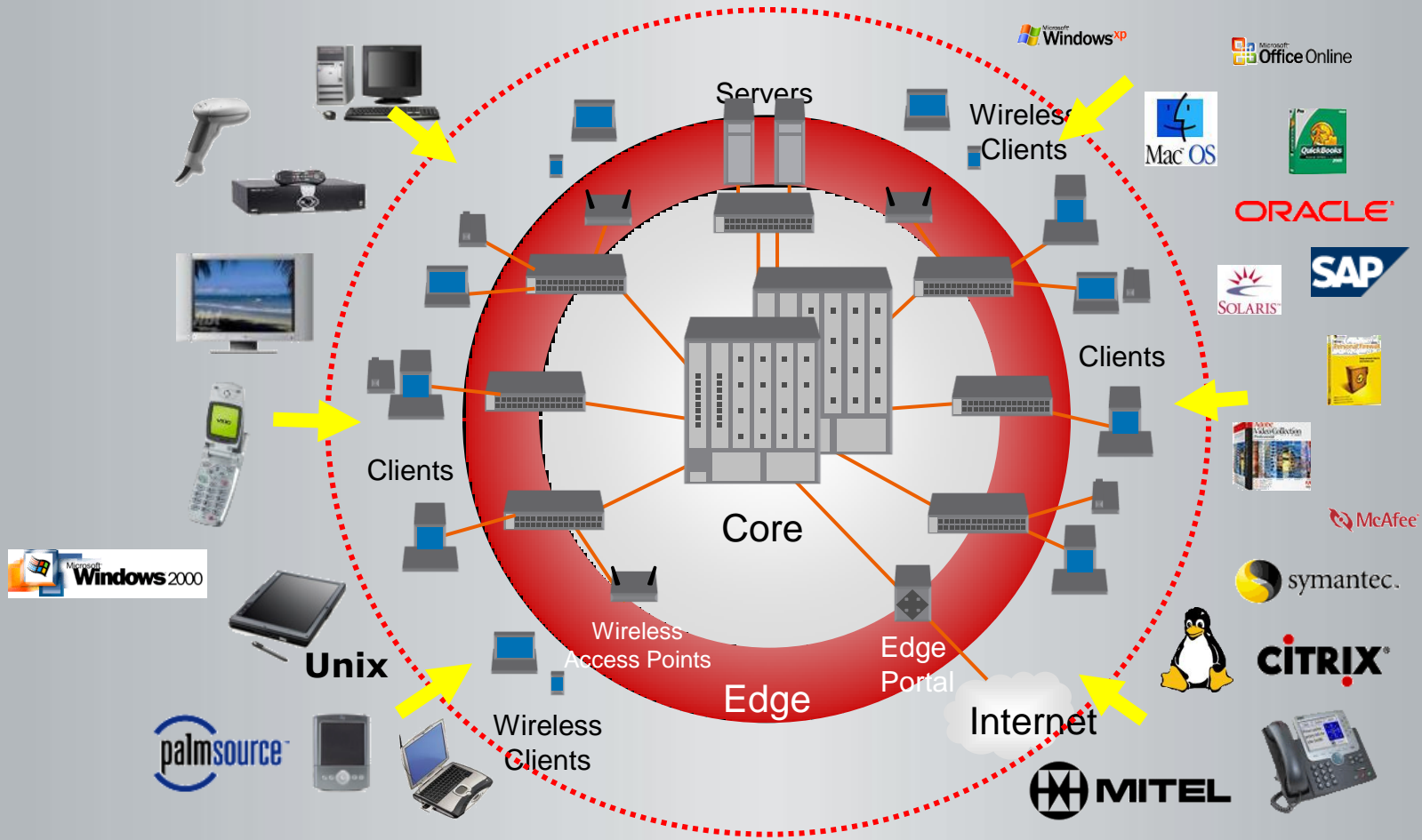


“Taking it to the Edge” Secure Business Solutions by ProCurve

Don Wisdom
President Datalink Networks



What's On Your Network?



