strongSwan - Feature #365

Multiple L2TP-IPsec clients behind same NAT

25.07.2013 14:43 - Pavel Kopchyk

Status:	Closed	**Start date:**	25.07.2013
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.0		
Resolution:	Fixed		

Description

I'm using 5.0.4 on a production server - no problem.

On the test server I installed 5.1.0rc1, and there appeared the problems:

55.33.22.17 - NAT router
55.33.22.19 - IPsec GW (strongSwan)
Clients - Windows 7 (L2TP IPsec VPN - IKEv1)

The first client connects and works:

```
Jul 25 14:14:36 moon charon: 14[NET] received packet: from 55.33.22.17[500] to 55.33.22.19[500] (3
84 bytes)
Jul 25 14:14:36 moon charon: 14[ENC] parsed ID_PROT request 0 [ SA V V V V V V V ]
Jul 25 14:14:36 moon charon: 14[ENC] received unknown vendor ID: 1e:2b:51:69:05:99:1c:7d:7c:96:fc:
bf:b5:87:e4:61:00:00:00:08
Jul 25 14:14:36 moon charon: 14[IKE] received NAT-T (RFC 3947) vendor ID
Jul 25 14:14:36 moon charon: 14[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Jul 25 14:14:36 moon charon: 14[ENC] received unknown vendor ID: 40:48:b7:d5:6e:bc:e8:85:25:e7:de:
7f:00:d6:c2:d3
Jul 25 14:14:36 moon charon: 14[ENC] received unknown vendor ID: fb:1d:e3:cd:f3:41:b7:ea:16:b7:e5:
be:08:55:f1:20
Jul 25 14:14:36 moon charon: 14[ENC] received unknown vendor ID: 26:24:4d:38:ed:db:61:b3:17:2a:36:
e3:d0:cf:b8:19
Jul 25 14:14:36 moon charon: 14[ENC] received unknown vendor ID: e3:a5:96:6a:76:37:9f:e7:07:22:82:
31:e5:ce:86:52
Jul 25 14:14:36 moon charon: 14[IKE] 55.33.22.17 is initiating a Main Mode IKE_SA
Jul 25 14:14:36 moon charon: 14[ENC] generating ID_PROT response 0 [ SA V V V ]
Jul 25 14:14:36 moon charon: 14[NET] sending packet: from 55.33.22.19[500] to 55.33.22.17[500] (13
6 bytes)
Jul 25 14:14:36 moon charon: 15[NET] received packet: from 55.33.22.17[500] to 55.33.22.19[500] (3
88 bytes)
Jul 25 14:14:36 moon charon: 15[ENC] parsed ID_PROT request 0 [ KE No NAT-D NAT-D ]
Jul 25 14:14:36 moon charon: 15[IKE] remote host is behind NAT
Jul 25 14:14:36 moon charon: 15[IKE] sending cert request for "C=CH, O=TEST, CN=strongSwan CA"
Jul 25 14:14:36 moon charon: 15[ENC] generating ID_PROT response 0 [ KE No CERTREQ CERTREQ NAT-D N
AT-D ]
Jul 25 14:14:36 moon charon: 15[NET] sending packet: from 55.33.22.19[500] to 55.33.22.17[500] (55
5 bytes)
Jul 25 14:14:36 moon charon: 06[NET] received packet: from 55.33.22.17[4500] to 55.33.22.19[4500]
(1580 bytes)
Jul 25 14:14:36 moon charon: 06[ENC] parsed ID_PROT request 0 [ ID CERT SIG CERTREQ ]
