Computer Security Day

QUT isi Information Security Institute

strongSwan

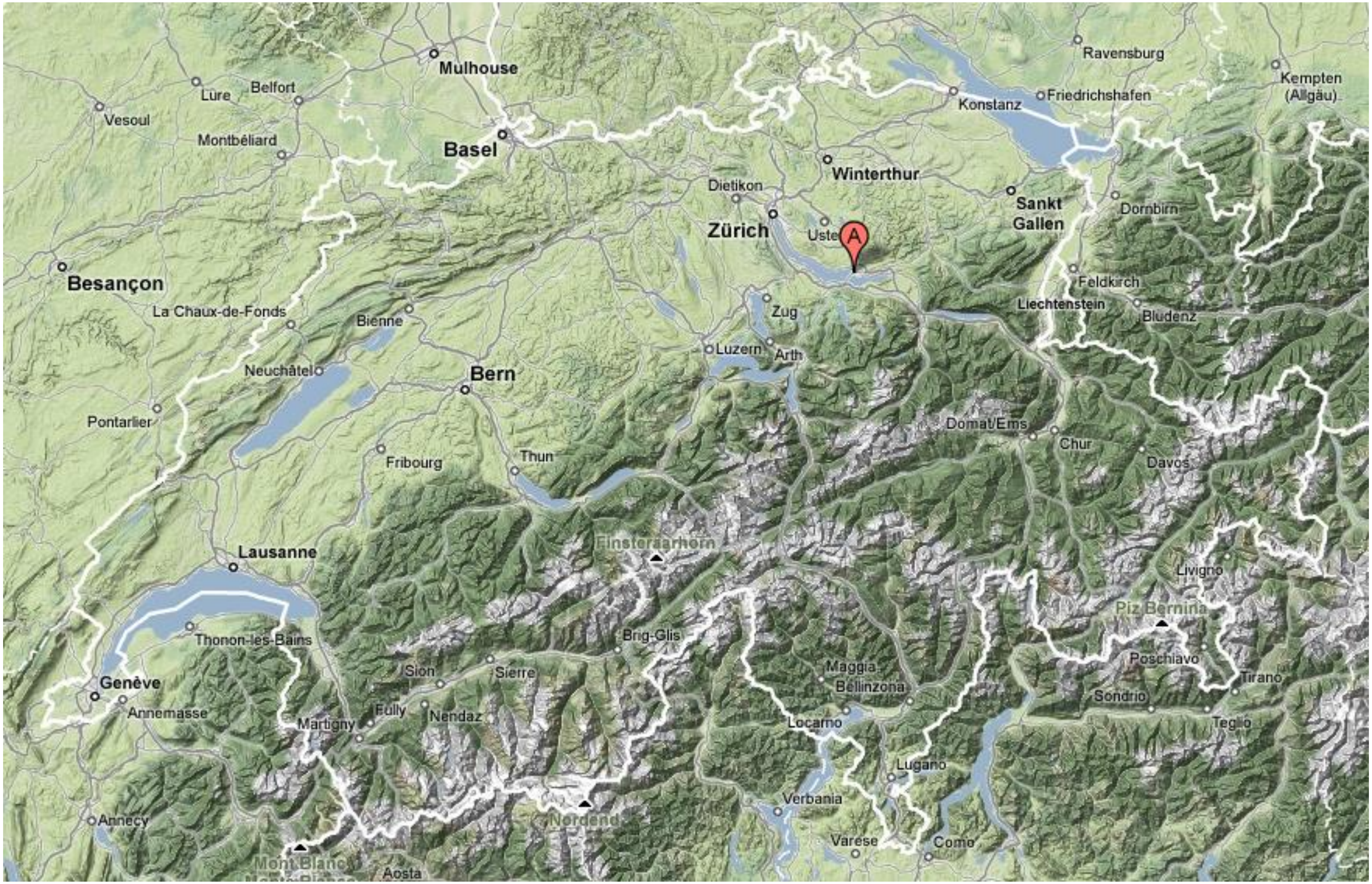
The Linux IPsec Solution

Prof. Andreas Steffen

andreas.steffen@hsr.ch

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

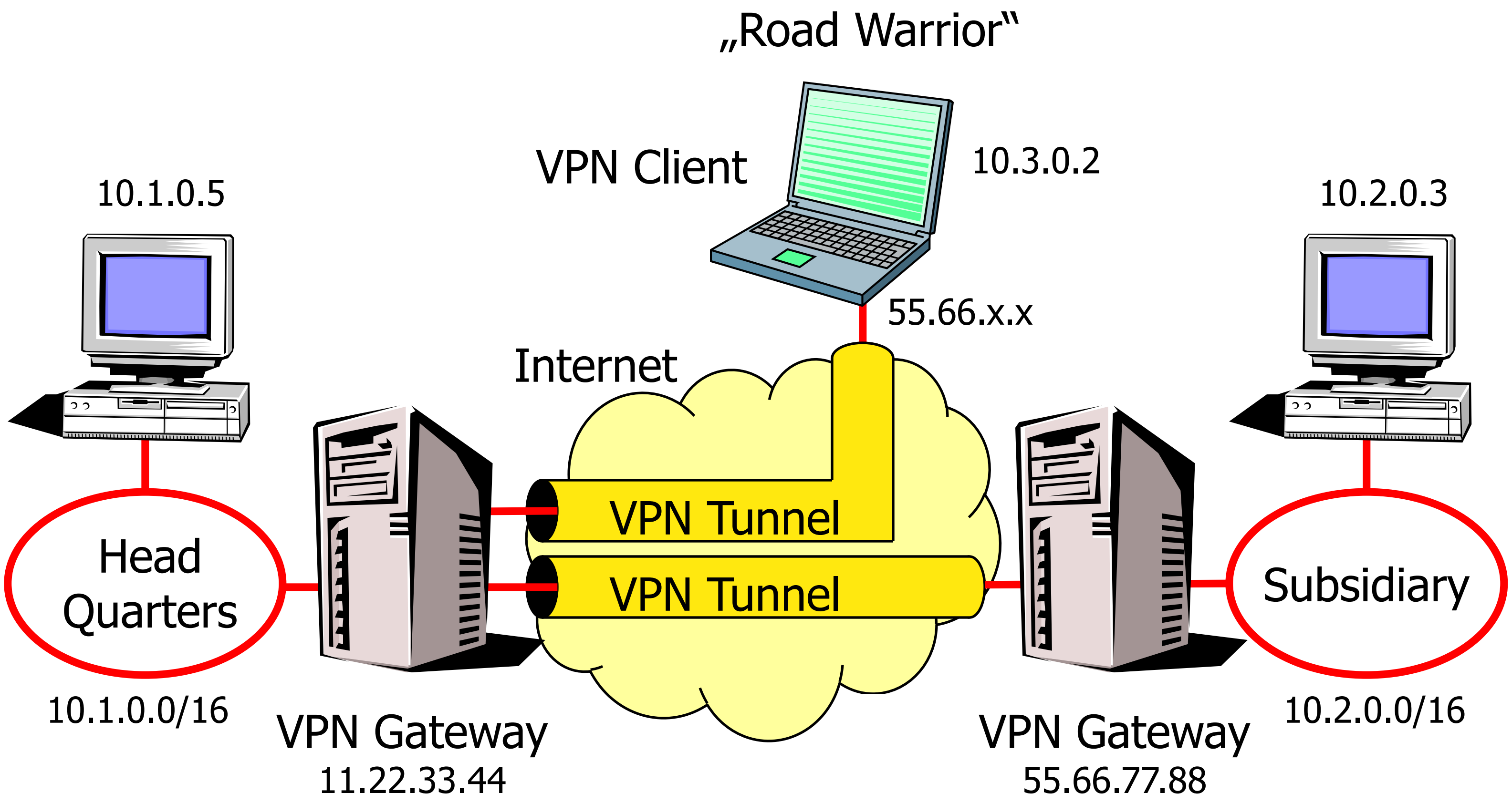
Where the heck is Rapperswil?