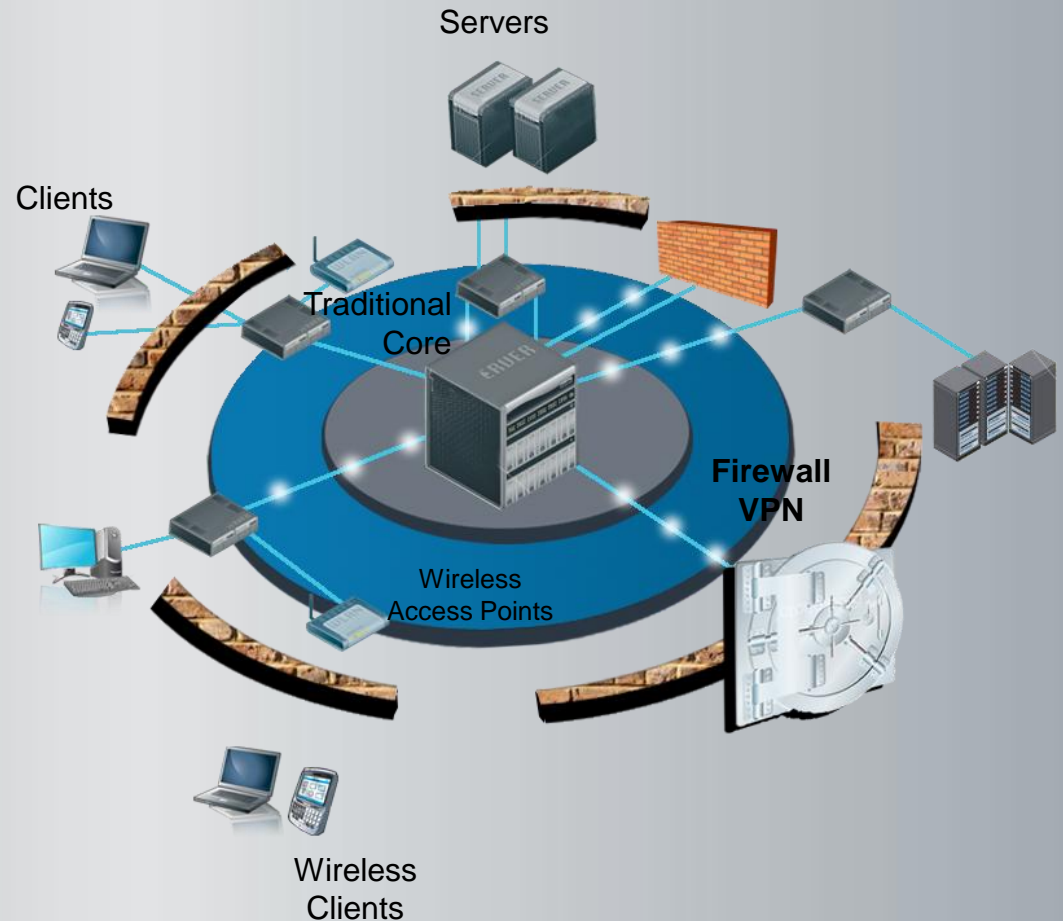
The fragmented approach does not work

Network Vendors

- Bolt-on security at the WAN perimeter
 - *Firewalls*
 - *IDS/IPS*
- Bolt-on security enforcement in the core
- Upgrade to get separate Wired and Wireless NAC

Security Vendors

- Overlay the network with dedicated security appliances
- Update host-based software with intrusive agents



