Interop Labs
Network Access Control

Interop Las Vegas 2007

Jan Trumbo

trumbo@opus1.com

Interop Labs

Interop Labs are:

- Technology Motivated,
- Open Standards Based,
- Vendor neutral,
- Test and Education focused,
- Initiatives…

With team members from:

- Industry
- Academia
- Government

Visit us at Booth 122!

Technical contributions to this presentation include:

- Steve Hanna, Juniper Networks and TCG TNC
- Kevin Koster, Cloudpath Networks, Inc.
- Karen O'Donoghue, Joel Snyder, and the whole Interop Labs NAC team

Objectives

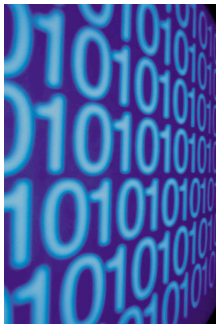
- This presentation will:
  - Provide a general introduction to the concept of **Network Access Control**
    - Highlight the three most well known solutions
  - Provide a context to allow a network engineer to *begin* to plan for NAC deployment
  - Articulate a vision for NAC
- This presentation will not:
  - Provide specifics on any of the three major approaches introduced
  - Delve into the underlying protocol details

Why Network Access Control?

- Desire to grant different network access to different users, e.g. employees, guests, contractors
- Network endpoints can be threats
  - Enormous enterprise resources are wasted to combat an increasing numbers of viruses, worms, and spyware
- Proliferation of devices requiring network connectivity
  - Laptops, phones, PDAs
- Logistical difficulties associated with keeping corporate assets monitored and updated

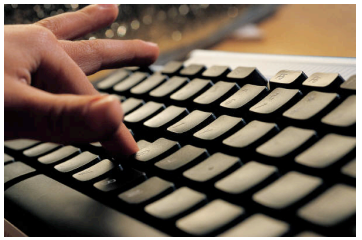
Network Access Control is

Who you are …



…should determine

What you can access



“Who” Has Several Facets

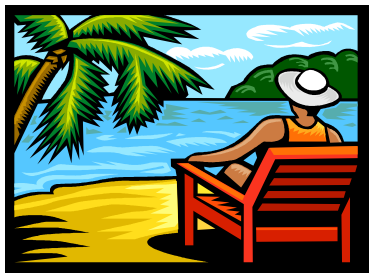
User Identity

+

End-point Security Assessment

+

Network Environment



Access Policy May Be Influenced By

- **Identity**
  - Jim (CTO), Steve (Network Admin), Sue (Engineering), Bob (Finance), Brett (Guest)
- Location
  - Secure room versus non-secured room
- Connection Method
  - Wired, wireless, VPN
- Time of Day
  - Limit after hours wireless access
  - Limit access after hours of employee's shift
- **Posture**
  - A/V installed, auto update enabled, firewall turned on, supported versions of software
  - Realtime traffic analysis feedback (IPS)

Sample Policy

IF user group="phone"

THEN VLAN="phone-vlan"

ELSE IF non-compliant AND user = "Alice"

THEN VLAN="quarantine" AND activate automatic remediation

ELSE IF non-compliant AND user = "Bob"

THEN VLAN="quarantine"

ELSE IF compliant

THEN VLAN="trusted"

ELSE deny all

NAC is More Than VLAN Assignment

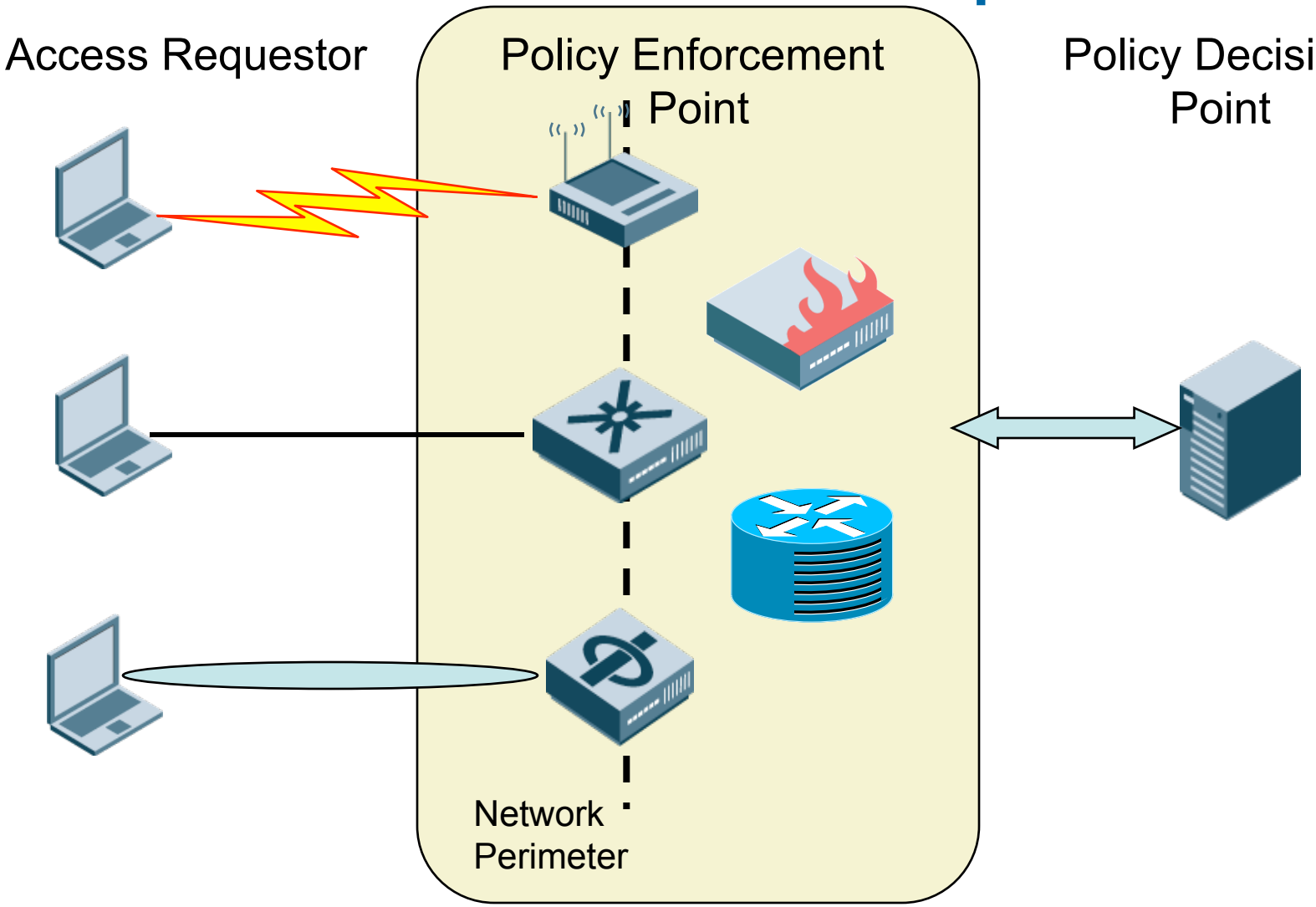
- Additional access possibilities:
  - Access Control Lists
    - Switches
    - Routers
  - Firewall rules
  - Traffic shaping (QoS)
- Non-edge enforcement options
  - Such as a distant firewall