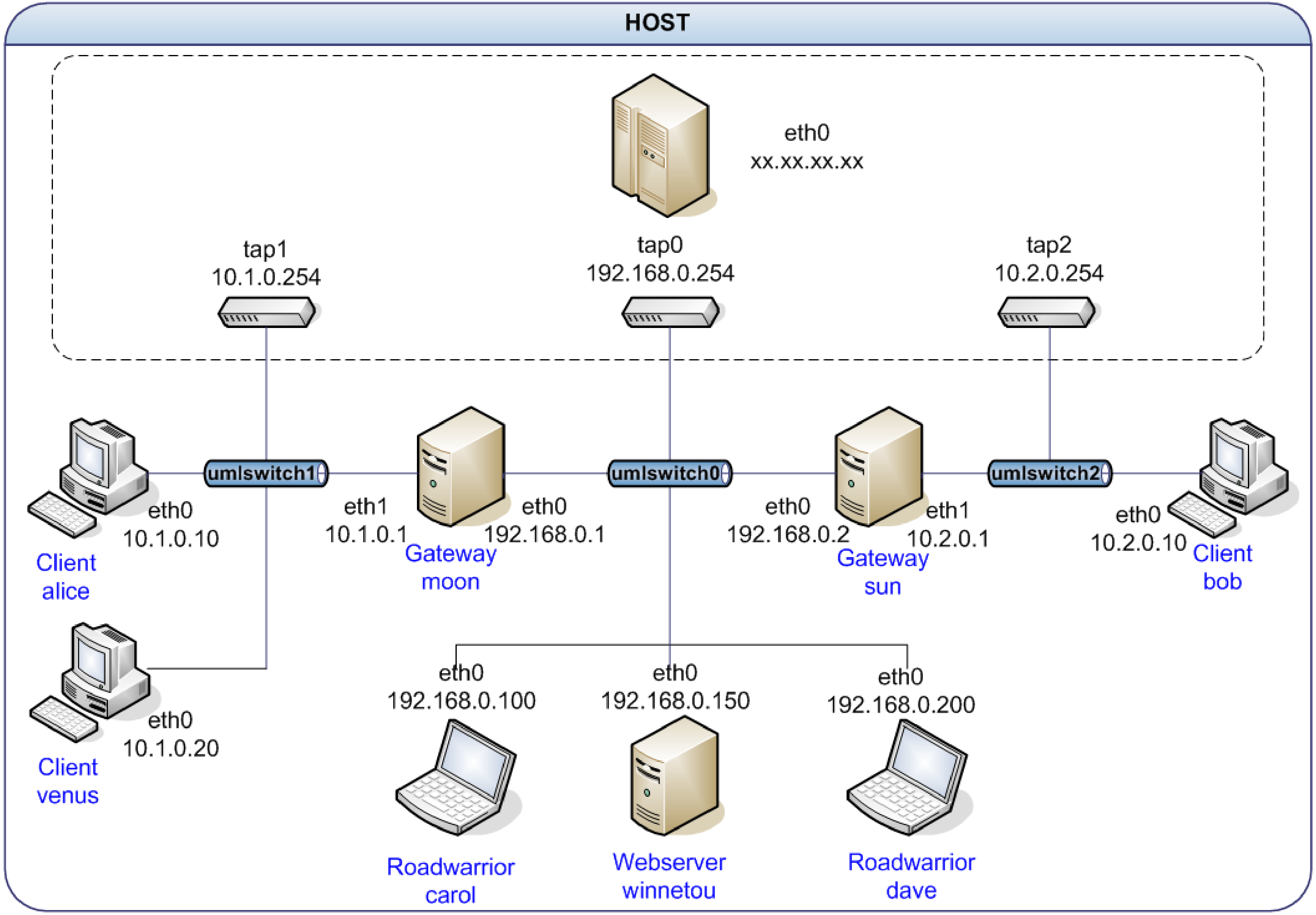
HSR - Hochschule für Technik Rapperswil

- University of Applied Sciences with about 1000 students
- Faculty of Information Technology (300-400 students)
- Bachelor Course (3 years), Master Course (+1.5 years)

Virtual Private Networks



strongSwan User-Mode-Linux VPN Testbed

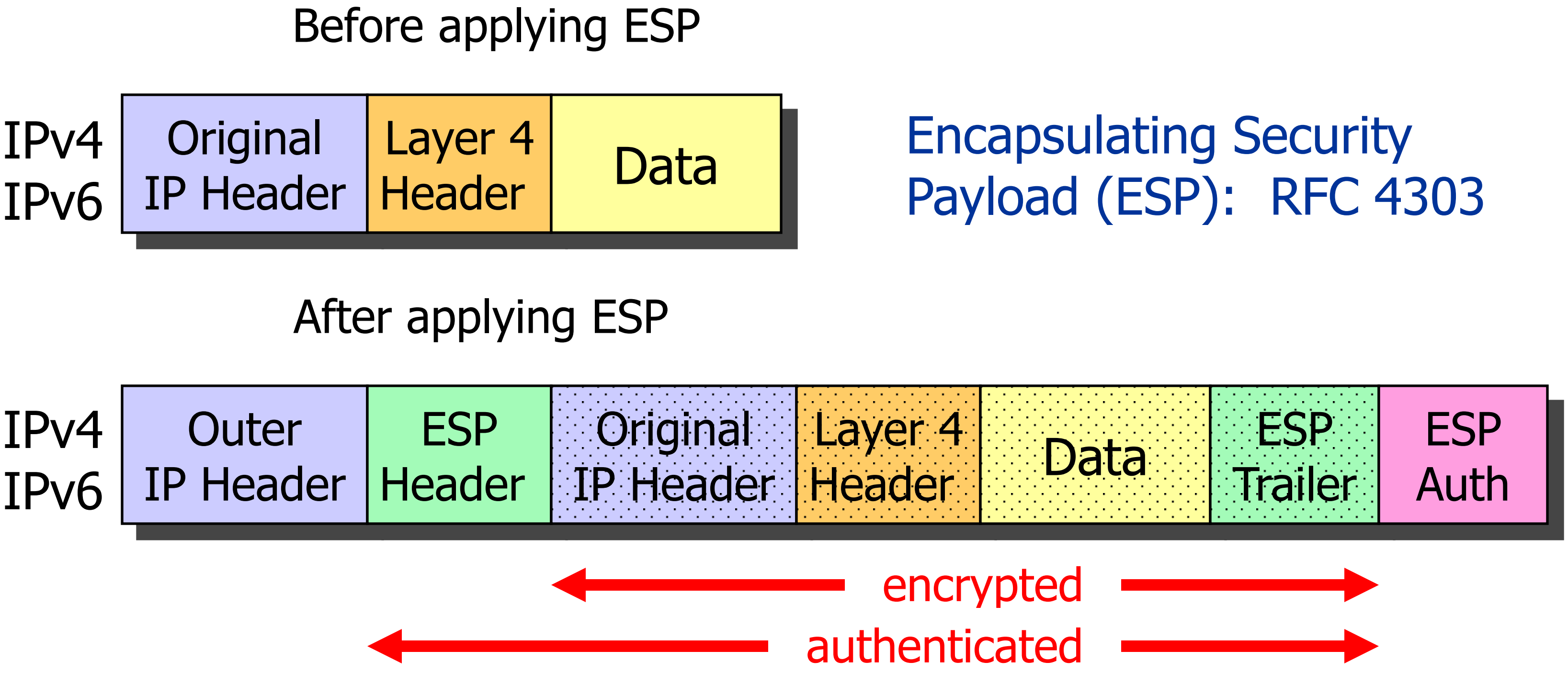


IPsec is a Layer 3 Standard

ESP/AH & IKE

v1 (1998) / v2 (2005)

