strongSwan - Issue #2665

giving up after 5 retransmits

14.05.2018 15:54 - Alexis Rapior

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.6.1	**Resolution:**	No feedback

Description

Hi StrongSwan team,

I have a built an IKEv2 VPN tunnel between strongswan (running on google cloud) and a Cisco ASA 5515X device.
Everything looks good and traffic is going on through the tunnel.

From time to time I can see in the log that the connection went down after 5 retransmits.

What may cause the issue? Network problem? Problem on the ASA side?

How can I prevent this to happen and the most important point how can I make Strongswan reconnect automatically to my Cisco device?

ipsec.conf:

```
conn %default
        ikelifetime=36000s
        keylife=10800s
        rekeymargin=3m
        keyingtries=%forever
        keyexchange=ikev2
        authby=psk
        dpdaction=restart
        dpddelay=30

conn sub-1
        left=%any
        leftsubnet=10.0.1.0/24
        leftid=A.A.A.A
        leftfirewall=yes
        right=B.B.B.B
        rightsubnet=192.168.1.0/24
        rightid=%any
        auto=start
        ike=aes256-sha1-modp1024
        esp=aes256-sha1-modp1024
```

/var/log/messages:

```
May X 08:46:46 linux charon: 11[ENC] generating INFORMATIONAL response 4279 [ ]
May X 08:46:46 linux charon: 11[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (76 byt
es)
May X 08:47:02 linux charon: 10[NET] received packet: from B.B.B.B[4500] to 10.0.1.10[4500] (76 by
tes)
May X 08:47:02 linux charon: 10[ENC] parsed INFORMATIONAL request 4280 [ ]
May X 08:47:02 linux charon: 10[ENC] generating INFORMATIONAL response 4280 [ ]
May X 08:47:02 linux charon: 10[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (76 byt
es)
May X 08:47:04 linux charon: 16[NET] received packet: from B.B.B.B[4500] to 10.0.1.10[4500] (76 by
tes)
May X 08:47:04 linux charon: 16[ENC] parsed INFORMATIONAL request 4280 [ ]
May X 08:47:04 linux charon: 16[IKE] received retransmit of request with ID 4280, retransmitting r
esponse
```

```
May X 08:47:04 linux charon: 16[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (76 byt
es)
May X 08:47:06 linux charon: 05[NET] received packet: from B.B.B.B[4500] to 10.0.1.10[4500] (76 by
tes)
May X 08:47:06 linux charon: 05[ENC] parsed INFORMATIONAL request 4280 [ ]
May X 08:47:06 linux charon: 05[IKE] received retransmit of request with ID 4280, retransmitting r
esponse
May X 08:47:06 linux charon: 05[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (76 byt
es)
May X 08:47:08 linux charon: 14[NET] received packet: from B.B.B.B[4500] to 10.0.1.10[4500] (76 by
tes)
May X 08:47:08 linux charon: 14[ENC] parsed INFORMATIONAL request 4280 [ ]
May X 08:47:08 linux charon: 14[IKE] received retransmit of request with ID 4280, retransmitting r
esponse
May X 08:47:08 linux charon: 14[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (76 byt
es)
May X 08:48:30 linux charon: 07[IKE] sending keep alive to B.B.B.B[4500]
May X 08:48:50 linux charon: 15[IKE] sending keep alive to B.B.B.B[4500]
May X 08:49:10 linux charon: 16[IKE] sending keep alive to B.B.B.B[4500]
May X 08:49:30 linux charon: 10[IKE] sending keep alive to B.B.B.B[4500]
May X 08:49:50 linux charon: 16[IKE] sending keep alive to B.B.B.B[4500]
May X 08:50:10 linux charon: 14[IKE] sending keep alive to B.B.B.B[4500]
May X 08:50:25 linux charon: 08[KNL] creating rekey job for CHILD_SA ESP/0xba396706/B.B.B.B
May X 08:50:25 linux charon: 08[IKE] establishing CHILD_SA VIV-sub-1{1551} reqid 58
May X 08:50:25 linux charon: 08[ENC] generating CREATE_CHILD_SA request 128 [ N(REKEY_SA) SA No KE
 TSi TSr ]
