



**You Can't Control People.  
Control What's On Your Network.**

## **Solving the Enterprise Information Security Problem – Common Approaches**

**Kurtis E. Minder – Mirage Networks**

# Topics

---

- Introduction – Who, What, etc.
- Ubiquitous Technologies
- Developing Technologies
- The Gap
- Network Access Control Present and Future
- Q&A



**You Can't Control People.**  
**Control What's On Your Network.**



## **Ubiquitous Technologies**

What are they? Why do they exist?

# Business Needs Drive Security Adoption

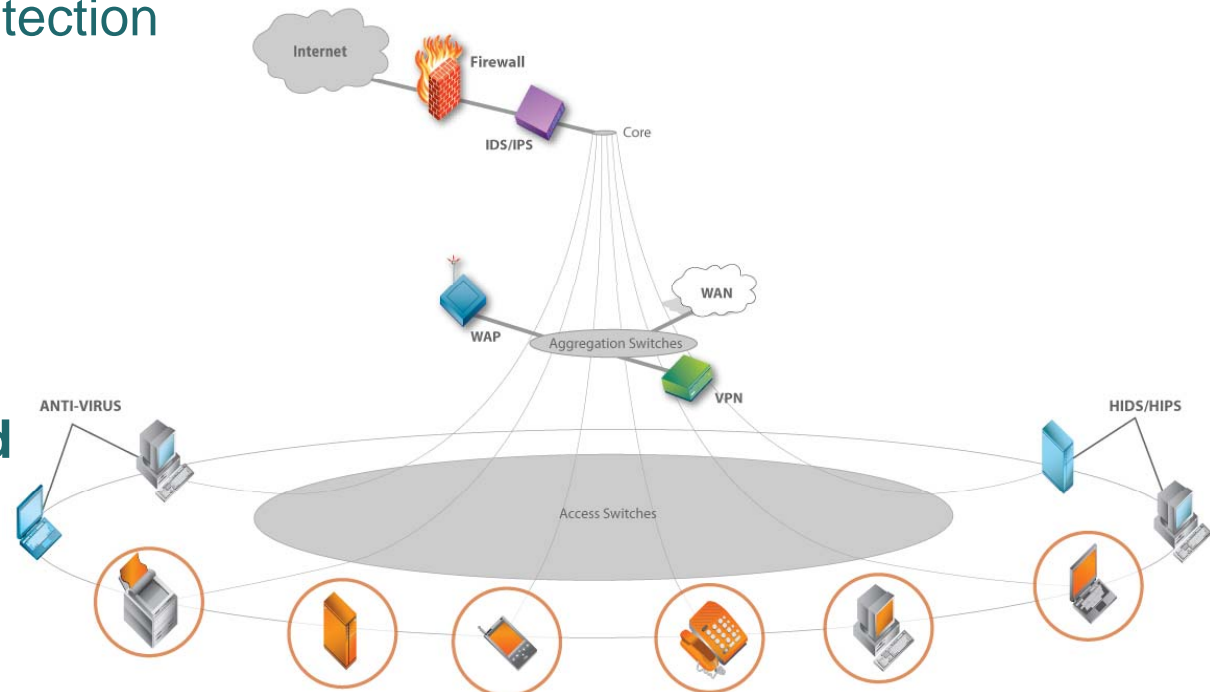
## 4 Ubiquitous Security technologies

- Anti-virus - Business driver: File sharing
- Firewalls - Business driver: Interconnecting networks (i.e. Internet)
- VPNs - Business driver: Remote connectivity
- IDS – Threat Detection

Each product fills a need in the security space

Challenges exist around security versus productivity

Typically products are not collaborative



## Anti-Virus

Anti-Virus provides software / desktop level risk management for workstations in the enterprise.

- Uses malicious code signature database to determine whether workstation was being attacked/compromised.
- Enterprise solutions evolved to provide central management and enhanced capability for workstation control. (McAfee Enterprise Policy Orchestrator.)
- As larger AV vendors acquire new technologies, feature set improves (DLP, Encryption, Config Management)



# Firewalls

The Firewall was adopted to protect corporate networks from would-be Internet attackers.

- Firewalls, deployed in-line, typically use a set of network layer rules to determine what traffic can enter/leave the network.
- Improvements to Firewall technology have been largely limited to performance. As bandwidth increased, Firewalls had to process faster. (Some FW companies have increased app visibility)
- New technologies are increasing FW capability to inspect traffic faster and more intelligently



# VPN

VPN (Virtual Private Networking) was adopted to provide secure remote access to corporate networks.

- Provides remote access via IPSEC or SSL to the corporate network
- Enhanced features can include workstation integrity checks and role based access control
- Also is often used to provide connectivity between networks for business to business transactions.



# Intrusion Detection / Prevention

IDS was developed to detect attacks on the network and alert the security administrator

- IPS, typically inline, added the capability to stop the attack automatically or manually
- IDS/IPS originally relied entirely on signatures, but evolved to include clever behavioral, heuristic-based algorithms to detect threats







**You Can't Control People.  
Control What's On Your Network.**



## **Developing Technologies**

What drives them?

# Data Loss Prevention

Data Loss Prevention (DLP) technology was developed as a direct result of lost corporate information from inside the network.

- DLP Technology uses a multi-faceted approach to solving the Data Leak problem, including network based sensors, workstation software, and complex policy management
- The technology is largely developed to keep corporate intellectual property and finance data from being distributed.
- Also used to maintain compliance initiatives around SOX, HIPAA; showing due diligence toward securing patient / customer data



# Disk Encryption

Disk encryption technologies were developed to protect data on stolen or compromised devices.

- Lost personal customer data and mandatory disclosure has driven the disk encryption market.
- The Payment Card Industry (PCI) has developed a set of standards for doing business with the credit card companies. These standards often dictate encryption when storing credit information.
- Hard drive manufacturers are now developing self encrypting drives in addition to the industry software-based approach



# Configuration Management

Configuration management was developed to maintain control over workstation software and patch deployment.

- Config management has evolved to include technologies like patch management, remote control, help desk portal integration, and software deployment
- Several different approaches to config management have evolved, including an appliance-based approach as well as agent/software approaches
- Many config management vendors offer hardware tracking and asset management as well



# Vulnerability Assessment / Management

Vulnerability assessment and vulnerability management have developed as automated tools to track and validate configuration / patch management as well as provide security posture assessment for the enterprise.

- There are several approaches to VM. Two primary approaches are network based and software based.
- Many of the larger vendors are offering a range of assessment and vulnerability tools for managing security posture. (Mostly through acquisition)



# Security Event / Information Management

Security event management (SEIM) grew from the need for intelligent and robust logging facilities for security tools.

- Typically an appliance based approach. Hardware is critical to reporting performance.
- Driven by powerful database engines, the SEIM correlation allows IT Security staff to review events across multiple products to determine a source





**You Can't Control People.**  
**Control What's On Your Network.**



**The Gap**

# How many security products does it take?

The logo for NetworkWorld, with "NETWORK" in blue and "WORLD" in black, underlined with a red line.

Attacks on peer-to-peer networks increased 357% in July 2007 over July 2006, with 32 attacks.

The logo for eWeek.com, with "e" in yellow and "WEEK.COM" in blue.

P2P Applications can turn any computer into an always-on bandwidth glutton because they run unattended, without any user intervention.



Music theft at 58 campuses targeted in latest wave of deterrence program



# Rogue Devices



Wireless access points and personal routers can cause mayhem on campus networks



Gaming consoles run operating systems just like every other computer - they are susceptible to malware.



Mobile Internet Devices (MIDs) will soon be monopolizing airtime on the access points.

## Instant Messaging Facts

The logo for NetworkWorld, with "NETWORK" in blue and "WORLD" in black, both in a bold, sans-serif font, with a red underline.

The total number of IM threats for 2007 so far is 226... that number is a 78% increase over the last year.

The logo for eWeek.com, with "e" in yellow and "WEEK" in blue, both in a bold, sans-serif font, followed by ".COM" in a smaller, blue, sans-serif font.

Security researchers have traced the W32/Sdbot-ADD worm attack against AOL's Instant Messenger network to a rootkit-powered botnet controlled by hackers in the Middle East.

