Inter-Cloud DDOS API Yang Model
draft-hares-i2nsf-ddos-yang-dm-00.txt

Abstract

This document defines a yang model that enables two Cloud providers to exchange DDoS based on Inter-Cloud DDoS Mitigation API [draft-fang-i2nsf-inter-cloud-ddos-mitigation-api-01].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 9, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

[I-D.ietf-i2nsf-problem-and-use-cases] proposes two different types of interfaces:

- North-bound interface (NBI) provided by the network security functions (NSFs)
- Interface between I2NSF user/client with network controller:

Cloud Providers need to have a NBI to the network security functions that can share DDoS information.

This document defines a yang data models based [I-D.fang-i2nsf-inter-cloud-ddos-mitigation-api] using the Yang model to provide the interface. This yang data module uses the ietf-i2nsf-capability model found in [draft-hres-i2nsf-capability-yang] which is based on the informational model found in on the [I-D.xia-i2nsf-capability-interface-im], and initial work done in [I-D.xia-i2nsf-service-interface-dm]. Terms used in document are defined in [I-D.ietf-i2nsf-terminology].
This yang data model assumes the inter-cloud interface looks like this:

Cloud-Provider-1          Cloud Provider 2
[client-software]<------>[agent software]
[agent-software] <-------->[client software]

The client-software reads/writes the data in the remote cloud environment. The agent software responds with information on this cloud.

[I-D.xia-i2nsf-capability-interface-im] defines the following type of functionality in NSFs.

- network security control
- content security control, and
- attack mitigation control

This document contains high-level yang for each type of control. The features in each section have been built up from the following sources:

- open-source: firewalls, IDS, IPS. This includes ECA policy for
- basic-firewalls: in router, switches, firewalls,
- firewall products commercial level
- specialized devices IDS, IPS

