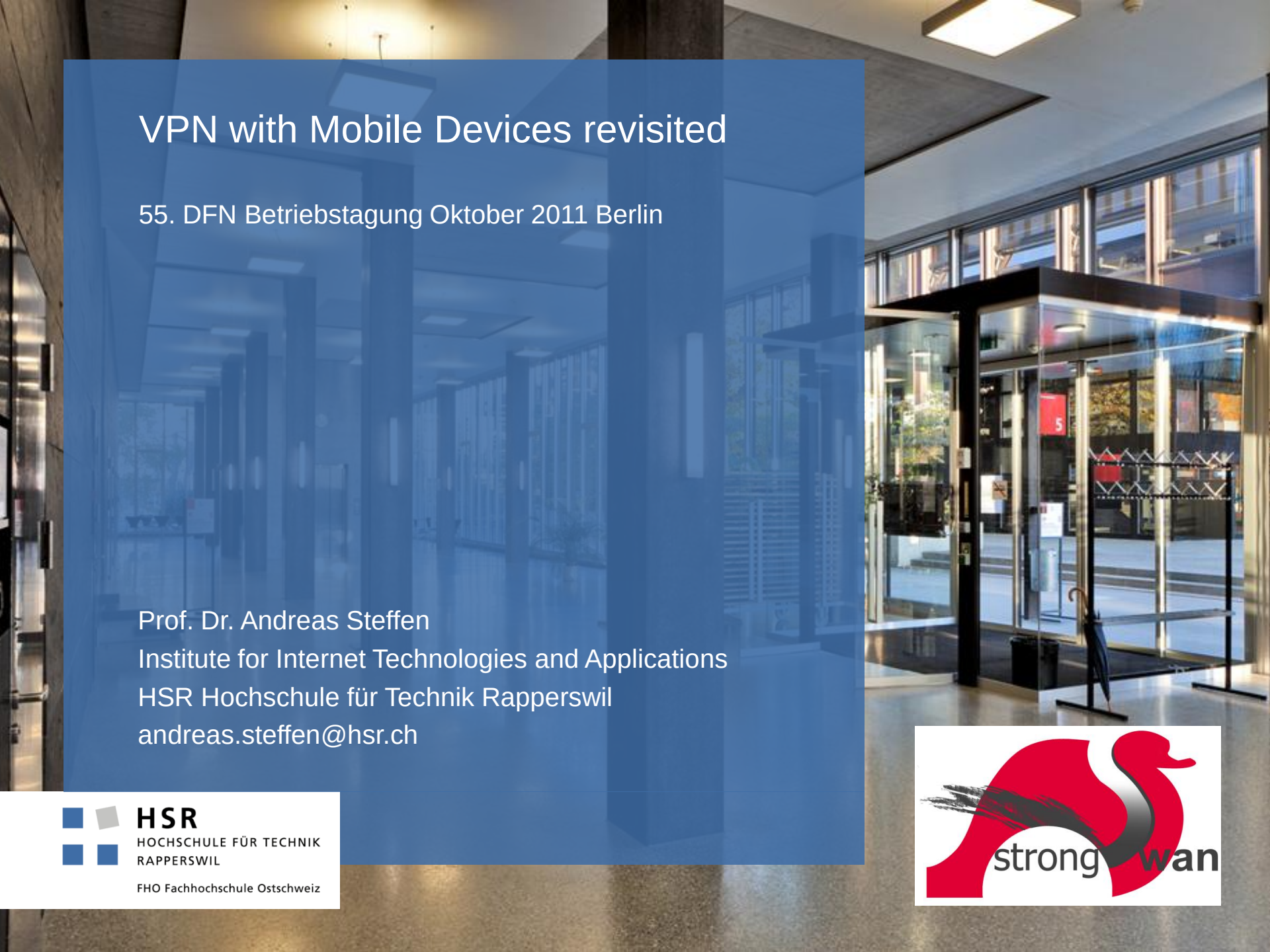
VPN with Mobile Devices revisited

55. DFN Betriebstagung Oktober 2011 Berlin

Prof. Dr. Andreas Steffen
Institute for Internet Technologies and Applications
HSR Hochschule für Technik Rapperswil
andreas.steffen@hsr.ch



HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

strongswan

Problemkreise bei Mobile Devices

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Multihoming bei mehreren Netzwerkkarten (UMTS, WLAN, etc)
  - ➔ IKEv2 MOBIKE Protokoll (RFC 4555)
- Routing im Innern des Tunnels bei dynamischen IP Adressen
  - ➔ Vergabe von virtuellen IP Adressen durch Pool oder DHCP
- Verfügbarkeit des Gateways
  - ➔ High Availability & Load Sharing
- Durch Malware verseuchte Mobile Devices
  - ➔ Trusted Network Connect & Platform Trust Service

VPN with Mobile Devices revisited

55. DFN Betriebstagung Oktober 2011 Berlin

MOBIKE – Mobility and Multihoming Protocol

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

IKEv2 Remote Access Szenario

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

```
#ipsec.secrets for roadwarrior carol

: RSA carolKey.pem "nH5ZQEWtku0RJEZ6"
```

```
#ipsec.secrets for gateway moon

: RSA moonKey.pem
```

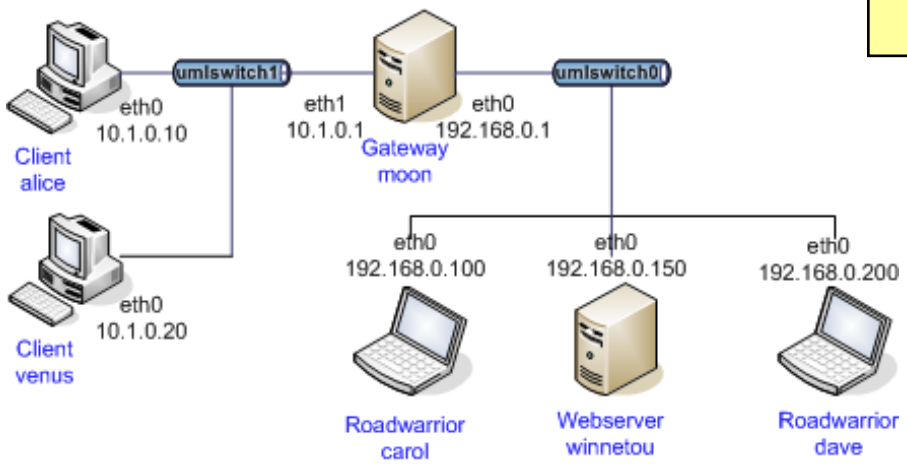
```
#ipsec.conf for roadwarrior carol

conn home
      keyexchange=ikev2
      leftsourceip=%config
      leftcert=carolCert.pem
      leftid=carol@strongswan.org
      leftfirewall=yes
      right=moon.strongswan.org
      rightid=@moon.strongswan.org
      rightsubnet=10.1.0.0/16
      auto=start
```