Jul 25 14:14:36 moon charon: 06[IKE] received cert request for 'C=CH, O=TEST, CN=strongSwan CA'
Jul 25 14:14:36 moon charon: 06[IKE] received end entity cert "C=CH, O=TEST, CN=client01"
Jul 25 14:14:36 moon charon: 06[CFG] looking for RSA signature peer configs matching 55.33.22.19..
.55.33.22.17[C=CH, O=TEST, CN=client01]
Jul 25 14:14:36 moon charon: 06[CFG] selected peer config "win7-ikev1"
Jul 25 14:14:36 moon charon: 06[CFG]   using certificate "C=CH, O=TEST, CN=client01"
Jul 25 14:14:36 moon charon: 06[CFG]   using trusted ca certificate "C=CH, O=TEST, CN=strongSwan C
A"
Jul 25 14:14:36 moon charon: 06[CFG] checking certificate status of "C=CH, O=TEST, CN=client01"
```

```
Jul 25 14:14:36 moon charon: 06[CFG] certificate status is not available
Jul 25 14:14:36 moon charon: 06[CFG]   reached self-signed root ca with a path length of 0
Jul 25 14:14:36 moon charon: 06[IKE] authentication of 'C=CH, O=TEST, CN=client01' with RSA succes
sful
Jul 25 14:14:36 moon charon: 06[IKE] authentication of 'moon.example.org' (myself) successful
Jul 25 14:14:36 moon charon: 06[IKE] IKE_SA win7-ikev1[1] established between 55.33.22.19[moon.exa
mple.org]...55.33.22.17[C=CH, O=TEST, CN=client01]
Jul 25 14:14:36 moon charon: 06[IKE] DPD not supported by peer, disabled
Jul 25 14:14:36 moon charon: 06[IKE] sending end entity cert "C=PL, ST=Poland, L=Warsaw, O=Asstra
AG, CN=moon.example.org, E=ca@asstra.by"
Jul 25 14:14:36 moon charon: 06[ENC] generating ID_PROT response 0 [ ID CERT SIG ]
Jul 25 14:14:36 moon charon: 06[NET] sending packet: from 55.33.22.19[4500] to 55.33.22.17[4500] (
1420 bytes)
Jul 25 14:14:36 moon charon: 08[NET] received packet: from 55.33.22.17[4500] to 55.33.22.19[4500]
(380 bytes)
Jul 25 14:14:36 moon charon: 08[ENC] parsed QUICK_MODE request 1 [ HASH SA No ID ID NAT-OA NAT-OA
]
Jul 25 14:14:36 moon charon: 08[IKE] received 3600s lifetime, configured 0s
Jul 25 14:14:36 moon charon: 08[IKE] received 250000000 lifebytes, configured 0
Jul 25 14:14:36 moon charon: 08[ENC] generating QUICK_MODE response 1 [ HASH SA No ID ID NAT-OA NA
T-OA ]
Jul 25 14:14:36 moon charon: 08[NET] sending packet: from 55.33.22.19[4500] to 55.33.22.17[4500] (
204 bytes)
Jul 25 14:14:36 moon charon: 07[NET] received packet: from 55.33.22.17[4500] to 55.33.22.19[4500]
(60 bytes)
Jul 25 14:14:36 moon charon: 07[ENC] parsed QUICK_MODE request 1 [ HASH ]
Jul 25 14:14:36 moon charon: 07[IKE] CHILD_SA win7-ikev1{1} established with SPIs c45fb2eb_i 24a67
9b0_o and TS 55.33.22.19/32[udp/l2tp] === 55.33.22.17/32[udp/l2tp]
... xl2tpd ...
```