2. Using this Yang module to implement the Inter-Cloud API

This yang module can be used by a clouder provider to consume another cloud provider’s services, or to provide services for another cloud provider. For example, Cloud Provider A can be a consumer of Cloud Provider B via logical interface link 1 (shown in figure 1 below). Cloud Provider B can be a consumer of Cloud Provider A via logical link 2.
The yang module provides a list of cloud-provider structures indexed by name. Within the cloud-provider structure there is a name (e.g. Cloud Provider A), and API types (consumer or provider or both), and security identity key. These features allow the

```

Cloud Provider A                  Cloud Provider B

+-------------------+                 +-------------------+
| Inter-Cloud       |                  | Inter-Cloud       |
| consumer          |                  |                   |
+-------------------+-------------------+
| DDoS Manager +1----+ DDos Manager |
| /cloud-           | provider /cloud-  |
| provider          | provider          |
| [A][B]            | [A][B]           |
+-------------------+-------------------+

Figure 1: Two cloud providers using Inter-Cloud DDoS API via yang module

Hares & Moskowitz Expires January 9, 2017
3. Inter-Cloud DDOS Yang Module

This section describes the Inter-Cloud DDOS Yang module. This section includes the following:

- high-level yang for ietf-i2nsf-cloud-DDoS yang module,
- mapping of Inter-Cloud API ([I-D.fang-i2nsf-inter-cloud-ddos-mitigation-api]) to specific Yang structures and NETCONF/RESTCONF function. The NETCONF/RESTCONF functions include NETCONF/RESTCONF calls, publication/subscription (pub/sub) push functional (I2RS requires pub/sub), and opstate.
- Overview of module utilized by ietf-i2nsf-cloud-DDoS yang module

3.1. High-level Yang modules

The this section has the high-level yang for ietf-i2nsf-cloud-ddos module. This module references the following submodules contained in this draft: cfg-cloud-mitigate-policy, cfg-mitigate-monitoring, i2nsf-capabilities, and cloud-mitigate-opstate.

Other data models that this module depends on are described in the next section.

- ietf-i2nsf-capability module [I-D.hares-i2nsf-capability-yang] (which is based on the information model in [I-D.xia-i2nsf-capability-interface-im])
- ietf-pkt-eca module in [I-D.ietf-i2rs-pkt-eca-data-model], and
- ietf-fb-rib module in [I-D.ietf-i2rs-fb-rib-data-model].

3.1.1. ietf-i2nsf-cloud-ddos Main module

ietf-i2nsf-cloud-ddos
  +--rw i2nsf-intercloud-ddos
    +--rw cloud-provider* [name]
      +--rw cloud-name string;
      +--rw cloud-api-type identitref
      +--rw cloud-sec-id uint64
    +--rw Inter-Cloud-DDoS-capabilities
      |    +--rw capability-query boolean
      |    +--rw mitigation-req boolean
      |    +--rw monitor-report boolean
      |    +--rw monitor-parms boolean
      |    +--rw knowledge-share boolean

Hares & Moskowitz Expires January 9, 2017 [Page 5]
Figure 1: ietf-i2nsf-cloud-DDos Model
High level yang structure

3.1.2. cfg-cfg-cloud-mitigate-policy sub-module
Figure 2: Configured cloud mitigation policy
High level yang structure

3.1.3. Operational state (cloud-mitigation_opstate)
```plaintext
+++ro cloud-mitigate_opstate
  +++ro stats-reset-id  uint64
  +++ro support-opstate [stats-pull-id]
   |  +++ro traffic-cnts  boolean
   |  +++ro mitigation-cnts boolean
   |  +++ro sflow-monitoring boolean
   |  +++ro share-blacklist boolean
   |  +++ro traffic-cnts
   |     +++ro pkts-matched uint64
   |     +++ro bytes-matches uint64
   |     +++ro mitigation-cnt
   |     +++ro hit-flood-rate-limit uint64
   |     +++ro used-sync-mitigation uint64
   |  +++ro used TCP-flood  uint64
   |  +++ro used UDP-flood  uint64
   |  +++ro hit-connect-max  uint64
   |  +++ro hit-newconnect-max uint64
   |     +++ro hit-frag-packet-rate-max uint64
   |     +++ro hit-packet-rate-max uint64
   |     +++ro hit-newconnect-rate-max uint64
   |  +++ro used-blackhole  uint64
   |  +++ro used-bgp-signals uint64
   |     +++ro used-24-community  uint64
   |     +++ro used-slash-24-removal uint64
   |  +++ro bgpflowspec-stat uint64
   |     uses fb-rib:ietf-fb-rib:bgp-fb-rib
   |  +++ro knowledge-sharing
   |     +++ro current-blacklist* [blacklist-id]
   |        +++ro black-list-id uint32
   |        +++ro ipv4-address ipv4-addr
   |        +++ro ipv6-address ipv6-addr
   |        +++ro transport-port uint16
   |     (need input on black list or existing yang model with)

Figure x - Operational state

3.1.4. Configuring Montoring (cfg-mitigate-monitoring module)

Hares & Moskowitz        Expires January 9, 2017                [Page 8]
Internet-Draft              Inter-Cloud DDoS                   July 2016

+-rw cfg-mitigate-monitoring
  +-rw opstate-monitoring
    |  +-rw traffic-stats  boolean
    |  +-rw detail-stats  boolean
    |  +-rw sflow-stats  boolean
    |  +-rw share-blacklist boolean
    |  +-rw pub-sub-retrieve boolean
    |  +-rw get-retrieve boolean
    +-rw sflow-redirect [endpoint-id]
      |  +-rw endpoint-id uint64
      |     |  +--rw endpoint-name string
      |     |  +--rw sflow-enabled boolean
      |     |  +--rw endpoint-ip   ip-addr
      |     |  +--rw start-time-sec uint64 //unix time second
      |  +-rw stop-time-sec  uint64 //unix time seconds

3.1.5. rpcs for Inter-Cloud Yang Module

rpc  for Inter-Cloud Yang modules

rpc:

  +--x start-mitigation
  |  +--input
  |     |  |  +--w cloud-name string
  |     |  |  |  |  +--w cloud-api-type identitref
  |     |  |     |  |  +--w cloud-sec-id uint64
  |     |  |     |  |  +--w policy-id uint64
  |     |  |     |  |  +--w request-identifier uint64
  |     |  +--x params
  |     +--output
  |     |  |  +--w cloud-name string
  |     |  |  |  |  +--w cloud-api-type identitref
  |     |  |     |  |  +--w cloud-sec-id uint64
  |     |  |     |  |  +--w policy-id uint64
  |     |  |     |  |  +--x cfg-mitigation boolean
  |     |  |     |  |  +--ro status identityref /reject, started, done
  |     |  +--ro cfg-mitigation-type string
  |     |     |  |  |  +--ro result-params
  |     |     |  |     |  |  (choice based on type )
  +--x stop-mitigation [policy-id]
  |  +--input
  |     |  |  +--w cloud-name string
  |     |  |  |  |  +--w cloud-api-type identitref
  |     |  |     |  |  +--w cloud-sec-id uint64
  |     |  |     |  |  +--w policy-id uint64
  |     |  |     |  |  +--w request-identifier uint64
3.1.6. notifications for Inter-Cloud Yang Module

This section describes the notifications that will be needed to form the DDoS capabilities. However, these notifications are not yet in the yang module.

notifications:
  +--n inter-cloud-capability-change
  |    ...  
  +--n policy-change
  | ... 
  +--n opstate-reset
  | ... 
  +--n mitigation-failure
  | ...
3.2. Implementing inter-Cloud DDoS API with Yang module

The implementation of the actions requested in Inter-Cloud DDoS API ([I-D.fang-i2nsf-inter-cloud-ddos-mitigation-api]) are the following:

- **query DDoS capabilities:** API specifies query/response pair (per [I-D.fang-i2nsf-inter-cloud-ddos-mitigation-api] section 4.1) This is implemented with the GET in Yang module as requested in the API. (per [I-D.fang-i2nsf-inter-cloud-ddos-mitigation-api] section 4.2.11)) The first thing a Cloud provider should query is the variable: Inter-Cloud-DDoS-capabilities/capability-query. If this value is true, then respondent provides cloud-capabilities entry with all the capabilities it will expose.

  * RESTCONF: GET/GET-response with array of mitigation DDoS mitigation.
  * NETCONF: GET/GET-response with array of mitigation
  * Alternative 1: pub/sub subscription for DDoS capabilities after the initial get.

- **Mitigation:** API specifies action request/response pair on based on a a pre-arranged agreement that specifies a set of policy rules (per [I-D.fang-i2nsf-inter-cloud-ddos-mitigation-api], section 4.1.2 and section 4.2.2). This data model places the policy rules in the cfg-attack-mitigate-policy array indexed by a policy-id. The action request/response need to:

  1. acknowledge the request
  2. Execute a particular DDOS capability
  3. second response with logged actions and mitigation status

The implementation of these functions are as follows;

  * NETCONF/RESTCONF rpc "start-mitigation" provides the two responses based on activity. The rpc is described in the section below.

  * RESTCONF functions of POST, GET, PUT, DELETE provide the add/change/delete functions for a particular policy cfg-attack-mitigate-policy indexed policy id.

  * NETCONF get, edit-config, and delete provide the add/change/delete functions for a particular policy cfg-attack-mitigate-policy indexed policy id.
* Addition 1: Allow pub/sub as a mechanism for a Cloud provider to provide notifications for policy opstate to remote Cloud provider I2NSF consumer.

* Addition 2: Allow pub/sub as a mechanism for Cloud provider to report changes in policy to remote cloud provider.

