InteropLabs
Network Access Control

Interop Las Vegas 2008

Robert Nagy
Accuvant Inc
Principal Security Consultant
rnagy@accuvant.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 151!

Technical contributions to this presentation include:

Kevin Koster, Cloudpath Networks, Inc.

Karen O'Donoghue, Jan Trumbo, 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 evolution of the current NAC 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 one vendor's solution.
  - Delve into the underlying protocol details

Why Network Access Control?

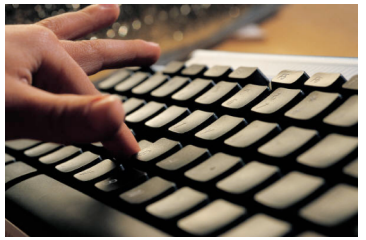
- Desire to grant different network access to different users, e.g. employees, guests, contractors
- Network endpoints can be threats
  - Enormous enterprise resources are wasted to combat an increasing numbers of viruses, worms, and spyware
- Proliferation of devices requiring network connectivity
  - 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

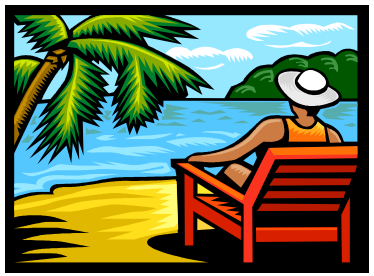
User Identity

+

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", ACL = phone-only

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

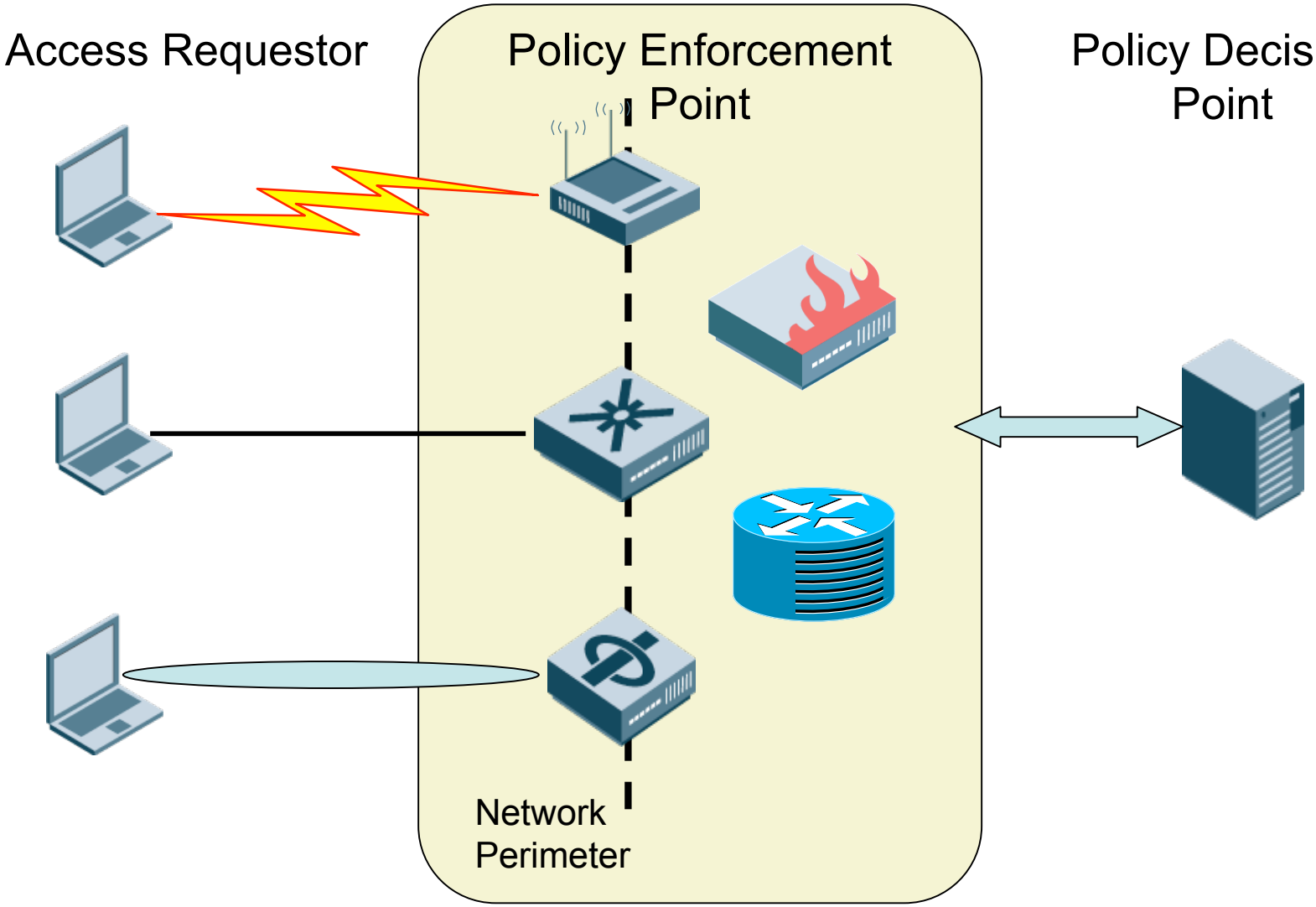
- Additional access possibilities:
  - Access Control Lists
    - Switches
    - Routers
  - Firewall rules
  - Traffic shaping (QoS)
- Non-edge enforcement options
  - Such as a distant firewall