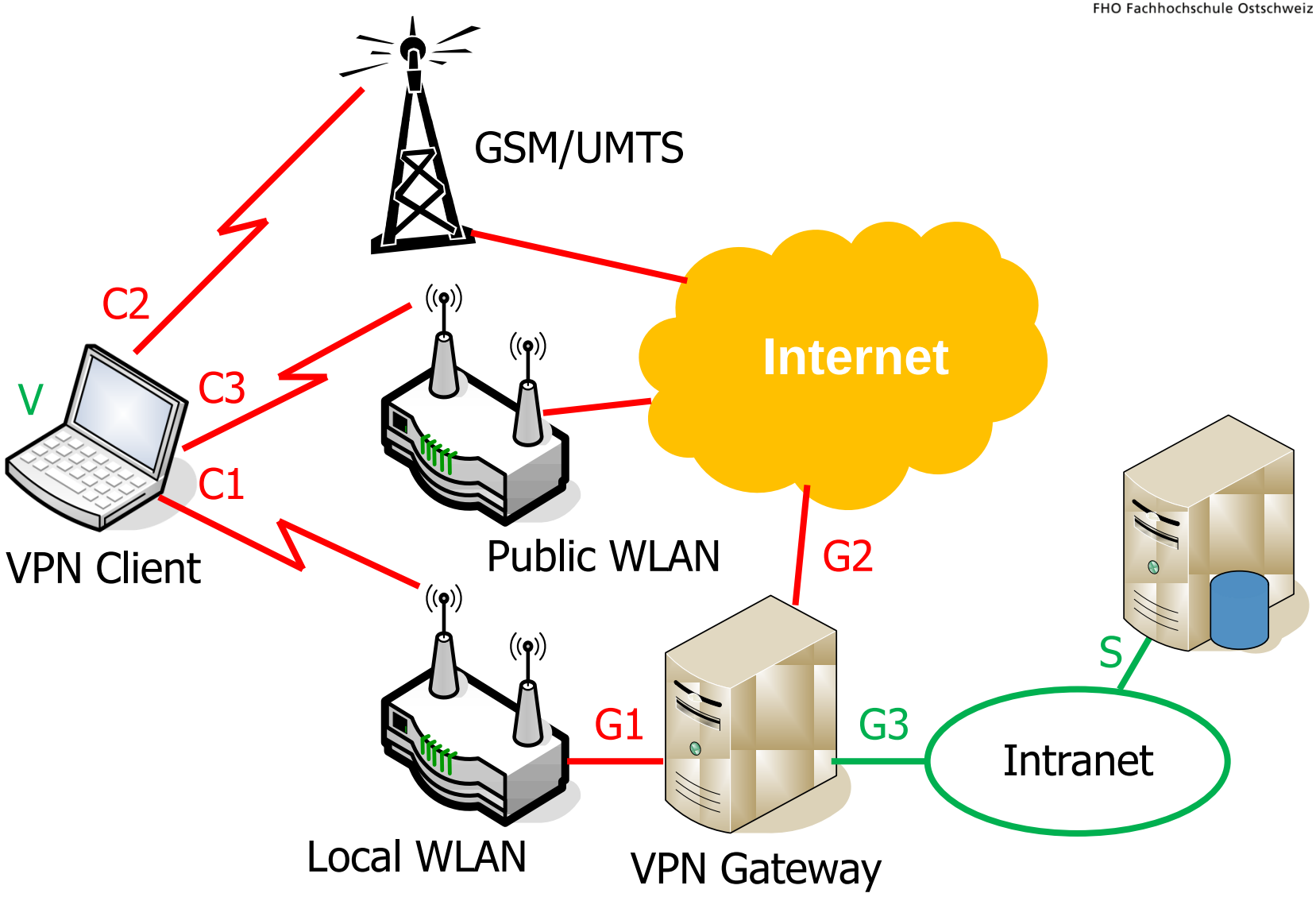
```
#ipsec.conf for gateway moon

config setup
      plutostart=no #IKEv1 not needed

conn rw
      keyexchange=ikev2
      leftsubnet=10.1.0.0/24
      leftcert=moonCert.pem
      leftid=@moon.strongswan.org
      leftfirewall=yes
      right=%any
      rightsourceip=10.3.0.0/24
      auto=add
```



VPN Multihoming Szenario I



VPN Multihoming Szenario II

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Lokale WLAN Verbindung, UMTS Interface im Standby

```
C1 -> G1: IKE_SA Req #0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
C1 <- G1: IKE_SA Res #0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ... ]
C1 -> G1: IKE_AUTH Req #1 [ IDi N(MOBIKE_SUP) N(ADD_4_ADDR C2) ... ]
C1 <- G1: IKE_AUTH Res #1 [ IDr N(MOBIKE_SUP) N(ADD_4_ADDR G2) N(ADD_4_ADDR G3) ]
```

IPsec SA: C1 <-> G1 IPsec Policy: V/32 <-> S/32

- VPN Client verlässt lokales WLAN und schaltet Defaultroute auf UMTS um

```
C2 -> G1: INFORMATIONAL Req #2 [ ]
C2 -> G2: INFORMATIONAL Req #2 [ ]
C2 -> G3: INFORMATIONAL Req #2 [ ]
C2 <- G2: INFORMATIONAL Res #2 [ ]
C2 -> G2: INFORMATIONAL Req #3 [ N(UPD_SA_ADDR) N(NATD_S_IP) N(NATD_D_IP) N(COOKIE2) ]
C2 <- G2: INFORMATIONAL Res #3 [ N(NATD_S_IP) N(NATD_D_IP) N(COOKIE2) ]
```

IPsec SA: C2 <-> G2 IPsec Policy: V/32 <-> S/32

- Der IPsec Tunnel muss nicht neu aufgebaut werden.
  Es wird nur die IPsec SA via IKEv2 MOBIKE (RFC 4555) aufdatiert
- Knacknuss: Wie sollen die gefundenen Routen priorisiert werden?

