Interop Labs
Network Access Control

Interop Las Vegas 2006

Karen O'Donoghue

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 2506!

Technical contributions to this presentation include:

- Steve Hanna, Juniper Networks and TCG TNC
- Kevin Koster, Cloudpath Networks, Inc.
- 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 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

Agenda

- Why NAC?
- What is a Policy?
- Generic NAC architecture
- What is emerging today?
- What are your first steps?
- Where can you learn more?

Why NAC?

- Proliferation of devices requiring network connectivity
  - Laptops, phones, PDAs
- Increasingly mobile workforce
  - Requiring roughly the same access regardless of where they are connecting from
- Mobile workforce is becoming infected
  - Enormous enterprise resources are wasted to combat an increasing numbers of viruses, worms, and spyware
- Logistical difficulties associated with keeping corporate assets monitored and updated

Policy Possibilities

- Who
  - 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

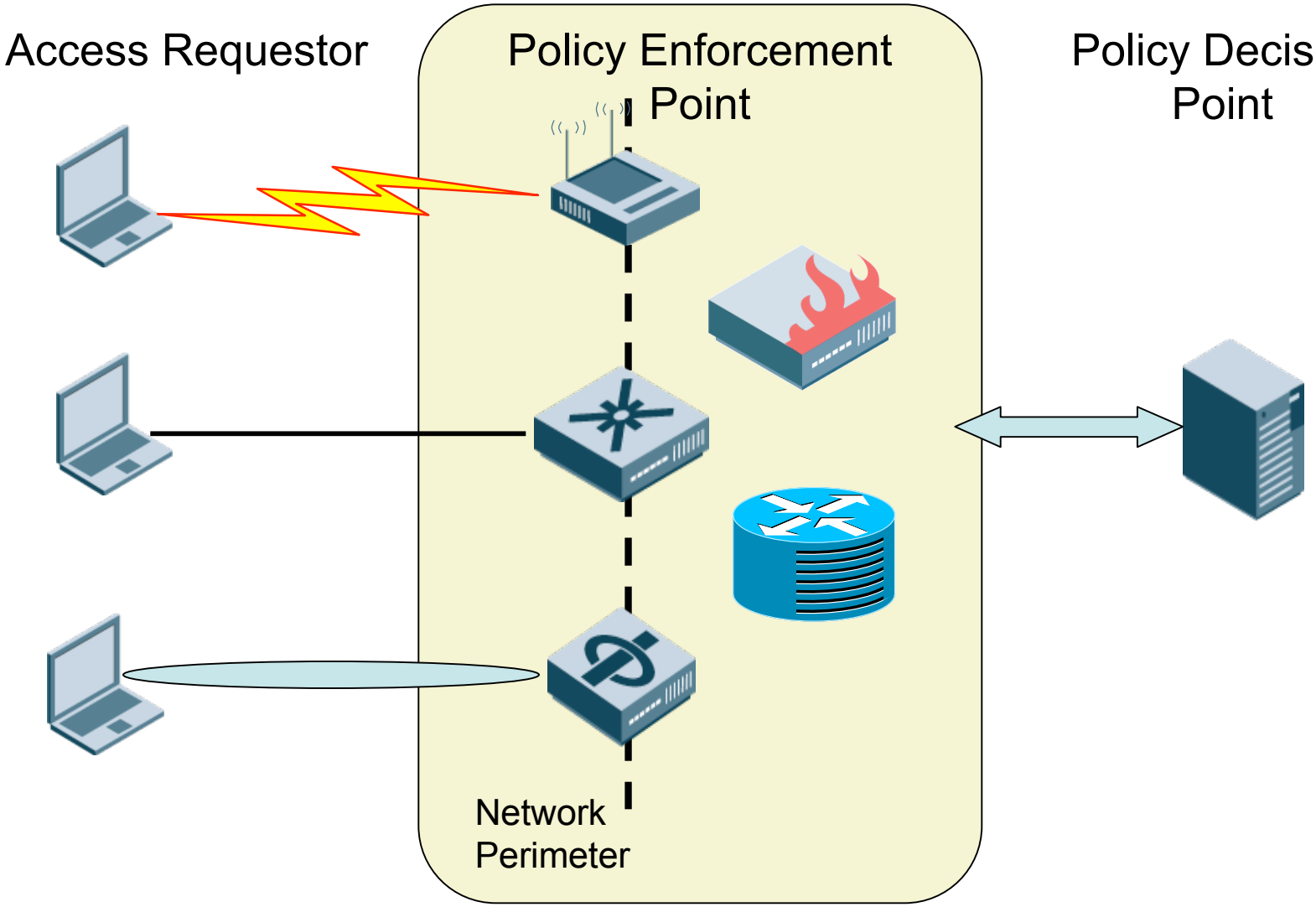
Is NAC only VLANS?

