



# I2 SALSA NetAuth Working Group

Internet2 Members Meeting  
Spring 2006

Kevin Amorin ~ Harvard University

# [ Overview ]

---

- Why “Automate Security and Policy Enforcement”?
- Internet2 : SALSA-NetAuth
- Strategies
- Architecture
- Components
- Wiki
- Use Case: Harvard University

# Why “Automate Security and Policy Enforcement”?

- Only automated approaches can scale and respond rapidly to large-scale incidents.
- Preventative policy enforcement reduces risk:
  - overall number of security vulnerabilities
  - the success of any particular attack technique.
- Automated remediation systems have a positive impact on a large number of hosts with a relatively small time investment from computing staff.

# [ Internet2 : SALSA-NetAuth ]

- Internet2 formed a working group under SALSA to address this problem in May 2004
- Charter: The SALSA-NetAuth Working Group will consider the data requirements, implementation, integration, and automation technologies associated with understanding and extending network security management related to:
  - 📁 Authorized network access (keyed by person and/or system)
  - 📄 Style and behavior of transit traffic (declarative and passive)
  - 🔍 Forensic support for investigation of abuse
- <http://security.internet2.edu/netauth>

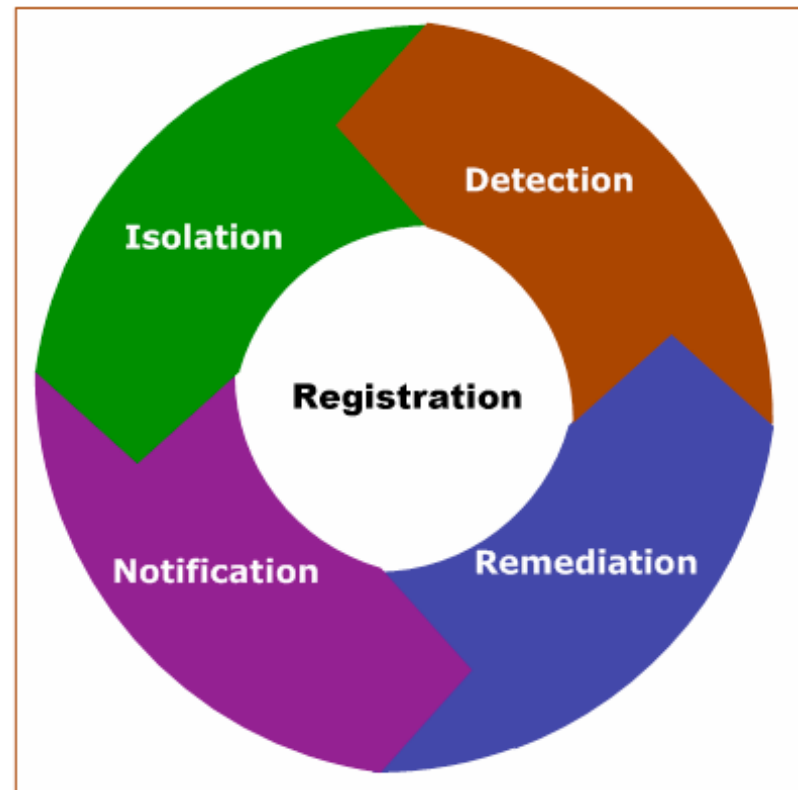
# [ Internet2 : SALSA-NetAuth ]

- Strategies for Automating Network Policy Enforcement *(completed)*
- Architecture for Automating Network Policy *(completed)*
- Components Framework for Policy-based Admission Control *(draft 1)*
- Wiki
- FWNA

# Strategies for Automating Network Policy Enforcement

There is a growing “Common Process” Consisting of Five Elements:

- Registration
- Detection
- Isolation
- Notification
- Remediation

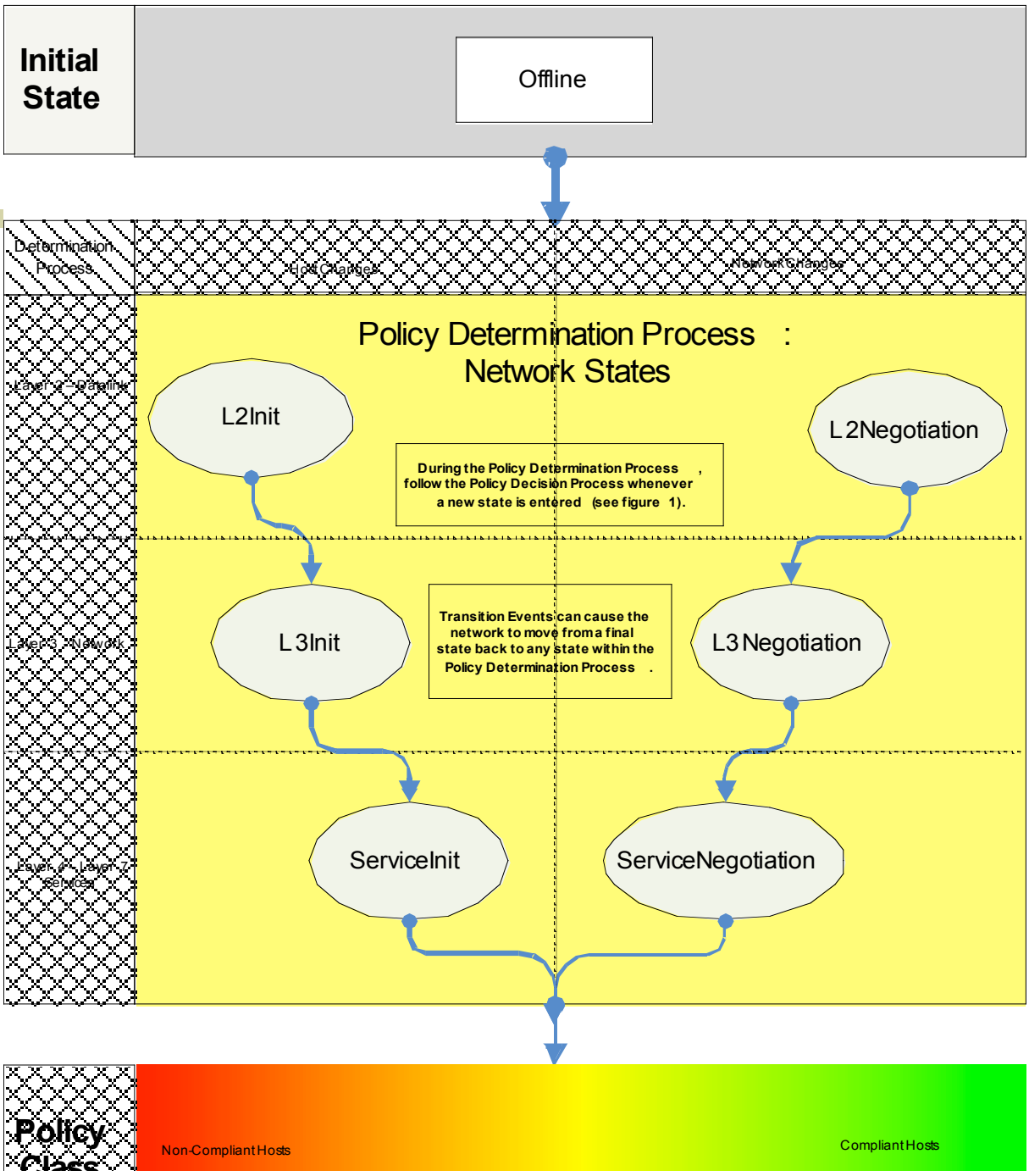


# [ Use Case: Harvard University ]

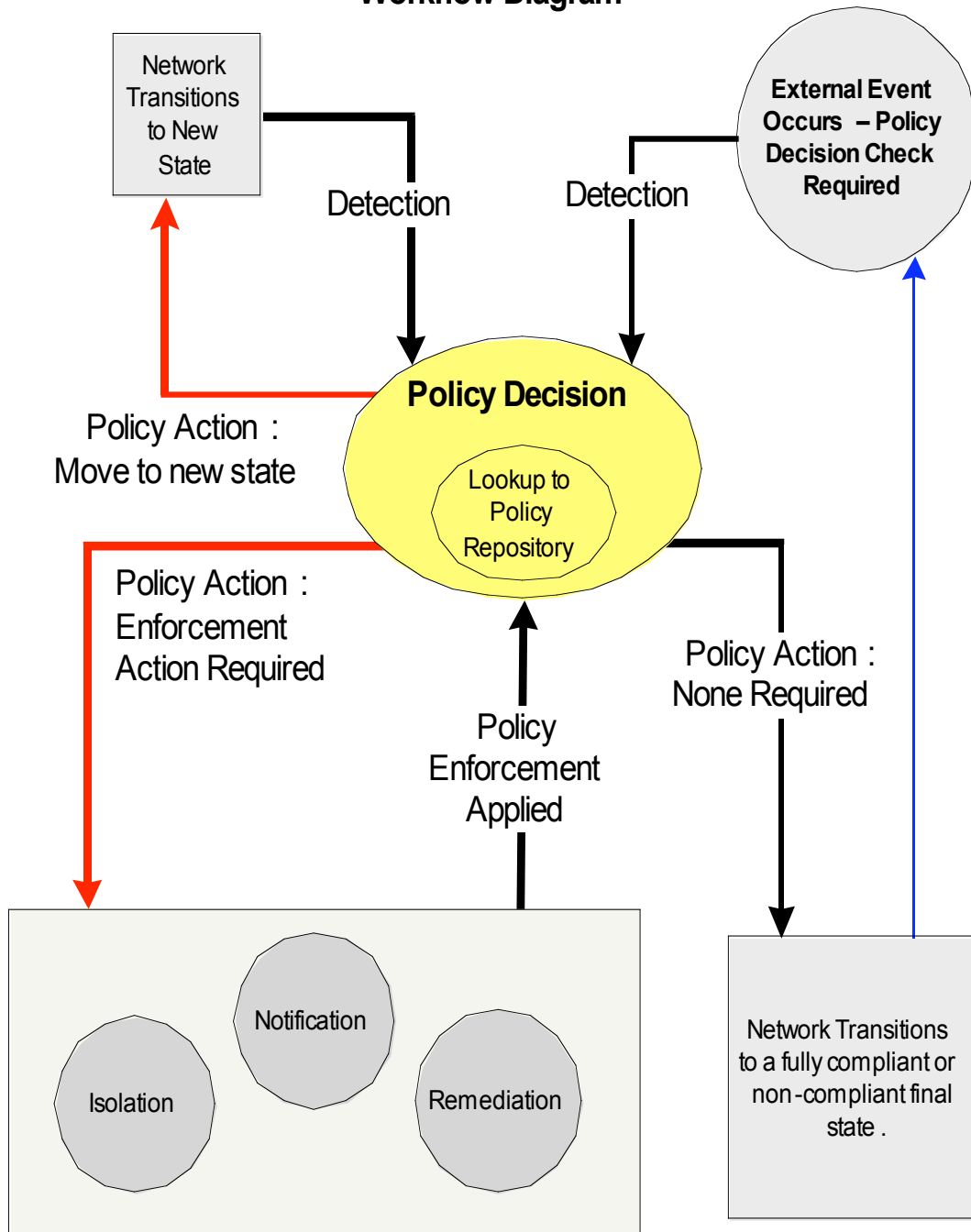
- PacketFence v1.6
- Initial registration isolation with “skip” period for “roaming scholars” (*registration/isolation*)
- Scanning at registration and periodic intervals (*detection*)
- Sensors to detection infection (*detection*)
- Each violation has a list of associated actions (email/log/isolate/external script) and remediation content (local content/remote URL) (*notification/remediation*)

# Architecture for Automating Network Policy

- At a very high level, network usage translates into allowing or blocking various sets of network flows.
- Filtering can be relatively simple, such as allowing all flows, or can be extraordinarily complex, such as the case of inline application proxies which make per-flow decisions based on application layer content
- Network and the host can be modeled in states with policies applied in each state.



