

I2RS working group  
Internet-Draft  
Intended status: Standards Track  
Expires: August 18, 2014

S. Hares  
Hickory Hill Consulting  
Q. Wu  
Huawei  
February 14, 2014

An Information Model for I2RS Reading Information Policy  
draft-hares-i2rs-im-read-info-policy-00

## Abstract

The Interface to the routing system (I2RS) specifies a new interface that a client (I2RS client) can utilize to interface to the routing system. Some applications that utilize the services of I2RS client may require a specific set of data in response to network events or conditions based on pre-established rules. In order to reduce the data flow through the network, the I2RS client needs to signal the I2RS agent to filter some of the collected data or events prior to transmission to the i2rs client. This functionality is necessary to meet the requirements I2RS enabled services which include service-layer routing improvements, and control of traffic flows and exit points.

This document introduces a read-only I2RS RIB policy Informational Model that provides filters for the reads and notifications from the I2RS RIB Info Model (IM). This model utilizes a generic information model (IM) for policy templates that is extensible and hierarchical. These templates support the features described by the I2RS architectural model.

## 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 August 18, 2014.

Internet-Draft

IM for policy

February 2014

## Copyright Notice

Copyright (c) 2014 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.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Reading of Network Policy Information . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Example of Use of Read Filter Policy Information Model . . . .	<a href="#">6</a>
3.1.	Read Filtering for Distributed Reaction to Network Based Attacks . . . . .	<a href="#">6</a>
3.2.	Remote Service Monitoring . . . . .	<a href="#">11</a>
3.3.	Within Data Center Routing . . . . .	<a href="#">13</a>
3.4.	Temporary overlays between Data Centers . . . . .	<a href="#">13</a>
<a href="#">4.</a>	Read Filter Policy Information Model . . . . .	<a href="#">13</a>
4.1.	Read Filter Policies . . . . .	<a href="#">14</a>
4.2.	Generic Informational Model Templates . . . . .	<a href="#">14</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">18</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">18</a>
<a href="#">7.</a>	Informative References . . . . .	<a href="#">18</a>
	Authors' Addresses . . . . .	<a href="#">19</a>

[1.](#) Introduction

The Interface to the Routing System (I2RS) [[I-D.ietf-i2rs-architecture](#)] provides read and write access to the information and state within the routing process within routing elements. The I2RS client interacts with one or more I2RS agents to collect information from network routing systems. One set of protocol independent use cases that the I2RS interface be used in are described in [[I-D.white-i2rs-use-case](#)] Protocol Independent Use Case for the Interface. These scenarios suggest that require I2RS

interfaces to be able to:

- o monitor available routes installed based on the routes installed in a RIB for a routing instance associated with forwarding device at a near real-time rate

- o interact with various policies configured on the forwarding devices, in order to inform the policies implemented by the dynamic routing processes.
- o interact with traffic flow and other network traffic level measurement protocols and systems, in order to determine path performance, top talkers, and other information required to make an informed path decision based on locally configured policy.

Processing of collected information at the I2RS agent may require the I2RS Agent to filter certain information or group pieces of information in order to reduce the data flow through the network to the I2RS client. Some applications utilizing the services of an I2RS client may also wish to require specific data in response to network events or conditions based on pre-established policy rules. For example if the traffic flow measured by network devices exceeds some limit, then the I2RS client may wish to query for all routes with some match pattern. This will allow service-layer routing improvements, and control of traffic flows and exit points.

This document introduces an information model (IM) for filtering policies enacted at I2RS agent before transmitting data to the I2RS client. The [[I-D.ietf-i2rs-architecture](#)] suggests that associated with the I2RS RIB model there will be "Policy-based Routing (ACLs)" and RIB "policy controls". This policy model utilizes the generic policy model found in [[I-D.hares-i2rs-info-model-policy](#)] and operates on the I2RS RIB information module [[I-D.ietf-i2rs-rib-info-model](#)]. The use of a generic policy model allows the creation of named templates for reading or writing to the I2RS RIB module that have three levels of structure (policy group, network policy, and Local elements of policy). The local elements of policy operate in the monitoring stage as read functionality and as filters for the I2RS agent transmission of data to the I2RS client.

Reading information via I2RS from the BGP protocol regarding BGP routes, BGP protocol events, and BGP protocol statistics may also be

needed to filter the information an I2RS agent sends to an I2RS client. The [[I-D.keyupdate-i2rs-bgp-usecases](#)] provides a use case for BGP monitoring in [section 5](#) where it indicates it is important to monitor prefixes of "high visibility" end-users for the announcement or withdraw of prefixes, the suppression of prefix announcements (due to flap damping), and alternate best path selections. It is also important to trace dropped routes, and statistics per EBGp session. These BGP prefixes may need to be tracked both at the BGP and at the active RIB level. The read policy described here for use by the I2RS agent for the RIB Information can be extended to support the read filtering for BGP.

