strongSwan - Bug #2573

updown script is not called if IKEv1 IKE_SA rekey/reauthentication fails due to retransmits

01.03.2018 15:40 - Marco Berizzi

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	ikev1		
Target version:	5.6.3		
Affected version:	5.6.1	**Resolution:**	Fixed

Description

Hello everyone,

I'm running strongswan 5.6.1 on slackware linux
64 bit. I have found a problem with my setup.
The down_client section in the updown script is
not executed when the IKE_SA is dropped. Here is
my config setup:

```
conn rw-mobile
        right=%any
        compress=yes
        leftupdown=/etc/ipsec.d/updown/_updown.strongswan.X11
        keylife=10h
        ikelifetime=12h
        rekey=yes
        keyingtries=1
        ike=aes128-sha1-modp1024,aes128-sha1-modp2048,aes256-sha384-ecp384
        esp=aes128-sha1-modp1024,aes128-sha1-modp2048,aes256-sha256-ecp384
        rightsubnet=10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,100.64.0.0/10

conn rw-mobile-10.180.0.0_internal
        also=rw-mobile
        auto=add
        leftsubnet=10.180.0.0/16
        left=10.81.110.254

conn rw-mobile-10.177.0.0_internal
        also=rw-mobile
        auto=add
        leftsubnet=10.177.0.0/16
        left=10.81.110.254
```

Here is the relevant log when the IKE_SA is dropped:

```
Jan 26 21:38:14 Pleiadi charon: 08[IKE] initiator did not reauthenticate as requested
Jan 26 21:38:14 Pleiadi charon: 08[IKE] reauthenticating IKE_SA rw-mobile-10.180.0.0_internal[17]
actively
Jan 26 21:38:14 Pleiadi charon: 08[IKE] initiating Main Mode IKE_SA rw-mobile-10.180.0.0_internal[
94] to 10.81.126.175
Jan 26 21:38:14 Pleiadi charon: 08[ENC] generating ID_PROT request 0 [ SA V V V V V ]
Jan 26 21:38:14 Pleiadi charon: 08[NET] sending packet: from 10.81.110.254[500] to 10.81.126.175[5
00] (312 bytes)
Jan 26 21:38:18 Pleiadi charon: 15[IKE] sending retransmit 1 of request message ID 0, seq 1
Jan 26 21:38:18 Pleiadi charon: 15[NET] sending packet: from 10.81.110.254[500] to 10.81.126.175[5
00] (312 bytes)
Jan 26 21:38:25 Pleiadi charon: 12[IKE] sending retransmit 2 of request message ID 0, seq 1
Jan 26 21:38:25 Pleiadi charon: 12[NET] sending packet: from 10.81.110.254[500] to 10.81.126.175[5
00] (312 bytes)
Jan 26 21:38:38 Pleiadi charon: 13[IKE] sending retransmit 3 of request message ID 0, seq 1
Jan 26 21:38:38 Pleiadi charon: 13[NET] sending packet: from 10.81.110.254[500] to 10.81.126.175[5
00] (312 bytes)
```

```
[...]
Jan 26 21:47:14 Pleiadi charon: 13[IKE] deleting IKE_SA rw-mobile-10.180.0.0_internal[17] between
10.81.110.254[CN=strongSwan Gateway]...10.81.126.175[CN=Maddalena]
Jan 26 21:47:14 Pleiadi charon: 13[IKE] sending DELETE for IKE_SA rw-mobile-10.180.0.0_internal[17
]
Jan 26 21:47:14 Pleiadi charon: 13[ENC] generating INFORMATIONAL_V1 request 1418042332 [ HASH D ]
Jan 26 21:47:14 Pleiadi charon: 13[NET] sending packet: from 10.81.110.254[500] to 10.81.126.175[5
00] (92 bytes)
```

