OpenVPN - DEPRECATED OPTION: --tls-remote

OpenVPN - DEPRECATED OPTION: --tls-remote

by **ummeegge** » July 29th, 2014, 10:26 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Hi all,
this post should be more a informative one but i think also a development subject for one of the coming IPFire releases.

This directive migration has been released with Core 100 --> http://planet.ipfire.org/post/ipfire-2- ... or-testing

What happens now:
This client log message,

CODE: SELECT ALL
```
DEPRECATED OPTION: --tls-remote, please update your configuration
```

appears since OpenVPN version 2.3, so the clientside directive "--tls-remote" will be removed from OpenVPN in one of the next versions --> https://community.openvpn.net/openvpn/w ... n23ManPage

from https://community.openvpn.net/openvpn/w ... n23ManPage:

> --tls-remote name (DEPRECATED)
> Accept connections only from a host with X509 name or common name equal to name. The remote host must also pass all other tests of verification.
>
> NOTE: Because tls-remote may test against a common name prefix, only use this option when you are using OpenVPN with a custom CA certificate that is under your control. Never use this option when your client certificates are signed by a third party, such as a commercial web CA.
>
> Name can also be a common name prefix, for example if you want a client to only accept connections to "Server-1", "Server-2", etc., you can simply use --tls-remote Server
>
> Using a common name prefix is a useful alternative to managing a CRL (Certificate Revocation List) on the client, since it allows the client to refuse all certificates except for those associated with designated servers.
>
> --tls-remote is a useful replacement for the --tls-verify option to verify the remote host, because --tls-remote works in a --chroot environment too.
>
> Please also note: This option is now deprecated. It will be removed either in OpenVPN v2.4 or v2.5. So please make sure you support the new X.509 name formatting described with the --compat-names option as soon as possible by updating your configurations to use --verify-x509-name instead.

so for future updates of OpenVPN on IPFire (2.4+) it could be important to modify existing client.ovpn´s and replace the "--tls-remote name" with the new "--verify-x509-name name type" directive.
Since OpenVPN client/server version 2.3.2 the new verify option can be used in client configs whereby "type" includes the possibilty of 3 different kinds of verification --> "subject", "name" and "name-prefix" .

from https://community.openvpn.net/openvpn/w ... n23ManPage:

> --verify-x509-name name type
> Accept connections only if a host's X.509 name is equal to name. The remote host must also pass all other tests of verification.
>
> Which X.509 name is compared to name depends on the setting of type. type can be "subject" to match the complete subject DN (default), "name" to match a subject RDN or "name-prefix" to match a subject RDN prefix. Which RDN is verified as name depends on the --x509-username-field option. But it defaults to the common name (CN), e.g. a certificate with a subject DN "C=KG, ST=NA, L=Bishkek, CN=Server-1" would be matched by:
>
> --verify-x509-name 'C=KG, ST=NA, L=Bishkek, CN=Server-1' and --verify-x509-name Server-1 name or you could use --verify-x509-name Server- name-prefix if you want a client to only accept connections to "Server-1", "Server-2", etc.
>
> --verify-x509-name is a useful replacement for the --tls-verify option to verify the remote host, because --verify-x509-name works in a --chroot environment without any dependencies.
>
> Using a name prefix is a useful alternative to managing a CRL (Certificate Revocation List) on the client, since it allows the client to refuse all certificates except for those associated with designated servers.
>
> NOTE: Test against a name prefix only when you are using OpenVPN with a custom CA certificate that is under your control. Never use this option with type "name-prefix" when your client certificates are signed by a third party, such as a commercial web CA.

This leads to a question which one of the "types" should be used for future versions on IPFire. At this time IPFire handles "--tls-remote" automatically and it can´t be configured over the WUI, this is handy cause the user doesn´t need to bother around with all that kind of settings, but should this remain in that way also for the new verification method ?

Also, to use "--verify-x509-name" the clients needs to have a version >= 2.3.2 otherwise the connection won´t come up.

May some people out there have some ideas, informations, ..., for this topic. Anyway a discussion about that might be interesting.

Greetings,

UE

Last edited by ummeegge on July 29th, 2014, 8:47 pm, edited 1 time in total.

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **StefanSchantl** » July 29th, 2014, 11:47 am

StefanSchantl
Core Developer
Posts: 822
Joined: December 3rd, 2008, 2:50 pm
Location: Steiermark

Hello Erik,

I think this would be a great topic for our development mailing list.

