Die strongSwan Open Source VPN Lösung

Open Source Trend Days 2013 Steinfurt

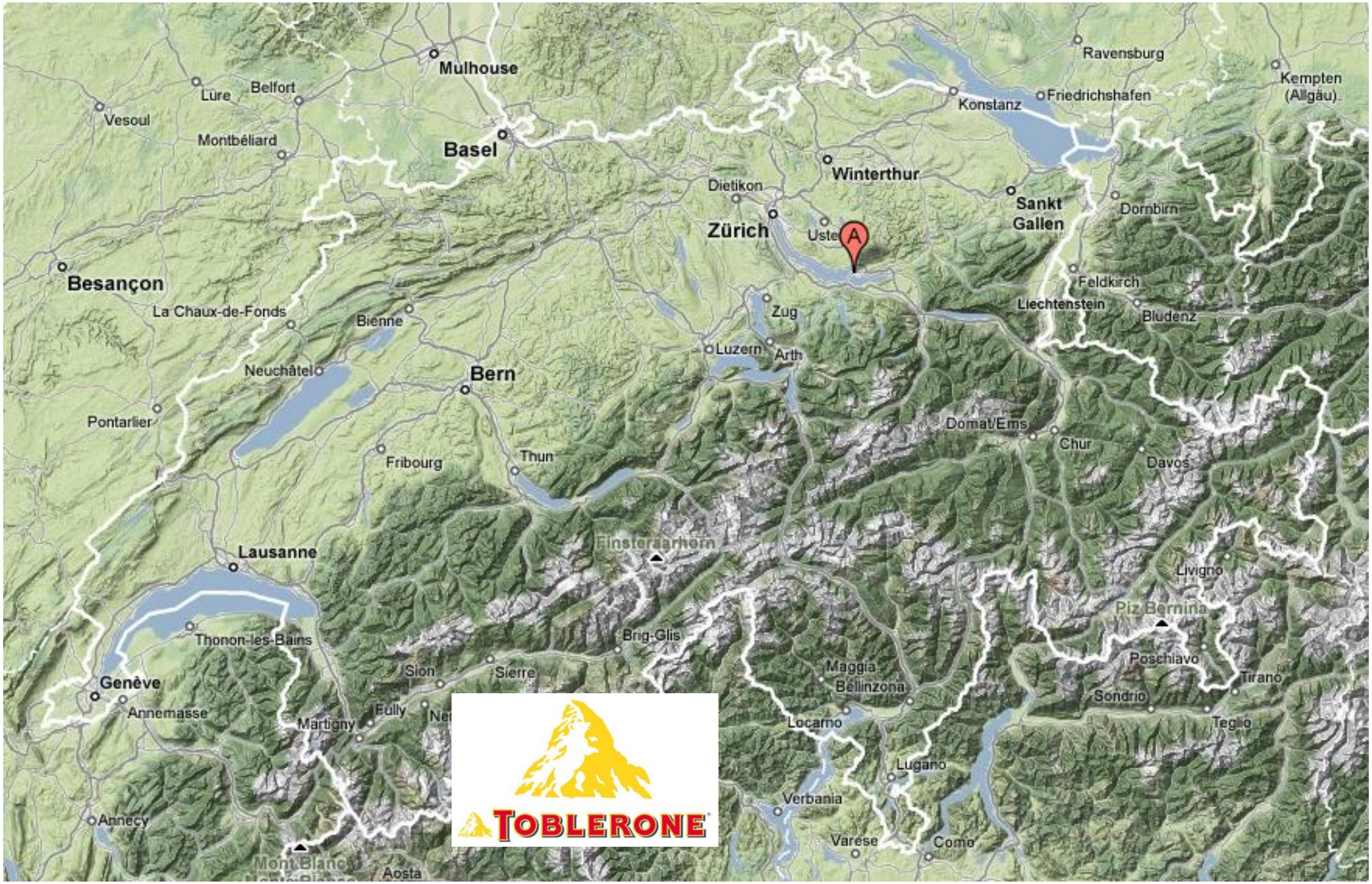
www.strongswan.org

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

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

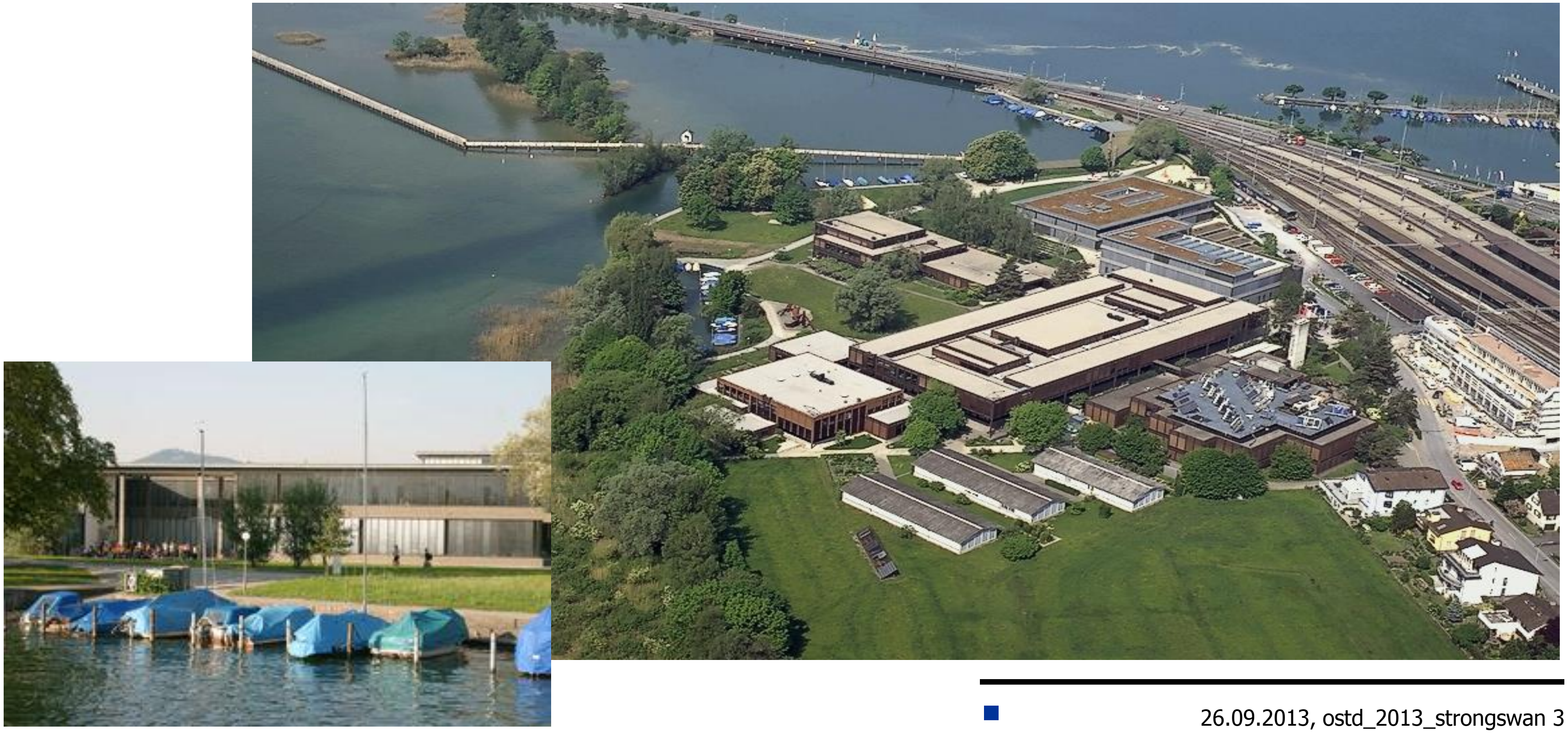
FHO Fachhochschule Ostschweiz

Wo um Gottes Willen liegt Rapperswil?



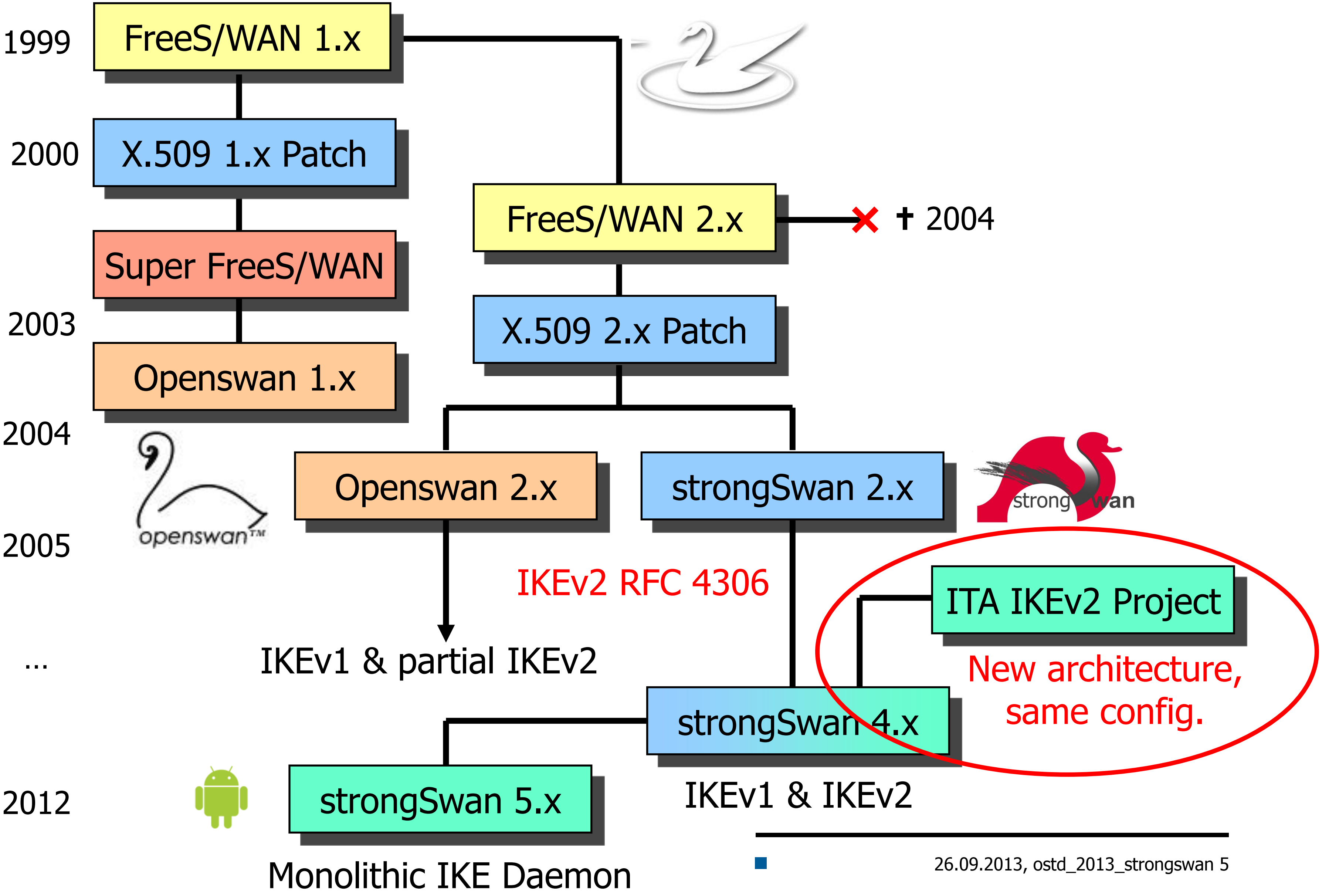
HSR - Hochschule für Technik Rapperswil

- Fachhochschule mit ca. 1500 Studierenden
- Studiengang für Informatik (300-400 Studierende)
- Bachelorstudium (3 Jahre), Masterstudium (+1.5 Jahre)

