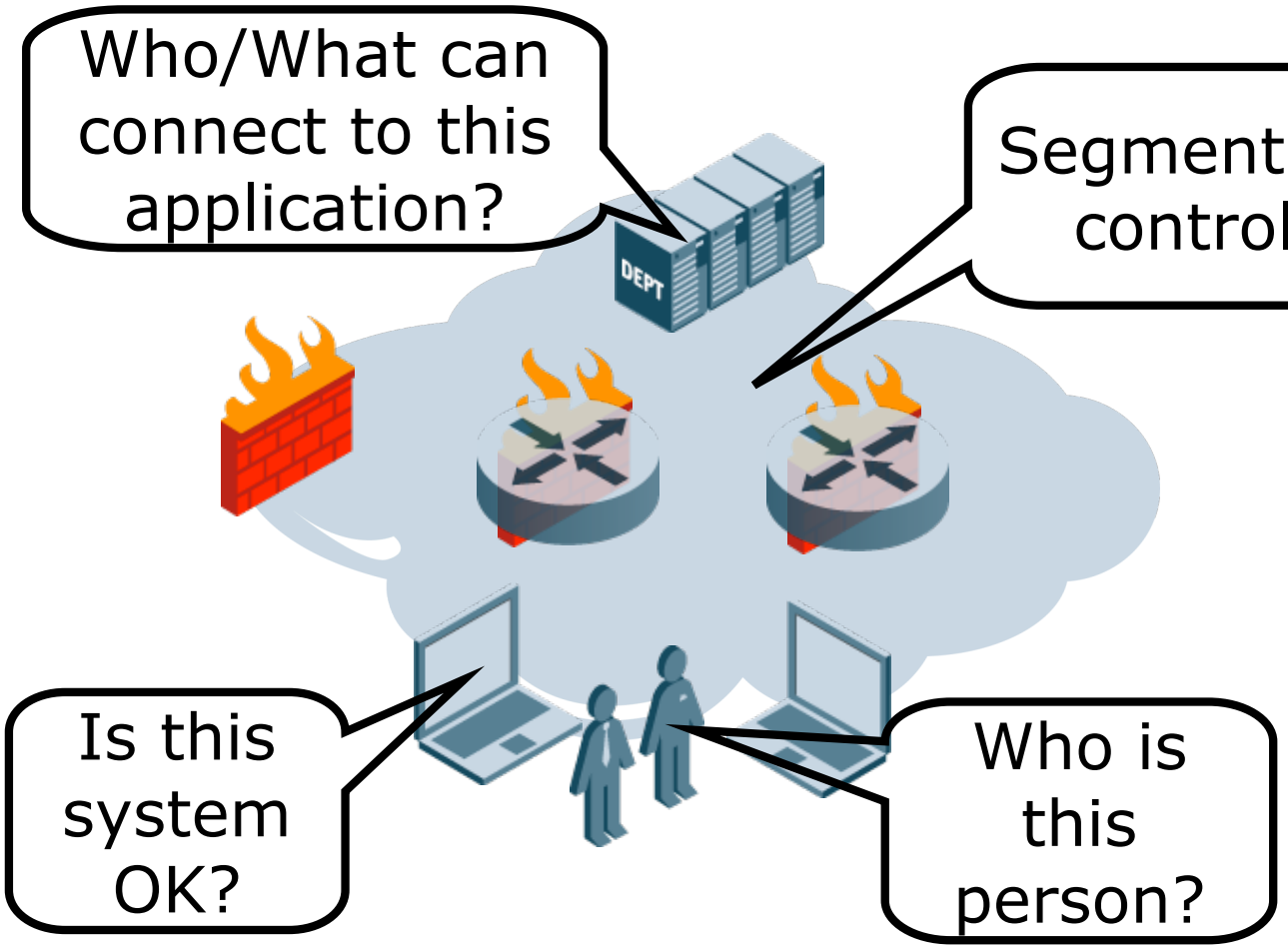
Improve Network Security with **Visibility** and with Control

Visibility

- **Means: Knowing what is happening on the network from a SECURITY point of view**
- **Also may mean: Knowing what is happening on the network from a NETWORK point of view**
- **(these "points of view" are not that far off)**



Improve Network Security with Visibility and with **Control**



Control

- **Means: Enabling control points on your network to direct and manage traffic**
- **Means: Changing the network to be a secure asset rather than an anything-goes utility**

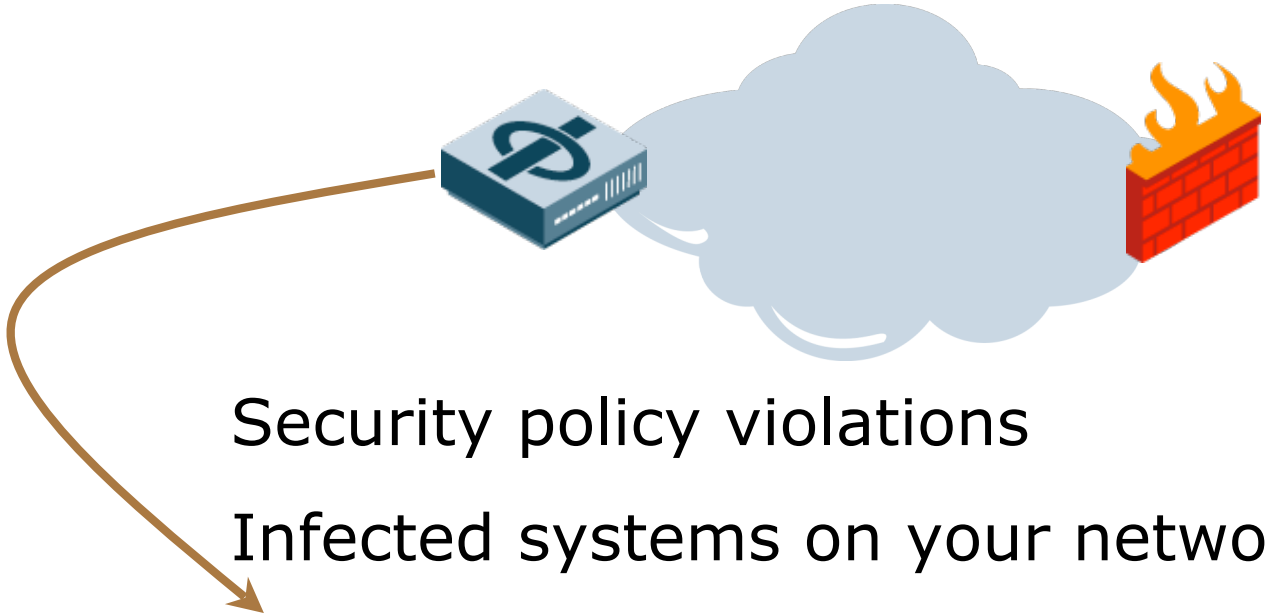
Goal:

Increase your ability to see security issues within the network

Strategy:

Add NIDS Intrusion Detection Sensors inside the core & DMZ networks

IDS is not *really* for detecting Intrusions



Security policy violations

Infected systems on your network

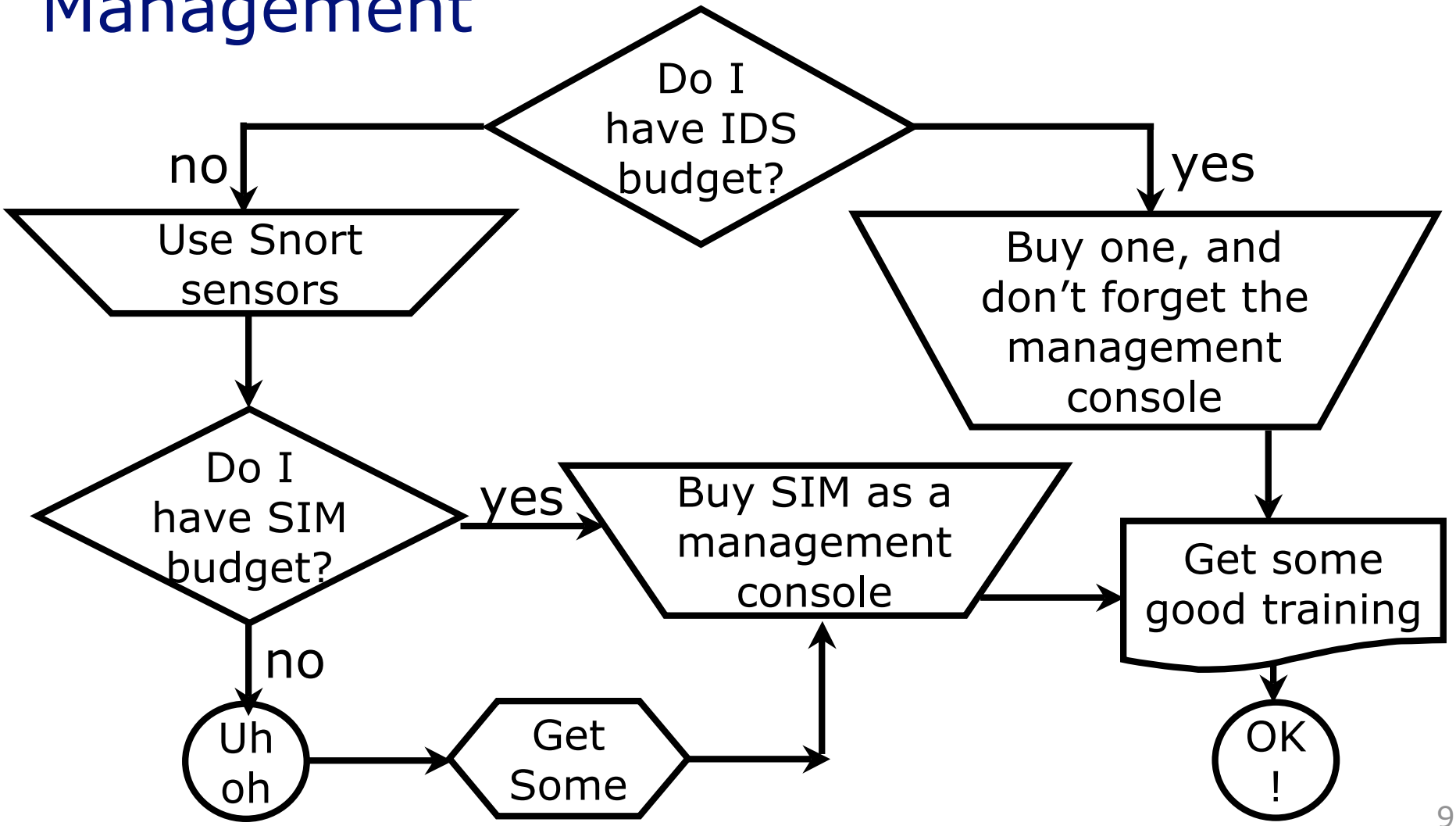
Mis-configured applications, firewalls, and systems