NAC is More Than Sniffing Clients for Viruses

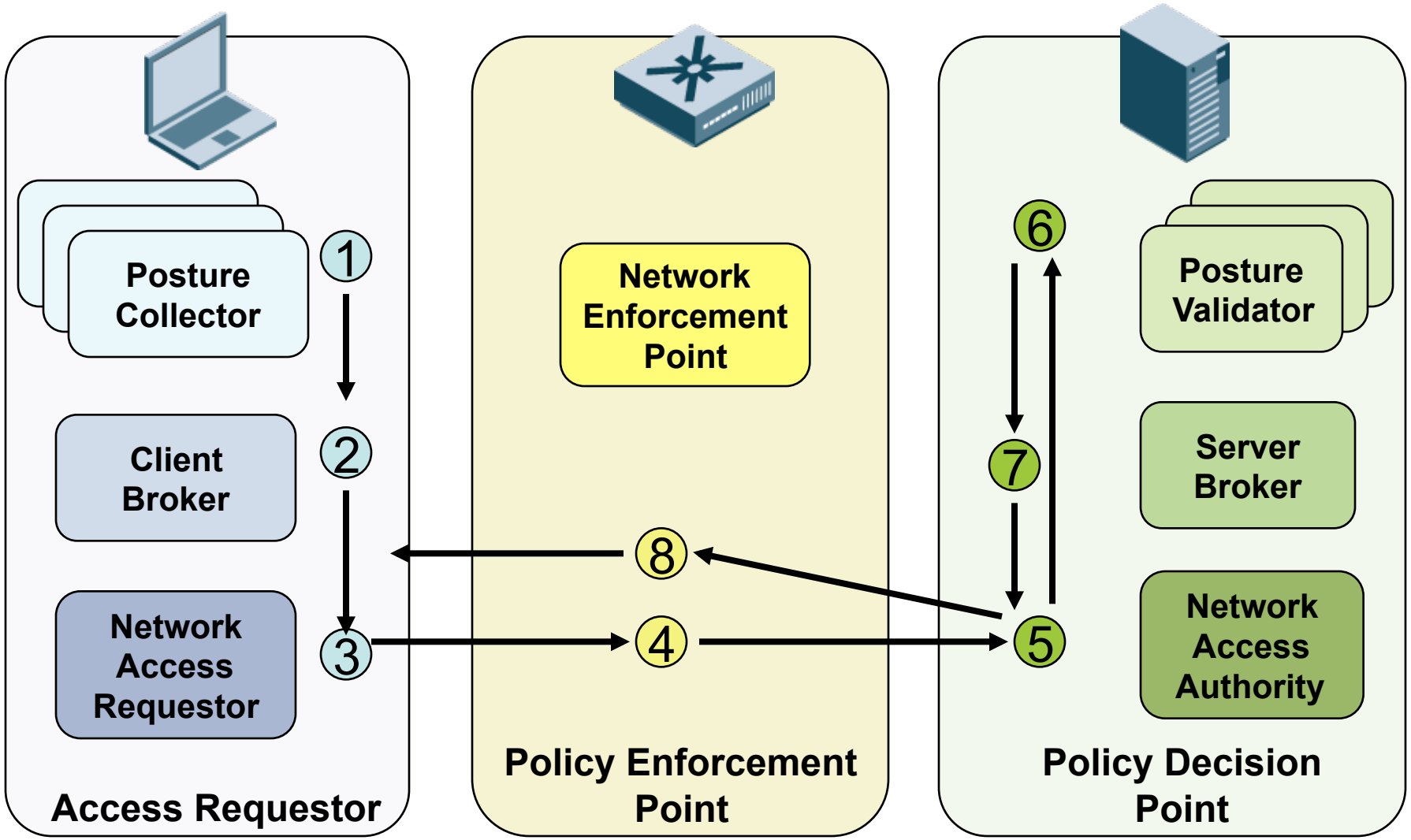
- Behavior-based assessment
  - Why is this printer trying to connect to ssh ports?
- VPN-connected endpoints cannot access HR database