# The Numbers Tell the Story

## “Protection” is in place...

- 98% use firewalls<sup>1</sup>
- 97% of companies protect machines with antivirus software<sup>1</sup>
- 79% use anti-spyware<sup>1</sup>
- 61% use email monitoring software<sup>1</sup>

## But it's not enough...

- Cost of malware: \$14.2B<sup>2</sup>
- 80% of companies experienced 1 or more **successful** attacks, 30% had more than 10<sup>3</sup>
- Worldwide, 32% of companies experience attacks involving business partners
  - 43% of those were infections, while 27% were unauthorized access<sup>4</sup>
- 75% of enterprises will be infected with malware that evaded traditional defenses<sup>5</sup>

<sup>1</sup> Computer Security Institute/FBI's 2006 Computer Crime and Security Survey

<sup>2</sup> Computer Economics, 2006

<sup>3</sup> ICISA Labs, 9<sup>th</sup> Annual Computer Virus Prevalence Survey

<sup>4</sup> Cybertrust, *Risky Business*, September 2006

<sup>5</sup> Gartner, *Gartner's Top Predictions for IT Organizations and Users, 2007 & Beyond*, December 2006 19

# Eliminate the “Low Hanging Fruit”

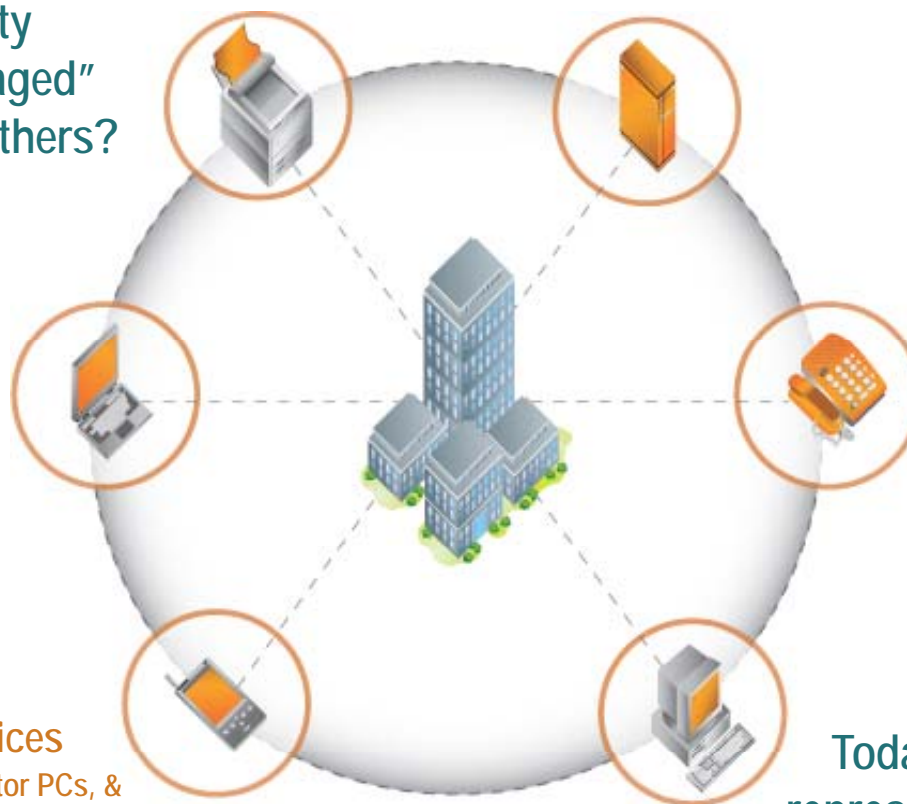
The majority of security solutions focus on “managed” devices. What about the others?

**Infected Devices**  
propagate threats, resulting in loss of productivity & hours of cleanup

**Unknown Devices**  
like home PCs, contractor PCs, & WiFi phones can introduce new threats or compromise data security

**Out-of-Policy Devices**  
are more vulnerable to malware attacks, while running services that could jeopardize security

Today, endpoint devices represent the greatest risk to network security — by propagating threats or being vulnerable to them.