NAC is More Than Sniffing Clients for Viruses

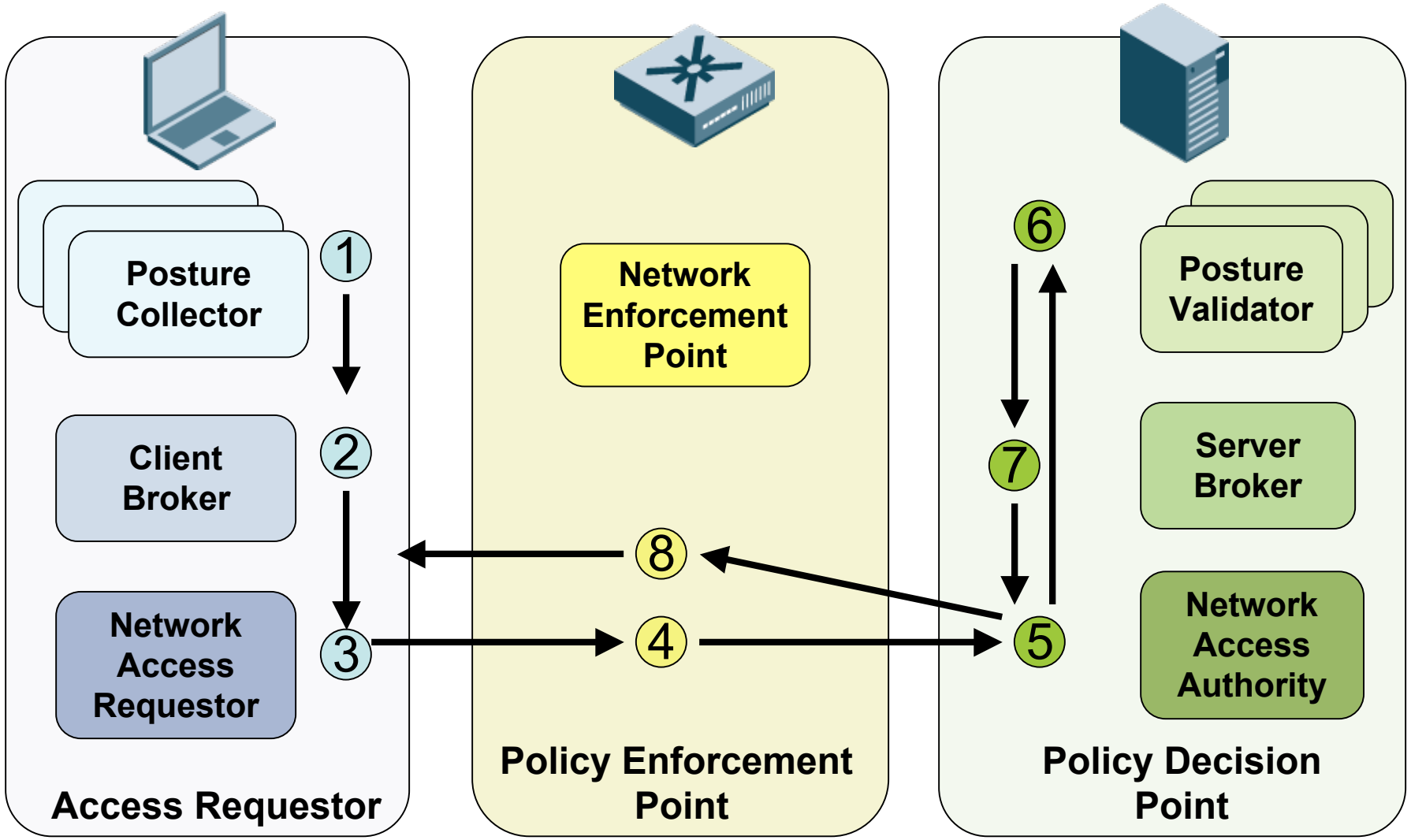
- Behavior-based assessment
  - Why is this printer trying to connect to ssh ports?
- VPN-connected endpoints cannot access HR database