VPN with Mobile Devices revisited

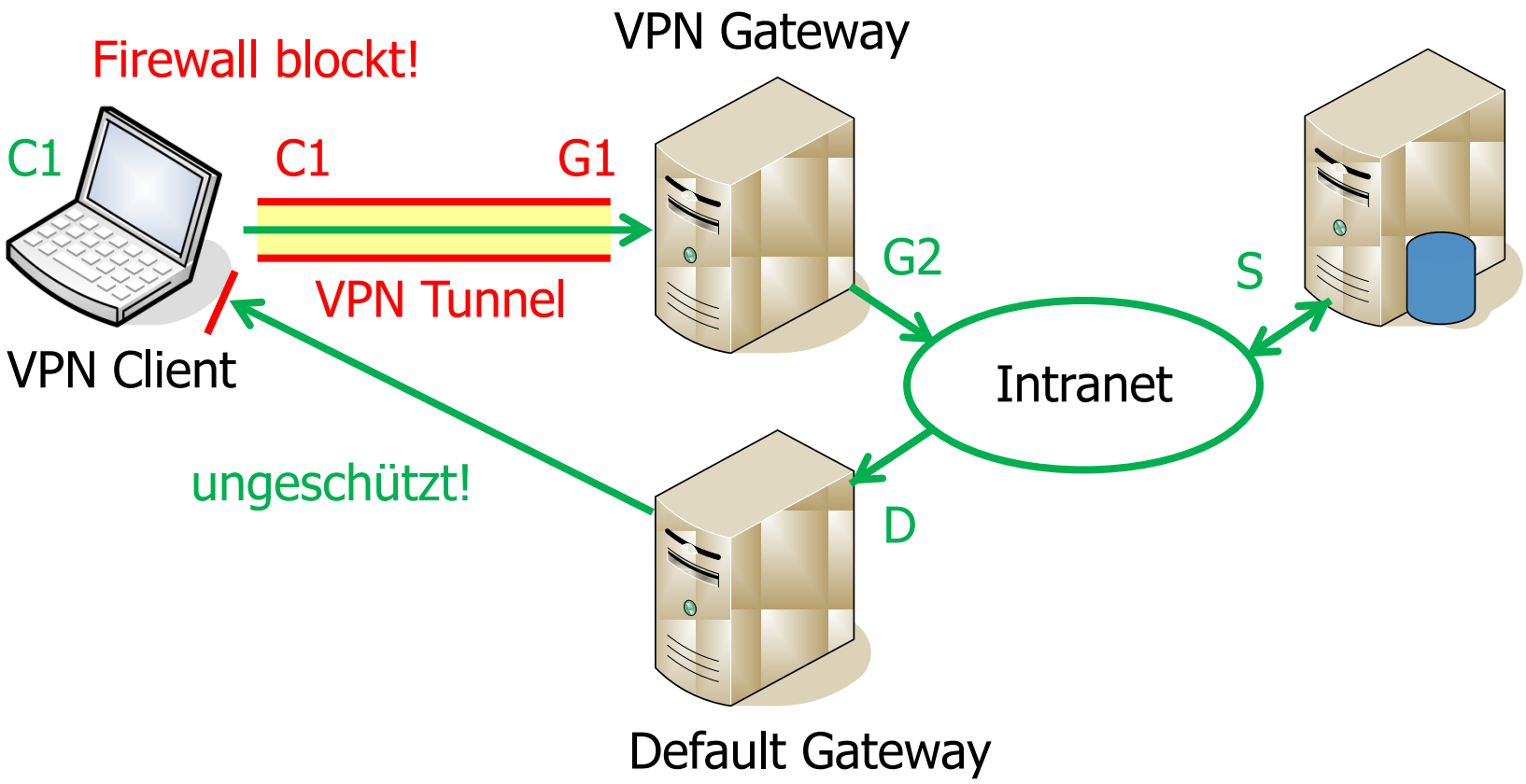
55. DFN Betriebstagung Oktober 2011 Berlin

Virtual IP Address Pools & DHCP Support

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

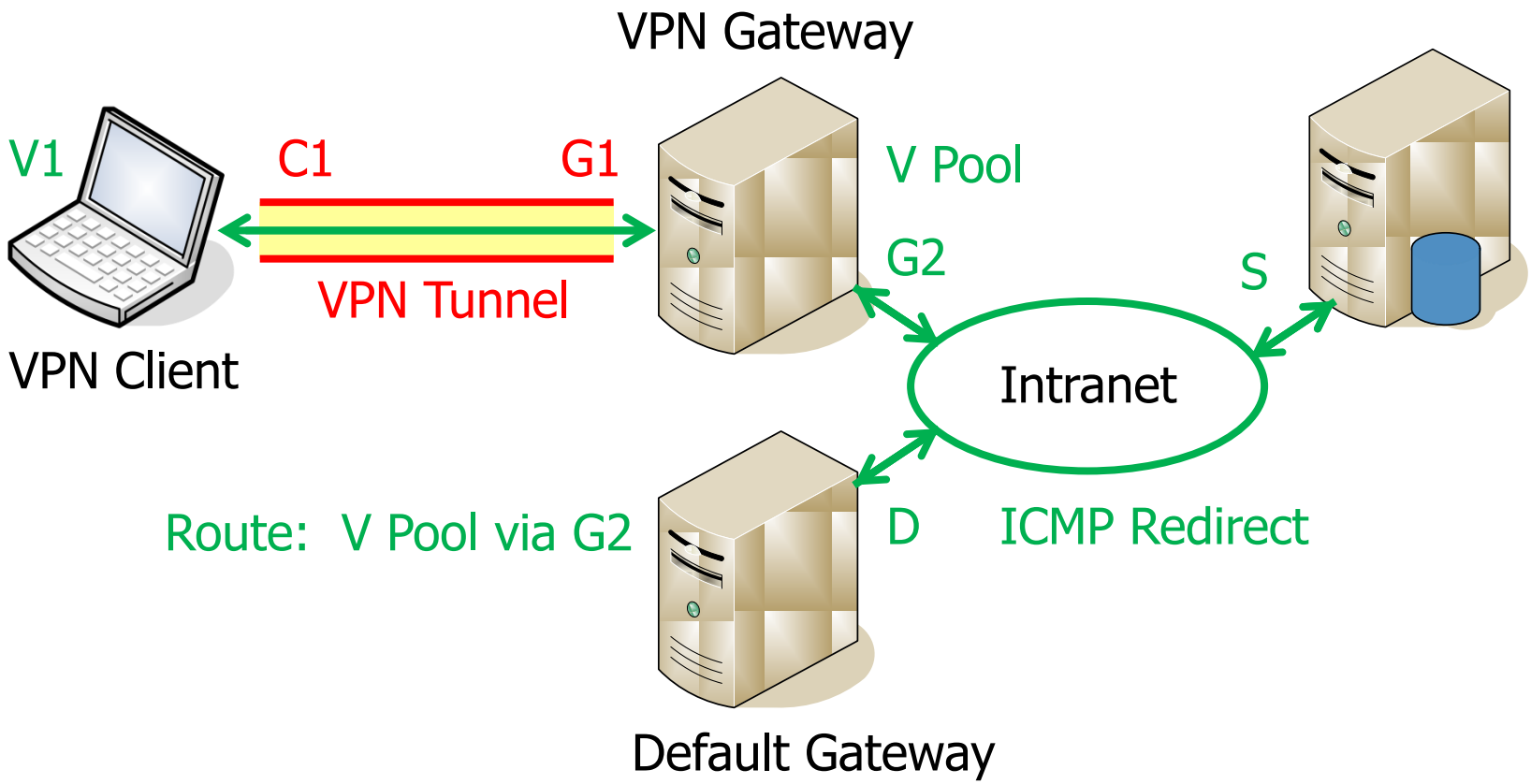
FHO Fachhochschule Ostschweiz

VPN Routing ohne Virtuelle IP Adresse



VPN Routing mit Virtueller IP Adresse

- Virtuelle IP und DNS Information via IKEv2 Configuration Payload



Flüchtiger RAM-basierter IP Address Pool

- Konfiguration in ipsec.conf

```
conn rw
     ...
     rightsourceip=10.3.0.0/24
     auto=add
```