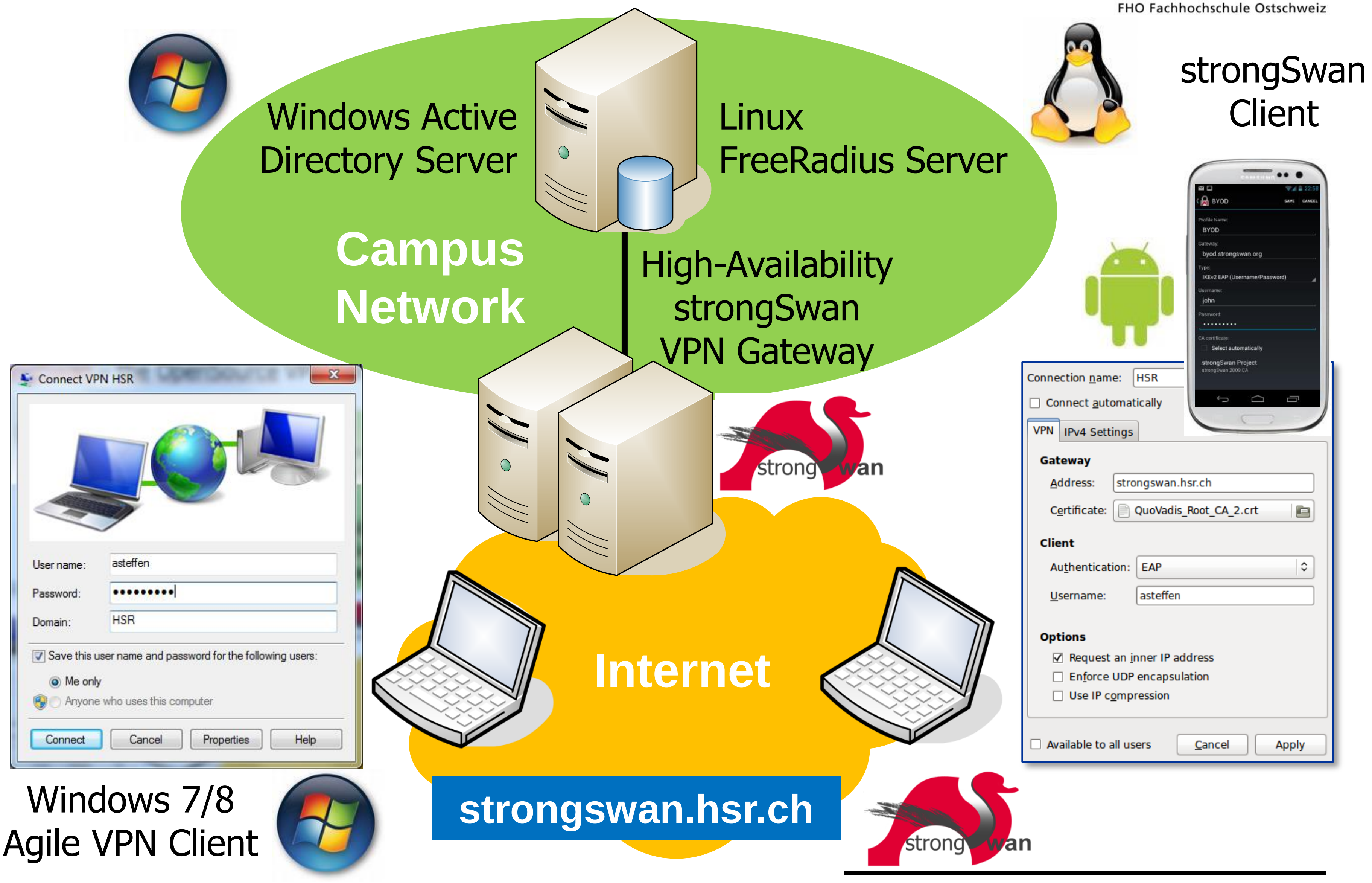


Das strongSwan Projekt

The strongSwan Open Source VPN Project



strongSwan – the Open Source VPN Solution



Windows Active Directory Server

Linux FreeRadius Server

Campus Network

High-Availability strongSwan VPN Gateway

Internet

strongswan.hsr.ch

strongSwan Client

Windows 7/8 Agile VPN Client

Connect VPN HSR

User name: asteffen
Password: ••••••••••
Domain: HSR

☑ Save this user name and password for the following users:
● Me only
○ Anyone who uses this computer

Connection name: HSR
□ Connect automatically

Gateway
Address: strongswan.hsr.ch
Certificate: QuoVadis_Root_CA_2.crt

Client
Authentication: EAP
Username: asteffen

Options
☑ Request an inner IP address
□ Enforce UDP encapsulation
□ Use IP compression

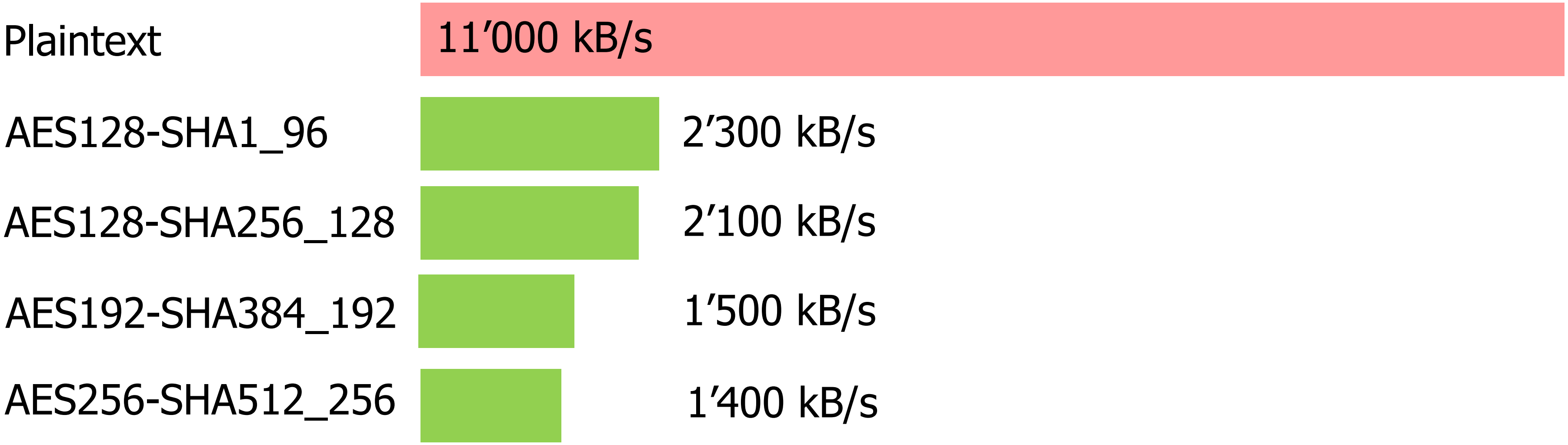
□ Available to all users

Profile Name: BYOD
Gateway: byod.strongswan.org
Type: IKEv2 EAP (Username/Password)
Username: john
Password: ••••••••••
CA certificate:
□ Select automatically
strongSwan Project
strongSwan 2009 CA

Supported Operating Systems and Platforms

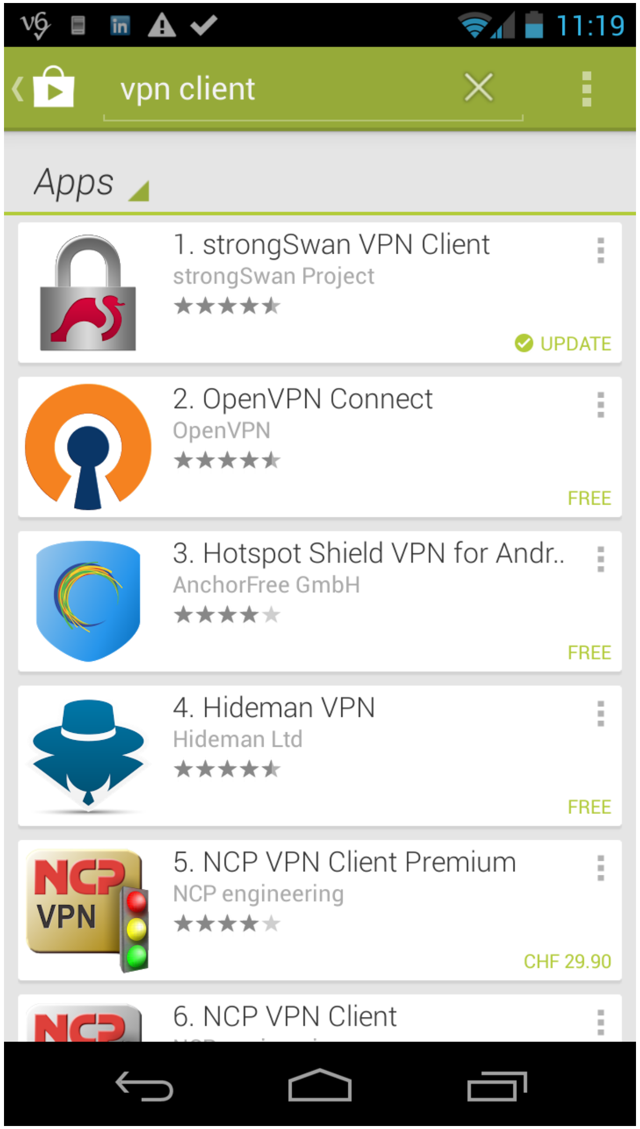
- Supported Operating Systems
  - Linux 2.6.x, 3.x (optional integration into NetworkManager)
  - Android 4.x App (using libipsec userland ESP encryption)
  - Mac OS X App (using libipsec userland ESP encryption)
  - Mac OS X (via command line)
  - FreeBSD
  - OpenWrt
- Supported Hardware Platforms (GNU autotools)
  - Intel i686/x86_64, AMD64
  - ARM, MIPS
  - PowerPC
- Supported Network Stacks
  - IPv4, IPv6
  - IPv6-in-IPv4 ESP tunnels
  - IPv4-in-IPv6 ESP tunnels

strongSwan on Raspberry Pi



- Performance measurement setup
  - Two Raspberry Pi hosts connected via 100 Mbit/s Ethernet
  - FTP download of an 18 MB file
- No Authenticated Encryption (AEAD) Support
  - Unfortunately the efficient AES-GCM ESP algorithm family is not enabled in the current Raspberry Pi kernel.

Free Download from Google Play Store



11:19

vpn client

Apps

1. strongSwan VPN Client
strongSwan Project
★★★★★
UPDATE

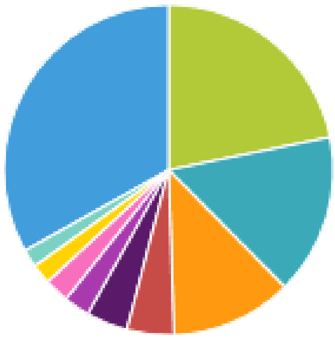
2. OpenVPN Connect
OpenVPN
★★★★★
FREE

3. Hotspot Shield VPN for Andr..
AnchorFree GmbH
★★★★☆
FREE

4. Hideman VPN
Hideman Ltd
★★★★★
FREE

5. NCP VPN Client Premium
NCP engineering
★★★★☆
CHF 29.90

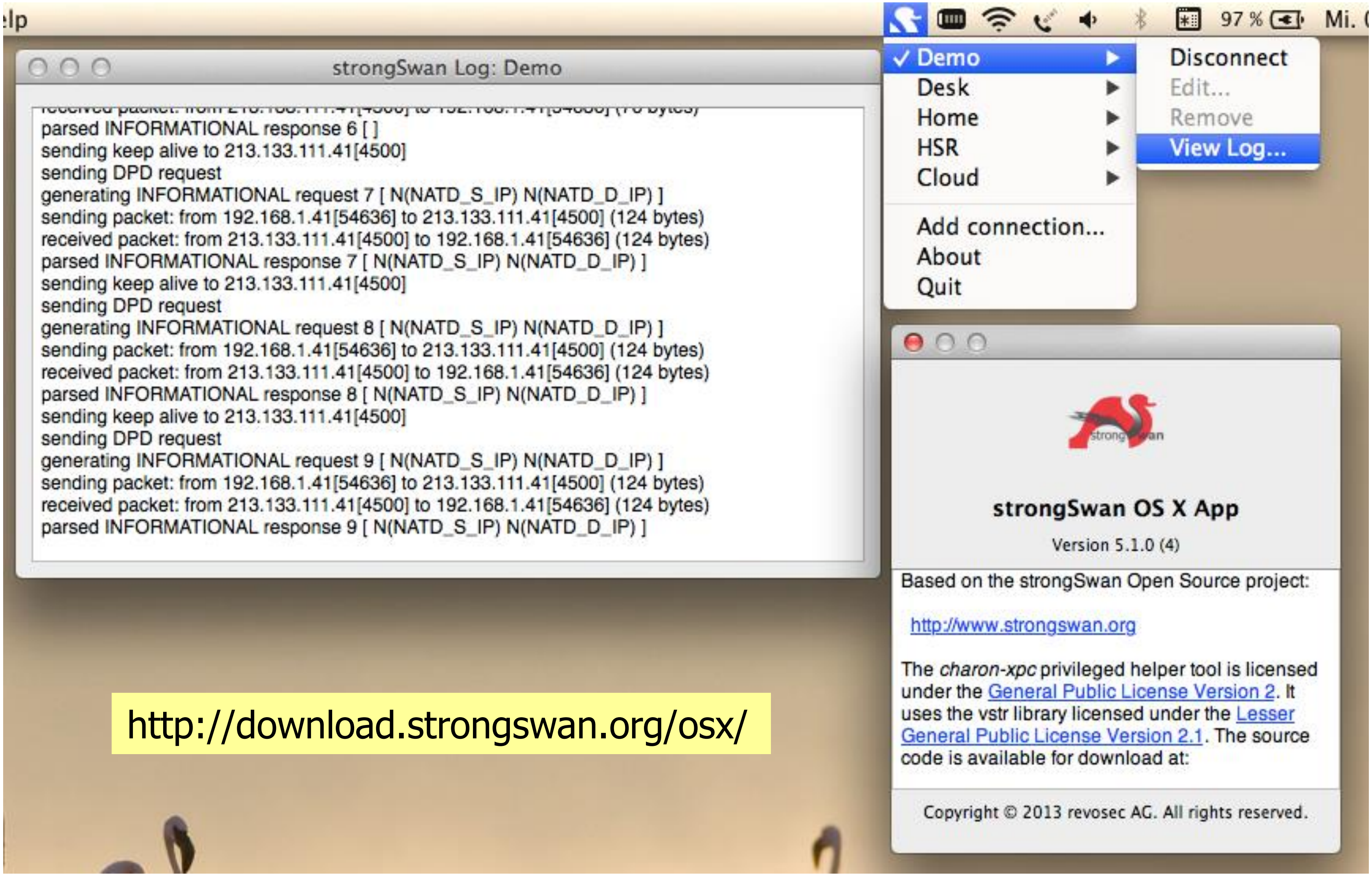
6. NCP VPN Client



Sep 24 2013:
6,605 installations

			YOUR APP	
☑	🟩	United States	1,441	21.82%
☑	🟦	China	1,038	15.72%
☑	🟧	Germany	790	11.96%
□	🟥	United Kingdom	303	4.59%
□	🟪	Russia	268	4.06%
□	🟪	Switzerland	169	2.56%
□	🟪	Canada	161	2.44%
□	🟨	Italy	130	1.97%
□	🟩	France	117	1.77%
	🟦	Others	2,188	33.13%