Policy about what I2RS can read from the RIB is contained in the following:

#### Read Policy Group

Policy is described by a set of policy rules that may be grouped into subsets. The read policy group provides model context (or scope) for the Policy rules within it. The model context has an identity, scope, role, precedence, priority and security model. In a policy group, policy rules and policy groups can be nested within other policy rules.

#### Network-Policy

contains a coherent set of rules to administer, manage, and control access between the I2RS client and the I2RS Agent.

#### Local Config

defines individual rules kept in the I2RS agent that are utilized to filter data sent to the I2RS client. The filters associated with the I2RS RIB Model, will include filters on the RIB Info model including: routing instance ID, RIB ID, route attributes, route, next-hop list, installation in FIB, Active in RIB, and unresolved.

## [2.](#) Reading of Network Policy Information

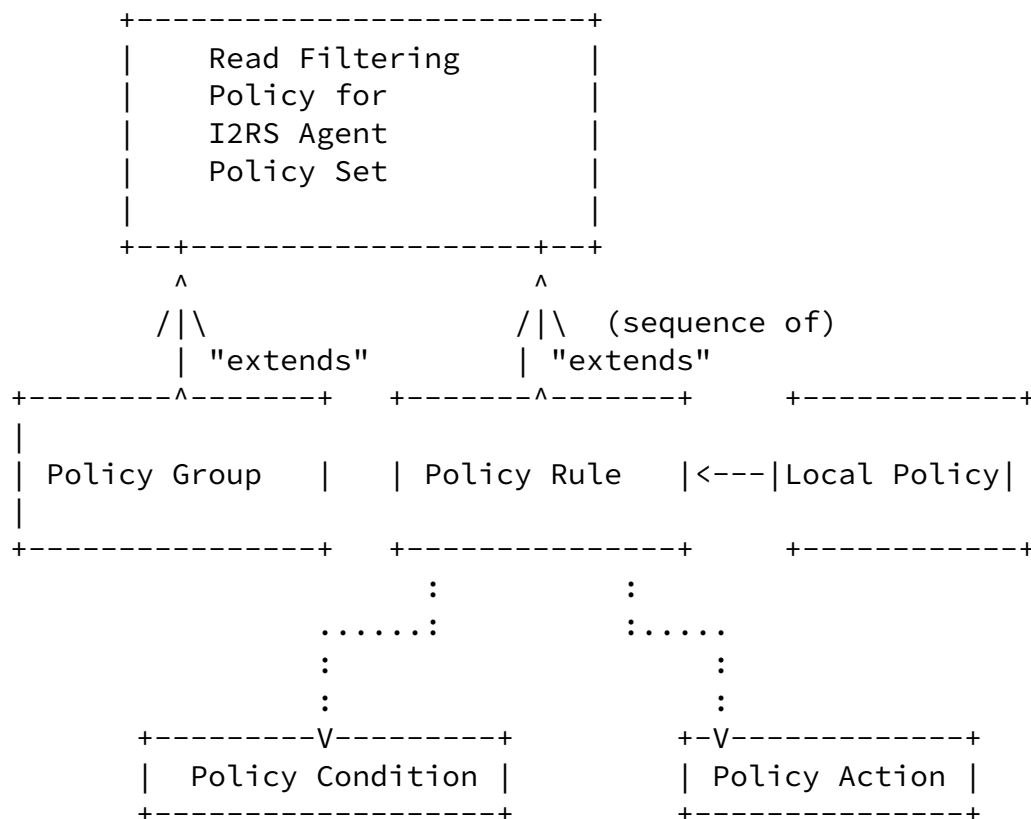
This section provides an overview of the Network Policy information

model. The next section contains an example of the RIB Filtering model.

I2RS client requesting filtered data from the I2RS agent sets the policy into a Network Policy list for Read Filtering. This policy list is created as a set of policy sets that contain a policy group with its associated policy rules. These policy rules are saved in the I2RS Agent's local store.

If the I2RS Agent fails, then these policy rules must be instantiated by the I2RS Client. The templates for the I2RS Agent may be part of the generic templates stored within the routing system and uploaded by name by the I2RS client. This would provide easy of maintenance for systems with these policy templates. However, this is not a requirement for the proper function of this Read Filtering Policy model.

Below is a diagram of the Read Filtering policy model.



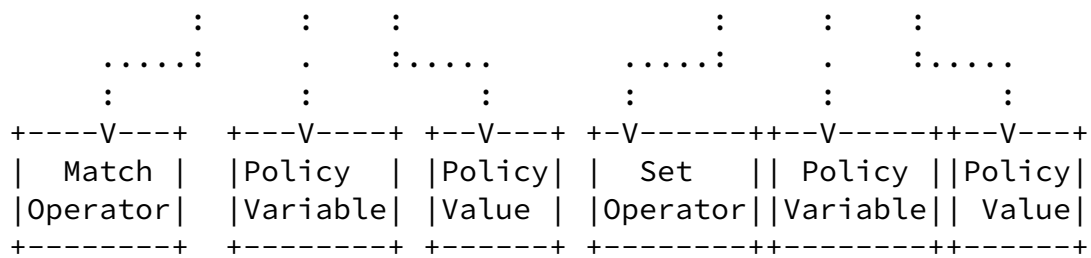


Figure 1: Overall model structure

## Policy set for Read Filtering Policy for I2RS agent

It is a policy set that describes all filtering that the I2RS Agent does prior to sending data to the I2RS Client. This policy set contains a set policy groups with their associated policy rules and an indication whether this will be stored locally at the I2RS Agent.

