strongSwan - Issue #3082

IPSec IKEv2 Client to VPN service

05.06.2019 16:52 - Bernd Bernikov

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.6.3	**Resolution:**	No feedback

Description

Hello.

I have already opened a strongswan IPsec IKEv2 topic in the [[OpenWRT Forum]https://forum.openwrt.org/t/ipsec-ikev2-client-to-vpn-service/37352], but nobody has answered so far.

Is my project even possible?

Thanks and Regards,
Bernd

History

#1 - 05.06.2019 17:35 - Tobias Brunner

- Category set to configuration

- Status changed from New to Feedback

The authentication failed on the peer, so read the peer's log. If you don't have access, try configuring your side correctly (authentication method, credentials, identities etc.).

#2 - 05.06.2019 18:14 - Bernd Bernikov

> The authentication failed on the peer, so read the peer's log.

Sorry for my bad English, but what do you mean by peer? I am a beginner in strongswan.

> If you don't have access, try configuring your side correctly (authentication method, credentials, identities etc.)

I do not have access to the Server, so my only option is to configure the client side correctly. And here is the problem. I do not know how. The configuration I have from different VPN providers for Ubuntu Linux.

OpenWRT is based on Linux, but the configuration of Ubuntu unfortunately does not work on OpenWRT.

Here is the last configuration of Ubuntu again:

```
conn PP-VPN
        keyexchange=ikev2
        dpdaction=clear
        dpddelay=300s
        rekey=no
        eap_identity="USERNAME"
        compress=no
        esp=aes256-sha1
        ike=aes256-sha1-curve25519
        leftauth=eap-mschapv2
        left=%defaultroute
        leftsourceip=%config
        right=amsterdam1.perfect-privacy.com
        rightauth=pubkey
        rightsubnet=0.0.0.0/0
        rightid="C=CH, ST=Zug, L=Zug, O=Perfect Privacy, CN=Perfect Privacy IPSEC CA, E=admin@perfect-privacy.
com"
        rightcert=/etc/ipsec.d/certs/perfect-privacy_ipsec_ca.pem
```

```
        type=tunnel
        auto=add
```