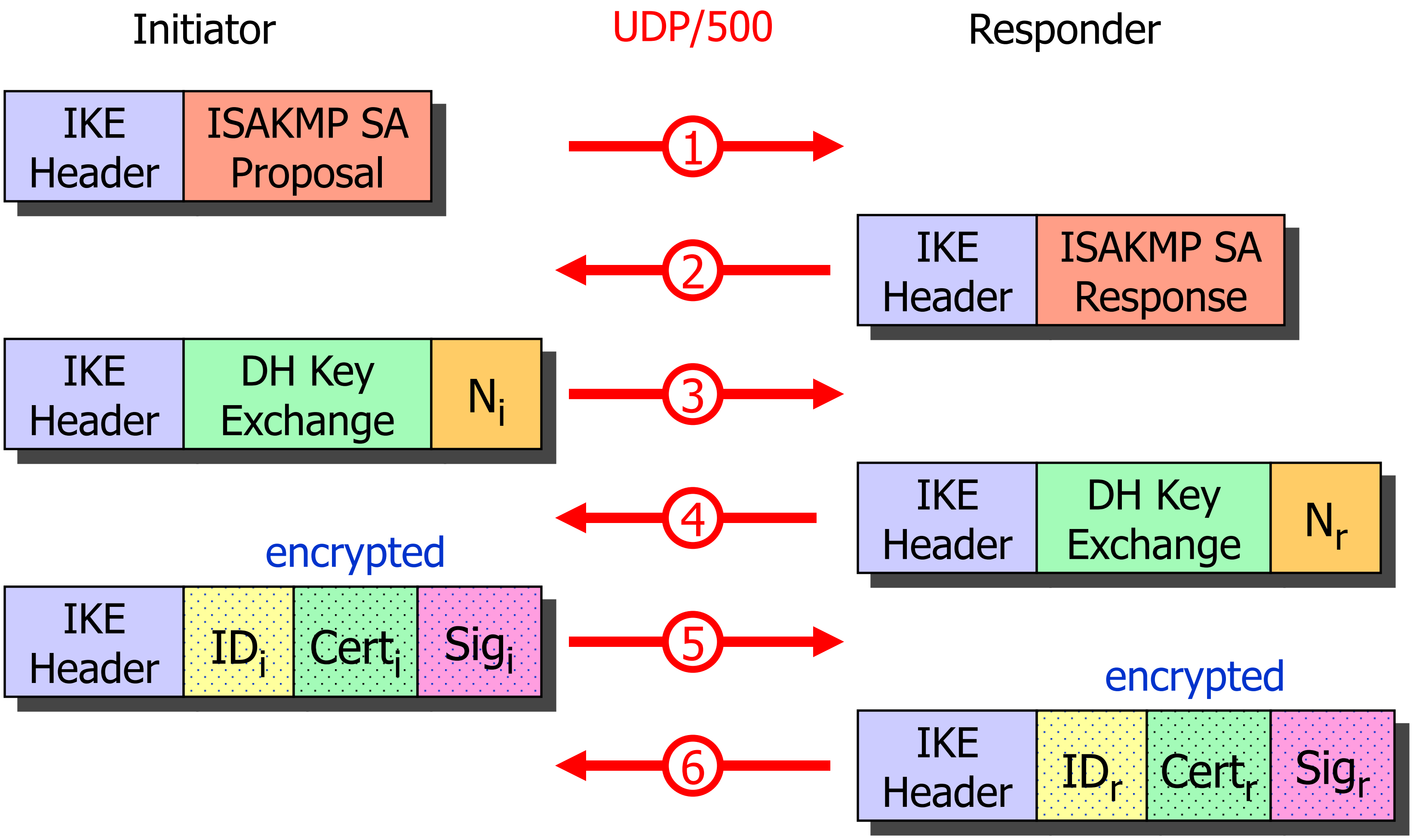
IPsec Tunnel Mode using ESP



Encapsulating Security Payload (ESP): RFC 4303

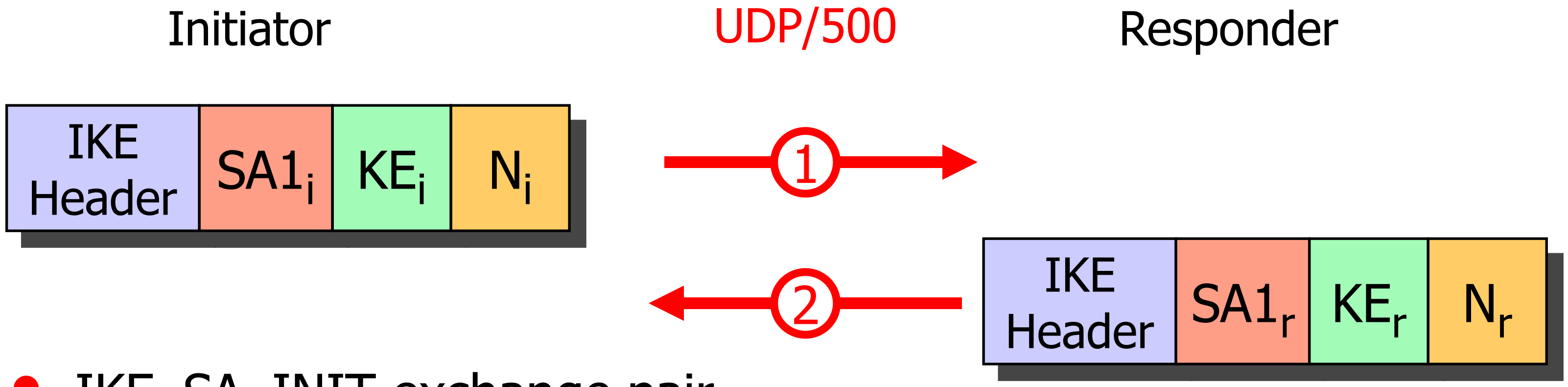
- IP protocol number for ESP: 50 (has no ports!!!)
- ESP authentication is optional but usually used in place of AH (51)
- ESP is implemented by the Linux 2.6 kernel (Dave Miller et al.)