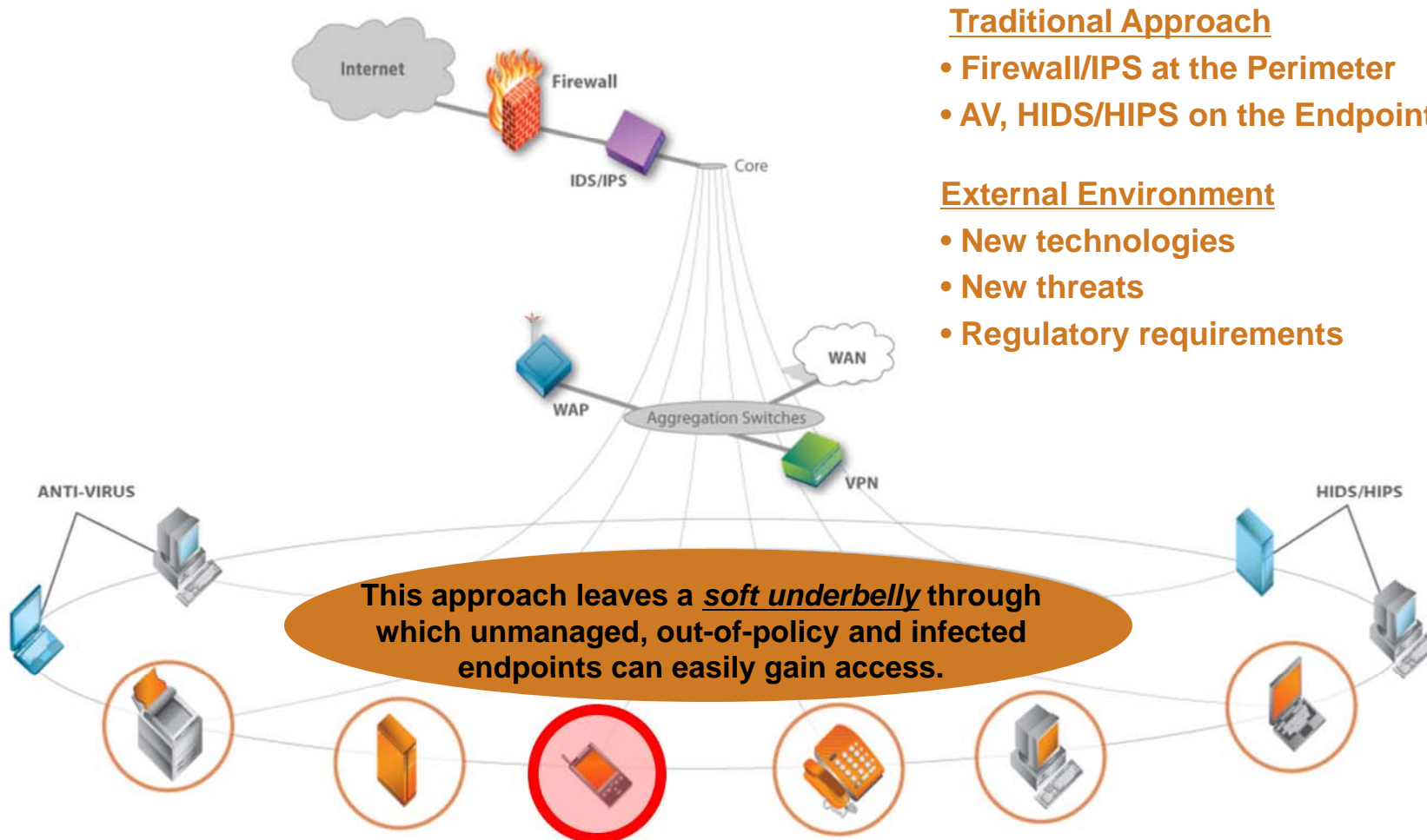


**You Can't Control People.**  
**Control What's On Your Network.**

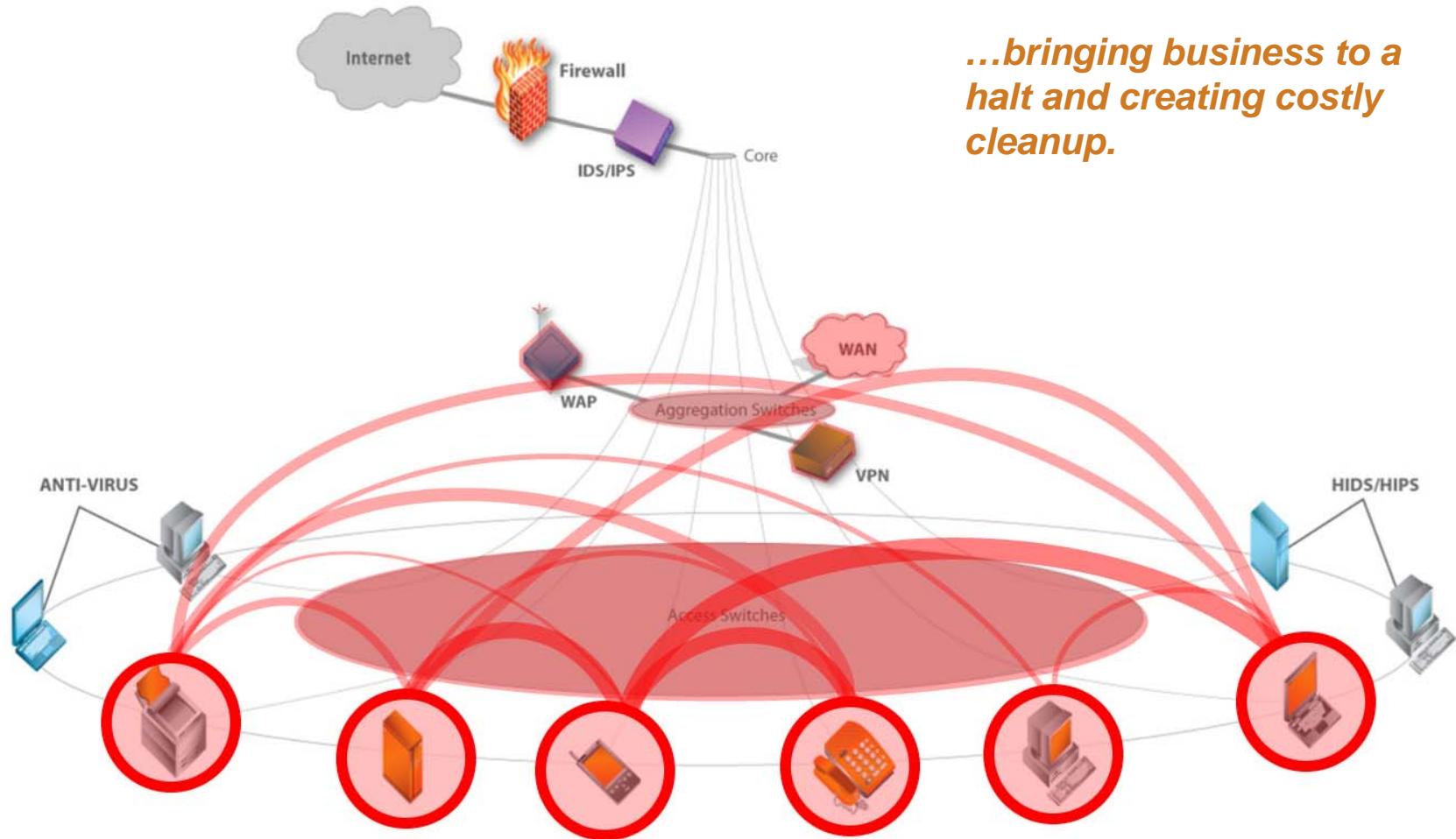


**Network Access Control**

# Traditional Approach to Network Security



# Exploiting the Network's Weakness



*...bringing business to a halt and creating costly cleanup.*

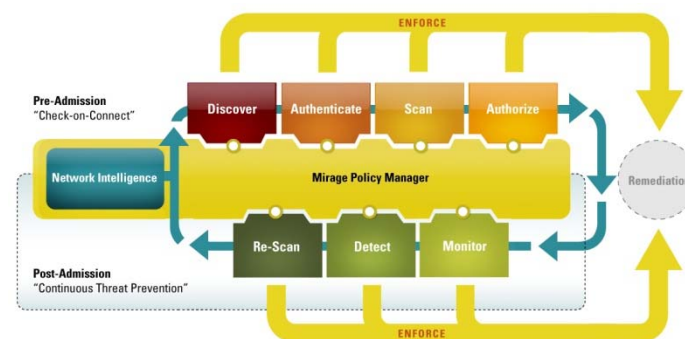
# Phases of NAC

## ● Pre-Admission

- Authentication
  - User / Role Authentication
  - Device Authentication
- Posture Assessment / Risk Assessment
  - Network-Based
  - Endpoint-Based

## ● Post-Admission

- Network Intelligence
- Traffic Analysis
- Quarantine



Full Cycle Network Access Control



# Technology Options

---

## ● Common approaches

- Leverage 802.1x or network infrastructure OS
  - Authenticate through existing EAP infrastructure to pass credentials to authentication server
- Special purpose DHCP server
  - Authentication usually web based and tied to authentication server
- Authentication proxy
  - NAC solution serves as a proxy between device and authentication server
- Inline security appliances (i.e. security switches)
  - Serve as a proxy between device and authentication server
- Real time network awareness
  - Authentication usually web based and tied to authentication server

# NAC Options

Agentless	On-demand Agent	Agent-based
Easy to deploy	Minimal deployment overhead	Deployment overhead
Protection for unmanaged environments	Protection for unmanaged environments	Covers endpoints with agent installed
Full endpoint coverage	Covers supported endpoints	Covers devices with agent installed
Weaker assessment for endpoint compliance policies	Reasonable assessment for endpoint compliance status	More robust assessment for endpoint compliance policies
No off-network endpoint monitoring	No off-network endpoint monitoring	Off network endpoint monitoring

# NAC Options

Out-of-band	In-line
Easy to deploy	Intrusive to deploy
No latency	Introduces another 'bump' on the wire
No point of failure	Introduces point of failure
Flexibility that protects investment	Limited options for investment
May not see every packet	Can have unlimited visibility

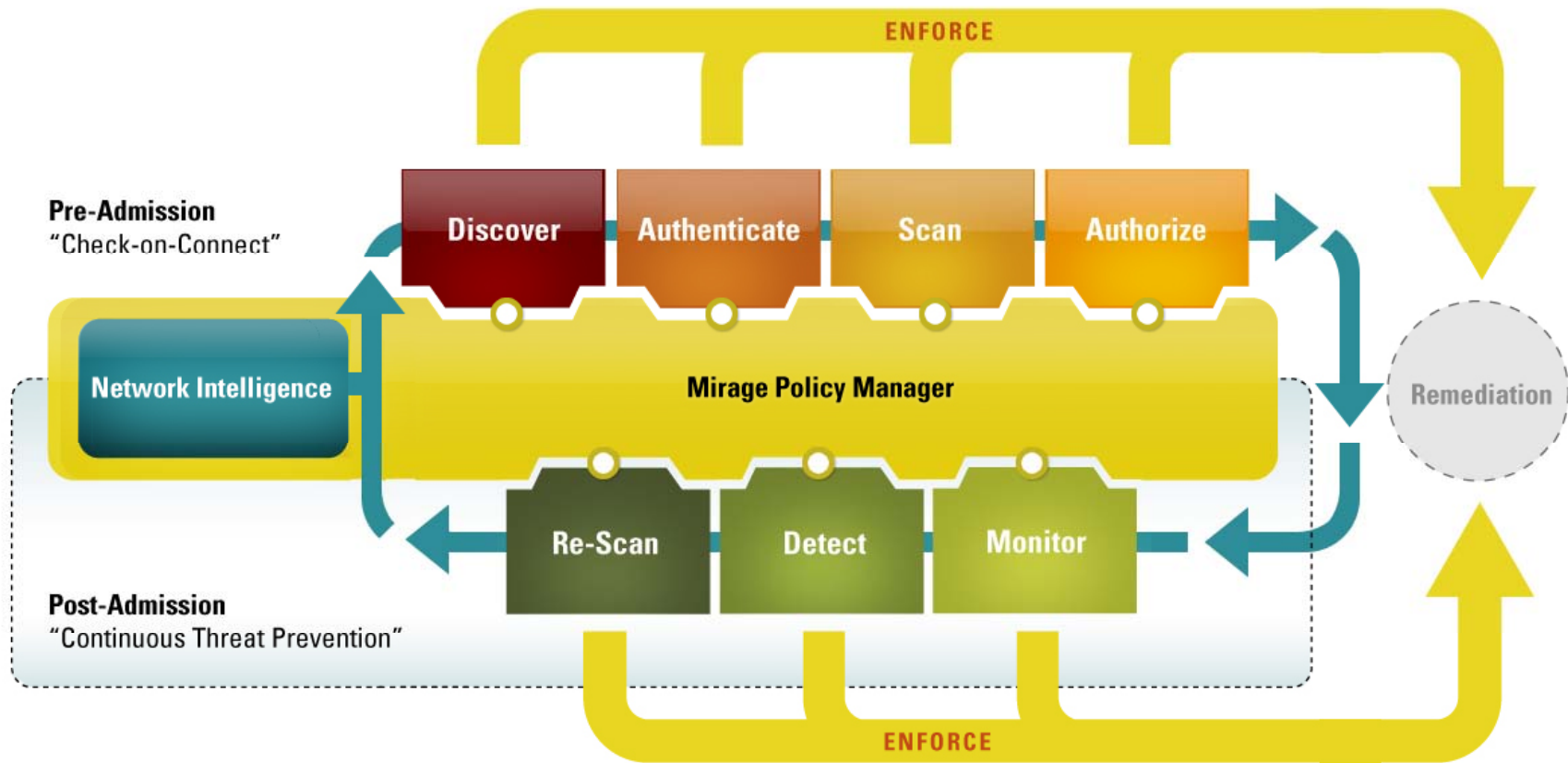
# NAC Options

Solution Appliance	Infrastructure Integration
Easy to deploy	Cumbersome to deploy
Deployment flexibility	Limited infrastructure support
Enforcement at the endpoint	Enforcement at a network choke point
Protects investment	Limits future options

