Interface to Network Security Functions (I2NSF)

IETF 94, Tuesday November 3, 2015, 09.00

Chairs:
Linda Dunbar <linda.dunbar@huawei.com>
Adrian Farrel <adrian@olddog.co.uk>

Note Well

- Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:
  - The IETF plenary session
  - The IESG, or any member thereof on behalf of the IESG
  - Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
  - Any IETF working group or portion thereof
  - Any Birds of a Feather (BOF) session
  - The IAB or any member thereof on behalf of the IAB
  - The RFC Editor or the Internet-Drafts function
- All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).
- Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.
- A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.
- A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Administrivia

- Charter:

  http://datatracker.ietf.org/wg/i2nsf/charter/

  - Mailing List:

    https://www.ietf.org/mailman/listinfo/i2nsf

    - Minutes Takers: Sue Hares & Cathy Zhou (t hanks!)
    - Jabber Scribe: Diego Lopez (thanks!)
    - Blue Sheets
      - Are now scanned and published

Reminders

- Agenda
  - https://tools.ietf.org/wg/i2nsf/agenda
- Meeting materials, slides, audio streams
  - http://tools.ietf.org/agenda/94/
- Jabber room
  - i2nsf@jabber.ietf.org
- Wiki and issue tracker
  - https://tools.ietf.org/wg/i2nsf/
  - It is all TBD, but a wiki is an open resource
- State your name clearly and slowly at the mic

Agenda

1. Administrivia and Agenda Bash
   Chairs (5 minutes : 5/150)
2. Reminder of Purpose and Focus of I2NSF
   Chairs (10 minutes : 15/150)
3. Deliverables and Milestones
   Chairs (10 minutes : 25/150)
4. Problem statement
   draft-dunbar-i2nsf-problem-statement
   Sue Hares (15 minutes : 40/150)
5. Use Cases and Gap Analysis
   draft-hares-i2nsf-use-case-gap-analysis
   Sue Hares (20 minutes : 60/150)
6. Framework
   draft-merged-i2nsf-framework
   Ed Lopez (15 minutes : 75/150)
7. Information Model of Interface to Network Security Functions Capability Interface
   draft-xia-i2nsf-capability-interface-im
   Frank Xia (15 minutes : 90/150)
8. Software-Defined Networking Based Security Services using Interface to Network Security Functions
   draft-jeong-i2nsf-sdn-security-services
   Jaehoon Paul Jeong (15 minutes : 105/150)
9. User-group based Mechanism for Service Layer
   draft-you-i2nsf-user-group-based-policy
   Jianjie You (10 minutes : 115/150)
10. Introduction to new I-Ds
    - draft-fang-i2nsf-inter-cloud-ddos-mitigation-api Luyuan Fang (5 minutes : 120/150)
    - draft-pastor-i2nsf-vnsf-attestation Diego Lopez (5 minutes : 125/150)
    - draft-zhou-i2nsf-capability-interface-monitoring Cathy Zhou (5 minutes : 130/150)
11. Any other business – open mic (10 minutes : 140/150)
12. Summary of WG actions and next steps
    Chairs (10 minutes : 150/150)

Purpose and Focus of I2NSF

- The purpose of I2NSF is to specify standard interfaces for clients, applications, or application controllers to inform network what/when/how they are willing to receive.
  - The focus is to define a set of software interfaces and data models for controlling and monitoring aspects of physical and virtual NSFs, enabling clients to specify rulesets.
  - With the standard interface, the clients or SDN (Security) Controller can dynamically control & monitor collections of distributed virtual/physical security functions by different vendors.

What is I2NSF Chartered to Work On?

- **To specify interfaces at two functional levels for the control and monitoring of network se curity functions:**
  - The Capability Layer: specifies how to control and monitor NSFs at a functional implementation level.
  - The Service Layer: defines how clients' security pol icies may be expressed to a security controller.
    - Only the simple Service Layer policies that are modeled as closely as possible on the Capability Layer are within the scope.

What is not in Charter?