For all forum user which didn't know about this list:

http://lists.ipfire.org/mailman/listinfo/development

Best regards,

-Stefan

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **ummeegge** » July 29th, 2014, 6:10 pm

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Hello Stefan,
good idea, i did that now --> http://lists.ipfire.org/pipermail/devel ... 00569.html .

Greetings,

Erik

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **ummeegge** » June 15th, 2015, 11:41 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Hi all,
to stay a little tuned in this topic, i wanted to leave you all a ovpnmain.cgi patch to solve the message "DEPRECATED OPTION: --tls-remote, please update your configuration" and be also prepared for OpenVPN-2.4.x where this directive will be removed.

Please backup your existing ovpnmain.cgi with a command like this e.g.

CODE: SELECT ALL
```
cp /srv/web/ipfire/cgi-bin/ovpnmain.cgi /srv/web/ipfire/cgi-bin/ovpnmain.cgi.bck
```

the patch looks then like this.

CODE: SELECT ALL
```
-> diff -u ovpnmain.cgi.core91 ovpnmain.cgi
--- ovpnmain.cgi.core91   2015-06-15 13:00:48.734685835 +0200
+++ ovpnmain.cgi   2015-06-15 13:09:53.238402672 +0200
@@ -2290,7 +2290,7 @@
     }
     print CLIENTCONF "verb 3\r\n";
     print CLIENTCONF "ns-cert-type server\r\n";
-    print CLIENTCONF "tls-remote $vpnsettings{ROOTCERT_HOSTNAME}\r\n";
+    print CLIENTCONF "verify-x509-name $vpnsettings{ROOTCERT_HOSTNAME} name\r\n";
     if ($vpnsettings{MSSFIX} eq 'on') {
    print CLIENTCONF "mssfix\r\n";
     }
```

this will change only the client.ovpn and reverts the '--tls-remote name' with '--verify-x509-name Server-1 name'.

Have started some tests and until now it looks good.

!!! Both directives are working until 2.4.x, then all clients should have replaced '--tls-remote name' with '--verify-x509-name Server-1 name' !!!

Some testing or other feedback might be nice.

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **fire_on_ip** » July 10th, 2015, 8:18 pm

fire_on_ip
Posts: 11
Joined: March 14th, 2014, 11:40 am

Hi ummeegge,

thanks for this helpful hint and patch.
I tried this and in general the "verify-x509-name" line seems to work.

I would like to add, however, that in order to use the ovpn configuration file with OpenVPN Connect client for Android I needed to also define

CODE: SELECT ALL
```
remote X.X.X.X
```

That is adding the following to /srv/web/ipfire/cgi-bin/ovpnmain.cgi

CODE: SELECT ALL
```
   print CLIENTCONF "remote $vpnsettings{ROOTCERT_HOSTNAME}\r\n";
```

Only after that the Android client connects without problems. It seems logic to me that the remote still needs to be defined somewhere. Should this be part of the patch?

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **ummeegge** » July 11th, 2015, 8:46 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Hi fire_on_ip,
this directive is already set but includes also the used port --> http://git.ipfire.org/?p=ipfire-2.x.git ... next#l2249 . The "Local VPN Hostname/IP:" section in the WUI is responsible for this configuration entry, so i ´am not sure where your problem is located.
What errors appears in your logs ? Which OpenVPN version on Android do you use ?

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **fire_on_ip** » July 11th, 2015, 8:04 pm

fire_on_ip
Posts: 11
Joined: March 14th, 2014, 11:40 am

Hi ummeegge,

Thanks for following up. I figured out what happened:
I had initially tried to set up clients before even enabling the server. There is somewhat of a quirk in ovpnmain.cgi currently. If you don't have any of the checkboxes "OpenVPN on RED", or "OpenVPN on BLUE" or "OpenVPN on ORANGE" checked, the WUI does not include the "Local VPN Hostname/IP:" in the remote directive like you said. (That's obvious from the if in the code you linked too.) So that's were my problem was. - Probably the wiki should be amended to tell people to first enable the server and then download the client packages.

(Then I had seen that the directive tls-remote was included in the ovpn file - and that is what brought me to this thread.)

Anyways, I can confirm that your patch for the verify-x509-name directive works (using OpenVPN Connect, latest version 1.1.16 from play store).

Cheers!

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **ummeegge** » July 12th, 2015, 1:34 pm

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Hi fire_on_ip,
and thanks for your testings and feedback.