Information leakage

Unauthorized servers and clients

A properly configured firewall and patch discipline means that an IDS is unlikely to catch an "intrusion"

What's hard about IDS is Management



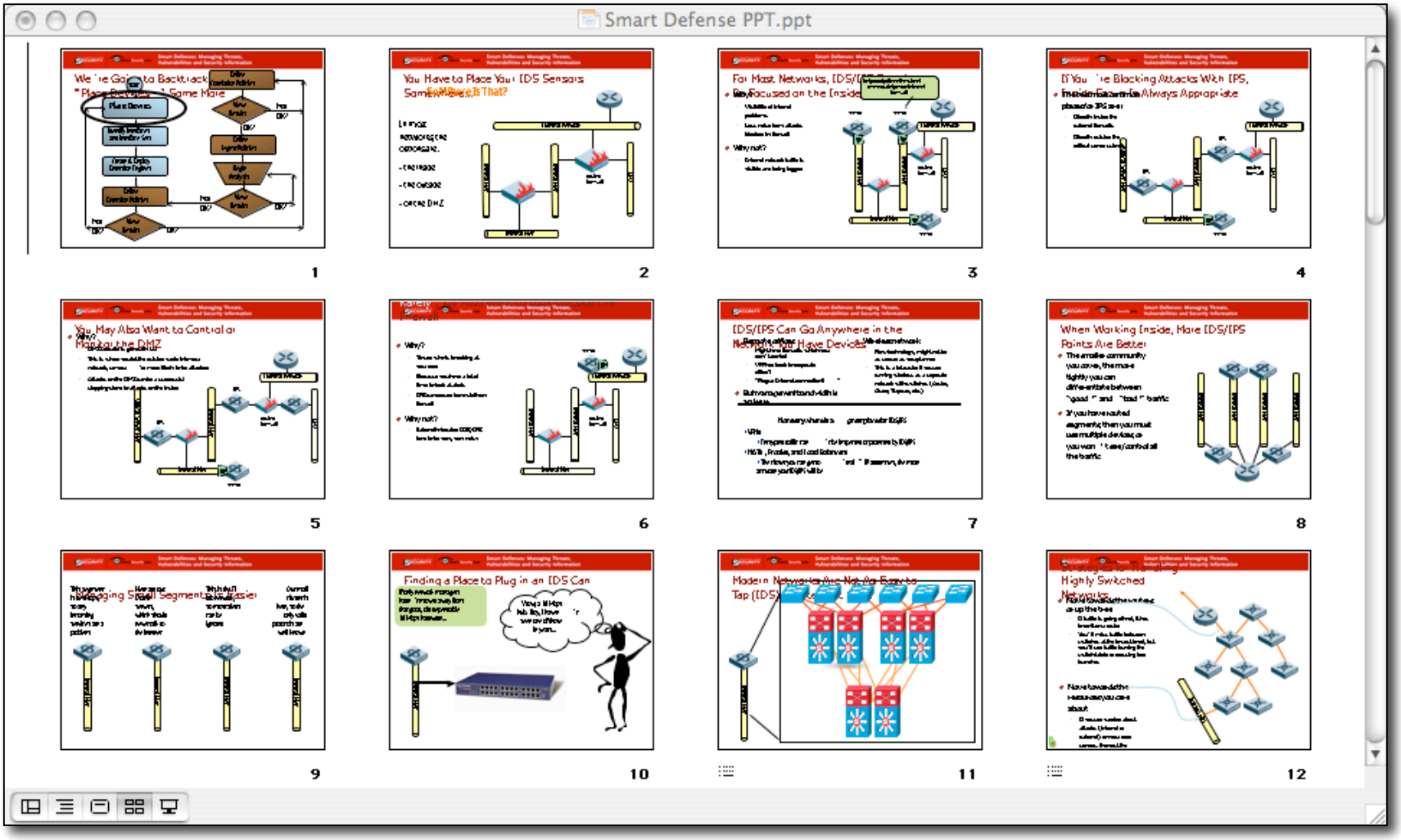
Most Common Errors in IDS Deployment and Operation

1) **Putting Sensors in the Wrong Place**
2) **Not Customizing IDS for Your Environment**
3) **Not Linking IDS to Network, Application, and Security Knowledge**
4) **Not Listening to What the IDS Says**
5) **Mistaking IDS for IPS**

No, really. If you aren't going to use the console *at least* once a week, you probably don't want to put this in place

An IPS drops packets; it's a firewall with a default-allow policy.
An IDS looks for anomalies, policy violations, malicious traffic, and funny packets.

We'll dive deep into IDS later today



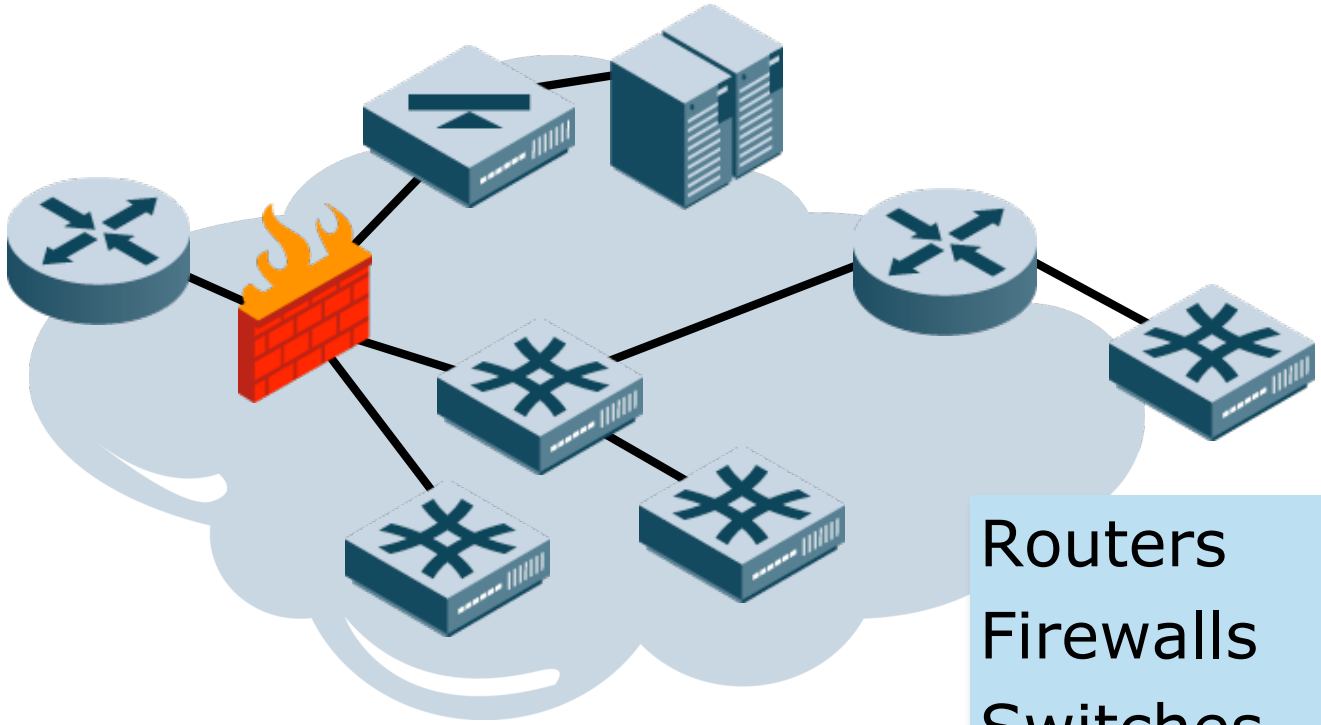
Goal:

Gain better insight into traffic and flows within the network

Strategy:

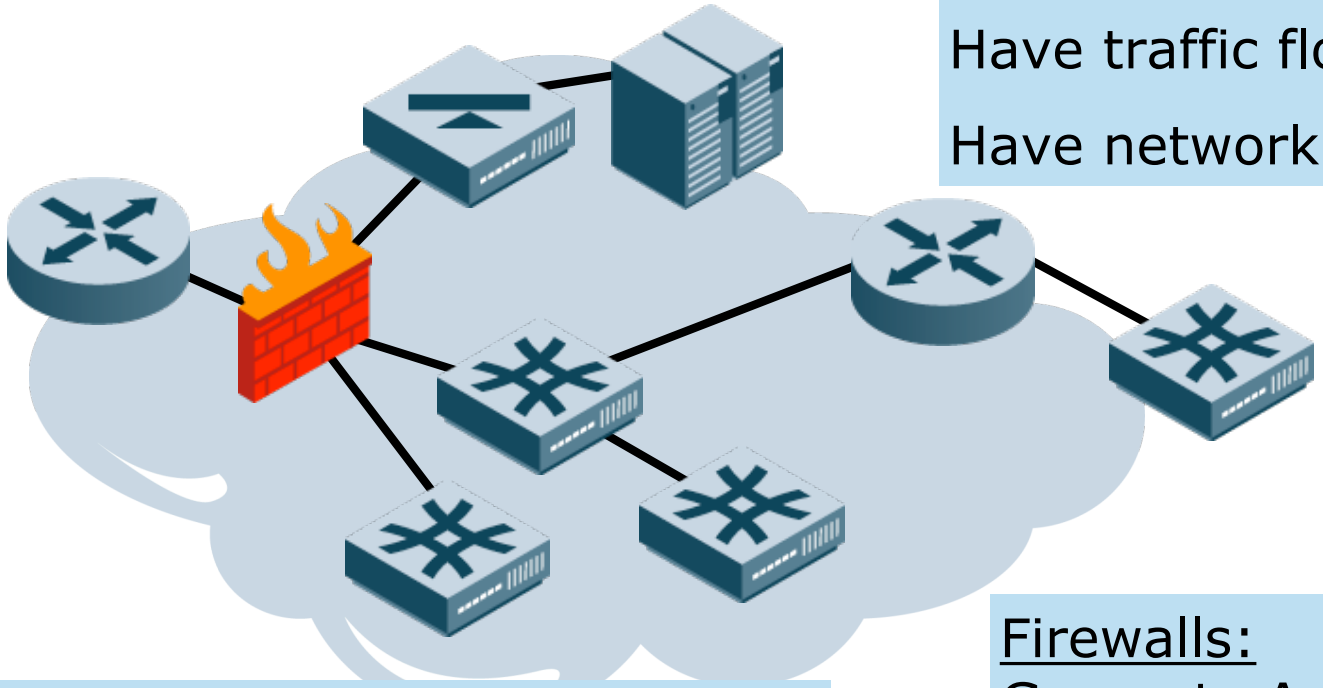
Collect and Analyze security and flow information from existing control points

You already have an abundance of instrumentation… use it!



- Routers
- Firewalls
- Switches
- Load Balancers
- Systems/Servers

Who is Talking and How Much? You already know!



Switches:
Generate Link Up/Down

Have traffic flow data (SNMP)

Have network topology info.

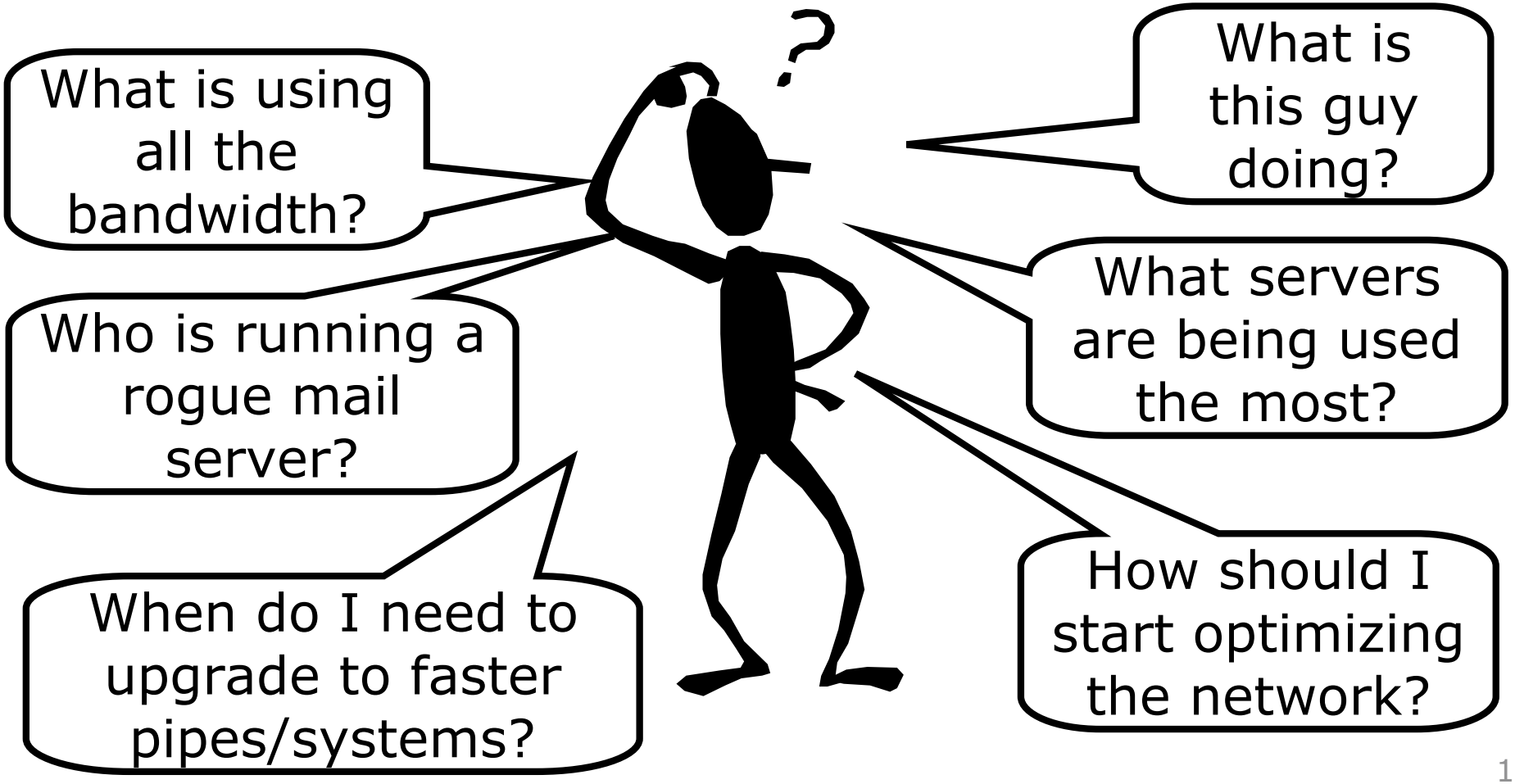
Routers:
Generate flow records (NetFlow, sFlow, etc.)

Generate ACL permit/deny

Firewalls:
Generate Accept and Deny

Generate traffic flow data in session end records

Once you have the data, you can answer important questions



Of course, it's not as easy as turning on logging and flow data

Asking for the data is pretty easy	**Understanding and analyzing the data requires additional tools**
The data will be expressed in "network" terms (such as IP address)	**You probably want different terms (such as username or NETBIOS name)**
Gathering Network Flow data may have other costs	**Cisco platforms are optimized to route packets, not report on them**

Action Items: Network Visibility

- **Investigate SIM products or open source tools to collect and *summarize* flow and session information**
- **Install open source tools or commercial products to monitor traffic counters at the switch port level and generate usage data**
- **Begin archiving session data (hey, disk is cheap) for future long-term analysis projects**

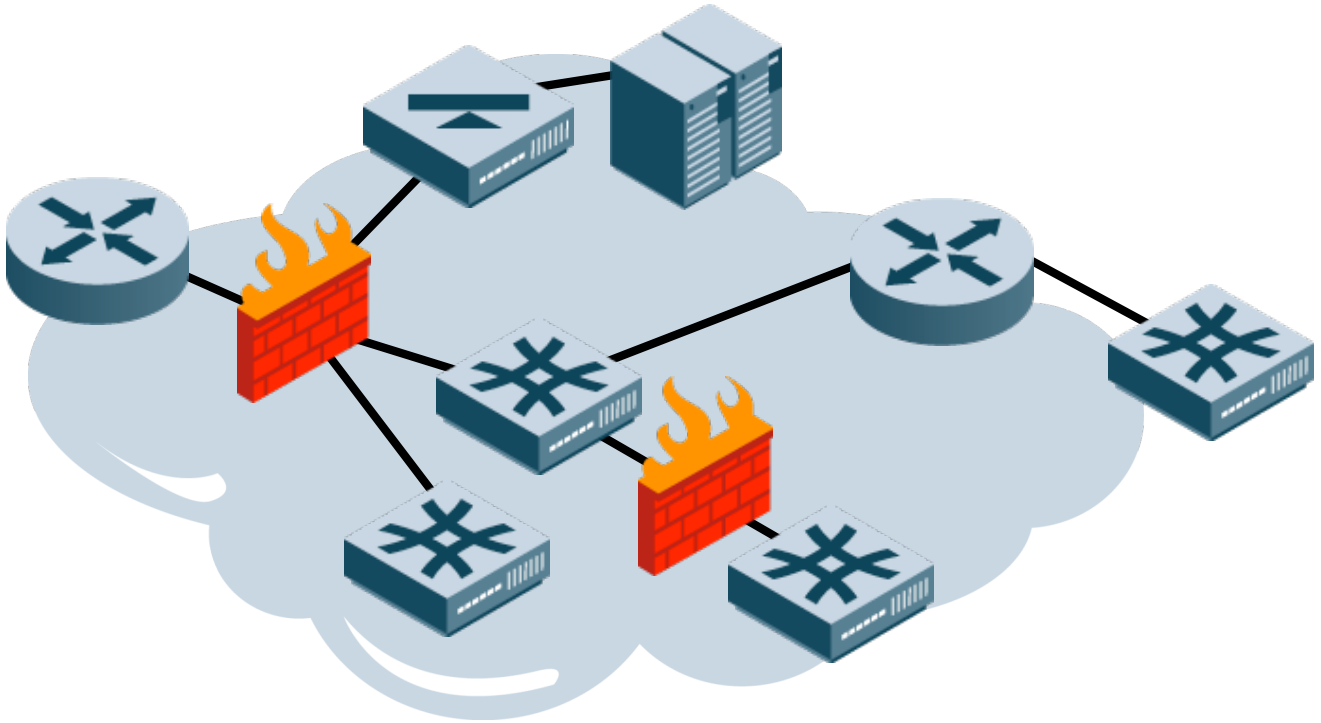
Goal:

Gain greater and more granular control over all traffic

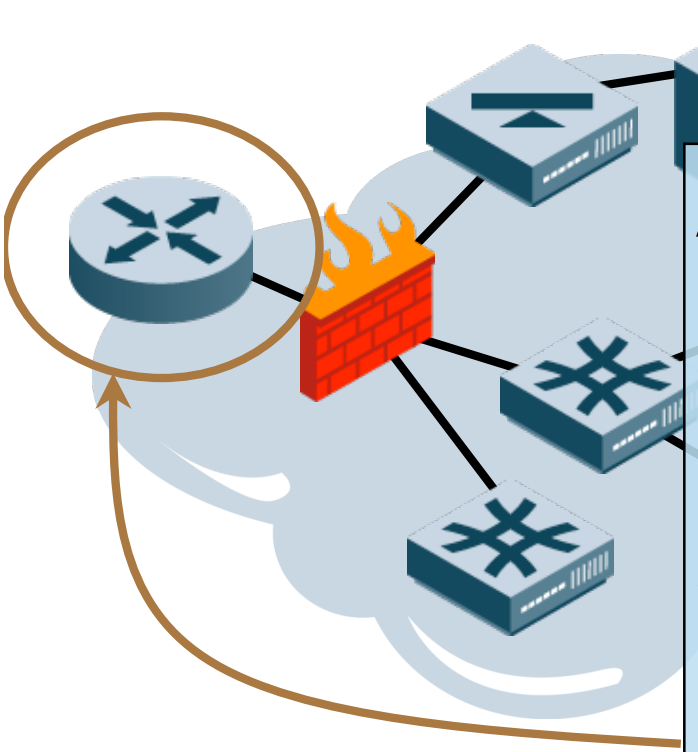
Strategy:

Enable security on devices you already own such as switches, routers, and firewalls

Your network already has lots of security control points… use them!