Proactive Security

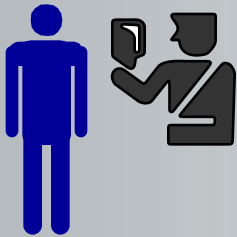
**Security
Offense**

**Security
Defense**

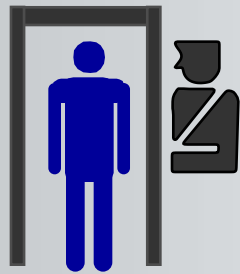
Secure Infrastructure

Analogy: Airline Security

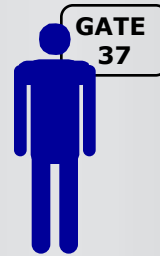
Verify Identity



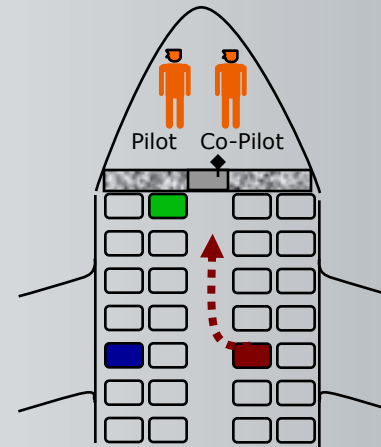
Scan for Compliance



Control Access



Monitor Behavior



Isolate Suspects



Evaluate Credentials

- 802.1x
- Web Auth
- MAC Auth
- RADIUS

Evaluate Integrity

- IDM agent
- Per Port policy enforcement
- Quarantine

Quarantine Threats

- Policy Based Manager
- Per Port
- Wired and Wireless
- Edge

ProCurve Networking
HP Innovation
ProActive

CONTRACTORS

GUEST

EMPLOYEES

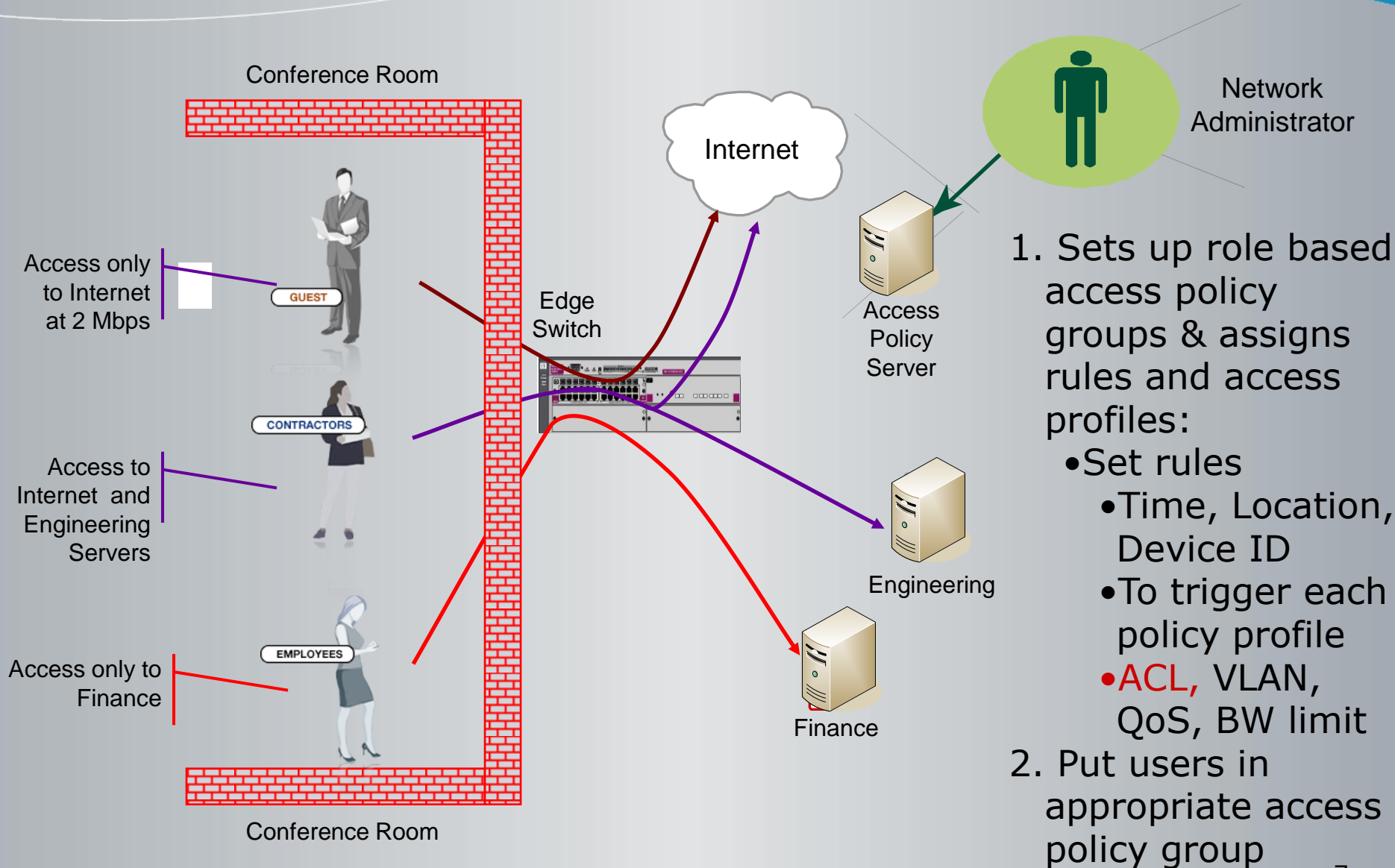
Protect

Intelligent EDGE



IDM User Experience

(Who, What, When, Where, How)