Mac OS X App



```
parsed INFORMATIONAL response 6 [ ]
sending keep alive to 213.133.111.41[4500]
sending DPD request
generating INFORMATIONAL request 7 [ N(NATD_S_IP) N(NATD_D_IP) ]
sending packet: from 192.168.1.41[54636] to 213.133.111.41[4500] (124 bytes)
received packet: from 213.133.111.41[4500] to 192.168.1.41[54636] (124 bytes)
parsed INFORMATIONAL response 7 [ N(NATD_S_IP) N(NATD_D_IP) ]
sending keep alive to 213.133.111.41[4500]
sending DPD request
generating INFORMATIONAL request 8 [ N(NATD_S_IP) N(NATD_D_IP) ]
sending packet: from 192.168.1.41[54636] to 213.133.111.41[4500] (124 bytes)
received packet: from 213.133.111.41[4500] to 192.168.1.41[54636] (124 bytes)
parsed INFORMATIONAL response 8 [ N(NATD_S_IP) N(NATD_D_IP) ]
sending keep alive to 213.133.111.41[4500]
sending DPD request
generating INFORMATIONAL request 9 [ N(NATD_S_IP) N(NATD_D_IP) ]
sending packet: from 192.168.1.41[54636] to 213.133.111.41[4500] (124 bytes)
received packet: from 213.133.111.41[4500] to 192.168.1.41[54636] (124 bytes)
parsed INFORMATIONAL response 9 [ N(NATD_S_IP) N(NATD_D_IP) ]
```

strongSwan OS X App

Version 5.1.0 (4)

Based on the strongSwan Open Source project:

http://www.strongswan.org

The *charon-xpc* privileged helper tool is licensed under the General Public License Version 2. It uses the vstr library licensed under the Lesser General Public License Version 2.1. The source code is available for download at:

Copyright © 2013 revosec AG. All rights reserved.

http://download.strongswan.org/osx/

Modular Plugin-Based Architecture (29/84)

- libstrongswan plugins

  aes af_alg agent blowfish ccm cmac constraints ctr curl des dnskey fips_prf gcm gcrypt gmp hmac keychain ldap md4 md5 mysql nonce openssl padlock pem pgp pkcs1 pkcs11 pcks12 pkcs7 pkcs8 pubkey random rc2 rdrand revocation sha1 sha2 soup sqlite sshkey test_vectors unbound x509 xcbc

- libcharon plugins

  addrblock android_dns android_log certexpire coupling dhcp duplicheck eap_aka eap_aka_3gpp2 eap_dynamic eap_qtc eap_identity eap_md5 eap_mschapv2 eap_peap eap_radius eap_sim eap_simaka_pseudonym eap_simaka_reauth eap_simaka_sql eap_sim_file eap_sim_pcsc eap_tls eap_tnc eap_ttls error_notify farp ha ipseckey kernel_libipsec led load_tester lookip maemo medcli medsrv osx_attr radattr smp socket_default socket_dynamic sql stroke systime_fix tnc_ifmap tnc_pdp uci unit_tester unity updown whitelist xauth_eap xauth_generic xauth_noauth xauth_pem

- libhydra plugins

  attr attr_sql kernel_klips kernel_netlink kernel_pfkey kernel_pfroute resolve

- libtnccs plugins

  tnccs_11 tnccs_20 tnccs_dynamic tnc_imc tnc_imv tnc_tnccs

Die strongSwan Open Source VPN Lösung

Open Source Trend Days 2013 Steinfurt

Remote Access mit zertifikat-basierter Authentisierung

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

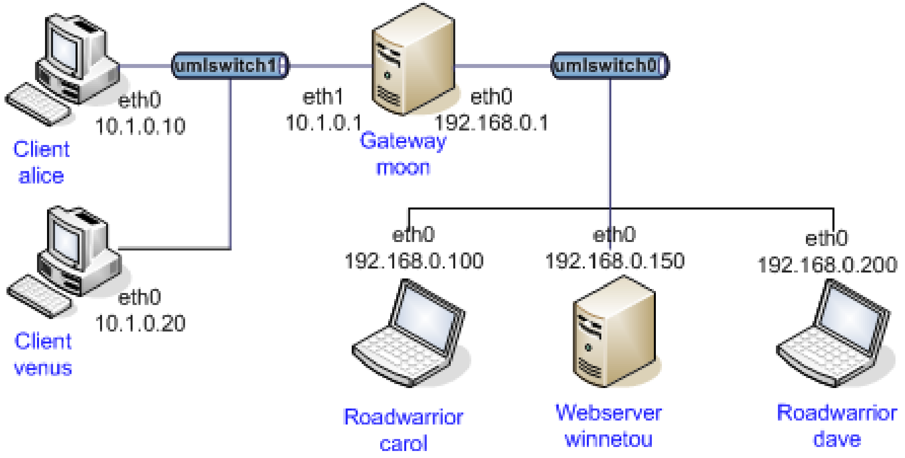
IKEv2 Remote Access Scenario

```
#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
     left=%any
     leftsourceip=%config
     leftcert=carolCert.pem
     leftid=carol@strongswan.org
     leftfirewall=yes
     right=192.168.0.1
     rightid=moon.strongswan.org
     rightsubnet=10.1.0.0/16
     auto=start
```

```
#ipsec.conf for gateway moon

conn rw
     keyexchange=ikev2
     left=%any
     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
```



IKEv2 Connection Setup

carol

```
05[ENC] generating IKE_SA_INIT request [SA KE No N(NATD_S_IP) N(NATD_D_IP)]
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 [SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ]
06[ENC] generating IKE_AUTH request [IDi CERT CERTREQ IDr AUTH CP SA TSi TSr]
06[NET] sending packet: from 192.168.0.100[4500] to 192.168.0.1[4500]
07[NET] received packet: from 192.168.0.1[4500] to 192.168.0.100[4500]
07[ENC] parsed IKE_AUTH response [IDr CERT AUTH CP SA TSi TSr N(AUTH_LFT)]
07[IKE] installing new virtual IP 10.3.0.1
07[AUD] established CHILD_SA successfully
```

moon

```
05[NET] received packet: from 192.168.0.100[500] to 192.168.0.1[500]
05[ENC] parsed IKE_SA_INIT request [SA KE No N(NATD_S_IP) N(NATD_D_IP)]
05[ENC] generating IKE_SA_INIT response [SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ]
05[NET] sending packet: from 192.168.0.1[500] to 192.168.0.100[500]
06[NET] received packet: from 192.168.0.100[4500] to 192.168.0.1[4500]
06[ENC] parsed IKE_AUTH request [IDi CERT CERTREQ IDr AUTH CP SA TSi TSr]
06[IKE] peer requested virtual IP %any
06[IKE] assigning virtual IP 10.3.0.1 to peer
06[AUD] established CHILD_SA successfully
06[ENC] generating IKE_AUTH response [IDr CERT AUTH CP SA TSi TSr N(AUTH_LFT)]
06[NET] sending packet: from 192.168.0.1[4500] to 192.168.0.100[4500]
```

IKEv2 Configuration Payload

carol

```
carol> ip addr list dev eth0
eth0: inet 192.168.0.100/24 brd 192.168.0.255 scope global eth0
      inet 10.3.0.1/32 scope global eth0

carol> ip route list table 220
10.1.0.0/24 dev eth0 proto static src 10.3.0.1
```

- A virtual IP requested and obtained through leftsourceip=%config is directly configured by strongSwan via the RT Netlink socket

moon

```
moon> ip addr list
eth0: inet 192.168.0.1/24 brd 192.168.0.255 scope global eth0
eth1: inet 10.1.0.1/16 brd 10.1.255.255 scope global eth1

moon> ip route list table 220
10.3.0.1 dev eth0 proto static src 10.1.0.1
```

- If a host has an internal interface which is part of the negotiated traffic selectors then this source address is assigned to tunneled IP packets.

Volatile RAM-based IP Address Pools

- Configuration in ipsec.conf

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

- Statistics

```
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'
```

- Referencing and sharing a volatile pool

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

Persistent SQL-based IP Address Pools I

- SQLite database table definitions

```
cd strongswan-x.y.z
cp testing/hosts/default/etc/ipsec.d/tables.sql /etc/ipsec.d
```

- Creation of SQLite database

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

- Connecting to the SQLite database

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

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

Persistent SQL-based IP Address Pools II

- Pool creation

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

- Configuration in ipsec.conf

```
conn rw
     keyexchange=ikev2
     ...
     rightsourceip=%bigpool
     auto=add
```

- Statistics

```
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
```

Die strongSwan Open Source VPN Lösung

Open Source Trend Days 2013 Steinfurt

Remote Access mit RADIUS-basierter Authentisierung

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

RADIUS-Based Authentication

```
#ipsec.secrets for roadwarrior carol

carol: EAP "Ar3etTnp"
```

```
#ipsec.secrets for gateway moon

: RSA moonKey.pem
```

```
#ipsec.conf for roadwarrior carol

conn home
     keyexchange=ikev2
     left=%any
     leftsourceip=%config
     leftauth=eap
     eap_identity=carol
     right=moon.strongswan.org
     rightid=moon.strongswan.org
     rightauth=pubkey
     rightsubnet=0.0.0.0/0
     auto=start
```

```
#ipsec.conf for gateway moon

conn rw
     keyexchange=ikev2
     left=%any
     leftauth=pubkey
     leftsubnet=10.1.0.0/24
     leftcert=moonCert.pem
     leftid=moon.strongswan.org
     right=%any
     rightsendcert=never
     rightauth=eap-radius
     rightsourceip=%radius
     eap_identity=%any
     auto=add
```

RADIUS Configuration

- /etc/strongswan.conf on gateway moon

```
charon {
  plugins {
    eap-radius {
      secret = gv6URkSs
      server = 10.1.0.10
      accounting  = yes
    }
  }
}
```

- /etc/freeradius/users on RADIUS server alice

```
carol Cleartext-Password := "Ar3etTnp"
      Framed-IP-Address = 10.3.0.1
dave  Cleartext-Password := "W7R0g3do"
      Framed-IP-Address = 10.3.0.2
```

RADIUS Accounting

- Accounting Record

```
Wed Jul 31 21:28:31 2013
    Acct-Status-Type = Stop
    Acct-Session-Id = "1375306104-1"
    NAS-Port-Type = Virtual
    Service-Type = Framed-User
    NAS-Port = 1
    NAS-Port-Id = "rw-eap"
    NAS-IP-Address = 192.168.0.1
    Called-Station-Id = "192.168.0.1[4500]"
    Calling-Station-Id = "192.168.0.100[4500]"
    User-Name = "carol"
    Framed-IP-Address = 10.3.0.1
    Framed-IPv6-Prefix = fec3::1/128
    Acct-Output-Octets = 7100
    Acct-Output-Packets = 5
    Acct-Input-Octets = 7100
    Acct-Input-Packets = 5
    Acct-Session-Time = 6
    Acct-Terminate-Cause = User-Request
    NAS-Identifier = "strongSwan"
    Acct-Unique-Session-Id = "5716061d9f73b686"
    Timestamp = 1375306111
```