## Workflow Diagram



Transition Events include such things as:

- Connections
- Network Disruptions
- Host Stack Changes
- Scanners
- Agents
- Flows
- Services
- Rules

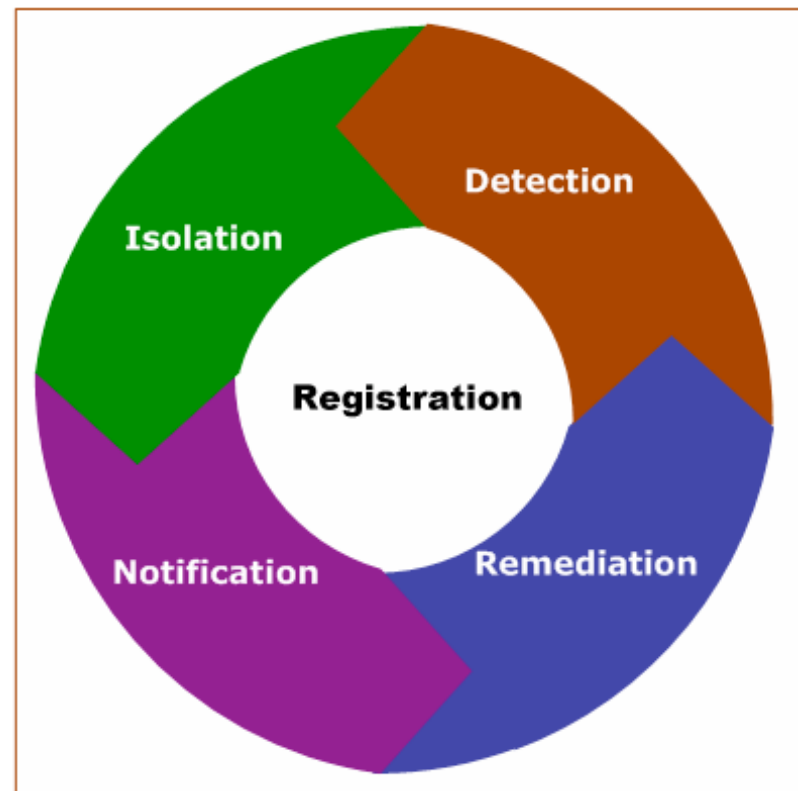
# [ Use Case: Harvard University ]

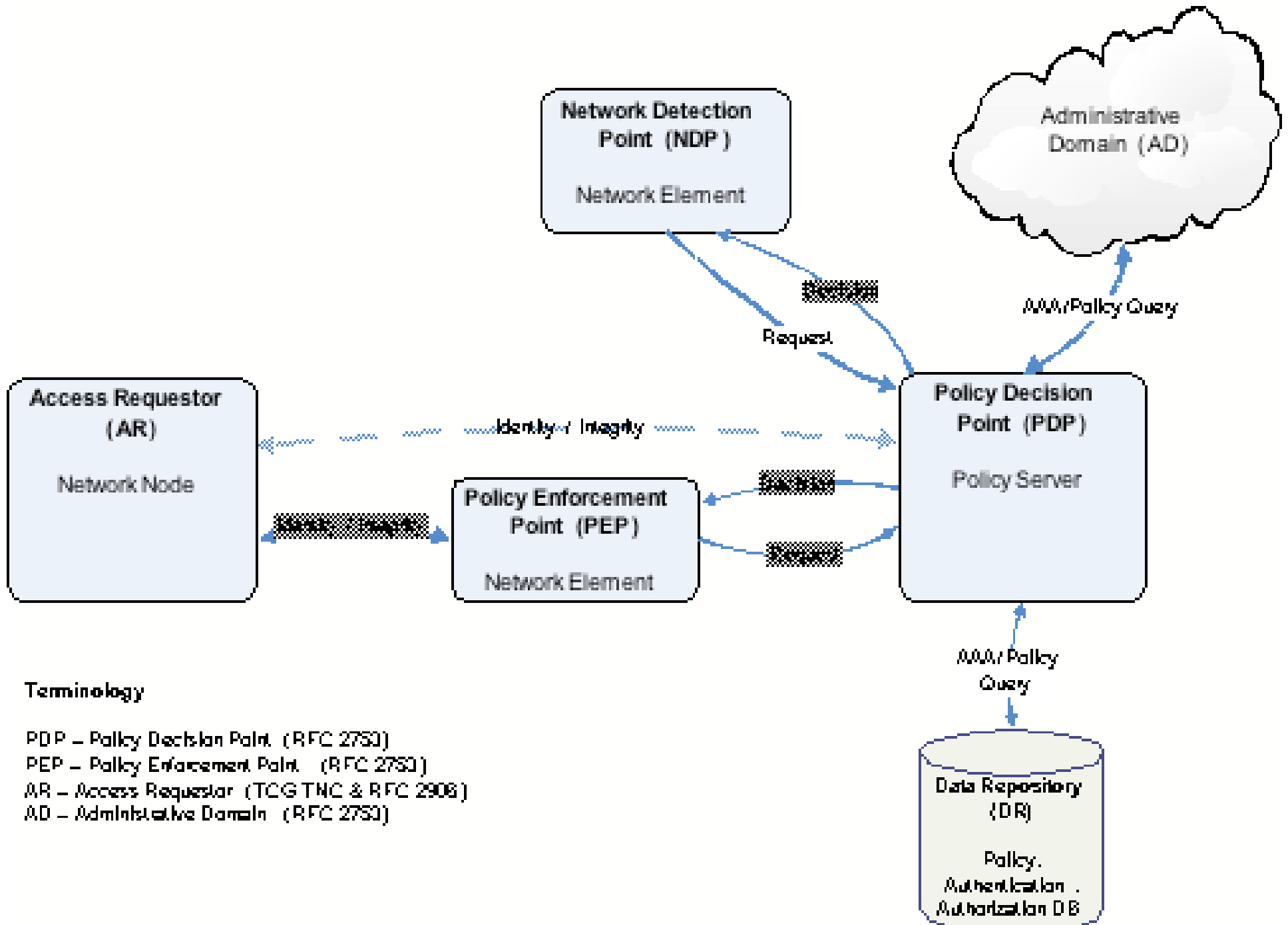
- L2 Init:
  - Initial host ARP will trigger a policy decision
- L2 Negotiation:
  - If the device is inline, a policy decision will trigger an iptables addition. If device is passive, ARP manipulation will overwrite host gateway.
- L3 Init: None.
- L3 Negotiation: None.
- Service Init: None.
- Service Negotiation: None