As you may see the user CHILD_SA are not dropped
because strongswan is not logging the '-' at Jan 26 21:47:14
Only the IKE_SA is dropped.

```
Jan 26 17:57:45 Pleiadi vpn: + CN=Maddalena 10.81.126.175 -- 10.81.110.254 == 10.180.0.0/16
Jan 26 17:58:08 Pleiadi vpn: + CN=Maddalena 10.81.126.175 -- 10.81.110.254 == 10.177.0.0/16
Jan 29 08:59:30 Pleiadi vpn: + CN=Maddalena 10.81.126.175 -- 10.81.110.254 == 10.180.0.0/16
Jan 29 09:09:34 Pleiadi vpn: + CN=Maddalena 10.81.126.175 -- 10.81.110.254 == 10.177.0.0/16
Jan 29 09:15:20 Pleiadi vpn: - CN=Maddalena 10.81.126.175 -- 10.81.110.254 == 10.177.0.0/16
Jan 29 09:18:21 Pleiadi vpn: + CN=Maddalena 10.81.126.175 -- 10.81.110.254 == 10.177.0.0/16
Jan 29 09:23:55 Pleiadi vpn: - CN=Maddalena 10.81.126.175 -- 10.81.110.254 == 10.177.0.0/16
Jan 29 09:58:09 Pleiadi vpn: + CN=Maddalena 10.81.126.175 -- 10.81.110.254 == 10.177.0.0/16
```

Is the the expected behaviour? or a bug?

Associated revisions

Revision ce0a770c - 12.04.2018 15:19 - Tobias Brunner

Merge branch 'ikev1-down-reauth'

This triggers child_updown() if IKEv1 reauthentication fails due to
retransmits. The SA is also tried to be reestablished.

Fixes #2573.

History

#1 - 01.03.2018 18:06 - Tobias Brunner

- Description updated

- Category set to ikev1

- Status changed from New to Feedback

IKEv1 is a legacy protocol, which has severe limitations. You should consider using IKEv2, in particular with mobile roadwarriors.

This issue here seems to be related to the fact that the server tries to rekey the IKE_SA. It is apparently not able to reach the client, so the new SA is eventually deleted (your log is incomplete, so that's just a guess) and the old SA probably expires (also not seen in the log). Does this happen a lot? If so, you might want to investigate why.

Anyway, the old SA has no CHILD_SAs assigned anymore (these were adopted by the new IKE_SA) so the updown script won't be called when it is deleted. And the other IKE_SA is in state CONNECTING, which means that no ike_updown() and no child_updown() events are triggered at all. I pushed a possible fix to the *2573-ikev1-down-reauth* branch. Let me know if that works for you.

#2 - 02.03.2018 10:40 - Marco Berizzi

- File jan26 added

Tobias Brunner wrote:

> IKEv1 is a legacy protocol, which has severe limitations. You should consider using IKEv2, in particular with mobile roadwarriors.

yes indeed but windows 10 doesn't support ikev2 in tunnel mode. I'm going to open a ticket with Micro$oft

> This issue here seems to be related to the fact that the server tries to rekey the IKE_SA. It is apparently not able to reach the client

yes indeed the mobile has gone away

> so the new SA is eventually deleted (your log is incomplete, so that's just a guess)

attached the full log for Jan 26
Let me know if you need the log for other dates

> Does this happen a lot?

there is about 15 mobile users around this configuration/strongswan ipsec gateway. I'm able to observe this problem after less than a week.

> Anyway, the old SA has no CHILD_SAs assigned anymore (these were adopted by the new IKE_SA) so the updown script won't be called when it is deleted. And the other IKE_SA is in state CONNECTING, which means that no ike_updown() and no child_updown() events are triggered at all. I pushed a possible fix to the *2573-ikev1-down-reauth* branch. Let me know if that works for you.

I will apply your patch next Wednesday because I'm out of office (I have already applied & compiled). I keep you informed.

Let me know if you need any other information.

