strongSwan - Issue #3462

VPN client on openwrt connected to VPN server. But can't go through VPN connection.

23.05.2020 16:39 - John YU

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.5.3	**Resolution:**	No feedback

Description

Client config: strongswan 5.5.3 on openwrt LEDE X86_64. Official firmware and official software.

ipsec.conf:

```
conn test
    keyexchange=ikev2
    ike=aes256-sha1-modp2048!
    esp=aes256-sha1!
    right=mydomain
    rightid=mydomain
    rightsubnet=0.0.0.0/0
    rightauth=pubkey
    leftsourceip=%config
    leftsendcert=never
    leftauth=eap-mschapv2
    eap_identity=user1
    auto=start
```

I can see that it's connected after command "ipsec up test" because the last message:

```
authentication of 'mydomain' with EAP successful
IKE_SA test[4] established between 192.168.0.84[192.168.0.84]...103.60.20.9[mydomain]
installing DNS server 8.8.8.8 to /etc/resolv.conf
installing DNS server 8.8.4.4 to /etc/resolv.conf
installing new virtual IP 10.31.2.1
CHILD_SA test{4} established with SPIs cd30257a_i c0bd2c25_o and TS 10.31.2.1/32 === 0.0.0.0/0
connection 'test' established successfully
```

Also I can ping 10.31.2.1 from server side.

But the thing is: the client could't go through VPN connection. When I traceroute 8.8.8.8:

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 46 byte packets
 1  192.168.0.253 (192.168.0.253)  0.586 ms  0.848 ms  0.541 ms
 2  lo100.sglebbras11.nw.aapt.net.au (210.8.1.230)  3.294 ms  3.105 ms  2.974 ms
 3  203.131.58.40 (203.131.58.40)  3.155 ms  3.122 ms  2.963 ms
 4  bu8.sglebbrdr11.aapt.net.au (202.10.14.27)  3.703 ms  3.677 ms  3.448 ms
 5  syd-gls-har-wgw1-be-30.tpgi.com.au (203.219.107.197)  4.073 ms  3.665 ms  4.021 ms
 6  syd-apt-ros-cdn11-be200.tpgi.com.au (203.29.134.125)  3.515 ms  203.29.134-61.tpgi.com.au (203
.29.134.61)  3.742 ms  3.754 ms
 7  209.85.149.84 (209.85.149.84)  3.872 ms  12.335 ms  5.004 ms
 8  108.170.247.65 (108.170.247.65)  3.880 ms  108.170.247.81 (108.170.247.81)  4.414 ms  108.170.
247.65 (108.170.247.65)  3.866 ms
 9  209.85.250.139 (209.85.250.139)  4.082 ms  209.85.255.175 (209.85.255.175)  3.743 ms  209.85.2
55.165 (209.85.255.165)  3.979 ms
10  dns.google (8.8.8.8)  3.659 ms  4.332 ms  3.695 ms
```

It doesn't go through 103.60.20.9

Command route:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.0.253   0.0.0.0         UG    0      0        0 eth0
192.168.0.0     *               255.255.255.0   U     0      0        0 eth0
192.168.0.253   *               255.255.255.255 UH    0      0        0 eth0
```

No gateway setup for 10.31.2.1

I'm sure that my 3 servers are working because windows, mac and mobile can get connected and go through VPN connection. Little difference between 3 servers but should be no problem:
server1: VPS in US. CentOS 6 with strongswan 5.6.0
server2: router in Sydney flashed with LEDE with strongswan 5.5.3. Behind NAT with UDP 500 and 4500 forwarded to it.
server3: router in Sydney flashed with openwrt 19.07.2 with strongswan 5.8.2. Main router with static IP 10.254.9.11/24, gw: 10.254.9.1. And DMZed to a public IP.

I also tested on 5.8.2 on client. Still the same problem.
So could you please have a look at this problem and tell me if I did something wrong. Thanks!

History

#1 - 25.05.2020 11:09 - Tobias Brunner

- Description updated

- Category set to configuration

- Status changed from New to Feedback

- Priority changed from High to Normal

Use ip route show table 220 to see the routes installed by storngSwan and not route. Also see HelpRequests.

#2 - 25.05.2020 12:49 - John YU

Tobias Brunner wrote:

> Use ip route show table 220 to see the routes installed by storngSwan and not route. Also see HelpRequests.

ip route show table 220

```
default via 192.168.0.253 dev eth0  proto static  src 10.31.2.2
```

ip route

```
default via 192.168.0.253 dev eth0  proto static  src 192.168.0.84
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.84
192.168.0.253 dev eth0  proto static  scope link  src 192.168.0.84
```

BTW:
192.168.0.253 is the gateway of VPN client's original network.

#3 - 25.05.2020 13:36 - Tobias Brunner

Looks OK. We can't help you further if you don't provide more information (see the link above).

#4 - 25.05.2020 14:50 - John YU

Tobias Brunner wrote:

> Looks OK. We can't help you further if you don't provide more information (see the link above).

Check all the info below. Tell me if you need more. Thank you once again!

ipsec statusall

```
Status of IKE charon daemon (strongSwan 5.5.3, Linux 4.4.182, x86_64):
```

```
  uptime: 29 hours, since May 24 16:46:39 2020
  worker threads: 10 of 16 idle, 6/0/0/0 working, job queue: 0/0/0/0, scheduled: 2
  loaded plugins: charon test-vectors ldap pkcs11 aes des blowfish rc2 sha2 sha1 md4 md5 random nonce x509 rev
ocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl gcrypt af-alg fips-prf gmp c
urve25519 agent xcbc cmac hmac ctr ccm gcm curl mysql sqlite attr kernel-netlink resolve socket-default connma
rk forecast farp stroke smp updown eap-identity eap-md5 eap-mschapv2 eap-radius eap-tls xauth-generic xauth-ea
p dhcp whitelist led duplicheck addrblock unity
Listening IP addresses:
  192.168.0.84
Connections:
         Syd:  %any...mydomain  IKEv2
         Syd:   local:  uses EAP_MSCHAPV2 authentication with EAP identity 'user1'
         Syd:   remote: [mydomain] uses public key authentication
         Syd:   child:  dynamic === 0.0.0.0/0 TUNNEL
Security Associations (1 up, 0 connecting):
         Syd[6]: ESTABLISHED 1 second ago, 192.168.0.84[192.168.0.84]...103.60.20.9[mydomain]
         Syd[6]: IKEv2 SPIs: e8aa5d415fca8989_i* 98a663ac94d2d38b_r, EAP reauthentication in 2 hours
         Syd[6]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
         Syd{10}:  INSTALLED, TUNNEL, reqid 5, ESP in UDP SPIs: c4772286_i c3d06f54_o
         Syd{10}:  AES_CBC_256/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 42 minutes
         Syd{10}:   10.31.2.1/32 === 0.0.0.0/0
```