## Policy Group

The policy group is a policy set which links to a set of policy rules, and contains an identity, scope, role, precedence, priority and security model.

## Policy Rule

The policy rules are a set of policies in which each policy is defined as: "< policy variable> matches value" where the result of the match can be a set operator of "SET policy variable TO value".

Policy Groups can include other policy groups. This aids in building up the policy set as logical components. Operational groups can utilize this to map the policy groups to actual operational service policies. In a similar fashion, policy sets could contain other policy sets.

## 3. Example of Use of Read Filter Policy Information Model

This section provides an example of the Read Filter Policy Information model. The example is taken from the protocol independent use cases use cases this I2RS architecture can be used in

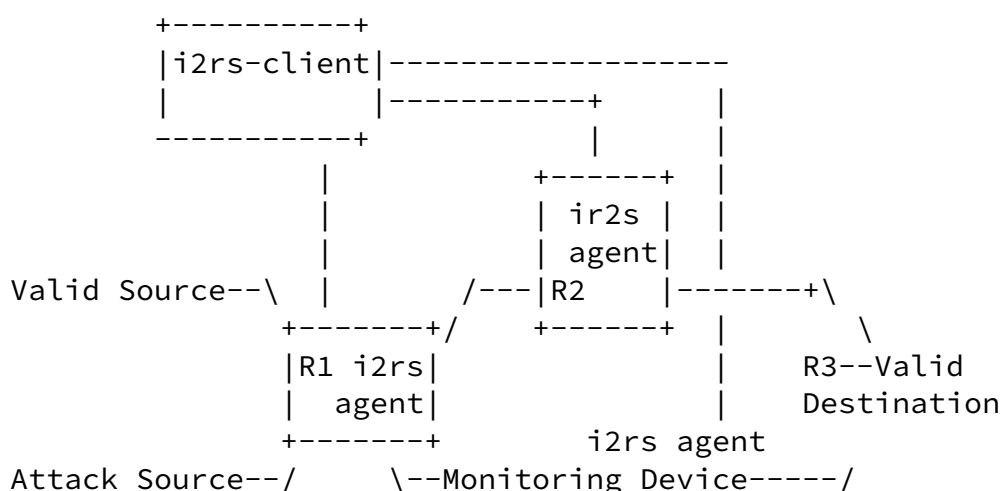
are described in [[I-D.white-i2rs-use-case](#)] Protocol Independent Use Case for the Interface which contains the following examples:

- o Distributed reaction to Network Based Attacks
- o Remote Service Routing
- o Within Data Center Routing
- o Temporary overlays between Data Centers

The specific read monitoring filtering policy is proposed for each use case.

### [3.1](#). Read Filtering for Distributed Reaction to Network Based Attacks

scenario:



### Figure 2 - Distributed reaction to Network Attacks

Description:

In the scenario of the of the Distributed Reactions, an I2RS client is attached to the routing functions on a two network devices (R1 and R2), and a network monitoring device (see figure 2). The routing device R1 has external ports upon which both valid sources and (upon attack) invalid sources may send data. The I2RS client is learning attack prefixes from the monitoring devices which are processing

samples of the traffic. A set of suspected prefixes are collected by the I2RS client from the monitoring devices. The I2RS Client uses these prefixes to control the attack mitigation reading and writing RIB policy.

Currently, the [[I-D.ietf-i2rs-rib-info-model](#)] only includes a "route change notification" or "next-hop resolution". Neither of these change notifications directly imply listening to a stream of the data below, but should. This draft is focused on the READ filters installed for the stream of notifications suggested by the [[I-D.ietf-i2rs-architecture](#)]

The I2RS Client sends command to the I2RS agent in R1 and R2 to request event notification of route changes for any destination routes matching (exact or longer) prefixes which begin with 129.10/16 or 192.169/16. The I2RS Client sends notification filter policies to the I2RS Agents at R1 and R2 to collect with the notification: the routing instance, the RIB, the Route(route-attributes, route-match, and next-hop list) for the watched prefixes. The I2RS Client also sends commands to the forwarding function of R1, R2, and the monitoring device to provide traffic statistics regarding the number of prefixes received with these routes beginning with the prefix 129.10/16 (match or longer), and 192.169/16 (match or longer).

The Read Filter policy is instantiated at R1 and R2 in order to filter just the routes necessary to track. Previous attack patterns have seen 192.169.10/24 or longer prefixes used to during the attack. A special detailed receive policy is also set-up to prepare for these attacks.