and the last systemlog:

```
authpriv.info ipsec_starter[3710]: Starting strongSwan 5.6.3 IPsec [starter]...
authpriv.info ipsec_starter[3710]: charon is already running (/var/run/charon.pid exists) -- skipping daemon s
tart
daemon.err modprobe: ah4 is already loaded
daemon.err modprobe: esp4 is already loaded
daemon.err modprobe: ipcomp is already loaded
daemon.err modprobe: xfrm4_tunnel is already loaded
daemon.err modprobe: xfrm_user is already loaded
authpriv.info ipsec_starter[3710]: starter is already running (/var/run/starter.charon.pid exists) -- no fork
done
authpriv.info ipsec_starter[3740]: Starting strongSwan 5.6.3 IPsec [starter]...
authpriv.info ipsec_starter[3740]: charon is already running (/var/run/charon.pid exists) -- skipping daemon s
tart
daemon.err modprobe: ah4 is already loaded
daemon.err modprobe: esp4 is already loaded
daemon.err modprobe: ipcomp is already loaded
daemon.err modprobe: xfrm4_tunnel is already loaded
daemon.err modprobe: xfrm_user is already loaded
authpriv.info ipsec_starter[3740]: starter is already running (/var/run/starter.charon.pid exists) -- no fork
done
authpriv.info ipsec_starter[3767]: Starting strongSwan 5.6.3 IPsec [starter]...
authpriv.info ipsec_starter[3767]: charon is already running (/var/run/charon.pid exists) -- skipping daemon s
tart
daemon.err modprobe: ah4 is already loaded
daemon.err modprobe: esp4 is already loaded
daemon.err modprobe: ipcomp is already loaded
daemon.err modprobe: xfrm4_tunnel is already loaded
daemon.err modprobe: xfrm_user is already loaded
authpriv.info ipsec_starter[3767]: starter is already running (/var/run/starter.charon.pid exists) -- no fork
done
daemon.info procd: Instance ipsec::instance1 s in a crash loop 6 crashes, 0 seconds since last crash
daemon.info : 00[DMN] signal of type SIGINT received. Shutting down
authpriv.info ipsec_starter[3450]: charon stopped after 200 ms
authpriv.info ipsec_starter[3450]: ipsec starter stopped
authpriv.info ipsec_starter[4653]: Starting strongSwan 5.6.3 IPsec [starter]...
daemon.err modprobe: ah4 is already loaded
daemon.err modprobe: esp4 is already loaded
daemon.err modprobe: ipcomp is already loaded
daemon.err modprobe: xfrm4_tunnel is already loaded
daemon.err modprobe: xfrm_user is already loaded
daemon.info : 00[DMN] Starting IKE charon daemon (strongSwan 5.6.3, Linux 4.14.95, armv7l)
daemon.info : 00[CFG] PKCS11 module '<name>' lacks library path
daemon.info : 00[LIB] curl SSL backend 'mbedTLS/2.16.1' not supported, https:// disabled
daemon.info : 00[CFG] disabling load-tester plugin, not configured
daemon.info : 00[LIB] plugin 'load-tester': failed to load - load_tester_plugin_create returned NULL
daemon.info : 00[LIB] plugin 'uci' failed to load: Error relocating /usr/lib/ipsec/plugins/libstrongswan-uci.s
o: uci_lookup: symbol not found
daemon.info : 00[CFG] attr-sql plugin: database URI not set
daemon.info : 00[NET] using forecast interface br-lan
daemon.info : 00[CFG] joining forecast multicast groups: 224.0.0.1,224.0.0.22,224.0.0.251,224.0.0.252,239.255.
255.250
daemon.info : 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
daemon.info : 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
daemon.info : 00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'
daemon.info : 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
daemon.info : 00[CFG] loading crls from '/etc/ipsec.d/crls'
daemon.info : 00[CFG] loading secrets from '/etc/ipsec.secrets'
daemon.info : 00[CFG]   loaded EAP secret for USERNAME
daemon.info : 00[CFG] sql plugin: database URI not set
daemon.info : 00[CFG] loaded 0 RADIUS server configurations
daemon.info : 00[CFG] HA config misses local/remote address
daemon.info : 00[CFG] coupling file path unspecified
daemon.info : 00[LIB] loaded plugins: charon test-vectors ldap pkcs11 aes des blowfish rc2 sha2 sha1 md4 md5 r
andom nonce x509 revocation pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl gcrypt af-alg fips-p
rf gmp curve25519 agent xcbc cmac hmac ctr ccm gcm curl mysql sqlite attr kernel-netlink resolve socket-defaul
t connmark forecast farp stroke vici smp updown eap-identity eap-md5 eap-mschapv2 eap-radius eap-tls xauth-gen
eric xauth-eap dhcp whitelist led duplicheck addrblock unity
daemon.info : 00[JOB] spawning 16 worker threads
authpriv.info ipsec_starter[4675]: charon (4676) started after 1140 ms
```

```
daemon.info : 06[CFG] received stroke: add connection 'PP-VPN'
daemon.info : 06[CFG]   loaded certificate "C=CH, ST=Zug, L=Zug, O=Perfect Privacy, CN=Perfect Privacy IPSEC C
A, E=admin@perfect-privacy.com" from '/etc/ipsec.d/certs/perfect-privacy_ipsec_ca.pem'
daemon.info : 06[CFG]   id '%any' not confirmed by certificate, defaulting to 'C=CH, ST=Zug, L=Zug, O=Perfect
 Privacy, CN=Perfect Privacy IPSEC CA, E=admin@perfect-privacy.com'
daemon.info : 06[CFG] added configuration 'PP-VPN'
daemon.info : 15[CFG] received stroke: initiate 'PP-VPN'
daemon.info : 07[IKE] initiating IKE_SA PP-VPN[1] to 85.17.28.145
authpriv.info : 07[IKE] initiating IKE_SA PP-VPN[1] to 85.17.28.145
daemon.info : 07[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH
_ALG) N(REDIR_SUP) ]
daemon.info : 07[NET] sending packet: from 109.91.77.56[500] to 85.17.28.145[500] (1068 bytes)
daemon.info : 09[NET] received packet: from 85.17.28.145[500] to 109.91.77.56[500] (265 bytes)
daemon.info : 09[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(FRAG_SUP) N
(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
