

SALSA-NetAuth

Joint Techs
Vancouver, BC
July 2005

Agenda

- NetAuth background
- NetAuth Strategies Document
- NetAuth Architecture Documents
- Applicability to federated network access environments
- What do we do next?

SALSA-NetAuth 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

SALSA-NetAuth Working Group: Initial activities

- *Investigation of requirements and implementations of network database and registration services in support of network security management; - **Complete, Strategies Document***
- *Investigation of extensions to these services to proactively detect and prevent unauthorized or malicious network activity. – **Strategies Document, Architecture Documents***
- *Analysis and proposal toward a pilot and eventual implementation to support network access to visiting scientists among federated institutions. – **In Progress – Architecture Documents***
- *Analysis of security applications that may result from extending these implementations. – **Overarching all activities***

SALSA-NetAuth Working Group: Roadmap

- Outlines the activities of the SALSA-NetAuth working group and all related sub-groups.
- Reflects the overall direction of the working group(s) and maintain consistency between the various efforts
 - SALSA-NetAuth Working Group Roadmap
 - Christopher Misra, 25 April 2005
 - <http://security.internet2.edu/netauth/#Docs>

SALSA-NetAuth Working Group: Initial Deliverables

- Investigation of extensions to these services to proactively detect and prevent unauthorized or malicious network activity.
- Strategies for Automating Network Policy Enforcement
 - Eric Gauthier, Phil Rodrigues, 20 April 2005
 - Final draft 200504
 - <http://security.internet2.edu/netauth/#Docs>

Strategies for Automating Network Policy Enforcement

- “(A) Structure and summary of approaches for automating technical policy enforcement as a condition for network access in colleges and universities”
 - Host isolation into specialized networks
 - Conditional network access
 - Initial document
 - Not the final answer

Strategies for Automating Network Policy Enforcement

- Preventative policy enforcement reduces
 - Total number of technical security vulnerabilities
 - The success of a particular piece of malware or attack technique.
- Isolation networks separate compromised and infected hosts
 - Minimize the spread of infection
 - Block external access from attackers.
- Automated remediation systems have a positive impact on a large number of hosts with a relatively small time investment from computing staff.

Strategies for Automating Network Policy Enforcement

- The Common Process
- Five steps
 - Registration
 - Detection
 - Isolation
 - Notification
 - Remediation
- Not necessarily in this order.

What direction are we focusing current and future energies?

- Architecture document(s)
 - How do we make NetAuth a designed infrastructure versus organic
 - We need a model to analyze these systems
 - How do we apply NetAuth systems to federated environments? (like FWNA/eduRoam)
 - What components implement this architecture

Architecture Document

- A framework to develop standardized mechanisms and detailed descriptions of how to directly implement policy enforcement using existing devices
 - NetAuth Architecture for Automating Network Policy Enforcement
 - Kevin Amarin, Eric Gauthier, July 2005
 - Draft 03
 - <http://security.internet2.edu/netauth/#Docs>

