A Policy-based Network Access Control

draft-ma-opsawg-ucl-acl-03

Qiufang Ma (Huawei)  Presenter
Qin Wu (Huawei)
Mohamed Boucadair (Orange)
Daniel King (Lancaster University)
Recap——Motivation and Goal

• Motivation: Conventional address based network access control is insufficient in the expression of real-world enterprise network access
  • Mobile office makes the IP addresses of employees change.
  • different security policies need to be applied to the same set of users under different circumstances (e.g., access location, user’s role, time-of-day, corporate device vs. BYOD, etc)

• Solution Overview: provides enforcement of NAC based on the group identity.
  • Access policies based on group identity are pre-determined and static
  • The group the user is assigned is dynamically determined during authentication
High-level Document Updates

• Thank you Joe, Michael, Adrian for review and valuable comments!

• Define a common schedule YANG module and reuse it in UCL module to support date and time based policy activation condition

• Extend ACL module to support a generalized endpoint-group to cover both users (e.g., enterprise employees) and devices (e.g., enterprise IoT devices, servers)

• Simplify the definition of endpoint group in UCL module

• Generalize the group-based ACL without limiting whether it can be used at network or device level

• Add usage examples

• Thorough editorial improvement
YANG Model Update

module: ietf-ucl-acl
augment /acl:acls/acl:acl/acl:aces/acl:ace/acl:matches:
  +--rw (user-control-groups)? {match-on-user-group}?
    +--:(source-match)
      |  +--rw source-match
      |  |  +--rw (match)?
      |  |  |  +--:(user-group)
      |  |  |  |  +--rw user-group-id? uint32
      |  |  |  |  +--:(IP-address)
      |  |  |  |  |  +--rw ipv4-network? inet:ipv4-prefix
      |  |  |  |  +--rw ipv6-network? inet:ipv6-prefix
    +--:(destination-match)
    +--rw destination-match
    +--rw (match)?
    +--:(user-group)
      |  +--rw user-group-id? uint32
      |  +--:(IP-address)
      |  |  +--rw ipv4-network? inet:ipv4-prefix
      |  |  +--rw ipv6-network? inet:ipv6-prefix
augment /acl:acls/acl:acl:acl:aces/acl:ace:
  +--rw time-range {match-on-user-group}?
  +--rw (time-range-type)?
    +--:(periodic-range)
      |  +--rw month* lmap:month-or-all
      |  +--rw day-of-month* lmap:day-of-months-or-all
      |  +--rw day-of-week* lmap:weekday-or-all
      |  +--rw hour* lmap:hour-or-all
    +--:(absolute-range)
      +--rw start-time? yang:date-and-time
      +--rw end-time? yang:date-and-time

BEFORE

• Compliant with sec.3.3.9 (period of time) and sec.3.3.10 (recurrence rule) in RFC5545, respectively;
• intended to be reusable in other scheduling contexts

NOW

• Can be used either as network model or device model
• Reuse ietf-schedule module to achieve time variant access policies
Next Steps

• Include Application as the third endpoint group type other than user and device
  • A device can run multiple applications to which different access policies are required to be applied
  • May require the device/controller to identify the application type based on traffic detection

• WG Adoption
Comments, Questions, Concerns?
Different Cases for PEP to Enforce ID/Address based ACL

The PEP which acquires both src and dst group ID from the AAA server might perform group-based ACL.

The PEP which only acquires dst group ID from the AAA server but works as the tunnel decapsulation and acquires src group ID from the nvo3 header might perform group-based ACL.

The PEP which cannot acquire src or dst group ID might perform address based ACL.

Carry the src group ID in the packet header.