You need control points *inside* the network to make this happen

Generic NAC Components

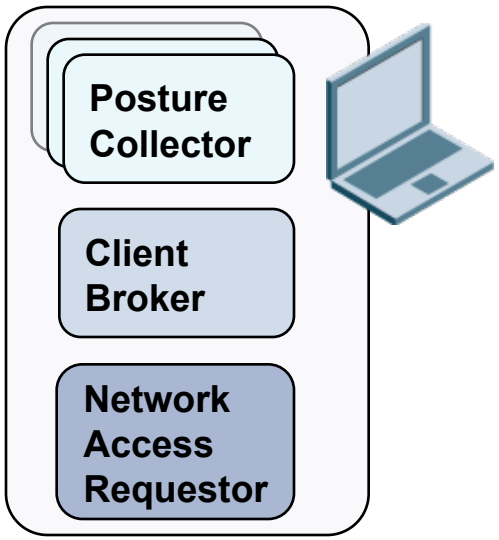


Sample NAC Transaction



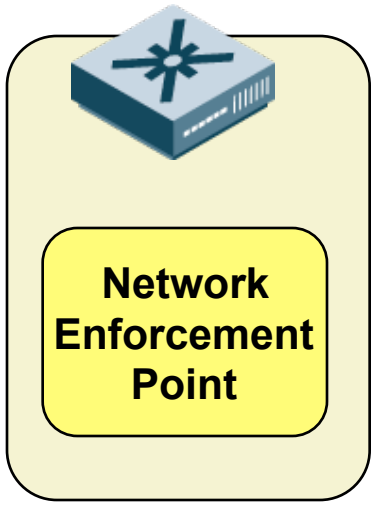
Access Requestors

- Sample Access Requestors
  - Laptops
  - PDAs
  - VoIP phones
  - Desktops
  - Printers



- Components of an Access Requestor / Endpoint
  - Posture Collector(s)
    - Collects security status information (e.g. A/V software installed and up to date, personal firewall turned on)
    - May be more than one per access requestor
  - Client Broker
    - Collects data from one or more posture collectors
    - Consolidates collector data to pass to Network Access Requestor
  - Network Access Requestor
    - Connects client to network (e.g. 802.1X supplicant or IPSec VPN client)
    - Authenticates user
    - Sends posture data to Posture Validators

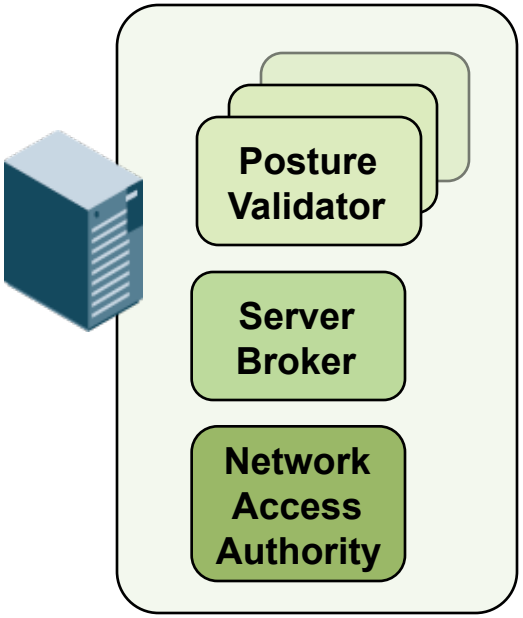
Policy Enforcement Points



Policy Enforcement Point

- Components of a Policy Enforcement Point
  - Network Enforcement Point
    - Provides access to some or all of the network
- Sample Policy Enforcement Points
  - Switches
  - Wireless Access Points
  - Routers
  - VPN Devices
  - Firewalls

Policy Decision Point

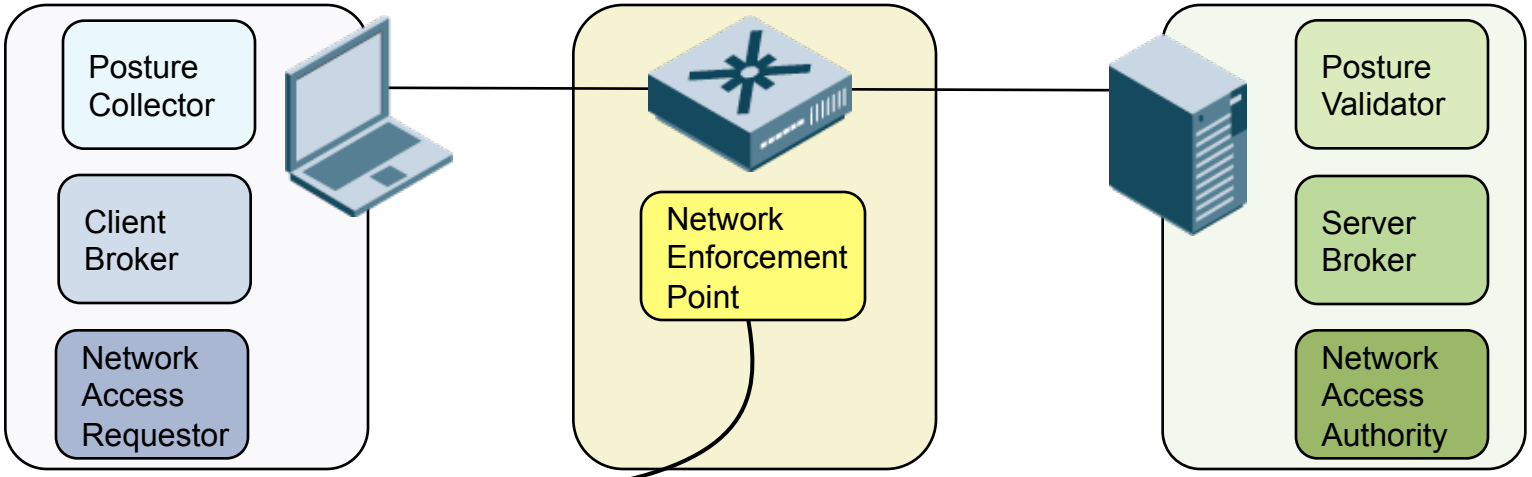


Policy Decision Point

- Components of a Policy Decision Point
  - Posture Validator(s)
    - Receives data from the corresponding posture collector
    - Validates against policy
    - Returns status to Server Broker
  - Server Broker
    - Collects/consolidates information from Posture Validator(s)
    - Determines access decision
    - Passes decision to Network Access Authority
  - Network Access Authority
    - Validates authentication and posture information
    - Passes decision back to Policy Enforcement Point