- Statistik

```
ipsec leases

Leases in pool 'rw', usage: 2/255, 2 online
         10.3.0.2   online   'dave@strongswan.org'
         10.3.0.1   online   'carol@strongswan.org'
```

- Referenzieren eines RAM-basierten Pools

```
conn rw1
     ...
     rightsourceip=%rw
     auto=add
```

Persistenter SQL-basierter IP Address Pool I

- SQLite Datenbankschema

```
http://wiki.strongswan.org/repositories/entry/strongswan/
            testing/hosts/default/etc/ipsec.d/tables.sql
```

- Erstellen der SQLite Datenbank

```
cat /etc/ipsec.d/table.sql | sqlite3 /etc/ipsec.d/ipsec.db
```

- Verbinden mit der SQLite Datenbank

```
# /etc/strongswan.conf - strongSwan configuration file

libhydra {
  plugins {
    attr-sql {
      database = sqlite:///etc/ipsec.d/ipsec.db
    }
  }
}
```

Persistenter SQL-basierter IP Address Pool II

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Definition des Pools

```
ipsec pool --add bigpool --start 10.3.0.1 --end 10.3.0.254 --timeout 48
allocating 254 addresses... done.
```

- Konfiguration in ipsec.conf

```
conn rw
     ...
     rightsourceip=%bigpool
     auto=add
```

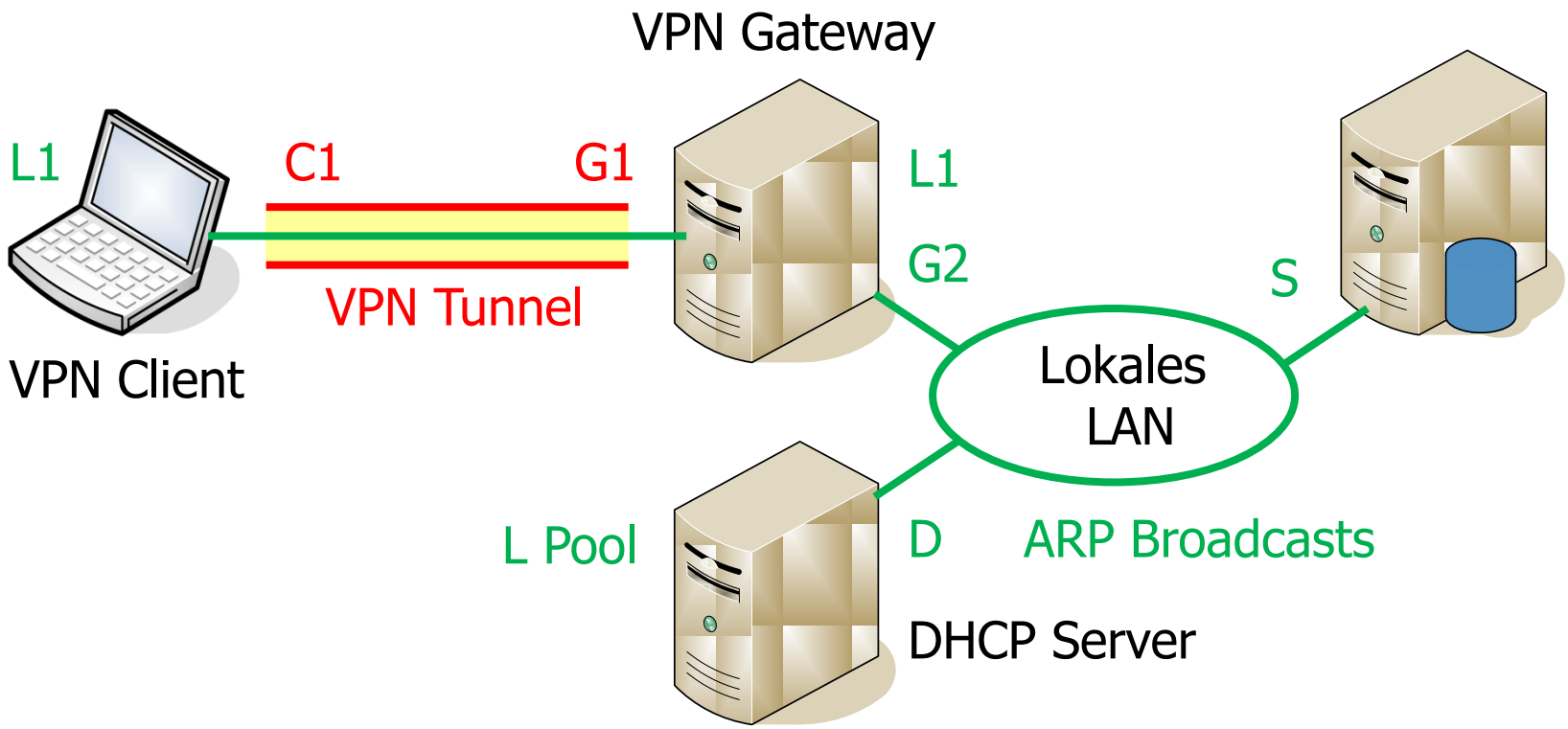
- Statistik

```
ipsec pool --status
name      start       end           timeout  size     online     usage
bigpool   10.3.0.1    10.3.0.254    48h      254      1 ( 0%)    2 ( 0%)

ipsec pool --leases --filter pool=bigpool
name      address  status start                end                  identity
bigpool   10.3.0.1 online Oct 22 23:13:50 2009                     carol@strongswan.org
bigpool   10.3.0.2 valid  Oct 22 23:14:11 2009 Oct 22 23:14:25 2009 dave@strongswan.org
```

VPN Gateway als ARP und DHCP Proxy

- VPN Gateway verlangt vom DHCP Server lokale IP Adresse und sendet sie via IKEv2 Configuration Payload an VPN Client.



