draft-raviolli-intarea-trusted-domain-srv6-01

https://datatracker.ietf.org/doc/draft-raviolli-intarea-trusted-domain-srv6/

IETF 117

INTAREA-WG Meeting

July 25, 2023

IETF

Why does this exist?

- SRv6 has known security vulnerabilities should an attacker be able to insert packets into the SRv6 domain
- RFC8402 section 8 clearly states that SRv6 that leaks beyond the boundaries of a domain creates a security violation
- RFC8754 also states, in section 5, that to mitigate attacks filtering into the domain is required.
- LPM filtering on every “external” facing port on a broad scale is neither scalable nor practical in an operational sense . This is due to a host of reasons from TCAM scaling on certain devices to simple human error (We have all seen how good operators are maintaining prefix filters on BGP!)

Attack Vectors

- Some of the attack vectors are documented at
  - https://mailarchive.ietf.org/arch/msg/v6ops/GbWiie-bjQ_Bp1JKB1PlDh_fPdc/
  - https://datatracker.ietf.org/doc/draft-li-spring-srv6-security-consideration/

What the draft attempts to accomplish

- Give operators who feel that it is necessary to protect themselves by further “closing” the domain an option to do so.
- Keep it simple – and avoid a re-work of SRv6 itself. All SRv6 functionality needs to be maintained, while allowing SRv6 to be used inside a trusted domain that “fails closed”
- Avoid creating a scenario that would require changes to silicon
- Enhance the deployment of SRv6 by allowing operators who will not deploy SRv6 because of the security concerns, a method to utilize the technology in a manner that addresses these concerns

How we accomplish this

- A global knob on a device that tells the device to run in “trusted domain srv6” mode.
  - If enabled, no SID processing will occur on packets that do not contain an SRv6 Trusted Domain ethertype
- A per-interface knob to enable processing (swapping in/out) of the SRv6 Trusted Domain ethertype
  - This is disabled by default – and unless enabled packets containing this ethertype will be dropped on ingress.
- The per interface method replicates the same method used to secure MPLS – on almost all devices MPLS requires explicit enablement on MPLS capable ports

Another note

- While we do not document the mechanisms to do so in the draft and consider it out of scope – attention needs to paid to the fact that:
  - It is possible to impose/enforce SRv6 Trusted domain ethertype on the ”border” interfaces and then revert to standard IPv6 ethertypes on the inside of the network
  - This has its own set of security concerns and is not an approach we would recommend – hence choosing to explicitly keep this out of scope

.

Next Steps

- We would like to ask for an adoption call on this draft so that work can progress within the working group and any further concerns can then be addressed in the context of the working group

- Questions?

Thanks!