InteropLabs Network Access Control Architecture Alphabet Soup

What is it?	TCG TNC	Microsoft NAP	Cisco NAC
Posture 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?'	Integrity Measurement Collector	System Health Agent	Posture Plug-in Applications
Client Broker "Middleware" that runs on the client and talks to the Posture Collectors, collecting their data, and passing it down to Network Access Requestor	TNC Client	NAP Agent	Cisco Trust Agent
Network Access Requestor Software that connects the client to network. Examples might be 802.1X supplicant or IPSec VPN client. Used to authenticate the user, but also as a conduit for Posture Collector data to make it to the other side	Network Access Requestor	NAP Enforcement Client	Cisco Trust Agent



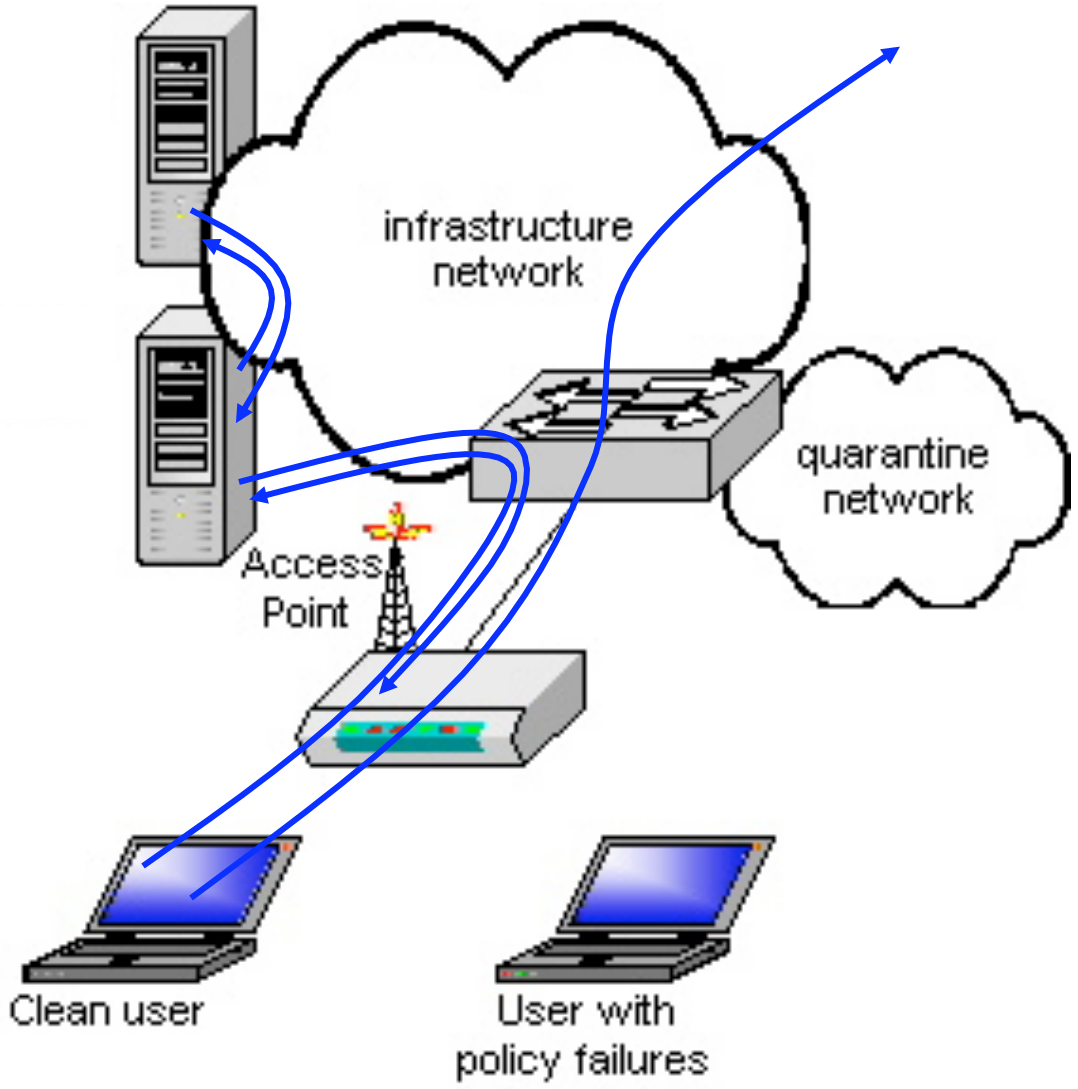
What is it?	TCG TNC	Microsoft NAP	Cisco NAC
Network Enforcement Point Component within the network that enforces policy, typically an 802.1X-capable switch or WLAN, VPN gateway, or firewall.	Policy Enforcement Point	NAP Enforcement Server	Network Access Device
Posture Validator Third-party software that receives status information from Posture Collectors on clients and validates the status information against stated network policy, returning a status to the TNC Server	Integrity Measurement Verifier	System Health Validator	Policy Vendor Server
Server Broker "Middleware" acting as an interface between multiple Posture Validators and the Network Access Authority	TNC Server	NAP Administration Server	Access Control Server
Network Access Authority A server responsible for validating authentication and posture information and passing policy information back to the Network Enforcement Point.	Network Access Authority	Network Policy Server	Access Control Server