- VPN Gateway beantwortet stellvertretend für VPN Client ARP Anfragen. Dadurch werden IP Pakete an den VPN Client automatisch getunnelt.

strongSwan SOHO Lösung für Windowsnetze

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

revobox office

Verbindungen | Benutzerkonten | Gerät | Log | Abmelden

VPN Verbindungs-Log

```
[21.07.11 22:26:26] initiating EAP_IDENTITY method (id 0x00)
[21.07.11 22:26:26] peer supports MOBIKE
[21.07.11 22:26:26] authentication of 'C=CH, O=revosec AG, CN=PBL6HJ7E' (myself) w
[21.07.11 22:26:26] sending end entity cert "C=CH, O=revosec AG, CN=PBL6HJ7E"
[21.07.11 22:26:26] generating IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/ID ]
[21.07.11 22:26:26] sending packet: from 10.10.1.24[4500] to 193.247.250.29[20089]
[21.07.11 22:26:26] received packet: from 193.247.250.29[20089] to 10.10.1.24[4500
[21.07.11 22:26:26] parsed IKE_AUTH request 2 [ EAP/RES/ID ]
[21.07.11 22:26:26] received EAP identity '1300-0010-3767-2178@upn.suisseid.ch'
[21.07.11 22:26:26] initiating EAP_TLS method (id 0x6E)
[21.07.11 22:26:26] generating IKE_AUTH response 2 [ EAP/REQ/TLS ]
[21.07.11 22:26:26] sending packet: from 10.10.1.24[4500] to 193.247.250.29[20089]
[21.07.11 22:26:27] received packet: from 193.247.250.29[20089] to 10.10.1.24[4500
[21.07.11 22:26:27] parsed IKE_AUTH request 3 [ EAP/RES/TLS ]
[21.07.11 22:26:27] received TLS 'renegotiation info' extension
[21.07.11 22:26:27] received TLS 'elliptic curves' extension
[21.07.11 22:26:27] received TLS 'ec point formats' extension
[21.07.11 22:26:27] negotiated TLS version TLS 1.0 with suite TLS_RSA_WITH_AES_128
[21.07.11 22:26:27] sending TLS server certificate 'C=CH, O=revosec AG, C
[21.07.11 22:26:27] sending TLS cert request for 'C=CH, O=SwissSign AG, C
[21.07.11 22:26:27] sending TLS cert request for 'C=ch, O=Swisscom, OU=Di
[21.07.11 22:26:27] sending TLS cert request for 'C=BM, O=QuoVadis Limite
[21.07.11 22:26:27] generating IKE_AUTH response 3 [ EAP/REQ/TLS ]
[21.07.11 22:26:27] sending packet: from 10.10.1.24[4500] to 193.247.250.
[21.07.11 22:26:27] received packet: from 193.247.250.29[20089] to 10.10.
[21.07.11 22:26:27] parsed IKE_AUTH request 4 [ EAP/RES/TLS ]
[21.07.11 22:26:27] generating IKE_AUTH response 4 [ EAP/REQ/TLS ]
[21.07.11 22:26:27] sending packet: from 10.10.1.24[4500] to 193.247.250.
```

revobox office v0.11- © 2011 revosec AG

www.revosec.ch

VPN with Mobile Devices revisited

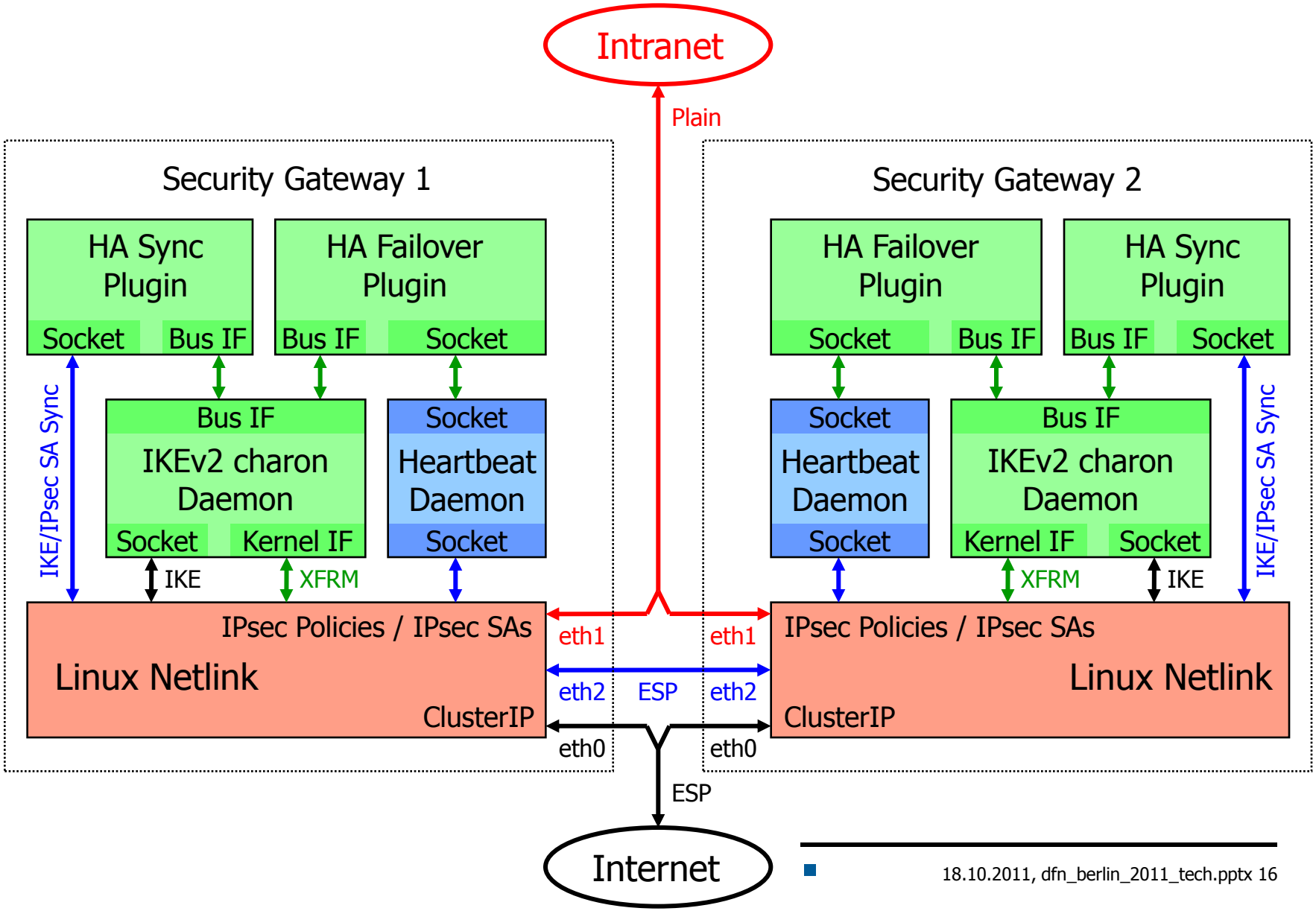
55. DFN Betriebstagung Oktober 2011 Berlin