/etc/config/firewall

```
config defaults
    option syn_flood    1
    option input        ACCEPT
    option output        ACCEPT
    option forward        ACCEPT
# Uncomment this line to disable ipv6 rules
#    option disable_ipv6    1

config zone
    option name        lan
    list   network        'lan'
    option input        ACCEPT
    option output        ACCEPT
    option forward        ACCEPT

config zone
    option name        wan
    list   network        'wan'
    list   network        'wan6'
    option input        ACCEPT
    option output        ACCEPT
    option forward        ACCEPT
    option masq        1
    option mtu_fix        1

config forwarding
    option src        lan
    option dest        wan

# We need to accept udp packets on port 68,
# see https://dev.openwrt.org/ticket/4108
config rule
    option name        Allow-DHCP-Renew
    option src        wan
    option proto        udp
    option dest_port    68
    option target        ACCEPT
    option family        ipv4

# Allow IPv4 ping
config rule
    option name        Allow-Ping
    option src        wan
    option proto        icmp
    option icmp_type    echo-request
    option family        ipv4
    option target        ACCEPT

config rule
    option name        Allow-IGMP
```

```
    option src         wan
    option proto        igmp
    option family        ipv4
    option target        ACCEPT

# Allow DHCPv6 replies
# see https://dev.openwrt.org/ticket/10381
config rule
    option name        Allow-DHCPv6
    option src         wan
    option proto        udp
    option src_ip        fc00::/6
    option dest_ip        fc00::/6
    option dest_port    546
    option family        ipv6
    option target        ACCEPT

config rule
    option name        Allow-MLD
    option src         wan
    option proto        icmp
    option src_ip        fe80::/10
    list icmp_type        '130/0'
    list icmp_type        '131/0'
    list icmp_type        '132/0'
    list icmp_type        '143/0'
    option family        ipv6
    option target        ACCEPT

# Allow essential incoming IPv6 ICMP traffic
config rule
    option name        Allow-ICMPv6-Input
    option src         wan
    option proto    icmp
    list icmp_type        echo-request
    list icmp_type        echo-reply
    list icmp_type        destination-unreachable
    list icmp_type        packet-too-big
    list icmp_type        time-exceeded
    list icmp_type        bad-header
    list icmp_type        unknown-header-type
    list icmp_type        router-solicitation
    list icmp_type        neighbour-solicitation
    list icmp_type        router-advertisement
    list icmp_type        neighbour-advertisement
    option limit        1000/sec
    option family        ipv6
    option target        ACCEPT

# Allow essential forwarded IPv6 ICMP traffic
config rule
    option name        Allow-ICMPv6-Forward
    option src         wan
    option dest        *
    option proto        icmp
    list icmp_type        echo-request
    list icmp_type        echo-reply
    list icmp_type        destination-unreachable
    list icmp_type        packet-too-big
    list icmp_type        time-exceeded
    list icmp_type        bad-header
    list icmp_type        unknown-header-type
    option limit        1000/sec
    option family        ipv6
    option target        ACCEPT

config rule
    option name        Allow-IPSec-ESP
    option src         wan
    option dest        lan
    option proto        esp
    option target        ACCEPT

config rule
    option name        Allow-ISAKMP
```

```
    option src         wan
    option dest         lan
    option dest_port    500
    option proto        udp
    option target        ACCEPT

# include a file with users custom iptables rules
config include
    option path /etc/firewall.user

config rule
    option src 'wan'
    option proto 'esp'
    option target 'ACCEPT'

config rule
    option src 'wan'
    option proto 'udp'
    option dest_port '500'
    option target 'ACCEPT'

config rule
    option src 'wan'
    option proto 'udp'
    option dest_port '4500'
    option target 'ACCEPT'

config rule
    option src 'wan'
    option proto 'ah'
    option target 'ACCEPT'
```

ip route show table all

```
default via 192.168.0.253 dev eth0  table 220  proto static  src 10.31.2.1
default via 192.168.0.253 dev eth0  proto static  src 192.168.0.84
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.84
192.168.0.253 dev eth0  proto static  scope link  src 192.168.0.84
local 10.31.2.1 dev eth0  table local  proto kernel  scope host  src 10.31.2.1
broadcast 127.0.0.0 dev lo  table local  proto kernel  scope link  src 127.0.0.1
local 127.0.0.0/8 dev lo  table local  proto kernel  scope host  src 127.0.0.1
local 127.0.0.1 dev lo  table local  proto kernel  scope host  src 127.0.0.1
broadcast 127.255.255.255 dev lo  table local  proto kernel  scope link  src 127.0.0.1
broadcast 192.168.0.0 dev eth0  table local  proto kernel  scope link  src 192.168.0.84
local 192.168.0.84 dev eth0  table local  proto kernel  scope host  src 192.168.0.84
broadcast 192.168.0.255 dev eth0  table local  proto kernel  scope link  src 192.168.0.84
unreachable default dev lo  proto kernel  metric 4294967295  error -101 pref medium
unreachable fd43:2d28:a581::/48 dev lo  proto static  metric 2147483647  error -113 pref medium
fe80::/64 dev eth0  proto kernel  metric 256  pref medium
unreachable default dev lo  proto kernel  metric 4294967295  error -101 pref medium
local ::1 dev lo  table local  proto none  metric 0  pref medium
local fe80:: dev lo  table local  proto none  metric 0  pref medium
local fe80::204:81ff:fe86:8021 dev lo  table local  proto none  metric 0  pref medium
ff00::/8 dev eth0  table local  metric 256  pref medium
unreachable default dev lo  proto kernel  metric 4294967295  error -101 pref medium
```

ip address

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1490 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:04:81:86:80:21 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.84/24 brd 192.168.0.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 10.31.2.1/32 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::204:81ff:fe86:8021/64 scope link
       valid_lft forever preferred_lft forever
```

```
Mon, 2020-05-25 22:33 00[DMN] Starting IKE charon daemon (strongSwan 5.5.3, Linux 4.4.182, x86_64)
Mon, 2020-05-25 22:33 00[LIB] plugin 'test-vectors': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'ldap': loaded successfully
Mon, 2020-05-25 22:33 00[CFG] PKCS11 module '<name>' lacks library path
Mon, 2020-05-25 22:33 00[LIB] plugin 'pkcs11': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'aes': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'des': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'blowfish': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'rc2': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'sha2': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'sha1': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'md4': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'md5': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'random': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'nonce': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'x509': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'revocation': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'constraints': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'pubkey': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'pkcs1': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'pkcs7': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'pkcs8': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'pkcs12': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'pgp': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'dnskey': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'sshkey': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'pem': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'openssl': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'gcrypt': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'af-alg': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'fips-prf': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'gmp': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'curve25519': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'agent': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'xcbc': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'cmac': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'hmac': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'ctr': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'ccm': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'gcm': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] curl SSL backend 'mbedTLS/2.7.10' not supported, https:// disabled
Mon, 2020-05-25 22:33 00[LIB] plugin 'curl': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'mysql': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] using SQLite 3.26.0, thread safety 1
Mon, 2020-05-25 22:33 00[LIB] plugin 'sqlite': loaded successfully
Mon, 2020-05-25 22:33 00[CFG] loaded legacy entry attribute INTERNAL_IP4_DNS: 08:08:08:08
Mon, 2020-05-25 22:33 00[CFG] loaded legacy entry attribute INTERNAL_IP4_NBNS: 08:08:08:08
Mon, 2020-05-25 22:33 00[LIB] plugin 'attr': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'attr-sql': loaded successfully
Mon, 2020-05-25 22:33 00[CFG] disabling load-tester plugin, not configured
Mon, 2020-05-25 22:33 00[LIB] plugin 'load-tester': failed to load - load_tester_plugin_create returned NULL
Mon, 2020-05-25 22:33 00[LIB] plugin 'kernel-netlink': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'resolve': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'socket-default': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'connmark': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'forecast': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'farp': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'stroke': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'smp': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'sql': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'updown': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'eap-identity': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'eap-md5': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'eap-mschapv2': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'eap-radius': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'eap-tls': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'xauth-generic': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'xauth-eap': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'dhcp': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'ha': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'whitelist': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'led': loaded successfully
```

