



Network Architecture for Automatic Security and Policy Enforcement

Internet2 Members Meeting
Fall 2005

Eric Gauthier ~ Boston University

Kevin Amorin ~ Harvard University

[Overview]

- Why “Automate Security and Policy Enforcement”?
- Internet2 : SALSA-Netauth
- Strategies
- Architecture
- Case Study: Boston University
- Case Study: Harvard University
- Components
- SALSA-Netauth: Upcoming work

Why “Automate Security and Policy Enforcement”?

From the SALSA-Netauth document *Strategies for Automating Network Policy Enforcement*:

“The major security challenge facing university residential networks and other large-scale end-user networks is the thousands of privately owned and unmanaged computers directly connected to an institution's relatively open, high-speed Internet connections. Security policy enforcement is often lax due to a lack of central control over end-user computers and an inability to tie the actions of these computers to particular individuals. A few times a year there are surge events, including the predictable start of each semester and the unpredictable and increasingly frequent reactions to large-scale security incidents, that require massive support intervention.

If these challenges are allowed to evolve unchecked, the result is the presence of thousands of unsecured computers that are prone to mass infection by malware or wide-scale compromise by increasingly unsophisticated attackers. Malware and attackers often specifically seek to harness large numbers of unsecured hosts for use in distributed file sharing, spam, and/or attack networks. The presence of these malicious overlay networks has been known for some time, but the full realization of fast, always-on Internet access has increased their size and potential for harm.” 3

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:
 1. Authorized network access (keyed by person and/or system)
 2. Style and behavior of transit traffic (declarative and passive)
 3. Forensic support for investigation of abuse
- <http://security.internet2.edu/netauth>

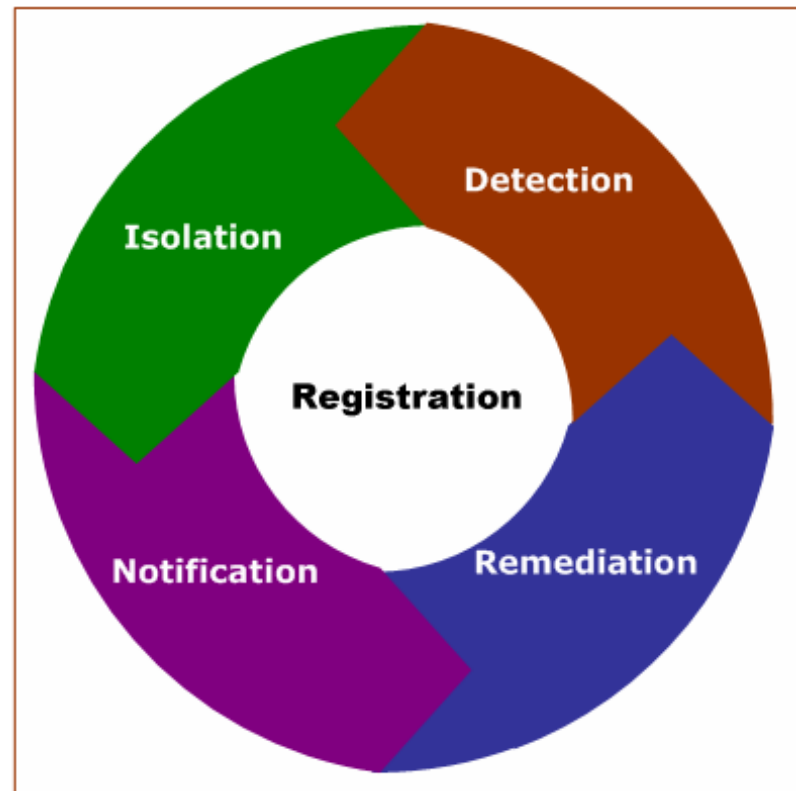
[Internet2 : SALSA-Netauth]

- Strategies for Automating Network Policy Enforcement *(completed)*
- Architecture for Automating Network Policy *(draft 4)*
- Components Framework for Policy-based Admission Control *(draft 1)*
- FWNA
- More...