> **fire_on_ip wrote:**
> If you don't have any of the checkboxes "OpenVPN on RED", or "OpenVPN on BLUE" or "OpenVPN on ORANGE" checked, the WUI does not include the "Local VPN Hostname/IP:" in the remote directive like you said. (That's obvious from the if in the code you linked too.) So that's were my problem was. - Probably the wiki should be amended to tell people to first enable the server and then download the client packages.

You will definitly need a hook in the 'OpenVPN on red' checkbox otherwise the FW rules won´t be set and only orange or only blue connections won´t work. You can find that in the Wiki also explained --> http://wiki.ipfire.org/en/configuration ... g/glob_set whereby i tried to formulate it a little better. Since the Wiki is community developed, everybody is invited to extend it or make it more understandable for everyone. If you find some unclear things and you got a better way to explain it, you are invited to do so 🙂 .

> **fire_on_ip wrote:**
> Anyways, I can confirm that your patch for the verify-x509-name directive works (using OpenVPN Connect, latest version 1.1.16 from play store).

Important to know, i ´am not really sure on which OpenVPN client version this directive do not work (backwards compatibility), but i have in mind something like =< 2.3.1 !? May those clients versions of OpenVPN could have problems to connect, so i ask myself if it is worth to bring on a checkbox with --tls-remote behind for compatibility reasons, apart from that some important Bugfixes was done until today (2.3.7), so it might be nevertheless better to update those clients <-- so not really sure about that ?!

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **fire_on_ip** » July 13th, 2015, 7:35 pm

fire_on_ip
Posts: 11
Joined: March 14th, 2014, 11:40 am

Hi UE,

thanks for the encouragement to edit the wiki. I shall do that and contribute some myself.

As for your question on when to replace the deprecated directive tls-remote by the new one verify-x509-name, my opinion is that it should be soon. Considering that mobile devices will be updated fairly regularly via the app store (itunes or play, respectively). The new versions of the clients all seem to support verify-x509-name. Are there any fairly recent versions of client software known that don't support that directive? On which platform? I am also going to try to test on Mac OS (probably tunnelblick).

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **ummeegge** » July 16th, 2015, 2:09 pm

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Your welcome,
i had some tests with Tunnelblick and no problems until now, i used at least Tunnelblick 3.6beta06 (build 4346) which had an interressting new feature called XOR scrample findable in version 2.3.7txp . I´ve patched the OpenVPN on a newly builded OpenVPN server version 2.3.7 --> viewtopic.php?f=50&t=14034 , but i got some recurring connection interrupts with this new technic.
Also the OpenVPN developers are aware of that code since it wasn´t properly checked by them, for detailed discussion on OpenVPN forum take a look in here --> https://forums.openvpn.net/topic12605.html .
Nevertheless a number of projects use the code/new feature already in their distributions.

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **mihaip** » March 21st, 2016, 6:57 pm

mihaip
Posts: 13
Joined: October 22nd, 2013, 9:51 pm

Sorry to unearth this topic, but i'm on core update 99 and this issue hasn't been patched.
Just to be clear, all i have to do is substitute line that says: <quote> print CLIENTCONF "tls-remote $vpnsettings{ROOTCERT_HOSTNAME}\r\n"; <end quote> with the line that says: <quote> print CLIENTCONF "verify-x509-name $vpnsettings{ROOTCERT_HOSTNAME} name\r\n"; <end quote>

(sans "quotes" obviously)

Regards,
Mihai

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **fire_on_ip** » March 21st, 2016, 9:28 pm

fire_on_ip
Posts: 11
Joined: March 14th, 2014, 11:40 am

Hi,
Yes, I had to patch the same after the previous 2-3 core updates, too. Several people have tested and it seems like the described patch does work fine. Could someone merge it? Thanks!

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **ummeegge** » March 22nd, 2016, 8:44 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

This patch seems to be forgotten but it has been updated again in the last days --> http://patchwork.ipfire.org/patch/35/ .
Nevertheless the OpenVPN update needs to be revised again cause the current actual version is 2.3.10 .