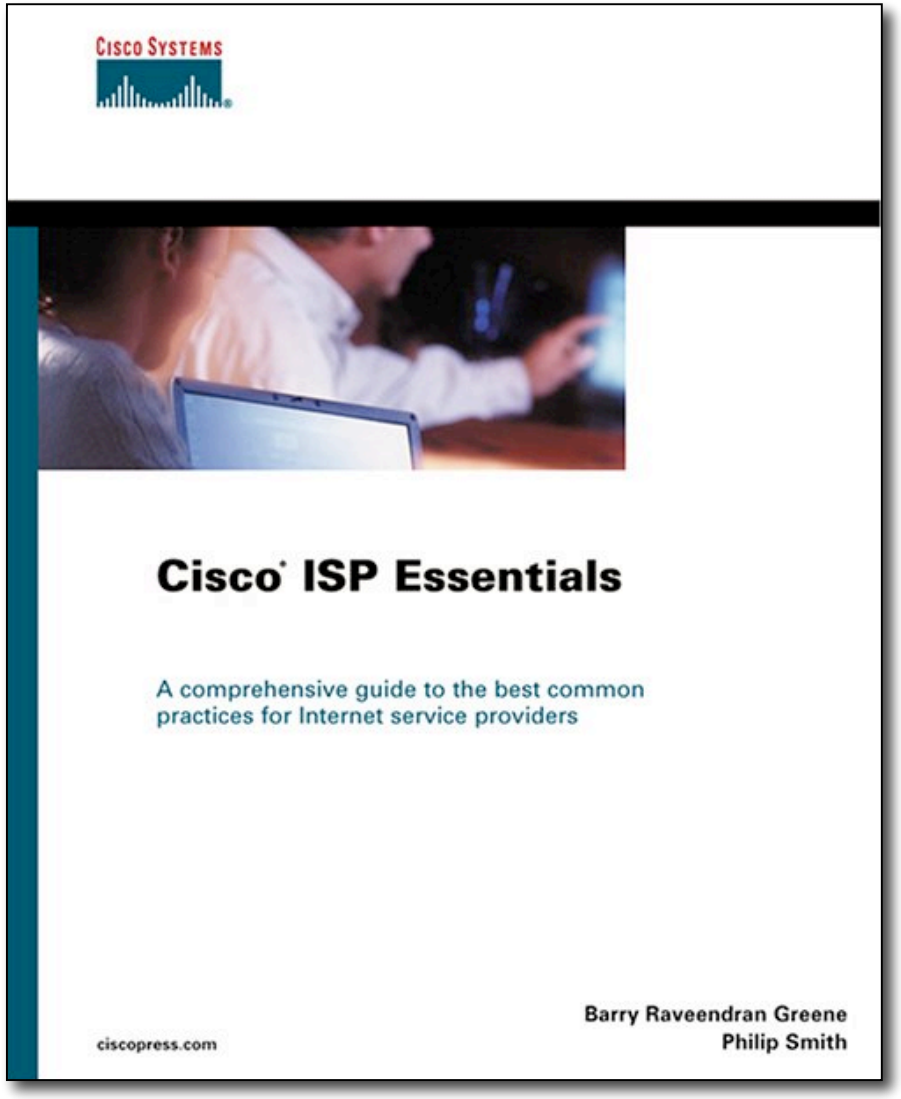


Your external router is a good first cleaner for traffic

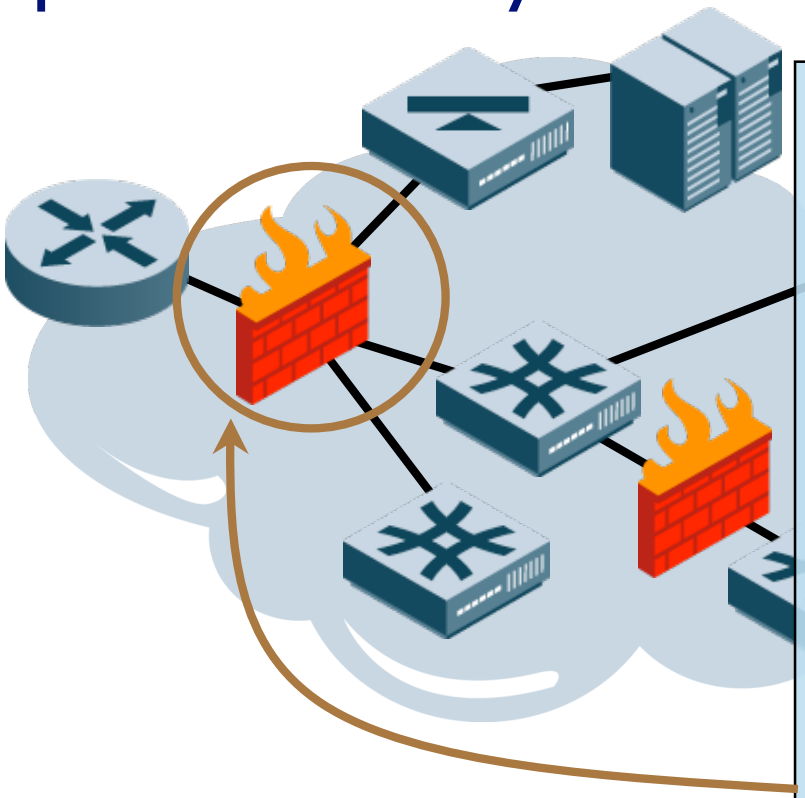


- Anti-spoofing ACL starts here
- Block access to control plane on external network
- Block traffic you don't want to waste logging on (Slammer, etc.)
- Alert on attempted control plane access

Don’t let the title mislead you: this book tells you how to secure your infrastructure Cisco devices!



Are you using all the features you paid for in your external firewall?



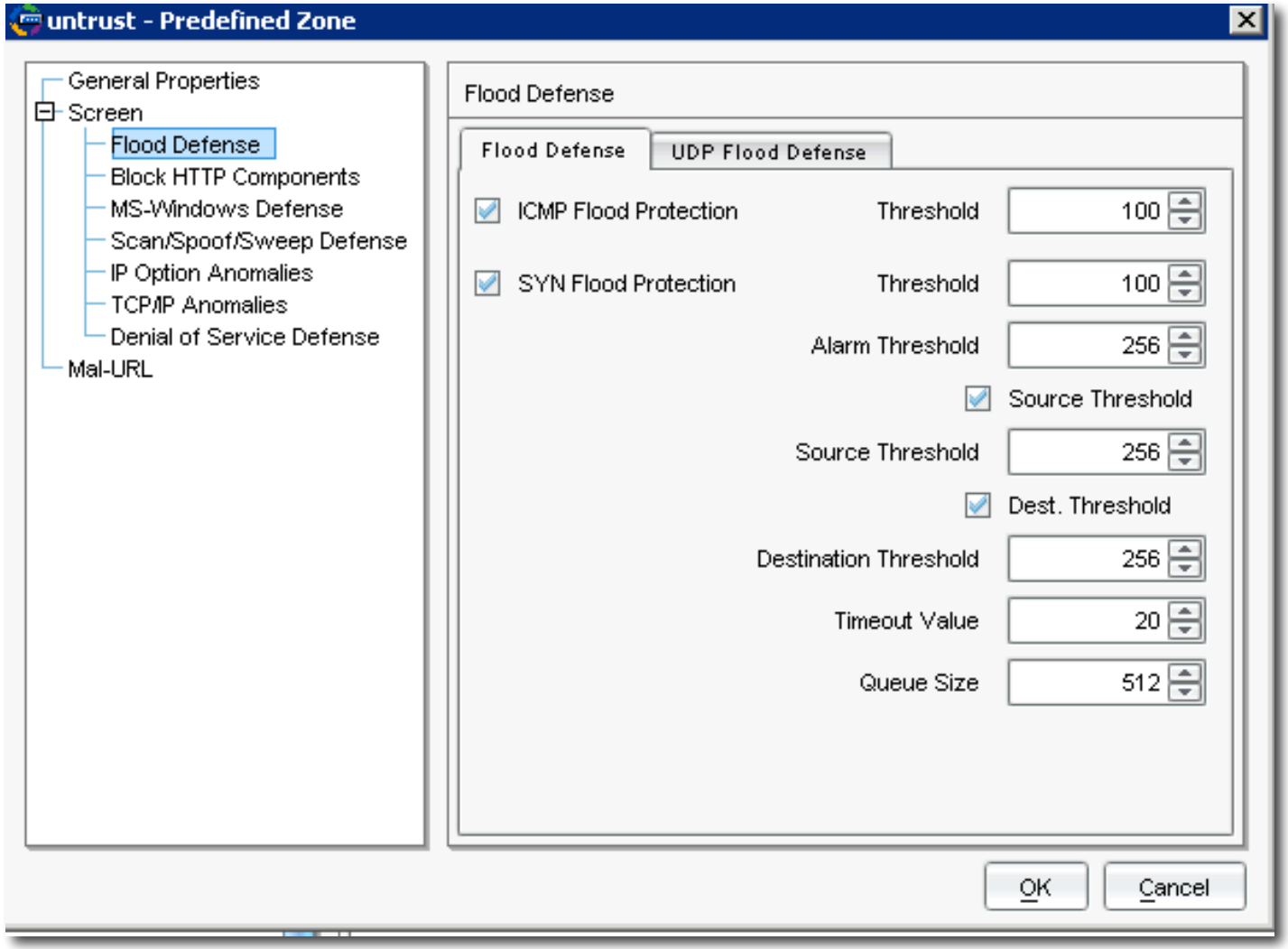
Most firewalls have rate-based DoS/IPS features… turn them on!

