strongSwan - Issue #3152

Problem connecting from Windows 7 but not from mobile

19.08.2019 18:36 - Farhad Sakhaei

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	interoperability		
Affected version:	5.8.0	**Resolution:**	Duplicate

Description

I tested this case on 3 different internet connections,
On my mobile phone (Android StrongSwan client) I can connect to my StrongSwan VPN connection using all 3 internet connections
But on Windows 7 I can connect using just one of my internet connections and cannot using 2 others
It seems the problem related to Windows 7 itself! Because I can connect using the same internet connection and Wifi on mobile
But it is strange which I can connect using one of those 3 connections on Windows 7!
What can be the problem?
Appreciate for any help

```
config setup
    # locally = left
    # remote = right

    # If the same user repeatedly logs in on a different device, yes disconnects the old connectio
n, creates a new connection;
    # no keeps the old connection and sends a notification; never with no, but does not send a not
ification.
    uniqueids = never

# Define the connection item, named %default, all connections will inherit it
conn %default

    # Whether compression is enabled, yes means that if compression is enabled, it will be enabled
.
    compress = yes
    # Data transfer protocol encryption algorithm list
    # The public IP address of the server can be the magic word %any, which means that it is taken
 from the local IP address table.
    left = %any
    # Server terminal network, magic word 0.0.0.0/0. If the virtual IP address is assigned to the 
client, it means that after iptables forwarding, the server must use the magic word.
    leftsubnet = 0.0.0.0/0
    # whether the participant is doing forwarding-firewalling (including masquerading) using iptab
les for traffic from subnet, which should be turned off for traffic to the other subnet
    leftfirewall = yes
    rightfirewall = yes
    # The port used by the server for ike authentication. The default is 500. If nat forwarding is
 used, 4500 is used.
    #leftikeport = 600
    #rightikeport = 4550
    # Client IP, same as above
    right = %any
    # Client virtual IP segment
    rightsourceip = 192.168.100.0/24
    # Client id, arbitrary
    rightid = %any
    # Specify the DNS between the server and the client, separated by "," 
    leftdns = 8.8.8.8,8.8.4.4
    rightdns = 8.8.8.8,8.8.4.4

# ios, mac os, win7+, linux
conn ANDROID-STRONGSWAN
    type = transport
    esp = aes256-sha256,aes256-sha1,3des-sha1!
    # Key exchange protocol encryption algorithm list
    ike = aes256-sha256-modp2048,aes256-sha1-modp2048,aes128-sha1-modp2048,3des-sha1-modp2048,aes256-sha256-modp1024,aes256-sha1-modp1024,aes128-sha1-modp1024,3des-sha1-modp1024!
    # Server authentication method, using certificate
    leftauth = pubkey
    rekey=no
    # Server certificate, which can be in PEM or DER format
    leftcert = server.cert.pem
    # Specify the public key of the server certificate
    leftsigkey = server.pub.pem
    # The server ID can be arbitrarily specified. The default is the subject of the server certificate, or the magic word %any, which means nothing.
    leftid = 185.17.146.30
    # Client authentication uses EAP extended authentication, looks like eap-mschapv2 is more general
    rightauth = eap-mschapv2
    # Specify client eap id
    eap_identity = %any
    # Enable IKE message fragmentation
    fragmentation = yes
    forceencaps = yes
    mobike=yes
    # How to handle this connection when the service starts. Add is added to the connection table.
    auto = add

conn android_xauth_psk
    keyexchange=ikev1
    leftauth=psk
    rightauth=psk
    rightauth2=xauth
    fragmentation = yes
    forceencaps = yes
    mobike=yes
    auto=add

conn networkmanager-strongswan
    leftauth=pubkey
    leftcert = server.cert.pem
    rightauth=pubkey
    rightcert= client.cert.pem
    auto=add

conn windows7
    keyexchange=ikev2
    ike=aes256-sha1-modp1024!
    rekey=no
    leftauth=pubkey
    leftcert=server.cert.pem
    rightauth=eap-mschapv2
    rightsendcert=never
    eap_identity=%any
    fragmentation = yes
    forceencaps = yes
    mobike=yes
    auto=add
```

Related issues:

Is duplicate of Issue #965: Windows 8.1 cannot connect to strongSwan on IKEv2...	**Closed**

History

#1 - 20.08.2019 09:32 - Tobias Brunner

- Is duplicate of Issue #965: Windows 8.1 cannot connect to strongSwan on IKEv2 error 809 added

#2 - 20.08.2019 09:32 - Tobias Brunner

- Category changed from windows to interoperability

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Priority changed from High to Normal

- Resolution set to Duplicate

> What can be the problem?