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **5p9** » March 31st, 2016, 9:40 pm

5p9
Mentor
Posts: 1865
Joined: May 1st, 2011, 3:27 pm

Hi @ all,

my first tests with ios & andriod and the new function verify-x509 looks like good, but i see in my logs warning-messages.
here my vpn settings - only client, for more details look here http://wiki.ipfire.org/en/configuration ... penvpn/ios :

CODE: SELECT ALL
```
tls-client
client
nobind
dev tun
proto udp
tun-mtu 1400
remote $IP $PORT
cipher AES-256-CBC
auth SHA512
verb 3
ns-cert-type server
verify-x509-name $TLS name
mssfix
<ca>
```

There is the logmessages for ios:

CODE: SELECT ALL
```
Mar 31 23:34:00 myipfire openvpnserver[2925]: 55.66.77.88:26528 TLS: Initial packet from [AF_INET]55.66.77.88:26528, s
Mar 31 23:34:04 myipfire openvpnserver[2925]: 55.66.77.88:26528 VERIFY SCRIPT OK: depth=1, C=DE, O=mygateway, CN=mygat
Mar 31 23:34:04 myipfire openvpnserver[2925]: 55.66.77.88:26528 CRL CHECK OK: C=DE, O=mygateway, CN=mygateway CA
Mar 31 23:34:04 myipfire openvpnserver[2925]: 55.66.77.88:26528 VERIFY OK: depth=1, C=DE, O=mygateway, CN=mygateway CA
Mar 31 23:34:04 myipfire openvpnserver[2925]: 55.66.77.88:26528 VERIFY SCRIPT OK: depth=0, C=DE, O=mygateway, CN=My-iO
Mar 31 23:34:04 myipfire openvpnserver[2925]: 55.66.77.88:26528 CRL CHECK OK: C=DE, O=mygateway, CN=My-iOS
Mar 31 23:34:04 myipfire openvpnserver[2925]: 55.66.77.88:26528 VERIFY OK: depth=0, C=DE, O=mygateway, CN=My-iOS
Mar 31 23:34:05 myipfire openvpnserver[2925]: 55.66.77.88:26528 Authenticate/Decrypt packet error: bad packet ID (may
Mar 31 23:34:05 myipfire openvpnserver[2925]: 55.66.77.88:26528 TLS Error: incoming packet authentication failed from
Mar 31 23:34:06 myipfire openvpnserver[2925]: 55.66.77.88:26528 Data Channel Encrypt: Cipher 'AES-256-CBC' initialized
Mar 31 23:34:06 myipfire openvpnserver[2925]: 55.66.77.88:26528 Data Channel Encrypt: Using 512 bit message hash 'SHA5
Mar 31 23:34:06 myipfire openvpnserver[2925]: 55.66.77.88:26528 Data Channel Decrypt: Cipher 'AES-256-CBC' initialized
Mar 31 23:34:06 myipfire openvpnserver[2925]: 55.66.77.88:26528 Data Channel Decrypt: Using 512 bit message hash 'SHA5
```

And here my Android logmessages:

CODE: SELECT ALL
```
Mar 31 20:25:38 myfire openvpnserver[2925]: 11.22.33.44:5390 TLS: Initial packet from [AF_INET]11.22.33.44:5390, sid=3
Mar 31 20:25:42 myfire openvpnserver[2925]: 11.22.33.44:5390 VERIFY SCRIPT OK: depth=1, C=DE, O=mygateway, CN=mygatewa
Mar 31 20:25:43 myfire openvpnserver[2925]: 11.22.33.44:5390 CRL CHECK OK: C=DE, O=mygateway, CN=mygateway CA
Mar 31 20:25:43 myfire openvpnserver[2925]: 11.22.33.44:5390 VERIFY OK: depth=1, C=DE, O=mygateway, CN=mygateway CA
Mar 31 20:25:43 myfire openvpnserver[2925]: 11.22.33.44:5390 VERIFY SCRIPT OK: depth=0, C=DE, O=mygateway, CN=droid10
Mar 31 20:25:43 myfire openvpnserver[2925]: 11.22.33.44:5390 CRL CHECK OK: C=DE, O=mygateway, CN=droid10
Mar 31 20:25:43 myfire openvpnserver[2925]: 11.22.33.44:5390 VERIFY OK: depth=0, C=DE, O=mygateway, CN=droid10
Mar 31 20:25:44 myfire openvpnserver[2925]: 11.22.33.44:5390 Authenticate/Decrypt packet error: bad packet ID (may be
Mar 31 20:25:44 myfire openvpnserver[2925]: 11.22.33.44:5390 TLS Error: incoming packet authentication failed from [AF
Mar 31 20:25:44 myfire openvpnserver[2925]: 11.22.33.44:5390 Authenticate/Decrypt packet error: bad packet ID (may be
Mar 31 20:25:44 myfire openvpnserver[2925]: 11.22.33.44:5390 TLS Error: incoming packet authentication failed from [AF
Mar 31 20:25:44 myfire openvpnserver[2925]: 11.22.33.44:5390 Authenticate/Decrypt packet error: bad packet ID (may be
Mar 31 20:25:44 myfire openvpnserver[2925]: 11.22.33.44:5390 TLS Error: incoming packet authentication failed from [AF
```