- NAC is not limited to dynamic VLAN configuration
- Additional access possibilities:
  - Access Control Lists
    - Switches
    - Routers
  - Firewall rules
  - Traffic shaping (QoS)
- Inline enforcement options

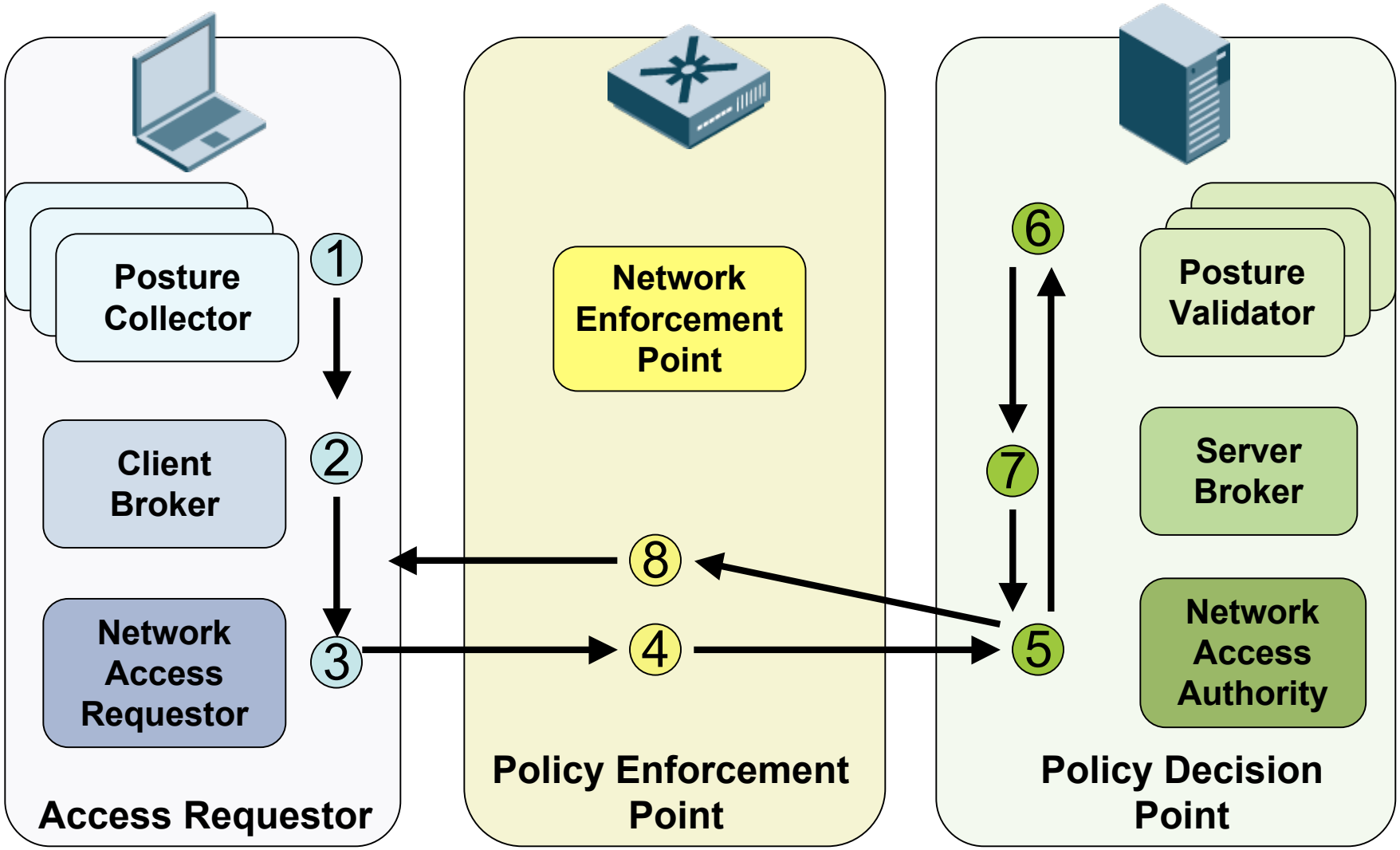
Agenda

- Why NAC?
- What is a Policy?
- Generic NAC architecture
- What is emerging today?
- What are your first steps?
- Where can you learn more?

