LF NETWORKING
Developer & Testing Forum

strongSwan Kernel-VPP plugin

An Overview

https://lfnetworking.org

K.W Fick
Nanoteq

Background

- Cryptographic solutions.
  - Layer 2 & 3 VPNs.
  - Secure Communications.
  - Hardware-based Cryptography (HSM).
- strongSwan port maintainer on FreeBSD.
- Desire for a 10+ Gbps layer 3 VPN.
- Initially tried to port VPP over to FreeBSD.
  - Had issues with VFIO.
  - Netmap with VPP did not provide the desired performance.
- Decided to rather use a Debian-based OS.

Comparison

strongSwan

- Supports IKE negotiation and management thereof.
- Supports the creation and management of SAs and policies.
- Offloads all data-channel cryptography to a kernel/userland IPsec implementation.

VPP

- Supports IKE negotiation.
- Supports the creation of SAs and policies.
- Supports the creation of tunnel/tap interfaces to create GRE/IP-IP/IPsec tunnels.

Purpose of the plugin

- IKE negotiation is managed by strongSwan.
- strongSwan installs the SAs and policies into VPP (as well as the management thereof).
- VPP uses the SAs or policies to create IPsec interfaces and configure the ESP tunnels to encrypt information.

* Note: For a route-based VPN, routes over the IPSec interface need to be installed in VPP.

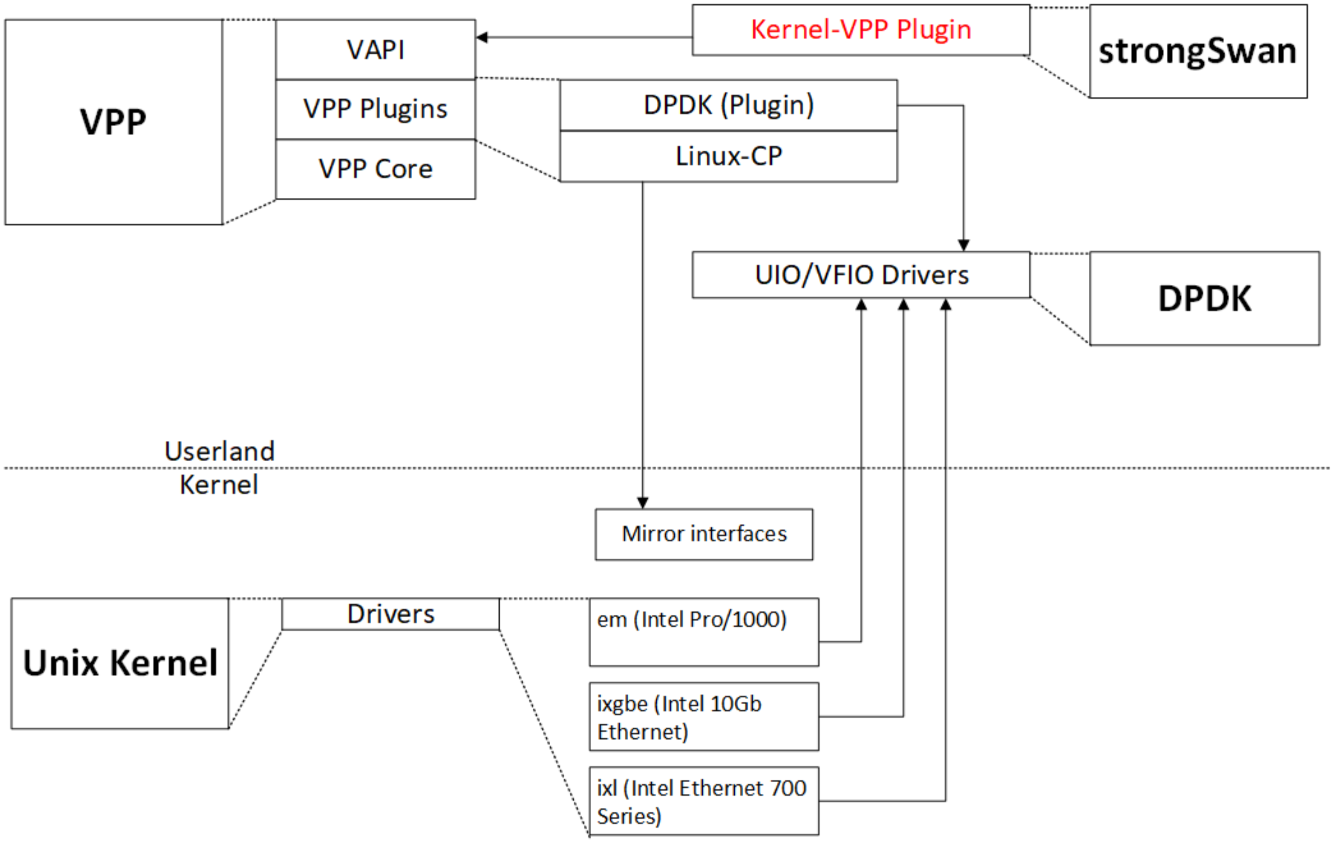
Operational Environment

- OS:
  - Debian 11.3
- Software:
  - strongSwan 5.9.5
  - DPDK 22.02
  - VPP 22.06
    - Linux-CP plugin
    - DPDK plugin
  - Intel-IPsec-MB 1.2

