A Policy-based Network Access Control

draft-ma-opsawg-ucl-acl-00

Qiufang Ma (Huawei)
Qin Wu (Huawei)
Mohamed Boucadair (Orange)
Daniel King (Old Dog Consulting)
Problem Statement

During 8am-5pm every workday:
- Deny source IP 10.2.2.0/24 to destination youtube.com
- Deny source IP 10.223.31.0/24 to destination youtube.com
- Deny source IP 172.225.7.41/32 to destination youtube.com

During off-hours and weekends:
- Permit source IP 10.2.2.0/24 to destination youtube.com
- Permit source IP 10.223.31.0/24 to destination youtube.com
- Permit source IP 172.225.7.41/32 to destination youtube.com

The address and/or ports based access control list (ACL) are often insufficient in the expression of real-world 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, type of network device used).
Solution Overview

• Ensure enforcement of access control policies based on user-group identity:
  During 8am-5pm every workday:
  ➢ Deny source group ID sales to destination youtube.com workday
  During off-hours and weekends:
  ➢ Permit source group ID sales to destination youtube.com non-workday

• What’s a user-group?
  ➢ An identifier that represents the collective identity of a group of users
  ➢ The ones who access the network and consumes specific network services/resources.
UCL Extension to the ACL model

### User-group based ACL example

<table>
<thead>
<tr>
<th>src</th>
<th>dst</th>
<th>Finance group</th>
<th>Sales group</th>
<th>10.1.1.0/24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales group</td>
<td>permit</td>
<td>permit</td>
<td>deny</td>
<td></td>
</tr>
<tr>
<td>Visitor group</td>
<td>deny</td>
<td>permit</td>
<td>deny</td>
<td></td>
</tr>
<tr>
<td>10.1.1.1/24</td>
<td>permit</td>
<td>deny</td>
<td>permit</td>
<td></td>
</tr>
</tbody>
</table>

To realize time variant access policies, e.g., restrict access to specific websites during 8am~5pm, every workday.

To cover the following types of access control:
- U2U: user-group to user-group access
- N2N: IP address prefix to IP prefix access
- U2N: user-group to IP prefix access.

### IETF-OPSAWG Hybrid Meeting

```
module: ietf-ucl-acl
augment /acl:acls/acl:acl:aces/acl:ace/acl:matches:
     +---rw (user-control-groups)?
         +---:(source-match)
             |     +---rw (destination-match)?
             |     +---:(user-group) (match-on-user-group)?
             |         |     +---rw user-group-name? string
             |         +---:(IP-address)
             |             |     +---rw ipv4-network? inet:ipv4-prefix
             |             |     +---rw ipv6-network? inet:ipv6-prefix
             |     +---:(destination-match)
             |     +---rw destination-match
             |         +---rw (destination-match)?
             |         +---:(user-group) (match-on-user-group)?
             |             |         |     +---rw user-group-name? string
             |             |         +---:(IP-address)
             |             |             |     +---rw ipv4-network? inet:ipv4-prefix
             |             |             |     +---rw ipv6-network? inet:ipv6-prefix
         +---:(time-range)
             |     +---rw (time-range-type)?
             |         +---:(periodic-range)
             |             |         |     +---rw month* imap:month-or-all
             |             |         |     +---rw day-of-month* imap:day-of-months-or-all
             |             |         |     +---rw day-of-week* imap:weekday-or-all
             |             |         |     +---rw hour* imap:hour-or-all
             |             |         +---:(absolute-range)
             |             |         |     +---rw start-time? yang:date-and-time
             |             |         |     +---rw end-time? yang:date-and-time
```
Alternatives to realize group ID to address mapping

If PEP is also the user authentication device, it already maintains the mapping information.

If PEP has no user group ID information, it queries the mapping from the controller side.

### Group ID | User name | IP address          | Login time |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alice</td>
<td>10.223.32.96/32</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>Bob</td>
<td>10.223.32.64/32</td>
<td>...</td>
</tr>
<tr>
<td>2</td>
<td>Cindy</td>
<td>10.223.32.144/32</td>
<td>...</td>
</tr>
</tbody>
</table>
Comments, Questions, Concerns?