Hi @LL,
i'm new to this community because i have some problems with my TP-Link AC1750 OpenWRT 18.06 Setup with strongswan-full.

I have a Sophos Headquarter with IKEv2 and a static PublicIP IPv4.
In the Homeoffice I'm using a FritzBox for personal Homeuse with a dynamic IPv4 --> Behind the FritzBox i have the OpenWRT Router (all traffic is routed from FritzBox to it).

I think i have some config issue in ipsec.conf

/etc/ipsec.conf

# Add connections here.
conn sophos
  ike_lifetime=3600s
  keylife=8h
  rekey_margin=3m
  keyingtries=5
  mobike=no

  # This server
  left=0.0.0.0/0
  left_id=fritzbox.dyndns.org
  # The network behind this server
  leftsourceip=10.0.2.1
  leftsubnet=10.0.2.0/24
  # The remote Sophos
  right=sophosip
  right_id=sophosip
  #The network behind remote Sophos
  rightsourceip=172.28.0.0/16
  #Connection parameters
  keyexchange=ikev2
  authby=secret
  ike=aes256-sha1-modp1024,aes128-sha1-modp1024,3des-sha1-modp1024!
  esp=aes256-sha256,aes256-sha1,3des-sha1!
  dpddelay=30
  dpdtimeout=120
  dpdaction=restart
  auto=start

/etc/ipsec.secret

sophospublicip : PSK "myPSK"

/etc/strongswan.conf

# strongswan.conf - strongSwan configuration file
#
# Refer to the strongswan.conf(5) manpage for details
Configuration changes should be made in the included files

```plaintext
charon {
  load = random nonce aes gmp sha1 sha2 curve25519 hmac stroke kernel-netlink socket-default upd
  own
    install_routes = 0
    load_modular = yes
    plugins {
      include strongswan.d/charon/*.conf
    }
}
include strongswan.d/*.conf
```

Now this is the log of the openwrt

Fri Mar 13 22:31:45 2020 daemon.info: 06[CFG] left nor right host is our side, assuming left=local
Fri Mar 13 22:31:45 2020 daemon.info: 10[ENC] parsed IKE_SA_INIT response 0 [ N(NO_PROP) ]
Fri Mar 13 22:31:45 2020 daemon.info: 10[IKE] received NO_PROPOSAL_CHOSEN notify error

And this is the log of Sophos:

2020-03-13 23:31:45 11[IKE] <68> no IKE config found for SophosIP...91.17.YYY.XXX, sending NO_PROPOSAL_CHOSEN
2020-03-13 23:31:45 11[ENC] <68> generating IKE_SA_INIT response 0 [ N(NO_PROP) ]

History

#1 - 15.03.2020 11:57 - Leon Brans
Hi @ll,
at this moment i got my configuration running, but without the correct routing. I think theres now a missconfiguration in right&leftsourceip

# Add connections here.
conn sophos
  ikelifetime=36000s
  keylife=8h
  rekeymargin=3m
  keyingtries=5
  mobike=no
  keyexchange=ikev2

# This server
left=0.0.0.0/0
leftid=openwrt
leftsourceip=10.0.2.1
leftsubnet=10.0.2.0/24
# The remote Sophos
#rightauth=psk
right=sophospublicip
rightid=sophospublicip
rightsubnet=172.28.0.0/16
rightsourceip=172.28.0.254

#Connection parameters
authby=secret
#eap_identity=
ike=aes256-sha256-modp2048
esp=aes256-sha256-modp2048
dpddelay=30
dpdtimeout=120
dpdaction=restart
auto=start

openwrt log

Sun Mar 15 09:25:27 2020 authpriv.info ipsec_starter[8784]: Starting strongSwan 5.6.3 IPsec [starter]...
Sun Mar 15 09:25:27 2020 daemon.err modprobe: ah4 is already loaded
Sun Mar 15 09:25:27 2020 daemon.err modprobe: esp4 is already loaded
Sun Mar 15 09:25:27 2020 daemon.err modprobe: ipcomp is already loaded
Sun Mar 15 09:25:27 2020 daemon.err modprobe: xfrm4_tunnel is already loaded
Sun Mar 15 09:25:27 2020 daemon.err modprobe: xfrm_user is already loaded
Sun Mar 15 09:25:27 2020 daemon.info : 00[DMN] Starting IKE charon daemon (strongSwan 5.6.3, Linux 4.9.152, mips)
Sun Mar 15 09:25:31 2020 daemon.info : 00[LIB] curl SSL backend 'mbedtls/2.16.3' not supported, https:// disabled
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] disabling load-tester plugin, not configured
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] PKCS11 module '<name>' lacks library path
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] loading crls from '/etc/ipsec.d/crls'
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] loading secrets from '/etc/ipsec.secrets'
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] loading IKE secret for SOP.HOS.IPX.XXX
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] adding connection 'sophos'
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] adding configuration 'sophos'
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] received stroke: add connection 'sophos'
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] left nor right host is our side, assuming left=local
Sun Mar 15 09:25:31 2020 daemon.info : 00[CFG] 'sophos' has both left- and rightsourcesip, but IKE can negotiate one virtual IP only, ignoring local virtual IP

[3/6]
sync -b '{"local_server":"SOP.HOS.IPX.XXX","remote_server":"FritzBoxPublicIP","action":"enable","family":0,"conntype":"ntn","compress":0}: success 0
2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (do_cop_updown_invoke_once) ---- exec subnet updown ++ up ++

2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (do_cop_updown_invoke_once) [NTN] NTN get actual...

