Scope of the I-D

I2NSF virtual meeting

September 6th 2017

Rafael Marín López and Gabriel López Millán

University of Murcia

Preliminary assumptions (based on SDN paradigm)

- A SDN controller is a **trusted** entity for the NSFs that it controls
- There is always a **bidirectional** secure communication channel between the SDN controller and the NSFs (e.g. NETCONF+SSL/SSH)
- The SDN controller can collect information from the NSFs and receive asynchronous notifications from them (e.g. if a NSF falls, the SDN controller will know). That is, the controller can monitor NSFs.
- Regardless of the SDN-based IPsec management, the SDN controller MUST be protected against attacks: it is a critic entity in the infrastructure

Scope

- Our I-D is **a SDN-based automated key distribution technique**. The SDN controller always generates fresh key material and parameters for IPsec management
- The I-D specifies how to configure **host-to-host** (e.g. host-to-host VPN, full mesh encryption) and **gateway-to-gateway** (e.g. site-to-site VPN)
- **Host-to-gateway** (e.g. remote access VPN) deserves further study, specially in case 2
- Case 1 or case 2 can be used depending on the scenario
- Based on these general scenarios, it is possible to apply our I-D to different more specific uses cases (i.e. SD-WAN, communication between VMs in datacenters…)

Final notes

- We have observed some interest in the industry (and academia) for the benefits of this kind of SDN-based automated management.
- There are solutions but with proprietary interfaces.
- In other words, it seems there may be a need to standardize an interface to operate with host-to-host and gateway-to-gateway (so far)
- It provides a solution that represents a tradeoff between powerful management and security