IETF terms

2006Apr04

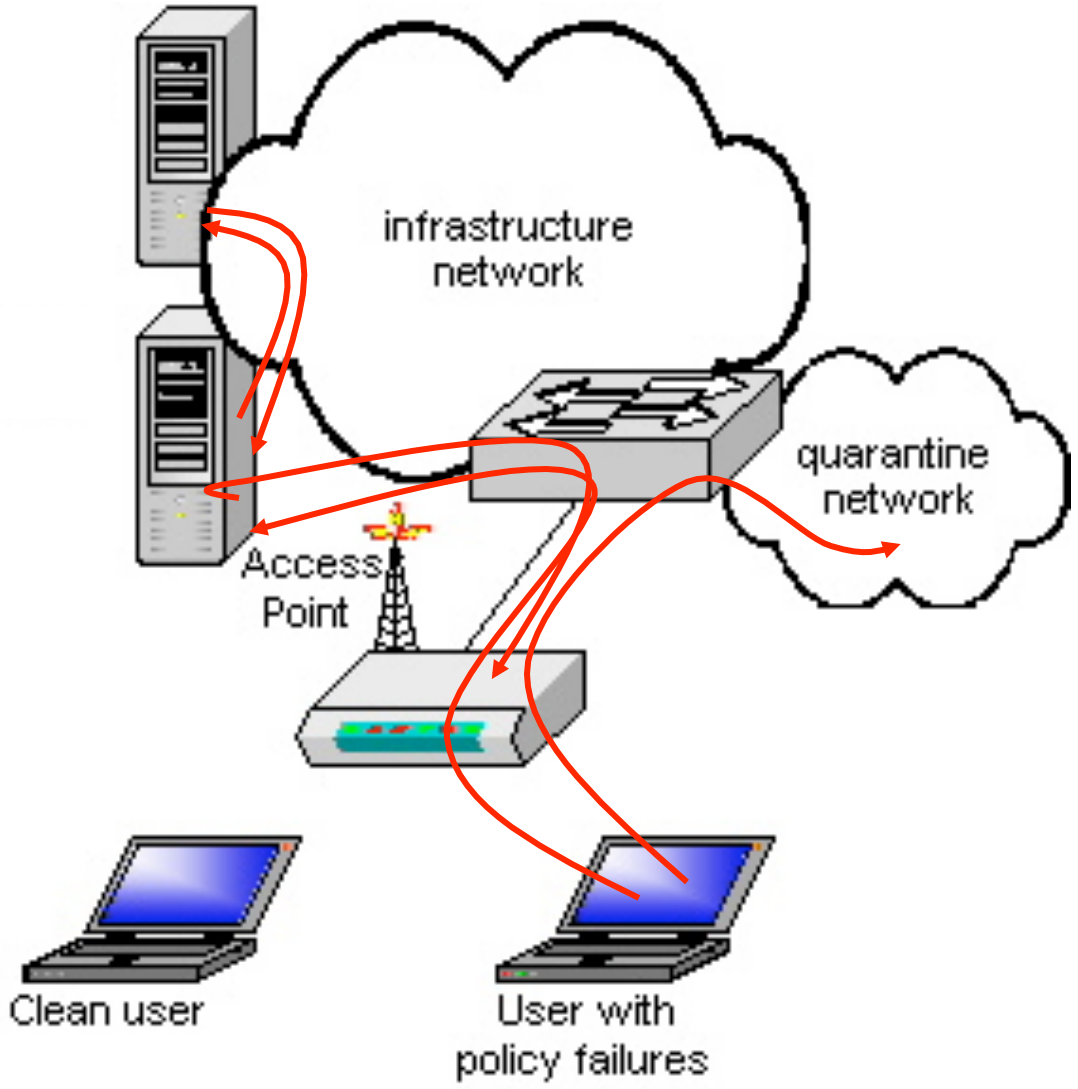
Example: Policy Enforcement

- Users who pass policy check are placed on production network
- Users who fail are quarantined



Example: Policy Enforcement

- Users who pass policy check are placed on production network
- Users who fail are quarantined



NAC Solutions

- There are three prominent solutions:
  - Cisco's Network Admission Control (CNAC)
  - Microsoft's Network Access Protection (NAP)
  - Trusted Computer Group's Trusted Network Connect (TNC)
- There are several proprietary approaches that we did not address

Cisco NAC
Network Admission Control

- Strengths
  - Many posture collectors for client
  - Installed base of network devices
- Limitations
  - More options with Cisco hardware
  - Not an open standard
  - Requires additional supplicant
- Status
  - Product shipping today

