Configuration of Advanced Security Functions with I2NSF Security Controller

https://datatracker.ietf.org/doc/draft-dong-i2nsf-asf-config/

Wei Pan        Huawei Technologies
Liang Xia      Huawei Technologies

IETF 103, Bangkok
November 2018
Motivations

- Additional enhancement and supplement to the base NSF facing data models.
  - Base draft defines the architecture of the NSF facing interface.
  - This draft defines the configuration data model of advanced security functions which are part of the ACTION.
  - Three most common advances security functions, the antivirus, the anti-ddos and the IPS.

- Other devices are able to reference the configured profiles, like switches, routers.

- Separate from base draft in prevent the base draft from being too long.
Antivirus

**Step 1: Filter the target traffic**
- Target protocols, target traffic directions
- Whitelist, matched traffic will be ignored

**Step 2: Extract and Compare**
- Extract signatures of files
- Compare with the virus signatures in the virus signature database (default)
- Exception rules
  - Exception application names
  - Exception signature identifications

**Step 3: Apply actions**
- Normal actions applied on the detected virus
  - Alert, Block, Declare, Delete-attachment, etc.
- Corresponding actions of the exception rules

module: ietf-i2nsf-asf-config-antivirus

```
  +--rw antivirus
      +--rw profiles
          +--rw profile* [name]
              +--rw name
              +--rw description?
              +--rw detect* [protocol-type direction]
                  |  +--rw protocol-type
                  |  +--rw direction
                  |  +--rw action?
              +--rw exception-application* [application-name]
                  |  +--rw application-name
                  |  +--rw application-action?
              +--rw exception-signature* [signature-id]
                  |  +--rw signature-id
                  |  +--rw signature-action?
          +--rw whitelists {antivirus-whitelists}?
              +--rw match-rules*
                  |  ...
              +--rw source-address*
              +--rw source-address-range*
                  |  ...
              +--rw destination-address*
              +--rw destination-address-range*
                  ...
```
Anti-DDoS

**Network/Transport Layer Anti-DDoS**
- TCP-SYN flood
  - TCP source authentication
  - TCP Proxy
- UDP flood
  - Fingerprint Learning
  - Rate limit
- ICMP flood
  - Rate limit

**Application Layer Anti-DDoS**
- HTTP and HTTPS flood
- DNS request flood
- DNS reply flood
- SIP flood

**Automatic baseline learning**

```bash
module: ietf-i2nsf-asf-config-antiddos
  +--rw antiddos
  |   +--rw profiles
  |     +--rw profile* [name]
  |        +--rw name
  |        +--rw description?
  |        +--rw syn-flood* [action]
  |            |   +--rw action syn-flood-action
  |            |   +--rw rate? uint32
  |        +--rw udp-flood* [action]
  |        |   ... +--rw http-flood* [action]
  |        |   ... +--rw https-flood* [action]
  |        |   ... +--rw dns-request-flood* [action]
  |        |   ... +--rw dns-reply-flood* [action]
  |        |   ... +--rw icmp-flood * [action]
  |        |   ... +--rw sip-flood* [action]
  |        |   ... +--rw detect-mode?
  |          +--rw baseline-learn
  |            +--rw auto-apply?
  |              +--rw start?
  |              +--rw mode?
  |              +--rw tolerance-value?
  |              +--rw learn-duration?
  |              +--rw learn-interval?
```
Intrusion Prevention System

- **Customize detection rules**
  - Default Signature Database
  - Signature set
    - A set of signature filtered by some specific conditions and to be used
    - Conditions include target, severity, OS, applications, protocols, etc.
  - Exception Signature

- **Extract and Compare**
  - Extract features of packets
  - Compare with the intrusion prevention signatures

- **Detection actions**
  - Default action of each signature
    - Allow, Alert, Block, etc.
  - Specific action of each signature set
  - Specific action of each exception signature

```plaintext
module: ietf-i2nsf-asf-config-ips
   +--rw ips
     +--rw profiles
       +--rw profile* [name]
         +--rw name
         +--rw description?
         +--rw signature-sets
           +--rw signature-set* [name]
             +--rw name
             +--rw action?
             +--rw application
               ...
             +--rw target?
             +--rw severity*
             +--rw operating-system*
             +--rw protocol
               ...
             +--rw category
               ...
           +--rw exception-signatures
             +--rw exception-signature* [id]
               +--rw id
               +--rw action?
```
Future work

- Optimize the existing configuration parameters in the data model.
- Include more security function profiles in the data model.
- Consider how these profiles can be referenced by other modules.