```
Mon, 2020-05-25 22:33 00[LIB] plugin 'duplicheck': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'coupling': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'uci' failed to load: Error relocating /usr/lib/ipsec/plugins/libstrongsw
an-uci.so: uci_lookup: symbol not found
Mon, 2020-05-25 22:33 00[LIB] plugin 'addrblock': loaded successfully
Mon, 2020-05-25 22:33 00[LIB] plugin 'unity': loaded successfully
Mon, 2020-05-25 22:33 00[KNL] known interfaces and IP addresses:
Mon, 2020-05-25 22:33 00[KNL]   lo
Mon, 2020-05-25 22:33 00[KNL]     127.0.0.1
Mon, 2020-05-25 22:33 00[KNL]     ::1
Mon, 2020-05-25 22:33 00[KNL]   eth0
Mon, 2020-05-25 22:33 00[KNL]     192.168.0.84
Mon, 2020-05-25 22:33 00[KNL]     fe80::204:81ff:fe86:8021
Mon, 2020-05-25 22:33 00[LIB] feature PUBKEY:BLISS in plugin 'pem' has unmet dependency: PUBKEY:BLISS
Mon, 2020-05-25 22:33 00[LIB] feature PUBKEY:DSA in plugin 'pem' has unmet dependency: PUBKEY:DSA
Mon, 2020-05-25 22:33 00[LIB] feature PRIVKEY:DSA in plugin 'pem' has unmet dependency: PRIVKEY:DSA
Mon, 2020-05-25 22:33 00[LIB] feature PRIVKEY:BLISS in plugin 'pem' has unmet dependency: PRIVKEY:BLISS
Mon, 2020-05-25 22:33 00[LIB] feature CERT_DECODE:OCSP_REQUEST in plugin 'pem' has unmet dependency: CERT_DECO
DE:OCSP_REQUEST
Mon, 2020-05-25 22:33 00[LIB] feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA3_224 in plugin 'gmp' has unmet dependenc
y: HASHER:HASH_SHA3_224
Mon, 2020-05-25 22:33 00[LIB] feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA3_256 in plugin 'gmp' has unmet dependenc
y: HASHER:HASH_SHA3_256
Mon, 2020-05-25 22:33 00[LIB] feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA3_384 in plugin 'gmp' has unmet dependenc
y: HASHER:HASH_SHA3_384
Mon, 2020-05-25 22:33 00[LIB] feature PRIVKEY_SIGN:RSA_EMSA_PKCS1_SHA3_512 in plugin 'gmp' has unmet dependenc
y: HASHER:HASH_SHA3_512
Mon, 2020-05-25 22:33 00[LIB] feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA3_224 in plugin 'gmp' has unmet dependen
cy: HASHER:HASH_SHA3_224
Mon, 2020-05-25 22:33 00[LIB] feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA3_256 in plugin 'gmp' has unmet dependen
cy: HASHER:HASH_SHA3_256
Mon, 2020-05-25 22:33 00[LIB] feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA3_384 in plugin 'gmp' has unmet dependen
cy: HASHER:HASH_SHA3_384
Mon, 2020-05-25 22:33 00[LIB] feature PUBKEY_VERIFY:RSA_EMSA_PKCS1_SHA3_512 in plugin 'gmp' has unmet dependen
cy: HASHER:HASH_SHA3_512
Mon, 2020-05-25 22:33 00[CFG] attr-sql plugin: database URI not set
Mon, 2020-05-25 22:33 00[LIB] feature CUSTOM:attr-sql in plugin 'attr-sql' failed to load
Mon, 2020-05-25 22:33 00[NET] using forecast interface eth0
Mon, 2020-05-25 22:33 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
Mon, 2020-05-25 22:33 00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
Mon, 2020-05-25 22:33 00[CFG]   loaded ca certificate "C=Self, O=Self, CN=Self" from '/etc/ipsec.d/cacerts/ca.
cert.pem'
Mon, 2020-05-25 22:33 00[CFG]   loaded ca certificate "C=CN, O=TrustAsia Technologies, Inc., OU=Domain Validat
ed SSL, CN=TrustAsia TLS RSA CA" from '/etc/ipsec.d/cacerts/ca1.cert.pem'
Mon, 2020-05-25 22:33 00[CFG]   loaded ca certificate "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert
Global Root CA" from '/etc/ipsec.d/cacerts/ca2.cert.pem'
Mon, 2020-05-25 22:33 00[CFG]   loaded ca certificate "C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limit
ed, CN=Sectigo RSA Domain Validation Secure Server CA" from '/etc/ipsec.d/cacerts/ca3.cert.pem'
Mon, 2020-05-25 22:33 00[CFG]   loaded ca certificate "C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Net
work, CN=USERTrust RSA Certification Authority" from '/etc/ipsec.d/cacerts/ca4.cert.pem'
Mon, 2020-05-25 22:33 00[CFG]   loaded ca certificate "C=SE, O=AddTrust AB, OU=AddTrust External TTP Network,
CN=AddTrust External CA Root" from '/etc/ipsec.d/cacerts/ca5.cert.pem'
Mon, 2020-05-25 22:33 00[LIB]   file coded in unknown format, discarded
Mon, 2020-05-25 22:33 00[LIB] building CRED_CERTIFICATE - X509 failed, tried 5 builders
Mon, 2020-05-25 22:33 00[CFG]   loading ca certificate from '/etc/ipsec.d/cacerts/ca6.cert.pem' failed
Mon, 2020-05-25 22:33 00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
Mon, 2020-05-25 22:33 00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'
Mon, 2020-05-25 22:33 00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
Mon, 2020-05-25 22:33 00[CFG] loading crls from '/etc/ipsec.d/crls'
Mon, 2020-05-25 22:33 00[CFG] loading secrets from '/etc/ipsec.secrets'
Mon, 2020-05-25 22:33 00[CFG]   loaded EAP secret for user1 %any
Mon, 2020-05-25 22:33 00[CFG] sql plugin: database URI not set
Mon, 2020-05-25 22:33 00[LIB] feature CUSTOM:sql in plugin 'sql' failed to load
Mon, 2020-05-25 22:33 00[CFG] loaded 0 RADIUS server configurations
Mon, 2020-05-25 22:33 00[CFG] HA config misses local/remote address
Mon, 2020-05-25 22:33 00[LIB] feature CUSTOM:ha in plugin 'ha' failed to load
Mon, 2020-05-25 22:33 00[CFG] coupling file path unspecified
Mon, 2020-05-25 22:33 00[LIB] feature CUSTOM:coupling in plugin 'coupling' failed to load
Mon, 2020-05-25 22:33 00[LIB] unloading plugin 'attr-sql' without loaded features
Mon, 2020-05-25 22:33 00[LIB] unloading plugin 'sql' without loaded features
Mon, 2020-05-25 22:33 00[LIB] unloading plugin 'ha' without loaded features
Mon, 2020-05-25 22:33 00[LIB] unloading plugin 'coupling' without loaded features
Mon, 2020-05-25 22:33 00[LIB] loaded plugins: charon test-vectors ldap pkcs11 aes des blowfish rc2 sha2 sha1 m
d4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl
```