May X 08:50:25 linux charon: 08[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (444 by
tes)
May X 08:50:29 linux charon: 09[IKE] retransmit 1 of request with message ID 128
May X 08:50:29 linux charon: 09[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (444 by
tes)
May X 08:50:36 linux charon: 12[IKE] retransmit 2 of request with message ID 128
May X 08:50:36 linux charon: 12[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (444 by
tes)
May X 08:50:49 linux charon: 07[IKE] retransmit 3 of request with message ID 128
May X 08:50:49 linux charon: 07[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (444 by
tes)
May X 08:51:09 linux charon: 16[IKE] sending keep alive to B.B.B.B[4500]
May X 08:51:13 linux charon: 05[IKE] retransmit 4 of request with message ID 128
May X 08:51:13 linux charon: 05[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (444 by
tes)
May X 08:51:13 linux charon: 14[KNL] creating rekey job for CHILD_SA ESP/0xc19536c8/10.0.1.10
May X 08:51:32 linux charon: 09[IKE] sending keep alive to B.B.B.B[4500]
May X 08:51:44 linux charon: 06[KNL] creating rekey job for CHILD_SA ESP/0xdaebef57/B.B.B.B
May X 08:51:48 linux charon: 11[KNL] creating rekey job for CHILD_SA ESP/0xc9d8622b/10.0.1.10
May X 08:51:52 linux charon: 15[IKE] sending keep alive to B.B.B.B[4500]
May X 08:51:54 linux charon: 10[KNL] creating rekey job for CHILD_SA ESP/0xccd47f2d/10.0.1.10
May X 08:51:55 linux charon: 05[IKE] retransmit 5 of request with message ID 128
May X 08:51:55 linux charon: 05[NET] sending packet: from 10.0.1.10[4500] to B.B.B.B[4500] (444 by
tes)
May X 08:52:14 linux charon: 13[IKE] sending keep alive to B.B.B.B[4500]
May X 08:52:29 linux charon: 09[KNL] creating rekey job for CHILD_SA ESP/0xe9481b29/B.B.B.B
May X 08:52:34 linux charon: 12[IKE] sending keep alive to B.B.B.B[4500]
May X 08:52:36 linux charon: 11[KNL] creating rekey job for CHILD_SA ESP/0x47080418/B.B.B.B
May X 08:52:54 linux charon: 15[IKE] sending keep alive to B.B.B.B[4500]
May X 08:53:01 linux charon: 16[KNL] creating rekey job for CHILD_SA ESP/0xc157e758/10.0.1.10
May X 08:53:10 linux charon: 14[KNL] creating delete job for CHILD_SA ESP/0xc15b5b53/10.0.1.10
May X 08:53:10 linux charon: 14[JOB] CHILD_SA ESP/0xc15b5b53/10.0.1.10 not found for delete
May X 08:53:10 linux charon: 13[IKE] v
May X 08:53:10 linux vpn: - B.B.B.B 192.168.1.0/24 == B.B.B.B -- 10.0.1.10 == 10.0.1.0/24
```

Thanks for your support,
Alexis

History

#1 - 14.05.2018 16:02 - Tobias Brunner

- Status changed from New to Feedback

- Priority changed from High to Normal

> From time to time I can see in the log that the connection went down after 5 retransmits.
>
> What may cause the issue? Network problem? Problem on the ASA side?

Either, both, no idea. Logs of the other end might help (to see if anything reaches it at that time). Maybe it already deleted the IKE_SA for some reason (failed IKE rekeying?).

> How can I prevent this to happen and the most important point how can I make Strongswan reconnect automatically to my Cisco device?

Until you find out what the problem is you can't really prevent it. But you should use *auto=route* and *dpdaction=clear* so the SA is automatically (re-)created when matching traffic occurs and no SA exists. You can also tune retransmission timeouts to e.g. close and recreate the SA earlier. *reauth=no* might also help (see ExpiryRekey).

#2 - 16.05.2018 10:58 - Alexis Rapior

Hi Tobias,

Thanks for the feedback. I changed the configuration accordingly, currently it looks fine.

Regards,
Alexis

#3 - 28.05.2018 08:56 - Alexis Rapior

Hi Tobias,

As stated in my last message everything was working fine until last week.