Architecture Document – Draft 03

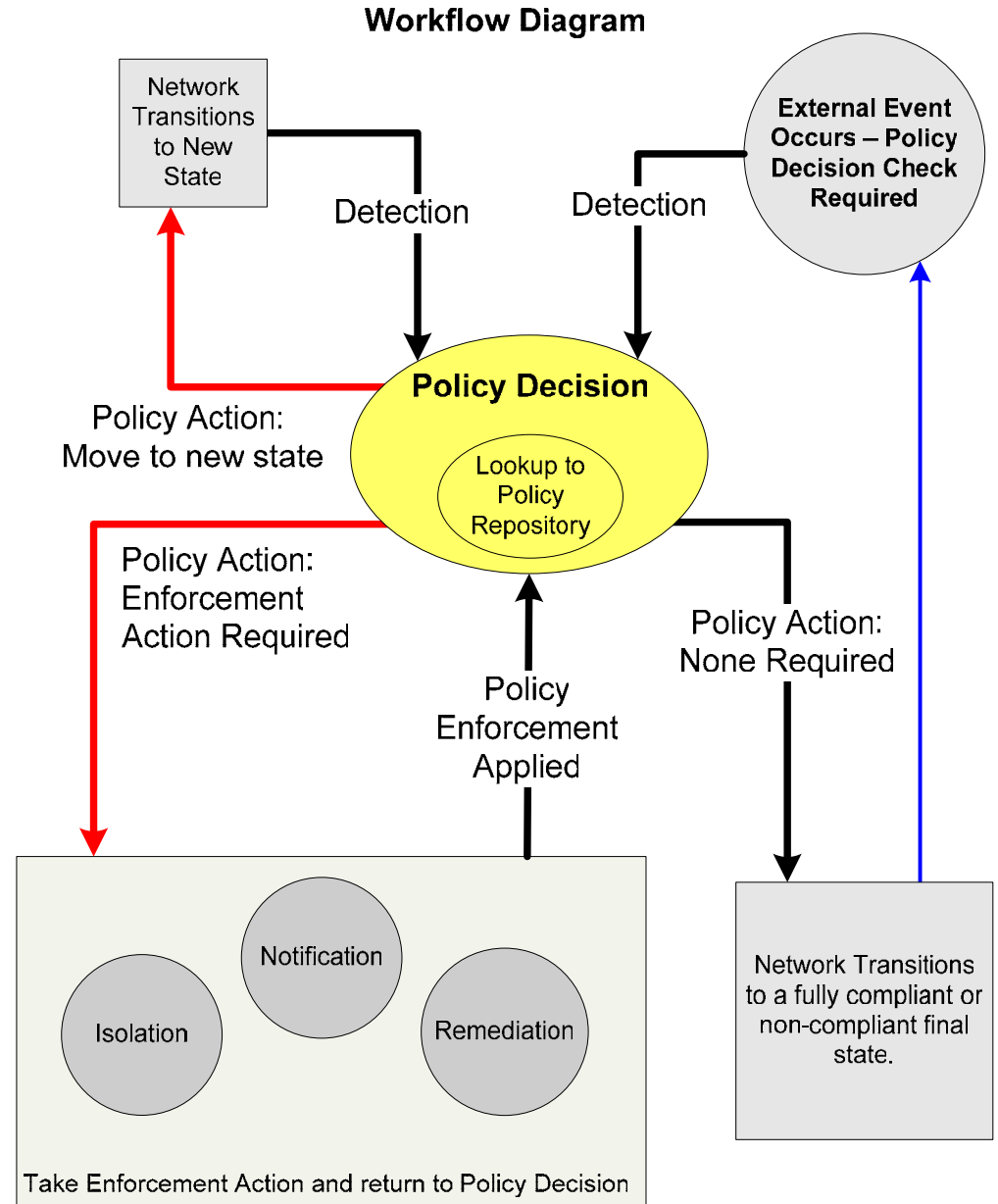
- To detail a policy enforcement architecture for network access.
- For analysis in both intra-campus and federated environments
- A guide for the development of new interoperable solutions.
- Draft 04 out hopefully by mid-August

Architecture Document – Draft 03

- Intended to be flexible, extensible, and interoperable with existing infrastructure
- Provide the necessary hooks to accommodate upcoming technologies such as federated authentication and authorization schemes.
 - Shibboleth, etc.
- How networks can implement network access policies even when network configurations and policies change dynamically

