strongSwan - Bug #319

Win7 to Strongswan 5.0.x connection issue in IKEv1 transport mode

27.03.2013 17:48 - laurent leonardon

Status:	Closed	**Start date:**	27.03.2013
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.1.0		
Affected version:	5.0.1	**Resolution:**	Fixed

Description

Hello,

I m currently using strongSwan to authenticate a Windows 7 client to access my Linux Server. I use the Win7 "Windows Firewall with Advanced Security" with the "Connection Security rules" features for the IPSEC connection (Allow me to automaticaly authenticate the Win7 laptop when it try to access the linux server without user action). This Win7 client seems to only support IKEv1.
To have the minimum of network and server impact I authenticate the win7 using transport mode and null encryption.

I was previously in strongswan version 4.x.x and I have updated strongSwan with the version 5.0.1.
Since the update I m not able anymore to connect my Win7 in transport mode to the Linux server with strongswan 5.0.x.
The main mode phase is ok but the quick mode never finish and I have no error message. I added in attachement files the Win7 configuration and a pcap file from the win 7 side.

My strongSwan configuration is the following:

```
root@corellia:/etc# more ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
    charondebug="ike 2, net 2"
       uniqueids = yes

conn %default
     auth=esp
     mobike=no

conn WIN7_Transport
 authby=psk
 esp=null-md5!
 ike=aes128-md5-modp1024,3des-md5-modp1024
 keyexchange=ikev1
 type=transport
 left=192.168.1.103
 right=192.168.1.2
 auto=start

#include /var/lib/strongswan/ipsec.conf.inc
```

I have the following ipsec status:

```
root@corellia:/etc# ipsec statusall
Status of IKE charon daemon (strongSwan 5.0.1, Linux 2.6.32-45-generic, i686):
  uptime: 14 minutes, since Mar 22 17:49:35 2013
  malloc: sbrk 135168, mmap 0, used 104336, free 30832
  worker threads: 8 of 16 idle, 7/1/0/0 working, job queue: 0/0/0/0, scheduled: 16
  loaded plugins: charon aes des sha1 sha2 md5 random nonce x509 revocation constraints pubkey pkc
s1 pkcs8 pgp dnskey pem fips-prf gmp xcbc cmac hmac attr kernel-netlink resolve socket-default str
oke updown xauth-generic
Listening IP addresses:
  172.16.1.254
```

```
  192.168.1.103
Connections:
         EFB:  192.168.1.103...192.168.1.2  IKEv1
         EFB:   local:  [192.168.1.103] uses pre-shared key authentication
         EFB:   remote: [192.168.1.2] uses pre-shared key authentication
         EFB:   child:  dynamic === dynamic TRANSPORT
Security Associations (1 up, 0 connecting):
         EFB[8]: ESTABLISHED 3 seconds ago, 192.168.1.103[192.168.1.103]...192.168.1.2[192.168.1.2
]
         EFB[8]: IKEv1 SPIs: c911ffdc4c6bf201_i 1b1a18a730dff768_r*, pre-shared key reauthenticati
on in 2 hours
         EFB[8]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
         EFB[8]: Tasks passive: QUICK_MODE
```

- I made some additionnal test and it work in tunnel mode with a similar configuration (except the type).
- I updated my StrongSwan with the 5.0.2 release and with this version nothing work... (tunnel or transport).

I don't know if it is a bug in the IKEv1 implementation in the 5.0.x release or an issue in my config and now I have no more idea and way forward to get something that work.

thanks in advance for your help or idea to resolve my issue.

Regards,
Laurent

Associated revisions

Revision 77ccff82 - 25.07.2013 17:08 - Tobias Brunner

ikev1: Always send ID payloads (traffic selectors) during Quick Mode

Especially Windows 7 has problems if the peer does not send ID payloads
for host-to-host connections (tunnel and transport mode).

Fixes #319.

History

#1 - 25.07.2013 17:11 - Tobias Brunner

- Description updated

- Category set to charon

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Priority changed from High to Normal

- Target version set to 5.1.0

- Resolution set to Fixed

It seems this is due to charon's persistence to **not** send ID payloads (traffic selectors) during Quick Mode if negotiating a host-to-host tunnel. I changed this with the associated commit by always sending these payloads, which should not have any negative side-effects.

Files

WIN7_to_Strongswan501_tun.pcapng	6.36 KB	27.03.2013	laurent leonardon