First I got a huge amount of keep alive sent to the Cisco gateway (almost 3000 times). This, I assume means that the remote gateway was not reachable correct?

```
charon: 14[IKE] sending keep alive to B.B.B.B[4500]
```

Secondly I got No such process messages, I assume that this pops up when traffic is detected and Strongwsan is trying to bring up the tunnel automatically, right? (8838 times in the logs)

```
charon: 08[KNL] creating delete job for CHILD_SA ESP/0xc9fc8038/A.A.A.A
charon: 15[KNL] creating delete job for CHILD_SA ESP/0x1817cd0d/B.B.B.B
charon: 05[KNL] querying SAD entry with SPI 1817cd0d failed: No such process (3)
```

The following system packages have also been updated automatically the same day, not sure if it can be related?

```
Updated: nspr.x86_64
Updated: nss-util.x86_64
Updated: libgcc.x86_64
Updated: libcom_err.x86_64
Updated: net-snmp-libs.x86_64
Updated: net-snmp-agent-libs.x86_64
Updated: net-snmp.x86_64
Updated: libss.x86_64
Updated: e2fsprogs-libs.x86_64
Updated: nss-softokn-freebl.x86_64
Updated: nss-softokn.x86_64
Updated: nss-sysinit.x86_64
Updated: nss.x86_64
Updated: NetworkManager-libnm.x86_64
Updated: NetworkManager.x86_64
Updated: nss-tools.x86_64
Updated: iptables.x86_64
Updated: iptables-services.x86_64
Updated: openldap.x86_64
Updated: NetworkManager-team.x86_64
Updated: NetworkManager-wifi.x86_64
Updated: NetworkManager-ppp.x86_64
Updated: NetworkManager-tui.x86_64
```

```
Updated: e2fsprogs.x86_64
Updated: net-snmp-devel.x86_64
Updated: net-snmp-utils.x86_64
Updated: libcom_err-devel.x86_64
Updated: rsyslog.x86_64
Updated: libstdc++.x86_64
Updated: ca-certificates.noarch
Updated: centos-release.x86_64
Updated: libgomp.x86_64
Updated: rdma-core.x86_64
Updated: libgcc.i686
Updated: libstdc++.i686
Updated: nss-softokn-freebl.i686
Updated: rdma-core.i686
```

The only solution to fix the issue was to restart the Strongswan service.

Regards,
Alexis

#4 - 28.05.2018 10:02 - Tobias Brunner

> First I got a huge amount of keep alive sent to the Cisco gateway (almost 3000 times). This, I assume means that the remote gateway was not reachable correct?

No, these keepalive packets are sent by the peer behind a NAT if there is no other outbound traffic (that would keep the NAT mappings alive). That means there is either no traffic at that time or there were no IPsec SAs at all (but with *auto=route* they should get created again if that's the case).

> Secondly I got No such process messages, I assume that this pops up when traffic is detected and Strongwsan is trying to bring up the tunnel automatically, right?

Looks more like these SAs expired (i.e. they were not rekeyed before they expired). There will be an attempt to retrieve usage stats when logging about deleted SAs, which fails if they expired (when the kernel notifies the daemon about this it already removed the SAs). That might indicate unsuitable rekeying settings.

> The following system packages have also been updated automatically the same day, not sure if it can be related?

Well, some are related to networking. But you should still focus on the actual problem (i.e. why is it not possible to reach the peer at some point, or why do the SAs get out of sync, or whatever actually the problem is).

#5 - 05.06.2018 14:35 - Alexis Rapior

Hi Tobias,

Since the last time I've setup a monitoring script which performs a basic ping on the public IP of the Cisco remote device and this every 30 seconds. Today I noticed that the remote device went down (during less than 1,5 minute) and produced the same errors as my previous post.

Can it be a solution to restart the strongswan service each time my monitoring script detects that the remote device is not reachable? I've the feeling that it's to brutal...

Regards,
Alexis

#6 - 05.06.2018 14:45 - Tobias Brunner

> Can it be a solution to restart the strongswan service each time my monitoring script detects that the remote device is not reachable? I've the feeling that it's to brutal...