Policy Determination Process

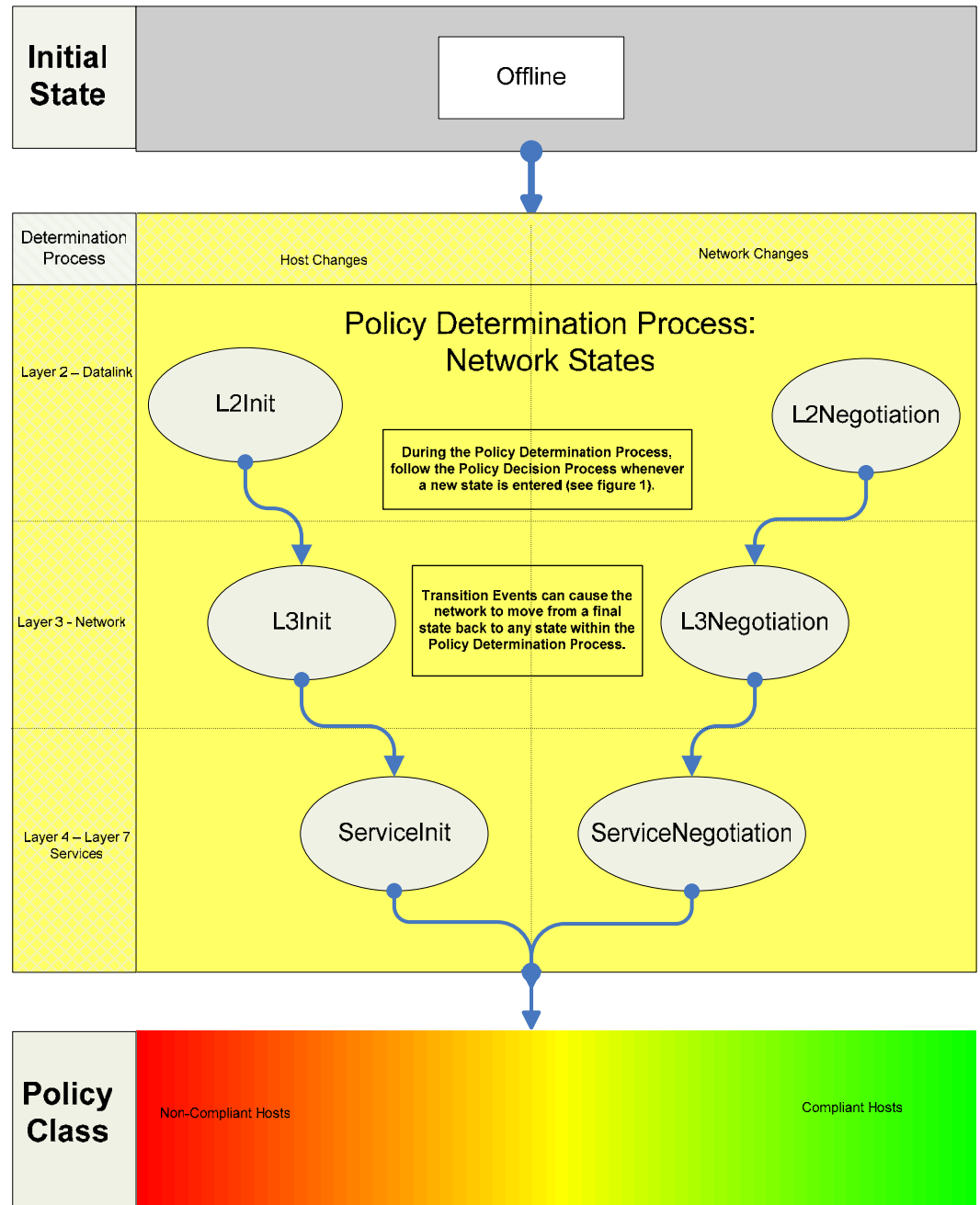
Policy determination is how the network determines whether or not a host is in compliance with network access policy



Network States

To implement network policy, hosts and networks should move through these states

Each time that a new state is entered, the network should follow the policy determination process



Components Document

- How do we apply the above model to physical (and virtual) network components
- Develop use cases and deployment scenarios
- Understand interoperability of devices
- Initial framework for possible code encouragement/development.
- Work in progress

How can you help?

- Participate in the NetAuth
 - Working group is open to all members of the Educause / Internet2 community.
 - Contribute to future documents
- These documents are still the beginning of what we hope to accomplish.

SALSA-NetAuth Working Group: Volunteers needed

- Homepage
 - <http://security.internet2.edu/netauth/index.html>
 - Draft charter
 - Mailing list
- Additional contacts
 - Steve Olshansky
 - Charles Yun
 - Christopher Misra