# NAC Options

<b>Behavioral Analysis</b>	<b>Signature-based Analysis</b>
Zero-day threat protection	No zero-day threat protection
Identifies threat variants	Can be thwarted by threat variants
Persistent, behavior-based policy creation	Requires updates
One-time cost	Renewable license costs

# Full Cycle NAC





**You Can't Control People.**  
**Control What's On Your Network.**

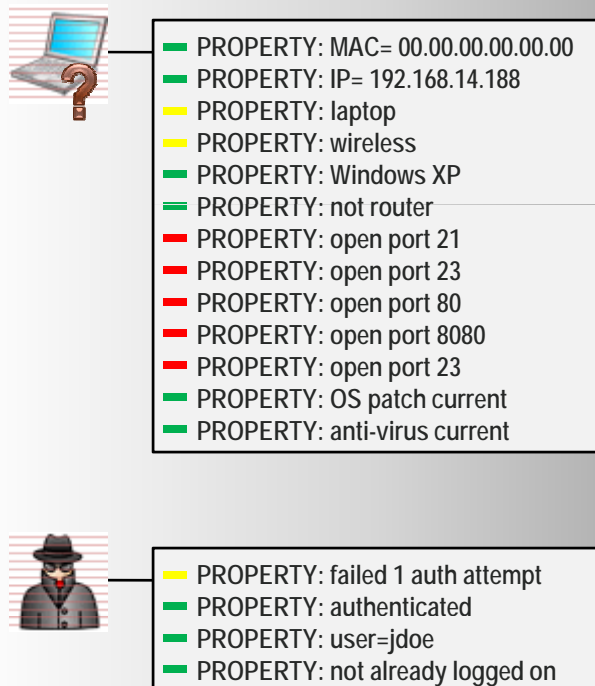


## **Future of NAC**

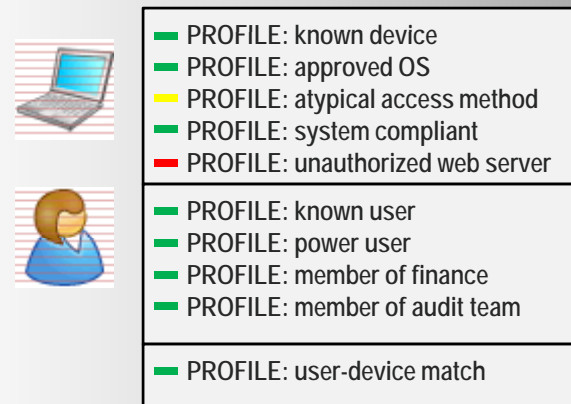
Adding context

# Extended Access Management

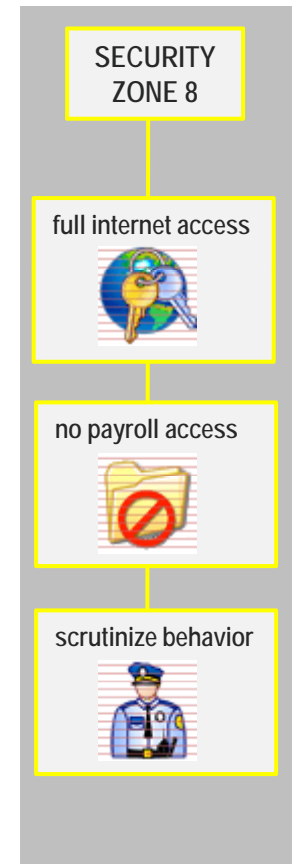
## PROPERTIES



## PROFILES



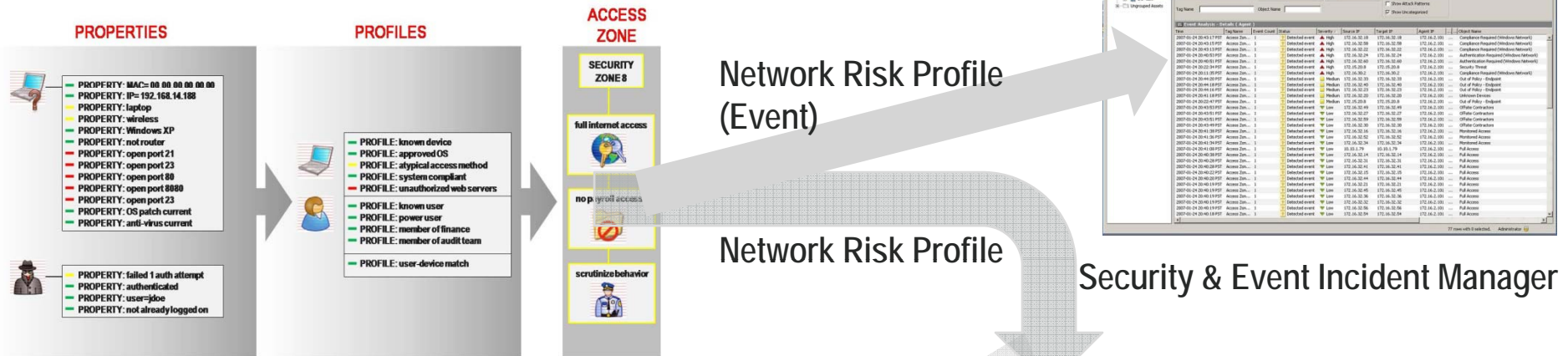
## ACCESS ZONE



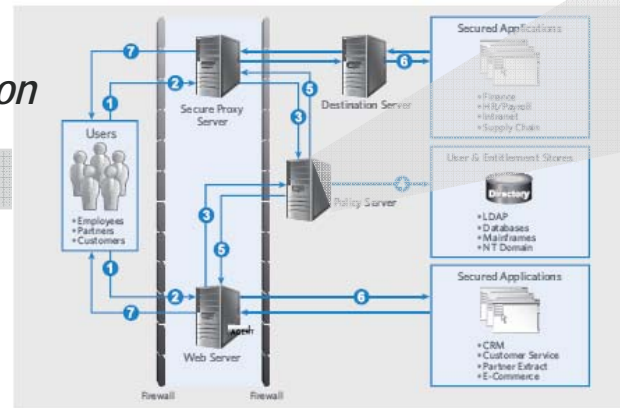


# Adaptive Identity Management

## Network Access Control Policy Domain



*Critical Transaction Notice*



## Identity & Access Management Policy Domain

You Can't Control People. **Control What's On Your Network.**



**You Can't Control People.  
Control What's On Your Network.**



## Summary

Why do we buy these things?

## What is our goal? Protect the triad.

---

- The business goal is to protect CIA.
  
- Confidentiality of Data
  - Assurance of data privacy. Only the intended and authorized recipients: individuals, processes or devices, may read the data.
  
- Integrity of that Data
  - Assurance of data non-alteration. Data integrity is having assurance that the information has not been altered in transmission, from origin to reception.
  
- Availability of the Data and Critical Business Assets
  - Assurance in the timely and reliable access to data services for authorized users. It ensures that information or resources are available when required.

## Network Security GOAL

---

- ...to minimize risk on the network with the least amount of administrative overhead and cost.
- Invest in solutions that eliminate the low-hanging fruit
  - The bulk of network attacks are opportunistic in nature, eliminate that risk
- Invest in solutions that have future / cost protection
  - Solutions that require daily maintenance have many hidden costs
- Invest in processes that compliment security infrastructure
  - Have threat mitigation and escalation plan
  - Consult local law regarding data forensics and legal admissibility

# How Does NAC Accomplish the Security GOAL?



- Typical security investments are largely re-active
  - Anti-virus relies on signatures and waits for an outbreak to occur to address the problem
  - IDS / IPS monitors traffic and re-actively addresses an outbreak at a choke point in the network
- Most security investments require significant attention to operate effectively or interfere with user productivity
  - IDS/IPS can require daily upkeep to remain effective
  - Anti-virus can interfere with desktop applications and cause help-desk pains
- NAC is pro-actively assessing risk and then re-enforcing with real-time monitoring at the desktop level, sometimes w/o software!
  - Some NAC solutions can address the risk management challenge out-of-band, infrastructure independent, software free, etc.
  - Behavioral threat assessment can require little or no daily upkeep
  - Following posture assessment, high risk devices are kept off the network completely



**You Can't Control People.  
Control What's On Your Network.**



**Thank You**

Q&A

Kurtis Minder  
Regional Director  
Mirage Networks

[kminder@miragenetworks.com](mailto:kminder@miragenetworks.com)  
847-563-4272  
[www.miragenetworks.com](http://www.miragenetworks.com)



