anima Y. Li
Internet-Draft L. Shen
Intended status: Standards Track Huawei Technologies
Expires: December 30, 2021 June 28, 2021

Autonomic IP Address To Access Control Groups Mapping
draft-yizhou-anima-ip-to-access-control-groups-00

Abstract

This document defines the autonomic technical objectives for IP address/prefix to access control groups mapping. The objectives defined can be used in Generic Autonomic Signaling Protocol (GRASP) to make the policy enforcement point receive IP address and its tied access control groups information directly from the access authentication points and then execute the group based policies.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Ubiquitous group based policy management makes sure that the users can obtain the same network access permission and QoS assurance wherever they access the campus network. That is, the permission and QoS assurance are tied to user role, rather than access points and/or IP address assigned.

Group means a number of endpoints connecting to the network that share common network policies. It facilitates the easy design and provision of policy. A user's role is usually a group indicated by a group ID. Group based policy management has been replacing the traditional IP address and/or port number based policy widely.

The policy enforcement point (PEP) requires the IP address/prefix and access control group mapping information of user in order to execute the group based policy. This mapping information is usually first available at the access authentication point (AAP) during the procedures of user access and authentication/authorization. However PEP may not be the access authentication point. Therefore IP and group mappings has to be passed to PEP.

This document defines the autonomic technical objectives for IP address/prefix and access control group mapping. In this document, group is also used for short to refer to the access control group. The Generic Autonomic Signaling Protocol (GRASP) [RFC8990] can make use of these technical objectives as the basic building blocks of a ubiquitous group based policy management solution, especially for a campus network.

Autonomic Networking Infrastructure (ANI) is designed to provide the elementary functions and services to be further integrated and used by Autonomic Service Agents (ASA) on nodes. The campus policy management ASA can integrate the function introduced in this document when necessary.

2. Terminologies

This document uses terminology defined in [RFC7575].

PEP: Policy Enforcement Point. A logical entity that enforces policy decisions [RFC3198]. The policy decisions are group based policies in this document.

AAP: Access Authentication Point. A logical entity that obtains the information of the attaching clients' assigned IP address/prefix and their access control groups. AAP may get the information from one or different resources, for example, DHCP [RFC2131] [RFC8415] server and/or RADIUS [RFC3198] server.

3. Problems

The traditional policy in a campus network is normally presented as IP prefix/address based, for example, "Deny the traffic from IP prefix X to IP prefix Y". Each of the access port of the switches is assigned a subnet prefix and each subnet implies a group. It works well when the end hosts are static. With the increasing deployment of wireless accessed users and more complicated and dynamic requirements of campus network policy, such an assumption no longer hold. For instance, a user from the engineering department may bring the laptop to access the campus network via a WiFi access point. Then it will be assigned an IP address from a different subnet prefix from the other fixed end hosts in the same engineering department. It is hard and tedious to provision the consistent policy with the other hosts in the same group for this specific IP address. Another example is a user can belong to more than one group, say group of department A and also VIP group. Group assignment is much more flexible than subnet defined IP address assignment.

Therefore group based policy is used in such cases. No matter what IP address is assigned to the user, its belonging access control groups have no change and the group based policies has no change too. For example, the policy can be "Allow the traffic from group engineering to group testing, and assign the traffic destined to VIP group the highest priority". In order to make group based policy work, the IP address and its group mapping information has to be stored on PEP so that IP addresses carried in data packet can be mapped to the group ID first and then the policy can be enforced.

IP and group mapping information is usually first available at the access authentication point (AAP). Figure 1 show a typical campus network. The policy enforcement point (PEP) can be core switches, while the access authentication point (AAP) is the access switch in the figure. AAP serves as the DHCP relay which remembers the IP address assigned to the client and/or at the same time it talks to AAA server to get the client's group information based on client's identity.

```
       +-------+     +-------+
       | core1 | --- | core2 |               core switches (PEP)
       +-------+    /+-------+
        |  \       /  |     \
        |   \     /   |      \
        |    \   /    |       \
        |     \ /     |        \
        |      \      |         \
    +-------+ / \ +-------+   +-------+
    | acc1  |/   \| acc2  |   | acc3  |        access switches
```

```
    +--------+    +--------+  +--------+           (AAP)
                                   |
                                   |
                                   |
                                   |
                               +--------+
                               | WiFi   |
                               | AP1    |      wifi access point
                               +--------+
```

Figure 1: Hierarchical Campus Network

A more complex campus network is shown in Figure 2. There are 4 PEPs are deployed at the key positions for different types of traffic. The AAPs obtaining a user's IP and group ID mapping information are access switches (not fully shown in the figure) which are the access nodes for the attaching clients.