# [ SALSA-NetAuth: Components ]

## Components Document

- A review of how commonly used systems fit into this architecture
- Mechanisms to create interoperability between these components
- Case studies of existing deployments

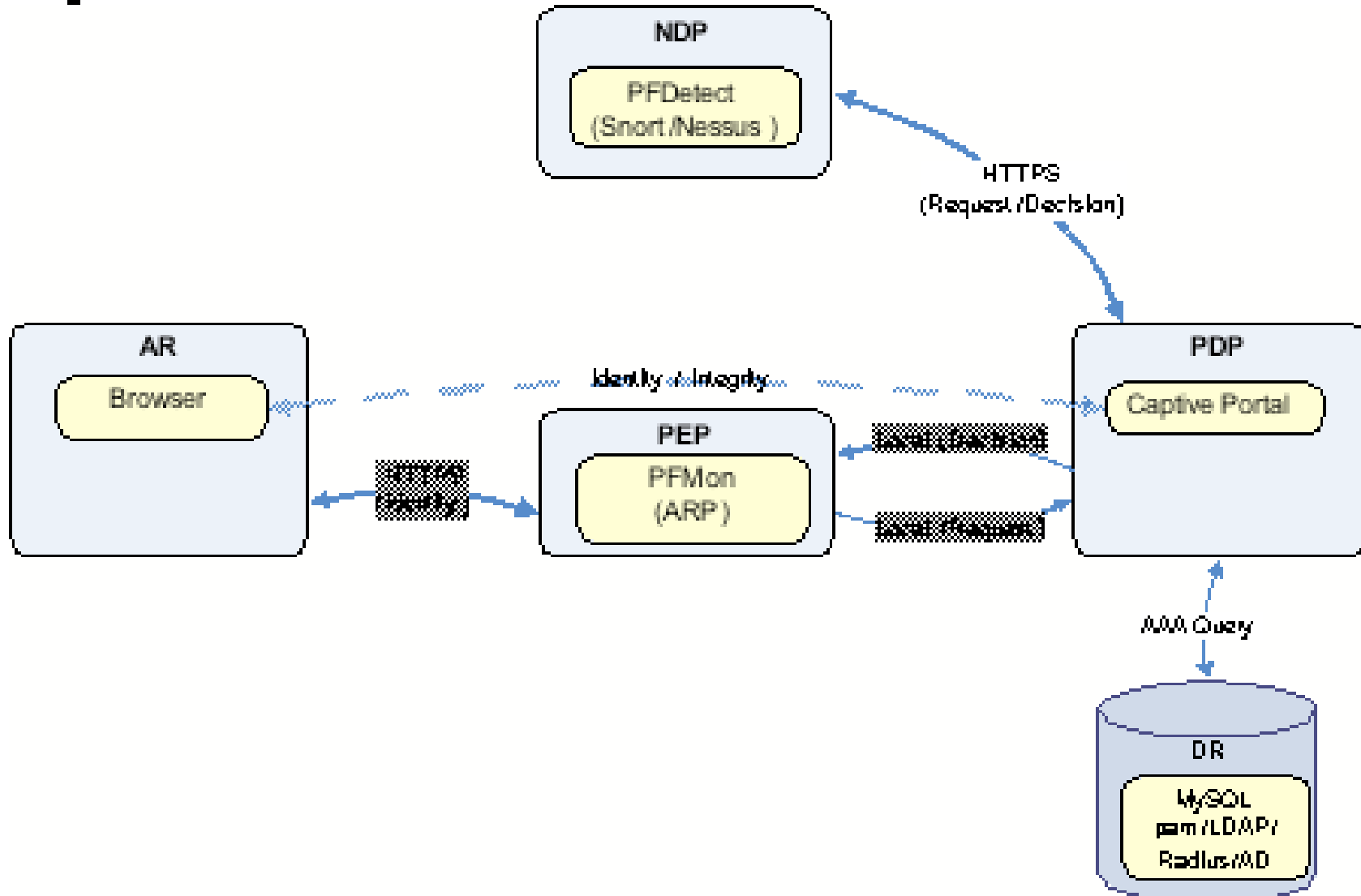




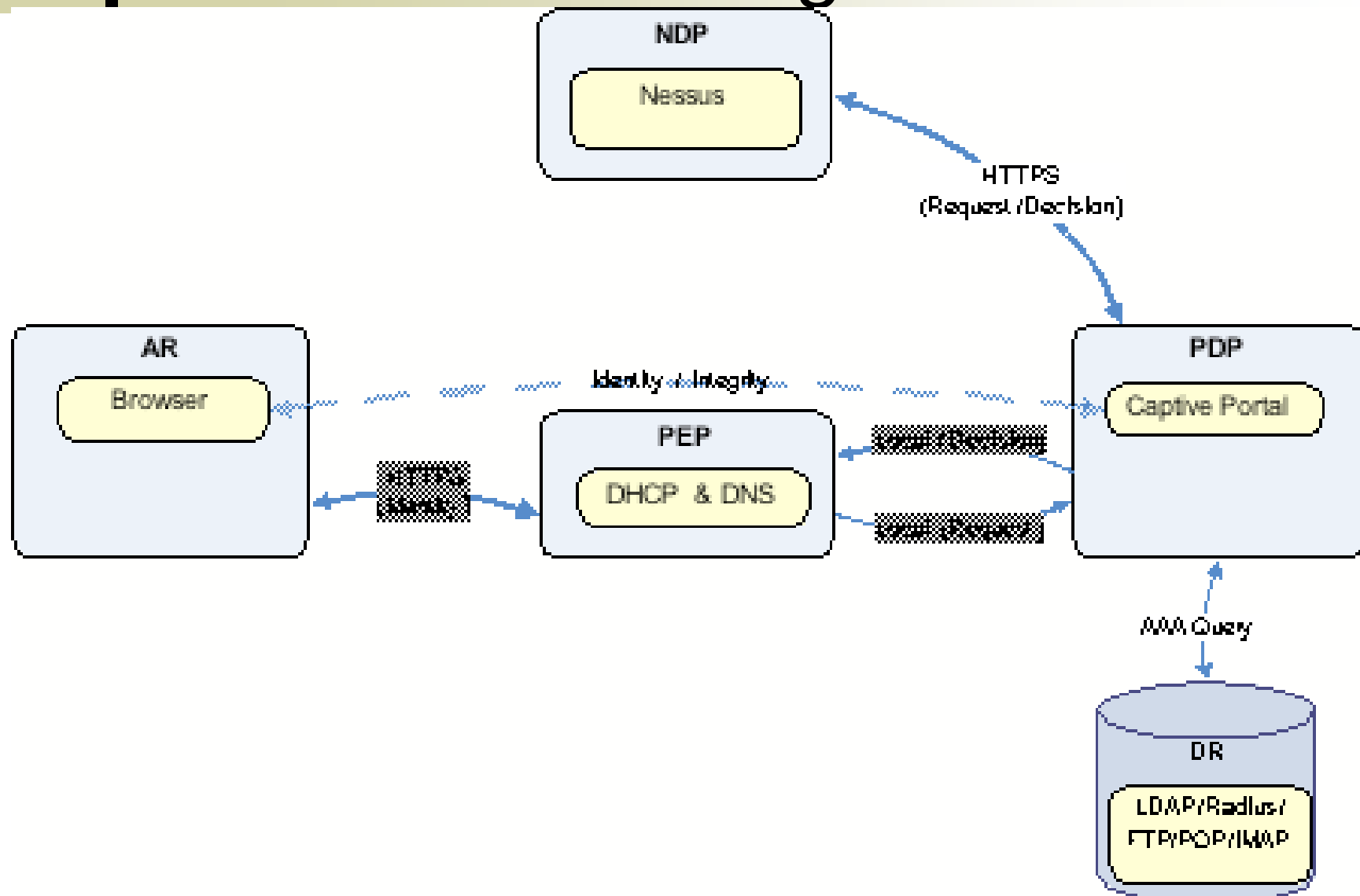
### Terminology

- PDP – Policy Decision Point (RFC 2753)
- PEP – Policy Enforcement Point (RFC 2753)
- AR – Access Requestor (TCG TNC & RFC 2906)
- AD – Administrative Domain (RFC 2753)

# Use Case: Harvard University



# Use Case: NetReg



# [ NetAuth Wiki ]

---

- <http://wiki.internet2.edu>
- FAQ
- Open source options
- Commercial options
  - Currently most comprehensive vendor list available in NAC

# [ Commercial Options ]

- 3com
- Bradford
- Cisco
- Checkpoint
- ConSentry
- EndForce
- Extreme
- Enterasys
- FourScout
- Full Armor
- HP ProCurve
- Impluse Point
- InfoBlox
- InfoExpress
- Ipass
- Juniper
- Latis Networks
- Lanscope
- LANDesk
- Lockdown Networks
- Nevis
- Nortel
- Mazu Networks
- Permeo
- Q1 Lab
- Reflex Security
- Roving Planet
- Seclarity
- SenForce
- Symantec
- Vernier
- Wave

# [ NetAuth & Open Source ]

- PacketFence
  - Kevin Amarin & David LaPorte
- RINGS
  - Dustin Brown