**You Can't Control People.**  
**Control What's On Your Network.**



**Extra Slides**

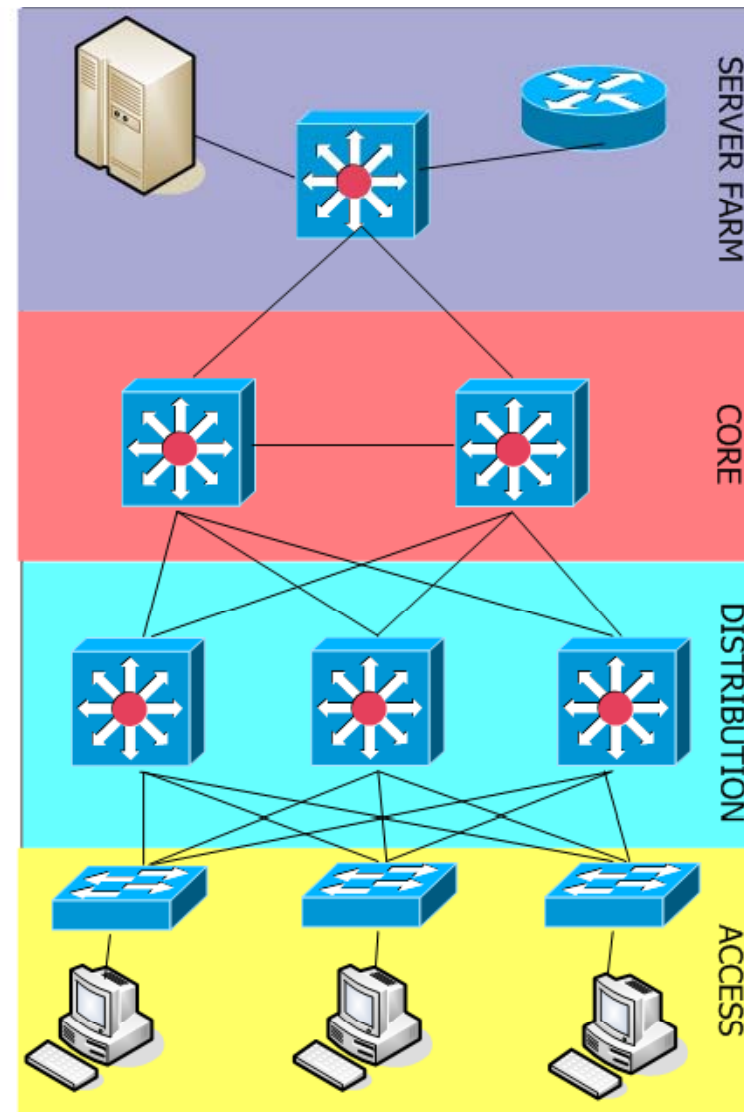
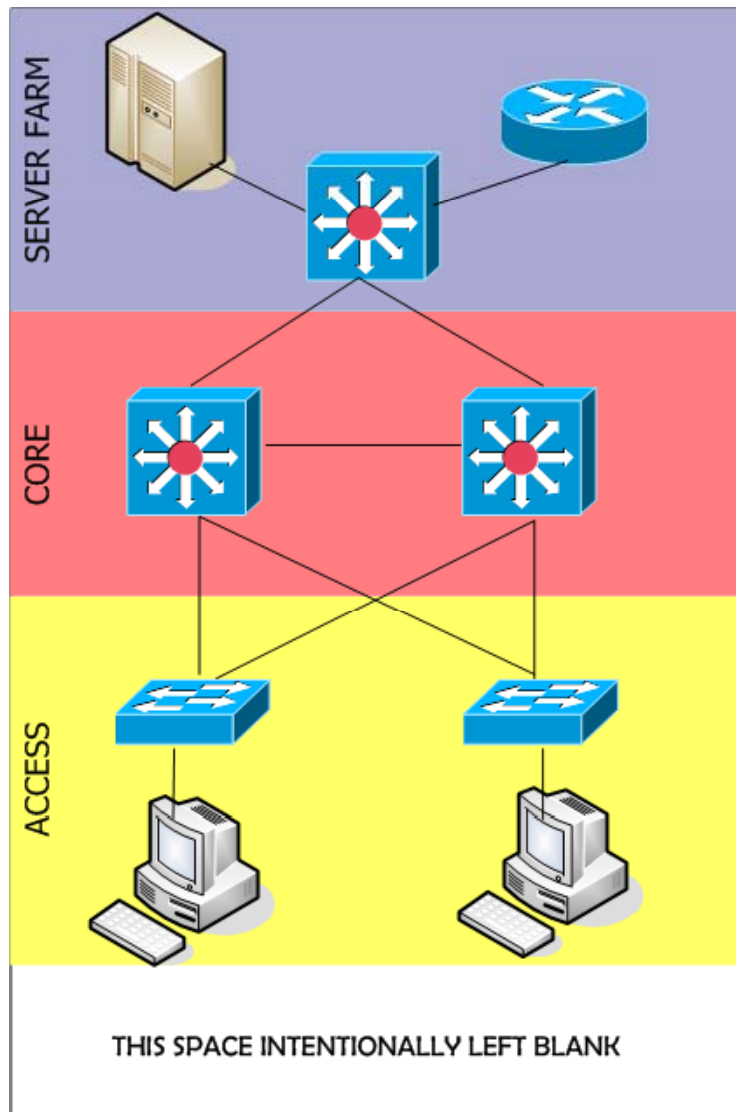
# Network Design Meets Security Design

---

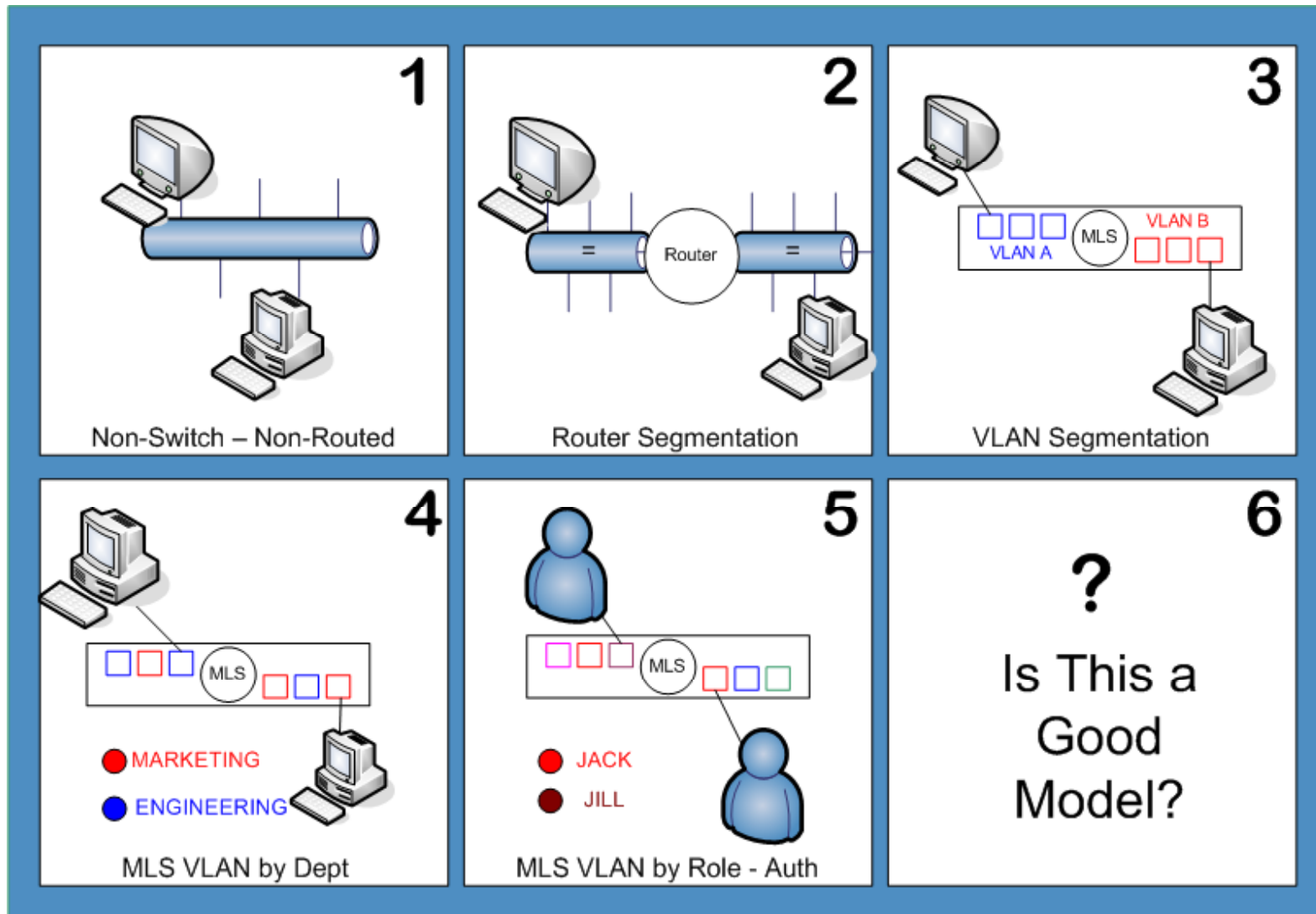
- Multi-layer Switching
  - Fundamental to network architecture
  - Supplemental to network security
  
- Getting closer to the desktop
  - Access switch technologies
  - Agent approaches
  
- Virtual Local Area Networks – (VLAN)s
  - Network segmentation or security tool?
  