The problem to be solved by Autonomic Networking here is how to make IP address/prefix and access control group mapping information available at PEP from AAP.

```
                            via SSL VPN tunnel     -----
                           +--------+            /       \
                           | user2  |-----------+Internet |
                           |(group1)|           |         |
                           +--------+            \-------/
                                                     |
                                                     |
                                                     |
                               +---------------------|--------+
           -----               |                     |        |
         /       \             |  +--------+     +--------+   |
        |   WAN   | --------------|  WAN   |     |SSL VPN |   |
        |         |            |  | border |     |Internet|   |
         \-------/             |  |firewall|     |gateway |   |
             |                 |  +--------+     +--------+   |
             |                 |      |PEP3         | PEP2    |
             |                 |      |        +-----+        |
      +------|---------+       |      |        |              |
```

```
      |      |         |       |  +---------+   | +---------+ |
      |  +---------+   |       |  | core    |---+ |         | |
      |  |  core   |   |       |  | switch  |-----|firewall | |
      |  | switch  |   |       |  +---------+     +---------+ |
      |  +---------+   |       |      |            PEP1       |
      |      |PEP4     |       |      |                       |
      |      |         |       |      |                       |
      |      |         |       |  +---------+     +---------+ |
      |  +---------+   |       |  | switch  | --- | switch  | |
      |  | switch  |   |       |  +---------+     +---------+ |
      |  +---------+   |       |      |                |      |
      |      |         |       |      |                |      |
      |      |         |       |  +---------+     +---------+ |
      |  +---------+   |       |  | user1   |     | user3   | |
      |  | user4   |   |       |  |(group1) |     |(group2) | |
      |  |(group2) |   |       |  +---------+     +---------+ |
      |  +---------+   |       |                              |
      |                |       |                              |
      |                |       |                              |
      |Branch          |       | Headquarter                  |
      +----------------+       +------------------------------+
```

Figure 2: Campus Networks with remote access

Some deployment uses a centralized controller to solve this problem. Every single AAP reports its IP and group ID mapping information to the controller. When a PEP receives a data packet, it queries the controller for the group IDs of the source and/or destination IP addresses and then enforce the group based policy. This approach requires an explicit controller able to talk to each and every AAP and PEP. In the deployment where the headquarter and branch campus networks are far apart, it will require controllers for each site to exchange information or have another super-controller to help exchange the information among sites. It introduces the complexity and interoperability issues.

Autonomic Networking (AN) puts the intelligence at the node level, to minimize dependency on human administrators and central management such as a controller. The Autonomic Networking approach discussed in this document is based on the assumption that there is a generic discovery and negotiation protocol that enables direct negotiation between the routers or switches. GRASP [RFC8990] is intended to be such a protocol which can make use of the technical objectives defined in the following sections as the basic building blocks of a ubiquitous group based policy management solution, especially for a campus network. The ultimate goal is self-management of campus networks which can expand over multiple sites and share the same set of policies, including self-configuration, self-optimization, self-healing and self-protection (sometimes collectively called self-X).

4. Autonomic IP Address to Access Control Groups Mapping Procedures

An Autonomic Service Agent (ASA) participates in IP address/prefix to access control groups mapping is called IPAddressToAccessControlGroups ASA in this document. The procedures carried out by IPAddressToAccessControlGroups ASA is illustrated below.

4.1. Behaviours of IP Address to Access Control Groups Mapping Requesting Nodes

IPAddressToAccessControlGroups requesting node is usually a PEP in a domain which executes the group based policy. So it needs to map an IP address/prefix to one or more group IDs first. Such mapping information will be stored locally until either timeout or withdrawn.

The request can be triggered by a data packet. Group based policy requires both the source and destination group IDs which are normally mapped from source and destination IP addresses. If any of such mapping is not locally available, the requesting node needs to ask for it. In some implementation, data packet encapsulation includes the source group ID directly such as in the reserved field in VXLAN

[RFC7348]. Therefore it is up to the requesting node to determine if both source and destination groups or only one of them to be queried. In some cases that the requesting node is a tunnel endpoint, it should be noted that usually the inner rather than outer IP addresses are to be used to query for the corresponding group id.

The request can also be sent periodically or voluntarily. It can happen when a newly booted requesting node wants to get the whole batch of IP address and access control group mapping information or when a requesting node would like have an explicit refreshment on the information.