Mail Gateway: mail proxy

IPFire - An open source firewall solution

IPFire 2.21 - Core Update 125 on i686
Intel Core i3-4130T @ 2.89GHz x2 - 8GB

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **ummeegge** » April 2nd, 2016, 8:41 am

ummeegge
Community Developer
Posts: 5001
Joined: October 9th, 2010, 10:00 am

Hello 5p9,
this message

CODE: SELECT ALL
```
Authenticate/Decrypt packet error: bad packet ID (may be a replay): [ #45 / time = (1459460040) Thu Mar 31 23:34:00 201
```

can indicates several "problems" but in your case the message are delivered only one time and the connection comes then up, in case of a real problem, this message occurs dozents of times and don´t let the connection comes up. Possible problems can be, the order in which the packages arrives are not o.k., the same packages can arrive multiple times, problems with a WLAN connection, problems with the ethernet adapter or network card (which it is not in your case 🙂), no/or_a_bad time syncronisation between OpenVPN server and client, or even a temporarily problem between you and your provider. If this is a real persistent problem it might be an idea to test the connection with TCP and go for a check if this can be solved in that way.

Nevertheless i think this one have not so much to do with the new directive, wich you can also test if you change, while this problem comes up, from the new '--verify-x509-name' to the old directive '--tls-remote' instead and go for a check if the same behaviour happens again.

Greetings,

UE

IPFire - An open source firewall solution
IPFire - An open source firewall solution

OpenVPN - DEPRECATED OPTION: --tls-remote

Locked Search this topic... 17 posts 1 2

Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **5p9** » May 12th, 2016, 2:01 pm

5p9
Mentor

Posts: 1865
Joined: May 1st, 2011, 3:27 pm

Hi,

my new testing 2 VPN Clientprofiles from the same Network (two devices) to connect on my fire, was very strange...
This one is the downloadprofile with ta- and p12 file from OVPN-WUI for my local PC:

CODE: SELECT ALL

```
#OpenVPN Client conf
tls-client
client
nobind
dev tun
proto udp
tun-mtu 1500
remote MY-GATEWAY 12345
pkcs12 MY-Cert.p12
cipher AES-256-CBC
auth SHA512
tls-auth ta.key
verb 3
ns-cert-type server
```

with those config i have no problems im my ovpnlog.

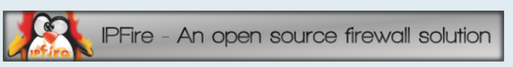
and with my customsetting i see temporary three times the TLS-Errors before the connection is normaly established:

CODE: SELECT ALL

```
#OpenVPN Client conf
tls-client
client
nobind
dev tun
proto udp
tun-mtu 1400
remote MY-GATEWAY 12345
cipher AES-256-CBC
auth SHA512
verb 3
ns-cert-type server
verify-x509-name ipfirename.local name
mssfix
```

i try in my next case to install my cert from the customsettings on my windows system and we will see 😀

Mail Gateway: mail proxy



Re: OpenVPN - DEPRECATED OPTION: --tls-remote

by **ummeegge** » June 2nd, 2016, 6:43 pm

ummeegge
Community Developer

Posts: 5001
Joined: October 9th, 2010, 10:00 am

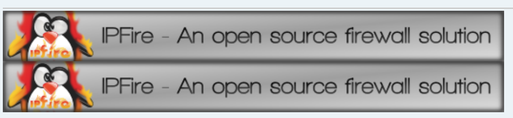
Hi all,
i would like to close this topic since the content has been released with Core 100 and there has been not that much negativ response causing this topic.

I would also like to thank all the people who helped out with testings to integrate that feature into IPFire environment (well done 😎).

Will leave this topic open for 2 more days to stay open for whichever requests.

Thanks and greetings,

UE



Locked 17 posts 1 2

‹ Return to “Development”

Powered by phpBB® Forum Software © phpBB Limited
Privacy | Terms