Strategies for Automating Network Policy Enforcement

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

- Registration
- Detection
- Isolation
- Notification
- Remediation

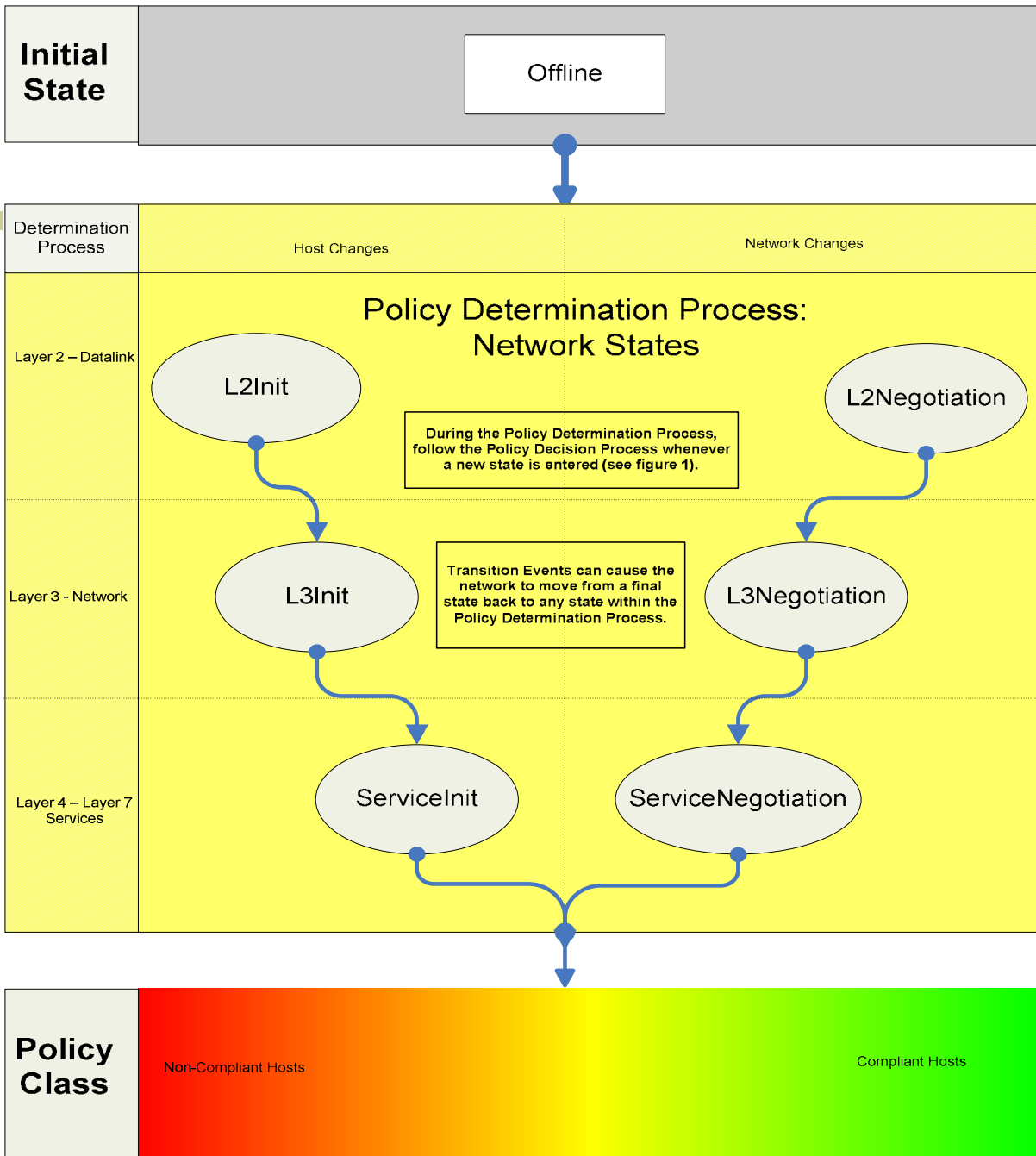


Architecture for Automating Network Policy

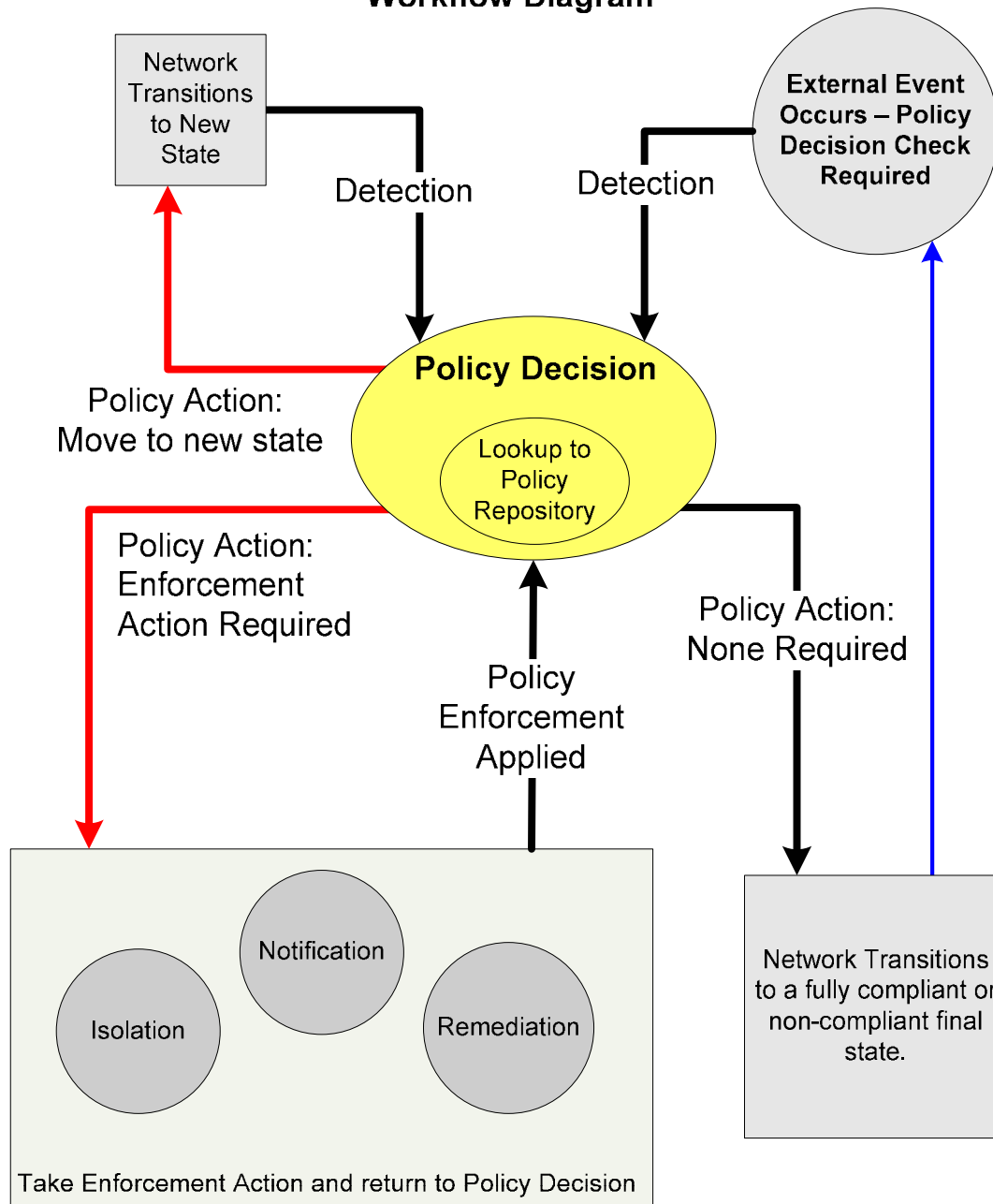
- “This architecture is intended as a framework to develop standardized mechanisms and detailed descriptions of how to directly implement policy enforcement using existing devices and as a guide for the development of new interoperable solutions. This framework is intended to be flexible, extensible, interoperable with existing infrastructure, and provide the necessary hooks to accommodate upcoming technologies such as federated authentication and authorization schemes.”