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

Generic NAC Components

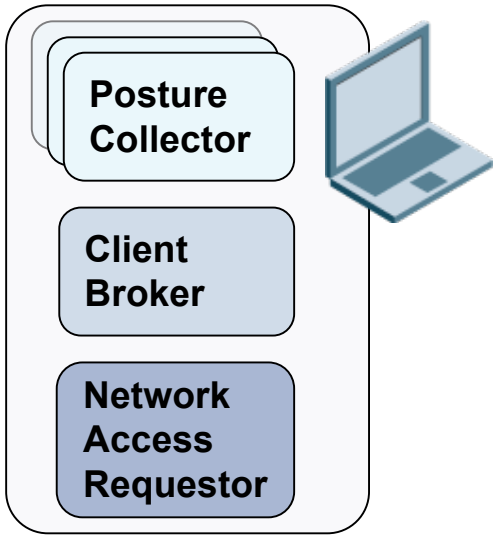


Sample NAC Transaction



Access Requestors

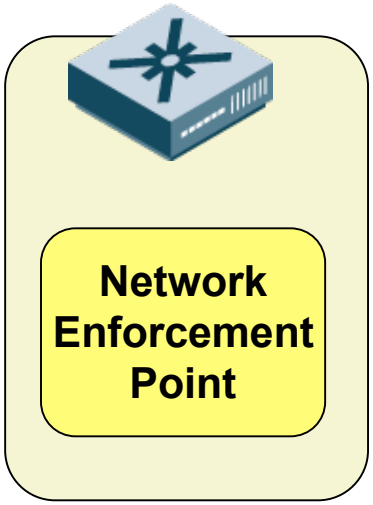
- Sample Access Requestors
  - Laptops
  - PDAs
  - VoIP phones
  - Desktops
  - Printers