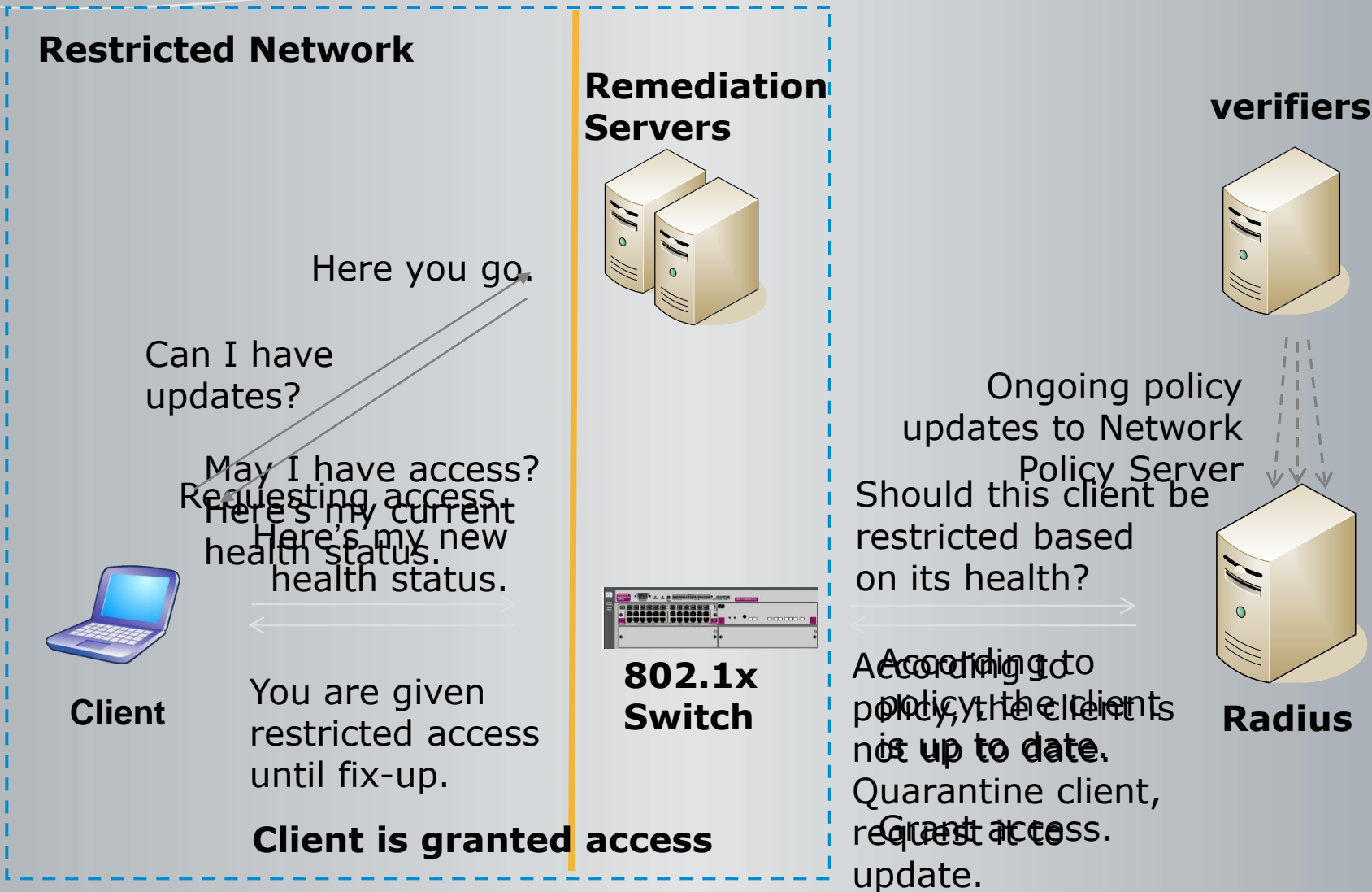


1. Sets up role based access policy groups & assigns rules and access profiles:

- Set rules
 - Time, Location, Device ID
 - To trigger each policy profile
 - ACL**, VLAN, QoS, BW limit