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

[Case Study: Boston University]

- Updated version of Southwestern University's NetReg v2.0 (*registration*)
- Isolation networks with customizable web pages (*isolation/notification*)
- Initial post-registration quarantine (*isolation/notification/remediation*)
- Custom one-time agent (*remediation*)
- Sensors to detect subsequent infection and policy violations (*detection*)

[Case Study: Boston University]

- L2 Init: None.
- L2 Negotiation: None.
- L3 Init:
 - Netreg/DHCP “tricks” to assign host to either a “compliant” network or isolation network
- L3 Negotiation: None.
- Service Init: None.
- Service Negotiation: None

[Case Study: Harvard University]

- PacketFence v1.5
- 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*)

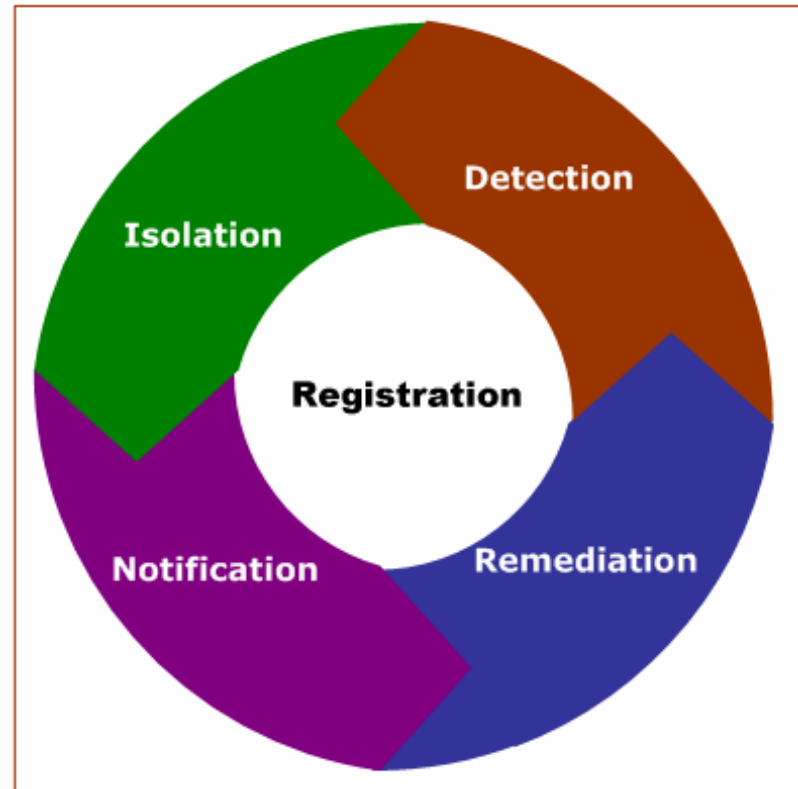
[Case Study: Harvard University]

- L2 Init:
 - Initial host ARP will trigger a policy decision
- L2 Negotiation:
 - If the decision is isolation, ARP manipulation will overwrite host gateway
- L3 Init: None.
- L3 Negotiation: None.
- Service Init: None.
- Service Negotiation: None