High Availability mit ClusterIP

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

strongSwan High-Availability Architektur



Lösungsansatz

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

- Die äusseren eth0 und inneren eth1 Interfaces von SG1 und SG2 teilen sich je eine Phantom IP Adresse mit zugehöriger Multicast MAC Adresse.
- Dadurch erhalten beide SGs alle verschlüsselten ESP Pakete auf eth0 und synchronisieren so ständig die Anti-Replay Sequenznummern.
- Auf der Basis von ClusterIP (Hash über Source IP und SPI des ESP Packets) entscheidet jeder SG für welche IPsec SAs er zuständig ist.
- ClusterIP (Hash über Destination IP und SPI der IPsec SA) wird auch ausgangsseitig auf die Klartextpakete von eth1 angewendet.
- Für IKEv2 ist nur ein Master SG zuständig. Alle IKEv2 und ESP Schlüssel werden auf dem Slave SG gespiegelt.
- Fällt ein SG aus, übernimmt der andere sofort sämtliche IPsec SAs.
- Fällt der Master SG aus, übernimmt sofort der Slave SG sofort die IKEv2 Verbindungen mit quasi-synchronisierten Sequenznummern.

VPN with Mobile Devices revisited

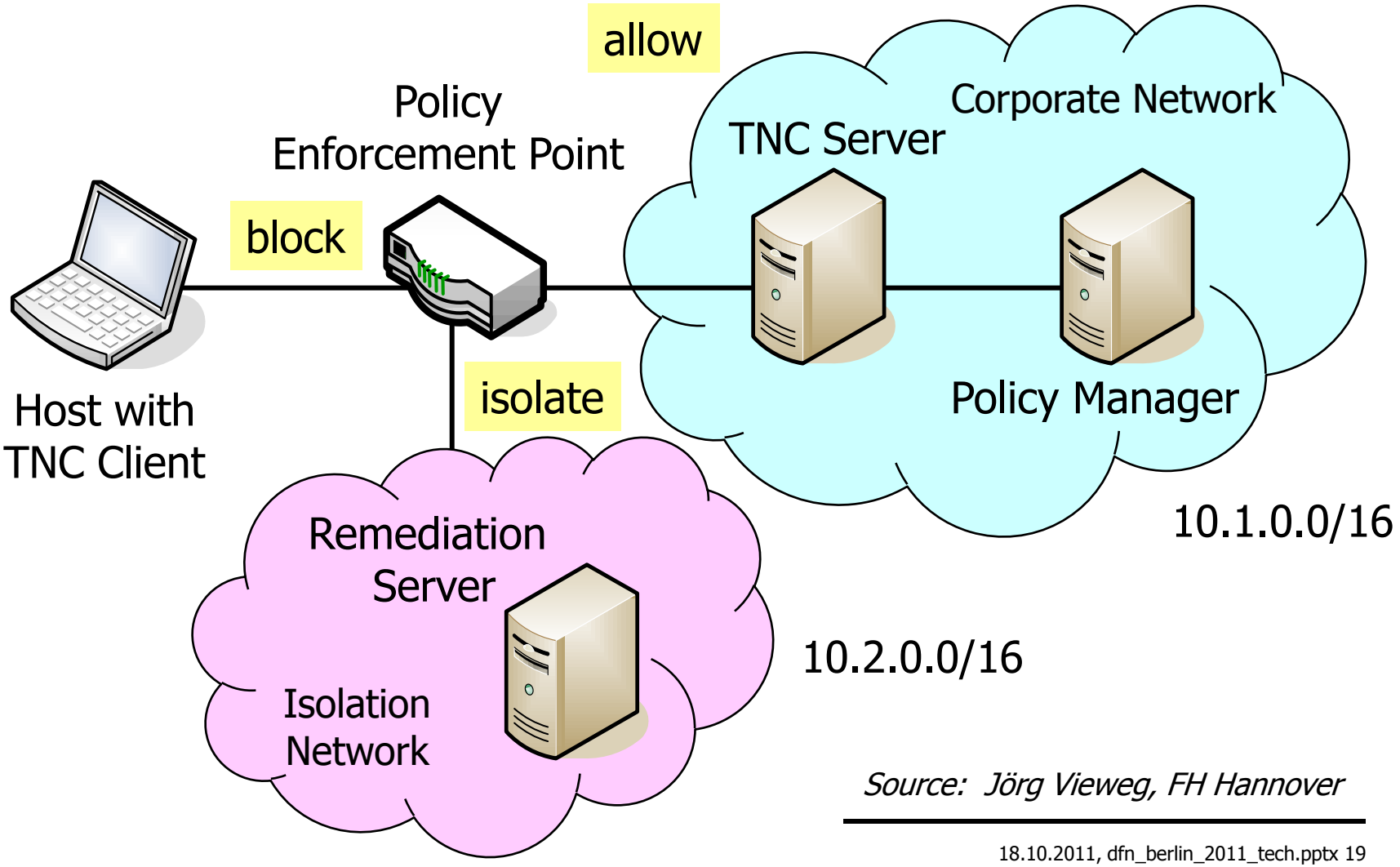
55. DFN Betriebstagung Oktober 2011 Berlin

Trusted Network Connect (TNC) & Platform Trust Service (PTS)

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

TNC Policy Enforcement



Source: Jörg Vieweg, FH Hannover

strongSwan Konfiguration auf der PEP Seite

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

```
conn rw-allow
     rightgroups=allow
     leftsubnet=10.1.0.0/16
     also=rw-eap
     auto=add
```

```
conn rw-isolate
     rightgroups=isolate
     leftsubnet=10.2.0.0/16
     also=rw-eap
     auto=add
```