Die strongSwan Open Source VPN Lösung

Open Source Trend Days 2013 Steinfurt

Nahtlose LAN Integration von Remote Access Clients

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

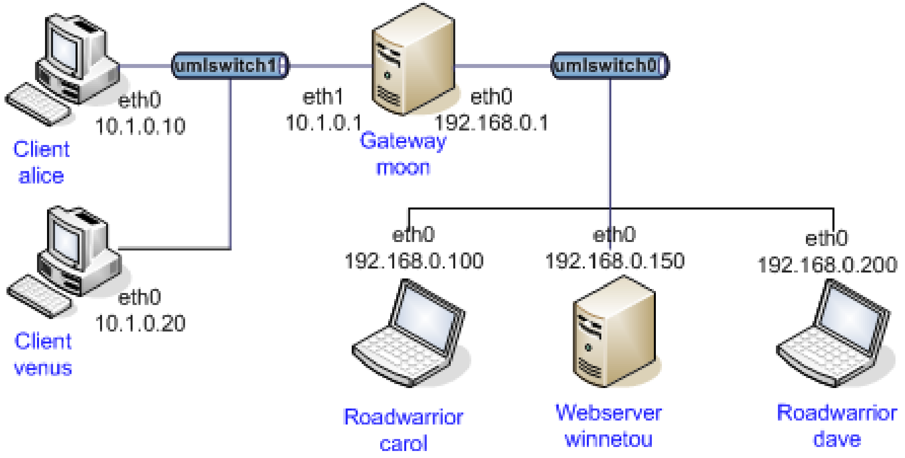
LAN Integration via DHCP and ARP

```
#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
     left=%any
     leftsourceip=%config
     leftcert=carolCert.pem
     leftid=carol@strongswan.org
     leftfirewall=yes
     right=192.168.0.1
     rightid=moon.strongswan.org
     rightsubnet=0.0.0.0/0
     auto=start
```

```
#ipsec.conf for gateway moon

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



DHCP Server Configuration

- strongswan.conf on gateway moon

```
charon {
  plugins {
    dhcp {
      server = 10.1.255.255
    }
  }
}
```

- The farp and dhcp plugins are required for the LAN use case

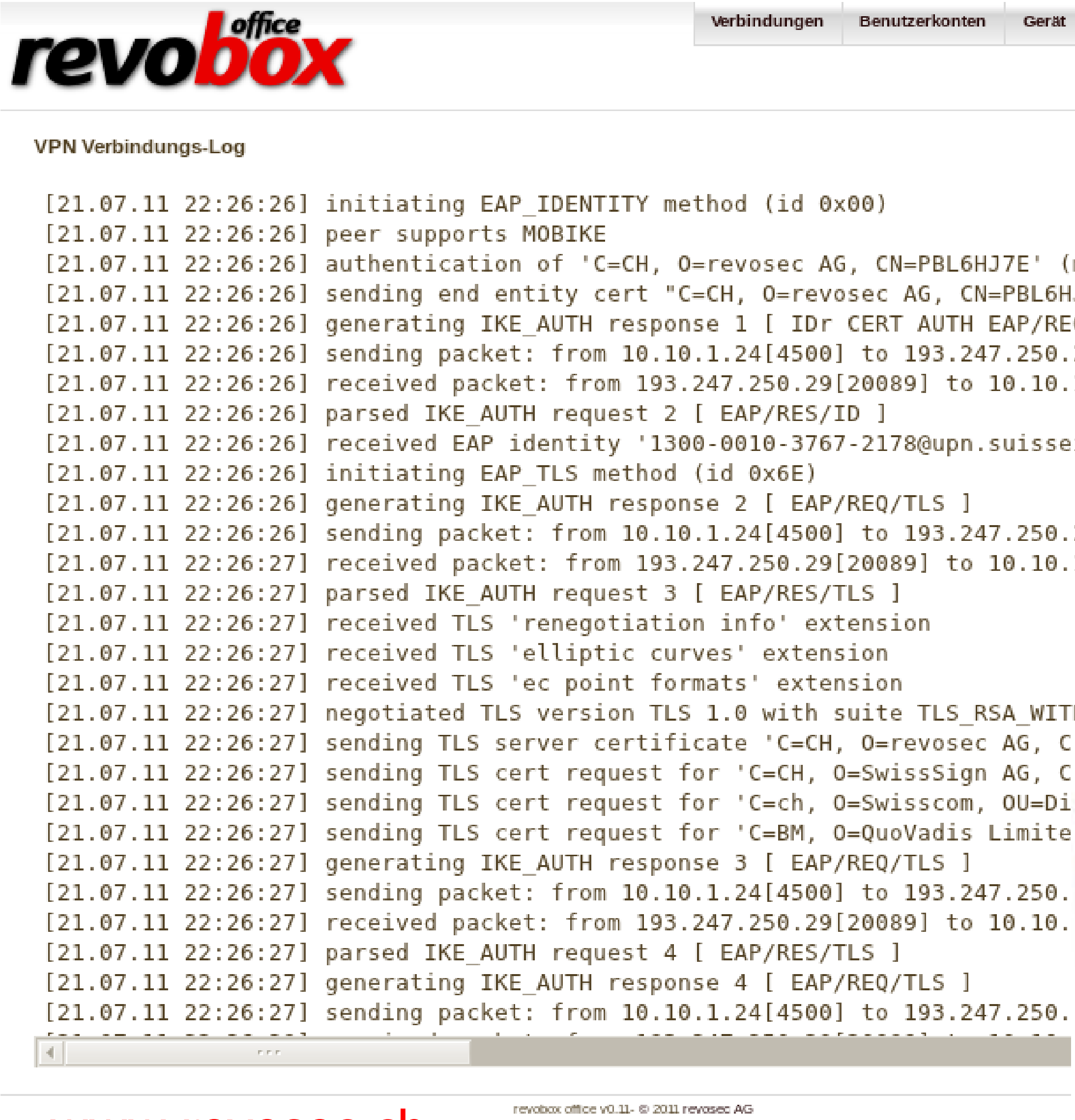
DHCP Server Configuration

- dhcpd configuration file on DHCP Server venus

```
ddns-update-style none;

subnet 10.1.0.0 netmask 255.255.0.0 {
  option domain-name            "strongswan.org";
  option domain-name-servers     10.1.0.20;
  option netbios-name-servers    10.1.0.10;
  option routers                 10.1.0.1;
  option broadcast-address       10.1.255.255;
  next-server                    10.1.0.20;

  range 10.1.0.50 10.1.0.60;
}

host carol {
  option dhcp-client-identifier "carol@strongswan.org";
  fixed-address                  10.1.0.30;
}

host dave {
  option dhcp-client-identifier "dave@strongswan.org";
  fixed-address                  10.1.0.40;
}
```

- Either static or dynamic address assignment

strongSwan SOHO Lösung für Windowsnetze



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

Die strongSwan Open Source VPN Lösung

Open Source Trend Days 2013 Steinfurt

Network Access Control

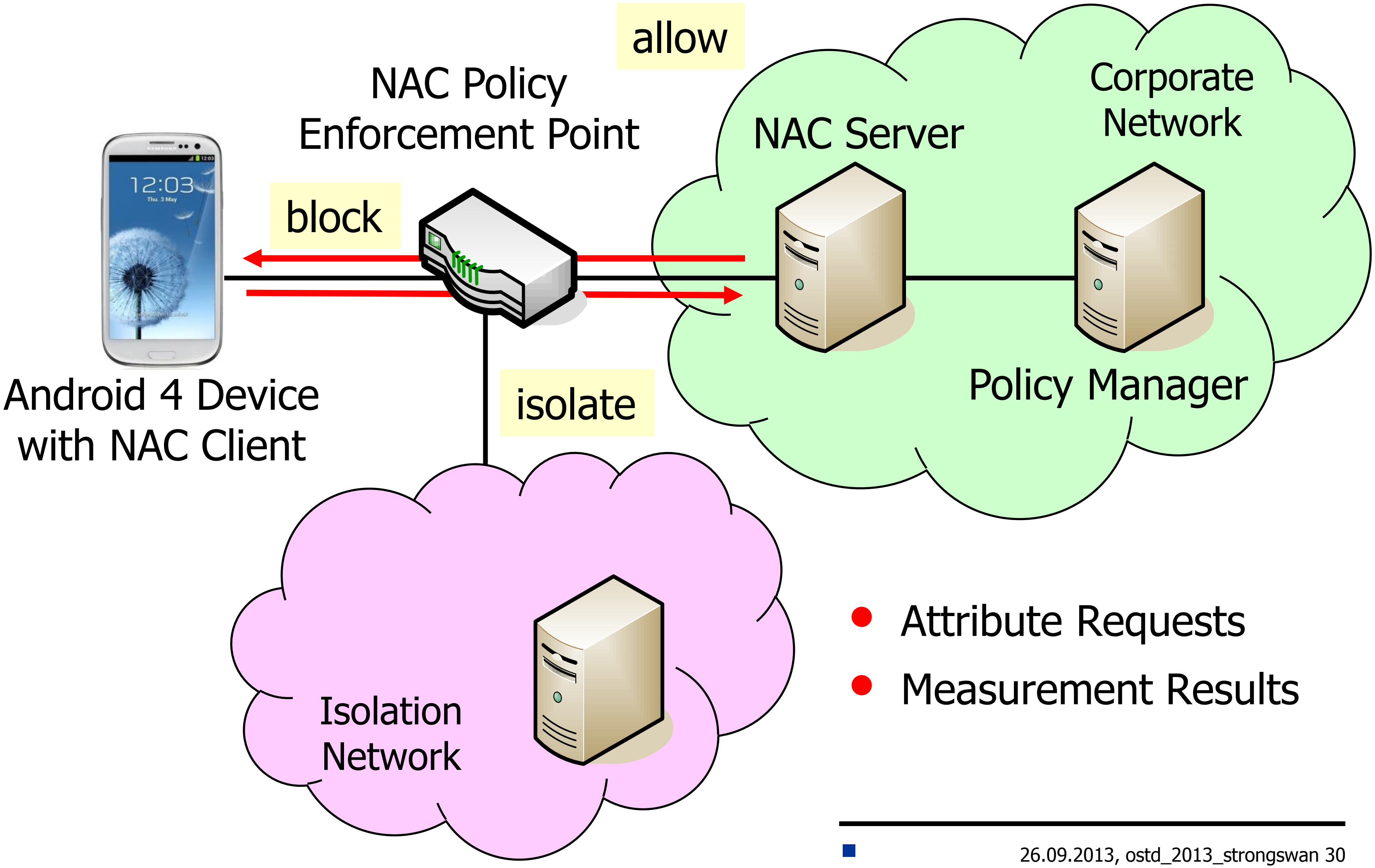
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

BYOD – Bring Your Own Device

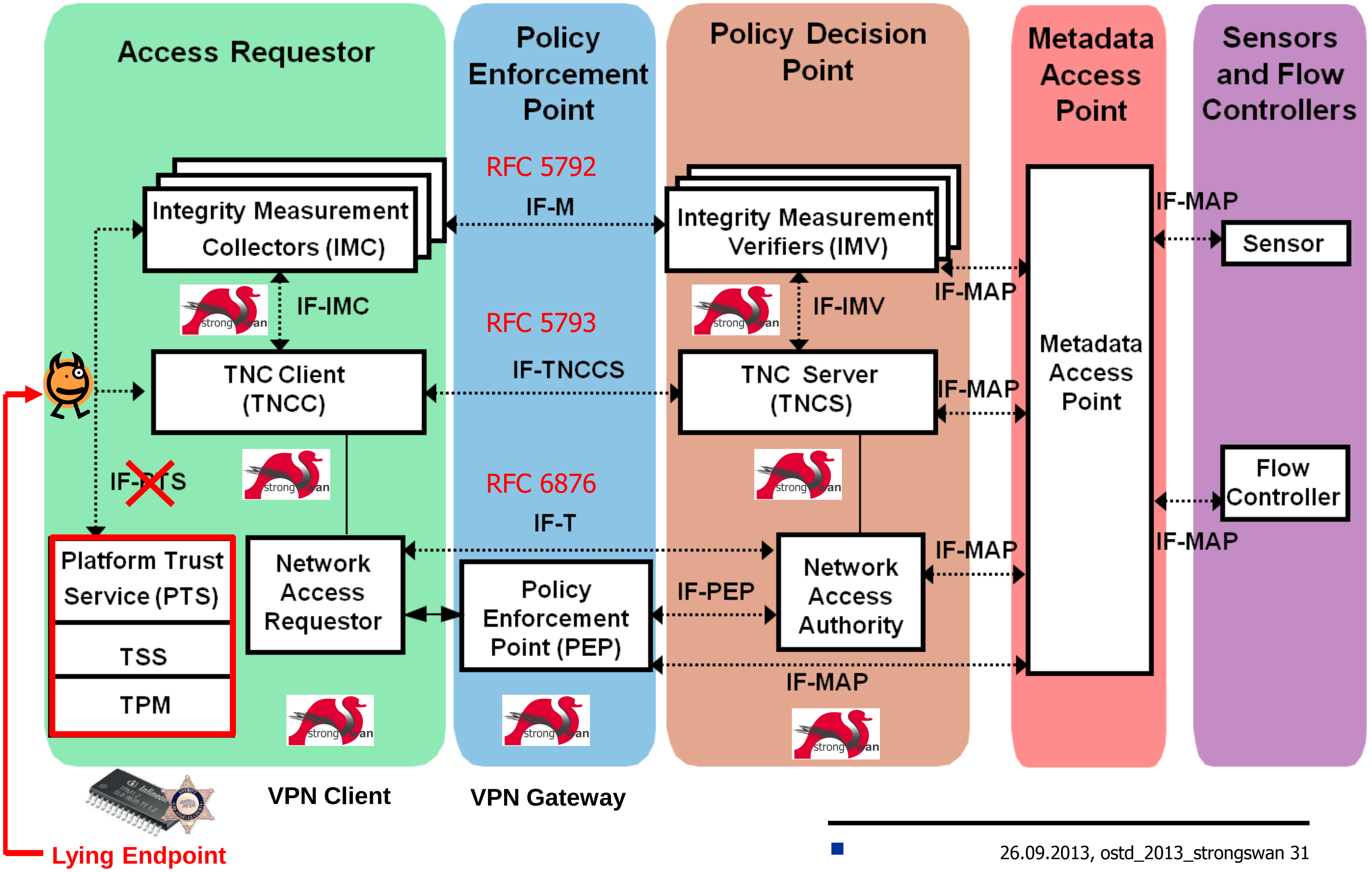
- Security Issues
  - Users do not protect access to their devices or use weak passwords or login methods.
  - Users download and install dangerous software packages containing malware from unknown sources.
  - Users do not regularly apply security updates to the installed software packages and operating system.
  - Users run server applications potentially giving third parties access to the corporate network and/or sensitive data
  - Malware might embed itself into the operating system, modifying system commands and libraries.

Android BYOD with Network Access Control



- Attribute Requests
- Measurement Results

Trusted Network Connect (TNC) Architecture



Layered TNC Protocol Stack

- IF-T Transport Protocol PT-TLS (RFC 6876) or PT-EAP