The policy filtering matches security attack vector named "red dog 1" so the operator decides to give this policy set an identity of "red dog 1" with a scope of read, a role of security monitoring, a precedence of 1, a priority of 1, and a security model of secure TCP. The network prefix 129.10/16 (exact or longer) is identified as red-net, and the prefix 192.169/16 (exact or longer) is weak-red-net. The 192.169.10/24 is identified as weak-red-watch.

traffic statistics per interface (Eg. exterior interface to network, attack source, and R1-R2 Interface).

The following diagram provides the filters for the first policy. The policy filtering matches attack vector "red dog 1" so the operator decides to give this policy set an identity of "red dog 1" with a scope of read, a role of security monitoring, a precedence of 1, a priority of 1, and a security model of secure TCP.

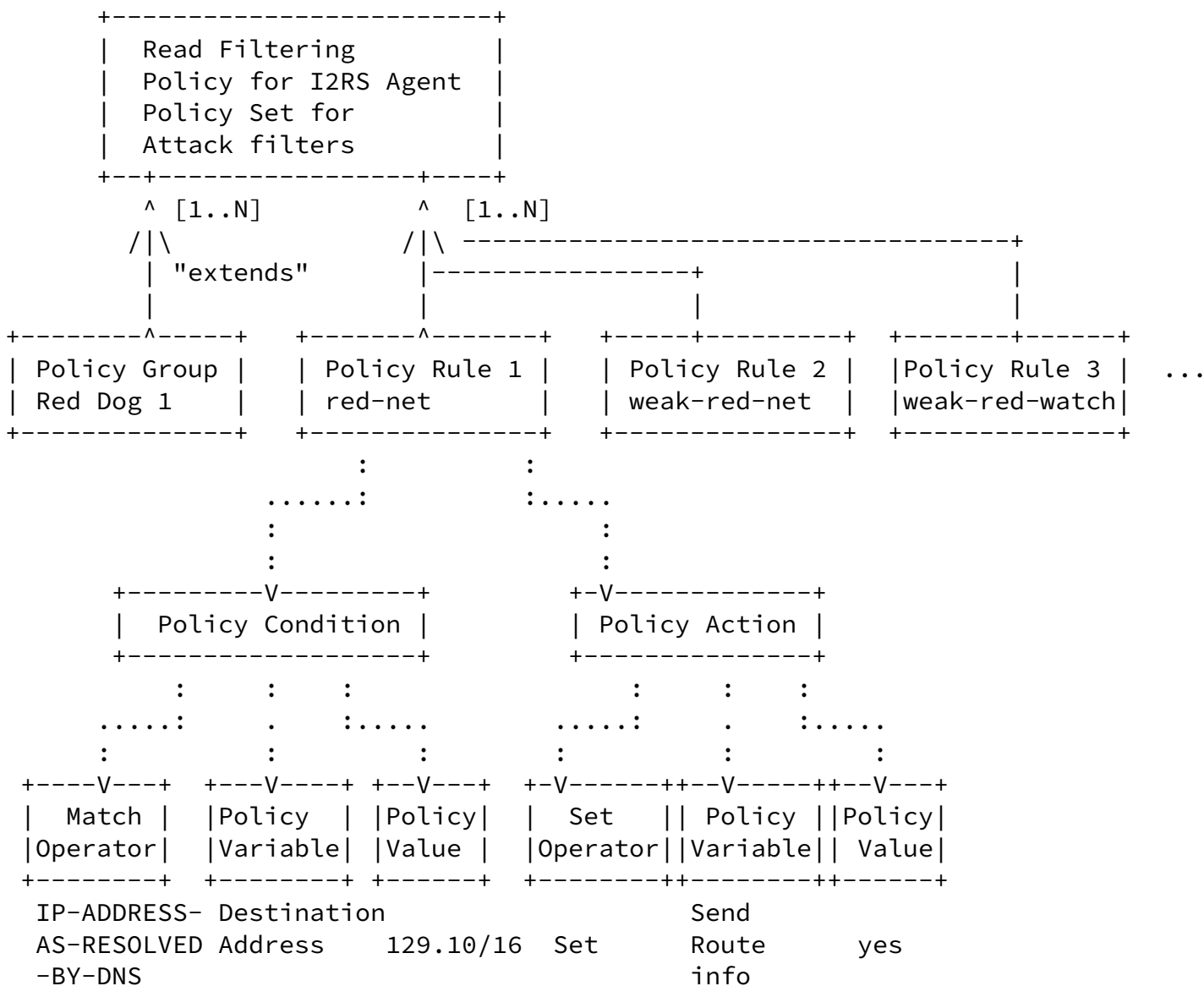


Figure 3: Example of read statistics filter

The following is the Read Filtering Policy Set 1

Policy Group

---

The policy group has an identity of "red dog 1", and a scope of "read", role: "security monitor", precedence of 1, priority of 1, and security model of "secure TCP".