Generic NAC Components

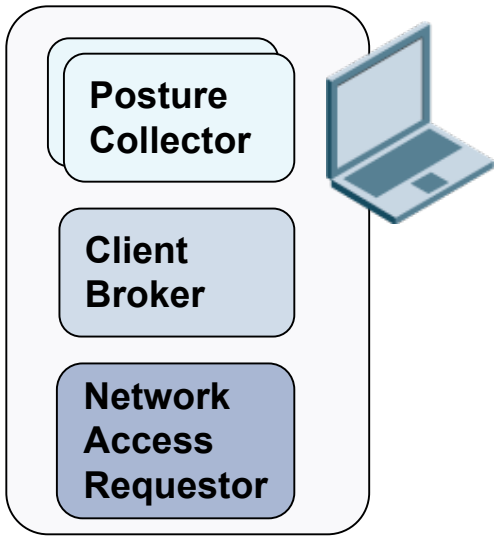


Sample NAC Transaction



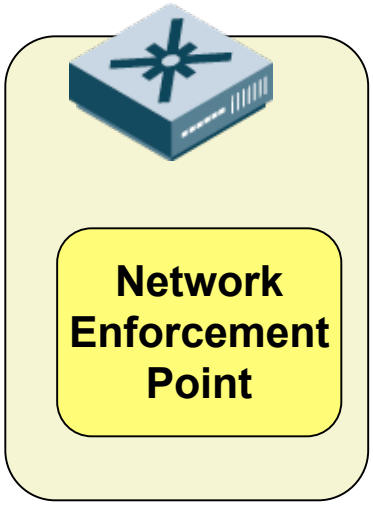
Access Requestors

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



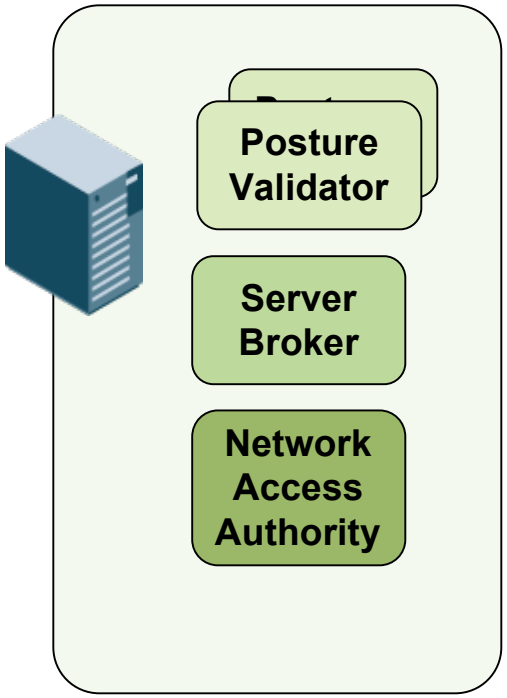
- Components of an Access Requestor/Endpoint
  - Posture Collector(s)
    - Collects security status information (e.g. A/V software installed and up to date, personal firewall turned on)
    - May be more than one per access requestor
  - Client Broker
    - Collects data from one or more posture collectors
    - 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