daemon.info : 09[IKE] received cert request for "C=CH, ST=Zug, L=Zug, O=Perfect Privacy, CN=Perfect Privacy IP
SEC CA, E=admin@perfect-privacy.com"
daemon.info : 09[IKE] sending cert request for "C=CH, ST=Zug, L=Zug, O=Perfect Privacy, CN=Perfect Privacy IPS
EC CA, E=admin@perfect-privacy.com"
daemon.info : 09[CFG] no IDi configured, fall back on IP address
daemon.info : 09[IKE] establishing CHILD_SA PP-VPN{1}
authpriv.info : 09[IKE] establishing CHILD_SA PP-VPN{1}
daemon.info : 09[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ IDr CPRQ(ADDR DNS) SA TSi TS
r N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_
SUP) ]
daemon.info : 09[NET] sending packet: from 109.91.77.56[4500] to 85.17.28.145[4500] (577 bytes)
daemon.info : 12[NET] received packet: from 85.17.28.145[4500] to 109.91.77.56[4500] (65 bytes)
daemon.info : 12[ENC] parsed IKE_AUTH response 1 [ N(AUTH_FAILED) ]
daemon.info : 12[IKE] received AUTHENTICATION_FAILED notify error
daemon.info : 00[DMN] signal of type SIGINT received. Shutting down
authpriv.info ipsec_starter[4675]: charon stopped after 200 ms
authpriv.info ipsec_starter[4675]: ipsec starter stopped
authpriv.info ipsec_starter[5503]: Starting strongSwan 5.6.3 IPsec [starter]...
daemon.err modprobe: ah4 is already loaded
daemon.err modprobe: esp4 is already loaded
daemon.err modprobe: ipcomp is already loaded
daemon.err modprobe: xfrm4_tunnel is already loaded
daemon.err modprobe: xfrm_user is already loaded
daemon.info : 00[DMN] Starting IKE charon daemon (strongSwan 5.6.3, Linux 4.14.95, armv7l)
daemon.info : 00[CFG] PKCS11 module '<name>' lacks library path
daemon.info : 00[LIB] curl SSL backend 'mbedTLS/2.16.1' not supported, https:// disabled
daemon.info : 00[CFG] disabling load-tester plugin, not configured
daemon.info : 00[LIB] plugin 'load-tester': failed to load - load_tester_plugin_create returned NULL
daemon.info : 00[LIB] plugin 'uci' failed to load: Error relocating /usr/lib/ipsec/plugins/libstrongswan-uci.s
o: uci_lookup: symbol not found
daemon.info : 00[CFG] attr-sql plugin: database URI not set
daemon.info : 00[NET] using forecast interface br-lan
daemon.info : 00[CFG] joining forecast multicast groups: 224.0.0.1,224.0.0.22,224.0.0.251,224.0.0.252,239.255.
255.250
daemon.info : 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
daemon.info : 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
daemon.info : 00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'
daemon.info : 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
daemon.info : 00[CFG] loading crls from '/etc/ipsec.d/crls'
daemon.info : 00[CFG] loading secrets from '/etc/ipsec.secrets'
daemon.info : 00[CFG]   loaded EAP secret for USERNAME
daemon.info : 00[CFG] sql plugin: database URI not set
daemon.info : 00[CFG] loaded 0 RADIUS server configurations
daemon.info : 00[CFG] HA config misses local/remote address
daemon.info : 00[CFG] coupling file path unspecified
daemon.info : 00[LIB] loaded plugins: charon test-vectors ldap pkcs11 aes des blowfish rc2 sha2 sha1 md4 md5 r
andom nonce x509 revocation pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl gcrypt af-alg fips-p
rf gmp curve25519 agent xcbc cmac hmac ctr ccm gcm curl mysql sqlite attr kernel-netlink resolve socket-defaul
t connmark forecast farp stroke vici smp updown eap-identity eap-md5 eap-mschapv2 eap-radius eap-tls xauth-gen
eric xauth-eap dhcp whitelist led duplicheck addrblock unity
daemon.info : 00[JOB] spawning 16 worker threads
authpriv.info ipsec_starter[5538]: charon (5539) started after 1080 ms
daemon.info : 07[CFG] received stroke: add connection 'PP-VPN'
daemon.info : 07[CFG]   loaded certificate "C=CH, ST=Zug, L=Zug, O=Perfect Privacy, CN=Perfect Privacy IPSEC C
A, E=admin@perfect-privacy.com" from '/etc/ipsec.d/certs/perfect-privacy_ipsec_ca.pem'
daemon.info : 07[CFG] added configuration 'PP-VPN'
daemon.info : 09[CFG] received stroke: initiate 'PP-VPN'
daemon.info : 08[IKE] initiating IKE_SA PP-VPN[1] to 85.17.28.145
authpriv.info : 08[IKE] initiating IKE_SA PP-VPN[1] to 85.17.28.145
daemon.info : 08[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH
```

```
_ALG) N(REDIR_SUP) ]
daemon.info : 08[NET] sending packet: from 109.91.77.56[500] to 85.17.28.145[500] (1068 bytes)
daemon.info : 12[NET] received packet: from 85.17.28.145[500] to 109.91.77.56[500] (265 bytes)
daemon.info : 12[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(FRAG_SUP) N
(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
daemon.info : 12[IKE] received cert request for "C=CH, ST=Zug, L=Zug, O=Perfect Privacy, CN=Perfect Privacy IP
SEC CA, E=admin@perfect-privacy.com"
daemon.info : 12[IKE] sending cert request for "C=CH, ST=Zug, L=Zug, O=Perfect Privacy, CN=Perfect Privacy IPS
EC CA, E=admin@perfect-privacy.com"
daemon.info : 12[CFG] no IDi configured, fall back on IP address
daemon.info : 12[IKE] establishing CHILD_SA PP-VPN{1}
authpriv.info : 12[IKE] establishing CHILD_SA PP-VPN{1}
daemon.info : 12[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ IDr CPRQ(ADDR DNS) SA TSi TS
r N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_
SUP) ]
daemon.info : 12[NET] sending packet: from 109.91.77.56[4500] to 85.17.28.145[4500] (577 bytes)
daemon.info : 04[NET] received packet: from 85.17.28.145[4500] to 109.91.77.56[4500] (65 bytes)
daemon.info : 04[ENC] parsed IKE_AUTH response 1 [ N(AUTH_FAILED) ]
daemon.info : 04[IKE] received AUTHENTICATION_FAILED notify error
```