#### Policy Rule 1

The policy rule 1 has an identity of "red-net". The policy condition is: has a policy variable of "IP-ADDRESS-AS-RESOLVED-BY-DNS", a policy variable of "Destination Address", and a policy value of 129.10/16. The Policy actions associated with Policy Rule 1 indicates a "SET" operator for the forwarding of any route matching 129.10/16 prefix with exact match or longer match, and an ACTION of "notify I2RS Client".

#### Policy Rule 2

The policy rule 2 has an identity of "weak-red-net". The policy condition is: has a policy variable of "IP-ADDRESS-AS-RESOLVED-BY-DNS", a policy variable of "Destination Address", and a policy value of 192.169/16. The Policy actions associated with Policy Rule 2 indicates a "SET" operator for the forwarding of any route matching 129.10/16 prefix with exact match or longer match, and an ACTION of "notify I2RS Client".

#### Policy Rule 3

The policy rule 3 has an identity of "weak-red-watch". The policy condition is: has a policy variable of "IP-ADDRESS-AS-RESOLVED-BY-DNS", a policy variable of "Destination Address", and a policy value of 192.168.10/24. The Policy actions associated with Policy Rule 3 indicates a "SET" operator for the sending of forwarding statistics on any data packet matching 192.168.10/24 prefix with exact match or longer match, and an ACTION of "notify I2RS Client".

#### Policy Rule 4

The policy rule 4 has an identity of "red-net stats". The policy condition is: has a policy variable of "IP-ADDRESS-AS-RESOLVED-BY-DNS", a policy variable of "Destination Address", and a policy value of 129.10/16. The Policy actions associated with Policy Rule 4 indicates a "SET" operator for the sending of forwarding statistics on any data packet matching 129.10/16 prefix with exact match or longer match from designated interfaces, and an and an ACTION of "notify I2RS Client".

#### Policy Rule 5

Internet-Draft

IM for policy

February 2014

The policy rule 5 has an identity of "weak-red-net stats". The policy condition is: has a policy variable of "IP-ADDRESS-AS-RESOLVED-BY-DNS", a policy variable of "Destination Address", and a policy value of 192.169/16. The Policy actions associated with Policy Rule 5 indicates a "SET" operator for the sending of forwarding statistics on any data packet matching 192.169/16 prefix with exact match or longer match from designated interfaces, and an ACTION of "notify I2RS Client"

#### Policy Rule 6

The policy rule 6 has an identity of "weak-red-net stats". The policy condition is: has a policy variable of "IP-ADDRESS-AS-RESOLVED-BY-DNS", a policy variable of "Destination Address", and a policy value of 192.169.10/24. The Policy actions associated with Policy Rule 6 indicates a "SET" operator for the sending of forwarding statistics on any data packet matching 192.169/16 prefix with exact match or longer match from designated interfaces, and an ACTION of "notify I2RS Client"

#### Read Policy List

The read policy list has the summary structure below. All Structures underneath the filter policies can utilize template from the three layer generic policy model found in [\[I-D.hares-i2rs-info-model-policy\]](#). Note that policy groups can be included in policy groups.

```

      read filter-policies
    0...N |
      policy set
          |-----|
    |---policy group [1-N]      policy rules [1-N]-- status
    |----| |                  |           |           |
          |                   |           |           |
    +-----+-----+-----+   policy   policy   enabled/disable
    |         |         |         |   condition Action   mandatory/optional
Identity role  priority precedence
          |

```

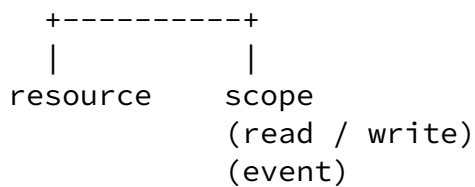
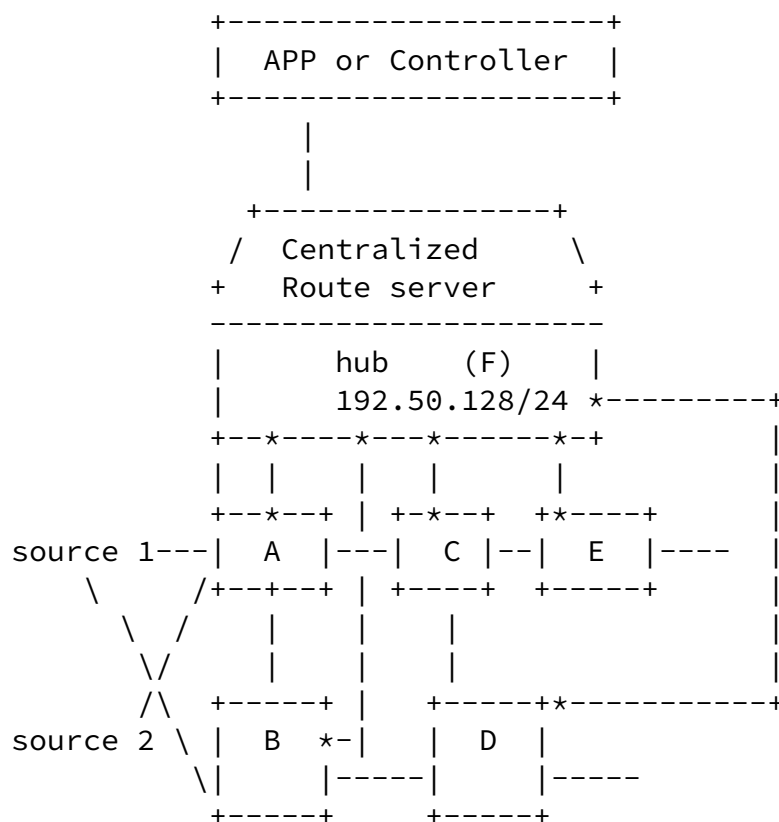