- 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

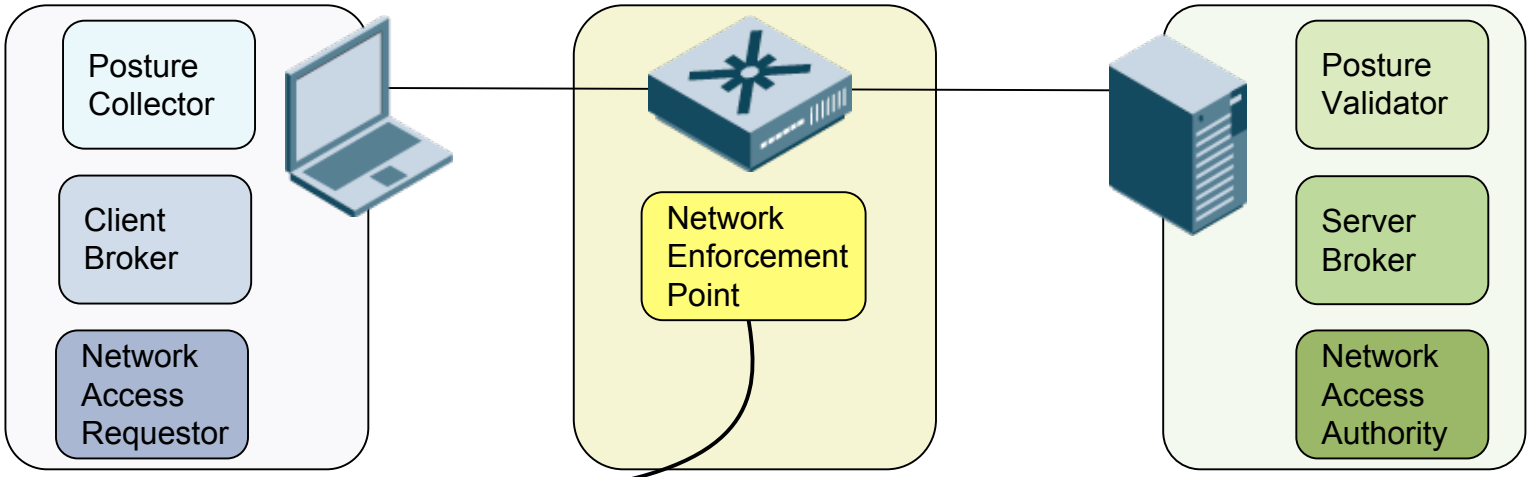
Policy Decision Point



- 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

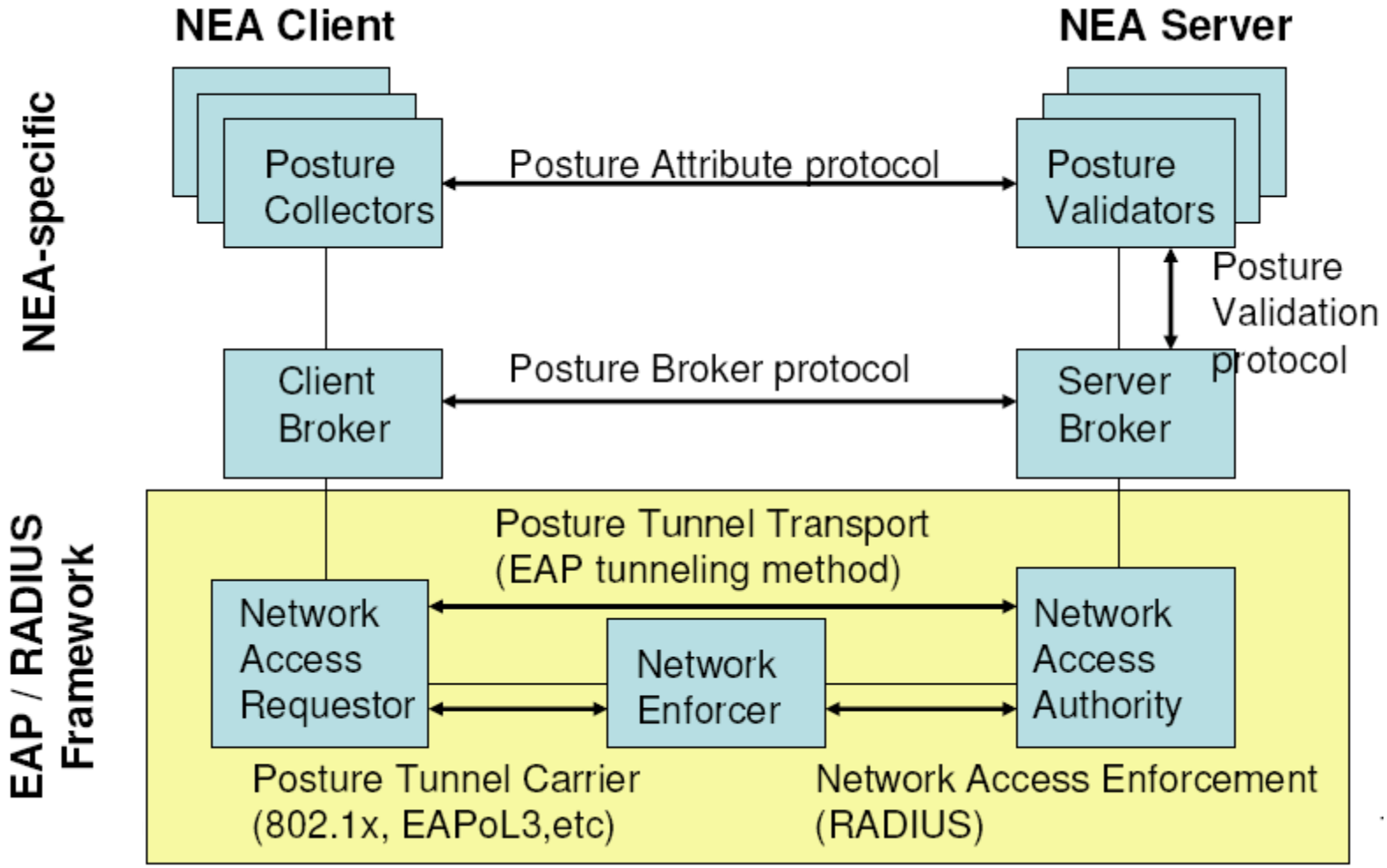


What is it?	TCG TNC	Microsoft NAP	Cisco NAC
Network Enforcement Point Component within the network that enforces policy, typically an 802.1X-capable switch or WLAN, VPN gateway, or firewall.	Policy Enforcement Point	NAP Enforcement Server	Network Access Device
Posture Validator Third-party software that 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

