A Policy-based Network Access Control

draft-ma-opsawg-ucl-acl-02

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

• Motivation: The address based access control list (ACL) are often insufficient in the expression of real-world enterprise network access

  • Mobile office makes the IP addresses of employees change frequently.

  • different security policies need to be applied to the same set of users under different circumstances (e.g., users' location, users' role, time-of-day, corporate device vs. BYOD, etc)

• Solution Overview: provides enforcement of network access control policies based on the group identity.
Document Updates since IETF 115

• Thank you Joe 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-specific level

• Add examples
Modules Overview

IETF schedule module

- Comply with sec.3.3.9 (period of time) and sec.3.3.10 (recurrence rule) in RFC5545, respectively;
- reusable in other scheduling contexts

UCL extension to the ACL model

time variant access policies, e.g., restrict access to a specific group during 8am~6pm, every workday
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 applied

• 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.