```
gcrypt af-alg fips-prf gmp curve25519 agent xcbc cmac hmac ctr ccm gcm curl mysql sqlite attr kernel-netlink r
esolve socket-default connmark forecast farp stroke smp updown eap-identity eap-md5 eap-mschapv2 eap-radius ea
p-tls xauth-generic xauth-eap dhcp whitelist led duplicheck addrblock unity
Mon, 2020-05-25 22:33 00[LIB] unable to load 17 plugin features (13 due to unmet dependencies)
Mon, 2020-05-25 22:33 00[JOB] spawning 16 worker threads
Mon, 2020-05-25 22:33 01[LIB] created thread 01 [15257]
Mon, 2020-05-25 22:33 02[LIB] created thread 02 [15258]
Mon, 2020-05-25 22:33 04[LIB] created thread 04 [15260]
Mon, 2020-05-25 22:33 03[LIB] created thread 03 [15259]
Mon, 2020-05-25 22:33 05[LIB] created thread 05 [15261]
Mon, 2020-05-25 22:33 09[LIB] created thread 09 [15265]
Mon, 2020-05-25 22:33 07[LIB] created thread 07 [15262]
Mon, 2020-05-25 22:33 08[LIB] created thread 08 [15264]
Mon, 2020-05-25 22:33 12[LIB] created thread 12 [15269]
Mon, 2020-05-25 22:33 10[LIB] created thread 10 [15266]
Mon, 2020-05-25 22:33 16[LIB] created thread 16 [15272]
Mon, 2020-05-25 22:33 06[LIB] created thread 06 [15263]
Mon, 2020-05-25 22:33 13[LIB] created thread 13 [15268]
Mon, 2020-05-25 22:33 14[LIB] created thread 14 [15270]
Mon, 2020-05-25 22:33 11[LIB] created thread 11 [15267]
Mon, 2020-05-25 22:33 15[LIB] created thread 15 [15271]
Mon, 2020-05-25 22:33 09[CFG] received stroke: add connection 'Syd'
Mon, 2020-05-25 22:33 09[CFG] conn Syd
Mon, 2020-05-25 22:33 09[CFG]   left=%any
Mon, 2020-05-25 22:33 09[CFG]   leftsourceip=%config
Mon, 2020-05-25 22:33 09[CFG]   leftauth=eap-mschapv2
Mon, 2020-05-25 22:33 09[CFG]   right=mydomain
Mon, 2020-05-25 22:33 09[CFG]   rightsubnet=0.0.0.0/0
Mon, 2020-05-25 22:33 09[CFG]   rightauth=pubkey
Mon, 2020-05-25 22:33 09[CFG]   rightid=mydomain
Mon, 2020-05-25 22:33 09[CFG]   eap_identity=user1
Mon, 2020-05-25 22:33 09[CFG]   ike=aes256-sha1-modp2048!
Mon, 2020-05-25 22:33 09[CFG]   esp=aes256-sha1!
Mon, 2020-05-25 22:33 09[CFG]   dpddelay=30
Mon, 2020-05-25 22:33 09[CFG]   dpdtimeout=150
Mon, 2020-05-25 22:33 09[CFG]   sha256_96=no
Mon, 2020-05-25 22:33 09[CFG]   mediation=no
Mon, 2020-05-25 22:33 09[CFG]   keyexchange=ikev2
Mon, 2020-05-25 22:33 17[LIB] created thread 17 [15273]
Mon, 2020-05-25 22:33 09[KNL] 103.60.20.9 is not a local address or the interface is down
Mon, 2020-05-25 22:33 09[CFG] added configuration 'Syd'
Mon, 2020-05-25 22:33 02[CFG] received stroke: initiate 'Syd'
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> using 192.168.0.84 as address to reach 103.60.20.9/32
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing IKE_VENDOR task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing IKE_INIT task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing IKE_NATD task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing IKE_CERT_PRE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing IKE_AUTH task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing IKE_CERT_POST task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing IKE_CONFIG task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing IKE_AUTH_LIFETIME task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing IKE_MOBIKE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing IKE_ME task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> queueing CHILD_CREATE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> activating new tasks
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating IKE_VENDOR task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating IKE_INIT task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating IKE_NATD task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating IKE_CERT_PRE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating IKE_ME task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating IKE_AUTH task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating IKE_CERT_POST task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating IKE_CONFIG task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating CHILD_CREATE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating IKE_AUTH_LIFETIME task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1>   activating IKE_MOBIKE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> initiating IKE_SA Syd[1] to 103.60.20.9
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> IKE_SA Syd[1] state change: CREATED => CONNECTING
Mon, 2020-05-25 22:33 02[LIB] <Syd|1> size of DH secret exponent: 2047 bits
Mon, 2020-05-25 22:33 02[CFG] <Syd|1> configured proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_20
48
Mon, 2020-05-25 22:33 02[CFG] <Syd|1> sending supported signature hash algorithms: sha1 sha256 sha384 sha512 i
dentity
Mon, 2020-05-25 22:33 02[ENC] <Syd|1> 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) ]
```

```
Mon, 2020-05-25 22:33 02[NET] <Syd|1> sending packet: from 192.168.0.84[500] to 103.60.20.9[500] (466 bytes)
Mon, 2020-05-25 22:33 08[NET] <Syd|1> received packet: from 103.60.20.9[500] to 192.168.0.84[500] (472 bytes)
Mon, 2020-05-25 22:33 08[ENC] <Syd|1> parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRA
G_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> received FRAGMENTATION_SUPPORTED notify
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> received SIGNATURE_HASH_ALGORITHMS notify
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> received CHILDLESS_IKEV2_SUPPORTED notify
Mon, 2020-05-25 22:33 08[CFG] <Syd|1> selecting proposal:
Mon, 2020-05-25 22:33 08[CFG] <Syd|1>   proposal matches
Mon, 2020-05-25 22:33 08[CFG] <Syd|1> received proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
Mon, 2020-05-25 22:33 08[CFG] <Syd|1> configured proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_20
48
Mon, 2020-05-25 22:33 08[CFG] <Syd|1> selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
Mon, 2020-05-25 22:33 08[CFG] <Syd|1> received supported signature hash algorithms: sha256 sha384 sha512 ident
ity
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> local host is behind NAT, sending keep alives
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> remote host is behind NAT
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> reinitiating already active tasks
Mon, 2020-05-25 22:33 08[IKE] <Syd|1>   IKE_CERT_PRE task
Mon, 2020-05-25 22:33 08[IKE] <Syd|1>   IKE_AUTH task
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> sending cert request for "C=Self, O=Self, CN=Self"
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> sending cert request for "C=CN, O=TrustAsia Technologies, Inc., OU=Domai
n Validated SSL, CN=TrustAsia TLS RSA CA"
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> sending cert request for "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=
DigiCert Global Root CA"
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> sending cert request for "C=GB, ST=Greater Manchester, L=Salford, O=Sect
igo Limited, CN=Sectigo RSA Domain Validation Secure Server CA"
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> sending cert request for "C=US, ST=New Jersey, L=Jersey City, O=The USER
TRUST Network, CN=USERTrust RSA Certification Authority"
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> sending cert request for "C=SE, O=AddTrust AB, OU=AddTrust External TTP
Network, CN=AddTrust External CA Root"
Mon, 2020-05-25 22:33 08[CFG] <Syd|1> no IDi configured, fall back on IP address
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> building INTERNAL_IP4_DNS attribute
Mon, 2020-05-25 22:33 08[IKE] <Syd|1> establishing CHILD_SA Syd
Mon, 2020-05-25 22:33 08[CFG] <Syd|1> proposing traffic selectors for us:
Mon, 2020-05-25 22:33 08[CFG] <Syd|1>  0.0.0.0/0
Mon, 2020-05-25 22:33 08[CFG] <Syd|1> proposing traffic selectors for other:
Mon, 2020-05-25 22:33 08[CFG] <Syd|1>  0.0.0.0/0
Mon, 2020-05-25 22:33 08[CFG] <Syd|1> configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
Mon, 2020-05-25 22:33 08[KNL] <Syd|1> got SPI cfff95f1
Mon, 2020-05-25 22:33 08[ENC] <Syd|1> generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ IDr CPRQ(ADD
R DNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Mon, 2020-05-25 22:33 08[NET] <Syd|1> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (396 bytes)
Mon, 2020-05-25 22:33 16[NET] <Syd|1> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (1244 byte
s)
Mon, 2020-05-25 22:33 16[ENC] <Syd|1> parsed IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/ID ]
Mon, 2020-05-25 22:33 16[IKE] <Syd|1> received end entity cert "C=Self, O=Self, CN=Self"
Mon, 2020-05-25 22:33 16[CFG] <Syd|1>   using certificate "C=Self, O=Self, CN=Self"
Mon, 2020-05-25 22:33 16[CFG] <Syd|1>   certificate "C=Self, O=Self, CN=Self" key: 2048 bit RSA
Mon, 2020-05-25 22:33 16[CFG] <Syd|1>   using trusted ca certificate "C=Self, O=Self, CN=Self"
Mon, 2020-05-25 22:33 16[CFG] <Syd|1> checking certificate status of "C=Self, O=Self, CN=Self"
Mon, 2020-05-25 22:33 16[CFG] <Syd|1> ocsp check skipped, no ocsp found
Mon, 2020-05-25 22:33 16[CFG] <Syd|1> certificate status is not available
Mon, 2020-05-25 22:33 16[CFG] <Syd|1>   certificate "C=Self, O=Self, CN=Self" key: 2048 bit RSA
Mon, 2020-05-25 22:33 16[CFG] <Syd|1>   reached self-signed root ca with a path length of 0
Mon, 2020-05-25 22:33 16[IKE] <Syd|1> authentication of 'mydomain' with RSA_EMSA_PKCS1_SHA2_256 successful
Mon, 2020-05-25 22:33 16[IKE] <Syd|1> server requested EAP_IDENTITY (id 0x00), sending 'user1'
Mon, 2020-05-25 22:33 16[IKE] <Syd|1> reinitiating already active tasks
Mon, 2020-05-25 22:33 16[IKE] <Syd|1>   IKE_AUTH task
Mon, 2020-05-25 22:33 16[ENC] <Syd|1> generating IKE_AUTH request 2 [ EAP/RES/ID ]
Mon, 2020-05-25 22:33 16[NET] <Syd|1> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:33 06[NET] <Syd|1> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (108 bytes
)
Mon, 2020-05-25 22:33 06[ENC] <Syd|1> parsed IKE_AUTH response 2 [ EAP/REQ/MSCHAPV2 ]
Mon, 2020-05-25 22:33 06[IKE] <Syd|1> server requested EAP_MSCHAPV2 authentication (id 0x16)
Mon, 2020-05-25 22:33 06[IKE] <Syd|1> reinitiating already active tasks
Mon, 2020-05-25 22:33 06[IKE] <Syd|1>   IKE_AUTH task
Mon, 2020-05-25 22:33 06[ENC] <Syd|1> generating IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Mon, 2020-05-25 22:33 06[NET] <Syd|1> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (140 bytes)
Mon, 2020-05-25 22:33 13[NET] <Syd|1> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (140 bytes
)
Mon, 2020-05-25 22:33 13[ENC] <Syd|1> parsed IKE_AUTH response 3 [ EAP/REQ/MSCHAPV2 ]
Mon, 2020-05-25 22:33 13[IKE] <Syd|1> EAP-MS-CHAPv2 succeeded: 'Welcome2strongSwan'
Mon, 2020-05-25 22:33 13[IKE] <Syd|1> reinitiating already active tasks
Mon, 2020-05-25 22:33 13[IKE] <Syd|1>   IKE_AUTH task
```