Generic Architecture



Source: NEA BOF at IETF65

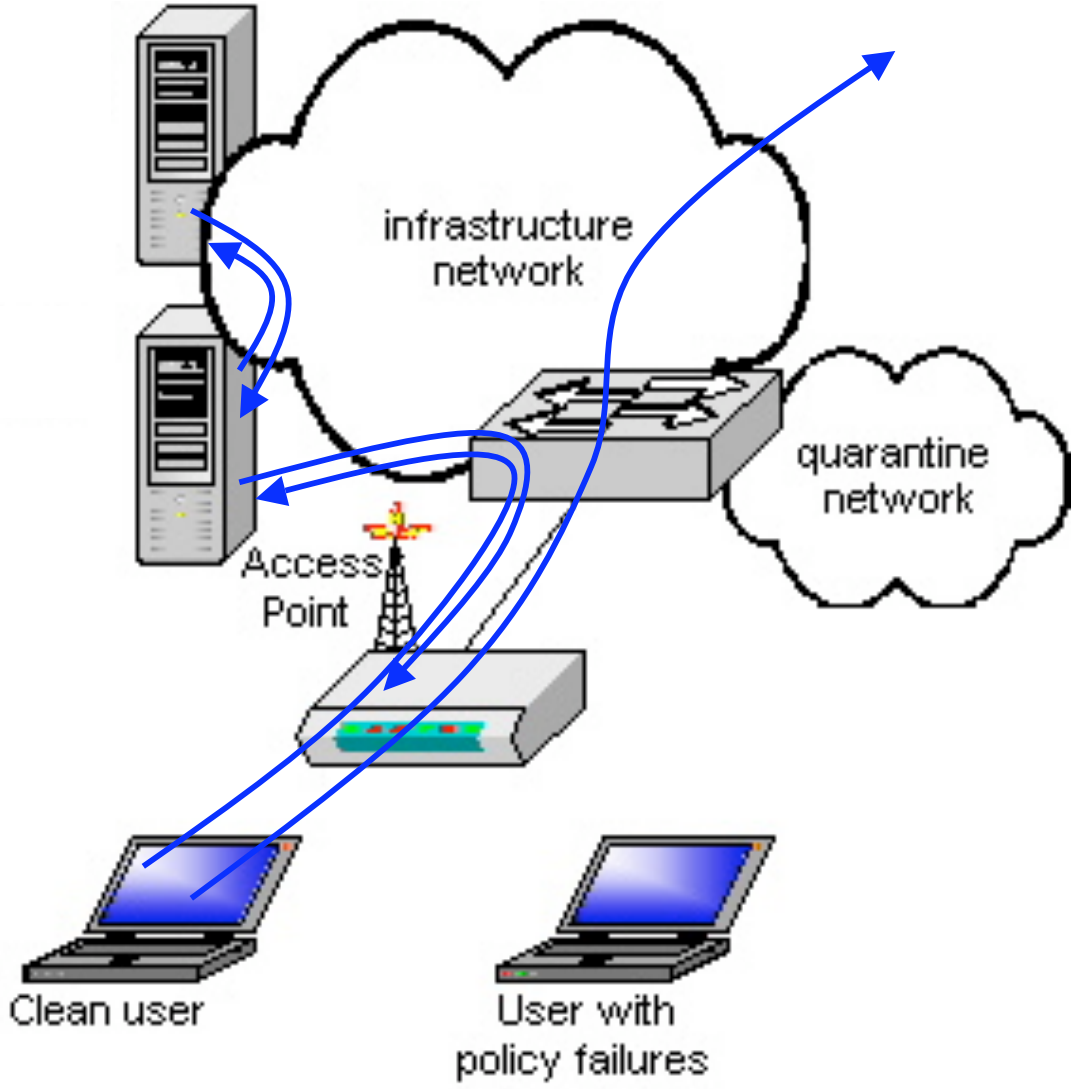
Protocol Requirements

Protocol	Examples
Posture Attribute (PA)	New
Posture Broker (PB)	New
Posture Transport Tunnel (PTT)	EAP-TTLS, PEAP, EAP-FAST
Posture Transport Carrier (PTC)	EAPoL2: 802.1x EAPoL3: PANA, NACP
Network Access Enforcement (NAE)	RADIUS
Posture Validation (PV)	New