It is brutal, use DPDs (*dpdaction=clear*) and *auto=route* instead. Then the SA is created automatically again if traffic matches the policy (e.g. your ping) and the other end is up again. If you feel it takes too long to recreate the connection, you might want to adjust the retransmission settings so the old SA is destroyed more quickly if the peer is not reachable.

#7 - 05.06.2018 15:52 - Alexis Rapior

> use DPDs (*dpdaction=clear*) and *auto=route* instead.

It's already in place.

The ping I perform is reaching the public IP of the peer and therefore will not match the policy.

> adjust the retransmission settings so the old SA is destroyed more quickly if the peer is not reachable.

which one? reduce the number of retries? I'm not sure to really understand.

#8 - 05.06.2018 16:22 - Tobias Brunner

> The ping I perform is reaching the public IP of the peer and therefore will not match the policy.

What's the ping for then? DPDs will have the same effect (i.e. check connectivity outside the tunnel) if you configure them. A ping is only necessary to check connectivity inside the tunnel (but then you'd have to terminate the connection and trigger it again to recover if it doesn't work anymore, but you might not want to do that just because a single ping failed).

> > adjust the retransmission settings so the old SA is destroyed more quickly if the peer is not reachable.
>
> which one? reduce the number of retries? I'm not sure to really understand.

You have to decide yourself, see the formula (you can send less of them, or send them in quicker succession, or differently distributed over time).

#9 - 05.06.2018 17:35 - Alexis Rapior

It seems that a process blocks all the other, please see below (IKE_DPD)

Tail of strongswan statusall when the failure happens:

```
...
Security Associations (1 up, 0 connecting):
   sub-1[27]: ESTABLISHED 8 hours ago, 10.0.1.10[A.A.A.A]...B.B.B.B[B.B.B.B]
   sub-1[27]: IKEv2 SPIs: a2539a0e2e934291_i* a06185fc164f9d20_r, rekeying in 87 minutes
   sub-1[27]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
   sub-1[27]: Tasks queued: CHILD_REKEY CHILD_REKEY CHILD_DELETE CHILD_DELETE CHILD_REKEY CHILD_REKEY CHILD_RE
KEY CHILD_REKEY CHILD_REKEY CHILD_REKEY CHILD_REKEY CHILD_REKEY CHILD_REKEY CHILD_REKEY CHILD_DELETE CHILD_DEL
ETE CHILD_REKEY CHILD_REKEY CHILD_REKEY CHILD_REKEY CHILD_DELETE CHILD_DELETE CHILD_DELETE CHILD_DELETE CHILD_
REKEY CHILD_REKEY CHILD_DELETE CHILD_DELETE CHILD_REKEY CHILD_REKEY CHILD_REKEY CHILD_REKEY CHILD_DELETE CHILD
_DELETE CHILD_DELETE CHILD_DELETE CHILD_REKEY CHILD_DELETE CHILD_DELETE CHILD_REKEY CHILD_DELETE CHILD_DELETE
CHILD_DELETE CHILD_DELETE CHILD_DELETE CHILD_DELETE CHILD_DELETE CHILD_DELETE CHILD_REKEY CHILD_REKEY CHILD_DE
LETE CHILD_DELETE CHILD_REKEY CHILD_REKEY CHILD_DELETE CHILD_DELETE
   sub-1[27]: Tasks active: IKE_DPD
   sub-2{986}:  INSTALLED, TUNNEL, reqid 2, ESP in UDP SPIs: cd7e95a8_i db487a55_o
   sub-2{986}:  AES_CBC_256/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying active
   sub-2{986}:   10.0.1.0/24 === 192.168.2.0/24
   sub-3{987}:  INSTALLED, TUNNEL, reqid 3, ESP in UDP SPIs: c9a97895_i 6a9600de_o
   sub-3{987}:  AES_CBC_256/HMAC_SHA1_96/MODP_1024, 254724 bytes_i (1823 pkts, 26242s ago), 223274 bytes_o (16
38 pkts, 26242s ago), rekeying active
   sub-3{987}:   10.0.1.0/24 === 192.168.3.0/24
   sub-6{988}:  INSTALLED, TUNNEL, reqid 6, ESP in UDP SPIs: cf788330_i b006f9ff_o
   sub-6{988}:  AES_CBC_256/HMAC_SHA1_96/MODP_1024, 0 bytes_i, 0 bytes_o, rekeying active
   sub-6{988}:   10.0.1.0/24 === 192.168.13.0/24
...
```

So even if the DPD option is setup it hang at a certain point of time because the remote peer was not reachable?