- Appliance or infrastructure?



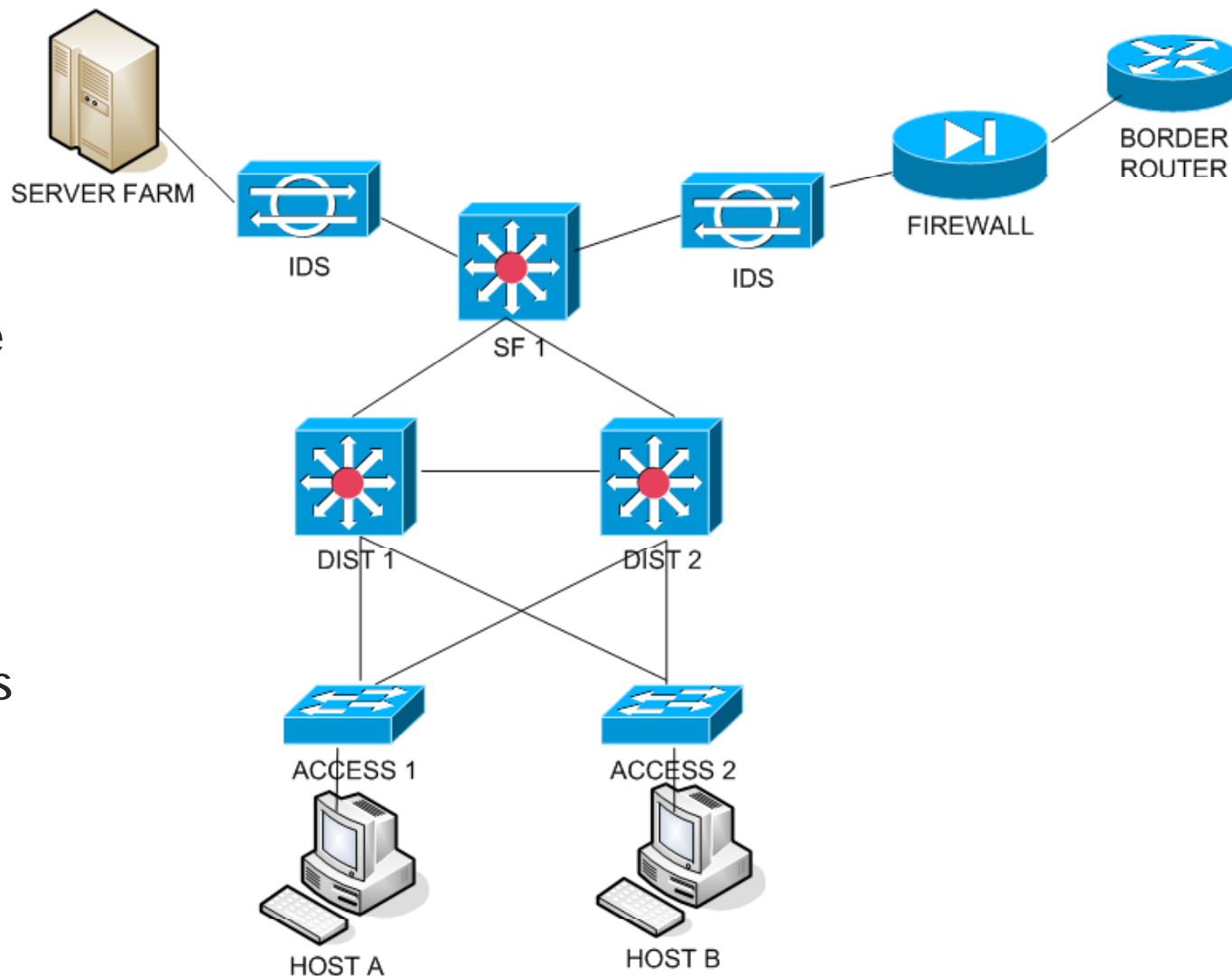
# Network Design Models



# Evolution of Network Device Segmentation – Where is 802.1x Going?



# Network Security Design Example

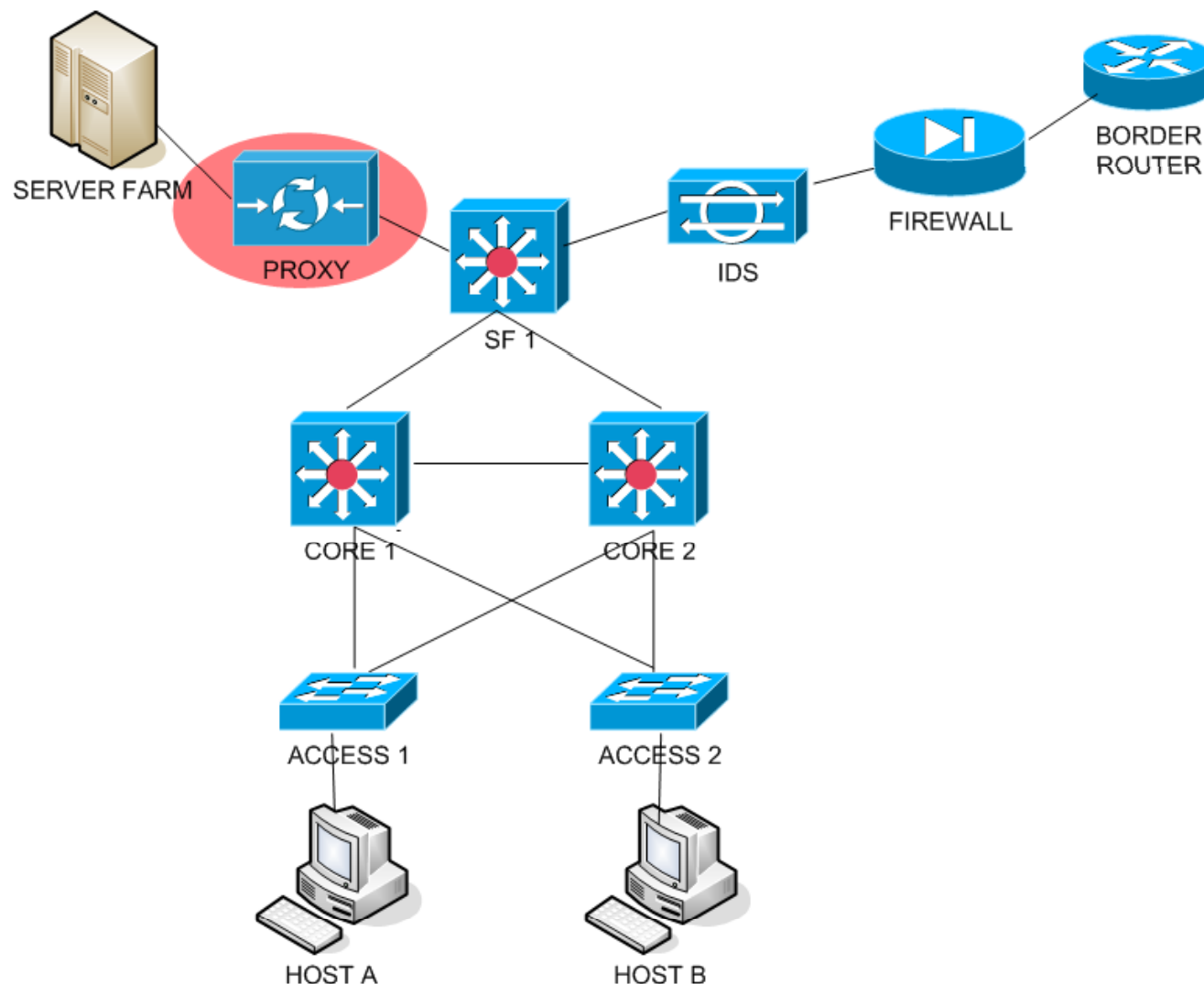


Typical network design includes security at the perimeter. This is a best practice

Also desktop software may be used to keep machines clean of virus and malicious content