Source: NEA BOF at IETF65

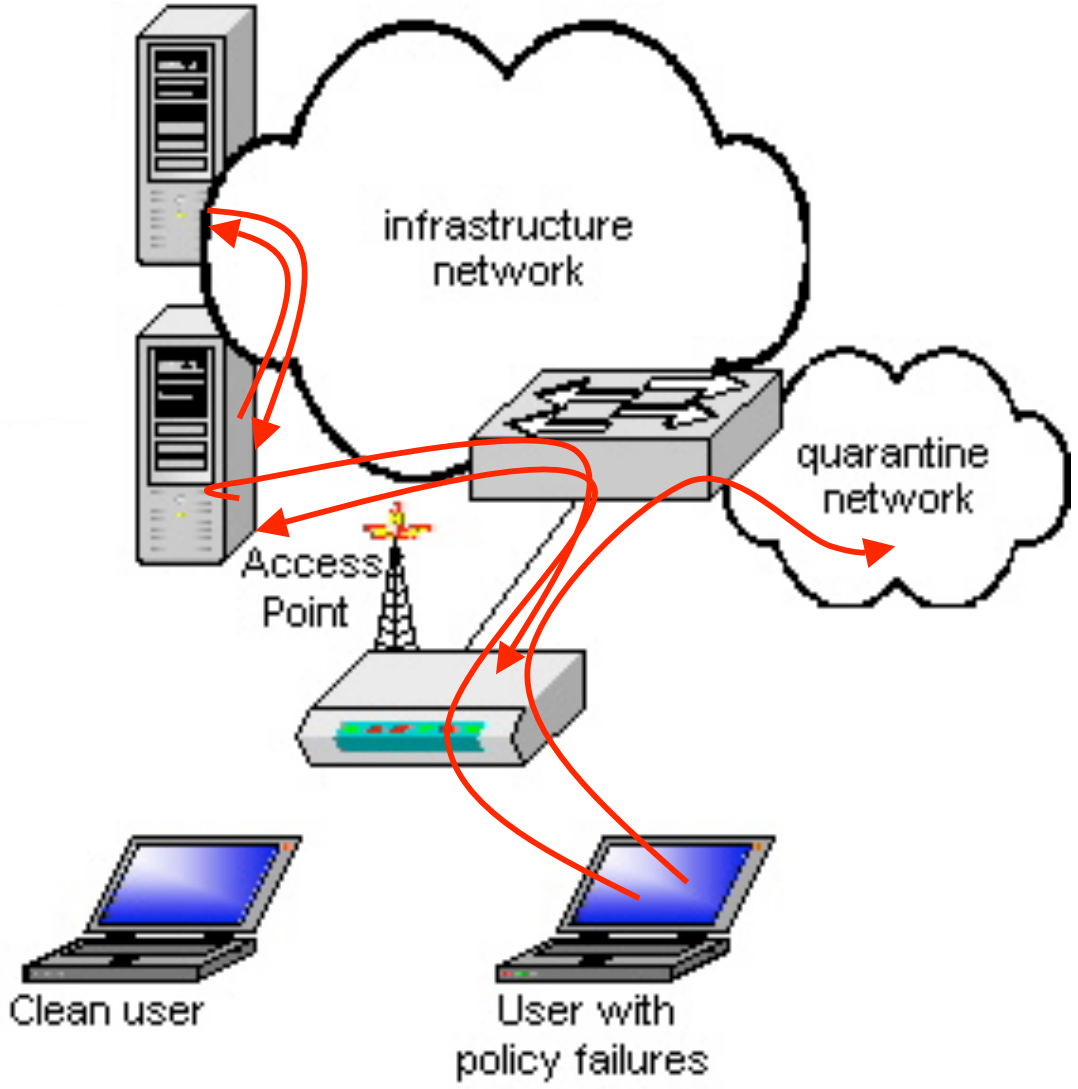
Example: Policy Enforcement

- 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



Agenda

- Why NAC?
- What is a Policy?
- Generic NAC architecture
- What is emerging today?
- What are your first steps?
- Where can you learn more?

NAC Solutions

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

Cisco NAC

- Strengths
  - Third party support for client
  - Installed base of network devices
- Limitations
  - Tied to Cisco hardware
  - Not an open standard
  - Requires third party supplicant for wireless
- Status
  - Product shipping today
  - Refinement of policy server expected (2007)