Do you have a "default pass all" for outbound traffic? If so, reconsider.

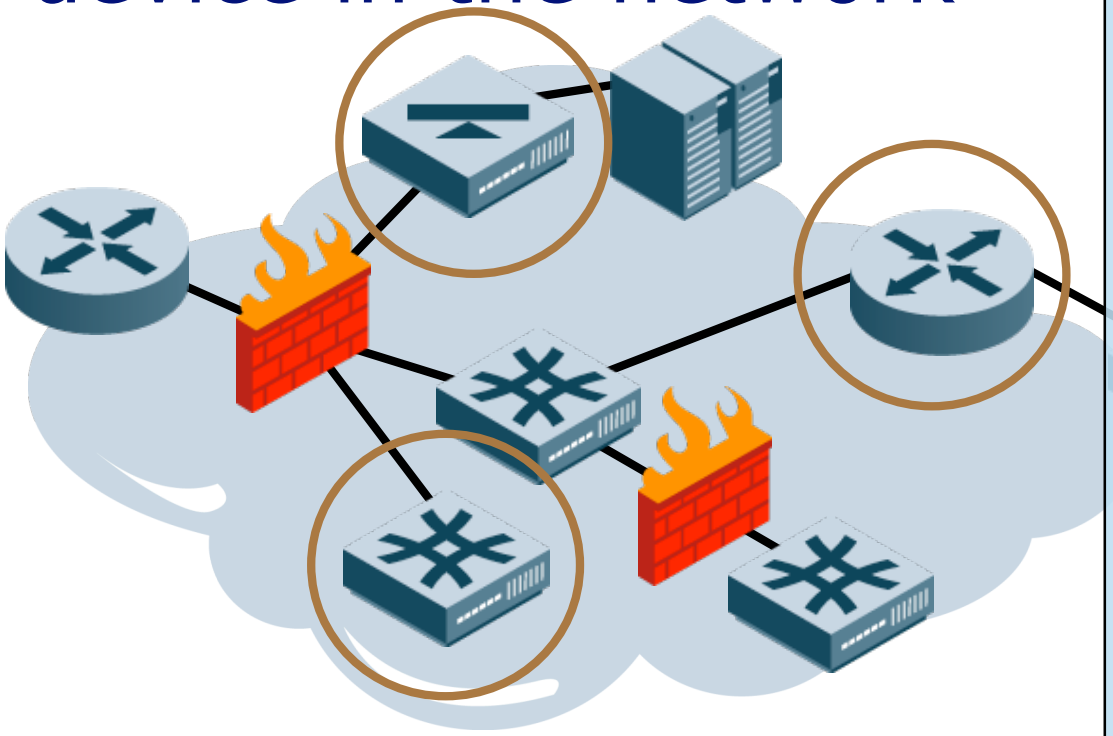
SMTP? Non-Web?

Secure your control plane traffic and disable non-secure management

Now is the time to explore all those little boxes



Control traffic TO and THRU each device in the network



Control plane management: either a separate management network (best) or ACLs (good)

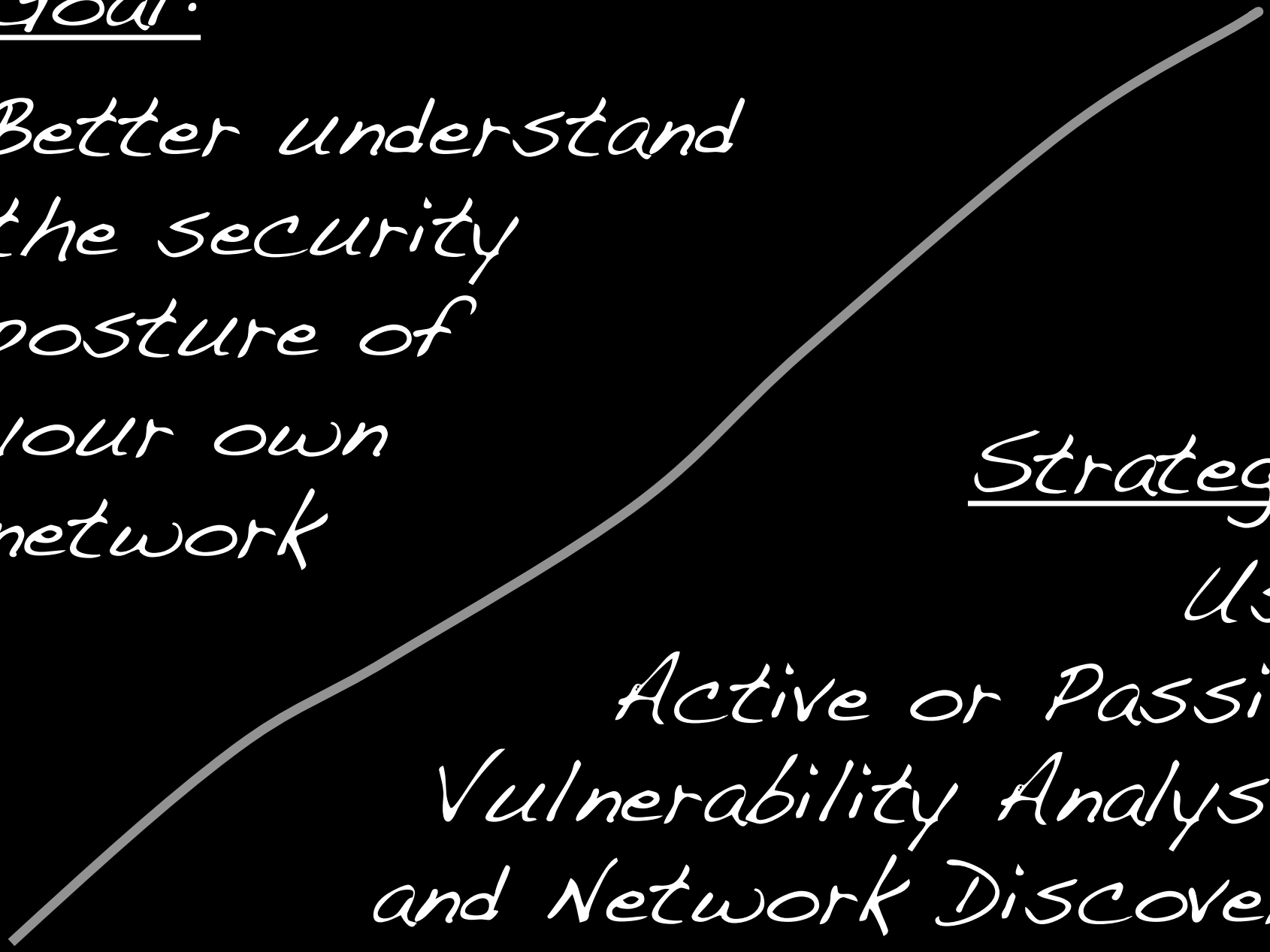
Traffic management: block and alert on common errors and worms; install anti-spoofing ACLs

Action Items: Leverage Existing Points

- **Enable security features on security devices (such as firewalls) that you already have but are not using**
  - **DoS protection most typical**
  - **Limited IPS features common**
- **Put coarse controls at external devices to protect control/management plane, anti-spoofing, and common worms**
- **Secure internal control/management plane traffic using either a separate "access ether" or ACLs; configuration tools**

Goal:

Better understand the security posture of your own network

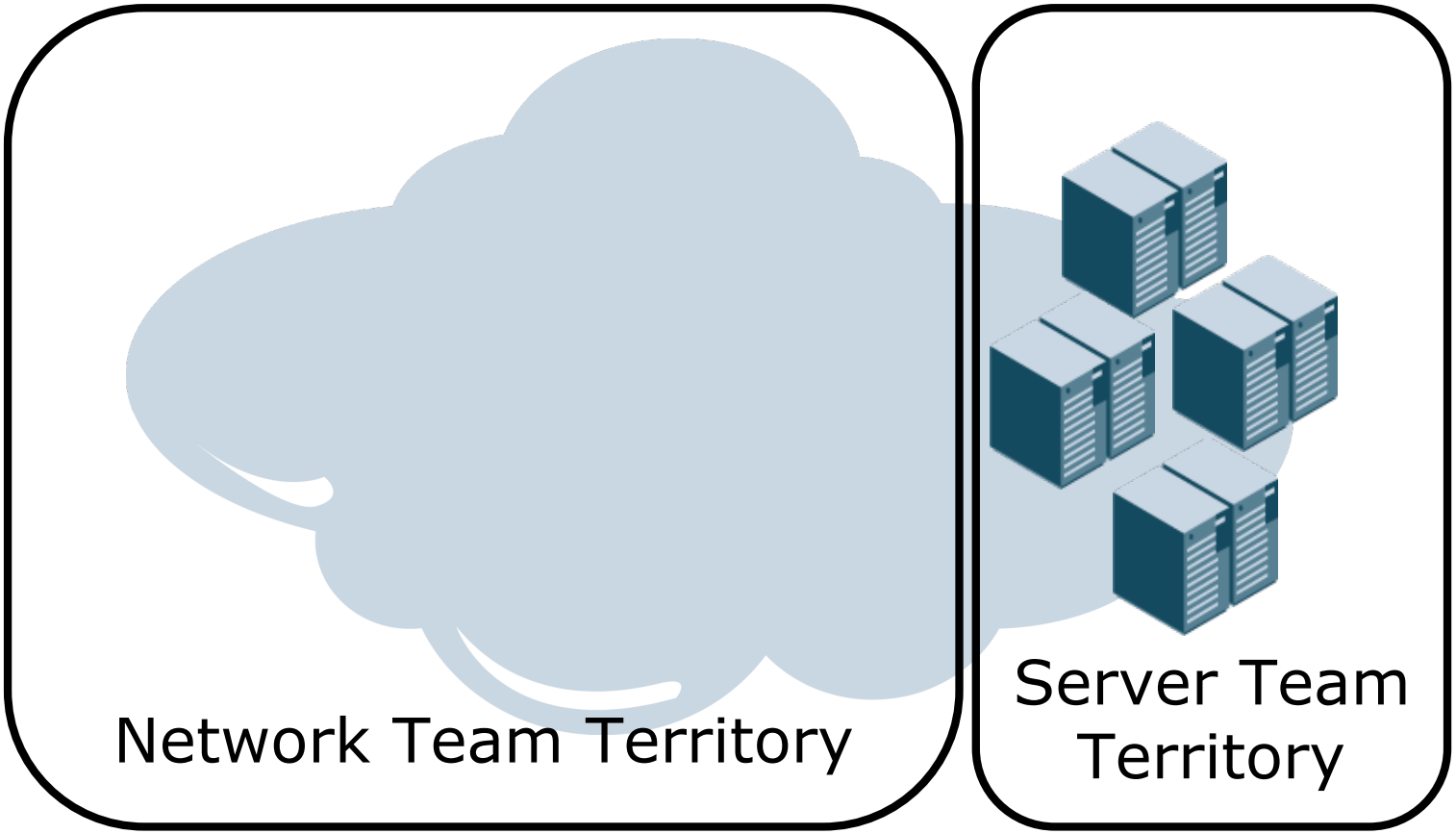


Strategy:

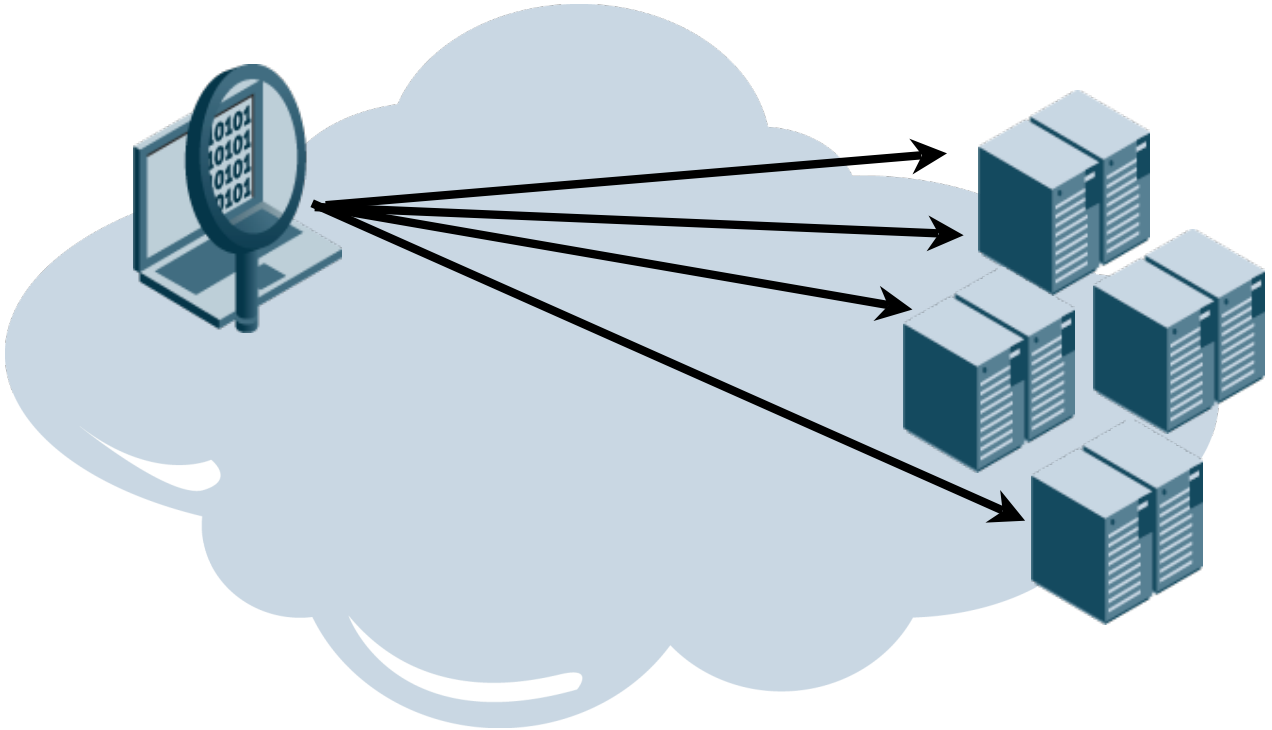
Use Active or Passive Vulnerability Analysis and Network Discovery

Knowing what services are running on the network has great value

The Server Team may think they know what's going on, but getting a second opinion is always useful.



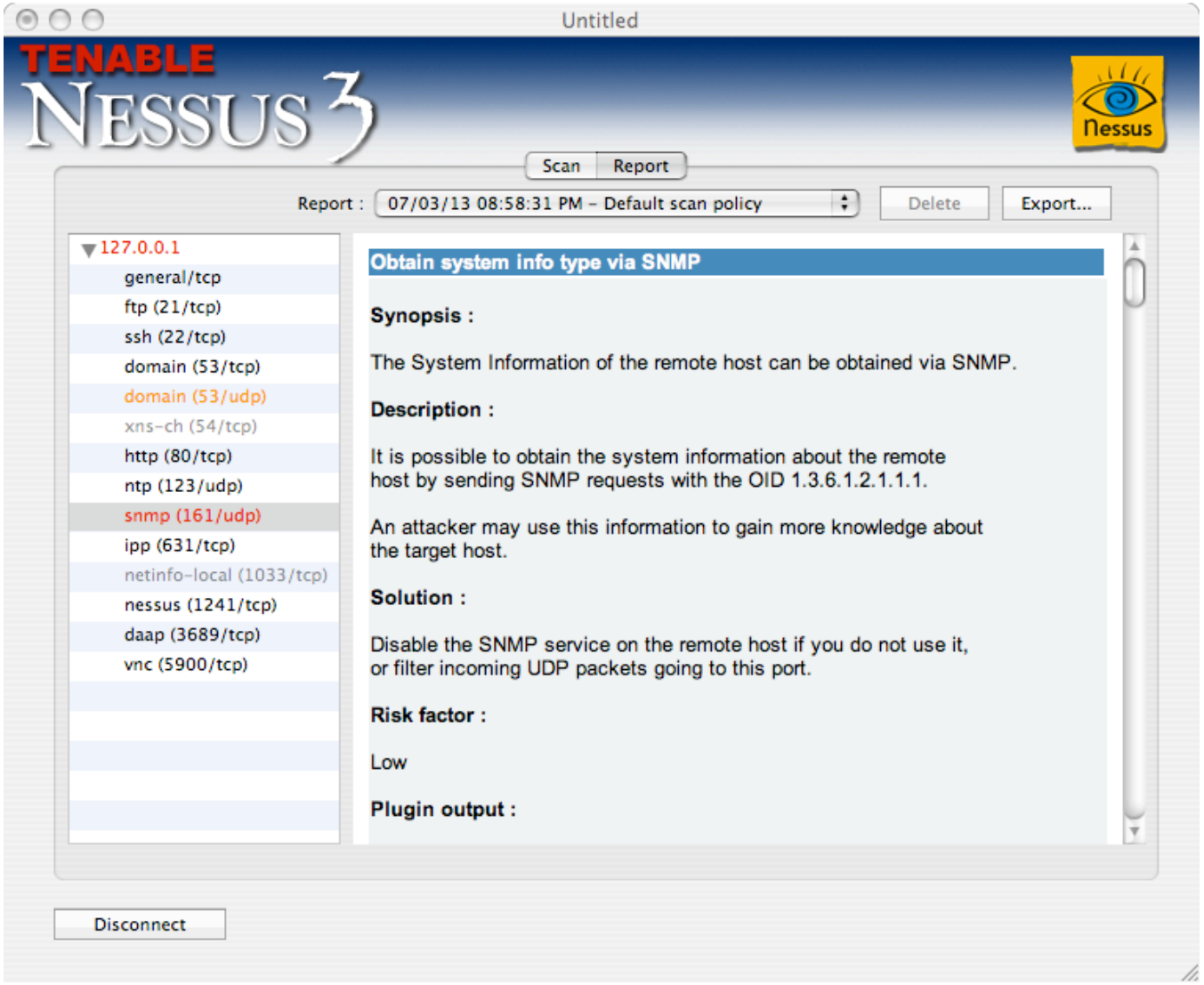
Active Scanning pounds systems looking for apps and vulnerabilities



Active scanning can tell you more than just services

Examples include:

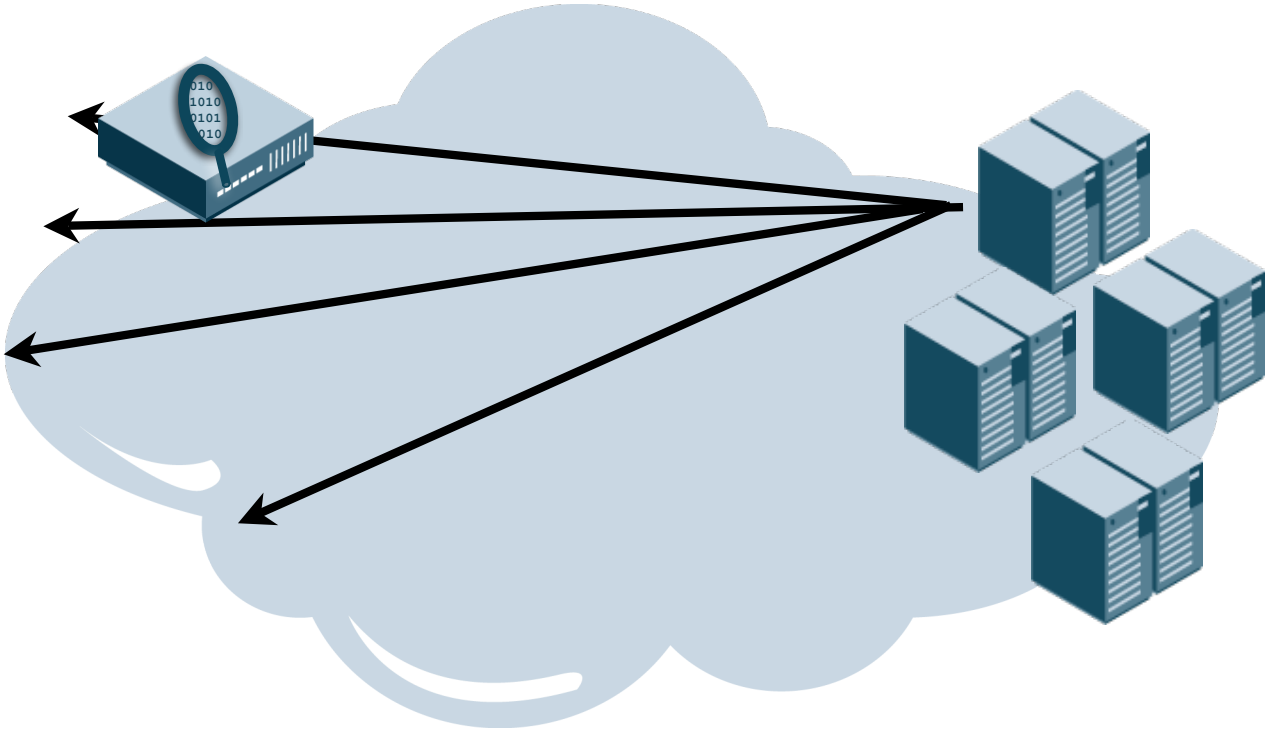
- Nessus
- Retina
- Core Impact
- ISS
- SARA
- Qualys
- Saint
- MS Baseline
- nmap



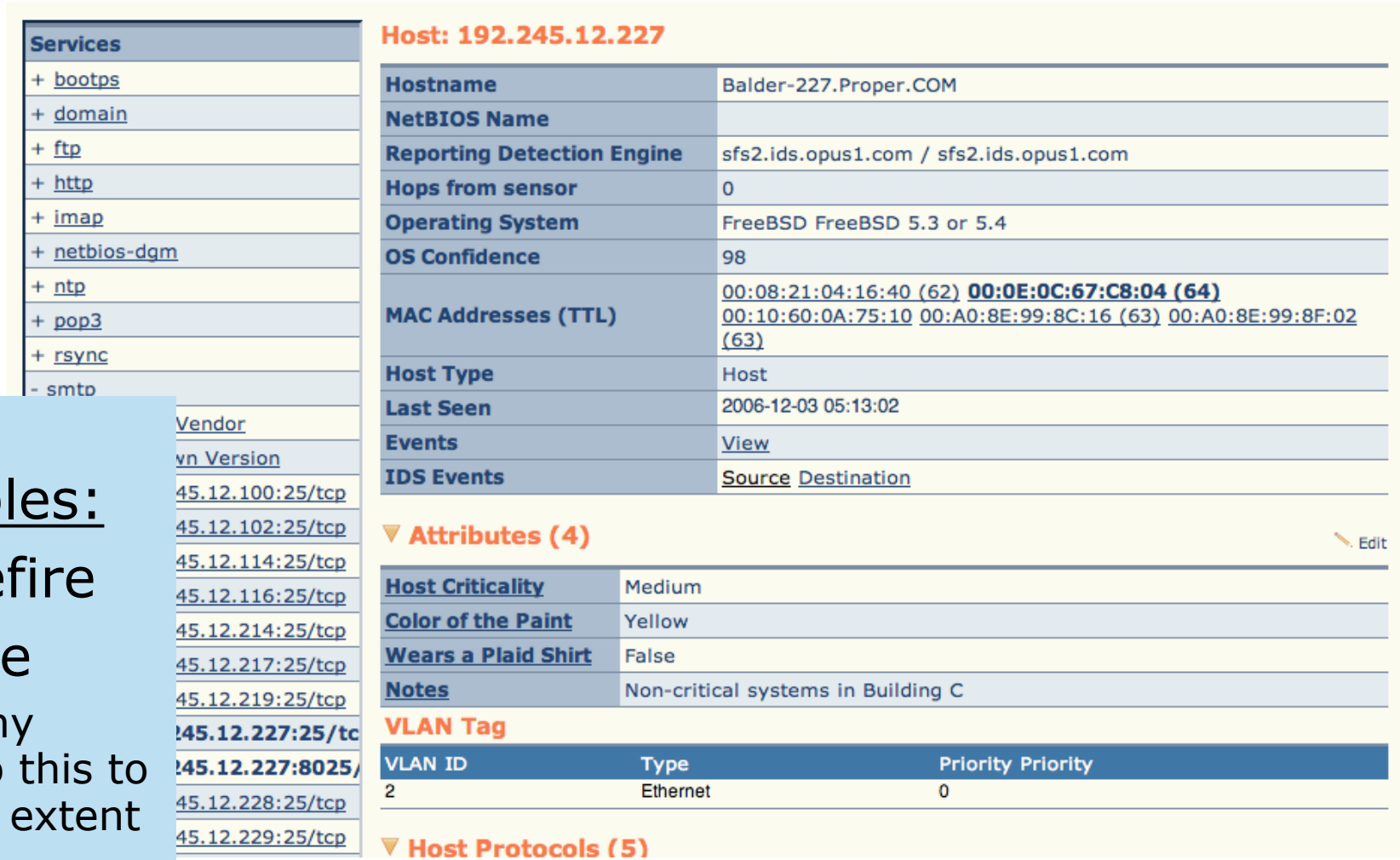
Active Scanning has a huge political cost that may drive you to Passive

- **Active scanning will crash systems and applications**
  - **It's a side-effect of how these things work**
  - **Even the most gentle scan can crash applications**
- **Active scanning is easily detectable and will set off alarms**
- **Sometimes folks don't like being scanned, especially if you work for different bosses**

Passive Scanning watches traffic looking for apps and vulnerabilities



Passive Scanning is more limited, but can give a lot of information still



Services
+ bootps
+ domain
+ ftp
+ http
+ imap
+ netbios-dgm
+ ntp
+ pop3
+ rsync
- smtp

Vendor
vn Version
45.12.100:25/tcp
45.12.102:25/tcp
45.12.114:25/tcp
45.12.116:25/tcp
45.12.214:25/tcp
45.12.217:25/tcp
45.12.219:25/tcp
245.12.227:25/tc
245.12.227:8025/
45.12.228:25/tcp
45.12.229:25/tcp

Host: 192.245.12.227

Hostname	Balder-227.Proper.COM
NetBIOS Name	
Reporting Detection Engine	sfs2.ids.opus1.com / sfs2.ids.opus1.com
Hops from sensor	0
Operating System	FreeBSD FreeBSD 5.3 or 5.4
OS Confidence	98
MAC Addresses (TTL)	00:08:21:04:16:40 (62) **00:0E:0C:67:C8:04 (64)** 00:10:60:0A:75:10 00:A0:8E:99:8C:16 (63) 00:A0:8E:99:8F:02 (63)
Host Type	Host
Last Seen	2006-12-03 05:13:02
Events	View
IDS Events	Source Destination

Attributes (4) Edit

Host Criticality	Medium
Color of the Paint	Yellow
Wears a Plaid Shirt	False
Notes	Non-critical systems in Building C

VLAN Tag

VLAN ID	Type	Priority Priority
2	Ethernet	0

Host Protocols (5)

Top Examples:

Sourcefire

Tenable

(But many IDSes do this to a limited extent anyway)

Action Items: Network Scanning

- **Add regular nmap-style (service and O/S scan) services to your network**
- **Research tradeoffs between active and passive scanners to see which might be right for you**
- **Work with desktop/server team to determine areas where information sharing about services can help you both**