```
Mon, 2020-05-25 22:33 13[ENC] <Syd|1> generating IKE_AUTH request 4 [ EAP/RES/MSCHAPV2 ]
Mon, 2020-05-25 22:33 13[NET] <Syd|1> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:33 14[NET] <Syd|1> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:33 14[ENC] <Syd|1> parsed IKE_AUTH response 4 [ EAP/SUCC ]
Mon, 2020-05-25 22:33 14[IKE] <Syd|1> EAP method EAP_MSCHAPV2 succeeded, MSK established
Mon, 2020-05-25 22:33 14[IKE] <Syd|1> reinitiating already active tasks
Mon, 2020-05-25 22:33 14[IKE] <Syd|1>   IKE_AUTH task
Mon, 2020-05-25 22:33 14[IKE] <Syd|1> authentication of '192.168.0.84' (myself) with EAP
Mon, 2020-05-25 22:33 14[ENC] <Syd|1> generating IKE_AUTH request 5 [ AUTH ]
Mon, 2020-05-25 22:33 14[NET] <Syd|1> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (92 bytes)
Mon, 2020-05-25 22:33 11[NET] <Syd|1> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (268 bytes
)
Mon, 2020-05-25 22:33 11[ENC] <Syd|1> parsed IKE_AUTH response 5 [ AUTH CPRP(ADDR DNS NBNS) SA TSi TSr N(MOBIK
E_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) ]
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> authentication of 'mydomain' with EAP successful
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> IKE_SA Syd[1] established between 192.168.0.84[192.168.0.84]...103.60.20
.9[mydomain]
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> IKE_SA Syd[1] state change: CONNECTING => ESTABLISHED
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> scheduling reauthentication in 9927s
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> maximum IKE_SA lifetime 10467s
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> processing INTERNAL_IP4_ADDRESS attribute
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> processing INTERNAL_IP4_DNS attribute
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> installing DNS server 8.8.8.8 to /etc/resolv.conf
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> processing INTERNAL_IP4_NBNS attribute
Mon, 2020-05-25 22:33 11[CFG] <Syd|1> handling INTERNAL_IP4_NBNS attribute failed
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> 192.168.0.84 is on interface eth0
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> installing new virtual IP 10.31.2.1
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> virtual IP 10.31.2.1 installed on eth0
Mon, 2020-05-25 22:33 11[CFG] <Syd|1> selecting proposal:
Mon, 2020-05-25 22:33 11[CFG] <Syd|1>   proposal matches
Mon, 2020-05-25 22:33 11[CFG] <Syd|1> received proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
Mon, 2020-05-25 22:33 11[CFG] <Syd|1> configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
Mon, 2020-05-25 22:33 11[CFG] <Syd|1> selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
Mon, 2020-05-25 22:33 11[CFG] <Syd|1> selecting traffic selectors for us:
Mon, 2020-05-25 22:33 11[CFG] <Syd|1>  config: 10.31.2.1/32, received: 10.31.2.1/32 => match: 10.31.2.1/32
Mon, 2020-05-25 22:33 11[CFG] <Syd|1> selecting traffic selectors for other:
Mon, 2020-05-25 22:33 11[CFG] <Syd|1>  config: 0.0.0.0/0, received: 0.0.0.0/0 => match: 0.0.0.0/0
Mon, 2020-05-25 22:33 11[CHD] <Syd|1> CHILD_SA Syd{1} state change: CREATED => INSTALLING
Mon, 2020-05-25 22:33 11[CHD] <Syd|1>   using AES_CBC for encryption
Mon, 2020-05-25 22:33 11[CHD] <Syd|1>   using HMAC_SHA1_96 for integrity
Mon, 2020-05-25 22:33 11[CHD] <Syd|1> adding inbound ESP SA
Mon, 2020-05-25 22:33 11[CHD] <Syd|1>   SPI 0xcfff95f1, src 103.60.20.9 dst 192.168.0.84
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> adding SAD entry with SPI cfff95f1 and reqid {1}
Mon, 2020-05-25 22:33 11[KNL] <Syd|1>   using encryption algorithm AES_CBC with key size 256
Mon, 2020-05-25 22:33 11[KNL] <Syd|1>   using integrity algorithm HMAC_SHA1_96 with key size 160
Mon, 2020-05-25 22:33 11[KNL] <Syd|1>   using replay window of 32 packets
Mon, 2020-05-25 22:33 11[CHD] <Syd|1> adding outbound ESP SA
Mon, 2020-05-25 22:33 11[CHD] <Syd|1>   SPI 0xc6ae1eba, src 192.168.0.84 dst 103.60.20.9
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> adding SAD entry with SPI c6ae1eba and reqid {1}
Mon, 2020-05-25 22:33 11[KNL] <Syd|1>   using encryption algorithm AES_CBC with key size 256
Mon, 2020-05-25 22:33 11[KNL] <Syd|1>   using integrity algorithm HMAC_SHA1_96 with key size 160
Mon, 2020-05-25 22:33 11[KNL] <Syd|1>   using replay window of 0 packets
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> adding policy 10.31.2.1/32 === 0.0.0.0/0 out [priority 583615, refcount
1]
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> adding policy 0.0.0.0/0 === 10.31.2.1/32 in [priority 383615, refcount 1
]
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> adding policy 0.0.0.0/0 === 10.31.2.1/32 fwd [priority 383615, refcount
1]
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> policy 10.31.2.1/32 === 0.0.0.0/0 out already exists, increasing refcoun
t
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> updating policy 10.31.2.1/32 === 0.0.0.0/0 out [priority 383615, refcoun
t 2]
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> getting a local address in traffic selector 10.31.2.1/32
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> using host 10.31.2.1
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> getting iface name for index 2
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> using 192.168.0.253 as nexthop and eth0 as dev to reach 103.60.20.9/32
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> installing route: 0.0.0.0/0 via 192.168.0.253 src 10.31.2.1 dev eth0
Mon, 2020-05-25 22:33 11[KNL] <Syd|1> getting iface index for eth0
Mon, 2020-05-25 22:33 11[CHD] <Syd|1> CHILD_SA Syd{1} state change: INSTALLING => INSTALLED
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> CHILD_SA Syd{1} established with SPIs cfff95f1_i c6ae1eba_o and TS 10.31
.2.1/32 === 0.0.0.0/0
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> peer supports MOBIKE
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> got additional MOBIKE peer address: 10.10.12.1
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> got additional MOBIKE peer address: fd02:8d05:5dd6::1
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> activating new tasks
```

