CICI Design Session – Trace of Policies to Rules to Logs

CICI Grant, Traceability Team (Hayes, Farrar) – Spring 2017

Personas

* Networkadmin/OpenFlow rulewriter — an IT person who writes OF programs/rules to satisfy AUP and org.policies, also bring network backup or maintain network

- Generic IT policies for network hardware - Router, antivirus, packet broker, snort, QRadar

* CTO — write AUP

* Dept CTO — write org. rules

* User - wants to use network

User Stories

CTO
* As CTO, I want my elements to be implemented in the network so that it is safe.
*As a CTO, I want to update the AUP so it is reflective of state of the art security doctrine.

Dept CTO
*As Dept CTO, I want my org. policies to "satisfy" the applicable AUP elements to that Univ. policies are met and network is safe.
*As Dept CTO, I want to update org. policies so they are reflective of state of the art security doctrine

User
* As a user, I want to be able to access network resources so that I can perform work

Network Admin
*As a network admin, I want to "write" Open Flow rules/programs so that org. policies and AUP elements are implemented and so that the network is safe.

Start

Import Nodes

Import Switches

Import Dhcp

Do the Lookups

Network.json

End

Check Org Policy against AUP

Check OF rules against org policy

Check OF rules against AUP

Dept CTO/Netw Admin

Check log against OF rules

Logs

Entries
Date & Time
Length
Type

ODC
IPAddress

DHCP

Radius

User
group membership
ID

OFrules

AUP

Org Policy

Elements

Elements