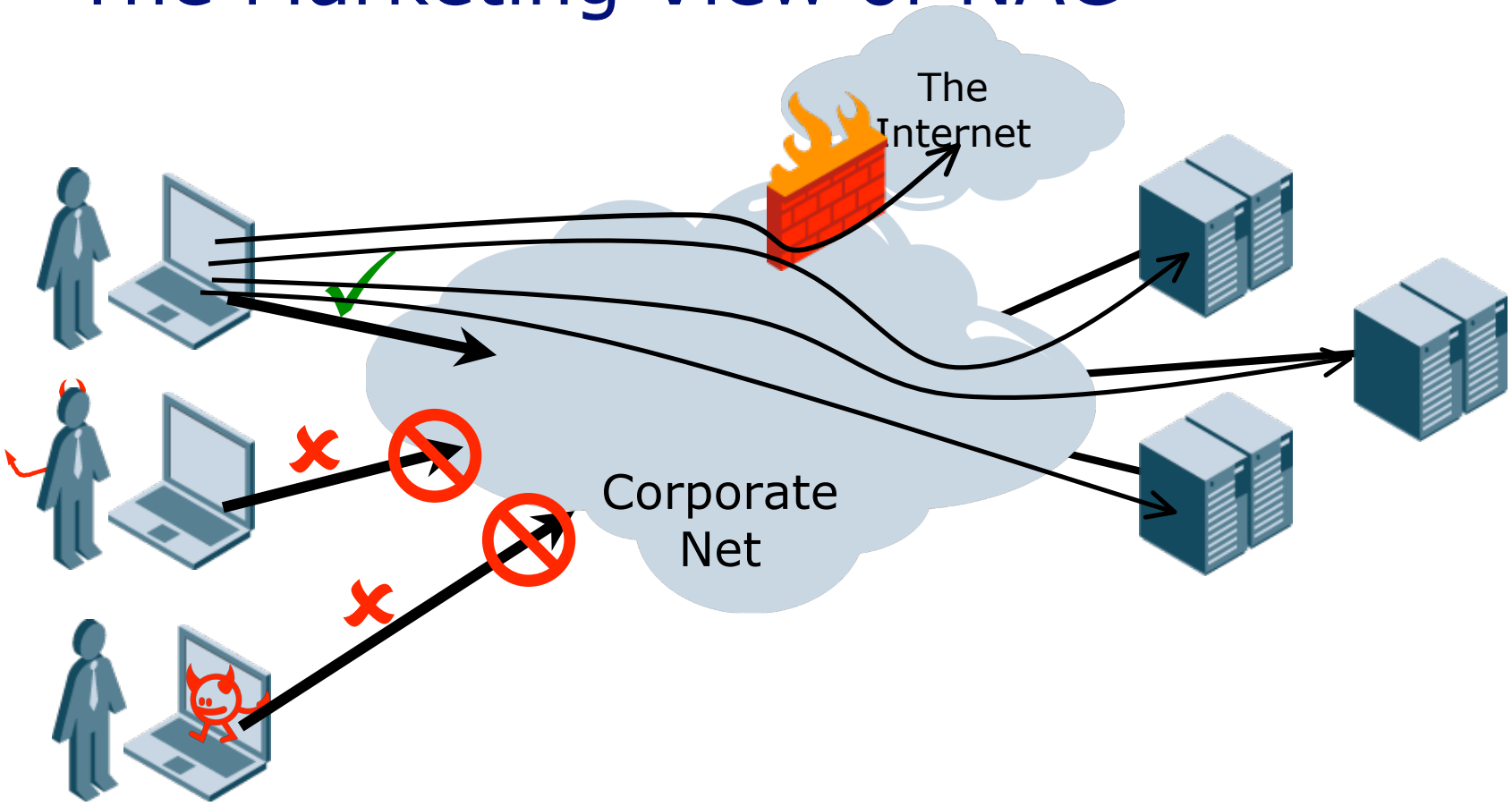
Goal:

Ensure only Authorized and "Safe" Users Connect to the Network

Strategy:

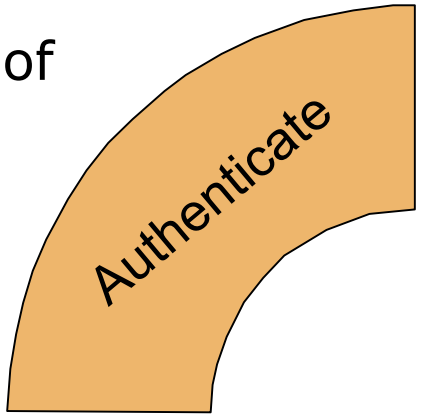
Use Network Access Control (NAC) to Authenticate, Validate, and Control all network usage

The Marketing View of NAC



NAC Has Four Components

1. Authentication of the user

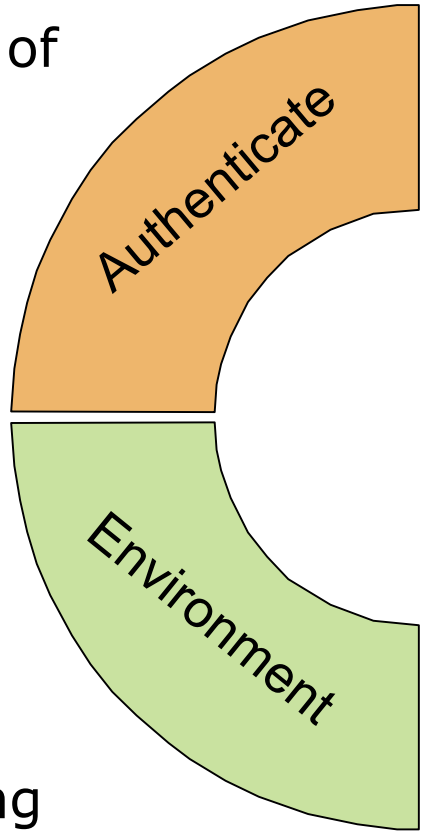


End users are authenticated before getting network access

Environmental Information Modifies Access or Causes Remediation

1. Authentication of the user

2. Use environmental information as part of policy decision making



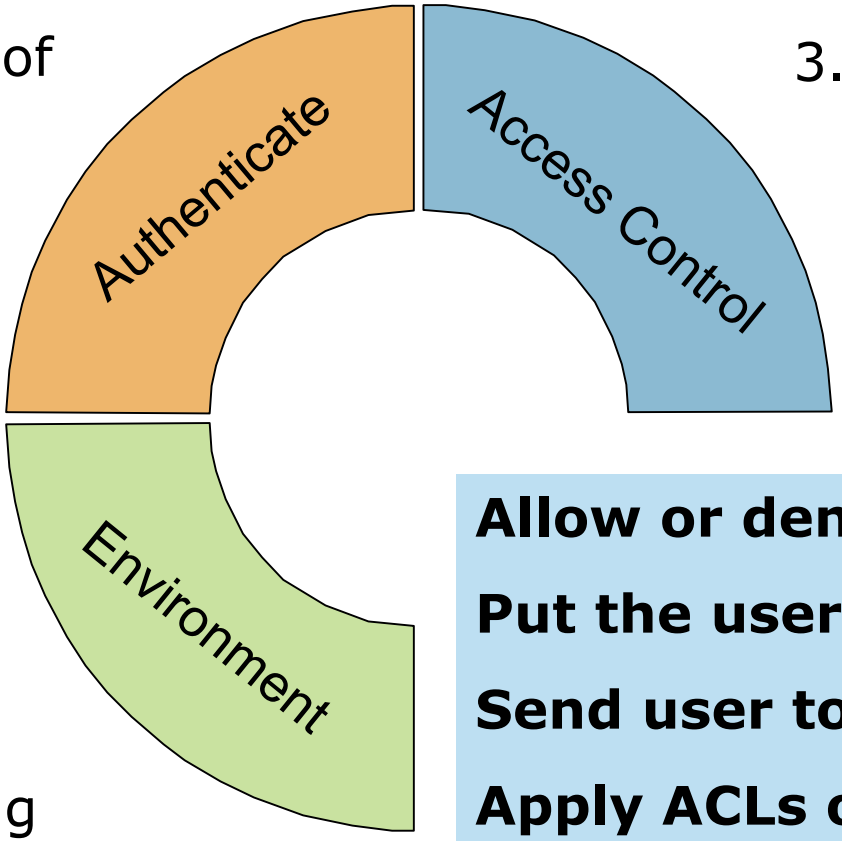
Where is the user coming from ?

When is the access request occurring?

What is the End Point Security posture of the end point?

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 as part of policy decision making

Allow or deny access.

Put the user on a VLAN.

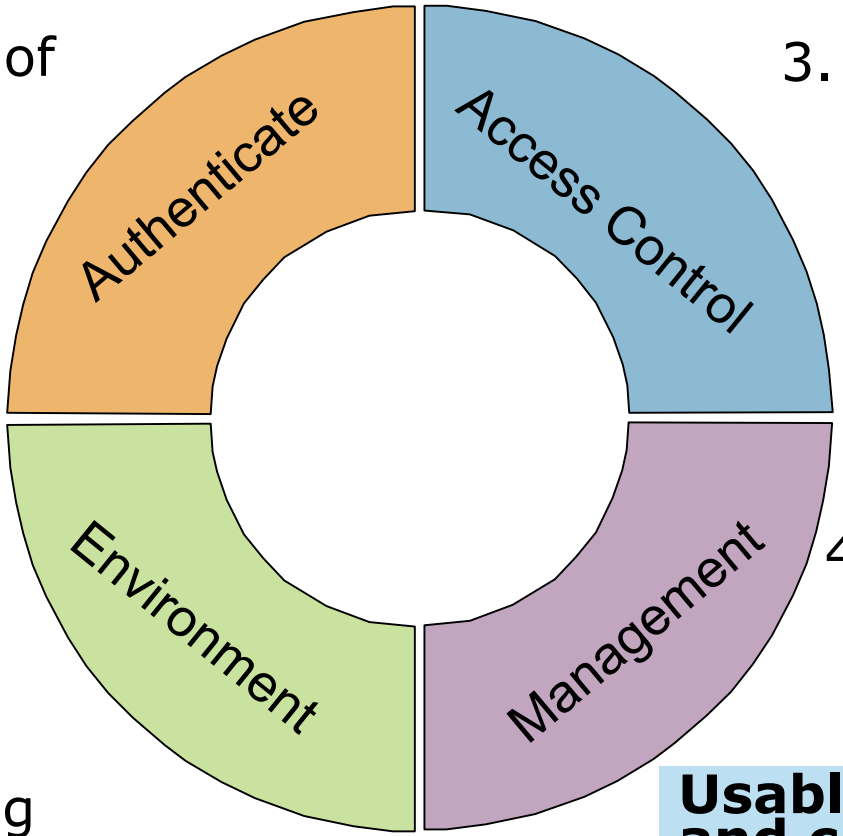
Send user to remediation.

Apply ACLs or firewall rules.

Management of Policy is the Weak Link in most NAC Solutions

1. Authentication of the user

2. Use environmental information as part of policy decision making



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

4. Manage it all

Usable management and cross-platform NAC normalization

Action Items: Network Access Control

- **Roll out authentication using 802.1X (you can call it WPA2) on wireless networks**
- **Meet with desktop team to discuss end-point security assessment and remediation strategies and how they would fit in NAC**
- **Inventory network assets (embedded devices and network devices) to determine how NAC would affect the network**

Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com

OPUS one