2. Put users in appropriate access policy group

Network Access Control 101



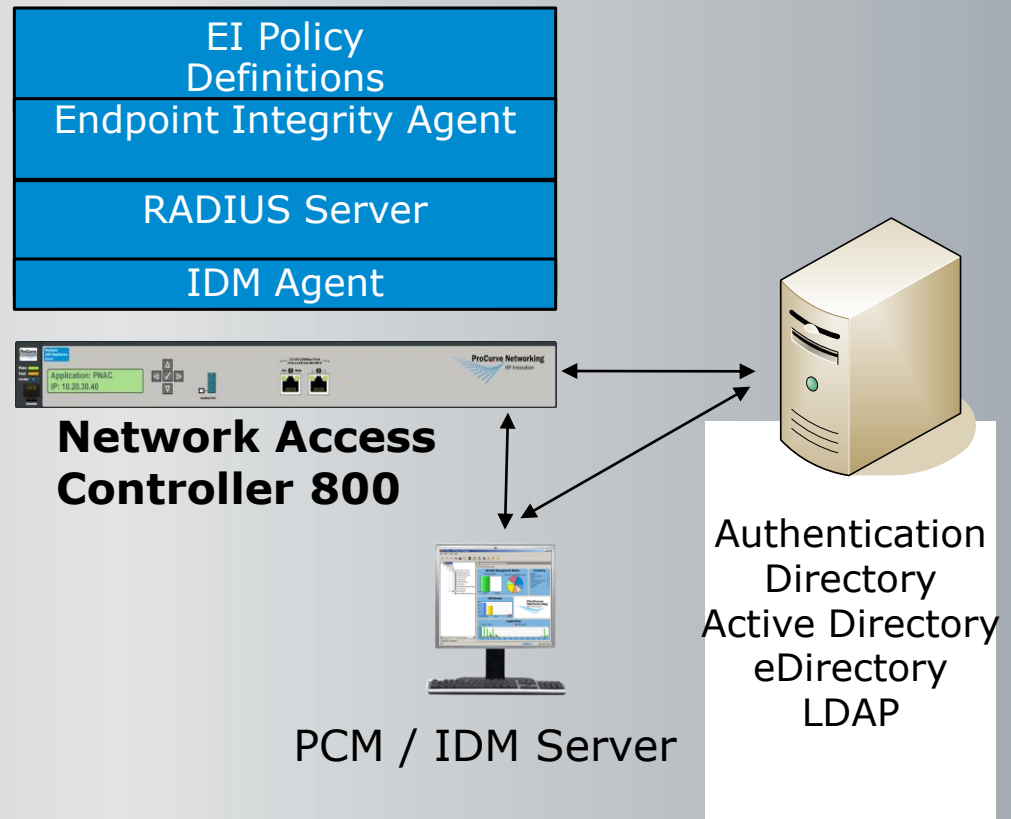
ProCurve Access Control Solution 2.0

Identity Driven Manager (IDM) & ProCurve Network Access Controller 800

Endpoint Tests for

- Operating Systems versions & updates
- Anti-Virus & Anti Spyware software
- Required or prohibited software

