Analysis of Existing Work for I2NSF

draft-zhang-gap-analysis-00

H.Rafiee
Dacheng Zhang
Huawei

IETF 91 I2NSF BoF

NSIS (1)

- NSIS is for standardizing an IP signaling protocol (RSVP) along data path for end points to request its unique QoS characteristics, unique FW policies or NAT needs (RFC5973) that are different from the FW/NAT original setting. The requests are communicated directly to the FW/NAT devices.
- NSIS is path-coupled, it's possible to message every participating device along a path without having to know its location, or its location relative to other devices

NSIS (2)

- The I2NSF doesn't require all network functions to comply.
- I2NSF is to define clients (applications) oriented descriptors (profiles, or attributes) to request/negotiate/validate network security functions that are not physically located on the local premises.

How I2NSF is different from SACM

SACM:

Security Assessment of End Points

- End points can be routers, switches, clustered DB, installed piece of software
- How to encode policies in a manner where assessment can be automated
- Example:
  - a Solaris 10 SPARC or Window 7 system used in a environment that requires adherence to a policy of Mission Critical Classified.
  - rules like "The maximum password age must be 30 days" and "The minimum password age must be 1 day"

I2NSF:

Interface to Network Security Functions

- Protocols for clients to request/query/ verify Security related functions from Network Providers

  Firewall
  DDOS/Anti-DOS
  Access control/Authorization/Authentication
  Remote identity management
  Secure Key management
  Intrusion Detection System/ Intrusion Prevention System (IDS/IPS)
  Threat detection: Eavesdropping, Trojans, viruses and worms, Malware, etc.

- Example:

  vCPE needs vFW that are hosted in the network.

  vCPE provides the “Group Policies” for the vFW, like A can talk to B & C, but B can’t talk to C.

PCP

- As indicated by the name, the Port Control Protocol (PCP) enables an IPv4 or IPv6 host to flexibly manage the IP address and port mapping information on Network Address Translators (NATs) or firewalls, to facilitate communication with remote hosts.

SFC

- IETF SFC is about mechanism of chaining together service functions; IETF SFC treats all those Service Functions as black box, i.e. SFC doesn’t care what actions those functions are performing. SFC defines the SFC header to carry Metadata with payload to those functions. But SFC itself doesn?t specify what content is encoded in the metadata.

ANIMA

- ANIMA (Autonomic Networking Integrated Model and Approach) introduces a control paradigm where network processes, driven by objectives (or intent), coordinate their local decisions, autonomically translate them into local actions, and adapt them automatically according to various sources of information including external information and protocol information bases.

Thanks