strongSwan - Issue #3669

Failed connection to IKE_SA (Checkpoint Server)

07.01.2021 19:05 - Andrea Mastellone

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	ikev1		
Affected version:	5.9.0	**Resolution:**	

Description

Hi,
I would like to VPN connect from my linux box to company server running Checkpoint server. I have got my private certificate and public server one, and I configured strongswan as suggested by the link
[[https://community.checkpoint.com/t5/Remote-Access-VPN/C2S-strongSwan-Roadwarrior-and-R80-30-working/td-p/67619]]
My PC is on a local net behind a router, and the company server is on a pubblic IP. I have configured the file ipsec.conf as attached.
When I launch command stronsgwan up cira, connection is not established with the following messages:

```
[root@andymema strongswan] # strongswan up cira
initiating Main Mode IKE_SA cira[1] to 156.14.252.1
generating ID_PROT request 0 [ SA V V V V V ]
sending packet: from 192.168.178.28[500] to 156.14.252.1[500] (240 bytes)
received packet: from 156.14.252.1[500] to 192.168.178.28[500] (124 bytes)
parsed ID_PROT response 0 [ SA V V ]
received FRAGMENTATION vendor ID
received NAT-T (RFC 3947) vendor ID
selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
sending packet: from 192.168.178.28[500] to 156.14.252.1[500] (244 bytes)
received packet: from 156.14.252.1[500] to 192.168.178.28[500] (271 bytes)
parsed ID_PROT response 0 [ KE No CERTREQ CERTREQ NAT-D NAT-D ]
received cert request for unknown ca 'O=MGMT-FW1..b8o2yn'
ignoring certificate request without data
local host is behind NAT, sending keep alives
authentication of 'O=MGMT-FW1..b8o2yn, OU=users, CN=a.mastellone' (myself) successful
sending end entity cert "O=MGMT-FW1..b8o2yn, OU=users, CN=a.mastellone"
generating ID_PROT request 0 [ ID CERT SIG N(INITIAL_CONTACT) ]
sending packet: from 192.168.178.28[4500] to 156.14.252.1[4500] (1244 bytes)
sending retransmit 1 of request message ID 0, seq 3
sending packet: from 192.168.178.28[4500] to 156.14.252.1[4500] (1244 bytes)
sending retransmit 2 of request message ID 0, seq 3
sending packet: from 192.168.178.28[4500] to 156.14.252.1[4500] (1244 bytes)
sending retransmit 3 of request message ID 0, seq 3
sending packet: from 192.168.178.28[4500] to 156.14.252.1[4500] (1244 bytes)
sending keep alive to 156.14.252.1[4500]
sending retransmit 4 of request message ID 0, seq 3
sending packet: from 192.168.178.28[4500] to 156.14.252.1[4500] (1244 bytes)
sending keep alive to 156.14.252.1[4500]
sending keep alive to 156.14.252.1[4500]
sending retransmit 5 of request message ID 0, seq 3
sending packet: from 192.168.178.28[4500] to 156.14.252.1[4500] (1244 bytes)
sending keep alive to 156.14.252.1[4500]
sending keep alive to 156.14.252.1[4500]
sending keep alive to 156.14.252.1[4500]
giving up after 5 retransmits
establishing IKE_SA failed, peer not responding
establishing connection 'cira' failed
```

Any clue? I attach here the charon.log file also. Thank in advance.

History

#1 - 08.01.2021 10:33 - Tobias Brunner

- Status changed from New to Feedback

As you can see, the peer doesn't respond. So without remote log we can only guess. Either it receives the request and doesn't respond for some reason (e.g. because it doesn't trust the client certificate), or it doesn't received it, which could be because port 4500 is blocked (the switch is due to NAT traversal) or there is an IP fragmentation issue (you could try to enable IKE fragmentation, but the peer might not support it).

#2 - 08.01.2021 12:33 - Andrea Mastellone

Tobias Brunner wrote:

> As you can see, the peer doesn't respond. So without remote log we can only guess. Either it receives the request and doesn't respond for some reason (e.g. because it doesn't trust the client certificate), or it doesn't received it, which could be because port 4500 is blocked (the switch is due to NAT traversal) or there is an IP fragmentation issue (you could try to enable IKE fragmentation, but the peer might not support it).

I have contacted sysadm, he will give me server logs in a short time. Meanwhile, I have added fragmentation option in ipsec.conf, but nothing changed. I don't know if this is important, but syadmn reported me that the server is running Checkpoint version 80.30SP, since I read that at least R81 is requested for strongswan client connection.

#3 - 08.01.2021 13:14 - Tobias Brunner

> Meanwhile, I have added fragmentation option in ipsec.conf, but nothing changed.

Is fragmentation used? (It's negotiated, so if the peer doesn't support/enable it, it won't make a difference.)

> I don't know if this is important, but syadmn reported me that the server is running Checkpoint version 80.30SP, since I read that at least R81 is requested for strongswan client connection.

No idea, don't have any experience with Checkpoint. But since you are using IKEv1 the version probably doesn't make a difference.

#4 - 08.01.2021 17:58 - Andrea Mastellone

- File trac.log added

Tobias Brunner wrote:

> > Meanwhile, I have added fragmentation option in ipsec.conf, but nothing changed.
>
> Is fragmentation used? (It's negotiated, so if the peer doesn't support/enable it, it won't make a difference.)

I don't know.

> > I don't know if this is important, but syadmn reported me that the server is running Checkpoint version 80.30SP, since I read that at least R81 is requested for strongswan client connection.
>
> No idea, don't have any experience with Checkpoint. But since you are using IKEv1 the version probably doesn't make a difference.

OK.

My sysadm has not yet given me server logs. I attach here a log from Window client of a regular connection, perhaps it can give us some hint. Thank you in advance for your effort.

Files

ipsec.conf	1.68 KB	07.01.2021	Andrea Mastellone
charon.log	88 KB	07.01.2021	Andrea Mastellone
trac.log	117 KB	08.01.2021	Andrea Mastellone