strongSwan - Bug #220

Incorrect IP address in policy for Windows l2tp client behind nat.

30.08.2012 11:11 - Eugene Sumin

Status:	Closed	**Start date:**	30.08.2012
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.0.1		
Affected version:	5.0.0	**Resolution:**	Fixed

Description

Tested configuration :

```
10.55.0.2 <=========> | 10.55.0.3 ( < NAT < ) 10.66.0.3 | <========> 10.66.0.1
debian 6 + strongswan 5.0           |           debian 6          |          Windows 7 (roa
d warrior)
```

Policy :
src 10.66.0.1/32 dst 10.55.0.2/32
src 10.55.0.2/32 dst 10.66.0.1/32

Should be
src 10.55.0.3/32 dst 10.55.0.2/32
src 10.55.0.2/32 dst 10.55.0.1/32

ipsec.conf
.... truncated ...
conn test_cert
auth=esp
authby=rsasig
auto=add
type=transport
left=10.55.0.2
leftcert=vpngw.pem
right=%any
rightsubnetwithin=0.0.0.0/0

ipsec.secrets
: RSA "vpngw.pem"

Is it bug or i'm doing something wrong ?

Associated revisions

Revision a889cfe5 - 14.09.2012 09:40 - Tobias Brunner

Change traffic selectors during Quick Mode in case of a NAT in transport mode

Windows 7 sends its internal address as TSi. While we don't support the
NAT-T drafts as used by Windows XP it is interesting to note that the
client there omits the TSi payload which then would automatically get set
to the public IP address of the client.

Fixes #220.

History

#1 - 06.09.2012 15:36 - Tobias Brunner

- Category set to charon

- Status changed from New to Assigned

- Assignee set to Tobias Brunner

- Target version set to 5.0.1

Yes, this is a bug. With transport mode over a NAT device the traffic selectors have to be adjusted so that they properly reflect the NAT situation. This is currently not done.

I wonder though, is there a particular reason why you use L2TP with Windows 7, now that Windows 7 comes with a proper [IKEv2 client](#).

#2 - 14.09.2012 09:45 - Tobias Brunner

- Status changed from Assigned to Resolved

- Resolution set to Fixed

Should be fixed with the associated commit.

#3 - 25.09.2012 09:35 - Tobias Brunner

- Status changed from Resolved to Closed