Internet Key Exchange – IKEv1 Main Mode

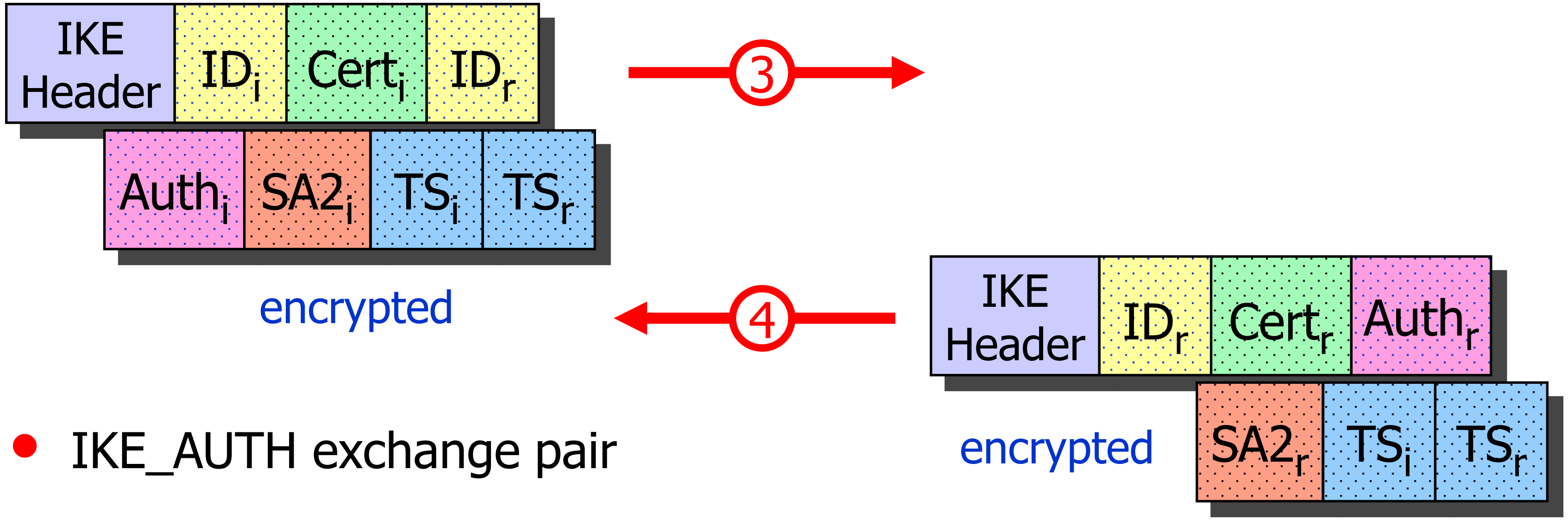


- IKEv1 Quick Mode – another three messages to negotiate traffic selectors

IKEv2 – Authentication and first Child SA

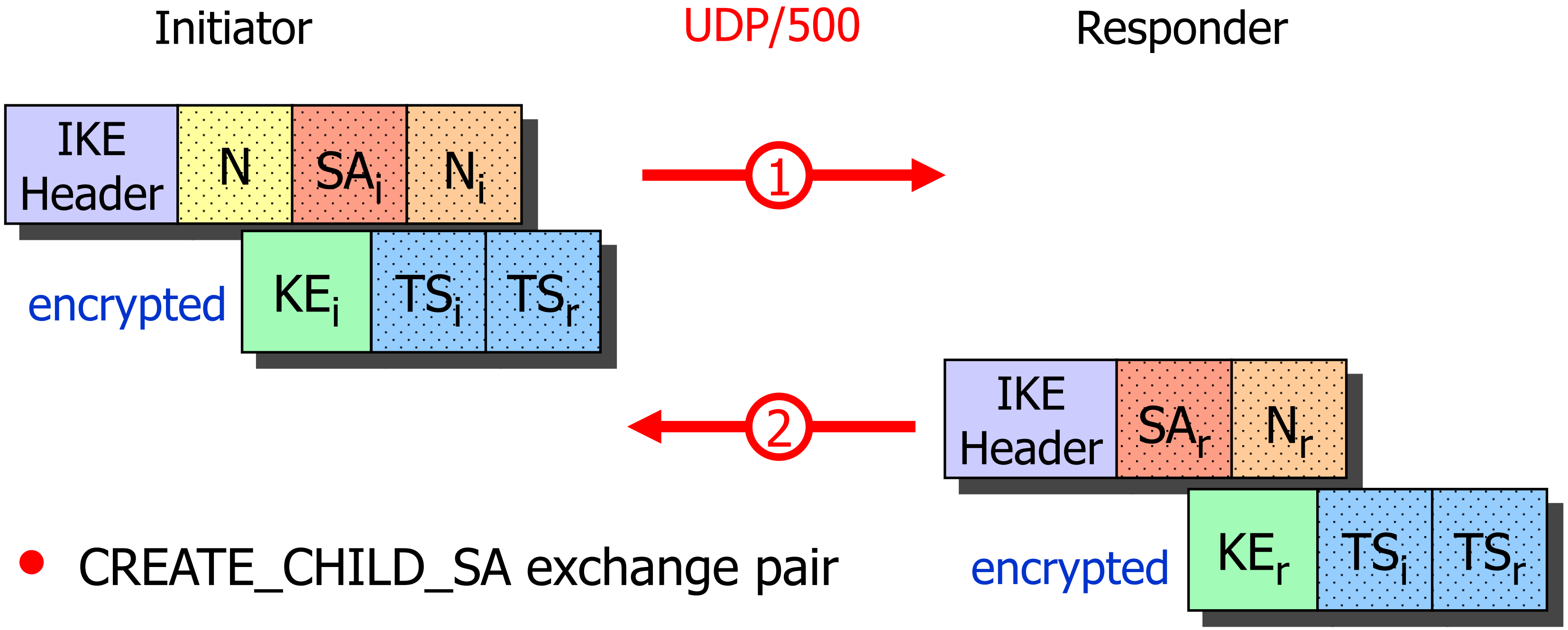


- IKE_SA_INIT exchange pair



- IKE_AUTH exchange pair

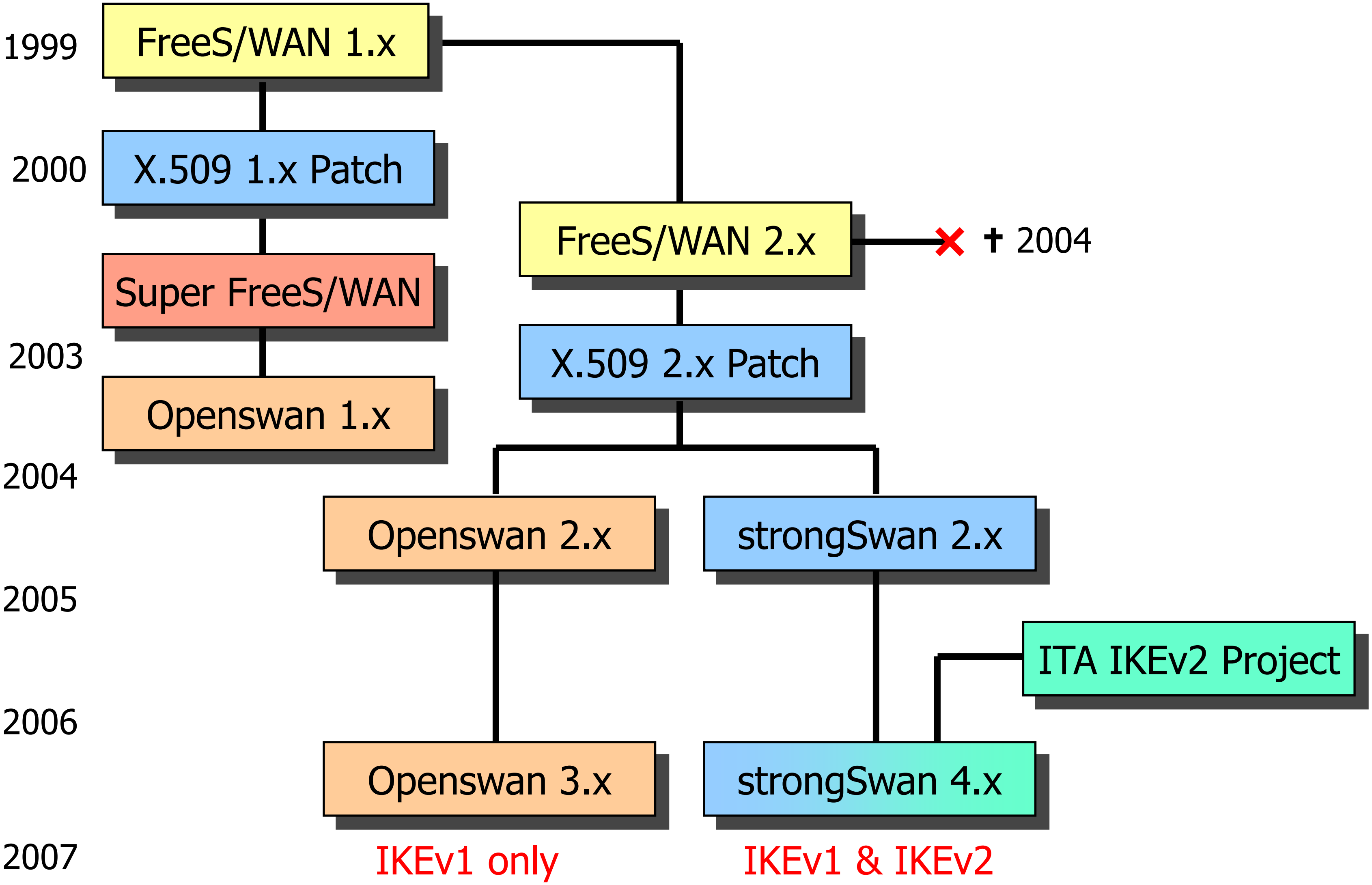
IKEv2 – Additional Child SAs



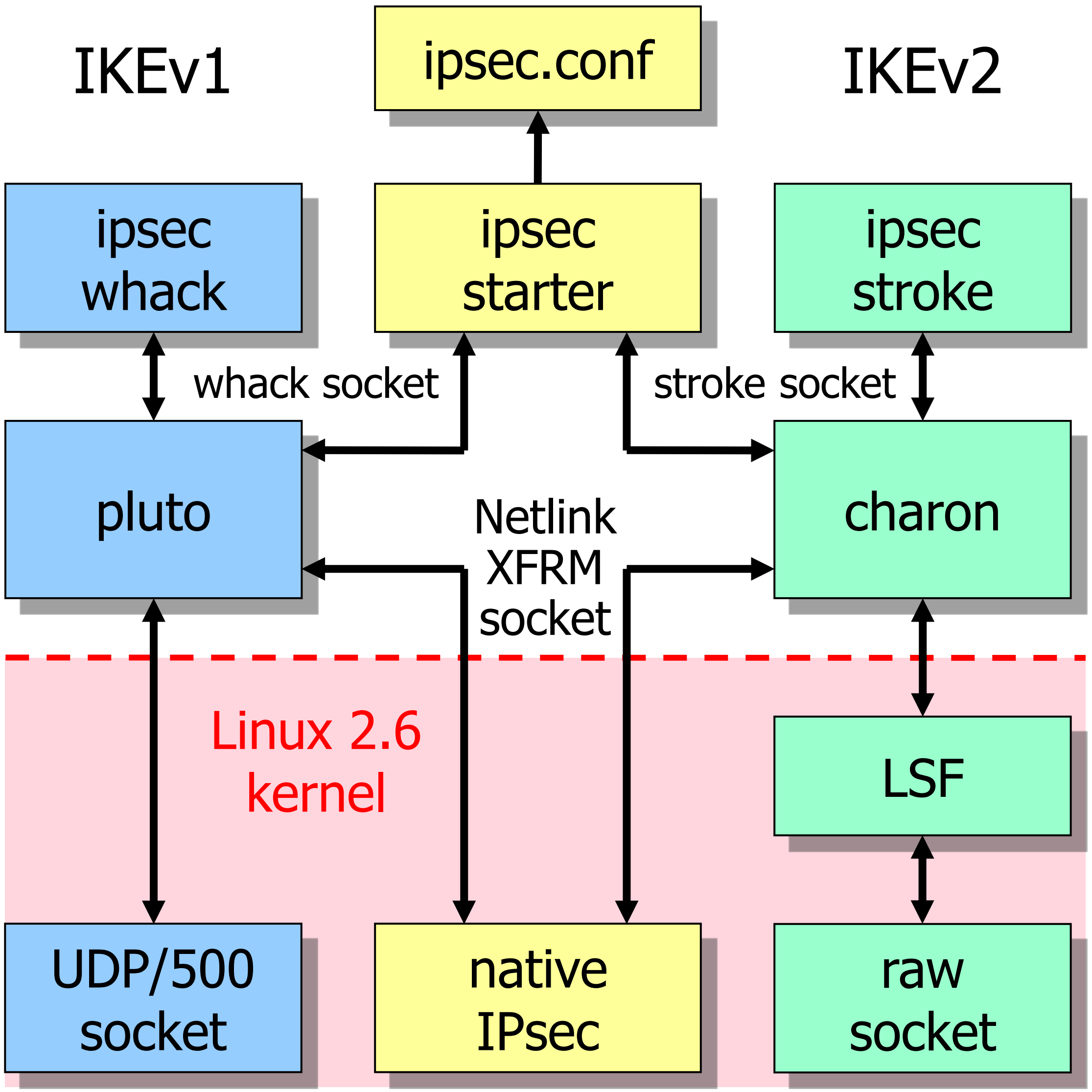
- CREATE_CHILD_SA exchange pair

strongSwan
Software Architecture

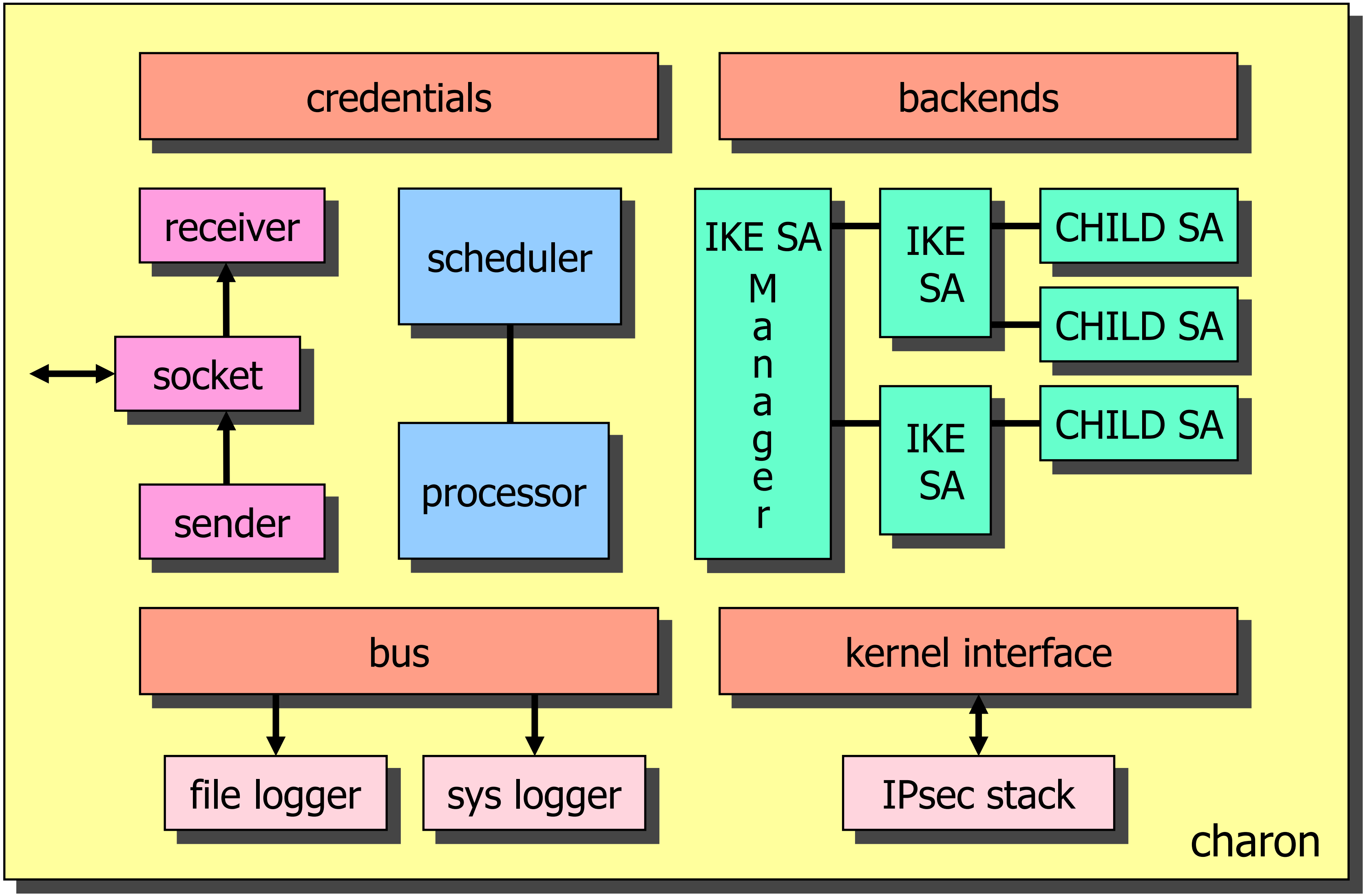
The FreeS/WAN Genealogy



The strongSwan IKE Daemons



IKEv2 Daemon – Software Architecture



16 concurrent worker threads

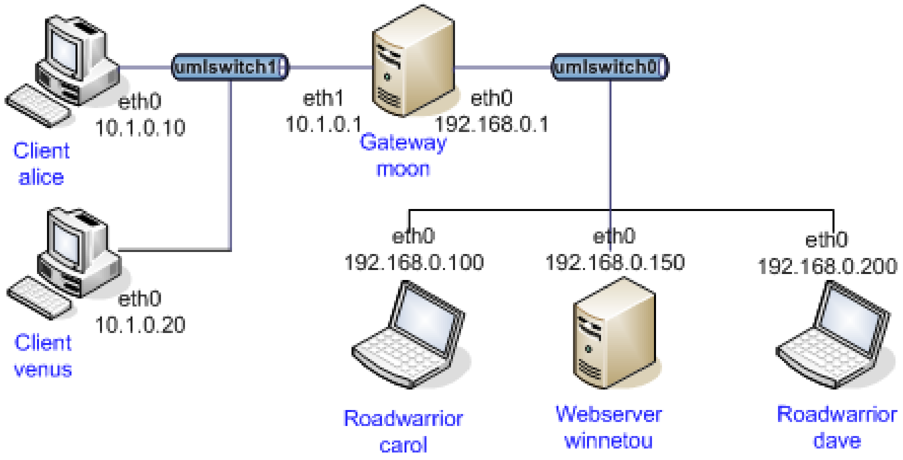
Configuration and Control

The FreeS/WAN way

IKEv2 Mixed PSK/RSA Authentication

```
#ipsec.secrets for roadwarrior carol

carol@strongswan.org : \
      PSK "FpZAZqEN6Ti9sqt4ZP5EWcqx"
```

```
#ipsec.conf for roadwarrior carol

conn home
     keyexchange=ikev2
     authby=psk
     left=%defaultroute
     leftsourceip=%config
     leftid=carol@strongswan.org
     leftfirewall=yes
     right=192.168.0.1
     rightid=@moon.strongswan.org
     rightsubnet=10.0.0.0/16
     auto=start
```



```
#ipsec.secrets for gateway moon