```
Mon, 2020-05-25 22:33 11[IKE] <Syd|1> nothing to initiate
Mon, 2020-05-25 22:33 07[KNL] getting iface index for eth0
Mon, 2020-05-25 22:33 10[CFG] received stroke: terminate 'Syd'
Mon, 2020-05-25 22:33 07[IKE] <Syd|1> queueing IKE_DELETE task
Mon, 2020-05-25 22:33 07[IKE] <Syd|1> activating new tasks
Mon, 2020-05-25 22:33 07[IKE] <Syd|1>   activating IKE_DELETE task
Mon, 2020-05-25 22:33 07[IKE] <Syd|1> deleting IKE_SA Syd[1] between 192.168.0.84[192.168.0.84]...103.60.20.9[
mydomain]
Mon, 2020-05-25 22:33 07[IKE] <Syd|1> IKE_SA Syd[1] state change: ESTABLISHED => DELETING
Mon, 2020-05-25 22:33 07[IKE] <Syd|1> sending DELETE for IKE_SA Syd[1]
Mon, 2020-05-25 22:33 07[ENC] <Syd|1> generating INFORMATIONAL request 6 [ D ]
Mon, 2020-05-25 22:33 07[NET] <Syd|1> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:33 02[NET] <Syd|1> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:33 02[ENC] <Syd|1> parsed INFORMATIONAL response 6 [ ]
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> IKE_SA deleted
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> IKE_SA Syd[1] state change: DELETING => DESTROYING
Mon, 2020-05-25 22:33 02[IKE] <Syd|1> removing DNS server 8.8.8.8 from /etc/resolv.conf
Mon, 2020-05-25 22:33 02[CHD] <Syd|1> CHILD_SA Syd{1} state change: INSTALLED => DESTROYING
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> deleting policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> policy still used by another CHILD_SA, not removed
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> updating policy 10.31.2.1/32 === 0.0.0.0/0 out [priority 583615, refcoun
t 1]
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> deleting policy 0.0.0.0/0 === 10.31.2.1/32 in
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> deleting policy 0.0.0.0/0 === 10.31.2.1/32 fwd
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> deleting policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> getting iface index for eth0
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> deleting SAD entry with SPI cfff95f1
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> deleted SAD entry with SPI cfff95f1
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> deleting SAD entry with SPI c6ae1eba
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> deleted SAD entry with SPI c6ae1eba
Mon, 2020-05-25 22:33 02[KNL] <Syd|1> deleting virtual IP 10.31.2.1
Mon, 2020-05-25 22:33 08[CFG] received stroke: initiate 'Syd'
Mon, 2020-05-25 22:33 02[KNL] <Syd|2> using 192.168.0.84 as address to reach 103.60.20.9/32
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing IKE_VENDOR task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing IKE_INIT task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing IKE_NATD task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing IKE_CERT_PRE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing IKE_AUTH task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing IKE_CERT_POST task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing IKE_CONFIG task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing IKE_AUTH_LIFETIME task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing IKE_MOBIKE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing IKE_ME task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> queueing CHILD_CREATE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> activating new tasks
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating IKE_VENDOR task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating IKE_INIT task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating IKE_NATD task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating IKE_CERT_PRE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating IKE_ME task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating IKE_AUTH task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating IKE_CERT_POST task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating IKE_CONFIG task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating CHILD_CREATE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating IKE_AUTH_LIFETIME task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2>   activating IKE_MOBIKE task
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> initiating IKE_SA Syd[2] to 103.60.20.9
Mon, 2020-05-25 22:33 02[IKE] <Syd|2> IKE_SA Syd[2] state change: CREATED => CONNECTING
Mon, 2020-05-25 22:33 02[LIB] <Syd|2> size of DH secret exponent: 2047 bits
Mon, 2020-05-25 22:33 02[CFG] <Syd|2> configured proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_20
48
Mon, 2020-05-25 22:33 02[CFG] <Syd|2> sending supported signature hash algorithms: sha1 sha256 sha384 sha512 i
dentity
Mon, 2020-05-25 22:33 02[ENC] <Syd|2> 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) ]
Mon, 2020-05-25 22:33 02[NET] <Syd|2> sending packet: from 192.168.0.84[500] to 103.60.20.9[500] (466 bytes)
Mon, 2020-05-25 22:33 09[NET] <Syd|2> received packet: from 103.60.20.9[500] to 192.168.0.84[500] (472 bytes)
Mon, 2020-05-25 22:33 09[ENC] <Syd|2> parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRA
G_SUP) N(HASH_ALG) N(CHDLESS_SUP) N(MULT_AUTH) ]
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> received FRAGMENTATION_SUPPORTED notify
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> received SIGNATURE_HASH_ALGORITHMS notify
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> received CHILDLESS_IKEV2_SUPPORTED notify
Mon, 2020-05-25 22:33 09[CFG] <Syd|2> selecting proposal:
Mon, 2020-05-25 22:33 09[CFG] <Syd|2>   proposal matches
Mon, 2020-05-25 22:33 09[CFG] <Syd|2> received proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
```