Access Requestor

- 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

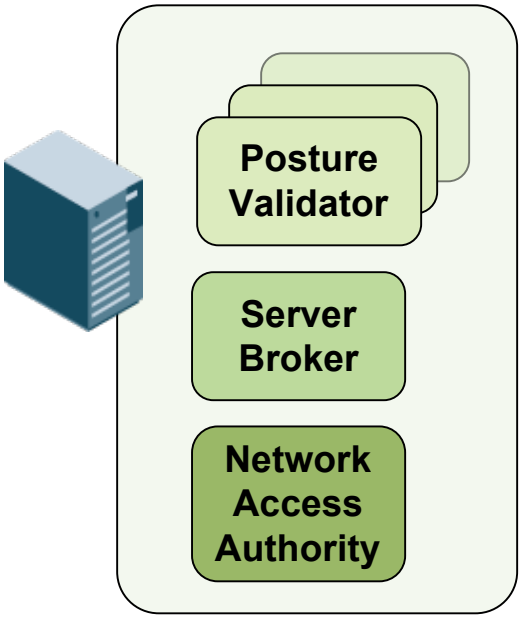
Policy Enforcement Points



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

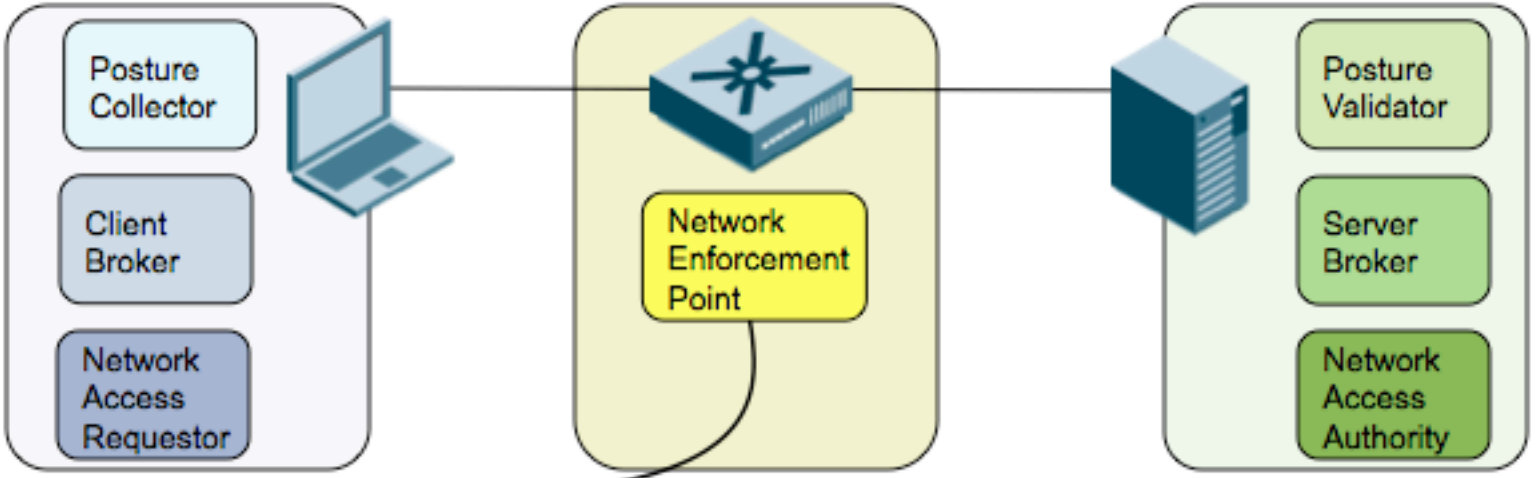


Policy Decision Point

- 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

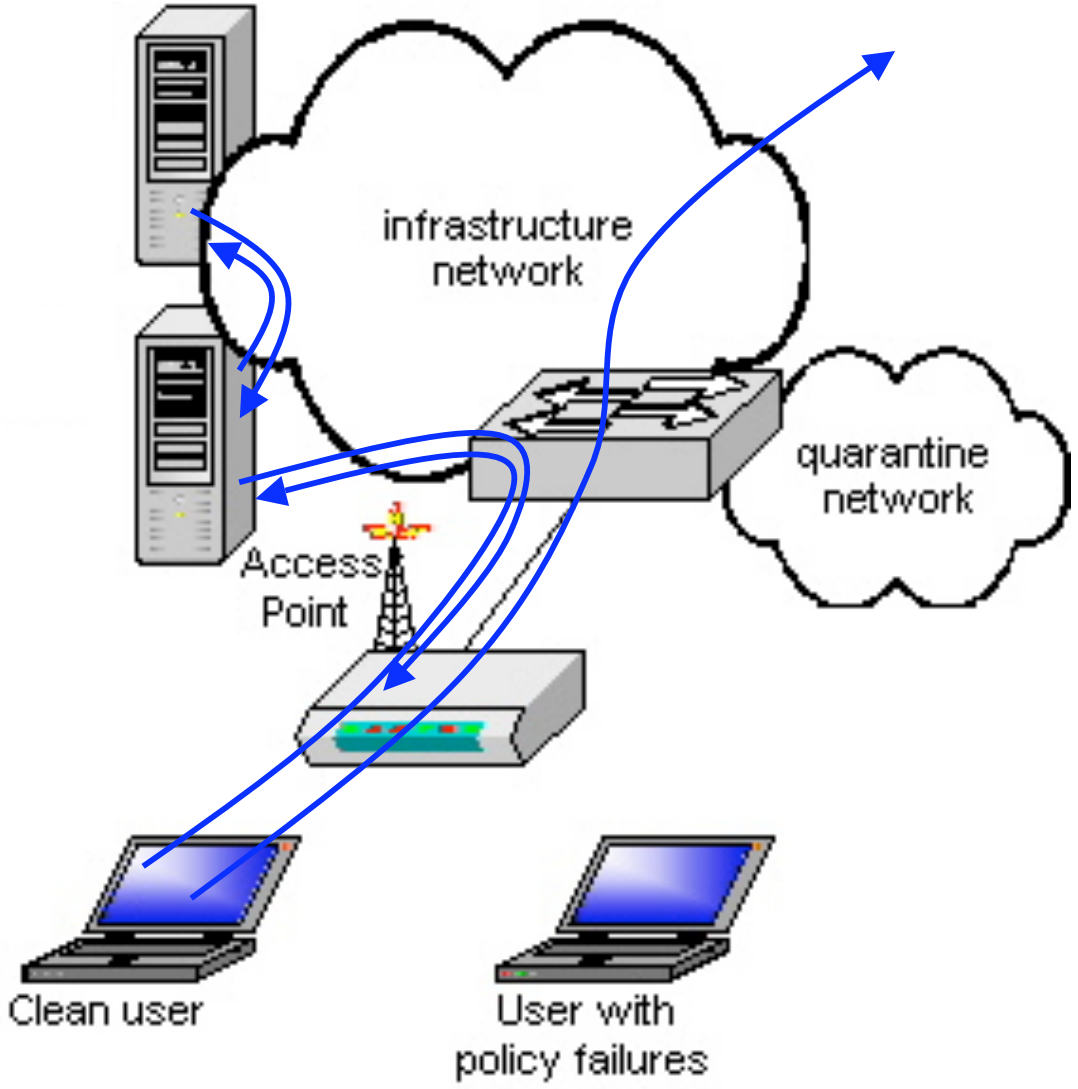
What is it?	TCG TNC	Microsoft NAP	IETF NEA
Posture Collector Third-party software that runs on the client and collects information on security status and applications, such as 'is A/V enabled and up-to-date?"	Integrity Measurement Collector	System Health Agent	Posture Collector
Client Broker "Middleware" that runs on the client and talks to the Posture Collectors, collecting their data, and passing it down to Network Access Requestor. In product form, this is generally bundled with the Network Access Requestor.	TNC Client	NAP Agent	Posture Broker Client
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	Posture Transport Client



What is it?	TCG TNC	Microsoft NAP	IETF NEA
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	Intermediary Devices
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 Server Broker.	Integrity Measurement Verifier	System Health Validator	Posture Validator
Server Broker "Middleware" acting as an interface between multiple Posture Validators and the Network Access Authority.	TNC Server	NAP Administration Server	Posture Broker 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	Posture Transport Server