Unfortunately, I can not continue.

#3 - 05.06.2019 18:30 - Tobias Brunner

> Sorry for my bad English, but what do you mean by peer? I am a beginner in strongswan.

Peer = other end (in IKE/IPsec the two parties are technically equivalent, only the configuration can restrict that and make one a clear client or server).

> > If you don't have access, try configuring your side correctly (authentication method, credentials, identities etc.)
>
> I do not have access to the Server, so my only option is to configure the client side correctly. And here is the problem. I do not know how. The configuration I have from different VPN providers for Ubuntu Linux.

There are only few options, either the server doesn't want to do EAP authentication with the client, or it doesn't like the client's identity it received (if you don't configure it via *leftid*, it defaults to the IP address, as the log tells you, maybe set it to the username you received from the VPN service provider). If this doesn't work you have to contact the VPN service provider as they are the only ones who know why their server rejected your client.

> OpenWRT is based on Linux, but the configuration of Ubuntu unfortunately does not work on OpenWRT.
>
> Here is the last configuration of Ubuntu again:
>
> [...]
>
> and the last systemlog:
>
> [...]
>
> Unfortunately, I can not continue.

#4 - 05.07.2019 00:54 - Bernd Bernikov

IPSec IKEv2 client is now running on Linux Mint 19.1.

But I have again problems with IPSec IKEv2 Client on OpenWRT 18.06.2.