Monitor and Report Mitigation: The feature provides for the monitoring and reporting of the a particular DDOS mitigation (per [I-D.fang-i2nsf-inter-cloud-ddos-mitigation-api] section 4.1.3 and section 4.2.3). This yang module utilizes the mitigation-opstate which provides a list of operational state per mitigation policy-id. The "cloud-mitigate_opstate" grouping has a "stats-reset-id" that implements an indicator if the stats have been reset. If the stats have not been reset, the counters should be monitonically increasing. The operations to handle add/change/delete for the monitoring policy are:

* RESTCONF POST, GET, PUT, and DELETE,

* NETCONF get, edit-config, and delete

* NETCONF pub/sub that indicate if the remote side has add/changed/deleted monitoring policy.

The operations to pull large amounts of monitoring data should utilize the pub/sub push facilities.

Knowledge sharing: Knowledge sharing looks to obtain remote Cloud Providers black list. This remote black list is part of the operational state retrieve (cloud-mitigate_opstate/knowledge-sharing). The knowledge-sharing capability indicates if the remote side supports this. The cfg-mitigate-monitoring grouping allows a policy to be configured to share-blacklist the black list.

4. Overview of Other Yang Modules referenced

This section review the other yang modules used by this mode. This section is provided for informational purposes. In the final revision of this yang model this section should be removed.

4.1. Filter-Based RIB data model

The filter-based RIB [I-D.ietf-i2rs-fb-rib-data-model] stores policy for flow specification configured in a node, distributed by I2RS, and received or configured by BGP peers and installed in the kernel. It is used by this model to store BGP flow specification policy received...
or locally configured so that it can be easily compared with other flow specification policy set in NSF devices.

Note: This section is provided for informational purposes. In the final revision of this yang model this section should be removed.

The High level yang for the filter-based RIB
Augments rt:logical-network-elements:
  :logical-network-element:network-instances: \
    network-instance

ietf-fb-rib module
  +--rw ietf-fb-rib
   +--rw default-instance-name string
   +--rw default-router-id rt:router-id
   +--rw config-fb-ribs
      if-feature "config-filter-based-RIB";
      uses fb-ribs;
   +--rw i2rs-fb-ribs
      if-feature "I2RS-filter-based-RIB";
      uses fb-rib-t:fb-ribs;
   +--rw bgp-fs-fb-ribs
      if-feature "BGP-FS-filter-based-RIB";
      uses fb-rib-t:fb-ribs;

ietf-fb-rib module
  +--rw ietf-fb-rib-opstate
   +--rw default-instance-name string
   +--rw default-router-id rt:router-id
   +--rw config-fb-rib-opstate
      if-feature "config-filter-based-RIB";
      uses fb-rib-t:fb-ribs-oper-status;
   +--rw i2rs-fb-rib-opstate {
      if-feature "I2RS-filter-based-RIB";
      uses fb-rib-t:fb-ribs-oper-status;
   } +--rw bgp-fs-fb-rib-opstate
      if-feature "BGP-FS-filter-based-RIB";
      uses fb-rib-t:fb-ribs-oper-status;