Figure 5 - read filter policies

### [3.2.](#) Remote Service Monitoring

scenario:



\*- are BGP RR connections

|- are hub/spoke connects

spokes: A,B,C,D,E nodes

hub: F node

The second use case mentioned in [[I-D.white-i2rs-use-case](#)] is an improvement of the hub and spoke overlay networks. Current hub and spoke networks balance between information held in the spoke table and optimized routing in the overlay, and mobility of nodes. Most solutions in this space use some form of centralized route server which keeps all routes (reachable destination and next hops), and has a protocol by which the route-server and spoke devices communicate, and caches at remote site. [[I-D.white-i2rs-use-case](#)] suggests that I2RS can provide an alternative control plane by allowing remote sites to register (or transmit through BGP) the reachable destinations at each site, along with the router within the forwarding path.

The [[I-D.ji-i2rs-usecases-ccne-service](#)] also provides a more detailed discussion of the centralized control element that supports using I2rs plus BGP Route-Reflectors (RR), I2RS plus MPLS-TE and PCE ([RFC4655](#)), (both stateless and stateful [[I-D.ietf-pce-stateful-pce](#)]).

For both use cases, the read filtering allows the centralized server to obtain notification of route changes (installed, active, who) and next-hop resolution per [[I-D.ietf-i2rs-rib-info-model](#)] for a particular range of addresses. In addition, interface failures will impact the possible route calculated at the hub. A notification stream watching interfaces and nexthop changes can be tailored to watch the interfaces for the main traffic path and backup paths.

#### Example Read Filters

Across the "\*"--\*" links the hub passes the I2RS and BGP protocol packets. Also across these links passes the the traffic forwarded to the hub, and then forward to the correct destination.

The route server sets policy group CCNE-2 to look for address changes in forwarding pathway routes in address range 192.50.128/18(match or longer), nexthop changes on 192.150.150/24, interface failures in 192.150.160/24, and failures for Route installs. Policy is name CCNE-2.

## Policy Group

The policy group has an identity of "CCNE-2", and a scope of "read", role: "route-server", precedence of 2, priority of 1, and security model of "secure TCP".

## Policy Rule 1

The policy rule 1 has an identity of "hub-net". The policy condition is: has a policy variable of "IP-ADDRESS-AS-RESOLVED-BY-DNS", a policy variable of "Destination Address", and a policy value of 192.50.128/18. The Policy actions associated with Policy Rule 1 indicates a "SET" operator for any route matching 128 prefix with exact match or longer match, and an ACTION of "notify I2RS Client"

## Policy Rule 2

The policy rule 2 has an identity of "CCNE NextHops". The policy condition is: has a policy variable of "IP-ADDRESS-AS-RESOLVED-BY-DNS", a policy variable of "NextHop Address", and a policy value of 192.168.150/24, and a SET Operator of "prefix-match", and an ACTION of "notify I2RS Client".

## Policy Rule 3

The policy rule 3 has an identity of "CCNE Interfaces". The policy condition is: has a policy variable of "IP-ADDRESS-AS-RESOLVED-BY-DNS", a policy variable of "interface address", and a policy value of 192.150.150/24, and status = "down". The Policy actions associated with policy rule 3 indicates a "SET" for match or longer, and "ACTION" is "notify I2RS Client".

## Policy Rule 4

The policy rule 4 has an identity of "CCNE Install Watch". The policy condition is: has a policy variable of "IP-ADDRESS-AS-RESOLVED-BY-DNS", a policy variable of "Routes", and a policy value of 192.150.128/18, Notification Status is "Route Change notification Return Code "No", and policy actions indicate "SET" for match or longer, and "ACTION" is "notify I2RS Client".