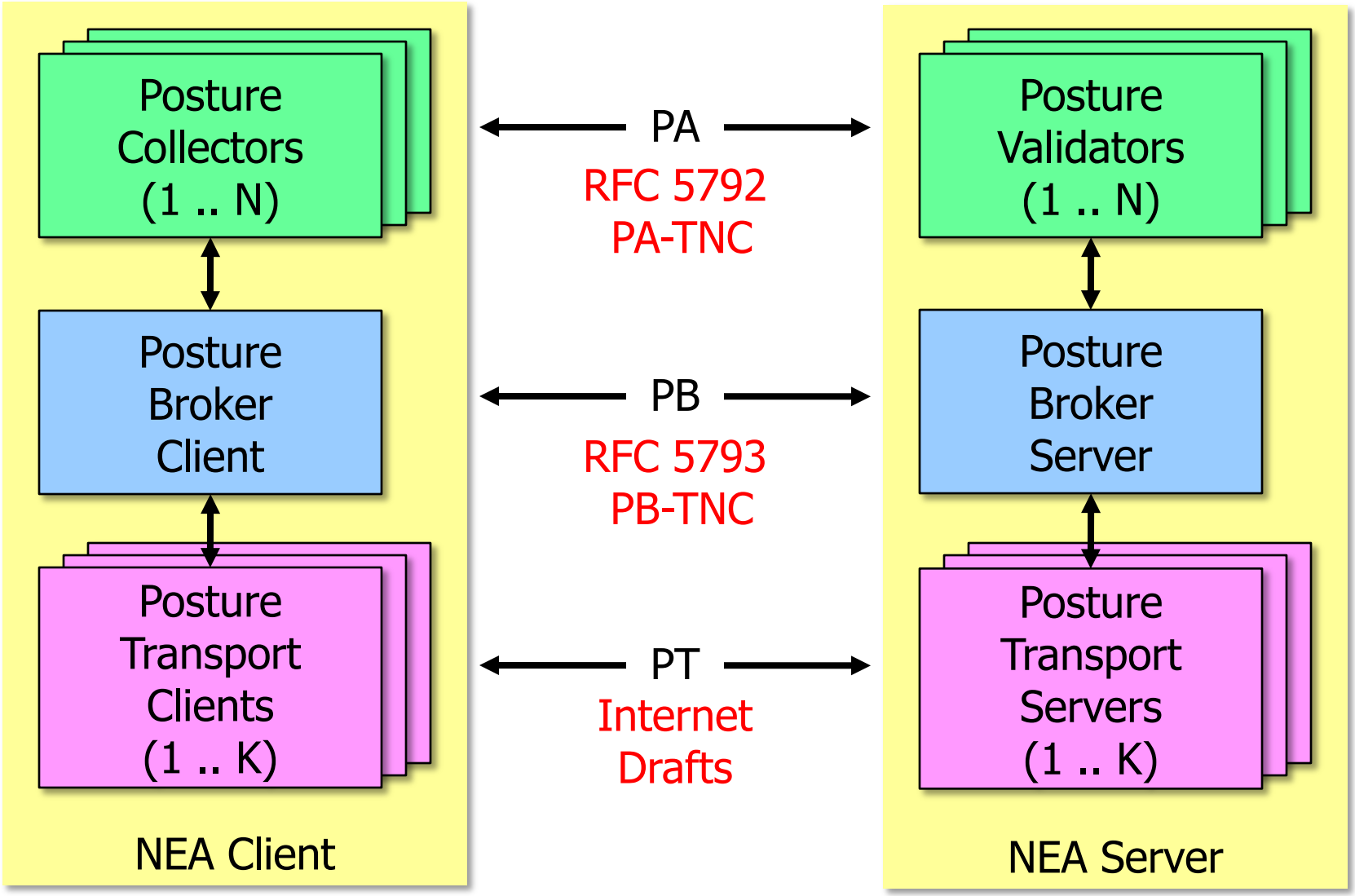
```
conn rw-eap
     left=192.168.0.1
     leftcert=moonCert.pem
     leftid=@moon.strongswan.org
     leftauth=eap-ttls
     leftfirewall=yes
     rightauth=eap-radius
     rightid=*@strongswan.org
     rightsendcert=never
     right=%any
```

IF-PEP Protokoll auf dem strongSwan PEP

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

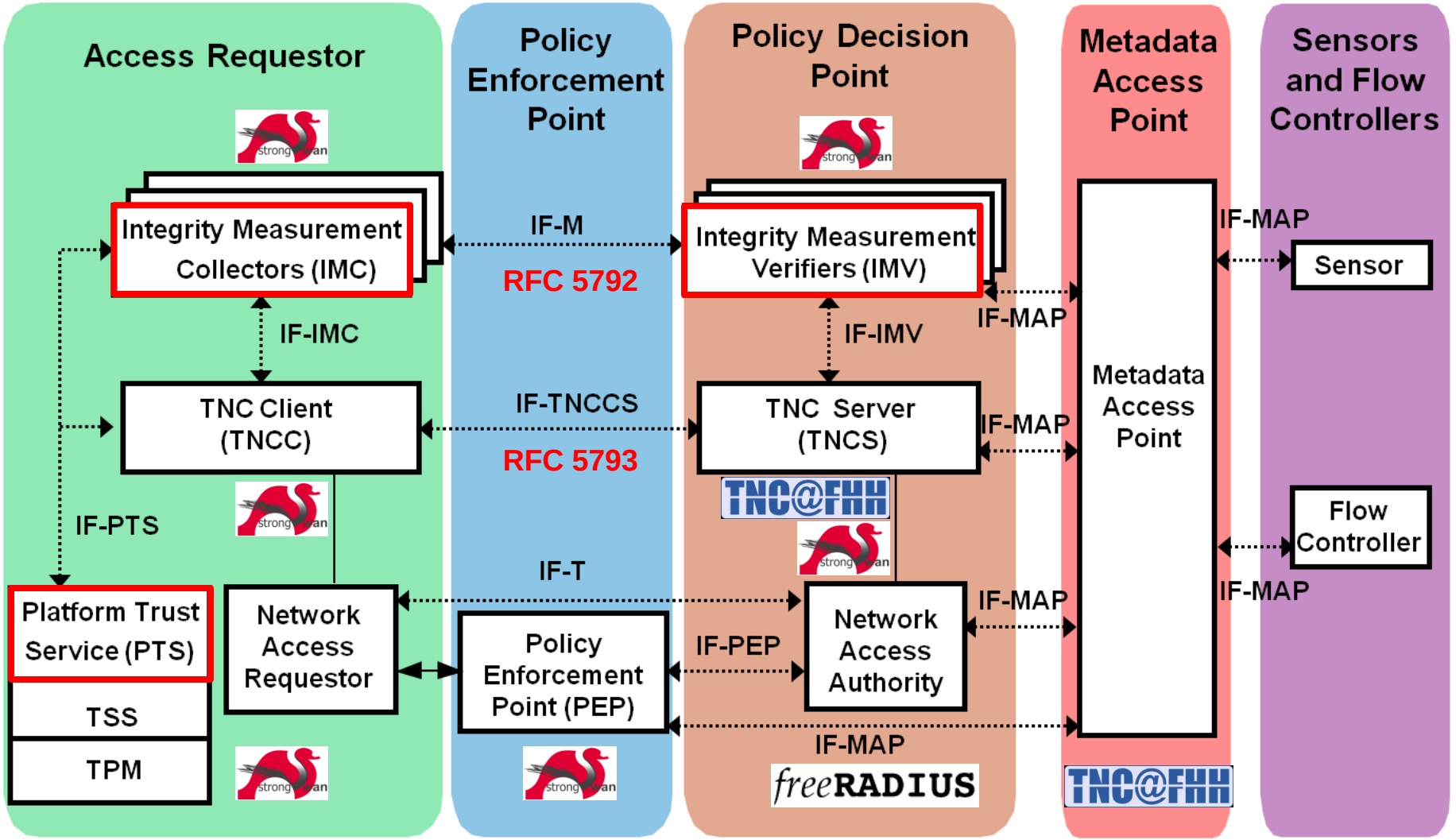
```
05[CFG] received RADIUS Access-Accept from server '10.1.0.10'
05[IKE] received RADIUS attribute Tunnel-Type: tag = 0, value = 9
05[IKE] received RADIUS attribute Filter-Id: 'allow'
05[IKE] RADIUS authentication of 'carol@strongswan.org' successful
05[IKE] EAP method EAP_TTLS succeeded, MSK established
05[ENC] generating IKE_AUTH response 11 [ EAP/SUCC ]
05[NET] sending packet: from 192.168.0.1[4500] to 192.168.0.100[4500]
04[NET] received packet: from 192.168.0.100[4500] to 192.168.0.1[4500]
04[ENC] parsed IKE_AUTH request 12 [ AUTH ]
04[IKE] authentication of 'carol@strongswan.org' with EAP successful
04[IKE] authentication of 'moon.strongswan.org' (myself) with EAP
04[IKE] IKE_SA rw-allow[1] established between
       192.168.0.1[moon.strongswan.org]...192.168.0.100[carol@strongswan.org]
02[CFG] received RADIUS Access-Accept from server '10.1.0.10'
02[IKE] received RADIUS attribute Tunnel-Type: tag = 0, value = 9
02[IKE] received RADIUS attribute Filter-Id: 'isolate'
02[IKE] RADIUS authentication of 'dave@strongswan.org' successful
02[IKE] EAP method EAP_TTLS succeeded, MSK established
02[ENC] generating IKE_AUTH response 11 [ EAP/SUCC ]
02[NET] sending packet: from 192.168.0.1[4500] to 192.168.0.200[4500]
01[NET] received packet: from 192.168.0.200[4500] to 192.168.0.1[4500]
01[ENC] parsed IKE_AUTH request 12 [ AUTH ]
01[IKE] authentication of 'dave@strongswan.org' with EAP successful
01[CFG] constraint check failed: group membership required
01[CFG] selected peer config 'rw-allow' inacceptable
01[CFG] switching to peer config 'rw-isolate,
01[IKE] authentication of 'moon.strongswan.org' (myself) with EAP
01[IKE] IKE_SA rw-isolate[2] established between
        192.168.0.1[moon.strongswan.org]...192.168.0.200[dave@strongswan.org]
```