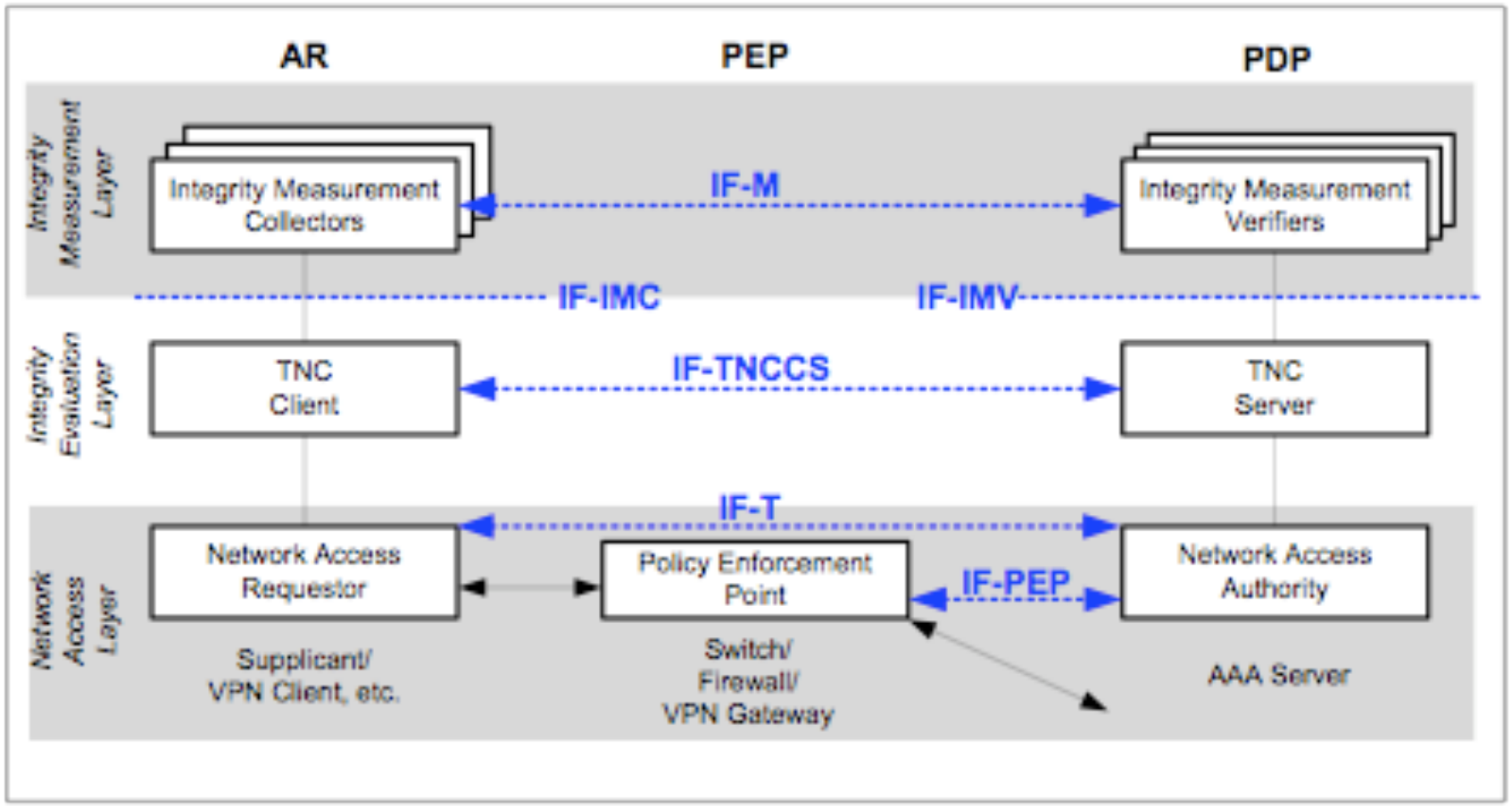
Microsoft NAP
Network Access Protection

- Strengths
  - Part of Windows operating system
  - Supports auto remediation
  - Network device neutral
- Limitations
  - Part of Windows operating system
  - Not an open standard
- Status
  - Client (Vista) shipping today; will be in XP SP3
  - Linux client available
  - Server (Longhorn) still in beta; 3rd parties shipping
    - Expect Longhorn (Windows Server 2008) release in 2007??

Trusted Computing Group (TCG) Trusted Network Connect (TNC)

- Strengths
  - Open standards based
  - Not tied to specific hardware, servers, or client operating systems
  - Multiple vendor backing - Juniper, Microsoft
- Limitations
  - Potential integration risk with multiple parties
- Status
  - Products shipping today
  - Tightly integrated with Microsoft NAP but products not shipping yet (Monday announcement)
  - Updated specifications released May 2007

TNC Architecture



Source: TCG

Current State of Affairs

- Multiple semi-interoperable solutions
  - Cisco NAC, Microsoft NAP, TCG TNC
  - Conceptually, all 3 are very similar
  - All with limitations
- Industry efforts at convergence and standardization
  - TCG
  - IETF

Getting Started - What's Most Important to You?

User Authentication

End Point Security

Enforcement Granularity

Where will NAC apply?

VPN WLAN Guests Desktops Computer Room Everywhere

Where Can You Learn More?

- Visit the Interop Labs Booth (#122)
  - Live Demonstrations of all three major NAC architectures *with engineers to answer questions*