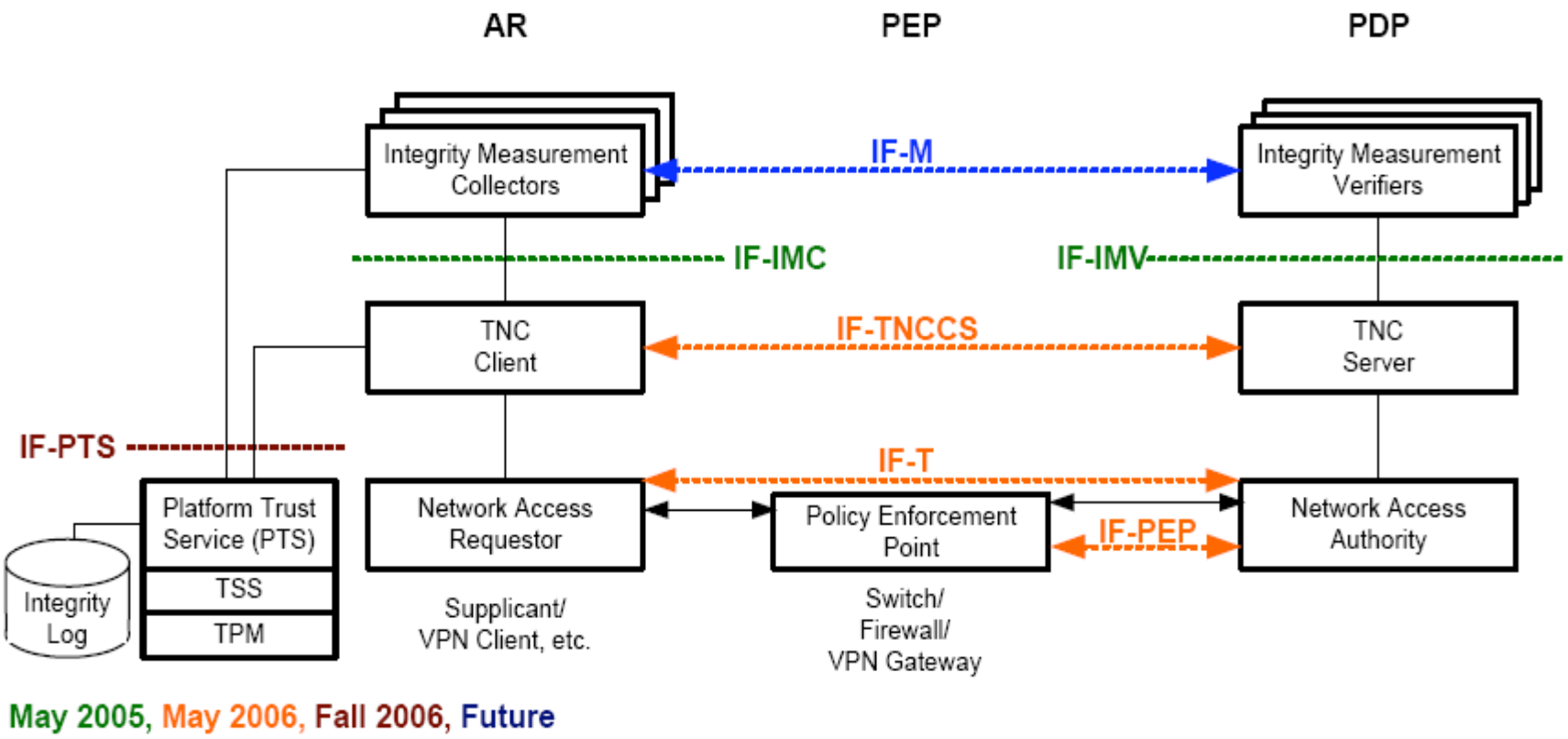
Microsoft NAP

- Strengths
  - Part of Windows operating system
  - Supports auto remediation
  - Network device neutral
- Limitations
  - Part of Windows operating system
  - Client support limited (only Vista guaranteed)
  - Not an open standard
- Status
  - Not shipping today
    - Expect release in early 2007.

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

- Strengths
  - Open standards based
    - Trusted Computing Group
  - Not tied to specific hardware, servers, or client operating systems
- Limitations
  - Still in its infancy
  - Potential integration risk with multiple parties
- Status
  - Currently no shipping products
    - Maybe Fall 2006
  - Updated specifications released May 2006

TNC Architecture



Source: TCG

Current State of Affairs

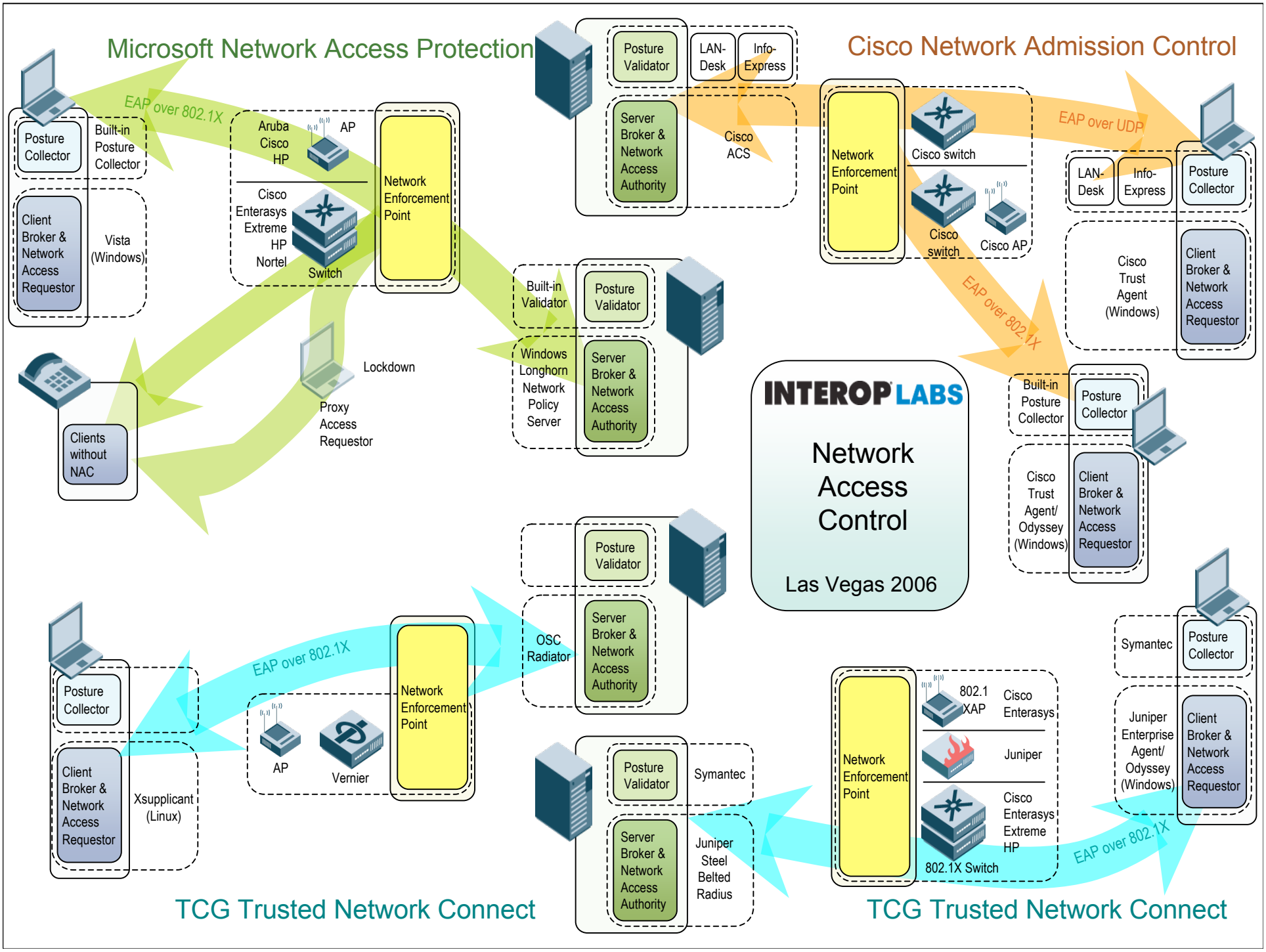
- Multiple non-interoperable solutions
  - Cisco NAC, Microsoft NAP, TCG TNC
  - Conceptually, all 3 are very similar
  - All with limitations
  - None completely functional
- Industry efforts at convergence and standardization
  - TCG
  - IETF

What is the IETF role?