Network Endpoint Assessment (RFC 5209)



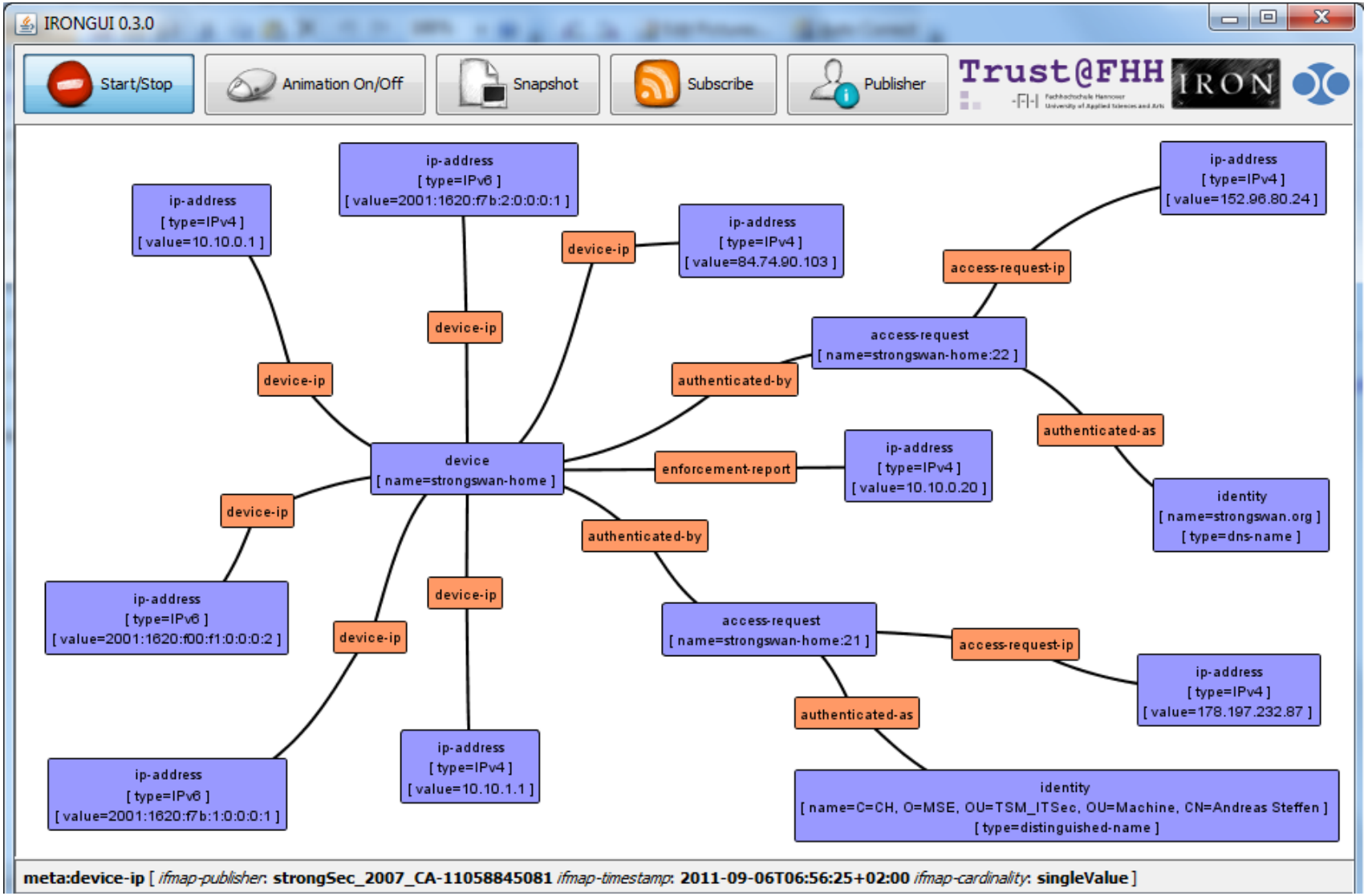
strongSwan als TNC Client und TNC Server

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz



strongSwan als TNC MAP Client

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz



http://trust.inform.fh-hannover.de/

Danke für Ihre Aufmerksamkeit!

Fragen?

www.strongswan.org