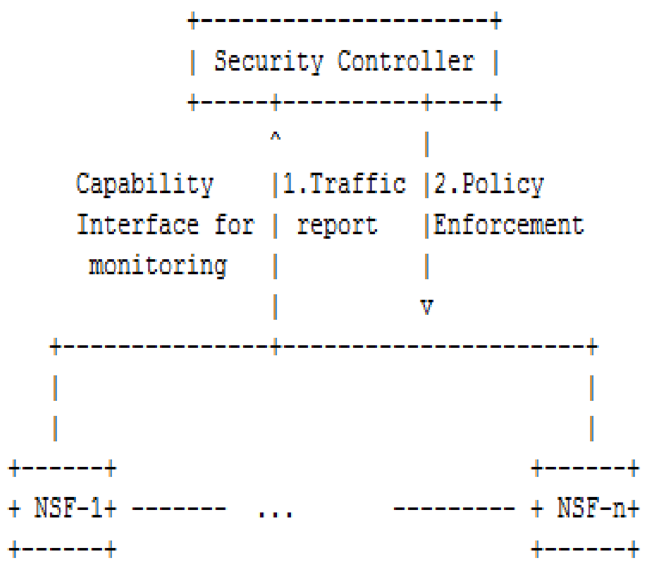
The Capability Interface for Monitoring Network Security Functions (NSF)

draft-zhou-i2nsf-capability-interface-monitoring-00

Introduction

- Rising security problems and attack types bring challenges for the security enterprises and organizations:
  - Various attack types, e.g., DDOS, botnets, spam, etc.
  - Large amount and isolated security information
  - No standardized interface for collecting information from various security vendors before i2nsf capability interface appears
- The capability interface:
  - Monitor the network status and collect traffic information from the NSF to make intelligent security decision and to dynamically adjust the sampling and steering policy.

Architecture



```
         +---------------------+
         | Security Controller |
         +-----+----------+----+
               ^          |
Capability     |1.Traffic |2.Policy
Interface for  | report   |Enforcement
 monitoring    |          |
               |          v
  +------------+---------------------+
  |                                  |
  |                                  |
+------+                          +------+
+ NSF-1+ -------   ...   -------- + NSF-n+
+------+                          +------+
```

- NSF -- >Security Controller: The NSF reports the monitoring information to the SC, e.g., abnormal flows, security logs, statistics or the suspicious attack sources or destinations.
- Security Controller -- > NSF: The security controller provides the attack mitigation and defense strategy with the acquired sampling traffic information for attack detection by the way of dynamically adjusting the flow sampling policy, e.g., flow information, sampling ratio, sampling encapsulation method and/or sampling point information. The policies may include: traffic cleaning and sampling adjustment.

Next Steps

- Solicit more inputs on the detailed monitoring information
- Improve the document with information model structure and grammar

- Questions/Comments?