I2NSF Charter

Network Security Function (NSF) is to ensure integrity, confidentiality and availability of network communications, to detect unwanted activity, and to block it or at least mitigate its effects. NSFs are provided and consumed in increasingly diverse environments. Users of NSFs could consume network security services hosted by one or more providers, which may be their own enterprise, service providers, or a combination of both. Likewise, service providers of NSFs may offer their customers network security services that consist of multiple security products and/or functions from different vendors. NSFs may be provided by physical and/or virtualized infrastructure. Without standard interfaces to control and monitor the behavior of NSFs, it has become virtually impossible for security service providers to automate service offerings that utilize different security functions from multiple vendors.

The primary goal of I2NSF is to define an information model, a set of software interfaces and data models for controlling and monitoring aspects of physical and virtual NSFs. Other aspects of NSFs, such as device or network provisioning and configuration, are out of scope. Controlling and monitoring of NSFs should include the ability to specify, query, monitor, and control the NSFs by one or more management entities. Since different security vendors support different features and functions on their devices, I2NSF will focus on flow-based NSFs that provide treatment to packets/flows, such as IPS/IDS, Web filtering, flow filtering, deep packet inspection, or pattern matching and remediation.

There are two layers of interfaces envisioned in the I2NSF approach:

- The I2NSF Capability Layer specifies how to control and monitor NSFs at a functional implementation level. That is, I2NSF will standardize a set of interfaces by which control and management of NSFs may be invoked, operated, and monitored. (I2NSF will not work on any other aspects of NSFs. Nor will I2NSF at this stage specify how to derive control and monitoring capabilities from higher level security policies for the Capability Layer.)
- The I2NSF Service Layer defines how clients’ security policies may be expressed and monitored. The Service Layer is out of scope for this phase of I2NSF’s work. However, I2NSF will provide a forum for Informational drafts on data models, APIs, etc. that demonstrate how service layer policies may be translated to Capability Layer functions.

The concrete work at the I2NSF Capability Layer includes development of

- An information model that defines concepts required for standardizing the control and monitoring of NSFs.
- A set of YANG data models, derived from the above information model.
- The capability registry (IANA) that enables the characteristics and behavior of NSFs to be specified using a vendor-neutral vocabulary without requiring the NSFs themselves to be standardized. The registry enables various mechanisms, including policy rules, to be used to match monitor and control functions to the needs of an application and/or environment.
- Examining the existing secure communication mechanisms to identify the appropriate ones for carrying the controlling and monitoring information between the NSFs and their management entity (or entities).
Standard interfaces for monitoring and controlling the behavior of NSFs are essential building blocks for Security Service Providers to automate the use of different NSFs from multiple vendors by their Security management entities. This work will leverage the existing protocols and data models defined by I2RS, Netconf, and NETMOD. If extensions to these protocols are needed, requirements will be developed by this WG, and the extensions will be developed in cooperation with the WGs responsible for the protocols.

The I2NSF WG’s deliverables include:

- Use cases, problem statement, gap analysis document [The WG will decide if to proceed as RFC]
- Framework Document, presenting an overview of the use of NSFs and the purpose of the models developed by the WG [The WG will decide if to proceed as RFC].
- A single, unified, Information Model for controlling and monitoring flow-based NSFs.
- Corresponding YANG Data Models derived from the above Information Model.
- IANA registry consideration for flow-based NSFs controlling and monitoring capabilities.[maybe merged into data models]

The WG may additionally choose to develop additional documents to describe requirements for extensions (if any) to existing protocols used by the WG, and how the data models are used to monitor and control flow-based NSFs, and to describe how to use I2RS, Netconf, and NETMOD to carry the content of the data models.

(The WG may decide that the Use cases, Framework, and gap analysis are simply reference documents during the lifetime of the WG and not to be published as an RFC.)

The WG will work closely with I2RS, Netconf and Netmod WGs. The WG will communicate with external SDOs like ETSI NFV and will encourage open source code development related to the WG scope in organizations like ONF, OpenStack, ODL, and OPNFV.

Suggested Milestones

- Use Cases, problem statement, and gap analysis Document: Charter time + 1 month
- Framework: Charter time + 4 months to WG Document
- Requirements for extensions to protocols: Charter time + 8 months to WG document
- Info model: Charter time + 8 months to WG Document
- IANA registry consideration + 12 months to WG Document
- All Early Drafts to IESG: 18 months

[decision point – +10 months]

- Data Models: Charter + 9 Months to WG Document
- Applicability Statements: 10 months to WG Document
- Data Models and Applicability Statements to IESG - 18 months