User-Group-based Security Policy for Capability Layer

draft-you-i2nsf-user-group-policy-capability-00

Presenter: John Strassner

Jianjie You (youjianjie@huawei.com)
John Strassner (john.sc.strassner@huawei.com)
Myo Zarny (myo.zarny@gmail.com)
Christian Jacquenet (christian.jacquenet@orange.com)
Sumandra Majee (S.Majee@f5.com)
Capability Interface

• Recall that a Capability
  – “ Defines a set of features that are available from a managed entity” (from draft-ietf-i2nsf-terminology-01)
  – Therefore, there should be no difference in defining consumer vs provider Capabilities
  – There IS a difference in how they are used

*Capability Info Model will be MERGED, but Capability DATA Model will be needed*
Motivation


draft-you-i2nsf-user-group-based-policy-02

draft-you-i2nsf-user-group-policy-capability-00
Option 1: Using Packet User-Group Labels

- Insert User-Group Label (UGL) into the packet
- Make forwarding decisions based on UGL
- Remove UGL

- Provide mapping policy between the n-tuple and User-Group ID
- Security policies based on user group identity

Security Controller

User-group-ID-capable domain

Ingress

NSF #1

NSF #2

...

NSF #n

Egress
Option 2: Using User-Group IDs Directly

- Identify appropriate fields in a packet, map them to a User-Group

Security Controller

- Provide mapping policy between the n-tuple and User-Group ID
- Security policies based on user group identity

User-group-ID-capable domain

Ingress
NSF #2
NSF #1
...
NSF #n
Egress
ECA for User-group-based Security Policy
ECA Policy Rule Paradigm

◆ Event
  ➢ external stimuli, such as alarms, user actions (e.g., logon and logoff, or access requests), and packet arrival or departure occurrences.

◆ Condition
  ➢ n-tuple of the incoming packet
  ➢ cross checking with other data, such as correlation with packets received from different ports or past time, or
  ➢ the current state of a flow

◆ Action
  ➢ Traffic-rate Action
  ➢ Traffic-detail Action
  ➢ Redirect Action
  ➢ Traffic-marking Action
Next Steps

• Solicit comments and suggestions on the mailing list
Thank you!