I try to connect a second client:

```
Jul 25 14:16:06 moon charon: 08[NET] received packet: from 55.33.22.17[1] to 55.33.22.19[500] (384
 bytes)
Jul 25 14:16:06 moon charon: 08[ENC] parsed ID_PROT request 0 [ SA V V V V V V V ]
Jul 25 14:16:06 moon charon: 08[ENC] received unknown vendor ID: 1e:2b:51:69:05:99:1c:7d:7c:96:fc:
bf:b5:87:e4:61:00:00:00:08
Jul 25 14:16:06 moon charon: 08[IKE] received NAT-T (RFC 3947) vendor ID
Jul 25 14:16:06 moon charon: 08[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Jul 25 14:16:06 moon charon: 08[ENC] received unknown vendor ID: 40:48:b7:d5:6e:bc:e8:85:25:e7:de:
7f:00:d6:c2:d3
Jul 25 14:16:06 moon charon: 08[ENC] received unknown vendor ID: fb:1d:e3:cd:f3:41:b7:ea:16:b7:e5:
be:08:55:f1:20
Jul 25 14:16:06 moon charon: 08[ENC] received unknown vendor ID: 26:24:4d:38:ed:db:61:b3:17:2a:36:
e3:d0:cf:b8:19
Jul 25 14:16:06 moon charon: 08[ENC] received unknown vendor ID: e3:a5:96:6a:76:37:9f:e7:07:22:82:
31:e5:ce:86:52
Jul 25 14:16:06 moon charon: 08[IKE] 55.33.22.17 is initiating a Main Mode IKE_SA
Jul 25 14:16:06 moon charon: 08[ENC] generating ID_PROT response 0 [ SA V V V ]
Jul 25 14:16:06 moon charon: 08[NET] sending packet: from 55.33.22.19[500] to 55.33.22.17[1] (136
bytes)
Jul 25 14:16:06 moon charon: 07[NET] received packet: from 55.33.22.17[1] to 55.33.22.19[500] (388
 bytes)
Jul 25 14:16:06 moon charon: 07[ENC] parsed ID_PROT request 0 [ KE No NAT-D NAT-D ]
Jul 25 14:16:06 moon charon: 07[IKE] remote host is behind NAT
Jul 25 14:16:06 moon charon: 07[IKE] sending cert request for "C=CH, O=TEST, CN=strongSwan CA"
Jul 25 14:16:06 moon charon: 07[ENC] generating ID_PROT response 0 [ KE No CERTREQ CERTREQ NAT-D N
AT-D ]
Jul 25 14:16:06 moon charon: 07[NET] sending packet: from 55.33.22.19[500] to 55.33.22.17[1] (555
bytes)
Jul 25 14:16:06 moon charon: 12[NET] received packet: from 55.33.22.17[1024] to 55.33.22.19[4500]
(1580 bytes)
Jul 25 14:16:06 moon charon: 12[ENC] parsed ID_PROT request 0 [ ID CERT SIG CERTREQ ]
Jul 25 14:16:06 moon charon: 12[IKE] received cert request for 'C=CH, O=TEST, CN=strongSwan CA'
Jul 25 14:16:06 moon charon: 12[IKE] received end entity cert "C=CH, O=TEST, CN=client02"
Jul 25 14:16:06 moon charon: 12[CFG] looking for RSA signature peer configs matching 55.33.22.19..
```

```
.55.33.22.17[C=CH, O=TEST, CN=client02]
Jul 25 14:16:06 moon charon: 12[CFG] selected peer config "win7-ikev1"
Jul 25 14:16:06 moon charon: 12[CFG]   using certificate "C=CH, O=TEST, CN=client02"
Jul 25 14:16:06 moon charon: 12[CFG]   using trusted ca certificate "C=CH, O=TEST, CN=strongSwan C
A"
Jul 25 14:16:06 moon charon: 12[CFG] checking certificate status of "C=CH, O=TEST, CN=client02"
Jul 25 14:16:06 moon charon: 12[CFG] certificate status is not available
Jul 25 14:16:06 moon charon: 12[CFG]   reached self-signed root ca with a path length of 0
Jul 25 14:16:06 moon charon: 12[IKE] authentication of 'C=CH, O=TEST, CN=client02' with RSA succes
sful
Jul 25 14:16:06 moon charon: 12[IKE] authentication of 'moon.example.org' (myself) successful
Jul 25 14:16:06 moon charon: 12[IKE] IKE_SA win7-ikev1[2] established between 55.33.22.19[moon.exa
mple.org]...55.33.22.17[C=CH, O=TEST, CN=client02]
Jul 25 14:16:06 moon charon: 12[IKE] DPD not supported by peer, disabled
Jul 25 14:16:06 moon charon: 12[IKE] sending end entity cert "C=PL, ST=Poland, L=Warsaw, O=Asstra
AG, CN=moon.example.org, E=ca@asstra.by"