```
[NET] received packet: from 152.96.15.29[50871] to 77.56.144.51[4500] (320 bytes)
[ENC] parsed IKE_AUTH request 8 [ EAP/RES/TTLS ]
[IKE] received tunneled EAP-TTLS AVP [EAP/RES/TNC]
```

- IF-M Measurement Protocol PA-TNC (RFC 5792)

```
[TNC] received TNCCS batch (160 bytes) for Connection ID 1
[TNC] PB-TNC state transition from 'Init' to 'Server Working'
[TNC] processing PB-TNC CDATA batch
[TNC] processing PB-Language-Preference message (31 bytes)
[TNC] processing PB-PA message (121 bytes)
[TNC] setting language preference to 'en`
```

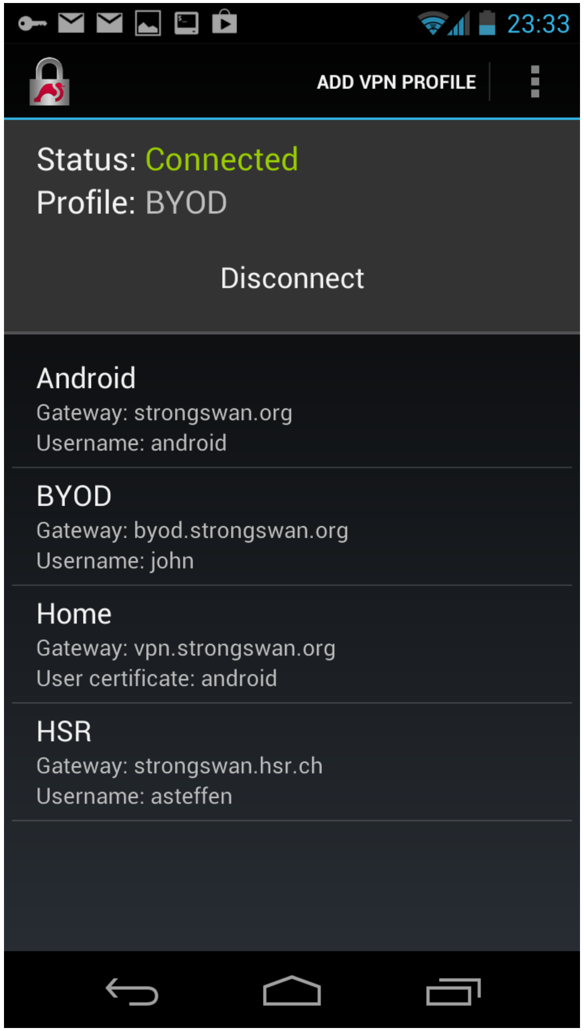
- IF-TNCCS TNC Client-Server Protocol PB-TNC (RFC 5793)

```
[TNC] handling PB-PA message type 'IETF/Operating System' 0x000000/0x00000001
[IMV] IMV 1 "OS" received message for Connection ID 1 from IMC 1
[TNC] processing PA-TNC message with ID 0xec41ce1d
[TNC] processing PA-TNC attribute type 'IETF/Product Information' 0x000000/0x00000002
[TNC] processing PA-TNC attribute type 'IETF/String Version' 0x000000/0x00000004
[TNC} processing PA-TNC attribute type 'ITA-HSR/Device ID' 0x00902a/0x00000008
```

- TNC Measurement Data

```
[IMV] operating system name is 'Android' from vendor Google
[IMV] operating system version is '4.2.1`
[IMV] device ID is cf5e4cbcc6e6a2db
```

strongSwan Android VPN Client



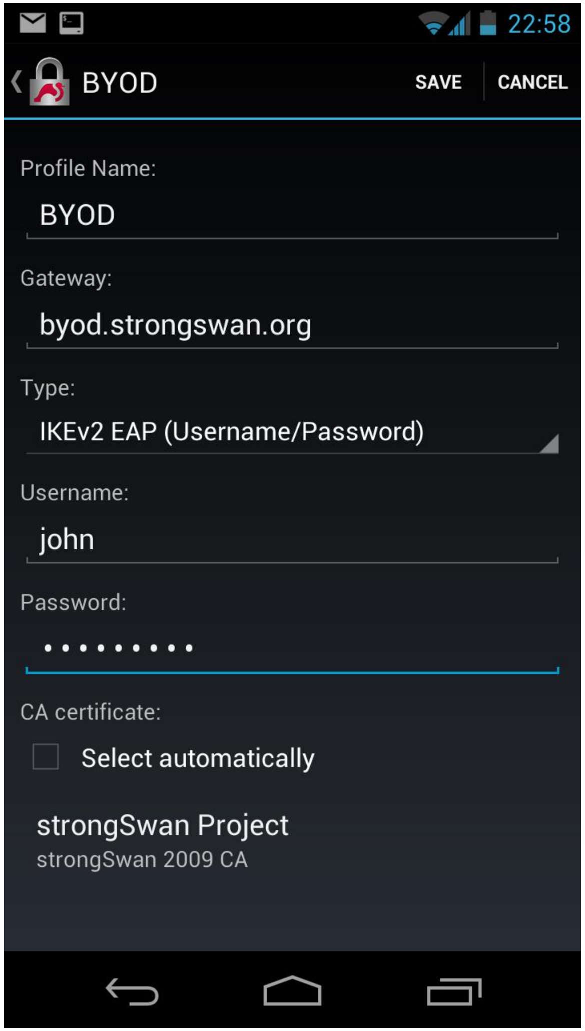
Status: Connected
Profile: BYOD

Android
Gateway: strongswan.org
Username: android

BYOD
Gateway: byod.strongswan.org
Username: john

Home
Gateway: vpn.strongswan.org
User certificate: android

HSR
Gateway: strongswan.hsr.ch
Username: asteffen



Profile Name: BYOD

Gateway: byod.strongswan.org

Type: IKEv2 EAP (Username/Password)

Username: john

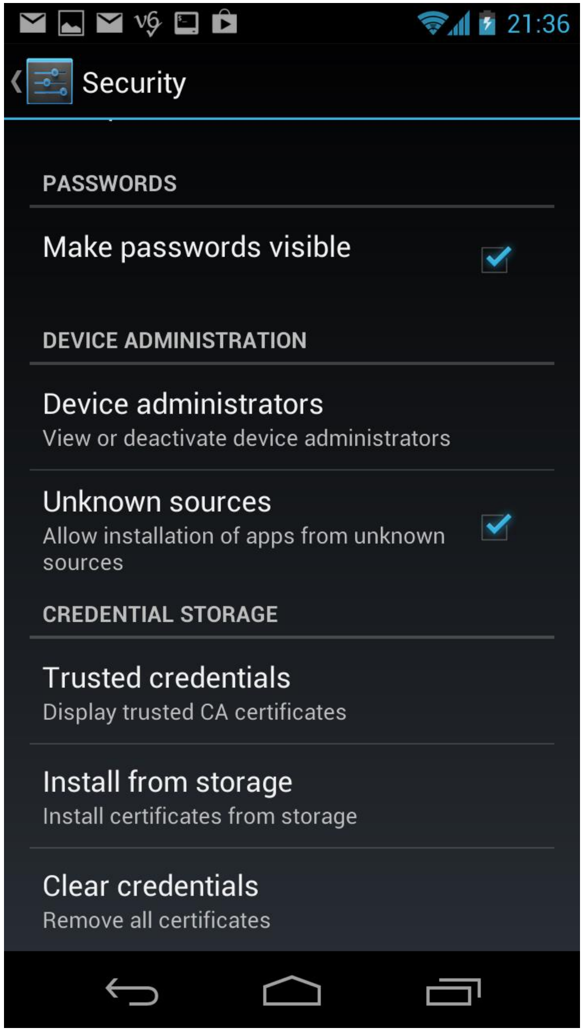
Password: ••••••••••

CA certificate:

□ Select automatically

strongSwan Project
strongSwan 2009 CA

Allow Download from Unknown Sources



PASSWORDS

Make passwords visible ☑

DEVICE ADMINISTRATION

Device administrators
View or deactivate device administrators

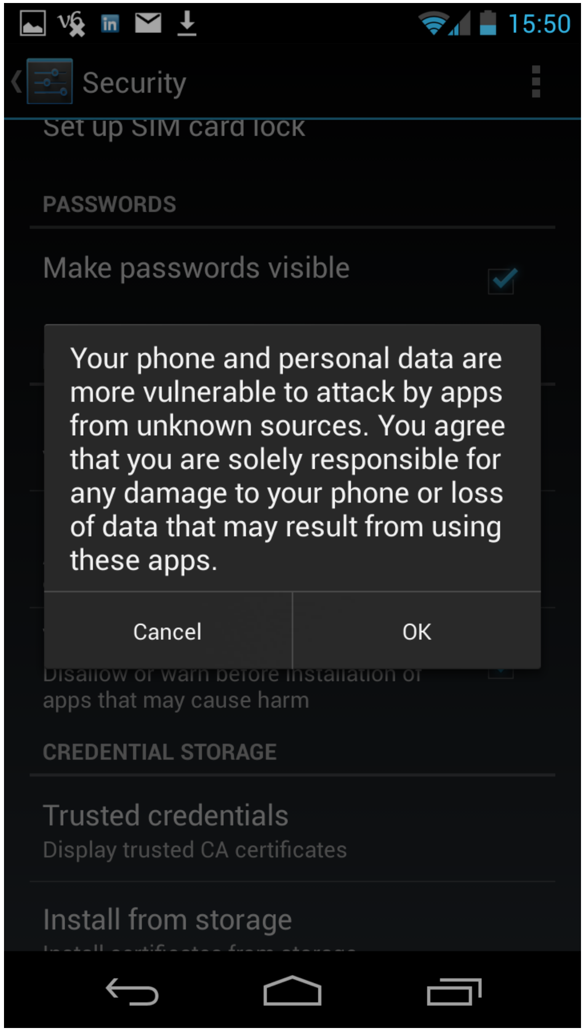
Unknown sources ☑
Allow installation of apps from unknown sources

CREDENTIAL STORAGE

Trusted credentials
Display trusted CA certificates

Install from storage
Install certificates from storage

Clear credentials
Remove all certificates



Set up SIM card lock

PASSWORDS

Make passwords visible ☑

Your phone and personal data are more vulnerable to attack by apps from unknown sources. You agree that you are solely responsible for any damage to your phone or loss of data that may result from using these apps.

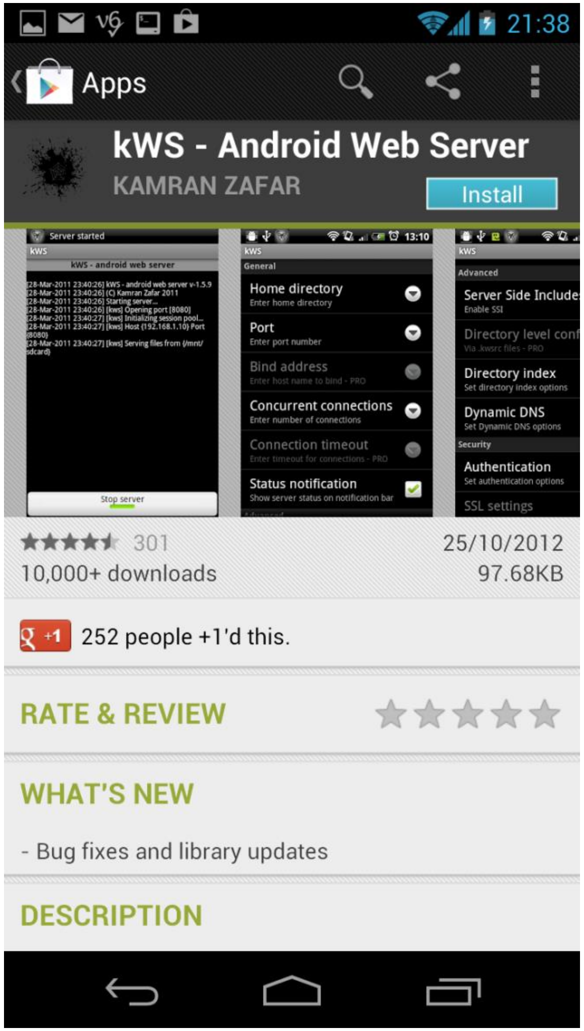
Disallow or warn before installation of apps that may cause harm

CREDENTIAL STORAGE

Trusted credentials
Display trusted CA certificates

Install from storage

Install Blacklisted Android Web Server Package



kWS - Android Web Server

KAMRAN ZAFAR

Server started

kWS

kWS - android web server