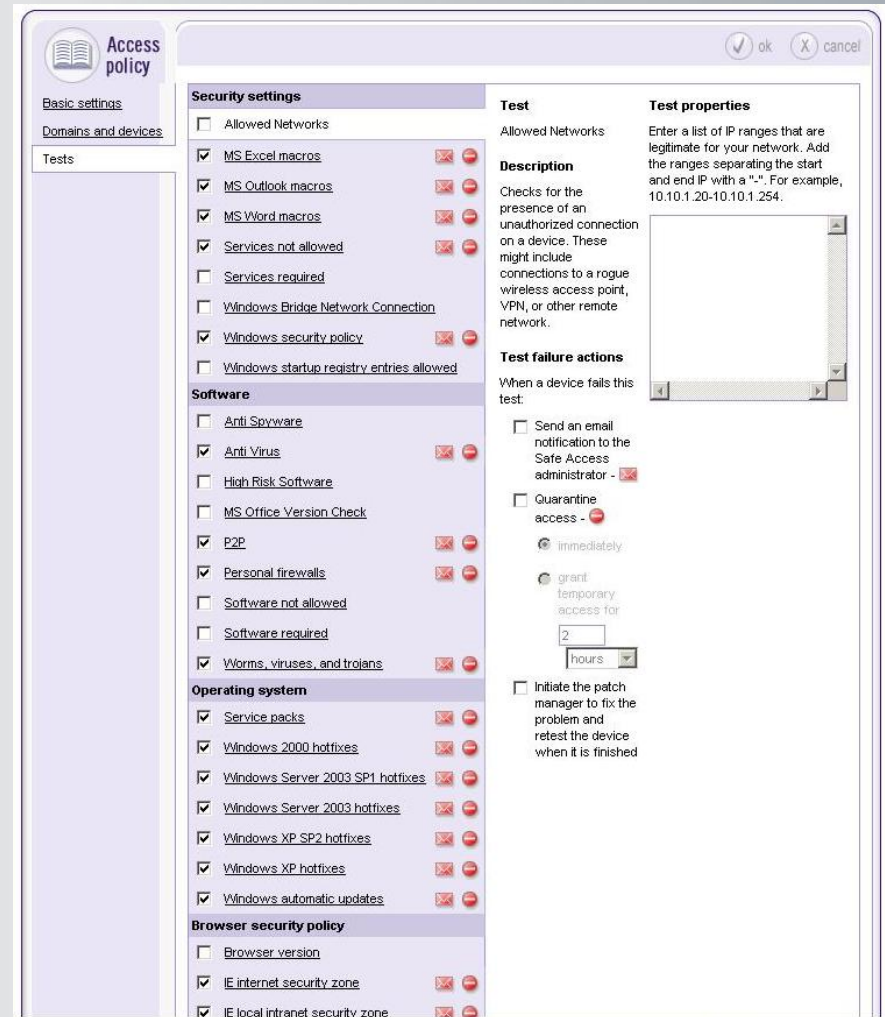
And more ...



Endpoint integrity

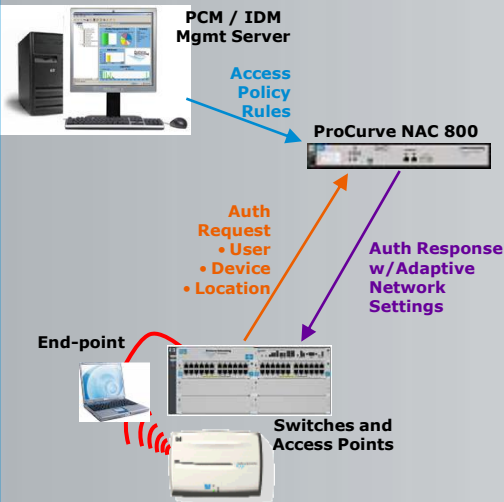
- Antivirus, spyware, firewalls, peer-to-peer, allowed and prohibited programs and services
- OS versions, services packs, hot-fixes
- Security settings for browsers and applications