Jul 25 14:16:06 moon charon: 12[ENC] generating ID_PROT response 0 [ ID CERT SIG ]
Jul 25 14:16:06 moon charon: 12[NET] sending packet: from 55.33.22.19[4500] to 55.33.22.17[1024] (
1420 bytes)
Jul 25 14:16:06 moon charon: 09[NET] received packet: from 55.33.22.17[1024] to 55.33.22.19[4500]
(380 bytes)
Jul 25 14:16:06 moon charon: 09[ENC] parsed QUICK_MODE request 1 [ HASH SA No ID ID NAT-OA NAT-OA
]
Jul 25 14:16:06 moon charon: 09[IKE] received 3600s lifetime, configured 0s
Jul 25 14:16:06 moon charon: 09[IKE] received 250000000 lifebytes, configured 0
Jul 25 14:16:06 moon charon: 09[ENC] generating QUICK_MODE response 1 [ HASH SA No ID ID NAT-OA NA
T-OA ]
Jul 25 14:16:06 moon charon: 09[NET] sending packet: from 55.33.22.19[4500] to 55.33.22.17[1024] (
204 bytes)
Jul 25 14:16:06 moon charon: 04[NET] received packet: from 55.33.22.17[1024] to 55.33.22.19[4500]
(60 bytes)
Jul 25 14:16:06 moon charon: 04[ENC] parsed QUICK_MODE request 1 [ HASH ]
Jul 25 14:16:06 moon charon: 04[CFG] unable to install policy 55.33.22.19/32[udp/l2tp] === 55.33.2
2.17/32[udp/l2tp] out (mark 0/0x00000000) for reqid 2, the same policy for reqid 1 exists
Jul 25 14:16:06 moon charon: 04[CFG] unable to install policy 55.33.22.17/32[udp/l2tp] === 55.33.2
2.19/32[udp/l2tp] in (mark 0/0x00000000) for reqid 2, the same policy for reqid 1 exists
Jul 25 14:16:06 moon charon: 04[CFG] unable to install policy 55.33.22.19/32[udp/l2tp] === 55.33.2
2.17/32[udp/l2tp] out (mark 0/0x00000000) for reqid 2, the same policy for reqid 1 exists
Jul 25 14:16:06 moon charon: 04[CFG] unable to install policy 55.33.22.17/32[udp/l2tp] === 55.33.2
2.19/32[udp/l2tp] in (mark 0/0x00000000) for reqid 2, the same policy for reqid 1 exists
Jul 25 14:16:06 moon charon: 04[IKE] unable to install IPsec policies (SPD) in kernel
Jul 25 14:16:06 moon charon: 04[KNL] deleting policy 55.33.22.19/32[udp/l2tp] === 55.33.22.17/32[u
dp/l2tp] out failed, not found
Jul 25 14:16:06 moon charon: 04[KNL] deleting policy 55.33.22.17/32[udp/l2tp] === 55.33.22.19/32[u
dp/l2tp] in failed, not found
Jul 25 14:16:06 moon charon: 04[KNL] deleting policy 55.33.22.19/32[udp/l2tp] === 55.33.22.17/32[u
dp/l2tp] out failed, not found
Jul 25 14:16:06 moon charon: 04[KNL] deleting policy 55.33.22.17/32[udp/l2tp] === 55.33.22.19/32[u
dp/l2tp] in failed, not found
Jul 25 14:16:06 moon charon: 04[IKE] sending DELETE for ESP CHILD_SA with SPI 93434c4e
Jul 25 14:16:06 moon charon: 04[ENC] generating INFORMATIONAL_V1 request 2674692744 [ HASH D ]
Jul 25 14:16:06 moon charon: 04[NET] sending packet: from 55.33.22.19[4500] to 55.33.22.17[1024] (
76 bytes)
Jul 25 14:16:41 moon charon: 06[NET] received packet: from 55.33.22.17[1024] to 55.33.22.19[4500]
(76 bytes)
Jul 25 14:16:41 moon charon: 06[ENC] parsed INFORMATIONAL_V1 request 2802980633 [ HASH D ]
Jul 25 14:16:41 moon charon: 06[IKE] received DELETE for ESP CHILD_SA with SPI 93434c4e
Jul 25 14:16:41 moon charon: 06[IKE] CHILD_SA not found, ignored
Jul 25 14:16:41 moon charon: 08[NET] received packet: from 55.33.22.17[1024] to 55.33.22.19[4500]
(92 bytes)
Jul 25 14:16:41 moon charon: 08[ENC] parsed INFORMATIONAL_V1 request 1884239400 [ HASH D ]
Jul 25 14:16:41 moon charon: 08[IKE] received DELETE for IKE_SA win7-ikev1[2]
Jul 25 14:16:41 moon charon: 08[IKE] deleting IKE_SA win7-ikev1[2] between 55.33.22.19[moon.exampl
e.org]...55.33.22.17[C=CH, O=TEST, CN=client02]
```

