strongSwan - Issue #3640

Problem surfing via VPN form Android APK on a sepcific Mobile Operator

25.11.2020 08:59 - Royi Cohen

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.9.1	**Resolution:**	

Description

following the description is issue #3632, we had to modify the MTU in the Android client apk in order for the VPN to establish the connection.
But now we are facing surfing issues for specific websites like cnn.com, that after trying to surf to these sites, the surfing is stopped.
Based on the instruction in [[https://wiki.strongswan.org/projects/strongswan/wiki/ForwardingAndSplitTunneling#MTUMSS-issues]] article we reduce the value of MSS on the server by running the following commands:
_ iptables -t mangle -A FORWARD -m policy --pol ipsec --dir in -p tcp -m tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1261:1536 -j TCPMSS --set-mss 1260
iptables -t mangle -A FORWARD -m policy --pol ipsec --dir out -p tcp -m tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1261:1536 -j TCPMSS --set-mss 1260

```
ip6tables -t mangle -A FORWARD -m policy --pol ipsec --dir in -p tcp -m tcp --tcp-flags SYN,RST SY
N -m tcpmss --mss 1161:1536 -j TCPMSS --set-mss 1160
        ip6tables -t mangle -A FORWARD -m policy --pol ipsec --dir out -p tcp -m tcp --tcp-flags S
YN,RST SYN -m tcpmss --mss 1161:1536 -j TCPMSS --set-mss 1160

iptables -t mangle -A PREROUTING -m policy --pol ipsec --dir in -p tcp -m tcp --tcp-flags SYN,RST
SYN -m tcpmss --mss 1261:1536 -j TCPMSS --set-mss 1260
        ip6tables -t mangle -A PREROUTING -m policy --pol ipsec --dir in -p tcp -m tcp --tcp-flags
 SYN,RST SYN -m tcpmss --mss 1161:1536 -j TCPMSS --set-mss 1160

iptables -t mangle -A POSTROUTING -m policy --pol ipsec --dir out -p tcp -m tcp --tcp-flags SYN,RS
T SYN -m tcpmss --mss 1261:1536 -j TCPMSS --set-mss 1260
        ip6tables -t mangle -A POSTROUTING -m policy --pol ipsec --dir out -p tcp -m tcp --tcp-fla
gs SYN,RST SYN -m tcpmss --mss 1161:1536 -j TCPMSS --set-mss 1160_
```

But we don't see any improvement...

any idea on how we can debug this issue?

History

#1 - 26.11.2020 09:27 - Royi Cohen

some more finding in :
We had to reduce the MTU size in the client APK to 1300 (default was 1400) in order to successfully establish the VPN connection on this specific mobile network.
When we increase the size of the MTU to 1500 on the server-side we notice some improvement in the surfing from the Android device but still surfing to some web sites, like cnn.com is not working.

We try to check the MTU size of the path to the Android device by running a ping command with a big packet size to the virtual IP of the device and we are getting a very big number: 9001
ping -s 14400 -M do 10.2.0.1

does not look like a real value... how can we check this value?

#2 - 26.11.2020 09:42 - Tobias Brunner

- Status changed from New to Feedback

> We try to check the MTU size of the path to the Android device by running a ping command with a big packet size to the virtual IP of the device and we are getting a very big number: 9001
> ping -s 14400 -M do 10.2.0.1

Do you get a response to this? I'd assume not and if no lower MTU is reported then PMTUD is not working. So you'd have to manually reduce the size until you get a response.

> does not look like a real value... how can we check this value?

9001 is the correct local MTU if jumbo frames are allowed on the outgoing interface.

#3 - 26.11.2020 09:52 - Royi Cohen

Tobias Brunner wrote:

> > We try to check the MTU size of the path to the Android device by running a ping command with a big packet size to the virtual IP of the device and we are getting a very big number: 9001
> > ping -s 14400 -M do 10.2.0.1
>
> Do you get a response to this? I'd assume not and if no lower MTU is reported then PMTUD is not working. So you'd have to manually reduce the size until you get a response.

No response, but this gives me the ability to get the value of the MTU... If I reduce the packetsize it will return a value...

> > does not look like a real value... how can we check this value?
>
> 9001 is the correct local MTU if jumbo frames are allowed on the outgoing interface.

#4 - 26.11.2020 11:43 - Royi Cohen

one correction, in the server, we changed the **fragment_size** to 1500, in the charon.conf file.