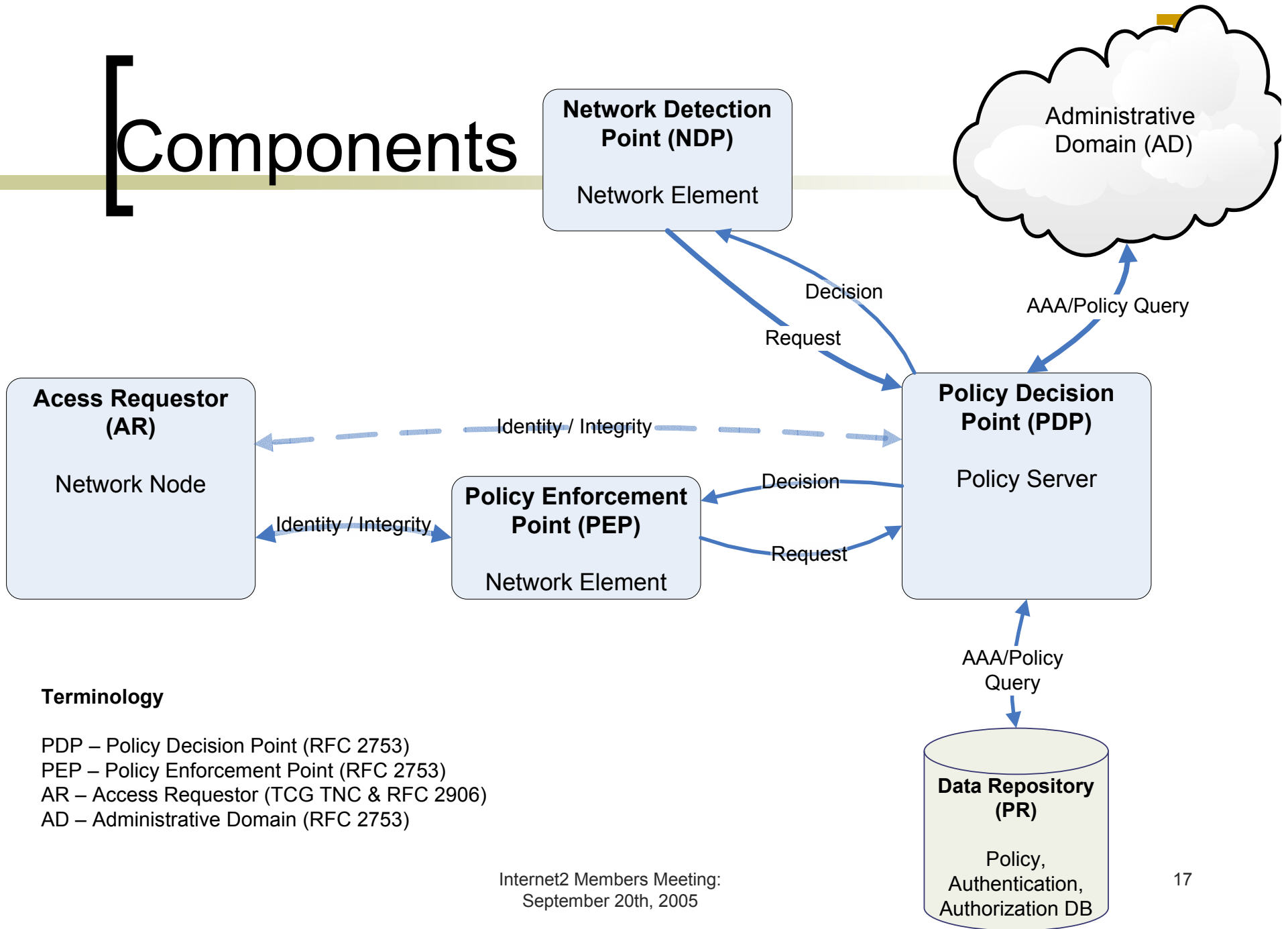
[SALSA-Netauth: “Components”]