- The Internet Engineering Task Force (IETF) is considering additional standards in this area
  - Network Endpoint Assessment BOF held in March 2005
  - Co-chaired by Cisco and TNC representatives
  - Formation of a working group under consideration

Agenda

- Why NAC?
- What is a Policy?
- Generic NAC architecture
- What is emerging today?
- What are your first steps?
- Where can you learn more?


Microsoft Network Access Protection
Posture Collector
Built-in Posture Collector
Client Broker & Network Access Requestor
Vista (Windows)
EAP over 802.1X
Aruba
Cisco
HP
AP
Cisco
Enterasys
Extreme
HP
Nortel
Switch
Network Enforcement Point
Clients without NAC
Lockdown
Proxy Access Requestor
Posture Validator
LAN-Desk
Info-Express
Server Broker & Network Access Authority
Cisco ACS
Built-in Validator
Windows Longhorn Network Policy Server
Cisco Network Admission Control
Network Enforcement Point
Cisco switch
Cisco switch
Cisco AP
EAP over UDP
EAP over 802.1X
LAN-Desk
Info-Express
Posture Collector
Cisco Trust Agent (Windows)
Client Broker & Network Access Requestor
Built-in Posture Collector
Posture Collector
Cisco Trust Agent/ Odyssey (Windows)
Client Broker & Network Access Requestor
INTEROP LABS
Network Access Control
Las Vegas 2006
Posture Collector
Client Broker & Network Access Requestor
Xsupplicant (Linux)
EAP over 802.1X
AP
Vernier
Network Enforcement Point
Posture Validator
Server Broker & Network Access Authority
OSC Radiator
Posture Validator
Symantec
Server Broker & Network Access Authority
Juniper Steel Belted Radius
TCG Trusted Network Connect
Network Enforcement Point
802.1 XAP
Cisco Enterasys
Juniper
Cisco Enterasys Extreme HP
802.1X Switch
EAP over 802.1X
Symantec
Posture Collector
Juniper Enterprise Agent/ Odyssey (Windows)
Client Broker & Network Access Requestor
TCG Trusted Network Connect

NAC Lab Participants

INTEROP LABS

NAC Team Engineers

- Steve Hultquist, Infinite Summit, Team Lead
- Chris Hessing, University of Utah
- Kevin Koster, Cloudpath Networks, Inc.
- Mike McCauley, Open System Consultants
- Karen O'Donoghue, US Navy
- Joel Snyder, Opus One Inc.
- Brett Thorson, RavenWing, Inc.
- Jan Trumbo, Opus One Inc.
- Craig Watkins, Transcend, Inc.

NAC Contributor Engineers

- Jack Coates, LANDesk
- Chris Edson, Microsoft
- Christian MacDonald, Juniper Networks
- Bryan Nairn, Lockdown Networks
- Jeff Reilly, Juniper Networks
- Mauricio Sanchez, Hewlett-Packard
- Eric Thomas, WildPackets, Inc.
- Mark Townsend, Enterasys Networks

NAC Contributors

- A10 Networks
- Aruba Networks
- Enterasys Networks
- Extreme Networks
- Cisco Systems
- Hewlett-Packard
- InfoExpress
- Juniper Networks
- LANDesk
- Lockdown Networks
- Microsoft
- Nortel Networks
- Open1X Project
- Open Systems Consultants
- Vernier Networks, Inc.

Getting started with NAC

- Answer three basic questions.
  - What is your access control policy?
  - What access methods do you want to protect?
  - What is your existing infrastructure?
- Test early and often
- Monitor the progress of open standards based solutions
- Don’t do this alone! (at least today)

Where can you learn more?

- Visit the Interop Labs Booth (#2506)
  - Live Demonstrations of all three major NAC architectures *with engineers to answer questions*
  - White Papers available:
    - ☐ What is NAC?
    - ☐ What is 802.1X?
    - ☐ Getting Started with Network Access Control
    - ☐ What is TCG's Trusted Network Connect?
    - ☐ What is Microsoft's Network Access Protection?
    - ☐ What is Cisco Network Admission Control?
    - ☐ What is the IETF NAC Strategy?
    - ☐ **Network Access Control Resources** 

INTEROP LABS

- Visit us online:
  - http://www.opus1.com/nac
    - Interop Labs white papers, this presentation, and demonstration layout diagram

Thank You!

Questions?

Interop Labs -- Booth 2506
http://www.opus1.com/nac