The IPAddressToAccessControlGroups ASA should send out a GRASP Discovery message that contains a IPAddressToAccessControlGroups Objective option in order to discover peers supporting this option. The requesting ASA acts as a GRASP synchronization initiator by sending a GRASP Request message with a IPAddressToAccessControlGroups Objective option. The ASA indicates an IP prefix or address in this option. This starts a GRASP synchronization process.

4.2. Behaviours of IP Address to Access Control Groups Mapping Providing Nodes

IPAddressToAccessControlGroups providing node is usually an AAP of a user in a domain. It obtains the mapping of IP address and group IDs of an endpoint in various ways. For instance, use RADIUS [RFC2865] or CAPWAP [RFC5415] to get the user's access control group IDs during authentication phase and/or use DHCP snooping to get the user's assigned IP address. Sometimes such mapping information can be statically provisioned based on port or VLAN. The mapping information is stored locally on AAP.

A device that receives a Discovery message with a IPAddressToAccessControlGroups Objective option should respond with a GRASP Response message if it contains a IPAddressToAccessControlGroups ASA. When this ASA receives a subsequent Request message, it should reply with a GRASP Synchronization messages. The Synchronization messages carry a IPAddressToAccessControlGroups Objective option, which will indicate the mappings between the IP address/prefix and group IDs. Optionally the expiration time can be tied to each mapping.

The IP address to access control groups mapping providing node can send the Flood Synchronization message if it has any update or withdraw regarding its providing mapping information.

The providing nodes of address to access control groups mapping information are usually at the edges and can be added or replaced

with the expansion of the network. The requesting nodes are normally aggregation or core nodes with more storage and capability to enforce the policy. Therefore the number of mapping information providing nodes is usually more than the number of requesting nodes. The providing node can be the one initiating the GRASP Discovery message as well and/or send the unsolicited Synchronization message [I-D.ietf-anima-grasp-distribution].

5. Autonomic IP Address to Access Control Groups Objectives

This section defines the GRASP technical objective options that are used to support autonomic IP address/prefix to access control groups mapping.

5.1. IPAddressToAccessControlGroups Objective Option

The IPAddressToAccessControlGroups Objective option is a GRASP objective option conforming to [RFC8990]. The name of this option is "IPAddressToAccessControlGroups". It carries the IP prefix/address and its mapping access control group id. The format of IPAddressToAccessControlGroups Objective option in CBOR (Concise Binary Object Representation [RFC8949]) is show in Concise data definition language (CDDL) [RFC8610] as follows. Tags for general IPv4 and IPv6 addresses and prefixes defined in [I-D.ietf-cbor-network-addresses] are used.

```
objective = ["IPAddressToAccessControlGroups",
             objective-flags, loop-count,
             [ip-address-or-prefix, *group-id]]

group-id = uint

; copied from draft-ietf-cbor-network-addresses, RFC YYYY TBD:

ip-address-or-prefix = ipv6-address-or-prefix/ipv4-address-or-prefix

ipv6-address-or-prefix = #6.54(ipv6-address / ipv6-prefix)
ipv4-address-or-prefix = #6.52(ipv4-address / ipv4-prefix)

ipv6-prefix = [ipv6-prefix-length, ipv6-prefix-bytes]
ipv4-prefix = [ipv4-prefix-length, ipv4-prefix-bytes]

ipv6-prefix-length = 0..128
ipv4-prefix-length = 0..32

ipv6-prefix-bytes = bytes .size (uint .le 16)
ipv4-prefix-bytes = bytes .size (uint .le 4)

ipv6-address = bytes .size 16
ipv4-address = bytes .size 4

; copied from the GRASP specification, RFC 8990:

   objective-flags = uint .bits objective-flag

   objective-flag = &(
     F_DISC: 0    ; valid for discovery
     F_NEG: 1     ; valid for negotiation
     F_SYNCH: 2   ; valid for synchronization
     F_NEG_DRY: 3 ; negotiation is a dry run
   )
   loop-count = 0..255
```

A common practice currently usually uses 16 bits to present a group ID. But the representation does not limit that. Zero group ID would be used for full retraction of a prefix or address.

6. Security Considerations

Security consideration for GRASP [RFC8990] applies in this document. The preferred security model is that devices are trusted following the secure bootstrap procedure [RFC8995] and that a secure Autonomic Control Plane (ACP) [RFC8994] is in place.