This is a typical network, simplified

# NAC Design - Proxy

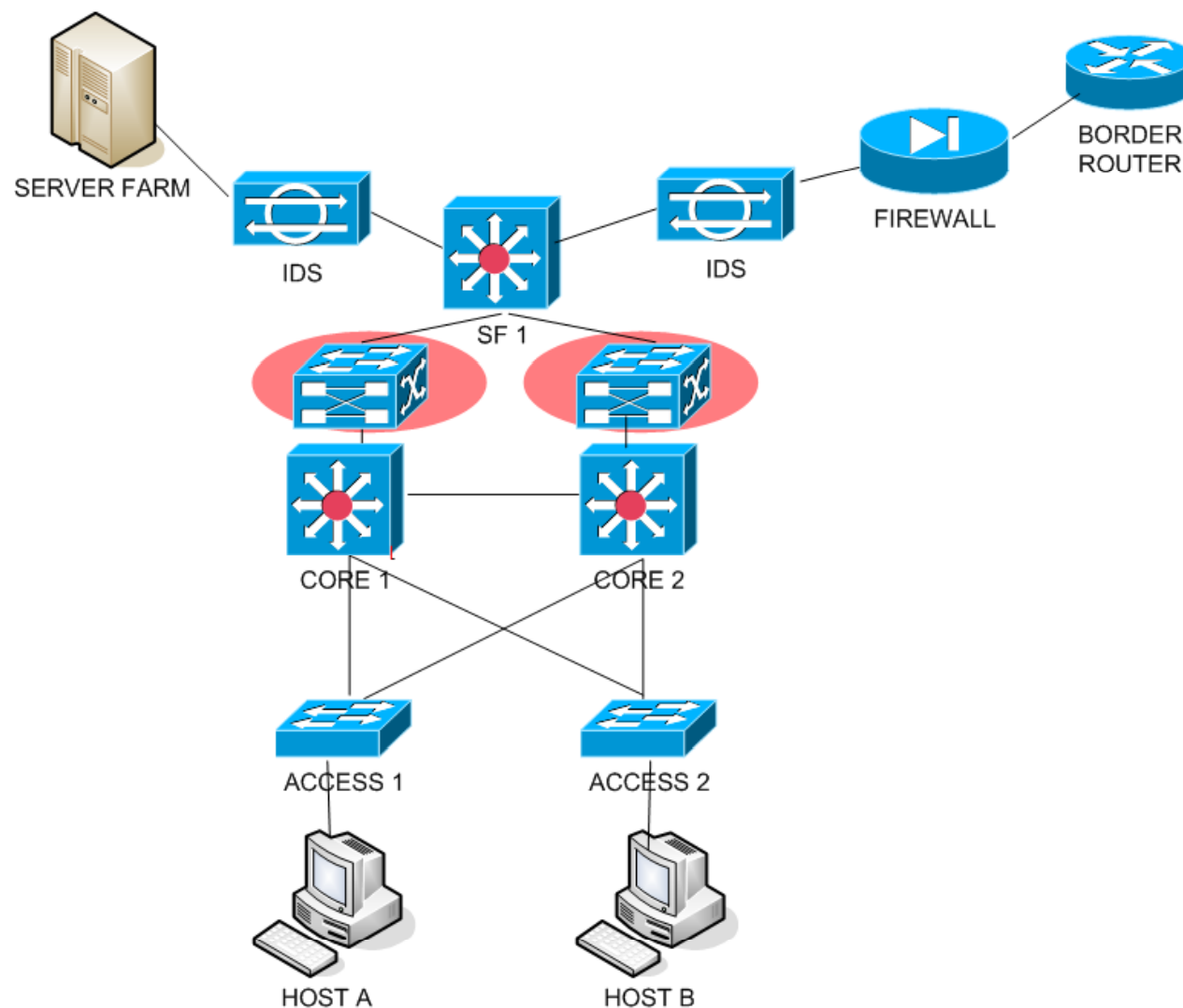


Using proxy technology to enforce NAC can be very effective since it supplies L3-7 visibility into packet data