High-level design

- strongSwan
  - Used for IKE negotiation including creation/destruction of SPD’s and SA’s.
  - Interfaces via VPP API.
- VPP
  - Creates IPsec/ESP tunnel.
  - Replaces kernel offloading.
- Linux Control Plane plugin
  - Mirrors interfaces and routes between the Linux kernel and VPP.
  - Can be used to interface with other network services (e.g. dynamic routing, snmp, etc.)
- DPDK
  - Provides data plane libraries.
  - VFIO/UIO driver to interface with crypto hardware (e.g. Intel’s QAT driver).
  - Intel’s libIPsec-MB for crypto acceleration.

High-level design (2)



K.W Fick
Nanoteq

Kernel-VPP Plugin

- Responsible for creating a Security Policy Database (SPD)
  - One SPD on initialisation.
  - Creation/deletion of multiple policies.
- Responsible for managing the Security Associations (SA).
  - Creation/deletion.
  - Handles re-keying/re-authentication.
  - Handles SA expiration.
- Scheduler to handle re-keying based on timeouts/expiration.
- SA Statistics.
  - Byte count.
  - Packet count.

Shortcomings

strongSwan

- Scheduler only handles SA expiry.
- Focus was on tunnel mode, not transport mode.
- Cannot update an SA.

VPP

- Separate traffic selectors for IPv4 and IPv6.
- No statistics available for the policies or the time that an SA has been in use.
- Network protocols are not configurable for the policies.
- IPsec policies cannot be configured to forward traffic.
- IPsec compression not supported.

Testing

Functional

- Creation/deletion of SA's, policies and SPDs.
- Rekey/reauth.
- Statistics.

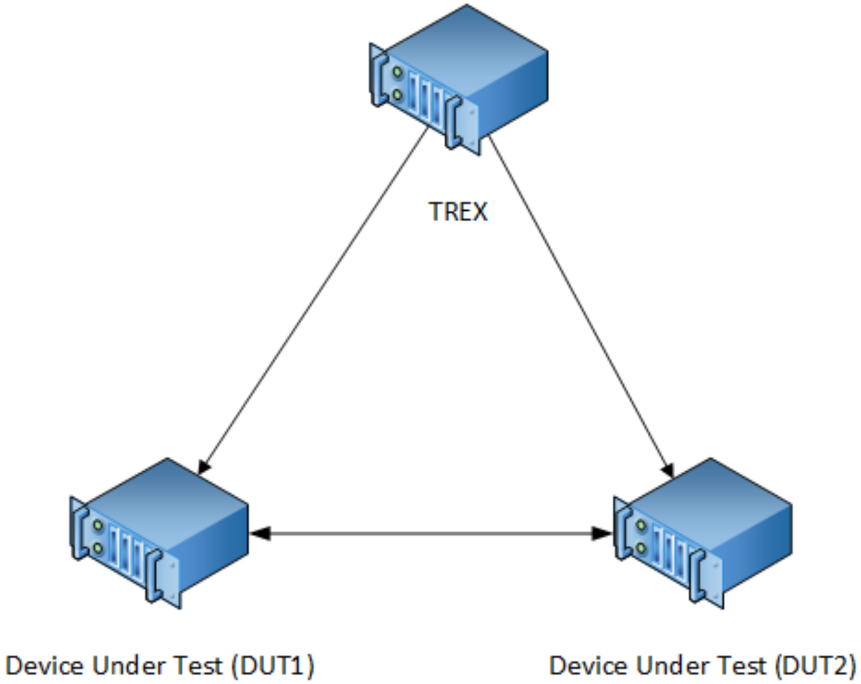
Use-case

- Site-to-Site
  - Route-based VPN
  - Policy-based VPN
- Host-to-host
- Roadwarrior

Testing (2)

Performance

- Stress
- Soak
- Load
- Spike



Desired functionality

- General
  - Automatic creation/deletion of the IPsec interfaces and ESP tunnels.
  - Integration with dynamic routing daemons (for route-based VPN).
  - Hardware-based Cryptography.
- Kernel-VPP Plugin
  - Updating an existing SA.
  - Statistics for the policies.
  - SA timers.

LF NETWORKING

LFN Developer & Testing Forum

Questions?

K.W Fick
Nanoteq