7. IANA Considerations

This document defines a new GRASP Objective option name: "IPAddressToAccessControlGroups". The IANA is requested to added it to the "GRASP Objective Names" subregistry defined by [RFC8990].

8. Acknowledgements

Thanks to Carsten Bormann, Brian Carpenter and Michael Richardson for useful suggestions and revising CDDL representations.

9. References

9.1. Normative References

[RFC7575] Behringer, M., Pritikin, M., Bjarnason, S., Clemm, A., Carpenter, B., Jiang, S., and L. Ciavaglia, "Autonomic Networking: Definitions and Design Goals", RFC 7575, DOI 10.17487/RFC7575, June 2015, <https://www.rfc-editor.org/info/rfc7575>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

[RFC8990] Bormann, C., Carpenter, B., Ed., and B. Liu, Ed., "GeneRic Autonomic Signaling Protocol (GRASP)", RFC 8990, DOI 10.17487/RFC8990, May 2021, <https://www.rfc-editor.org/info/rfc8990>.

[I-D.ietf-anima-grasp-distribution] Liu, B., Xiao, X., Hecker, A., Jiang, S., Despotovic, Z., and Brian, "Information Distribution over GRASP", draft-ietf-anima-grasp-distribution-02 (work in progress), March 2021.

[I-D.ietf-cbor-network-addresses]

Richardson, M., "CBOR tags for IPv4 and IPv6 addresses and prefixes", draft-ietf-cbor-network-addresses-04 (work in progress), April 2021.

9.2. Informative References

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC3198] Westerinen, A., Schnizlein, J., Strassner, J., Scherling, M., Quinn, B., Herzog, S., Huynh, A., Carlson, M., Perry, J., and S. Waldbusser, "Terminology for Policy-Based Management", RFC 3198, DOI 10.17487/RFC3198, November 2001, <https://www.rfc-editor.org/info/rfc3198>.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <https://www.rfc-editor.org/info/rfc5415>.

[RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", RFC 7348, DOI 10.17487/RFC7348, August 2014, <https://www.rfc-editor.org/info/rfc7348>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

[RFC8994] Eckert, T., Ed., Behringer, M., Ed., and S. Bjarnason, "An Autonomic Control Plane (ACP)", RFC 8994, DOI 10.17487/RFC8994, May 2021, <https://www.rfc-editor.org/info/rfc8994>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

Appendix A. Objective Examples

This appendix shows a number of examples of objective defined in this document conforming to the CDDL syntax given in Section 5.1.

```
["IPAddressToAccessControlGroups", 15, 101,
   [54([4, h'A50386A78BA56FA4BBC734281C51']), 3506, 2698, 4562]]

["IPAddressToAccessControlGroups", 5, 73, [52(h'9946B8A3'), 2881,
           2265, 1720, 2450]]

["IPAddressToAccessControlGroups", 15, 161,
           [54(h'39F3045B641AD291B057CD1857A7314A')]]

["IPAddressToAccessControlGroups", 15, 2, [52(h'98A1CE4F')]]

["IPAddressToAccessControlGroups", 15, 66, [52(h'69A16BFE'), 2601,
           1851, 3876, 1405]]

["IPAddressToAccessControlGroups", 15, 254,
  [54(h'38AB303B8895DC95068CE00248D2FE91'), 4019, 1166, 3113]]

["IPAddressToAccessControlGroups", 15, 63, [52([4, h'0B48']), 3035,
           1181]]
```

```
["IPAddressToAccessControlGroups", 15, 44, [52(h'01F1D8FF'), 3099,
           1577, 1138, 1670]]

["IPAddressToAccessControlGroups", 15, 181,
           [54(h'2C74719F9355BA4E3BDE5689D1FE4CB0')]]

["IPAddressToAccessControlGroups", 15, 129, [52(h'A2EF97C7'), 3149,
           2728]]

["IPAddressToAccessControlGroups", 15, 18,
   [54(h'CD3868615B00D72A61A028822FEE6407'), 1832, 4605, 360, 3030]]

["IPAddressToAccessControlGroups", 15, 171,
           [54(h'46929AE1103FDF6407A239323F71C234')]]

["IPAddressToAccessControlGroups", 15, 42, [52([7, h'8E05'])]]

["IPAddressToAccessControlGroups", 15, 180,
           [54([41, h'2D85855FA9C3772AAB2F']), 672, 1205]]
```


Authors' Addresses

Yizhou Li
Huawei Technologies

Email: liyizhou@huawei.com

Li Shen
Huawei Technologies

Email: kevin.shenli@huawei.com