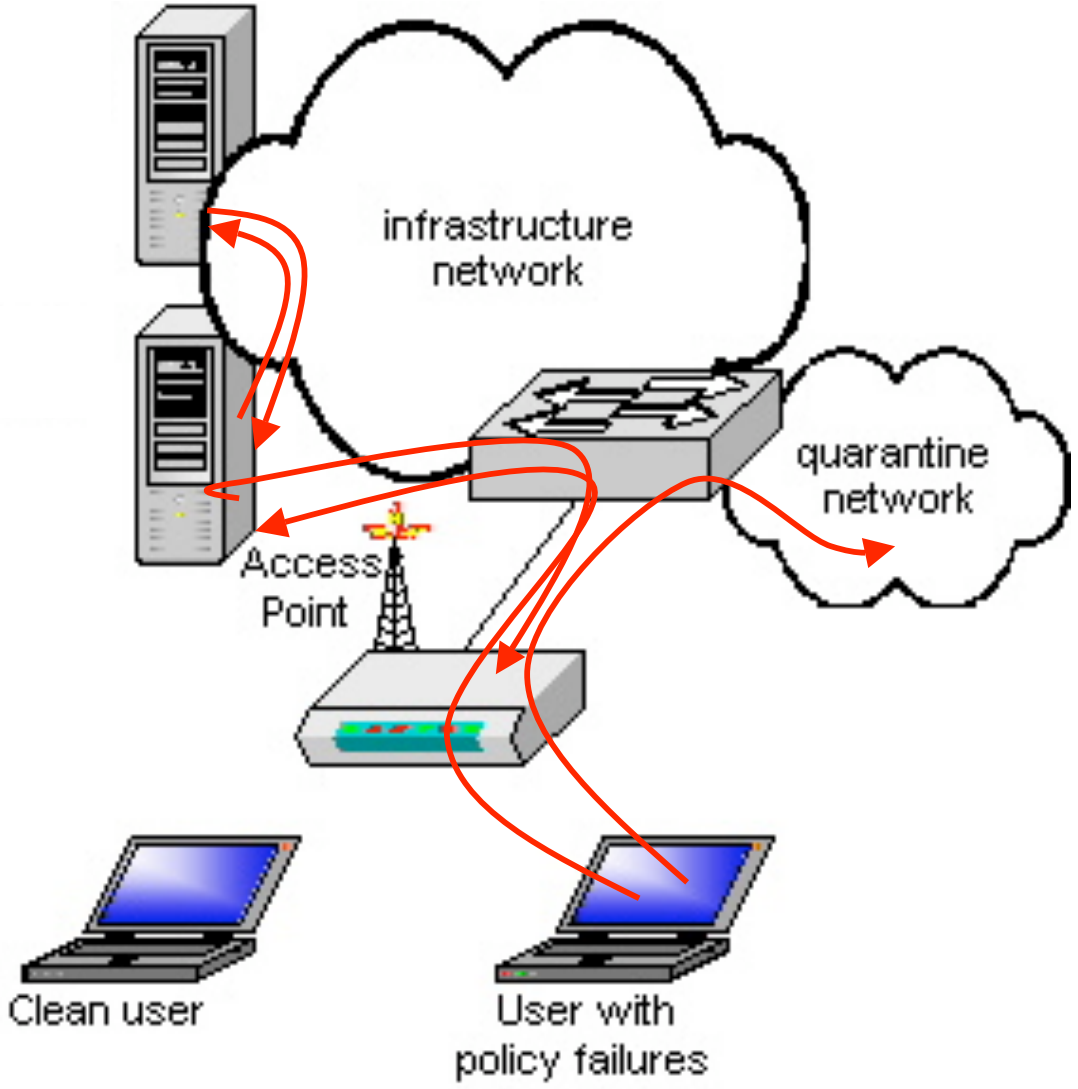
Example: Policy Enforcement

- 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 - Last Years Slide

- 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

NAC Solutions - This Years Slide

- Moving towards industry convergence:
  - NAP and TCG(TNC) are moving ever closer
  - Cisco renewed focus on interoperability with NAP
  - Cisco consolidating their NAC appliance solution
- There are several proprietary approaches that we did not address
- All 3 major players are moving ever closer
- This ultimately benefits you the implementer!
- Still a way to go until nirvana :-)

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 (Windows Server 2008)