So that's why I got a huge amount of:

```
...
charon:0[KNL] querying SAD entry with SPI db487a55 failed: No such process (3)
charon: 10[KNL] querying SAD entry with SPI b006f9ff failed: No such process (3)
charon: 10[KNL] querying SAD entry with SPI d1ba3ba0 failed: No such process (3)
charon: 10[KNL] querying SAD entry with SPI bc7c3eef failed: No such process (3)
charon: 10[KNL] querying SAD entry with SPI 136497bf failed: No such process (3)
charon: 10[KNL] querying SAD entry with SPI 1544693e failed: No such process (3)
charon: 10[KNL] querying SAD entry with SPI 07f0e7b0 failed: No such process (3)
charon: 10[KNL] querying SAD entry with SPI 0ad445aa failed: No such process (3)
charon: 10[KNL] querying SAD entry with SPI 8f604f48 failed: No such process (3)
```

```
charon: 10[KNL] querying SAD entry with SPI 6d30622b failed: No such process (3)
charon: 10[KNL] querying SAD entry with SPI e5f46973 failed: No such process (3)
...
```

I'm stucked and I'm not sure that it comes from the retransmission.

#10 - 05.06.2018 19:24 - Tobias Brunner

That looks completely wrong. Why are there so many CHILD_SA rekeyings/deletions? Did you mess up the lifetime configs? Or does your peer do some really strange stuff? Read the log for details on what's going on.

#11 - 06.06.2018 09:13 - Alexis Rapior

Hi,

I've 15 tunnels established with the SA so i think it's correct.

```
conn sub-1
        left=%any
        leftsubnet=10.0.1.0/24
        leftid=A.A.A.A
        leftfirewall=yes
        right=B.B.B.B
        rightsubnet=192.168.1.0/24
        rightid=%any
        auto=route
        ike=aes256-sha1-modp1024
        esp=aes256-sha1-modp1024

conn sub-2
        also=sub-1
        rightsubnet=192.168.2.0/24

conn sub-3
        also=sub-1
        rightsubnet=192.168.3.0/24

conn sub-4
        also=sub-1
        rightsubnet=192.168.11.0/24

conn sub-5
        also=sub-1
        rightsubnet=192.168.12.0/24

conn sub-6
        also=sub-1
        rightsubnet=192.168.13.0/24

conn sub-7
        also=sub-1
        rightsubnet=192.168.14.0/24

conn sub-8
        also=sub-1
        rightsubnet=192.168.21.0/24

conn sub-9
        also=sub-1
        rightsubnet=192.168.23.0/24

conn sub-10
        also=sub-1
        rightsubnet=192.168.37.0/24

conn sub-11
        also=sub-1
        rightsubnet=192.168.100.0/24

conn sub-12
        also=sub-1
        rightsubnet=172.16.196.0/23

conn sub-13
        also=sub-1
```

```
        rightsubnet=192.168.200.0/23

conn sub-14
        also=sub-1
        rightsubnet=172.16.202.0/24

conn sub-15
        also=sub-1
        rightsubnet=192.168.4.0/24
```

#12 - 06.06.2018 10:18 - Tobias Brunner

> I've 15 tunnels established with the SA so i think it's correct.

I see.

#13 - 06.06.2018 10:23 - Alexis Rapior

OK, so no further suggestion to fix my issues?

#14 - 06.06.2018 10:36 - Tobias Brunner

> OK, so no further suggestion to fix my issues?

What's the issue? If there is no connectivity, DPDs will obviously have to be retransmitted and will block other tasks (which woulnd't be successful anyway, but any one of them acts as DPD too). So time the DPDs right (see the link in my first comment) and also with the lifetimes of your SAs (other link in a comment above) so that the SAs are re-created again when traffic matches the installed policies.