New tests developed and delivered regularly



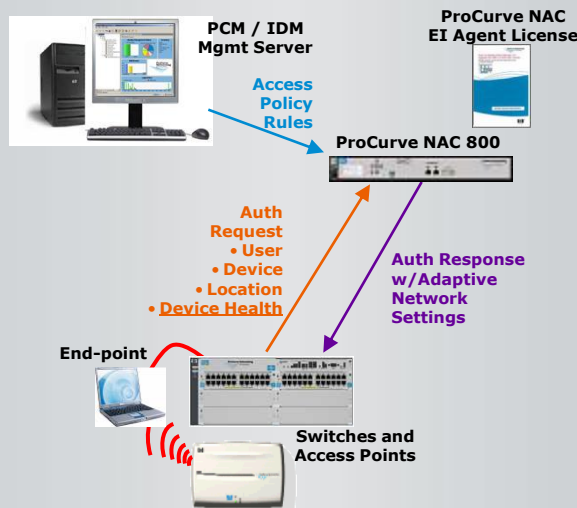
Flexible Solution Options

Solution Option #1: Adaptive Network Access



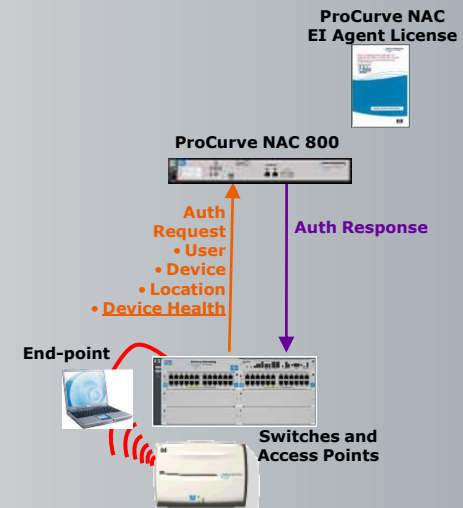
ProCurve Network Devices
+ Identity Driven Manager

Solution Option #2: Adaptive Network Access w/ Endpoint Integrity



ProCurve Network Devices
+ Identity Driven Manager
+ ProCurve NAC 800
w/ ProCurve NAC EI Agents

Solution Option #3: Access Control w/ Endpoint Integrity Check



ProCurve Network Devices
+ ProCurve NAC 800
w/ ProCurve NAC EI Agents



Defense





Industry standard network traffic monitoring technology

- RFC3176
- HP invented packet sampling technology
- First demonstrated with CERN in 1991
- XRMON included in HP Networking products since 1993
- sFlow introduced to ProCurve products in 2001

Provides complete network-wide visibility into:

- Layer 2, 3, 4 and above information
- Bandwidth utilization
- Top talkers, protocols, applications

Measurements from every switch and interface all of the time

Scalable to every port, up to 10Gb/s speeds

Extensible architecture: wireless, storage, WAN....

Network Immunity Manager Deployment Scenarios

Detection Analysis

- Duplicate IP
- IP spoofing
- IP fan out
- DNS tunneling
- Packet size deviation used
- Protocol anomalies
- TCP/UDP Fan out

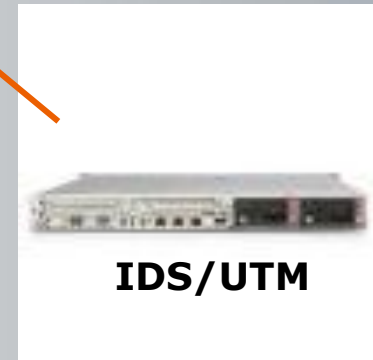


ProCurve Manager Network Immunity Manager

- NBAD/sFlow based virus alert

sFlow samples

Virus Throttling
alert



IDS/UTM

Per port response,
Reconfiguration of switch

Virus Response Methods

- Quarantine VLAN
- Offender MAC lockout
- Offender port shutdown
- Offender port rate limiting
- Offender port mirroring for deeper analysis
- Enable sflow at the offender port
- Email notification

Infected
End-point



Security Standards Leadership

Defense

IEEE 802.1

Ethernet Switching Standards

-----> *Working Group Vice-Chair*

IEEE 802.1AE

MAC Security / Ethernet Encryption

-----> *Voting member, Contributor*

IEEE 802.1af

Encryption Key Agreement Protocol

-----> *Voting member, Contributor*

IEEE 802.1AR

Secure Device Identity

-----> *Voting member,
Contributor*

IEEE 802.1X

Port Authentication Protocol

-----> *Initiated standard, Key
Technical Contributor*

Trusted Computing Group

End Device Compliance Authorization

-----> *Initiated standard, Interim
Chair, Editor of IF-PEP*

IETF Radius Extensions

Identity Driven Manager (IDM) Attributes

-----> *Internet-Draft Editor,
Technical Advisor*

IETF NEA

Network Endpoint Assessment

-----> *TCG/TNC Liaison,
Contributor*

ProActive

A decorative graphic consisting of several blue lines and dots. On the left, a series of small blue dots forms a curved path that transitions into several solid blue lines of varying lengths and thicknesses, all pointing towards the right. The lines are arranged in a way that suggests motion or a network structure.

ProCurve Networking

HP Innovation