Thanks a lot Tobias for quick response and for the fix

#3 - 02.03.2018 17:05 - Tobias Brunner

> IKEv1 is a legacy protocol, which has severe limitations. You should consider using IKEv2, in particular with mobile roadwarriors.

> yes indeed but windows 10 doesn't support ikev2 in tunnel mode. I'm going to open a ticket with Micro$oft

What do you mean? Tunnel mode is the only mode the agile VPN client supports.

#4 - 08.03.2018 15:45 - Marco Berizzi

Hi Tobias,

yesterday at 13:00 CET I have applied your patch to strongswan 5.6.2
For now I don't see any problem, but I would like to wait till next week.

PS: I hope it will not hurt you, as this is off-topic. About windows 10. I'm not using the agile vpn client.
I'm running this command from the powershell:

New-NetIPSecRule -DisplayName "10.180.0.0/16 - ChildSA" -KeyModule IKEv1 -Phase1AuthSet (Get-NetIPsecPhase1AuthSet -DisplayName "strongwan.public.ip.address - Phase 1 Auth Set").name -Mode Tunnel -LocalAddress 192.168.59.98 -RemoteAddress 10.180.0.0/16 -LocalTunnelEndpoint 192.168.59.98 -RemoteTunnelEndpoint strongwan.public.ip.address -InboundSecurity Require -OutboundSecurity Require -Enabled true -QuickModeCryptoSet (Get-NetIPsecQuickModeCryptoSet -DisplayName "strongwan.public.ip.address - Phase 2 Crypto set").name

and I get this output (command completed successfully):

```
Caption                 :
Description             :
ElementName             : 10.180.0.0/16 - ChildSA
InstanceID              : {9229d3c5-c19f-4ab9-b24f-b3c3a90a02fc}
CommonName              :
PolicyKeywords          :
Enabled                 : True
PolicyDecisionStrategy  : 2
PolicyRoles             :
ConditionListType       : 3
CreationClassName       : MSFT|FW|ConSecRule|{9229d3c5-c19f-4ab9-b24f-b3c3a90a02fc}
ExecutionStrategy       : 2
Mandatory               :
PolicyRuleName          :
Priority                :
RuleUsage               :
SequencedActions        : 3
SystemCreationClassName :
SystemName              :
LimitNegotiation        :
DisplayGroup            :
DisplayName             : 10.180.0.0/16 - ChildSA
EnforcementStatus       : NotApplicable
MainModeCryptoSet       : {E5A5D32A-4BCE-4e4d-B07F-4AB1BA7E5FE1}
Phase1AuthSet           : {92b5f37e-7426-4d85-abf6-4ad26f5cc019}
Phase2AuthSet           : Default
```

Platforms : {}
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
PrimaryStatus : OK
Profiles : 0
QuickModeCryptoSet : {0b7c545c-bfa3-4da0-8aed-bc1014232e0e}
RuleGroup :
Status : The rule was parsed successfully from the store. (65536)
StatusCode : 65536
AllowSetKey : False
AllowWatchKey : False
BypassTunnelIfEncrypted : False
InboundSecurity : Require
KeyModule : IKEv1
LocalTunnelEndpoint : {192.168.59.98}
Machines :
MaxReturnPathLifetimeSeconds : 0
Mode : Tunnel
OutboundSecurity : Require
RemoteTunnelEndpoint : {strongwan.public.ip.address}
RemoteTunnelEndpointDNSName :
RequireAuthorization : False
Users :
PSComputerName :
IPsecRuleName : {9229d3c5-c19f-4ab9-b24f-b3c3a90a02fc}
ID : {9229d3c5-c19f-4ab9-b24f-b3c3a90a02fc}
Name : {9229d3c5-c19f-4ab9-b24f-b3c3a90a02fc}
Group :
Profile : Any
Platform : {}
SecIn : Require
SecOut : Require
RemoteTunnelHostname :
ForwardPathLifetime : 0
EncryptedTunnelBypass : False
User : Any
Machine : Any

But if I try to change the -KeyModule to IKEv2 I get this error:

New-NetIPSecRule -DisplayName "10.190.0.0/16 - ChildSA" -KeyModule IKEv2 -Phase1AuthSet (Get-NetIPsecPhase1AuthSet -DisplayName "strongwan.public.ip.address - Phase 1 Auth Set").name -Mode Tunnel -LocalAddress 192.168.59.98 -RemoteAddress 10.190.0.0/16 -LocalTunnelEndpoint 192.168.59.98 -RemoteTunnelEndpoint strongwan.public.ip.address -InboundSecurity Require -OutboundSecurity Require -Enabled true -QuickModeCryptoSet (Get-NetIPsecQuickModeCryptoSet -DisplayName "strongwan.public.ip.address - Phase 2 Crypto set").name

+ New-NetIPSecRule -DisplayName "10.190.0.0/16 - ChildSA" -KeyModule IK ...
+ ~~~~~~
+ CategoryInfo : InvalidArgument: (MSFT_NetConSecRule:root/standardcimv2/MSFT_NetConSecRule) [New-NetIPsecRule], CimExc
eption
+ FullyQualifiedErrorId : HRESULT 0x80070057,New-NetIPsecRule

#5 - 08.03.2018 18:48 - Tobias Brunner

> yesterday at 13:00 CET I have applied your patch to strongswan 5.6.2
> For now I don't see any problem, but I would like to wait till next week.

OK, let me know.

> About windows 10. I'm not using the agile vpn client.

Is there a particular reason you don't use that client? (Can also be configured via PowerShell cmdlet.)

> But if I try to change the -KeyModule to IKEv2 I get this error:
>
> New-NetIPSecRule -DisplayName "10.190.0.0/16 - ChildSA" -KeyModule IKEv2 -Phase1AuthSet (Get-NetIPsecPhase1AuthSet -DisplayName "strongwan.public.ip.address - Phase 1 Auth Set").name -Mode Tunnel -LocalAddress 192.168.59.98 -RemoteAddress 10.190.0.0/16 -LocalTunnelEndpoint 192.168.59.98 -RemoteTunnelEndpoint strongwan.public.ip.address -InboundSecurity Require -OutboundSecurity Require -Enabled true -QuickModeCryptoSet (Get-NetIPsecQuickModeCryptoSet -DisplayName "strongwan.public.ip.address - Phase 2 Crypto set").name
>
> + New-NetIPSecRule -DisplayName "10.190.0.0/16 - ChildSA" -KeyModule IK ...

+ ~~~~~~
+ CategoryInfo : InvalidArgument: (MSFT_NetConSecRule:root/standardcimv2/MSFT_NetConSecRule) [New-NetIPsecRule], CimExc eption
+ FullyQualifiedErrorId : HRESULT 0x80070057,New-NetIPsecRule

No idea. Maybe some of the options are not compatible with IKEv2 (e.g. regarding the authentication) or this really is a limitation of this interface/implementation.

#6 - 09.03.2018 10:26 - Marco Berizzi

Hi Tobias,

a quick update.
There seems to be a little harmless cosmetic glitch.

Take a look:

Mar 8 01:02:28 Pleiadi charon: 07[IKE] initiator did not reauthenticate as requested
Mar 8 01:02:28 Pleiadi charon: 07[IKE] reauthenticating IKE_SA rw-mobile-10.180.0.0[7] actively
Mar 8 01:02:28 Pleiadi charon: 07[IKE] initiating Main Mode IKE_SA rw-mobile-10.180.0.0[286] to 88.213.227.248
Mar 8 01:02:28 Pleiadi charon: 07[ENC] generating ID_PROT request 0 [SA V V V V V]
Mar 8 01:02:28 Pleiadi charon: 07[NET] sending packet: from strongswan.public.ip.address[4500] to 88.213.227.248[4500] (312 bytes)
Mar 8 01:02:28 Pleiadi charon: 11[NET] received packet: from 88.213.227.248[4500] to strongswan.public.ip.address[4500] (102 bytes)
Mar 8 01:02:28 Pleiadi charon: 11[ENC] parsed INFORMATIONAL_V1 request 773520122 [N(NO_PROP)]
Mar 8 01:02:28 Pleiadi charon: 11[IKE] received NO_PROPOSAL_CHOSEN error notify
Mar 8 01:02:28 Pleiadi vpn: - 0x0p+0ny 10.0.1.68/32 88.213.227.248 -- strongswan.public.ip.address 10.180.0.0/16

