Usecase and Requirements for new XFRMI

a secunet's point of view

Christian Langrock

secunet Security Networks AG

IPSec Workshop Dresden 2018



Requirements

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



Requirements

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



Requirements

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



Requirements

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



Requirements

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



Solution



Usecase Solution

▶ VTIs



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]
-(p)eth1 192.168.x.y/24
  Security Domain n
                        vtin (t)---
                       vti6n (t)---
  [0.0.0.0/0 dev vtin]
  [::/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 → IPv4 + IPv6
- ▶ only 1 wildcard interface possible
- ightharpoonup it's all done by the host ightarrow slow



Shortcomings

VTIs are not the answer

- ► 2 VTIs per NetNS needed → IPv4 + IPv6
- ▶ only 1 wildcard interface possible
- ightharpoonup it's all done by the host ightarrow slow



Shortcomings

VTIs are not the answer

- ► 2 VTIs per NetNS needed → IPv4 + IPv6
- ▶ only 1 wildcard interface possible
- lacktriangle it's all done by the host o slow



▶ XFRM should be enforced

- ▶ Interfamily support \rightarrow IPv4 + IPv6 through one interface
- ▶ multiple XFRMI with address *any*
- ightharpoonup performace ightarrow offloading support



6 / 6

C. Langrock (secunet) XFRMI Usecase 2018

- ► XFRM should be enforced
- ► Interfamily support → IPv4 + IPv6 through one interface
- ▶ multiple XFRMI with address *any*
- ightharpoonup performace ightarrow offloading support



Whishlist

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



Whishlist

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