```
[28-Mar-2011 23:40:26] kWS - android web server v-1.5.9
[28-Mar-2011 23:40:26] (C) Kamran Zafar 2011
[28-Mar-2011 23:40:26] Starting server...
[28-Mar-2011 23:40:26] [kws] Opening port [8080]
[28-Mar-2011 23:40:27] [kws] Initializing session pool...
[28-Mar-2011 23:40:27] [kws] Host {192.168.1.10} Port
{8080}
[28-Mar-2011 23:40:27] [kws] Serving files from {/mnt/
sdcard}
```

kWS

General

- Home directory – Enter home directory
- Port – Enter port number
- Bind address – Enter host name to bind - PRO
- Concurrent connections – Enter number of connections
- Connection timeout – Enter timeout for connections - PRO
- Status notification – Show server status on notification bar ☑

kWS

Advanced

- Server Side Include – Enable SSI
- Directory level conf – Via .kwsrc files - PRO
- Directory index – Set directory index options
- Dynamic DNS – Set Dynamic DNS options

Security

- Authentication – Set authentication options
- SSL settings

★★★★☆ 301 — 25/10/2012

10,000+ downloads — 97.68KB

+1 252 people +1'd this.

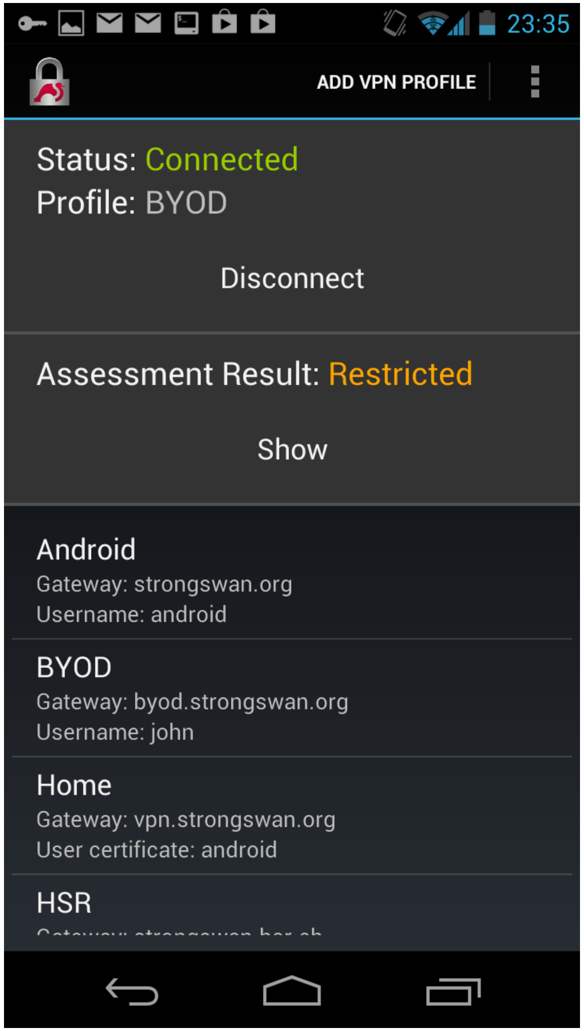
RATE & REVIEW ☆☆☆☆☆

WHAT'S NEW

- Bug fixes and library updates

DESCRIPTION

Minor Non-Compliance: Isolate Client



Status: Connected
Profile: BYOD

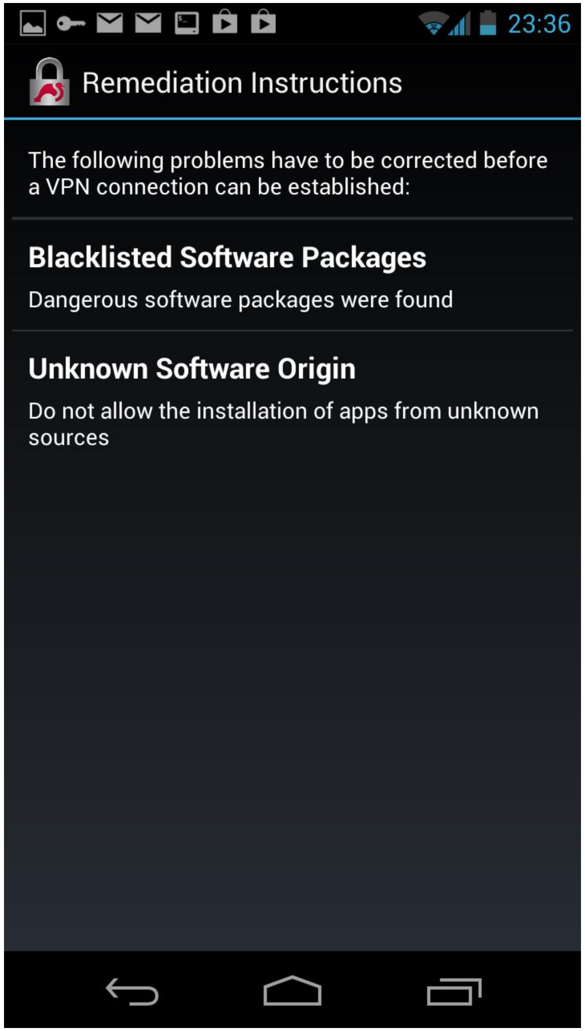
Assessment Result: Restricted

Android
Gateway: strongswan.org
Username: android

BYOD
Gateway: byod.strongswan.org
Username: john

Home
Gateway: vpn.strongswan.org
User certificate: android

HSR

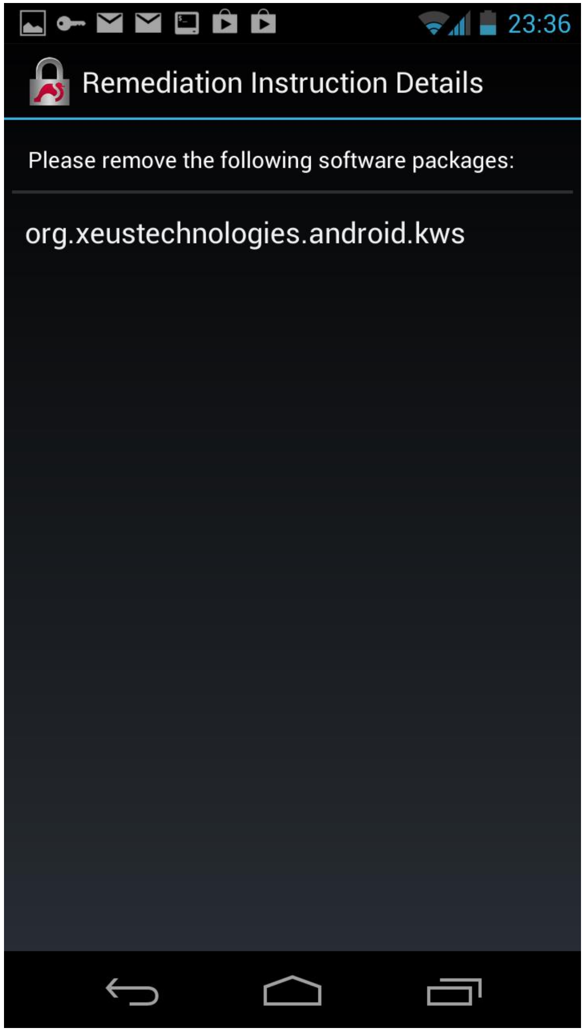


Remediation Instructions

The following problems have to be corrected before a VPN connection can be established:

Blacklisted Software Packages
Dangerous software packages were found

Unknown Software Origin
Do not allow the installation of apps from unknown sources

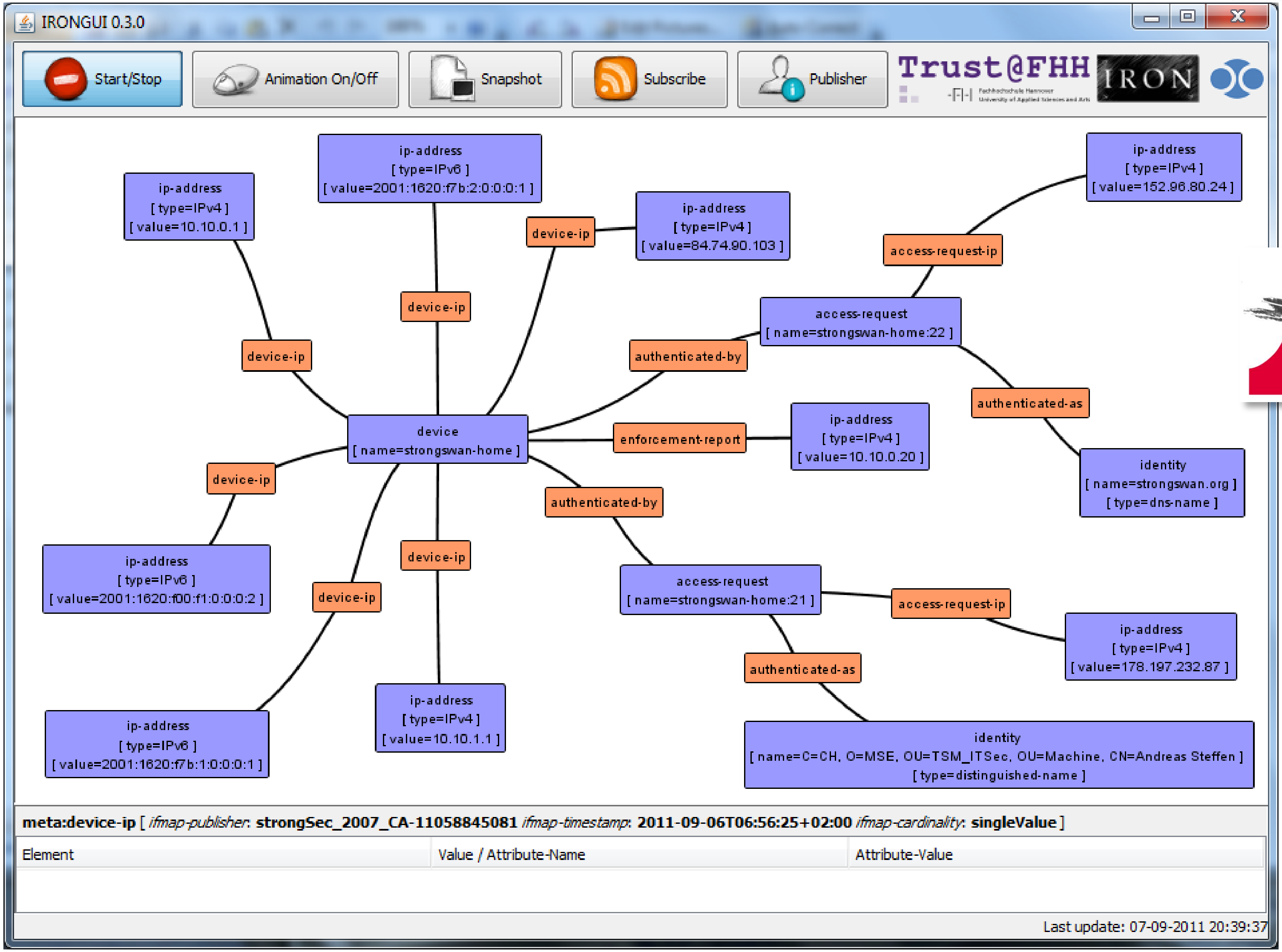


Remediation Instruction Details

Please remove the following software packages:

org.xeustechnologies.android.kws

TNC Metadata Access Point (MAP) Protocol


IRONGUI 0.3.0
Start/Stop
Animation On/Off
Snapshot
Subscribe
Publisher
Trust@FHH
IRON
ip-address [type=IPv4] [value=10.10.0.1]
ip-address [type=IPv6] [value=2001:1620:f7b:2:0:0:0:1]
device-ip
ip-address [type=IPv4] [value=84.74.90.103]
ip-address [type=IPv4] [value=152.96.80.24]
access-request-ip
device-ip
access-request [name=strongswan-home:22]
device-ip
authenticated-by
authenticated-as
device [name=strongswan-home]
enforcement-report
ip-address [type=IPv4] [value=10.10.0.20]
identity [name=strongswan.org] [type=dns-name]
device-ip
authenticated-by
ip-address [type=IPv6] [value=2001:1620:f00:f1:0:0:0:2]
device-ip
device-ip
access-request [name=strongswan-home:21]
access-request-ip
ip-address [type=IPv4] [value=178.197.232.87]
authenticated-as
ip-address [type=IPv4] [value=10.10.1.1]
ip-address [type=IPv6] [value=2001:1620:f7b:1:0:0:0:1]
identity [name=C=CH, O=MSE, OU=TSM_ITSec, OU=Machine, CN=Andreas Steffen] [type=distinguished-name]

meta:device-ip [*ifmap-publisher*: **strongSec_2007_CA-11058845081** *ifmap-timestamp*: **2011-09-06T06:56:25+02:00** *ifmap-cardinality*: **singleValue**]

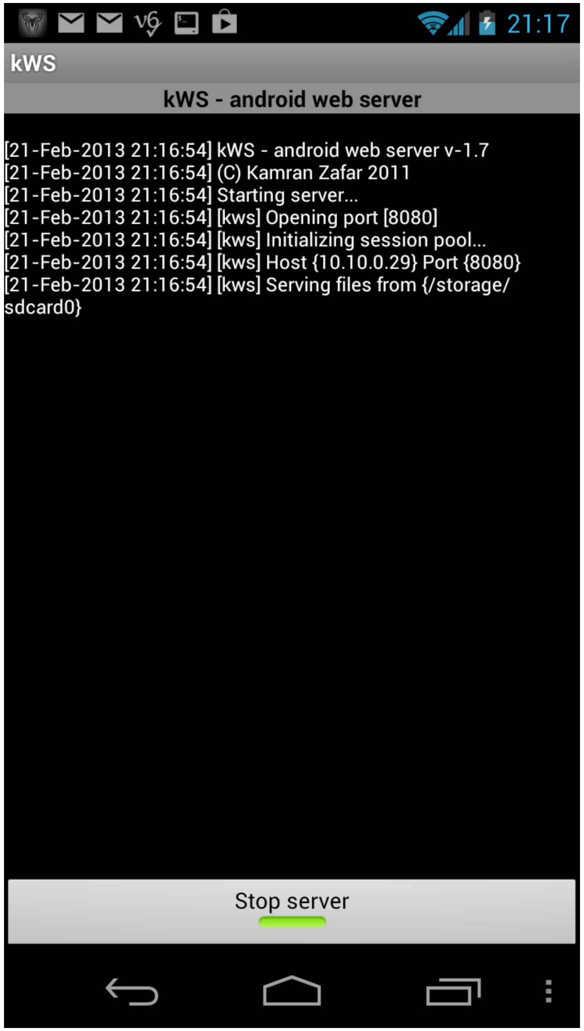
Element	Value / Attribute-Name	Attribute-Value

Last update: 07-09-2011 20:39:37

MAP-Client

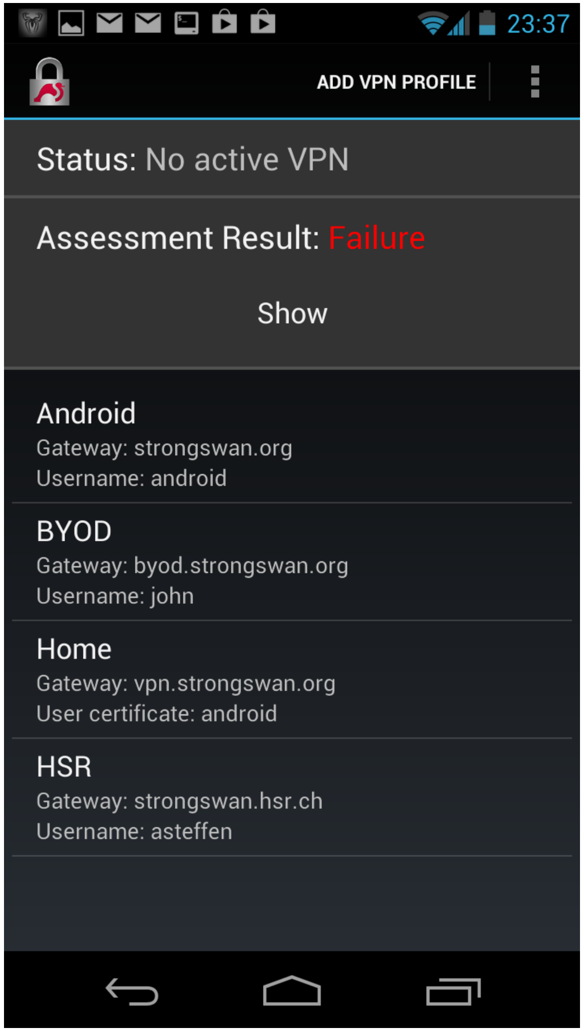
IRON Project FH Hannover (MAP-Server)

Start the Android Web Server