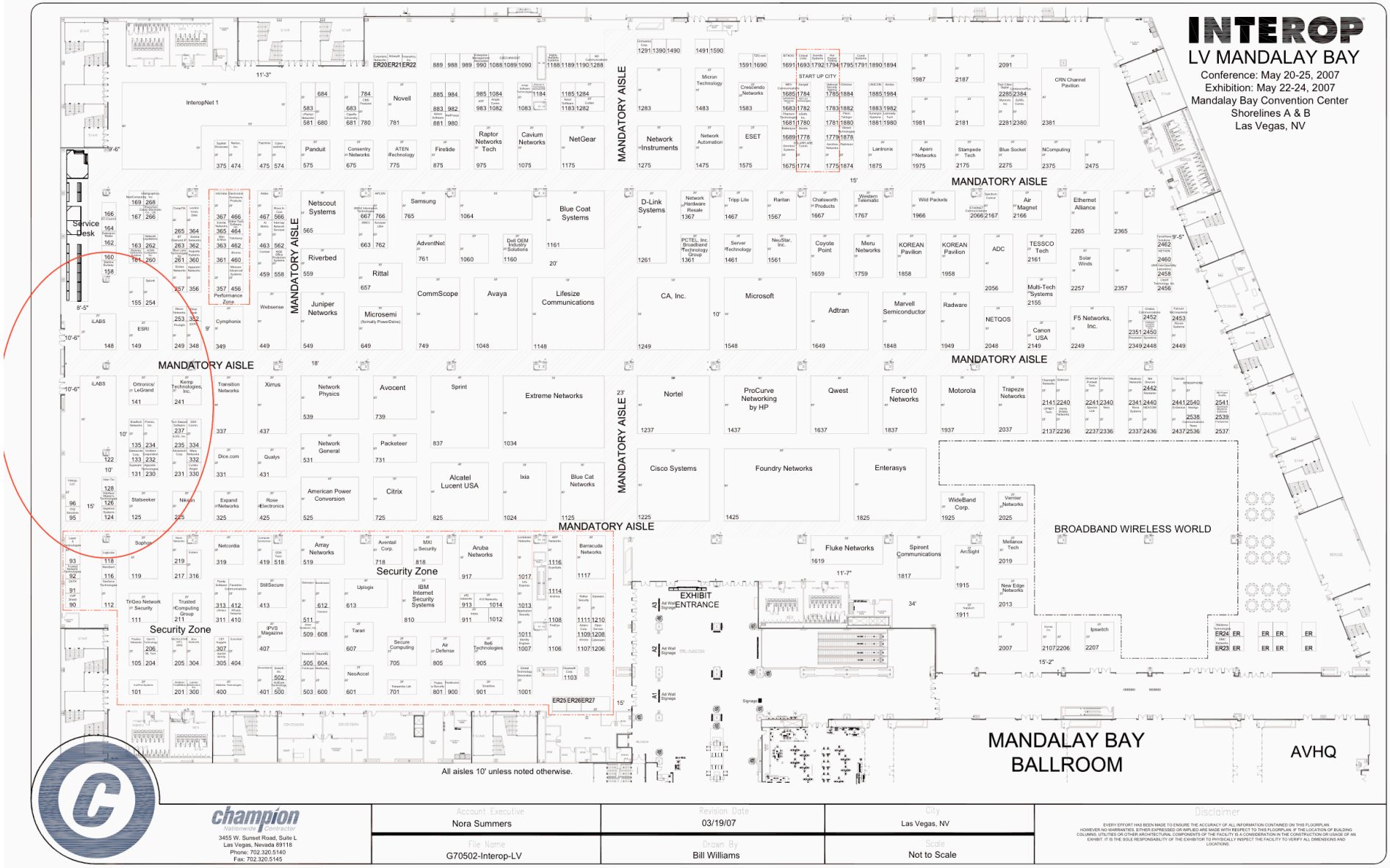
- Visit Interop Labs online:

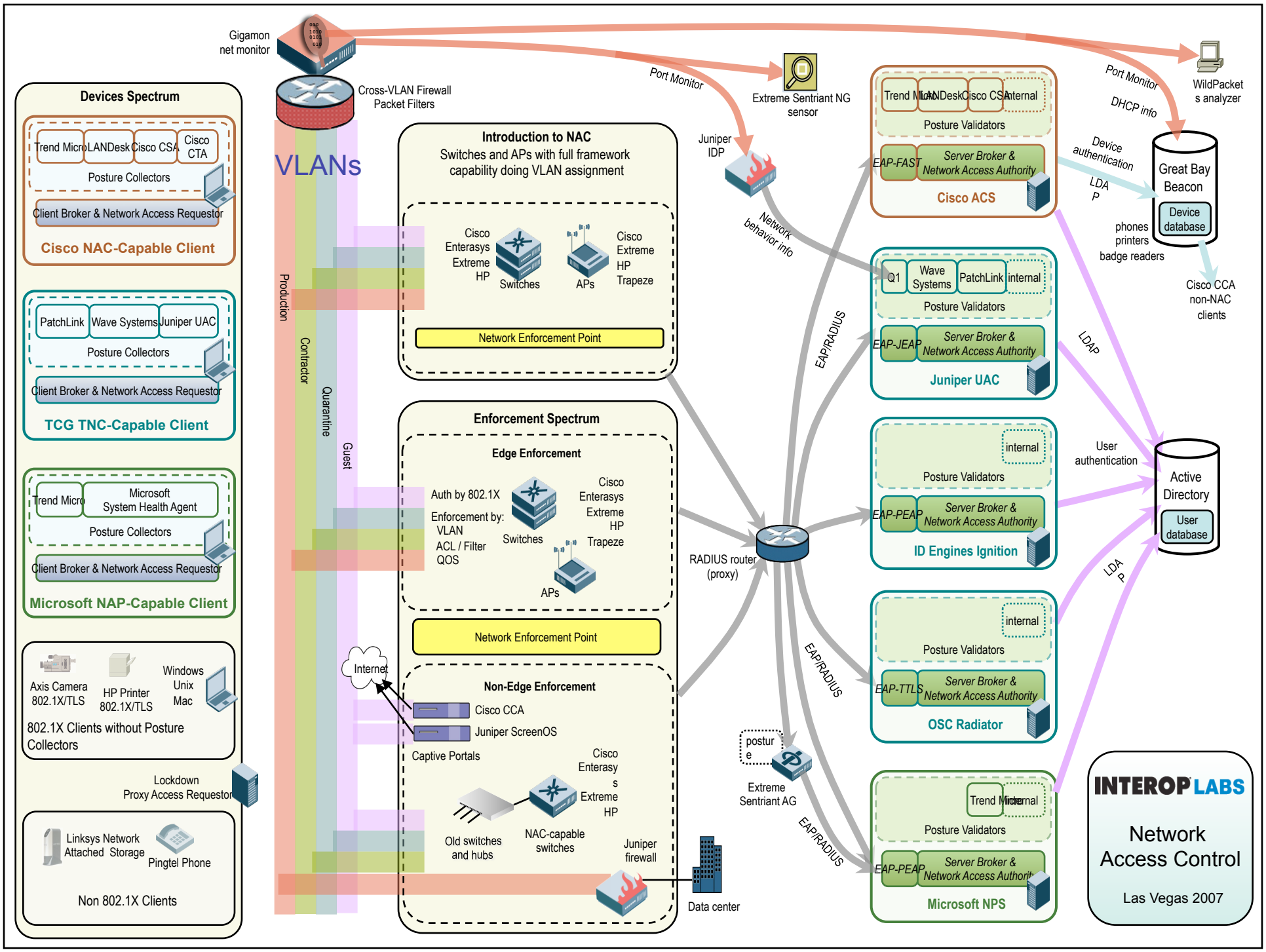
  Interop Labs white papers, this presentation, and demonstration layout diagram