The following additions to the RIB Info model are needed to support this use case

- o Notification for interface change
- o Notification for Route change
- o Notification for NextHop change

### [3.3.](#) Within Data Center Routing

scenario: TBD

### [3.4.](#) Temporary overlays between Data Centers

scenario: TBD

## [4.](#) Read Filter Policy Information Model

This section specifies the network policy information model in Routing Backus-Naur Form (RBNF, [[RFC5511](#)]). The policy definitions utilize the generic information model for policy. The RBNF form below is split into two parts: specific read filter policies, and a reference section for the generic information model ([\[I-D.hares-i2rs-info-model-policy\]](#))

### [4.1.](#) Read Filter Policies

```
<Read-Filter-Policies> ::= [<Policy-Set>]
<Policy-Set> ::= [<Policy-Group>]
```

### [4.2.](#) Generic Informational Model Templates

This section provides the RBNF definitions from utilized from the generic information model ([\[I-D.hares-i2rs-info-model-policy\]](#)). This section is informational and will be removed once referencing issues to the generic model have been resolved.

```

<PolicyGroup> ::= <Identity>
                  <Role>
                  <priority>
                  <precedence>
                  <Policy-Rule>
                  [<Supporting-Policy-Group>]
                  [<Policy-Group-Extension>]

<Scope> ::= <Read-Scope>
            | <Write-Scope>

<Role> ::= <Resource>
            | <Scope>

            <Policy-Group-Extension> ::= <>
            ...

<network-policy-rule> ::= (<policy-rule>...)

<policy-rule> ::= <Identity>
                  <priority>
                  <precedence>
                  <Role>
                  (<Condition>
                   (<Action>...))
                  <Security-Model>
                  [<policy-rule-extension>]

<Scope> ::= (<Read> [<read-scope>]) |
            (<Write> [<write-scope>])
            (<Notification> [<notification-scope>])

<Role> ::= <Resource> | <Scope>

<Security-Model> ::= <First-Matching> | <All-Matching>

```

```

<policy-rule-extension> ::= <i2rs-policy-extension> |
                            ...
<condition> ::= <variable>
                (<value>...)

```

```

        [<Match-Operator>]
        [<condition-extension>]

<Match-Operator> ::= <IS-SET-MEMBER'>
                    | <IN-INTEGGER-RANGE>
                    | <IP-ADDRESS-AS-RESOLVED-BY-DNS>
                    | <Match-Operator-extension>

<condition-extension> ::= <i2rs-condition-extension> |
                        ...

<action> ::= <variable>
            <value>
            <Set-Operator>
            <Notify-Operator>
            [<action-extension> ]

<action-extension> ::= <i2rs-action-extension> |
                    ...

<local-policy-rule> ::= (<local-policy-rule>...)
<local-policy-rule> ::= <Identity>
                        <priority>
                        <precedence>
                        <Role>
                        (<Condition>
                         (<Action>...))
                        <Security-Model>

<Scope> ::= (<Read> [<read-scope>]) |
            (<Write> [<write-scope>])

<Role> ::= <Resource> | <Scope>

<Security-Model> ::= <First-Matching>|
                    <All-Matching>
                    ...

<condition> ::= <variable>
                (<value>...)
                [<Match-Operator>]
                [<condition-extension>]

<Match-Operator> ::= <IS-SET-MEMBER'>
                    | <IN-INTEGGER-RANGE>

```

```

|<IP-ADDRESS-AS-RESOLVED-BY-DNS>
|<Match-Operator-extension>

<condition-extension> ::= <i2rs-condition-extension> |
...
<action> ::= <variable>
             <value>
             <Set-Operator>
             [<action-extension>]

<action-extension> ::= <i2rs-action-extension> |
...

```

The elements of the Policy Group information model are as follows:

- o Each policy group is captured in its own list, distinguished via a identity, role, priority, precedence.
- o A policy group has a certain role, such as resource or scope. A policy group can even have multiple roles simultaneously. The role, are captured in the list of "role" component.
- o A policy role has a certain Scope, such as read scope or write=scope. A policy group can even have multiple scope simultaneously. The scope, or scopes, are captured in the list of "scope" components.
- o A policy has a certain priority, such as priority 0-255. A policy can only have one priority. The priority is captured in the list of "priority" component.
- o A policy rule can inherit properties (e.g., identity,role,priority, precedence) from policy group. A policy rule also can have its own properties, e.g., enabled, mandatory, usage.
- o The policy group elements can be extended with policy-specific components (policy-extensions, policy-group-extension respectively).

The elements of the Network-Policy Rule information model are as follows:

- o A policy can in turn be part of a hierarchy of policies, building on top of other policies. Each policy is captured in its own level, distinguished via a policy-identity.

Internet-Draft

IM for policy

February 2014

- o Policy rule inherit scope from policy group. A policy rule has a certain Scope, such as read scope or write scope. A policy rule can even have multiple scope simultaneously. The scope, or scopes, are captured in the list of "scope" components.
- o Furthermore, a policy rule contains conditions and actions, each captured in their own list.
- o A condition contains a variable and a value and use a match operator, to connect variable with value. An examples of an operator might be a "IP ADDRESS AS RESOLVED BYDNS" or "Set to a member". Also, a condition can in turn map onto other condition in an underlay policy. This is captured in list "supporting-condition".
- o An action contains a variable and a value. An action uses Set operator to connect variable with value. Analogous to a node, an action can in turn map onto other actions in an underlay policy. This is captured in list "supporting-action".
- o The policy, condition, action and operator elements can be extended with policy-specific components (policy-extensions, condition-extension, action-extension and operator-extension respectively).