```
Mon, 2020-05-25 22:33 09[CFG] <Syd|2> configured proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_20
48
Mon, 2020-05-25 22:33 09[CFG] <Syd|2> selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
Mon, 2020-05-25 22:33 09[CFG] <Syd|2> received supported signature hash algorithms: sha256 sha384 sha512 ident
ity
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> local host is behind NAT, sending keep alives
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> remote host is behind NAT
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> reinitiating already active tasks
Mon, 2020-05-25 22:33 09[IKE] <Syd|2>   IKE_CERT_PRE task
Mon, 2020-05-25 22:33 09[IKE] <Syd|2>   IKE_AUTH task
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> sending cert request for "C=Self, O=Self, CN=Self"
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> sending cert request for "C=CN, O=TrustAsia Technologies, Inc., OU=Domai
n Validated SSL, CN=TrustAsia TLS RSA CA"
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> sending cert request for "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=
DigiCert Global Root CA"
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> sending cert request for "C=GB, ST=Greater Manchester, L=Salford, O=Sect
igo Limited, CN=Sectigo RSA Domain Validation Secure Server CA"
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> sending cert request for "C=US, ST=New Jersey, L=Jersey City, O=The USER
TRUST Network, CN=USERTrust RSA Certification Authority"
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> sending cert request for "C=SE, O=AddTrust AB, OU=AddTrust External TTP
Network, CN=AddTrust External CA Root"
Mon, 2020-05-25 22:33 09[CFG] <Syd|2> no IDi configured, fall back on IP address
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> building INTERNAL_IP4_DNS attribute
Mon, 2020-05-25 22:33 09[IKE] <Syd|2> establishing CHILD_SA Syd
Mon, 2020-05-25 22:33 09[CFG] <Syd|2> proposing traffic selectors for us:
Mon, 2020-05-25 22:33 09[CFG] <Syd|2>  0.0.0.0/0
Mon, 2020-05-25 22:33 09[CFG] <Syd|2> proposing traffic selectors for other:
Mon, 2020-05-25 22:33 09[CFG] <Syd|2>  0.0.0.0/0
Mon, 2020-05-25 22:33 09[CFG] <Syd|2> configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
Mon, 2020-05-25 22:33 09[KNL] <Syd|2> got SPI c64cc1f2
Mon, 2020-05-25 22:33 09[ENC] <Syd|2> generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ IDr CPRQ(ADD
R DNS) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Mon, 2020-05-25 22:33 09[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (396 bytes)
Mon, 2020-05-25 22:33 07[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (1244 byte
s)
Mon, 2020-05-25 22:33 07[ENC] <Syd|2> parsed IKE_AUTH response 1 [ IDr CERT AUTH EAP/REQ/ID ]
Mon, 2020-05-25 22:33 07[IKE] <Syd|2> received end entity cert "C=Self, O=Self, CN=Self"
Mon, 2020-05-25 22:33 07[CFG] <Syd|2>   using certificate "C=Self, O=Self, CN=Self"
Mon, 2020-05-25 22:33 07[CFG] <Syd|2>   certificate "C=Self, O=Self, CN=Self" key: 2048 bit RSA
Mon, 2020-05-25 22:33 07[CFG] <Syd|2>   using trusted ca certificate "C=Self, O=Self, CN=Self"
Mon, 2020-05-25 22:33 07[CFG] <Syd|2> checking certificate status of "C=Self, O=Self, CN=Self"
Mon, 2020-05-25 22:33 07[CFG] <Syd|2> ocsp check skipped, no ocsp found
Mon, 2020-05-25 22:33 07[CFG] <Syd|2> certificate status is not available
Mon, 2020-05-25 22:33 07[CFG] <Syd|2>   certificate "C=Self, O=Self, CN=Self" key: 2048 bit RSA
Mon, 2020-05-25 22:33 07[CFG] <Syd|2>   reached self-signed root ca with a path length of 0
Mon, 2020-05-25 22:33 07[IKE] <Syd|2> authentication of 'mydomain' with RSA_EMSA_PKCS1_SHA2_256 successful
Mon, 2020-05-25 22:33 07[IKE] <Syd|2> server requested EAP_IDENTITY (id 0x00), sending 'user1'
Mon, 2020-05-25 22:33 07[IKE] <Syd|2> reinitiating already active tasks
Mon, 2020-05-25 22:33 07[IKE] <Syd|2>   IKE_AUTH task
Mon, 2020-05-25 22:33 07[ENC] <Syd|2> generating IKE_AUTH request 2 [ EAP/RES/ID ]
Mon, 2020-05-25 22:33 07[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:33 10[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (108 bytes
)
Mon, 2020-05-25 22:33 10[ENC] <Syd|2> parsed IKE_AUTH response 2 [ EAP/REQ/MSCHAPV2 ]
Mon, 2020-05-25 22:33 10[IKE] <Syd|2> server requested EAP_MSCHAPV2 authentication (id 0xB7)
Mon, 2020-05-25 22:33 10[IKE] <Syd|2> reinitiating already active tasks
Mon, 2020-05-25 22:33 10[IKE] <Syd|2>   IKE_AUTH task
Mon, 2020-05-25 22:33 10[ENC] <Syd|2> generating IKE_AUTH request 3 [ EAP/RES/MSCHAPV2 ]
Mon, 2020-05-25 22:33 10[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (140 bytes)
Mon, 2020-05-25 22:33 16[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (140 bytes
)
Mon, 2020-05-25 22:33 16[ENC] <Syd|2> parsed IKE_AUTH response 3 [ EAP/REQ/MSCHAPV2 ]
Mon, 2020-05-25 22:33 16[IKE] <Syd|2> EAP-MS-CHAPv2 succeeded: 'Welcome2strongSwan'
Mon, 2020-05-25 22:33 16[IKE] <Syd|2> reinitiating already active tasks
Mon, 2020-05-25 22:33 16[IKE] <Syd|2>   IKE_AUTH task
Mon, 2020-05-25 22:33 16[ENC] <Syd|2> generating IKE_AUTH request 4 [ EAP/RES/MSCHAPV2 ]
Mon, 2020-05-25 22:33 16[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:33 06[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:33 06[ENC] <Syd|2> parsed IKE_AUTH response 4 [ EAP/SUCC ]
Mon, 2020-05-25 22:33 06[IKE] <Syd|2> EAP method EAP_MSCHAPV2 succeeded, MSK established
Mon, 2020-05-25 22:33 06[IKE] <Syd|2> reinitiating already active tasks
Mon, 2020-05-25 22:33 06[IKE] <Syd|2>   IKE_AUTH task
Mon, 2020-05-25 22:33 06[IKE] <Syd|2> authentication of '192.168.0.84' (myself) with EAP
Mon, 2020-05-25 22:33 06[ENC] <Syd|2> generating IKE_AUTH request 5 [ AUTH ]
Mon, 2020-05-25 22:33 06[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (92 bytes)
```

```
Mon, 2020-05-25 22:33 13[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (268 bytes
)
Mon, 2020-05-25 22:33 13[ENC] <Syd|2> parsed IKE_AUTH response 5 [ AUTH CPRP(ADDR DNS NBNS) SA TSi TSr N(MOBIK
E_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) ]
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> authentication of 'mydomain' with EAP successful
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> IKE_SA Syd[2] established between 192.168.0.84[192.168.0.84]...103.60.20
.9[mydomain]
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> IKE_SA Syd[2] state change: CONNECTING => ESTABLISHED
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> scheduling reauthentication in 10148s
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> maximum IKE_SA lifetime 10688s
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> processing INTERNAL_IP4_ADDRESS attribute
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> processing INTERNAL_IP4_DNS attribute
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> installing DNS server 8.8.8.8 to /etc/resolv.conf
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> processing INTERNAL_IP4_NBNS attribute
Mon, 2020-05-25 22:33 13[CFG] <Syd|2> handling INTERNAL_IP4_NBNS attribute failed
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> 192.168.0.84 is on interface eth0
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> installing new virtual IP 10.31.2.1
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> virtual IP 10.31.2.1 installed on eth0
Mon, 2020-05-25 22:33 13[CFG] <Syd|2> selecting proposal:
Mon, 2020-05-25 22:33 13[CFG] <Syd|2>   proposal matches
Mon, 2020-05-25 22:33 13[CFG] <Syd|2> received proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
Mon, 2020-05-25 22:33 13[CFG] <Syd|2> configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
Mon, 2020-05-25 22:33 13[CFG] <Syd|2> selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
Mon, 2020-05-25 22:33 13[CFG] <Syd|2> selecting traffic selectors for us:
Mon, 2020-05-25 22:33 13[CFG] <Syd|2>  config: 10.31.2.1/32, received: 10.31.2.1/32 => match: 10.31.2.1/32
Mon, 2020-05-25 22:33 13[CFG] <Syd|2> selecting traffic selectors for other:
Mon, 2020-05-25 22:33 13[CFG] <Syd|2>  config: 0.0.0.0/0, received: 0.0.0.0/0 => match: 0.0.0.0/0
Mon, 2020-05-25 22:33 13[CHD] <Syd|2> CHILD_SA Syd{2} state change: CREATED => INSTALLING
Mon, 2020-05-25 22:33 13[CHD] <Syd|2>   using AES_CBC for encryption
Mon, 2020-05-25 22:33 13[CHD] <Syd|2>   using HMAC_SHA1_96 for integrity
Mon, 2020-05-25 22:33 13[CHD] <Syd|2> adding inbound ESP SA
Mon, 2020-05-25 22:33 13[CHD] <Syd|2>   SPI 0xc64cc1f2, src 103.60.20.9 dst 192.168.0.84
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> adding SAD entry with SPI c64cc1f2 and reqid {2}
Mon, 2020-05-25 22:33 13[KNL] <Syd|2>   using encryption algorithm AES_CBC with key size 256
Mon, 2020-05-25 22:33 13[KNL] <Syd|2>   using integrity algorithm HMAC_SHA1_96 with key size 160
Mon, 2020-05-25 22:33 13[KNL] <Syd|2>   using replay window of 32 packets
Mon, 2020-05-25 22:33 13[CHD] <Syd|2> adding outbound ESP SA
Mon, 2020-05-25 22:33 13[CHD] <Syd|2>   SPI 0xc4222f1e, src 192.168.0.84 dst 103.60.20.9
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> adding SAD entry with SPI c4222f1e and reqid {2}
Mon, 2020-05-25 22:33 13[KNL] <Syd|2>   using encryption algorithm AES_CBC with key size 256
Mon, 2020-05-25 22:33 13[KNL] <Syd|2>   using integrity algorithm HMAC_SHA1_96 with key size 160
Mon, 2020-05-25 22:33 13[KNL] <Syd|2>   using replay window of 0 packets
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> adding policy 10.31.2.1/32 === 0.0.0.0/0 out [priority 583615, refcount
1]
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> adding policy 0.0.0.0/0 === 10.31.2.1/32 in [priority 383615, refcount 1
]
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> adding policy 0.0.0.0/0 === 10.31.2.1/32 fwd [priority 383615, refcount
1]
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> policy 10.31.2.1/32 === 0.0.0.0/0 out already exists, increasing refcoun
t
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> updating policy 10.31.2.1/32 === 0.0.0.0/0 out [priority 383615, refcoun
t 2]
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> getting a local address in traffic selector 10.31.2.1/32
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> using host 10.31.2.1
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> getting iface name for index 2
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> using 192.168.0.253 as nexthop and eth0 as dev to reach 103.60.20.9/32
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> installing route: 0.0.0.0/0 via 192.168.0.253 src 10.31.2.1 dev eth0
Mon, 2020-05-25 22:33 13[KNL] <Syd|2> getting iface index for eth0
Mon, 2020-05-25 22:33 13[CHD] <Syd|2> CHILD_SA Syd{2} state change: INSTALLING => INSTALLED
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> CHILD_SA Syd{2} established with SPIs c64cc1f2_i c4222f1e_o and TS 10.31
.2.1/32 === 0.0.0.0/0
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> peer supports MOBIKE
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> got additional MOBIKE peer address: 10.10.12.1
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> got additional MOBIKE peer address: fd02:8d05:5dd6::1
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> activating new tasks
Mon, 2020-05-25 22:33 13[IKE] <Syd|2> nothing to initiate
Mon, 2020-05-25 22:33 07[KNL] getting iface index for eth0
Mon, 2020-05-25 22:33 02[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:33 02[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:33 15[CFG] proposing traffic selectors for us:
Mon, 2020-05-25 22:33 15[CFG]  dynamic
Mon, 2020-05-25 22:33 15[CFG] proposing traffic selectors for other:
Mon, 2020-05-25 22:33 15[CFG]  0.0.0.0/0
Mon, 2020-05-25 22:33 15[KNL] <Syd|2> querying SAD entry with SPI c64cc1f2
Mon, 2020-05-25 22:33 15[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
```