- I2NSF will not specify abstract or sophisticated policies from clients. Expressing policies in ways other than the model used by the Capability Layer is out of scope.
- The translation mechanism/methods from Service Layer policies to Capability layer commands are out of scope

Deliverables

- A single document covering use cases, problem statement, and gap analysis document. This document will initially be produced for reference as a living list to track and record di scussions: the working group may decide to not publish this document as an RFC.
- A framework document, presenting an overview of the use of NSFs and the purpose of th e models developed by the working group. This document will also be a reference text to guide the main work and the working group may decide to not publish this document as a n RFC.
- If the working group considers it necessary, a single, unified, Information Model to descri be the control and monitoring of flow-based NSFs.
- YANG data models for the control and monitoring of NSFs.
- A vendor-neutral vocabulary to enable the characteristics and behavior of NSFs to be sp ecified without requiring the NSFs themselves to be standardized, so that "security contr oller" or "manager" have a common base to choose the appropriate NSFs (by different v endors) that can fulfill the requests requested by clients.
- An examination of existing secure communication mechanisms to identify the appropriate ones for carrying the controlling and monitoring information between the NSFs and their management entities. This document may also be produced as a working document that is not published as an RFC.

Milestones

Nov 2015 Adopt use Cases, problem statement, and gap analysis as WG document

Feb 2016 Adopt framework as WG document

Jun 2016 Adopt requirements for extensions to protocols as WG document

Jun 2016 Adopt examination of existing secure communication mechanisms as WG document

Jun 2016 Adopt info model as WG document (if desired)

Jul 2016 Adopt data models as WG document

Aug 2016 WG decides whether to progress adopted drafts for publication as RFCs (use cases, framework, information model, and examination of existing secure communication mechanisms)

Aug 2016 Adopt applicability statements as WG Document

Oct 2016 Adopt IANA registry consideration as WG document

Apr 2017 All early drafts to IESG for publication (if WG decided to proceed): use cases, problem statement, and gap analysis document; framework document; information model requirements for extensions to protocols document; examination of existin

How to Work and How to Avoid Pitfalls

- There are some risks!
  - Continued exploration of architecture and use cases
    - Of course we ***do*** need to complete the work
    - But we don’t need to document every possible use case
  - Failure to start work on the concrete deliverables as i ndividual I-Ds
    - Before we can adopt an I-D we would like to see something worth adopting
    - That means getting down to work now
      - Don’t leave it until two weeks before IETF-95 (please!)
    - The chairs can facilitate Design Teams if that would help
      - But we would prefer you to self-organise

How the Chairs Propose to Drive You

- We want to provide you with the tools to do your work
- Design teams and mailing lists if you need them
  - But we prefer open discussion on the main list
- Use the wiki to record and report
  - Add to it as you see fit and we will curate it
- Use the issue tracker to record concerns and track progress
  - Please don’t just bash out issues in the tracker as this can come close to a DoS attack ☺
    - Raise your concern on the mailing list
    - Agree on the list that the concern is valid and needs to be addressed (and that it is not a duplicate)
    - Enter a new issue in the tracker
    - Work on a solution and include it in an I-D that is posted
    - Close the issue with a pointer to the resolution

Main Agenda

4. Problem statement
   draft-dunbar-i2nsf-problem-statement
   Sue Hares (15 minutes : 40/150)
5. Use Cases and Gap Analysis
   draft-hares-i2nsf-use-case-gap-analysis
   Sue Hares (20 minutes : 60/150)
6. Framework
   draft-merged-i2nsf-framework
   Diego Lopez (15 minutes : 75/150)
7. Information Model of Interface to Network Security Functions Capability Interface
   draft-xia-i2nsf-capability-interface-im
   Frank Xia (15 minutes : 90/150)
8. Software-Defined Networking Based Security Services using Interface to Network Security Funct ions
   draft-jeong-i2nsf-sdn-security-services
   Jaehoon Paul Jeong (15 minutes : 105/150)
9. User-group based Mechanism for Service Layer
   draft-you-i2nsf-user-group-based-policy
   Jianjie You (10 minutes : 115/150)

Other I-Ds

- Just to point you to the I-Ds so you can go and read them and comment on list
  - No time for questions or discussion
- Authors please spend ***no more than five minutes*** to tell us:
  - Purpose of the work
  - Where it fits in the I2NSF Charter
  - Status (Early idea? Mature draft? Code written? Problem in the field?)
  - Next steps for the work
- Interface to Network Security Functions Demo Outline Design
  draft-xie-i2nsf-demo-outline-design-00 (Yuming Xie)
    - The Capability Interface for Monitoring Network Security Functions (NSF) in I2N SF
      draft-zhou-i2nsf-capability-interface-monitoring (Cathy Zhou)
- Inter-Cloud DDoS Mitigation API
  draft-fang-i2nsf-inter-cloud-ddos-mitigation-api (Luyuan Fang)
- Remote Attestation Procedures for virtualized NSFs (vNSFs) through the I2NSF S ecurity Controller
  draft-pastor-i2nsf-vnsf-attestation (Diego Lopez)
- Anyone else?
  - Existing drafts
  - Planned drafts?