strongSwan - Feature #782

Android 5.0 IPv4 is blocked when a IPv6-only tunnel is established

06.12.2014 02:55 - JC Sargenton

Status:	Closed	**Start date:**	06.12.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	android		
Target version:			
Resolution:	Fixed		

Description

When setting up an IPv6-only tunnel (using standard EAP-MSCHAPv2 Windows-like config), Android 5.0 blocks all IPv4 traffic.

From the Android API Reference, it seems the new default behavior is to block packets from the address family that is not used within the tunnel.

A new API function was introduced in API Level 21 to allow the other address family to pass unaffected outside the tunnel. I couldn't find any reference to this function in Strongswan source code. So I guess it is not currently used.
http://developer.android.com/reference/android/net/VpnService.Builder.html#allowFamily%28int%29

Server-side

```
$ ipsec --version
Linux strongSwan U5.2.1/K3.13.0-39-generic

$ uname -a
Linux hostnmae 3.13.0-39-generic #66-Ubuntu SMP Tue Oct 28 13:30:27 UTC 2014 x86_64 x86_64 x86_64
GNU/Linux
```

ipsec.conf

```
conn android
        left=10.10.10.10
        leftsubnet=2000::/3
        leftcert=serverCert.pem
        lefthostaccess=yes
        leftfirewall=yes
        right=%any
        rightauth=eap-mschapv2
        eap_identity=%any
        rightsourceip=2001:db8:100::/96
        rightdns=2001:db8::53
        ike=aes256-sha256-modp2048!
        esp=aes256-sha256-modp2048!
        keyexchange=ikev2
        auto=add
```

Client-side

Android 5.0, strongSwan 5.2.1dr1
Profile TYpe: IKEv2 EAP (Username/Password)

Associated revisions

Revision f14feed0 - 28.07.2015 13:55 - Tobias Brunner

Merge branch 'android-updates'

Fixes the roaming behavior on Android 5+, a linker issue on Android M,
a few bugs, and adds several new advanced options for VPN profile (MTU,
server port, split tunneling).

Also adds methods and a constructor to parse settings_t from a string instead of a file.

Fixes #782, #847, #865.

History

#1 - 28.07.2015 14:20 - Tobias Brunner

- Tracker changed from Issue to Feature

- Category set to android

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- % Done set to 0

- Resolution set to Fixed

Version 1.5.0 of the app now uses this method to allow traffic of the unused address family to bypass the VPN. There are also two new options to disable this for a specific family and block traffic that is not destined for the VPN.