The local network-policy model extends the Network-Policy Rule information model. The elements of the local network-policy model are the local network-policy model as follows:

- o A local policy rule can in turn be part of a hierarchy of policies, building on top of other policies. Each local configuration policy is captured in its own level, distinguished via a policy identity.
- o A local policy rule inherit scope from policy group. A local policy rule has a certain Scope, such as read scope or write scope. A local policy rule can even have multiple scope simultaneously. The scope, or scopes, are captured in the list of "scope" components.

- o Furthermore, a local policy contains conditions and actions, each captured in their own list.
- o A condition contains a variable and a value and use a match operator, to connect variable with value. An examples of an operator might be a" IP ADDRESS AS RESOLVED BYDNS" or "Set to a member". Also, a condition can in turn map onto other condition

in an underlay policy. This is captured in list "supporting-condition".

- o An action contains a variable and a value. An action uses Set operator to connect variable with value. Analogous to a node, an action can in turn map onto other actions in an underlay policy. This is captured in list "supporting-action".
- o The local policy, condition, action and operator elements can be extended with policy-specific components (condition-extension, action-extension and operator-extension respectively).

## [5.](#) IANA Considerations

This draft includes no request to IANA.

## [6.](#) Security Considerations

TBD.

## [7.](#) Informative References

[I-D.hares-i2rs-info-model-policy]

Hares, S. and W. Wu, "An Information Model for Network policy", [draft-hares-i2rs-info-model-policy-00](#) (work in progress), January 2014.

[I-D.ietf-i2rs-architecture]

Atlas, A., Halpern, J., Hares, S., Ward, D., and T. Nadeau, "An Architecture for the Interface to the Routing System", [draft-ietf-i2rs-architecture-01](#) (work in progress), February 2014.

[I-D.ietf-i2rs-rib-info-model]

Bahadur, N., Folkes, R., Kini, S., and J. Medved, "Routing Information Base Info Model", [draft-ietf-i2rs-rib-info-model-01](#) (work in progress), October 2013.

[I-D.ietf-pce-stateful-pce]

Crabbe, E., Medved, J., Minei, I., and R. Varga, "PCEP Extensions for Stateful PCE", [draft-ietf-pce-stateful-pce-07](#) (work in progress), October 2013.

[I-D.ji-i2rs-usecases-ccne-service]

Ji, X., Zhuang, S., and T. Huang, "I2RS Use Cases for Control of Forwarding Path by Central Control Network Element (CCNE)", [draft-ji-i2rs-usecases-ccne-service-00](#) (work in progress), October 2013.

Hares & Wu

Expires August 18, 2014

[Page 18]

---

Internet-Draft

IM for policy

February 2014

[I-D.keyupate-i2rs-bgp-usecases]

Patel, K., Fernando, R., Gredler, H., and S. Amante, "Use Cases for an Interface to BGP Protocol", [draft-keyupate-i2rs-bgp-usecases-00](#) (work in progress), March 2013.

[I-D.keyupate-i2rs-bgp-usecases]

Patel, K., Fernando, R., Gredler, H., and S. Amante, "Use Cases for an Interface to BGP Protocol", [draft-keyupate-i2rs-bgp-usecases-00](#) (work in progress), March 2013.

[I-D.white-i2rs-use-case]

White, R., Hares, S., and A. Retana, "Protocol Independent Use Cases for an Interface to the Routing System", [draft-white-i2rs-use-case-01](#) (work in progress), August 2013.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[RFC3060] Moore, B., Ellessen, E., Strassner, J., and A. Westerinen, "Policy Core Information Model -- Version 1 Specification", [RFC 3060](#), February 2001.

[RFC3644] Snir, Y., Ramberg, Y., Strassner, J., Cohen, R., and B. Moore, "Policy Quality of Service (QoS) Information Model", [RFC 3644](#), November 2003.

- [RFC4655] Farrel, A., Vasseur, J., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", [RFC 4655](#), August 2006.
- [RFC5394] Bryskin, I., Papadimitriou, D., Berger, L., and J. Ash, "Policy-Enabled Path Computation Framework", [RFC 5394](#), December 2008.
- [RFC5511] Farrel, A., "Routing Backus-Naur Form (RBNF): A Syntax Used to Form Encoding Rules in Various Routing Protocol Specifications", [RFC 5511](#), April 2009.

#### Authors' Addresses

Susan Hares  
Hickory Hill Consulting  
7453 Hickory Hill  
Saline, CA 48176  
USA

Email: [shares@ndzh.com](mailto:shares@ndzh.com)

Hares & Wu

Expires August 18, 2014

[Page 19]

---

Internet-Draft

IM for policy

February 2014

Qin Wu  
Huawei  
101 Software Avenue, Yuhua District  
Nanjing, Jiangsu 210012  
China

Email: [sunseawq@huawei.com](mailto:sunseawq@huawei.com)

