

Collaboration Agreement for Security Service Function

draft-mglt-i2nsf-ssf-collaboration-00.txt

D. Migault, A. Ranjbar

- IETF96- Berlin

Motivations

Enabling different domains to collaborate

Typical use case:

- A WebApplication firewall detects an attacks
- The WebApplication alerts the Cloud Provider
 - ▶ Configure firewall in its domain

Can we do more ? [Yes]

In order to mitigate the Cloud Provider, should be able to collaborate with the downstream ISPs

Collaboration

Collaboration is different from orchestration:

- Your collaborator may not want to collaborate
- Your collaborator may agree on less resource than expected

Collaboration MUST be:

- Flexible
- Negotiable to limit the engagement of a provider

In the document, we define the "Best Effort" mode for a collaboration:

- The provider only provide on-path service to a fraction of the flow
 - ▶ Treated packets are sent over an Standard Path
 - ▶ Non treated packets are sent over an Alternate Path

Collaboration Agreement

The Collaboration agreement describes the collaboration:

- ca_id
- initiator
- provider
- collaboration mode (Best Effort, Resilient)
- resource
 - ▶ How can we define resource (cgroup, AWS terminology) ?
- SSF type
 - ▶ How to describe an security service ?
- expiration time
- interconnections (Standard Path, Alternate Path)
- direction

Collaboration Protocol

Collaboration Protocol is based:

- HTTPS
- JSON objects

Collaboration agreement based on IKEv2 principle:

- Initiator sends a list of proposals
 - ▶ Each proposal has different parameter types
 - ▶ A proposal can have multiple values associated to each type
- Provider
 - ▶ Selects a single proposal
 - ▶ Selects a single value associated to each type

Collaboration Protocol

Collaboration management operations

- END_AGREEMENT
- UPDATE_EXPIRATION_DATE
- UPDATE_RESOURCE
- REDIRECT_SSF

Questions

Is this protocol/use case of interest ?

Is JSON the appropriated way to go?

- ▶ Is YANG an alternative ?

Are they any competing protocols ?

- Netconf, restconf ...

Any standard to express:

- resources
- security services

Thank you for your attention