#15 - 06.06.2018 11:37 - Alexis Rapior

The issue is that the remote peer came back (ping successful in my monitoring) and even if traffic was initiated in one of the 15 tunnels, strongswan was blocked because of

```
sub-1[27]: Tasks active: IKE_DPD
```

Only restarting the service solved the situation.

#16 - 06.06.2018 11:44 - Tobias Brunner

> The issue is that the remote peer came back (ping successful in my monitoring) and even if traffic was initiated in one of the 15 tunnels, strongswan was blocked because of
> [...]
> Only restarting the service solved the situation.

Obviously, the daemon has to conclude that the peer is dead first (i.e. the message has to be retransmitted a number of times without a response), how long that takes depends on your settings (the default is 165 seconds). Adjust these settings if you feel it takes too long.

#17 - 06.06.2018 13:57 - Alexis Rapior

Thanks for your help.

I changed retransmit_tries = 5 to retransmit_tries = 1.
This means that if the remote peer is not answering (down or not reachable) the SA will be cleared (because of dpdaction=clear) after one retransmit (4 seconds by default).
If some traffic is detected afterwards the SA will be created automatically (because of auto=route).

Am I correct?

#18 - 06.06.2018 14:46 - Tobias Brunner

> This means that if the remote peer is not answering (down or not reachable) the SA will be cleared (because of dpdaction=clear) after one retransmit (4 seconds by default).

Yes, but it's only closed 7 seconds later (it waits for an answer first).

> If some traffic is detected afterwards the SA will be created automatically (because of auto=route).
>
> Am I correct?

Yes, correct.

#19 - 07.06.2018 10:56 - Alexis Rapior

Hi,

with auto=route, the connection is not started if the traffic is initiated from the right subnet.

I've now changed auto=start, dpdaction=hold and reauth=yes.

#20 - 07.06.2018 11:00 - Tobias Brunner

> with auto=route, the connection is not started if the traffic is initiated from the right subnet.

Obviously, the other peer has to initiate the connection if the traffic is initiated there (so it has to be configured similarly).

> I've now changed auto=start, dpdaction=hold and reauth=yes.

Set *reauth=no* if you use trap policies (which you do with *dpdaction=hold* after the connection broke down once, but you'll have the same issue again if the other peer does not reinitiate the connection when it needs to sent traffic to you), or configure make-before-break reauthentication (if the peer supports it).

#21 - 07.06.2018 12:11 - Alexis Rapior

Then how to make sure that the connection is initiated again when the peer is up again?
dpdaction=restart and retransmit_tries to 100 or something like this?

#22 - 07.06.2018 12:27 - Tobias Brunner

> Then how to make sure that the connection is initiated again when the peer is up again?

Let the other peer initiate the connection when ready and it's necessary.

> dpdaction=restart and retransmit_tries to 100 or something like this?

You can try (no need to set *retransmit_tries* that high, due to the exponential back-off you'd have to also define *retransmit_limit*, just use *keyingtries=%forever*).

#23 - 07.06.2018 14:06 - Alexis Rapior

ok, so if I set dpdaction=restart, retransmit_tries=5 and keyingtries=%forever means that if the remote peer is down after retransmit has reached the limit (5), strongswan will restart the connection endlessly until the peer is up again because of keyingtries=%forever?

#24 - 26.06.2018 08:31 - Alexis Rapior

- File Remote Desktop Connection.png added

Hi Tobias,

With the last settings, the connection seems to me more reliable.
However I have observed that sometimes I have multiple CHILD SA established to the same subnet (attached screenshot).
I don't know why and how I can prevent it?

Thanks,
Alexis

#25 - 26.06.2018 10:04 - Tobias Brunner

> However I have observed that sometimes I have multiple CHILD SA established to the same subnet (attached screenshot).
> I don't know why and how I can prevent it?

You'd need to determine how they were created. If the reason is that both ends created the SA concurrently and no duplicate was detected you can't really do anything about it (unless you write your own plugin/script that checks for this and deletes one of the SAs).

#26 - 11.01.2019 23:28 - Noel Kuntze

- Status changed from Feedback to Closed

- Resolution set to No feedback

Files

Remote Desktop Connection.png	153 KB	26.06.2018	Alexis Rapior