And get a 809 error.

It looks like this is the reason for the error

```
Jul 25 14:16:06 moon charon: 04[CFG] unable to install policy 55.33.22.19/32[udp/l2tp] === 55.33.2
2.17/32[udp/l2tp] out (mark 0/0x00000000) for reqid 2, the same policy for reqid 1 exists
Jul 25 14:16:06 moon charon: 04[CFG] unable to install policy 55.33.22.17/32[udp/l2tp] === 55.33.2
2.19/32[udp/l2tp] in (mark 0/0x00000000) for reqid 2, the same policy for reqid 1 exists
Jul 25 14:16:06 moon charon: 04[CFG] unable to install policy 55.33.22.19/32[udp/l2tp] === 55.33.2
2.17/32[udp/l2tp] out (mark 0/0x00000000) for reqid 2, the same policy for reqid 1 exists
Jul 25 14:16:06 moon charon: 04[CFG] unable to install policy 55.33.22.17/32[udp/l2tp] === 55.33.2
2.19/32[udp/l2tp] in (mark 0/0x00000000) for reqid 2, the same policy for reqid 1 exists
Jul 25 14:16:06 moon charon: 04[IKE] unable to install IPsec policies (SPD) in kernel
```

Related issues:

Related to Issue #712: Windows connect failed with error 809	**Closed**	**22.09.2014**

Associated revisions

Revision c72fa57a - 20.02.2015 16:34 - Martin Willi

Merge branch 'connmark'

Introduce a connmark plugin that uses Netfilter conntracks mark to select the
correct return-path SAs for client-initiated connections. This can be used
to distinguish transport mode clients behind the same NAT router.

Fixes #365.

History

#1 - 25.07.2013 15:31 - Tobias Brunner

- Tracker changed from Bug to Issue

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

This setup is not supported without special consideration. It actually never was, but it didn't produce an error message before.

The problem is that two clients behind the same NAT that both use transport mode can't be distinguished in many situations. In the L2TP case both clients will try to install the same IPsec policy <public NAT IP>[udp/l2tp] === <server IP>[udp/l2tp].

In 5.1.0 updating policies, while they are still actively used by another connection, is prevented and now results in the error message you posted. In earlier releases the server simply updated the policy with the *reqid* of the second SA. But that just masked the issue as traffic to the first client was then sent to the second one, which is clearly not the intention.

If you can't change the client configuration, so that each client uses a distinct source port for L2TP (instead of 1701), your options are limited to implementing some kind of mapping on the server. Since each client probably gets its own NAT mapping on the NAT device (in your case 4500 and 1024) you might be able to NAT each to a separate virtual IP, or map those to a distinct policy by using XFRM marks (duplicate policies can be installed if their XFRM marks are different). Not sure about the details as I've never tried this.

Anyway, with Windows 7 clients your best option is to use IKEv2.

#2 - 25.07.2013 17:14 - Tobias Brunner

- Tracker changed from Issue to Bug

- Target version deleted (5.1.0)

#3 - 25.07.2013 17:14 - Tobias Brunner

- Tracker changed from Bug to Issue

#4 - 06.08.2013 18:21 - Pavel Kopchyk

Tobias, thanks for the explanation again.
So it is necessary to move forward (move to IKEv2).

#5 - 23.10.2014 23:53 - Alex Brew

So, what developers can say about it [[http://www.mail-archive.com/users@lists.strongswan.org/msg08057.html]] within this situation ?

#6 - 20.02.2015 17:08 - Martin Willi

- Tracker changed from Issue to Feature

- Category set to libcharon

- Status changed from Feedback to Closed

- Assignee changed from Tobias Brunner to Martin Willi

- Target version set to 5.3.0

- Resolution set to Fixed

I've just merged the new connmark plugin to the master branch. That plugin allows you install identical transport mode policies and use Netfilter conntrack marks to distinguish multiple connection flows. This can be used for L2TP sessions or any other traffic that conntrack can track. Refer to the provided test case for an example configuration.

#7 - 20.02.2015 17:48 - Martin Willi

Some additional plugin documentation is now available on the connmark wiki page.

#8 - 22.04.2015 11:47 - Tobias Brunner

- Related to Issue #712: Windows connect failed with error 809 added