syslog is logging 0x0p+0ny instead of the PLUTO_PEER_ID:

CN=Carmine 10.0.1.68/32 88.213.227.248 -- strongswan.public.ip.address 10.180.0.0/16

#7 - 09.03.2018 17:25 - Tobias Brunner

> syslog is logging 0x0p+0ny instead of the PLUTO_PEER_ID:
>
> CN=Carmine 10.0.1.68/32 88.213.227.248 -- strongswan.public.ip.address 10.180.0.0/16

Yeah, the problem is that the IKE_SA, from which some of the information passed to the updown script comes, has not yet been established, so there is, for instance, no remote identity yet. That is, it is set to ID_ANY, which, when printed as string, results in %any.

Now, there is this funny printf call in the updown script (source:src/_updown/_updown.in#L220, the comment above it says something about octal escape sequences, ¯_(□)_/¯) that will try to evaluate the %a specifier. Depending on the source of printf (shell, coreutils) that might result in an error (because %a is not supported), or, as seen here, the evaluation of an argument as double value that's printed in hex. printf will assume 0 for missing arguments, which is why you see 0x0p+0 followed by the rest of the identity string i.e. ny.

I guess we could just remove these printf calls (they were added in bb7b613b83 as a replacement for echo -e $PLUTO_PEER_ID calls, but why escape sequences in these identities were evaluated in the first place I don't know). Alternatively, we could perhaps use something like printf "%b" "$PLUTO_PEER_ID", which according to the man pages should evaluate escape sequences in the passed string, but, since the string is passed as argument, leave % sequences alone. However, I don't know how portable %b is (at least the versions in bash, coreutils and FreeBSD support it).

#8 - 12.03.2018 10:07 - Marco Berizzi

Tobias Brunner wrote:

> Is there a particular reason you don't use that client? (Can also be configured via PowerShell cmdlet.)

I don't know if the agile can be used when there is another vpn client (cisco any connect for example) already active.

Tobias,

This morning I got this:

Mar 9 20:10:46 Pleiadi vpn: - 0x0p+0ny 192.168.1.106/32 151.49.89.60 -- strongswan.public.ip.address 10.180.0.0/16
Mar 11 04:45:13 Pleiadi vpn: - 0x0p+0ny 10.31.173.2/32 193.57.249.10 -- strongswan.public.ip.address 10.180.0.0/16
Mar 12 09:06:03 Pleiadi vpn: - 0x0p+0ny 10.10.10.155/32 95.244.61.54 -- strongswan.public.ip.address 10.180.0.0/16

this is the evidence that your patch is working.

You can close this bug.

Thanks a lot for the quick support.

PS: will it be included in 5.6.3?

#9 - 12.03.2018 10:25 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from child_sa not dropped when the ike_sa are deleted to updown script is not called if IKEv1 IKE_SA rekey/reauthentication fails due to retransmits

- Assignee set to Tobias Brunner

- Target version set to 5.6.3

> Is there a particular reason you don't use that client? (Can also be configured via PowerShell cmdlet.)

> I don't know if the agile can be used when there is another vpn client (cisco any connect for example) already active.

No idea. But since e.g. the Cisco client is pretty invasive (i.e. tries to block other traffic) it might not work.

> PS: will it be included in 5.6.3?

Yes.

#10 - 12.04.2018 15:24 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed

Files

jan26	1.11 MB	02.03.2018	Marco Berizzi