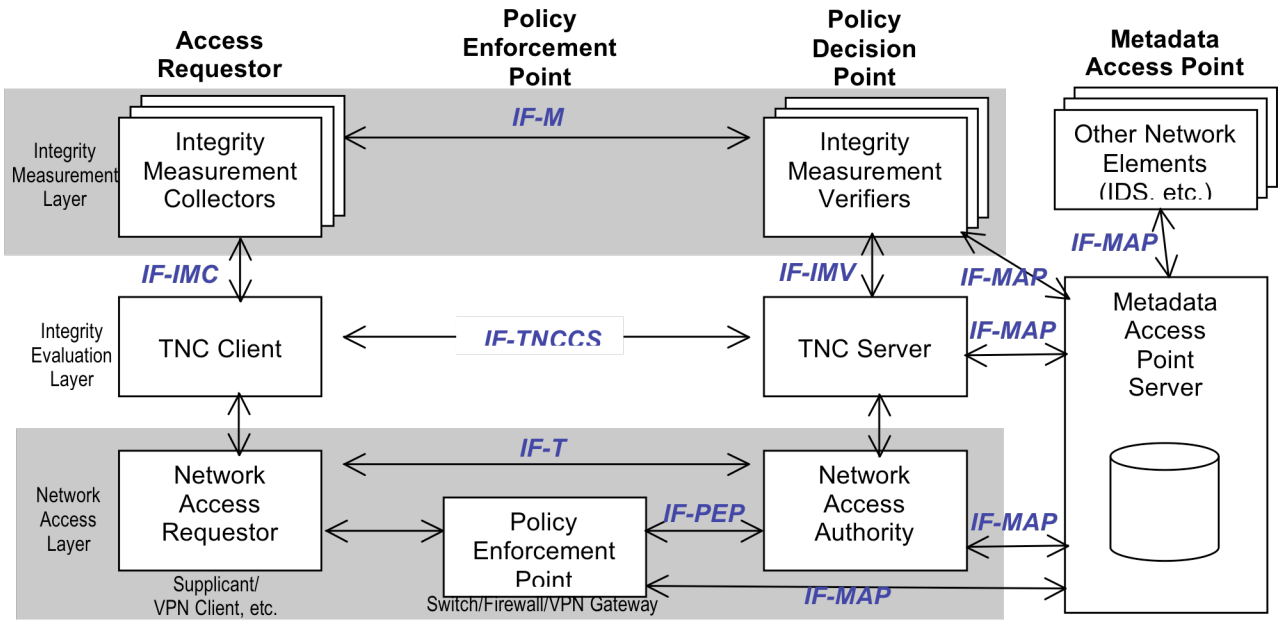
Cisco NAC Network Admission Control

- Strengths
  - Many posture collectors for client for NAC solution
  - NAC integration with Microsoft NAP
  - Large and diverse installed base of network and security/NAC devices
- Limitations
  - More options with Cisco hardware which may make planning harder
  - Not an open standard
  - Requires additional supplicant with NAC solution
- Status
  - Products shipping today
  - Cool stuff is coming which I expect to be announced soon…

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

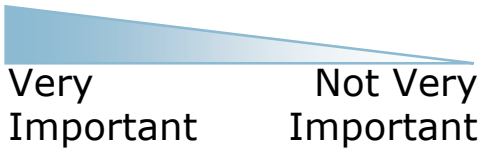
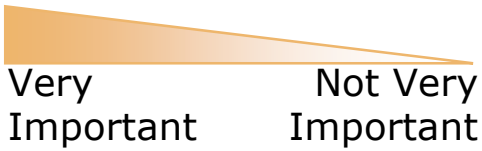
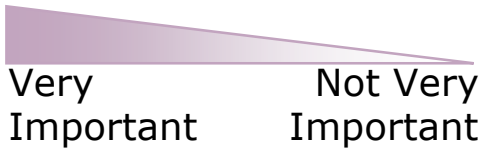
- Strengths
  - Open standards based
  - Not tied to specific hardware, servers, or client operating systems
  - Multiple vendor backing - Juniper, Microsoft
- Limitations
  - Potential integration risk with multiple parties
- Status
  - Products shipping today
  - Common ground with Microsoft NAP continues to move towards interoperability
  - Updated specifications released May 2007

TNC Architecture



Source: TCG

Getting Started - What's Most Important to You?

User Authentication	End Point Security	Enforcement Granularity
		
Very Important — Not Very Important	Very Important — Not Very Important	Very Important — Not Very Important

Where will NAC apply?

VPN WLAN Guests Desktops Computer Room Everywhere

Where Can You Learn More?

- Visit the Interop Labs Booth (#151)
  - Live Demonstrations of many multi-vendor NAC architectures *with engineers to answer questions*

- Visit Interop Labs online:

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

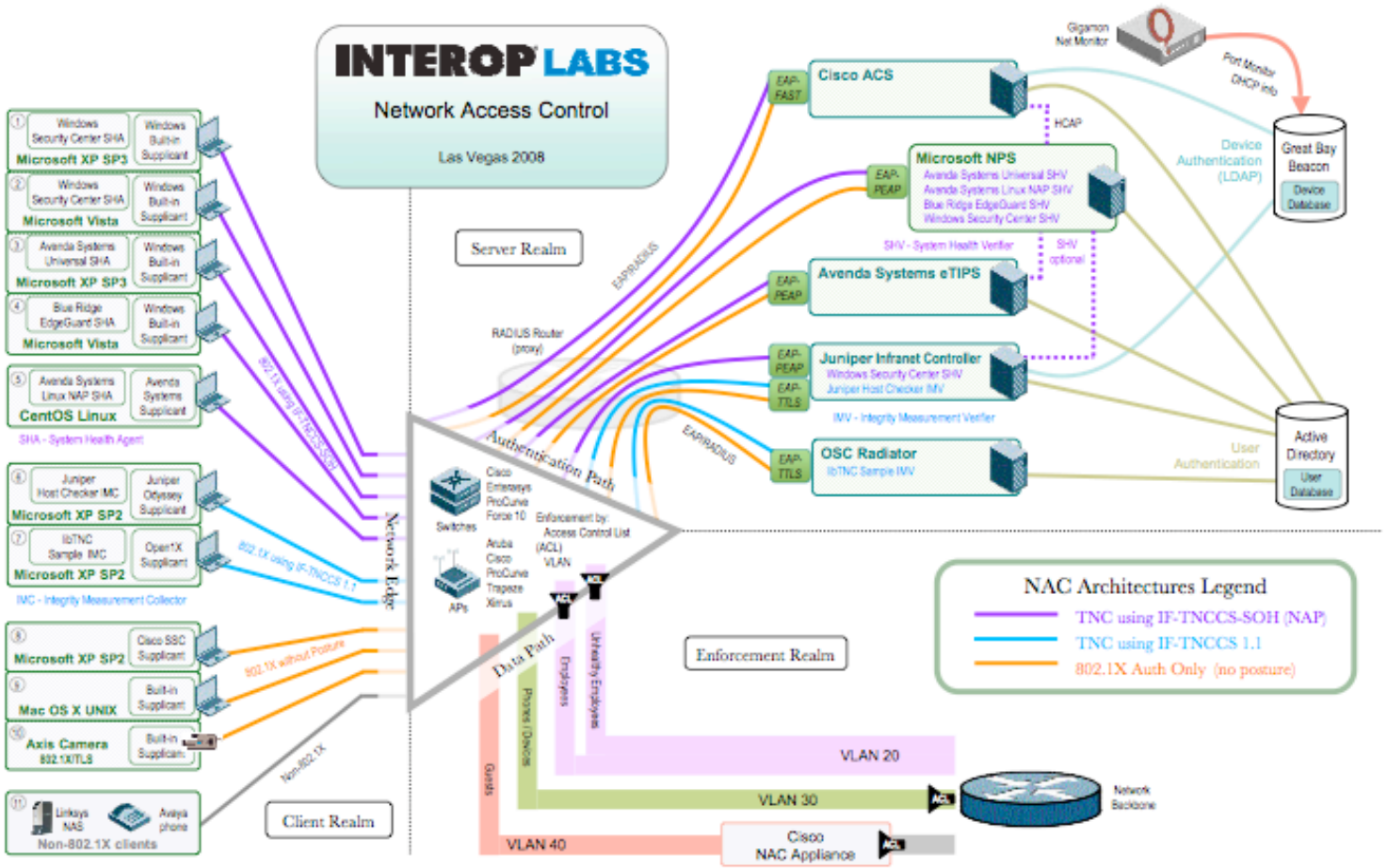
  Network Access Control

  http://www.opus1.com/nac

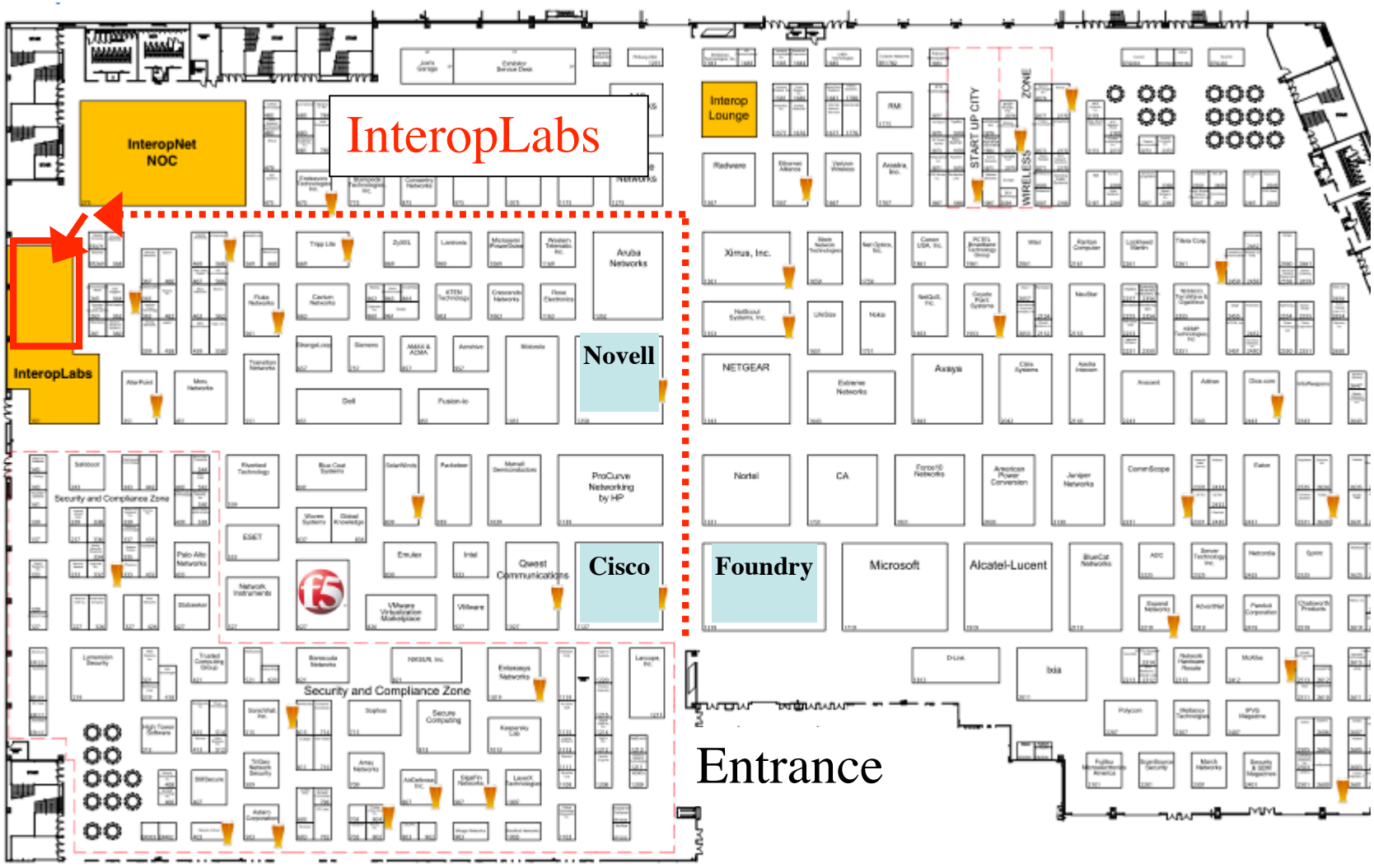
  Unified Communications

  http://www.opus1.com/uc

INTEROP LABS


INTEROP LABS
Network Access Control
Las Vegas 2008
Server Realm
Client Realm
Enforcement Realm
Network Edge
Authentication Path
Data Path
RADIUS Router (proxy)
EAP/RADIUS
Cisco ACS
EAP-FAST
HCAP
Microsoft NPS
Avenda Systems Universal SHV
Avenda Systems Linux NAP SHV
Blue Ridge EdgeGuard SHV
Windows Security Center SHV
EAP-PEAP
SHV - System Health Verifier
SHV optional
Avenda Systems eTIPS
Juniper Infranet Controller
Windows Security Center SHV
Juniper Host Checker IMV
EAP-TTLS
IMV - Integrity Measurement Verifier
OSC Radiator
libTNC Sample IMV
Gigamon Net Monitor
Port Monitor DHCP info
Device Authentication (LDAP)
Great Bay Beacon
Device Database
User Authentication
Active Directory
User Database
Microsoft XP SP3
Windows Security Center SHA
Windows Built-in Supplicant
Microsoft Vista
Avenda Systems Universal SHA
Blue Ridge EdgeGuard SHA
CentOS Linux
Avenda Systems Linux NAP SHA
Avenda Systems Supplicant
SHA - System Health Agent
Microsoft XP SP2
Juniper Host Checker IMC
Juniper Odyssey Supplicant
libTNC Sample IMC
OpenIX Supplicant
IMC - Integrity Measurement Collector
802.1X using IF-TNCCS-SOH
802.1X using IF-TNCCS 1.1
802.1X without Posture
Non-802.1X
Cisco SSC Supplicant
Mac OS X UNIX
Built-in Supplicant
Axis Camera
802.1X/TLS
Linksys NAS
Avaya phone
Non-802.1X clients
Switches
Cisco Enterasys ProCurve Force 10
APs
Aruba Cisco ProCurve Trapeze Xirrus
Enforcement by: Access Control List (ACL) VLAN
Guests
Private Devices
Employees
Unhealthy Employees
VLAN 20
VLAN 30
VLAN 40
Network Backbone
Cisco NAC Appliance
NAC Architectures Legend
TNC using IF-TNCCS-SOH (NAP)
TNC using IF-TNCCS 1.1
802.1X Auth Only (no posture)

Visit the InteropLabs



INTEROP

See This Presentation Again!

Tuesday 4/29/08	Wednesday 4/30/08	Thursday 5/1/08
		InteropLabs: UC Class 10:00am - 10:45am