  Network Access Control
  http://www.opus1.com/nac

  VOIP: Wireless & Security
  http://www.opus1.com/voip

INTEROP LABS


INTEROP
LV MANDALAY BAY
Conference: May 20-25, 2007
Exhibition: May 22-24, 2007
Mandalay Bay Convention Center
Shorelines A & B
Las Vegas, NV
MANDATORY AISLE
Service Desk
Security Zone
EXHIBIT ENTRANCE
BROADBAND WIRELESS WORLD
MANDALAY BAY BALLROOM
AVHQ
All aisles 10' unless noted otherwise.
champion
Nationwide Contractor
3455 W. Sunset Road, Suite L
Las Vegas, Nevada 89118
Phone: 702.320.5140
Fax: 702.320.5145
Account Executive
Nora Summers
Revision Date
03/19/07
City
Las Vegas, NV
File Name
G70502-Interop-LV
Drawn By
Bill Williams
Scale
Not to Scale
Disclaimer


Gigamon net monitor
Cross-VLAN Firewall Packet Filters
Port Monitor
Extreme Sentriant NG sensor
Port Monitor
DHCP info
WildPackets analyzer
Devices Spectrum
Trend Micro
LANDesk
Cisco CSA
Cisco CTA
Posture Collectors
Client Broker & Network Access Requestor
Cisco NAC-Capable Client
PatchLink
Wave Systems
Juniper UAC
Posture Collectors
Client Broker & Network Access Requestor
TCG TNC-Capable Client
Trend Micro
Microsoft System Health Agent
Posture Collectors
Client Broker & Network Access Requestor
Microsoft NAP-Capable Client
Axis Camera 802.1X/TLS
HP Printer 802.1X/TLS
Windows Unix Mac
802.1X Clients without Posture Collectors
Lockdown Proxy Access Requestor
Linksys Network Attached Storage
Pingtel Phone
Non 802.1X Clients
VLANs
Production
Contractor
Quarantine
Guest
Introduction to NAC
Switches and APs with full framework capability doing VLAN assignment
Cisco Enterasys Extreme HP
Switches
APs
Cisco Extreme HP Trapeze
Network Enforcement Point
Enforcement Spectrum
Edge Enforcement
Auth by 802.1X
Enforcement by:
VLAN
ACL / Filter
QOS
Switches
APs
Cisco Enterasys Extreme HP Trapeze
Network Enforcement Point
Internet
Non-Edge Enforcement
Cisco CCA
Juniper ScreenOS
Captive Portals
Old switches and hubs
NAC-capable switches
Cisco Enterasys Extreme HP
Juniper firewall
Data center
Juniper IDP
Network behavior info
RADIUS router (proxy)
EAP/RADIUS
EAP/RADIUS
EAP/RADIUS
EAP/RADIUS
Extreme Sentriant AG
Trend Micro
LANDesk
Cisco CSA
Internal
Posture Validators
EAP-FAST
Server Broker & Network Access Authority
Cisco ACS
Device authentication
LDAP
Great Bay Beacon
Device database
phones printers badge readers
Cisco CCA non-NAC clients
Q1
Wave Systems
PatchLink
internal
Posture Validators
EAP-JEAP
Server Broker & Network Access Authority
Juniper UAC
LDAP
internal
Posture Validators
EAP-PEAP
Server Broker & Network Access Authority
ID Engines Ignition
User authentication
Active Directory
User database
LDAP
internal
Posture Validators
EAP-TTLS
Server Broker & Network Access Authority
OSC Radiator
Trend Micro
internal
Posture Validators
EAP-PEAP
Server Broker & Network Access Authority
Microsoft NPS
INTEROP LABS
Network Access Control
Las Vegas 2007

Where can you learn more?

White Papers available in the Interop Labs:

What is Network Admission Control?
What is 802.1X?
Getting Started with Network Admission Control
What is the TCG's Trusted Network Connect?
What is Microsoft Network Access Protection?
What is Cisco Network Admission Control?
What is the IETF's Network Endpoint Assessment?
Switch Functionality for 802.1X-based NAC
Exception Cases and NAC
Get the "NAC" of Troubleshooting
NAC Resources

INTEROP LABS

Free USB key to the first 600 attendees!

(has all NAC and VOIP materials)

http://www.opus1.com/nac

NAC Lab Participants

INTEROP LABS

InteropLabs NAC Team Members

Karen O'Donoghue, US Navy, Team Lead	Kevin Koster, Cloudpath Networks
Bill Clary, grandmotherboard.org	Jeff Fulsom, Univ of Utah
Joel Snyder, Opus One	Mike McCauley, Open Systems Consultants
Jan Trumbo, Opus One	Henry He, UNH IOL
Chris Hessing, Identify Engines	Lynn Haney, TippingPoint
Terry Simons, Identity Engines	

InteropLabs NAC Vendor Engineers

Thomas Howard, Cisco Systems, Inc.
Mark Townsend, Enterasys
Mike Skripek, Extreme Networks
Charles Owens, Great Bay Software
Eric Holton, HP Procurve
Bret Jordan, Identify Engines
Bob Filer, Juniper Networks
Chrisitan McDonald, Juniper Networks
Denzil Wessels, Juniper Networks
Steve Hanna, Juniper Networks
Oliver Chung, Lockdown Networks
Pat Fetty, Microsoft
Don Gonzales, Patchlink
Scott VanWart, Q1 Labs
Tim McCarthy, Trapeze Networks
Ryan Holland, Trend Micro
Alwin Yu, Trend Micro
Amit Deshpande, Wave Systems

http://www.opus1.com/nac

Thank You!

Questions?

Interop Labs -- Booth 122
http://www.opus1.com/nac