Probably an IP fragmentation issue. Windows 7 does not support IKE fragmentation (recent releases of Windows 10 do), so large IKE messages are fragmented on the IP level and such fragments are often dropped by ISPs. See the referenced issue for more.

#3 - 20.08.2019 10:28 - Farhad Sakhaei

Thanks for the reply,
is it possible to add fragmentation support to Windows 7?
Or another way to authenticate like a certificate method for Windows 7?

#4 - 20.08.2019 10:29 - Farhad Sakhaei

Tobias Brunner wrote:

> > What can be the problem?
>
> Probably an IP fragmentation issue. Windows 7 does not support IKE fragmentation (recent releases of Windows 10 do), so large IKE messages are fragmented on the IP level and such fragments are often dropped by ISPs. See the referenced issue for more.

Thanks for the reply,
is it possible to add fragmentation support to Windows 7?
Or another way to authenticate like a certificate method for Windows 7?

#5 - 20.08.2019 10:44 - Noel Kuntze

No, fragmentation support can not be added. This is a problem on the Windows side. Please provide a log as shown on the HelpRequests page.

#6 - 20.08.2019 10:52 - Farhad Sakhaei

Noel Kuntze wrote:

> No, fragmentation support can not be added. This is a problem on the Windows side. Please provide a log as shown on the HelpRequests page.

So this means we can't use certificate-based authentication too? Or it will work on Windows 7?

#7 - 20.08.2019 11:31 - Noel Kuntze

> Windows 7 does not support IKE fragmentation (recent releases of Windows 10 do),[...]

#8 - 21.08.2019 23:51 - Farhad Sakhaei

Noel Kuntze wrote:

> > Windows 7 does not support IKE fragmentation (recent releases of Windows 10 do),[...]

OK, I connected through one of my internet connections which didn't have any problem, then switched my Wifi to another connection which has problems of connecting,
The VPN connection is still connected and it is working great!
It seems that the problem is with authentication only, not the whole transfer
So is there any solution to bypass this step?

#9 - 22.08.2019 13:21 - Noel Kuntze

Try giving the clients the certificate of the server and set leftsendcert=no. If authenticating the Windows client against the server then still works, this might be a viable solution for you. If you do that, the certificate needs to be always the same one the server has though and I don't know if that is a possible solution at all.
And yes, IKE is only the management protocol. Data traffic is passed through the ESP or ESP in UDP protocol.

#10 - 23.08.2019 10:14 - Farhad Sakhaei

Noel Kuntze wrote:

> Try giving the clients the certificate of the server and set leftsendcert=no. If authenticating the Windows client against the server then still works, this might be a viable solution for you. If you do that, the certificate needs to be always the same one the server has though and I don't know if that is a possible solution at all.
> And yes, IKE is only the management protocol. Data traffic is passed through the ESP or ESP in UDP protocol.

Thank you for your following issues,
I installed the server certificate on the client, still didn't success on authentication,
Is it possible to add l2tp support to Strongswan to cover Windows 7 clients?
Thank you for your support

#11 - 24.08.2019 23:23 - Farhad Sakhaei

Noel Kuntze wrote:

> Try giving the clients the certificate of the server and set leftsendcert=no. If authenticating the Windows client against the server then still works, this might be a viable solution for you. If you do that, the certificate needs to be always the same one the server has though and I don't know if that is a possible solution at all.
> And yes, IKE is only the management protocol. Data traffic is passed through the ESP or ESP in UDP protocol.

Hiiii
I downloaded and installed TheGreenBow VPN Client (https://www.thegreenbow.com/vpn_products.html)
It works on Windows 7 with support of fragmentation, Although I didn't check that option,
It works great on all connections,
Such Free client will help us too much for users on Windows, is it possible?