: RSA moonKey.pem

carol@strongswan.org : \
      PSK "FpZAZqEN6Ti9sqt4ZP5EWcqx"

dave@strongswan.org : \
      PSK "jVzONCF02ncsgiSlmIXeqhGN"
```

```
#ipsec.conf for gateway moon

conn rw
     keyexchange=ikev2
     authby=rsasig
     left=%defaultroute
     leftsubnet=10.1.0.0/16
     leftcert=moonCert.pem
     leftid=@moon.strongswan.org
     leftfirewall=yes
     right=%any
     rightsourceip=10.3.0.0/16
     auto=add
```

stroke: Control Interface I

```
carol> ipsec start

05[AUD] initiating IKE_SA 'home' to 192.168.0.1
05[ENC] generating IKE_SA_INIT request 0 [SA KE No N N]
05[NET] sending packet: from 192.168.0.100[500] to 192.168.0.1[500]
06[NET] received packet: from 192.168.0.1[500] to 192.168.0.100[500]
06[ENC] parsed IKE_SA_INIT response 0 [SA KE No N N]
06[ENC] generating IKE_AUTH request 1 [IDi CERTREQ IDr AUTH CP SA TSi TSr]
06[NET] sending packet: from 192.168.0.100[500] to 192.168.0.1[500]
07[NET] received packet: from 192.168.0.1[500] to 192.168.0.100[500]
07[ENC] parsed IKE_AUTH response 1 [IDr CERT AUTH CP SA TSi TSr N]
07[ENC] IKE_SA 'home' established between 192.168.0.100...192.168.0.1
07[IKE] installing new virtual IP 10.3.0.1
07[AUD] CHILD_SA 'home' established successfully
```