4.2. Packet ECA Policy

The packet eca policy yang model [I-D.ietf-i2rs-pkt-eca-data-model] is used by the filter-based RIB and the I2NSF capability model. The high level yang for this model is described below.
module ietf-pkt-eca-policy
  +--rw pkt-eca-policy-cfg
    +--rw pkt-eca-policy-set
      +--rw groups* [group-name]
        +--rw group-name string
        +--rw vrf-name string
        +--rw address-family
      +--rw group-rule-list* [rule-name]
        +--rw rule-name
        +--rw rule-order-id
        +--rw default-action-id integer
        +--rw default-resolution-strategy-id integer
      +--rw rules* [order-id rule-name]
        +--rw order-id
        +--rw rule-name
      +--rw cfg-rule-conditions [cfgr-cnd-id]
        +--rw cfgr-cnd-id integer
        +--rw eca-event-match
          +--rw time-event-match*
            .. (time of day)
        +--rw eca-condition-match
          +--rw eca-pkt-matches*
            .. (L1-L4 matches)
          +--rw eca-user-matches*
            (user, schedule, region, target, state, direction)
      +--rw cfg-rule-actions [cfgr-action-id]
        +--rw cfgr-action-id
        +--rw eca-actions* [action-id]
          +--rw action-id uint32
          +--rw eca-ingress-act*
            .. (permit, deny, mirror)
          +--rw eca-fwd-actions*
            .. (invoke, tunnel encap, fwd)
          +--rw eca-egress-act*
            ..
          +--rw eca-qos-actions*
            ..
          +--rw eca-security-actions*
      +--rw pc-resolution-strategies* [strategy-id]
        +--rw strategy-id integer
        +--rw filter-strategy identityref
          .. FMR, ADTP, Longest-match
        +--rw global-strategy identityref
        +--rw mandatory-strategy identityref
        +--rw local-strategy identityref
        +--rw resolution-fcn uint32
        +--rw resolution-value uint32
| +--rw resolution-info  string |
| +--rw associated-ext-data* |
|   | +--rw ext-data-id integer |
| +--rw cfg-external-data* [cfg-ext-data-id] |
|   | +--rw cfg-ext-data-id integer |
|   | +--rw data-type integer |
|   | +--rw priority uint64 |
|   | uses external-data-forms |

4.3.  Capability high level model

The following yang model is available in [I-D.hares-i2nsf-capability-yang] and references [I-D.ietf-i2rs-pkt-eca-data-model].

The High level yang for the data model
ietf-i2nsf-capability
  +--rw nsf-capabilities
      +--rw capability* [name]
          +--rw nsf-name string
          +--rw cfg-net-sectl-capabilities
              |  uses pkt-eca-policy:pkt-eca-policy-set
          +--rw cfg-net-sec-content-capabilities
              |  uses i2nsf-content-caps
              |  uses i2nsf-content-sec-actions
          +--rw cfg-attack-mitigate-capabilities*
              |  uses i2nsf-mitigate-caps
          +--rw ITResource [ITResource-name]
              |  uses cfg-ITResources

Figure 2: ietf-i2nsf-capabilities
High level yang structure

5. YANG Modules

TBD

6. IANA Considerations

TBD. This model will require URN assignment for yang module.

7. Security Considerations

Security concerns across-domain need to be discussed here.

8. References

8.1. Normative References

[I-D.fang-i2nsf-inter-cloud-ddos-mitigation-api]
Fang, L. and D. Bansal, "Inter-Cloud DDoS Mitigation API",
draft-fang-i2nsf-inter-cloud-ddos-mitigation-api-01 (work
in progress), March 2016.

[I-D.hares-i2nsf-capability-yang]
Hares, S. and R. Moskowitz, "I2NSF Capability Yang Model",
draft-hares-i2nsf-capability-yang-00 (work in progress),
July 2016.
8.2. Informative References

[I-D.ietf-i2nsf-gap-analysis]
Hares, S., Moskowitz, R., and D. Zhang, "Analysis of Existing work for I2NSF", draft-ietf-i2nsf-gap-analysis-00 (work in progress), February 2016.

[I-D.ietf-i2nsf-problem-and-use-cases]

[I-D.ietf-i2nsf-terminology]

[I-D.i2rs-pkt-eca-data-model]
[I-D.ietf-netmod-acl-model]

[I-D.ietf-opsawg-firewalls]

[I-D.xia-i2nsf-capability-interface-im]

[I-D.xia-i2nsf-service-interface-dm]


RFC 7277, DOI 10.17487/RFC7277, June 2014,

Authors’ Addresses

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
USA
Phone: +1-734-604-0332
Email: shares@ndzh.com

Robert Moskowitz
HTT Consulting
Oak Park, MI
USA
Phone: +1-248-968-9809
Email: rgm@htt-consult.com