strongSwan - Bug #597

Ikev1 Cisco unity problem with multiple subnets after rekey

21.05.2014 11:22 - kyle rhodes

Status:	Closed	**Start date:**	21.05.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.2.1		
Affected version:	5.1.2	**Resolution:**	Fixed

Description

Hi,

I am new to ipsec and strongswan and I am experiencing a problem after the ipsec SA is re-keyed.
The clients are running Strongswan V5.1.2 with the Cisco unity extension enabled, they are talking to a Cisco device.
We have 2 subnets configured, the tunnel is established fine and we able to access both machines at the other end, if the client end re-keys then both subnets are still accessible,
if the Cisco end re-keys then only the first subnet is accessible, this can be seen from the (edited) logs below.

ipsec.conf:

```
config setup
    cachecrls=no
    uniqueids=never

conn conn
    authby=xauthrsasig
    xauth=client
    xauth_identity=conn3
    leftcert=/path/to/cer/cer.cer
    left=%defaultroute
    leftid="CN=secret"
    leftsourceip=%config
    right=x.x.x.x
    rightid=abc.co.uk
    rightsubnet=a.a.a.a/32,b.b.b.b/32
    ike=---------------!
    esp=----------!
    auto=start
    keyingtries=%forever
    keyexchange=ikev1
    modeconfig=pull
    dpdaction=restart
    dpddelay=100s
    dpdtimeout=500s
    fragmentation=yes
    closeaction=restart
    ikelifetime=14400
    lifetime=7200
```

Both subnets are initially setup:

```
May 20 21:38:58 02[ENC] <conn|4> parsed QUICK_MODE response 1652122708 [ HASH SA No ID ID ]
May 20 21:38:58 02[IKE] <conn|4> CHILD_SA conn{1} established with SPIs c8f7cadd_i 9928ace5_o and
TS z.z.z.z/32 === a.a.a.a/32 b.b.b.b/32
```

If the server end rekeys, then only one subnet is setup:

```
May 20 23:20:58 04[IKE] <conn|4> detected rekeying of CHILD_SA conn{1}
May 20 23:20:58 04[ENC] <conn|4> generating QUICK_MODE response 2461818133 [ HASH SA No ID ID ]
May 20 23:20:58 04[NET] <conn|4> sending packet: from f.f.f.f[4500] to x.x.x.x[4500] (188 bytes)
May 20 23:20:59 11[NET] <conn|4> received packet: from x.x.x.x[4500] to f.f.f.f[4500] (76 bytes)
```

```
May 20 23:20:59 11[ENC] <conn|4> parsed QUICK_MODE request 2461818133 [ HASH ]
May 20 23:20:59 11[IKE] <conn|4> CHILD_SA conn{1} established with SPIs c3f19a93_i 686570c0_o and
TS dynamic === a.a.a.a/32
```

If the client end rekeys, then both subnets are setup:

```
May 21 08:18:33 12[KNL] creating rekey job for ESP CHILD_SA with SPI f8836e7c and reqid {1}
May 21 08:18:33 09[ENC] <conn|1> generating QUICK_MODE request 4101817566 [ HASH SA No ID ID ]
May 21 08:18:33 09[NET] <conn|1> sending packet: from f.f.f.f[4500] to x.x.x.x[4500] (172 bytes)
May 21 08:18:34 08[NET] <conn|1> received packet: from x.x.x.x[4500] to f.f.f.f[4500] (156 bytes)
May 21 08:18:34 08[ENC] <conn|1> parsed QUICK_MODE response 4101817566 [ HASH SA No ID ID ]
May 21 08:18:34 08[IKE] <conn|1> CHILD_SA conn{1} established with SPIs c8af0fc2_i fc1fd8e0_o and
TS z.z.z.z/32 === a.a.a.a/32 b.b.b.b/32
```

Any help would be greatly appreciated.

History

#1 - 17.07.2014 17:30 - Tobias Brunner

- File 0001-unity-Handle-narrowing-according-to-roles-in-the-IKE.patch added

- Tracker changed from Issue to Bug

- Description updated

- Category set to libcharon

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

- Priority changed from High to Normal

- Target version set to 5.2.1

The *unity* plugin modifies the traffic selectors that are exchanged during quick mode. As initiator it sets the remote traffic selector to 0.0.0.0/0 as responder it does the same for the local traffic selector. The IPsec policies that are installed are then based on the UNITY_SPLIT_INCLUDE attributes exchanged during ModeConfig.

For the client (same goes for the server, with local/remote reversed):

```
Sent to server:
  local: <virtual IP>
  remote: 0.0.0.0/0
Actually installed:
  local: <virtual IP>
  remote: <subnets received in split-include attributes>
```

The problem is that this replacement is currently based on the **Quick Mode initiator** flag, not the **IKE_SA initiator** flag. These are the same when the road-warrior connection is initially established (the client is the initiator of both the IKE_SA and the Quick Mode exchange), and also when the client initiates the CHILD_SA rekeying, but they are not when the server does so.

So when the client rekeys the CHILD_SA everything is basically the same as it was during the initial exchange. On the other hand, if the server initiates the rekeying the *unity* plugin assumes it acts as responder, so what it does is this: It replaces the local traffic selector with 0.0.0.0/0 (*dynamic* in the log) and uses only the first subnet of the remote traffic selector.

Could you please try if the attached patch fixes the issue. With it the *unity* plugin will strictly adhere to the role of a peer in the IKE_SA and not the one in the Quick Mode exchange.

#2 - 02.09.2014 11:06 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed

Applied with a45ba880c8. Another Unity fix by Martin was applied too (cfdc620a3f1a).

Files

0001-unity-Handle-narrowing-according-to-roles-in-the-IKE.patch	2.18 KB	17.07.2014	Tobias Brunner