It can also be a point of failure and latency

Downstream traffic may be missed

# NAC Design - Inline

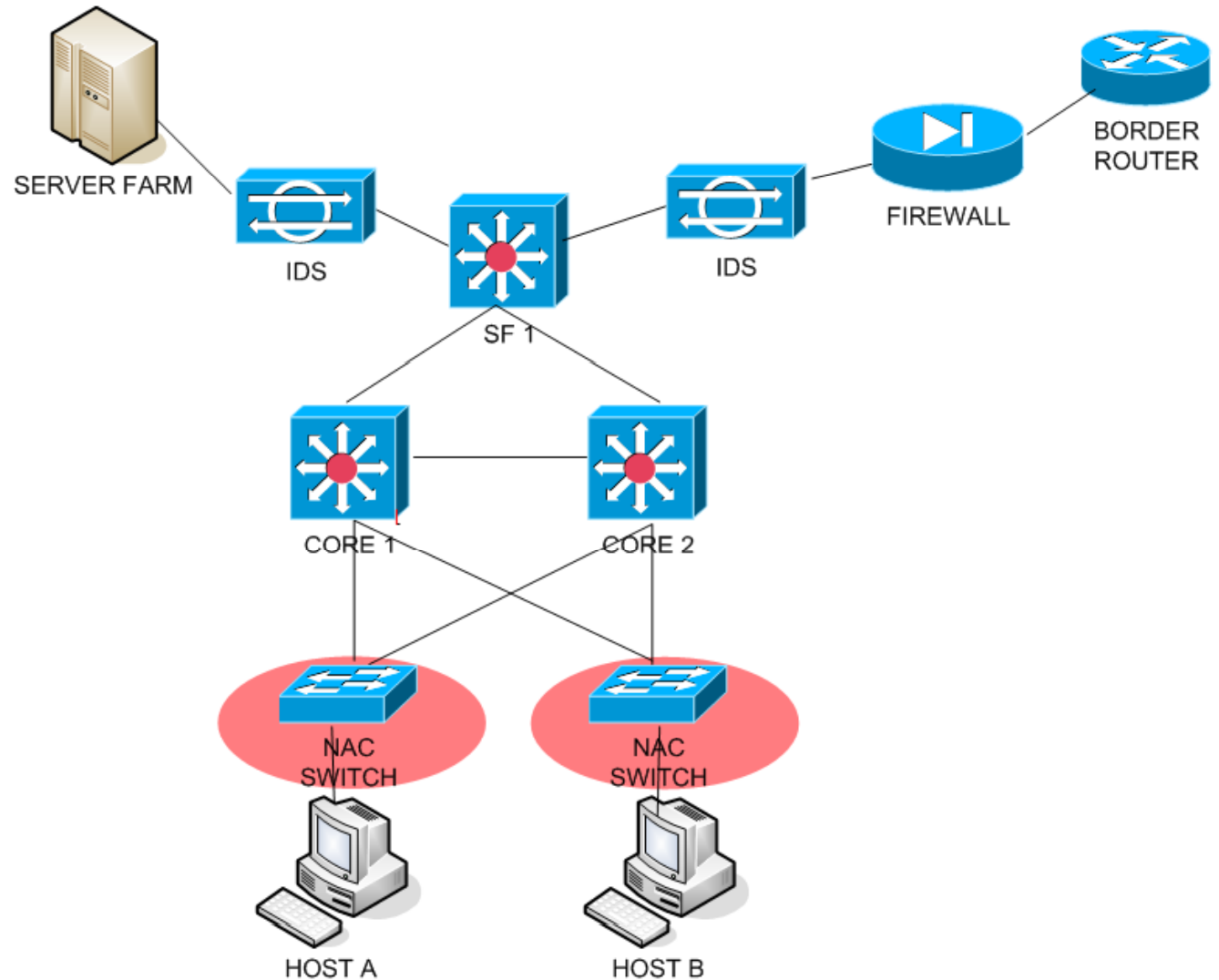


Inline NAC enforcers effectiveness are directly impacted by network placement

Point of failure/latency possible

Downstream missed

# NAC Design – Access Switch Replacement



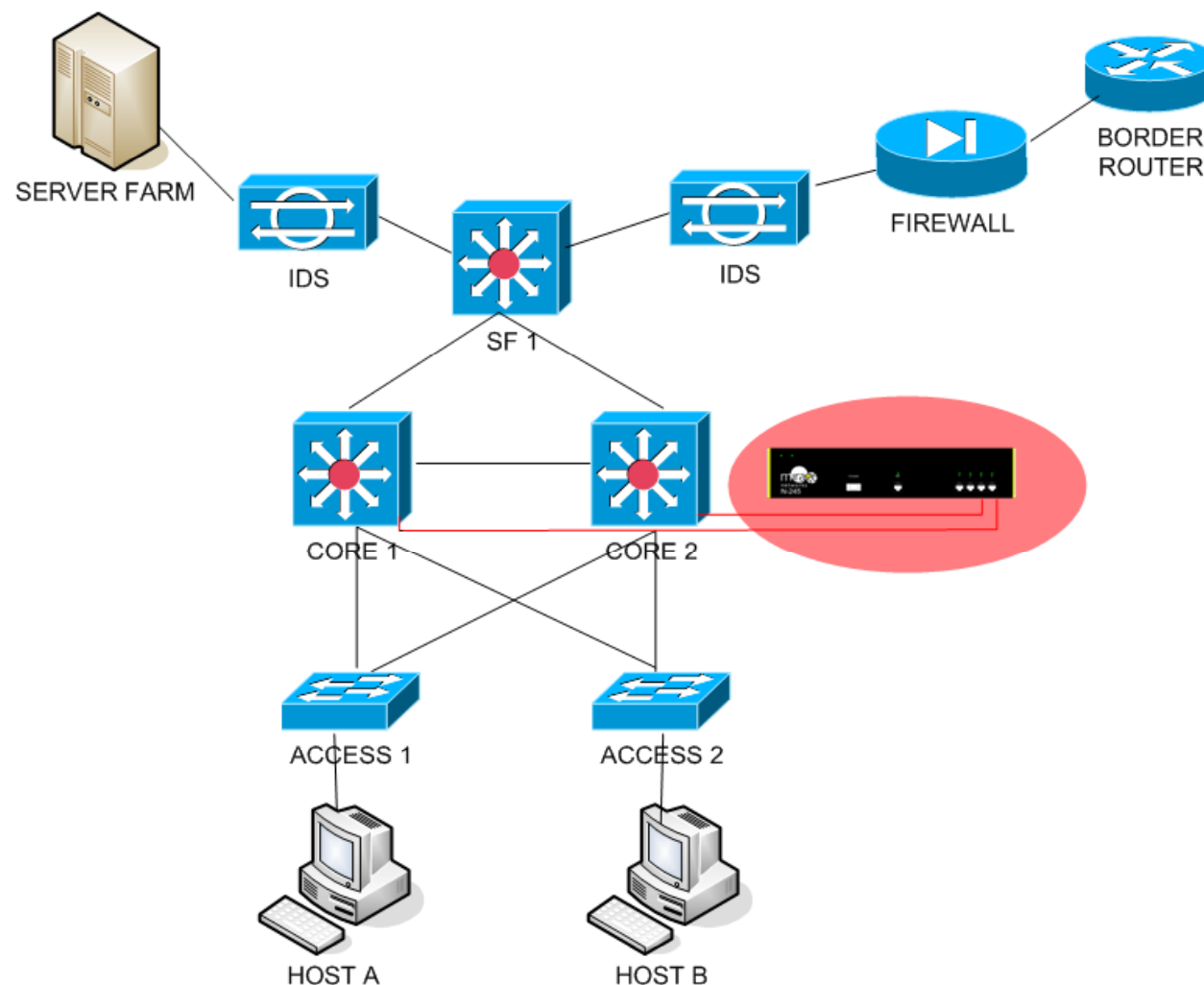
Access switch NAC devices are a viable solution

L3-7 visibility

Expensive

Not a switch

# NAC Design – OOB



Out of band solutions are ideal for complex network environments

Supports heterogeneous environments

Sees all traffic

May need complex switch integration

# Monitoring Post Network Entry

- The forgotten element of Network Access Control
  - Why is monitoring a critical element of NAC?
    - Can't effectively check for all threats on entry - takes too long
    - Security policy state can change post entry - users initiate FTP after access is granted
    - Infection can occur post entry - e-mail and web threats can change security state of the device
  
- This is critical to network awareness / intelligence
  - Monitoring is both for threats and policy adherence - takes advantage of policy definition of NAC solution
  - Works hand in hand with NAC quarantine services



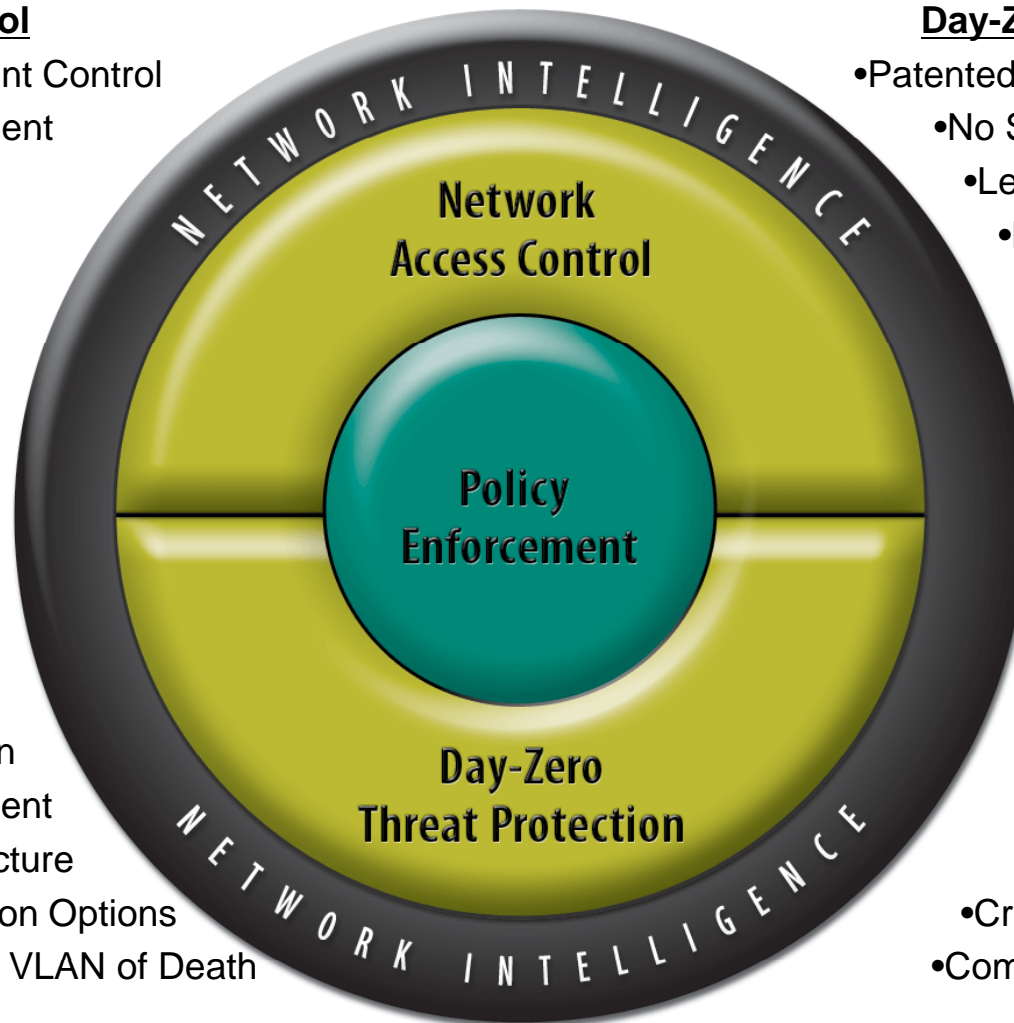
# Mirage Networks Endpoint Control

## Network Access Control

- Comprehensive Endpoint Control
- On-entry Risk Assessment
- Policy Enforcement
- IP Telephony Enabled
- Wireless Support
- Out-of-Band
- Agentless

## Policy Enforcement

- Surgical Quarantining
- Customized remediation
- Infrastructure-Independent
- No Network Re-architecture
- Flexible Self-Remediation Options
- ARP Management - No VLAN of Death



## Day-Zero Threat Protection

- Patented Behavioral Technology
- No Signatures, No Updates
- Leverages Dark IP Space
- Minimal False Positives
- Customized Policies
- Day Zero

## Network Intelligence

- Central Mgmt
- Asset Tracking
- Network Visibility
- Executive Reports
- Cross Network Correlation
- Compliance & Audit Support

# Strategic Partners



IBM Internet Security Systems (formerly ISS) has formed an alliance with Mirage Networks to provide Network Access Control to global enterprise customers. (Signed November, 2006)



Extreme Networks provides organizations with the resiliency, adaptability and simplicity required for a truly converged network that supports voice, video and data over a wired or wireless infrastructure, while delivering high-performance and advanced security features. (Signed March, 2005)

**MITSUI & CO., LTD.**

Mitsui Bussan Secure Directions, a subsidiary of Mitsui & Co., Ltd. - one of the world's most diversified and comprehensive trading and services companies - powers Mirage NAC sales in the Japanese marketplace. (Signed October, 2004)



AT&T resells Mirage NAC in its managed services portfolio. Marketed as AT&T Managed IPS™, it represents the AT&T commitment to enabling business to be conducted effectively, efficiently and securely across both wired and wireless IP networks. (Signed March, 2005)



Part of the Avaya DevConnect Program, Mirage works with Avaya to develop world-class interior network defense solutions, particularly for emerging IP telephony technology.

# Selected Customers

## Finance



## Government



## Healthcare



## Professional Services



## Higher Education



## K-12










## Manufacturing



## Other



# Mirage NAC is the Answer

-  Full Cycle: Pre- and Post-Admission Policy Enforcement
-  Out of Band Deployment; no latency, switch integration
-  Infrastructure Independent: All networks, All devices, All OSs
-  Zero Day protection without signatures
-  Agentless: Easy to Deploy and Manage
-  Quarantines without switch integration
-  Patented technology