stroke: Control Interface II

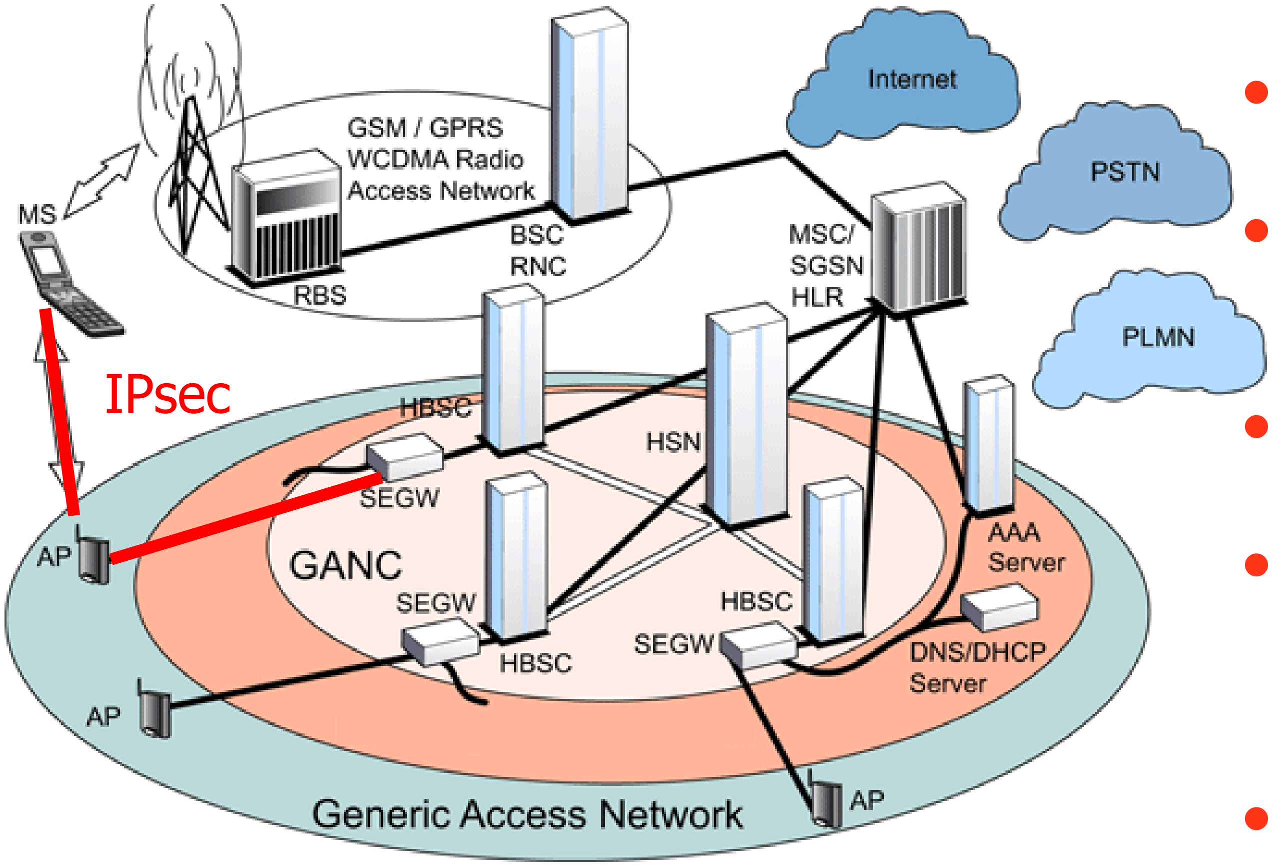
```
carol> ipsec status

Performance:
  uptime: 5 seconds, since Apr 28 18:30:36 2008
  worker threads: 11 idle of 16, job queue load: 1, scheduled events: 5
Listening IP addresses:
  192.168.0.100
  fec0::10
Connections:
  home: 192.168.0.100[carol@strongswan.org]...192.168.0.1[moon.strongswan.org]
  home: dynamic/32 === 10.1.0.0/16
Security Associations:
  home[1]: ESTABLISHED, 192.168.0.100[carol@strongswan.org]...
                        192.168.0.1[moon.strongswan.org]
  home[1]: IKE SPIs: 15993ec81138c1b1_i* ce054ec02da36c8e_r, reauth in 51 minutes
  home{1}: INSTALLED, TUNNEL, ESP SPIs: c51cf634_i cf2c3efd_o
  home{1}: AES_CBC-128/HMAC_SHA1_96, rekeying in 14 minutes, last use: 2s_i 2s_o
  home{1}: 10.3.0.1/32 === 10.1.0.0/16
```

IKEv2 Interoperability Workshops

Spring 2007 in Orlando, Florida
Spring 2008 in San Antonio, Texas

- strongSwan successfully interoperated with IKEv2 products from Alcatel-Lucent, Certicom, CheckPoint, Cisco, Furukawa, IBM, Ixia, Juniper, Microsoft, Nokia, SafeNet, Secure Computing, SonicWall, and the IPv6 TAHI Project.

EAP Authentication or how to earn money

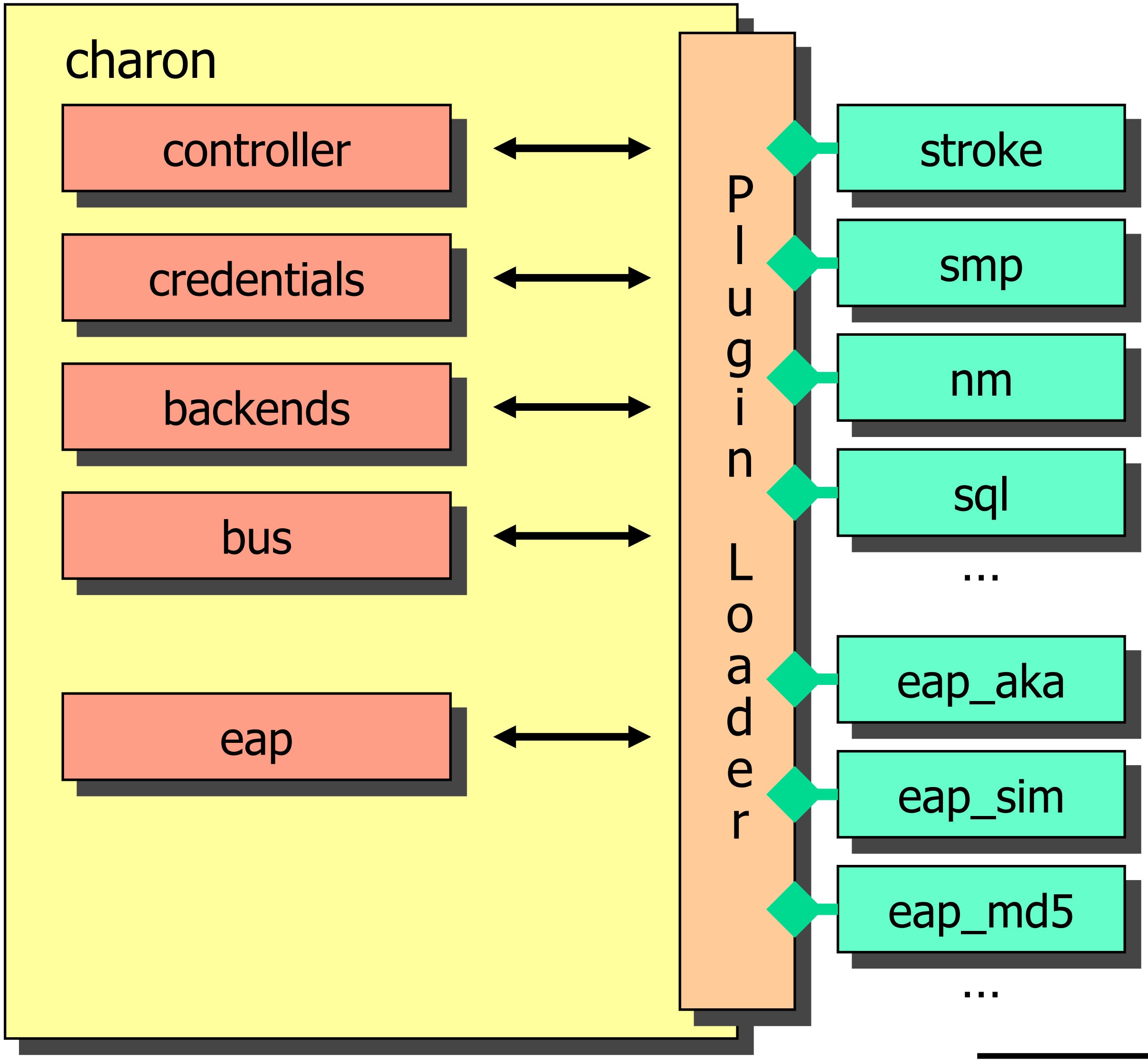


- strongSwan used in FemtoCells
- strongSwan used in industry-grade SEGWs
- Up to 20‘000 concurrent tunnels
- Multiple cores with HW acceleration, e.g. Cavium Networks OCTEON MIPS64
- Google‘s Android???