Here are the error messages:

```
received netlink error: Function not implemented (38)
unable to add SAD entry with SPI cbd2b552 (FAILED)
received netlink error: Function not implemented (38)
unable to add SAD entry with SPI c46edfda (FAILED)
unable to install inbound and outbound IPsec SA (SAD) in kernel
failed to establish CHILD_SA, keeping IKE_SA
peer supports MOBIKE
sending DELETE for ESP CHILD_SA with SPI cbd2b552
```

"received netlink error: Function not implemented" usually means the kernel does not support at least one of the negotiated algorithms, right?

Here is the Output of: ipsec statusall

```
Connections:
          PP:  %any...rotterdam.perfect-privacy.com  IKEv2, dpddelay=300s
          PP:   local:  uses EAP_MSCHAPV2 authentication with EAP identity 'username'
          PP:   remote: uses public key authentication
          PP:   child:  dynamic === 0.0.0.0/0 TUNNEL, dpdaction=clear
Security Associations (1 up, 0 connecting):
          PP[1]: ESTABLISHED 14 minutes ago, 10.4.133.241[10.4.133.241]...31.204.152.102[rotterdam.perfect-pri
vacy.com]
          PP[1]: IKEv2 SPIs: 6d1667c2fc0ce171_i* de144c7c1747bd3d_r, EAP reauthentication in 2 hours
          PP[1]: IKE proposal: AES_GCM_16_256/PRF_HMAC_SHA2_512/CURVE_25519
```

How can I solve this?

#5 - 05.07.2019 12:24 - Tobias Brunner

> How can I solve this?

KernelModules or try changing the config if it's due to unsupported algorithms.

#6 - 28.07.2019 18:56 - Bernd Bernikov

I have now successfully established an IKEv2 connection to ProtoVPN.

ipsec.conf:

```
conn lan-passthrough
    leftsubnet=192.168.1.1/24 # Replace with your LAN subnet
    rightsubnet=192.168.1.1/24 # Replace with your LAN subnet
    authby=never # No authentication necessary
    type=pass # passthrough
    auto=route # no need to ipsec up lan-passthrough
```

```
conn test
 left=%defaultroute
 leftsourceip=%config
 leftauth=eap-mschapv2
 eap_identity="username"
 right=37.58.58.229
 rightsubnet=0.0.0.0/0
 rightauth=pubkey
 #rightid=%37.58.58.229
 rightca=/etc/ipsec.d/cacerts/protonvpn.der
 keyexchange=ikev2
 rightfirewall=yes
 type=tunnel
 auto=add
```

But there is still no traffic. Do I need an ipsec0 tunnel and how can I create it?

with?

```
ip tunnel add ipsec0 local 192.168.1.1 remote 37.58.58.229 mode vti key 42
sysctl -w net.ipv4.conf.ipsec0.disable_policy=1
ip link set ipsec0 up
ip route add 10.0.0.0/8 dev ipsec0
ifconfig ipsec0 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
```

Is the ipsec0 configuration correct?

But with this ipsec0 configuration there is still no traffic. I need more help or an idea.

#7 - 06.08.2019 00:12 - Bernd Bernikov

Can someone help please?

#8 - 12.08.2019 14:47 - Tobias Brunner

> But there is still no traffic. Do I need an ipsec0 tunnel and how can I create it?

You don't. IntroductionTostrongSwan has some basic information on how IPsec works on Linux. You need to provide more information for us to help (see HelpRequests).

#9 - 09.10.2019 11:35 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No feedback

#10 - 10.12.2019 16:34 - Bernd Bernikov

Hello.

I can now establish a VPN connection on OpenWRT. With this script all LAN devices use the VPN tunnel:

/etc/ipsec.user:

```
case "$PLUTO_VERB" in
up-client)
        iptables -t nat -A postrouting_wan_rule -s 192.168.1.0/24 -m policy --dir out --pol none -j SNAT --to-source "$PLUTO_MY_SOURCEIP4_1"
        ;;
down-client)
        iptables -t nat -F postrouting_wan_rule
        ;;
esac
```

But with this script I only get the VPN IPv4 IP. My VPN provider also offers an IPv6 IP.

How do I modify the script for an IPv6 IP too?

Do I have to add "$PLUTO_MY_SOURCEIP6_1"? And how?