```
[21-Feb-2013 21:16:54] kWS - android web server v-1.7
[21-Feb-2013 21:16:54] (C) Kamran Zafar 2011
[21-Feb-2013 21:16:54] Starting server...
[21-Feb-2013 21:16:54] [kws] Opening port [8080]
[21-Feb-2013 21:16:54] [kws] Initializing session pool...
[21-Feb-2013 21:16:54] [kws] Host {10.10.0.29} Port {8080}
[21-Feb-2013 21:16:54] [kws] Serving files from {/storage/
sdcard0}
```

Major Non-Compliance: Block Client



Status: No active VPN

Assessment Result: Failure

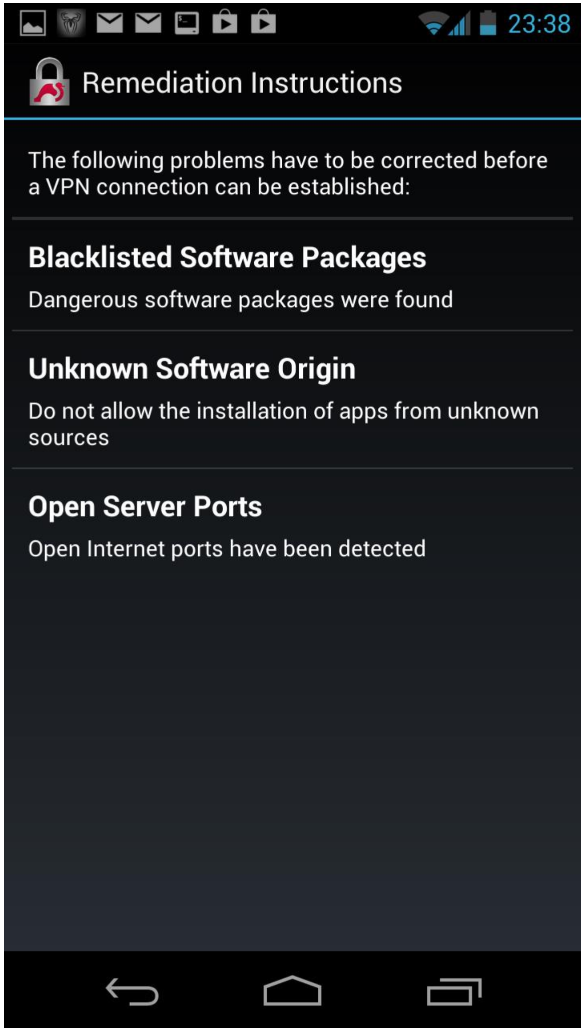
Show

Android
Gateway: strongswan.org
Username: android

BYOD
Gateway: byod.strongswan.org
Username: john

Home
Gateway: vpn.strongswan.org
User certificate: android

HSR
Gateway: strongswan.hsr.ch
Username: asteffen



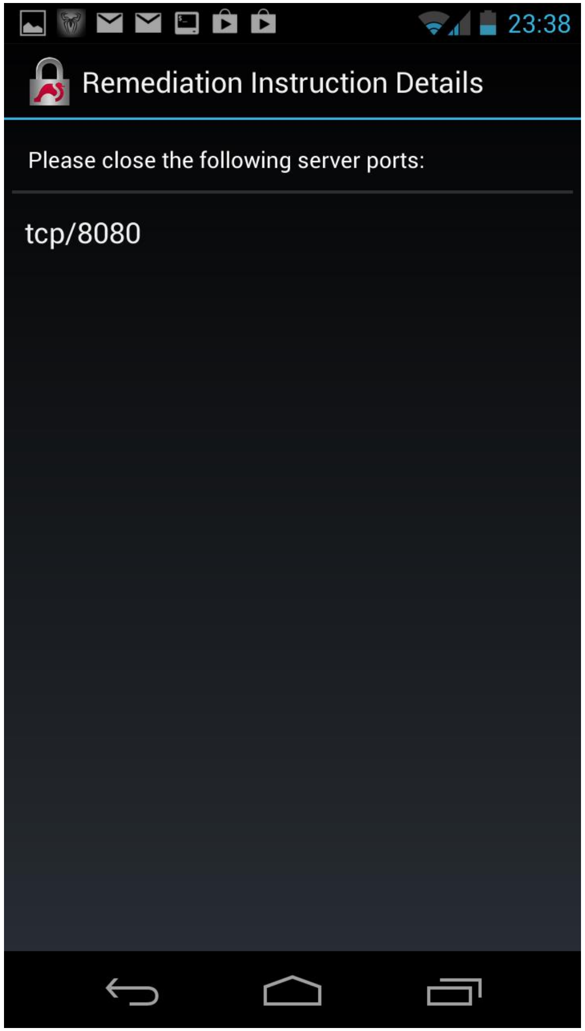
Remediation Instructions

The following problems have to be corrected before a VPN connection can be established:

Blacklisted Software Packages
Dangerous software packages were found

Unknown Software Origin
Do not allow the installation of apps from unknown sources

Open Server Ports
Open Internet ports have been detected

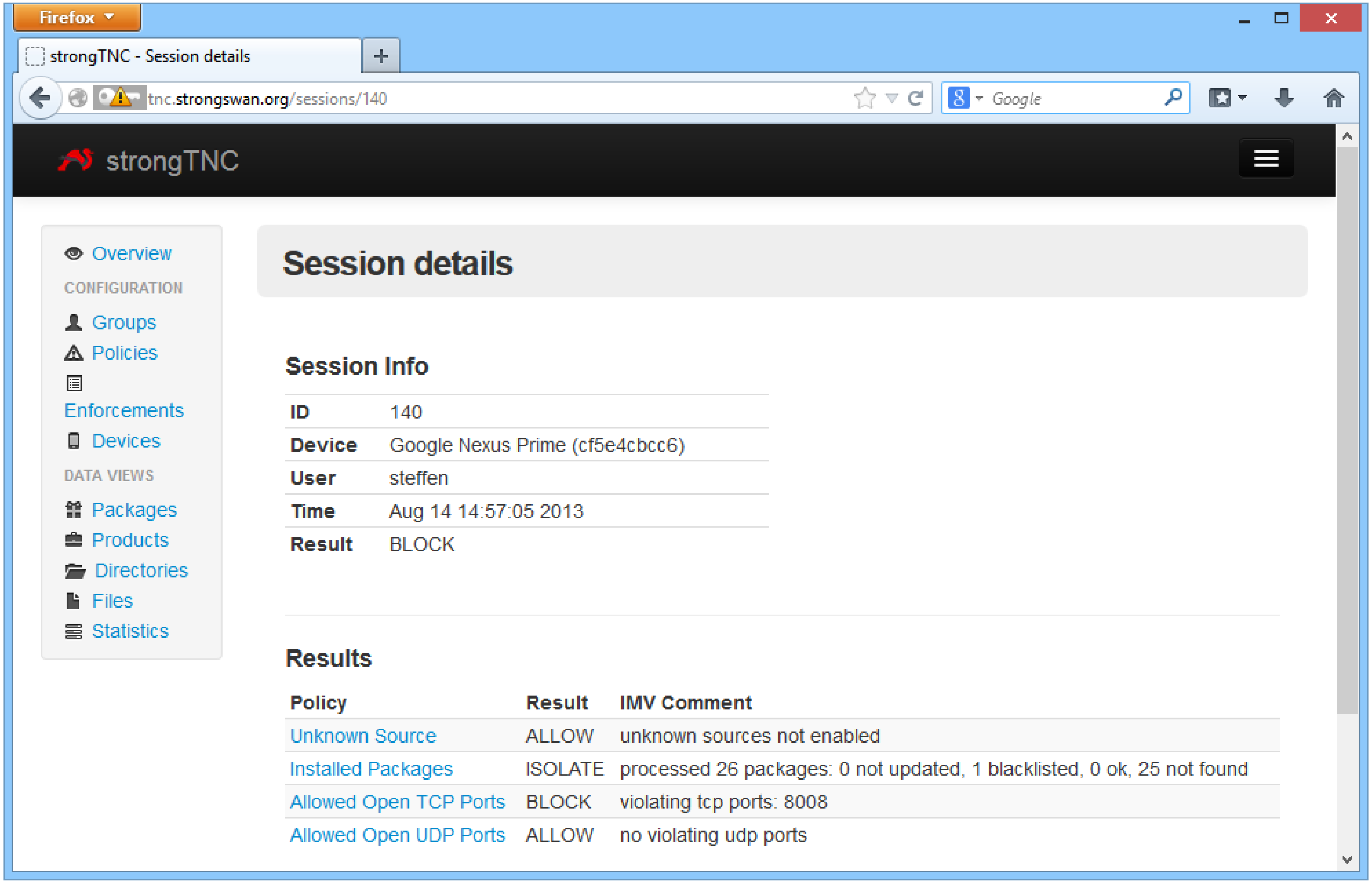


Remediation Instruction Details

Please close the following server ports:

tcp/8080

strongTNC Policy Manager



Session details

Session Info

ID	140
Device	Google Nexus Prime (cf5e4cbcc6)
User	steffen
Time	Aug 14 14:57:05 2013
Result	BLOCK

Results

Policy	Result	IMV Comment
Unknown Source	ALLOW	unknown sources not enabled
Installed Packages	ISOLATE	processed 26 packages: 0 not updated, 1 blacklisted, 0 ok, 25 not found
Allowed Open TCP Ports	BLOCK	violating tcp ports: 8008
Allowed Open UDP Ports	ALLOW	no violating udp ports

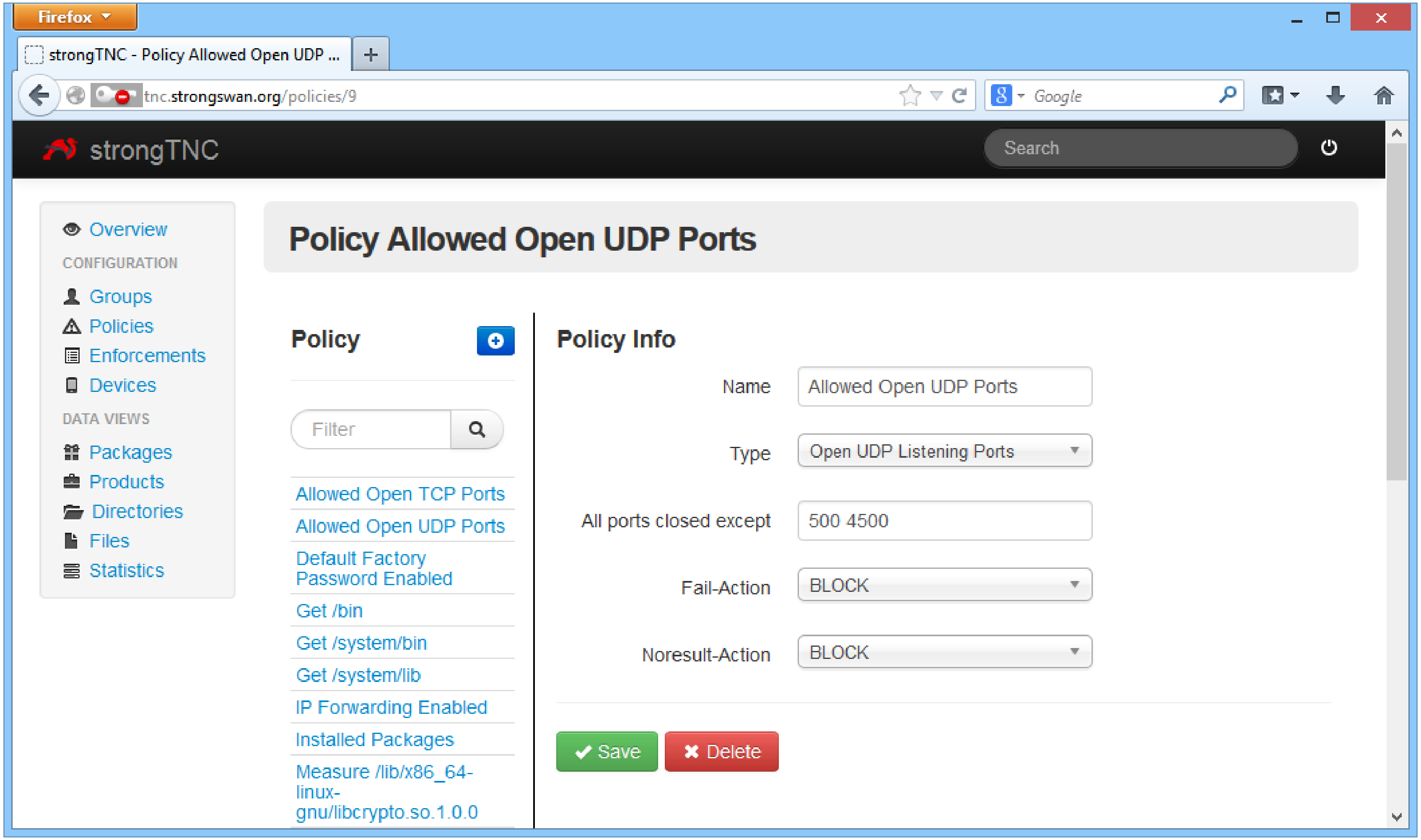
https://github.com/strongswan/strongTNC

Measurement Policies and Enforcements

Currently supported policy types:

PWDEN	Factory Default Password Enabled	
FWDEN	Forwarding Enabled	
TCPOP	TCP Ports allowed to be Open	Closed Port Default Policy
TCPBL	TCP Ports to be Blocked	Open Port Default Policy
UDPOP	UDP Ports allowed to be Open	Closed Port Default Policy
UDPBL	UDP Ports to be Blocked	Open Port Default Policy
PCKGS	Installed Packages	
UNSRC	Unknown Sources	
SWIDT	Software ID (SWID) Tag Inventory	
FREFM	File Reference Measurement	SHA1/SHA256 Hash
FMEAS	File Measurement	SHA1/SHA256 Hash
FMETA	File Metadata	Create/Modify/Access Times
DREFM	Directory Reference Measurement	SHA1/SHA256 Hashes
DMEAS	Directory Measurement	SHA1/SHA256 Hashes
DMETA	Directory Metadata	Create/Modify/Access Times

Add/Edit Policies

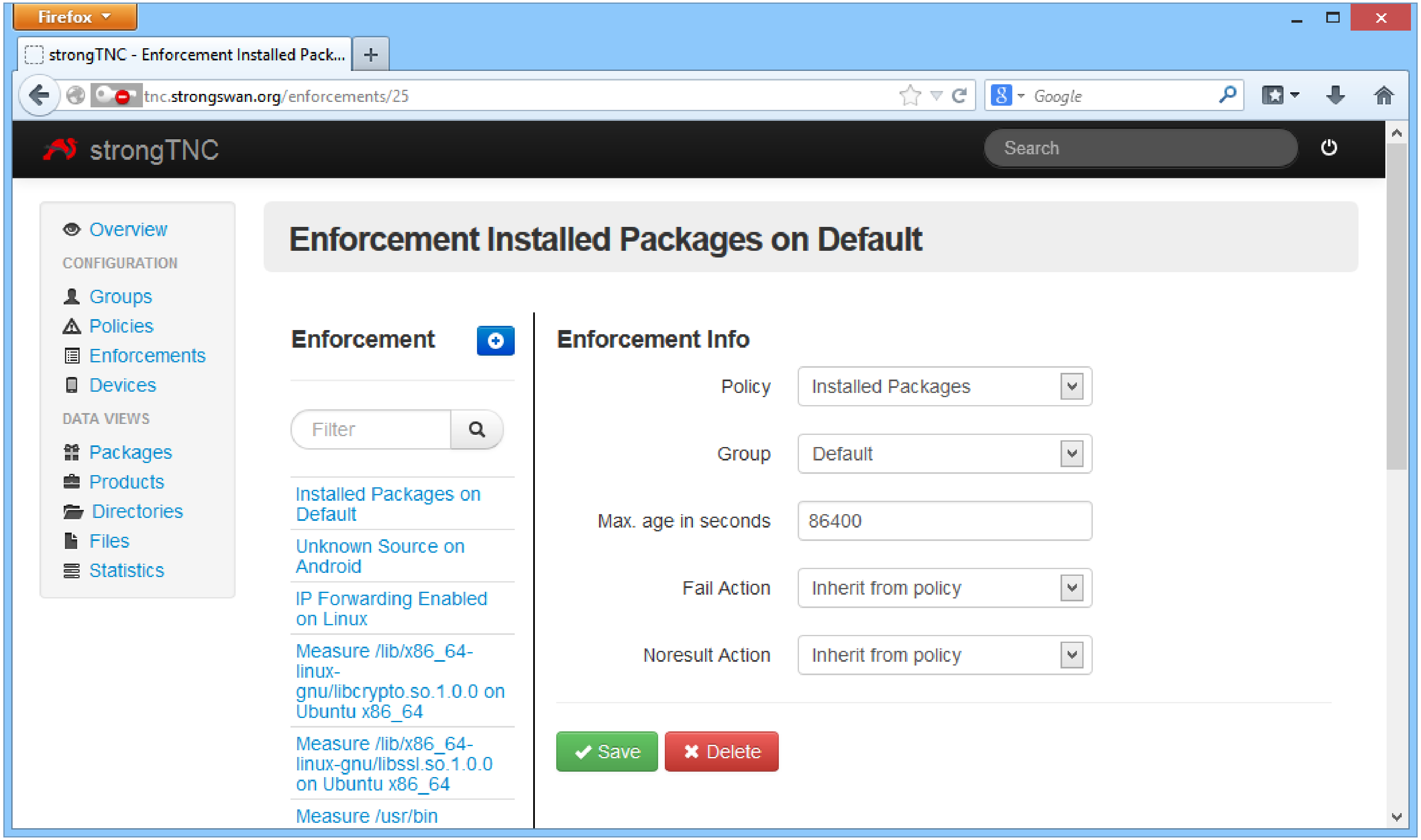


Policy Allowed Open UDP Ports

Policy Info

Name	Allowed Open UDP Ports
Type	Open UDP Listening Ports
All ports closed except	500 4500
Fail-Action	BLOCK
Noresult-Action	BLOCK

Define Enforcements



Enforcement Installed Packages on Default

Enforcement

Filter

- Installed Packages on Default
- Unknown Source on Android
- IP Forwarding Enabled on Linux
- Measure /lib/x86_64-linux-gnu/libcrypto.so.1.0.0 on Ubuntu x86_64
- Measure /lib/x86_64-linux-gnu/libssl.so.1.0.0 on Ubuntu x86_64
- Measure /usr/bin

Enforcement Info

Policy	Installed Packages
Group	Default
Max. age in seconds	86400
Fail Action	Inherit from policy
Noresult Action	Inherit from policy

TNC Summary

- The TNC protocols have become Internet Standards
- The TNC protocols are platform-independent and allow interoperability
- The TNC protocols support trustworthy TPM-based remote attestation
- The strongSwan BYOD Showcase demonstrates that TNC is ready for use
- The strongTNC policy manager bases measurements on past client behaviour

Danke für die Aufmerksamkeit!

Fragen?

www.strongswan.org