Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 22, 2016

E. Lear
Cisco Systems

January 19, 2016

Using DNS Names in the IETF ACL Model
draft-lear-ietf-netmod-acl-dnsname-00

Abstract

End points are commonly referenced by higher level functions through the DNS. This is especially the case in cloud-based functions, which might have hundreds of IP addresses for the same name. This brief memo extends the IETF-ACL model to allow access-control via domain names.

Status of This Memo

This Internet-Draft will expire on July 22, 2016.

Copyright Notice

Table of Contents

1. Introduction

The IETF-ACL model [I-D.ietf-netmod-acl-model] specifies a schema for access lists. That model is intentionally kept constrained to the small number of packet-passing functions that are considered ubiquitous. While that is a necessary step, there are a number of circumstances in which it will not be sufficient. In a world where load balancing and shifting commonly takes place, it may not be practical to maintain the complete list of IP addresses in all instances. Furthermore, even in more static environments, occasionally the name to address mapping needs to change. Lastly, there are resources that may not be tied to packet processing at all that may yet be well described by this augmentation. Allowing domain names in ACLs reduces the number of points within a network that need to be reconfigured when such changes take place.

This memo specifies an extension to IETF-ACL model such that domain names may be referenced by augmenting the "matches" element. Different implementations may deploy differing methods to maintain the mapping between IP address and domain name, if indeed any are needed. However, the intent is that resources that are referred to using a name should be authorized (or not) within an access list.

The structure of the change is as follows:

```
augment
/acl:access-lists/acl:acl/acl:access-list-entries
   /acl:ace/acl:matches/acl:ace-type/acl:ace-ip:
   +--rw source-dnsname?        inet:host
   +--rw destination-dnsname?   inet:host
```

The choice of this particular point in the access-list model is based on the assumption that we are in some way referring to IP-related

resources, as that is what the DNS returns. A domain name in our context is defined in [RFC6991].

2. Element Definitions

The following elements are defined.

2.1. source-dnsname

The argument corresponds to a domain name of a source as specified by inet:host. Depending on how the model is used, it may or may not be resolved, as required by the implementation and circumstances.

2.2. destination-dnsname

The argument corresponds to a domain name of a destination as specified by inet:host. Depending on how the model is used, it may or may not be resolved, as required by the implementation and circumstances.

3. The ietf-acl-dnsname Model

```
<CODE BEGINS>file "ietf-acl-dnsname.yang";

module ietf-acl-dnsname {
  yang-version 1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-acl-dnsname";
  prefix "ietf-acl-dnsname";


  import ietf-access-control-list {
    prefix "acl";
  }

  import ietf-inet-types
  {
    prefix "inet";
  }

  organization
    "Cisco Systems, Inc.";

  contact
    "Eliot Lear
     lear@cisco.com
    ";

  description
```

```
       "This YANG module defines a component that augments the
        IETF description of an access list to allow dns names
        as matching criteria.";

     revision "2016-01-14"  {
       description "Initial revision";
       reference "This document?";
     }

     augment "/acl:access-lists/acl:acl/" +
        "acl:access-list-entries/acl:ace/" +
        "acl:matches/acl:ace-type/acl:ace-ip" {
       description "adding domain names to matching";

       leaf source-dnsname {
         type inet:host;
         description "domain name to be matched against";
       }
       leaf destination-dnsname {
         type inet:host;
         description "domain name to be matched against";
       }
     }

   }

   <CODE ENDS>
```

4. Example

The following example is taken from [I-D.ietf-netmod-acl-model] (the optional and irrelevant components have been removed). It allows traffic from www.cloud.example.com.

```
<?xml version='1.0' encoding='UTF-8'?>
  <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <access-lists
   xmlns="urn:ietf:params:xml:ns:yang:ietf-access-control-list"
  xmlns:ietf-acl-dnsname="urn:ietf:params:xml:ns:yang:ietf-acl-dnsname">
       <acl>
        <acl-oper-data />
        <access-list-entries>
          <ace>
            <matches>
          <source-dnsname>
             www.cloud.example.com
          </destination-dnsname>
            </matches>
            <actions>
              <permit />
            </actions>
            <rule-name>rule1<rule-name/>
          </ace>
        </access-list-entries>
        <acl-name>sample-dns-acl<acl-name/>
        <acl-type>ipv4-acl<acl-type/>
      </acl>
    </access-lists>
  </data>
```

5. Security Considerations

If the mapping between a domain name and the underlying resource to which it refers becomes stale, the access list will be incorrect. It is therefore important that implementations employ some means for maintaining the mapping, if it is required. In those circumstances, when other systems are in play, those other systems would be required to indicate what domains they are attempting to connect to. Under the current circumstances, this is readily observable. However, in future such information sharing may raise privacy concerns, and the name and mapping may not be available to the system employing the ACL model.

6. IANA Considerations

The IANA is not requested to make any changes. The RFC Editor is requested to remove this section prior to publication.

7. Acknowledgments

The author wishes to acknowledge Kiran Koushik and Einar Nilsen-Nygaard for their review and contributions to this work.

8. Normative References

[I-D.ietf-netmod-acl-model]
Bogdanovic, D., Koushik, K., Huang, L., and D. Blair, "Network Access Control List (ACL) YANG Data Model", draft-ietf-netmod-acl-model-06 (work in progress), December 2015.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <http://www.rfc-editor.org/info/rfc6991>.

Author's Address

Eliot Lear
Cisco Systems
Richtistrasse 7
Wallisellen CH-8304
Switzerland

Phone: +41 44 878 9200
Email: lear@cisco.com