- The 3GPP Generic Access Network (GAN) enables GSM and UMTS services to be delivered over unlicensed WLAN Access Points (APs). Using IKEv2 EAP-SIM or EAP-AKA authentication the Mobile Station (MS) sets up an IPsec tunnel to the GAN Controller (GANC).

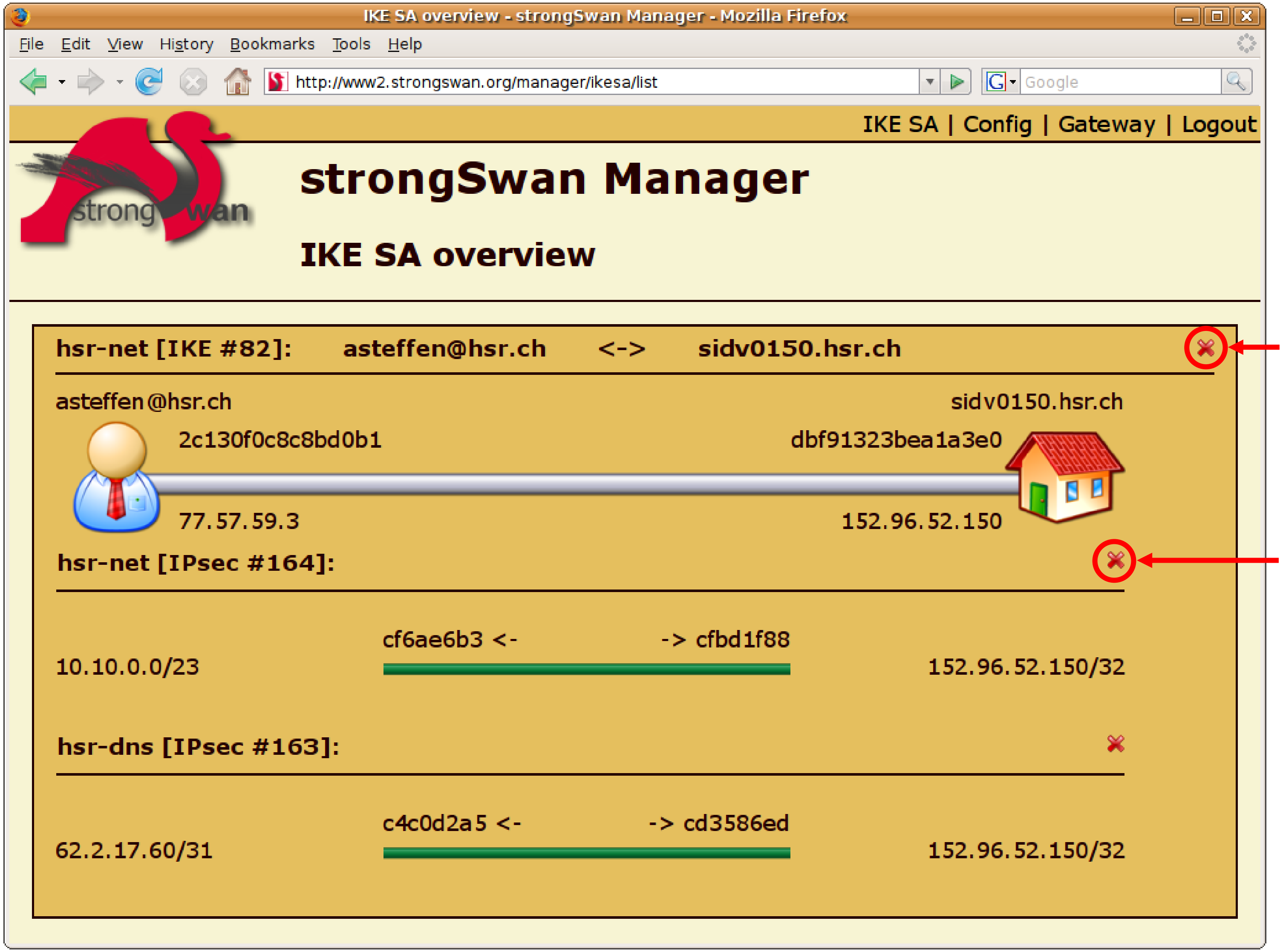
Configuration and Control
The modular way

Plugins for charon



- smp
  XML-based control and management protocol.
  Implementation:
  strongSwan Manager
- nm
  DBUS-based plugin for NetworkManager
- sql
  Generic SQL interface for configurations, credentials & logging.
  Implementations:
  SQLite & MySQL
- eap_x
  Any EAP protocol.

strongSwan Manager



IKE SA overview - strongSwan Manager - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www2.strongswan.org/manager/ikesa/list
Google
IKE SA | Config | Gateway | Logout
strongSwan

strongSwan Manager

IKE SA overview

hsr-net [IKE #82]: asteffen@hsr.ch <-> sidv0150.hsr.ch

asteffen@hsr.ch sidv0150.hsr.ch

2c130f0c8c8bd0b1 dbf91323bea1a3e0

77.57.59.3 152.96.52.150

hsr-net [IPsec #164]:

cf6ae6b3 <- -> cfbd1f88

10.10.0.0/23 152.96.52.150/32

hsr-dns [IPsec #163]:

c4c0d2a5 <- -> cd3586ed

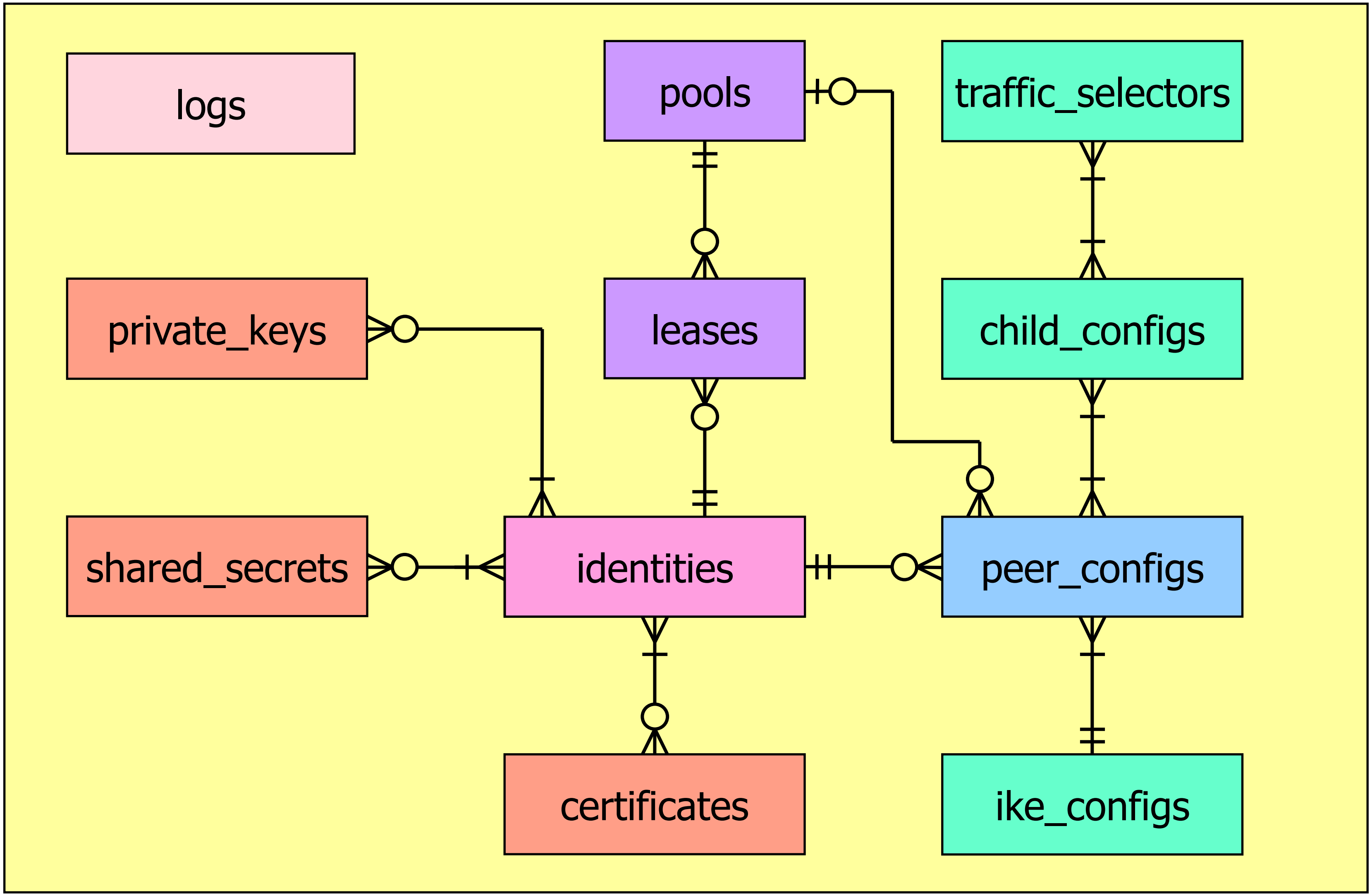
62.2.17.60/31 152.96.52.150/32

take down IKE SA

take down IPsec SA

FastCGI written in C with ClearSilver templates

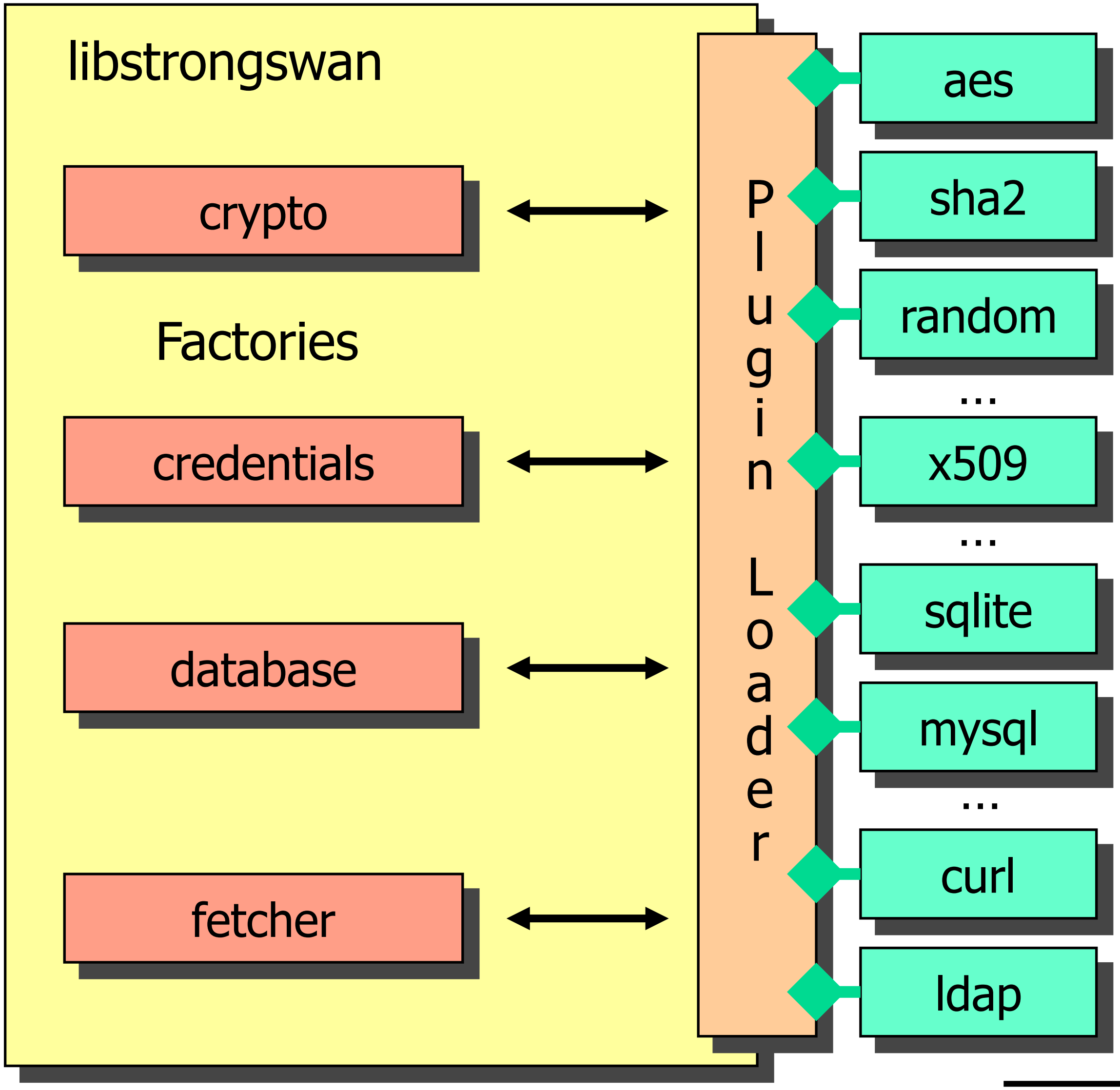
strongSwan Entity Relationship Diagram



SQLite and MySQL implementations

Modular Crypto Plugins

Plugins for libstrongswan

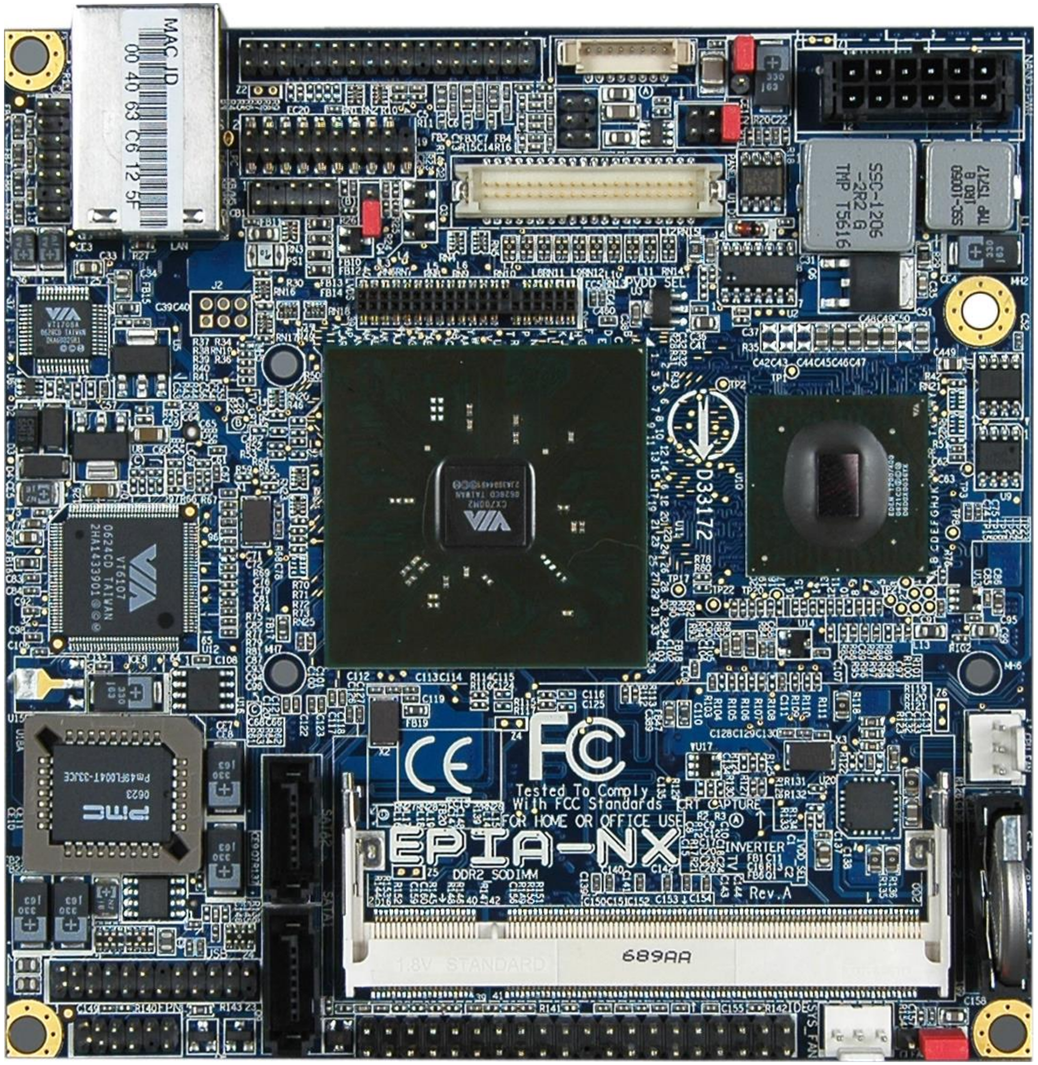


- Non-US crypto code
- No OpenSSL library
- ECCN: No License Required (NLR)

- Certificate retrieval (HASH-and-URL)
- CRL fetching, OCSP

VIA EPIA-NX PadLock Crypto-Processor

- padlock plugin
  AES/SHA
  HW acceleration
- openssl plugin
  uses libcrypto-0.9.8
  OpenSSL library
  - ECP DH groups
  - ECDSA signatures
  - HW engine support



Thank you for your attention!

Questions?

Thank you for your attention!

Questions?