Autonomic IP to Access Control Group Mapping

draft-yizhou-anima-ip-to-access-control-groups

Presenter: Yizhou Li

IETF111
Usage scenarios – background of group based policy

• Traditional (pre-known VLAN/subnet + ACL) based access control is relatively static in the campus network
  • Tie the same group of hosts by assuming they are accessing from a pre-assigned switch/ports/VLAN/subnet --- not any more.
  • Most provisioning uses pre-assigned IP/prefix as source/destination IP in matching rule, like in ACL or prioritized forwarding at the exit point --- a big burden of provision and maintenance when an end host IP/prefix is not known upfront.

• Group based policy is being widely used as a replacement
  • Groups and rules based on groups can be provisioned in advance and irrespective of end user’s IP/prefix
  • Require the policy execution point to locally have IP/prefix to access control group mapping info to check against the data packet.
Example topology 1 – simple case

Two Terms:
- **PEP**: Policy Enforcement Point.
  - Places to put PEP vary: scale, simplicity, single/dual homed uplink, L2/L3 topology, node capability....
  - Highly centralized: only at core layer
  - Highly distributed: at every access switches
- **AAP**: Access Authentication Point.
  - Responsible for its attaching end users.
  - Places to put AAP also vary
  - Obtain the IP address/prefix information, e.g. via DHCP snooping, proxy, prefix-delegation, configs
  - Obtain the group (ID) information, e.g. via 802.1x+AAA
  - Keep the (IP, group) bindings

Requirement: PEPs get IP to group info from AAP
- PEP and AAP on different nodes
- PEP requires full set info (src, dest) while each AAP may only have a subset of info for its responsible end hosts
Example topology 2 – more complex case

- PEPs are located at different places
- Specific traffic can be directed to certain PEP, e.g. PEP1 is for intra HQ traffic.
- More complex group definition and policy enforcement rules
- Requirement: PEPs get IP to group info from AAP
Proposal: define new GRASP objective

• To distribute IP address/prefix to access control group IDs mapping info from AAP to PEP

```plaintext
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
```
Procedures

• Providing Node: AAP
  • Send unsolicited Synchronization to PEP upon a new/updated/withdrawn binding
  • Send Synchronization as a response to the Request

• Requesting node: PEP
  • Send a Request for binding info when the source or destination group is either unavailable from data packet directly or no hitting entry from local stored info
  • May send Request periodically or voluntarily, e.g. before local entry timeout, re-booting...
To be discussed

• Can PEP1 respond PEP2?

If the responding node can be PEP, PEP is usually not the owner of the binding info.
• Inconsistent info may occur?
• Add a parameter like “confidence level”?
• PEP decides if request should be further passed down?
Next Steps

• Revise the document based on the comments
• Suggestions are welcome to the mailing list or to me (liyizhou@huawei.com)