- Southwestern NetReg
  - Robert Lowe
- CMU NetReg
  - Kevin Miller

# [ Other Vendor Work ]

- Network Admission Control (NAC)
  - Cisco gear end-to-end
  - Windows CTA Required
  - Many different moving parts
- Trusted Network Connect (TNC)
  - Vendor Interoperability
  - Slow Moving
  - 802.1x only
- Network Access Protection (NAP)
  - Longhorn & Vista required (Q19 2007)

# [ SALSA-Netauth: Upcoming ]

- Draft 2 of Components Document
- Additional Wiki Contributions
  - FAQ
  - Commercial & Open Source Solutions
  - <http://wiki.internet2.edu>
- Federated Wireless Network Authentication (FWNA).

# [ SALSA-Netauth: FWNA ]

- Enable members of one institution to authenticate to the wireless network at another institution using their home credentials.
- Often called the “roaming scholar” problem in HiEd.
- Wired networks handled as well.

# [ Thanks! ]

---

- Internet2 / Educause for supporting the SALSA-NetAuth working group (join us!)
- Eric Gauthier, Kevin Miller, Chris Misra, Phil Rodrigues and the entire NetAuth working group

# [ Questions? ]



Kevin Amarin ~ [kamarin@harvard.edu](mailto:kamarin@harvard.edu)

NetAuth

[salsa-netauth@internet2.edu](mailto:salsa-netauth@internet2.edu)

<http://security.internet2.edu/netauth/>