Usecase and Requirements for new XFRMI
a secunet’s point of view

Christian Langrock

secunet Security Networks AG

IPSec Workshop Dresden 2018
Use case

Requirements

- environment with multiple security domains
- separation via network name spaces
- only 1 kind of transition between NetNS allowed
- ensure encryption or drop it
- simplify routing
Usecase

Requirements

- environment with multiple security domains
- separation via network name spaces
- only 1 kind of transition between NetNS allowed
- ensure encryption or drop it
- simplify routing
Use Case

Requirements

- environment with multiple security domains
- separation via network name spaces
- only 1 kind of transition between NetNS allowed
  - ensure encryption or drop it
  - simplify routing
Use case

Requirements

- environment with multiple security domains
- separation via network name spaces
- only 1 kind of transition between NetNS allowed
- ensure encryption or drop it
- simplify routing
Usecase
Requirements

- environment with multiple security domains
- separation via network name spaces
- only 1 kind of transition between NetNS allowed
- ensure encryption or drop it
- simplify routing
Use case

Solution

- VTIs
Use Case Overview

Security Domain 1

+-----------------------------+ | Non-secure domain +-----------------------------+
| vti1 (t)--- . | | |
| vti61 (t)--- . | | |
| [0.0.0.0/0 dev vti1] | | 10.2.2.1/24 eth0(p)--- |
| [::/0 dev vti61] | | X . |
| | | . |
| -(p)eth1 192.168.x.y/24 | | F . |
| | | . |
| +-----------------------------+ | R . |
| | | . |
| Security Domain n | | M . |
+-----------------------------+ | . |
| | | . |
| vti1 (t)--- . | | |
| vti6n (t)--- . | | |
| [0.0.0.0/0 dev vti1] | | |
| [::/0 dev vti6n] | +-----------------------------+ |
| | | . |
| -(p)eth1 192.168.x.y/24 | |
| | |
| +-----------------------------+ |

(p) = physical interface
(t) = tunnel interface
Shortcomings
VTIs are not the answer

- 2 VTIs per NetNS needed $\rightarrow$ IPv4 + IPv6
  - only 1 wildcard interface possible
  - it’s all done by the host $\rightarrow$ slow
Shortcomings
VTIs are not the answer

- 2 VTIs per NetNS needed → IPv4 + IPv6
- only 1 wildcard interface possible
- it’s all done by the host → slow
Shortcomings

VTIs are not the answer

- 2 VTIs per NetNS needed → IPv4 + IPv6
- only 1 wildcard interface possible
- it’s all done by the host → slow
Resulting Requirements for new XFRMI

Whishlist

- XFRM should be enforced
- Interfamily support $\rightarrow$ IPv4 + IPv6 through one interface
- multiple XFRMI with address *any*
- performance $\rightarrow$ offloading support
Resulting Requirements for new XFRMI

Whishlist

- XFRM should be enforced
- Interfamily support → IPv4 + IPv6 through one interface
  - multiple XFRMI with address *any*
  - performance → offloading support
Resulting Requirements for new XFRMI

Whishlist

- XFRM should be enforced
- Interfamily support → IPv4 + IPv6 through one interface
- multiple XFRMI with address *any*
- performance → offloading support
Resulting Requirements for new XFRMI

Whishlist

- XFRM should be enforced
- Interfamily support → IPv4 + IPv6 through one interface
- multiple XFRMI with address *any*
- performance → offloading support