AS natedlan FROM tblvpnconnhostrel AS rel JOIN tblhost AS h ON h.hostid = rel.hostid JOIN tblhost AS nath ON rel.natedhost = nath.hostid WHERE rel.connectionid = $1 AND rel.hostlocation = 'L'
AND h.netid = $2 AND h.netmask = $3 LIMIT 1;

2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (do_cop_updown_invoke_once) [IPSEC0] using ipsec dummy interface 'ipsec0'

2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (do_cop_updown_invoke_once) [NET] (get_src_ip) source address for 172.28.0.0 is IP: 172.28.0.254 table 220: success 0

2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (add_routes) no routes to add for HO2 on interface ipsec0

2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (run_shell) 'ip route add 10.0.2.0/24 dev ipsec0 src 172.28.0.254 table 220': success 0

2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (run_shell) 'ip route flush cache': success 0

2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (run_shell) '/bin/service fwm:vpn_connection_chains -t json -s nosync -b '{"me":"SOP.HOS.IPX.XXX","peer":"FritzBoxPublicIP","mynet":"172.28.0.0/16","peernet":"10.0.2.0/24","conntype":"Port8_ppp","myproto":0,"myport":0,"peerproto":0,"peerport":0,"conntype":"ntn","actnet":","compress":0,"conn_id":1}': success 0

2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (run_shell) 'ip route flush cache': success 0

2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (run_shell) 'ip route add 10.0.2.0/24 dev ipsec0 src 172.28.0.254 table 220': success 0

2020-03-15 10:25:33 21[APP] [COP-UPDOWN] (run_shell) 'ip route flush cache': success 0

2020-03-15 10:26:03 07[IKE] <HO2-1|97> sending DPD request
2020-03-15 10:26:03 07[ENC] <HO2-1|97> generating INFORMATIONAL request 0 [ ]
2020-03-15 10:26:03 07[NET] <HO2-1|97> sending packet: from SOP.HOS.IPX.XXX[4500] to FritzBoxPublicIP[4500] (80 bytes)
2020-03-15 10:26:03 17[NET] <HO2-1|97> received packet: from FritzBoxPublicIP[4500] to SOP.HOS.IPX.XXX[4500] (80 bytes)
2020-03-15 10:26:03 17[ENC] <HO2-1|97> parsed INFORMATIONAL request 2 [ ]
2020-03-15 10:26:03 17[NET] <HO2-1|97> generating INFORMATIONAL response 2 [ ]
2020-03-15 10:26:03 17[NET] <HO2-1|97> sending packet: from SOP.HOS.IPX.XXX[4500] to FritzBoxPublicIP[4500] (80 bytes)
2020-03-15 10:26:03 11[NET] <HO2-1|97> received packet: from FritzBoxPublicIP[4500] to SOP.HOS.IPX.XXX[4500] (80 bytes)
2020-03-15 10:26:03 11[ENC] <HO2-1|97> parsed INFORMATIONAL response 0 [ ]

#2 - 16.03.2020 09:47 - Tobias Brunner
- Category changed from network / firewall to configuration
- Status changed from New to Feedback

leftsourceip=10.0.2.1
leftsubnet=10.0.2.0/24

No.
rightsubnet=172.28.0.0/16
rightsourceip=172.28.0.254

And no.

Please read VirtualIP and maybe ForwardingAndSplitTunneling and perhaps IntroductionTostrongSwan.

19.03.2020
Tobias Brunner wrote:

[...]

No.

[...]

And no.

Please read VirtualIP and maybe ForwardingAndSplitTunneling and perhaps IntroductionTostrongSwan.

Hi Thanks for your answer, i already read the article VirtualIP, Problem is that the Sophos doesn't create a virtual IP so requesting IP fails.

I wonder that the Tunnel comes up but no traffic is going through...

i also disabled firewall on Openwrt

#4 - 17.03.2020 14:01 - Tobias Brunner

i already read the article VirtualIP

Then you obviously didn't do that thoroughly, as what you configured goes against what's advised there.

Problem is that the Sophos doesn't create a virtual IP so requesting IP fails.

Then don't configure left/rightsourceip at all, as described on said wiki page.