InteropLabs: NAC Class 11:15am - 12:00pm	InteropLabs: NAC Class 11:15am - 12:00pm	InteropLabs: NAC Class 11:00am - 11:45pm
InteropLabs: UC Class 12:15pm - 1:00pm	InteropLabs: UC Class 12:15pm - 1:00pm	

Where can you learn even 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?
Merger of TNC and NAP
What is the IETF's Network Endpoint Assessment?
Switch Functionality for 802.1X-based NAC
Handling NAC Exception Cases
NAC Resources
VLANs vs ACLs

INTEROP LABS

Free USB key to the first 600 attendees!

(has all NAC and Unified Communications materials)

http://www.opus1.com/nac

NAC Lab Participants

INTEROP LABS

InteropLabs NAC Team Members

Kevin Koster, Cloudpath Networks, Team Lead	Jim Martin, Woven Systems
Rob Nagy, Accuvant Inc, NAC Instructor	Joel Snyder, Opus One
Craig Watkins, Transcend, Inc.	Karen O'Donoghue, NSWCDD
Gerard Goubert, Cisco Systems, Inc.	Lynn Haney, TippingPoint Technologies, Inc.
Jan Trumbo, Opus One	Mike McCauley, Open Systems Consultants

InteropLabs NAC Vendor Engineers

Asim Rasheed, Ixia
Barb Cline, Blue Ridge Networks, Inc.
Bhagya Prasad NR, Avenda Systems
Bob Durkee, Great Bay Software
Charles Owens, Great Bay Software
Ernie Brown, Xirrus Corp.
Faith Comlekoglu, Blue Ridge Networks, Inc.
Greg Hankins, Force10 Networks, Inc.
Ingo Bente, Fachhochschule Honnover
Jeff Reilly, Juniper Networks, Inc.
Josef von Helden, Fachhochschule Hannover
King Won, Gigamon Systems LLC
Mark Townsend, Enterasys Networks, Inc.
Myke Rydalch, Xirrus Corp.
Mike Steinmetz, Fachhochschule Hannover
Mitsunori Sagae, Cisco Systems, Inc.
Nathan Jenne, ProCurve Networking by HP
Pat Fetty, Microsoft Corporation
Pattabhi Attaluri, Avenda Systems
Prem Ananthakrishnan, Cisco Systems, Inc.
Rick Duchaney, Great Bay Software
Saurabh Pradhan, Trapeze Networks
Steve Pettit, Great Bay Software
Ted Fornoles, Trapeze Networks
Thenu Kittappa, Aruba Networks
Tom Maufer, Mu Security
Thomas Howard, Cisco Systems, Inc.
Tim McCarthy, Trapeze Networks
Tom Gilbert, Blue Ridge Networks

http://www.opus1.com/nac

Thank You!

Questions?

Interop Labs -- Booth 151
http://www.opus1.com/nac