“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



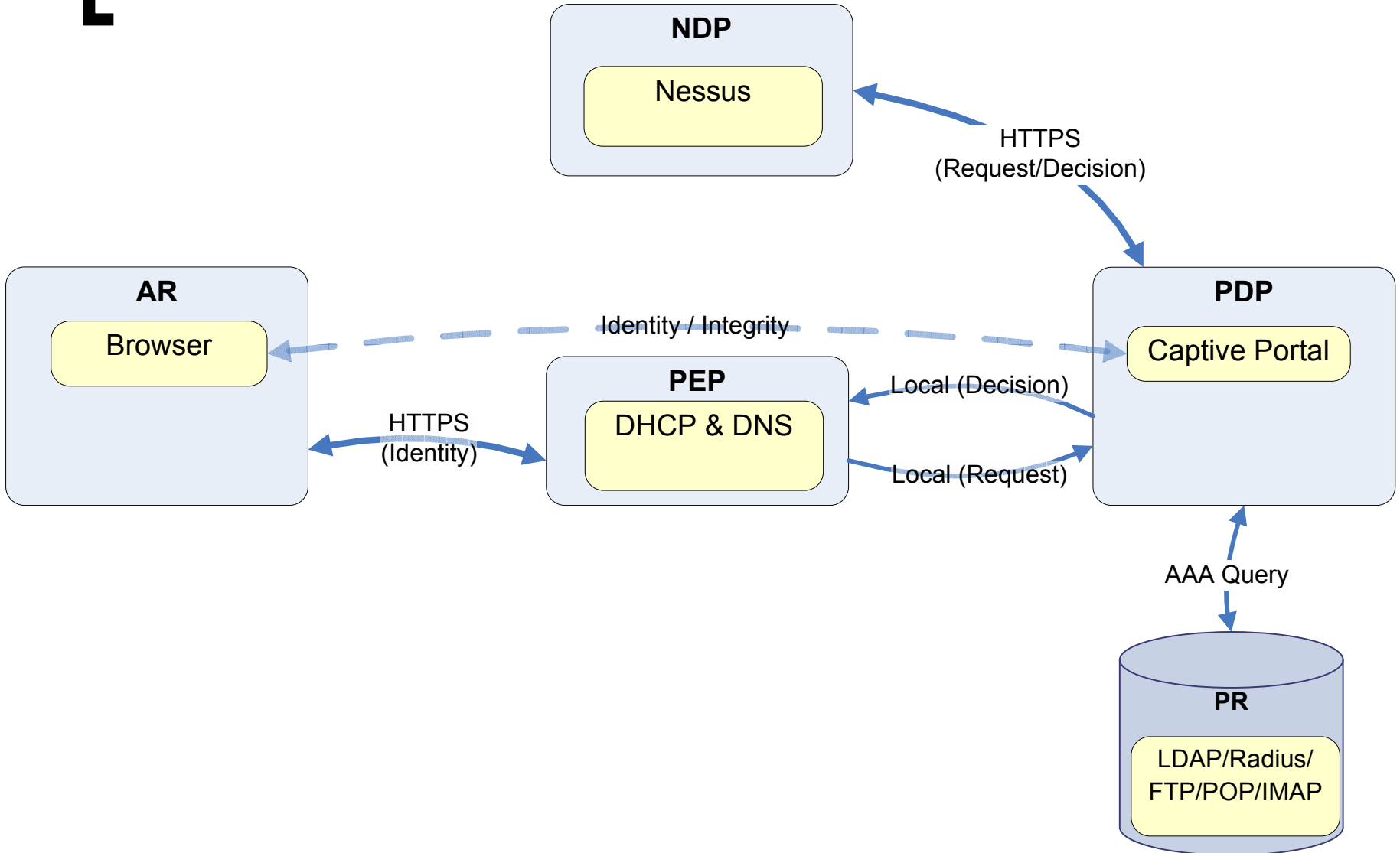
[Components



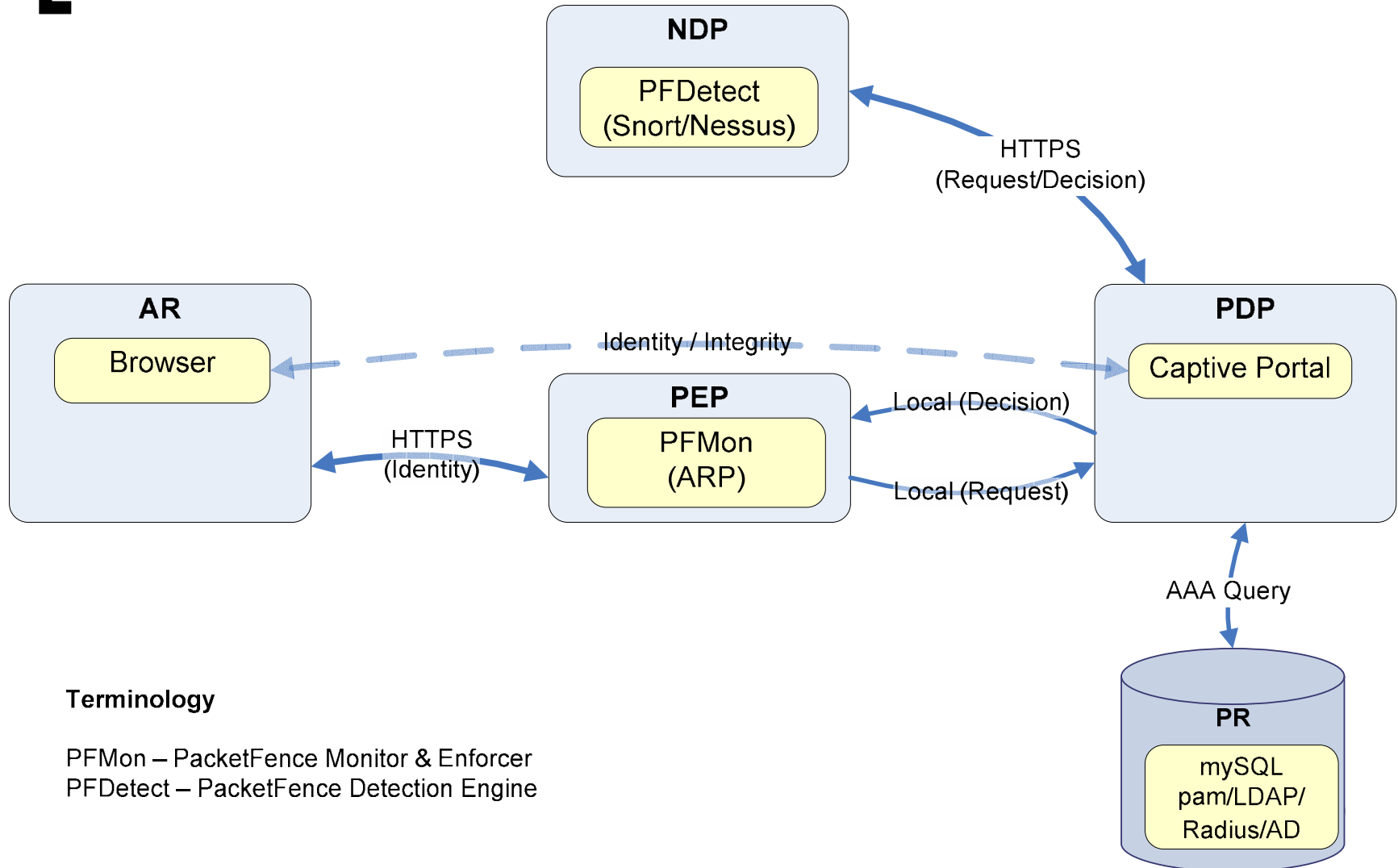
Terminology

- 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: NetReg]



[Use Case: PacketFence]



Terminology

PFMon – PacketFence Monitor & Enforcer
PFDetect – PacketFence Detection Engine

[Other Vendor work]

- Network Admission Control (NAC)
 - Cisco only end-to-end
 - Phase 2 switch/AP support?
(Q1,Q2,Q3,Q4 2005-)
 - Windows CTA Required (Guests)
 - What about open networks (Columbia)?
 - Many different moving parts
 - How does clean access fit in?

[Other Vendor work]

- Trusted Network Connect (TNC)
 - Vendor operability
 - TNC Client required
 - Slow moving
 - Very focused on proving Integrity
 - IM-T, IM-PEP currently not defined
 - May not encompass all of Network Admission

[SALSA-Netauth: Upcoming]

- Complete Architecture Document
 - Draft 2 of Components Document
 - Vendor Discussions
 - Reference Model?
-
- 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.

[SALSA-Netauth: FWNA]

- In many cases today, once authenticated, all users obtain same level of service
- FWNA is about identity discovery
- We must be able to separately provision services from authentication and attributes:
 - Technical setup (IP address, QoS, ACL, etc..)
 - Access policy
 - Billing

[SALSANetauth: FWNA]

- 802.1x
 - Often used with WPA or WPA2 (802.11i)
 - Or middlebox access controller
- EAP authentication
 - Exact EAP type selected by home institution, deployed on client machines
- Phase 1: “Simple” RADIUS peering
 - Integration with existing authn backend
 - EduRoam

[Thanks!]

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

[Questions?]



Eric Gauthier ~ elg@bu.edu

Kevin Amarin ~ kamarin@harvard.edu

NetAuth

salsa-netauth@internet2.edu

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