```
Mon, 2020-05-25 22:33 11[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:33 11[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:33 11[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
Mon, 2020-05-25 22:34 14[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:34 14[ENC] <Syd|2> parsed INFORMATIONAL request 0 [ ]
Mon, 2020-05-25 22:34 14[ENC] <Syd|2> generating INFORMATIONAL response 0 [ ]
Mon, 2020-05-25 22:34 14[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:34 11[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:34 11[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:34 13[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:34 13[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:34 13[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
Mon, 2020-05-25 22:34 16[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:34 16[ENC] <Syd|2> parsed INFORMATIONAL request 1 [ ]
Mon, 2020-05-25 22:34 16[ENC] <Syd|2> generating INFORMATIONAL response 1 [ ]
Mon, 2020-05-25 22:34 16[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:34 06[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:34 06[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:34 13[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:34 13[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:34 13[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
Mon, 2020-05-25 22:35 10[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:35 10[ENC] <Syd|2> parsed INFORMATIONAL request 2 [ ]
Mon, 2020-05-25 22:35 10[ENC] <Syd|2> generating INFORMATIONAL response 2 [ ]
Mon, 2020-05-25 22:35 10[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:35 14[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:35 14[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:35 13[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:35 13[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:35 13[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
Mon, 2020-05-25 22:35 11[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:35 11[ENC] <Syd|2> parsed INFORMATIONAL request 3 [ ]
Mon, 2020-05-25 22:35 11[ENC] <Syd|2> generating INFORMATIONAL response 3 [ ]
Mon, 2020-05-25 22:35 11[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:35 08[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:35 08[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:35 07[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:35 07[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:35 07[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
Mon, 2020-05-25 22:36 14[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:36 14[ENC] <Syd|2> parsed INFORMATIONAL request 4 [ ]
Mon, 2020-05-25 22:36 14[ENC] <Syd|2> generating INFORMATIONAL response 4 [ ]
Mon, 2020-05-25 22:36 14[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:36 06[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:36 06[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:36 09[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:36 09[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:36 09[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
Mon, 2020-05-25 22:36 07[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:36 07[ENC] <Syd|2> parsed INFORMATIONAL request 5 [ ]
Mon, 2020-05-25 22:36 07[ENC] <Syd|2> generating INFORMATIONAL response 5 [ ]
Mon, 2020-05-25 22:36 07[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:36 13[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:36 13[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:36 15[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:36 15[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:36 15[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
Mon, 2020-05-25 22:37 14[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:37 14[ENC] <Syd|2> parsed INFORMATIONAL request 6 [ ]
Mon, 2020-05-25 22:37 14[ENC] <Syd|2> generating INFORMATIONAL response 6 [ ]
Mon, 2020-05-25 22:37 14[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:37 13[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:37 13[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:37 09[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:37 09[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:37 09[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
Mon, 2020-05-25 22:37 02[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:37 02[ENC] <Syd|2> parsed INFORMATIONAL request 7 [ ]
Mon, 2020-05-25 22:37 02[ENC] <Syd|2> generating INFORMATIONAL response 7 [ ]
Mon, 2020-05-25 22:37 02[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:37 02[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:37 02[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:37 11[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:37 11[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:37 11[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
```

```
Mon, 2020-05-25 22:38 16[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:38 16[ENC] <Syd|2> parsed INFORMATIONAL request 8 [ ]
Mon, 2020-05-25 22:38 16[ENC] <Syd|2> generating INFORMATIONAL response 8 [ ]
Mon, 2020-05-25 22:38 16[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:38 02[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:38 02[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:38 11[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:38 11[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:38 11[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
Mon, 2020-05-25 22:38 10[NET] <Syd|2> received packet: from 103.60.20.9[4500] to 192.168.0.84[4500] (76 bytes)
Mon, 2020-05-25 22:38 10[ENC] <Syd|2> parsed INFORMATIONAL request 9 [ ]
Mon, 2020-05-25 22:38 10[ENC] <Syd|2> generating INFORMATIONAL response 9 [ ]
Mon, 2020-05-25 22:38 10[NET] <Syd|2> sending packet: from 192.168.0.84[4500] to 103.60.20.9[4500] (76 bytes)
Mon, 2020-05-25 22:38 15[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:38 15[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:38 11[KNL] <Syd|2> querying policy 10.31.2.1/32 === 0.0.0.0/0 out
Mon, 2020-05-25 22:38 11[KNL] <Syd|2> querying SAD entry with SPI c4222f1e
Mon, 2020-05-25 22:38 11[IKE] <Syd|2> sending keep alive to 103.60.20.9[4500]
```

#5 - 25.05.2020 14:58 - Tobias Brunner

Only packets with the virtual IP as source address will match the IPsec policies. So you have to exclude the tunneled traffic from the masquerading NAT rule (see ForwardingAndSplitTunneling).

#6 - 25.05.2020 15:47 - John YU

Tobias Brunner wrote:

> Only packets with the virtual IP as source address will match the IPsec policies. So you have to exclude the tunneled traffic from the masquerading NAT rule (see ForwardingAndSplitTunneling).

Great! Strongswan in openwrt can go through VPN connection now(checked by command "traceroute"). Thanks!

But now another problem is:
All the devices connected to this router can't go online now.
Previously before I exclude the tunneled traffic from the masquerading NAT rule (execute the command "iptables -t nat -I POSTROUTING -m policy --pol ipsec --dir out -j ACCEPT"), they can go online, just not go through VPN connection.

Could you please tell me how to fix it? Thank you once more!

#7 - 26.05.2020 10:27 - Tobias Brunner

> All the devices connected to this router can't go online now.
> Previously before I exclude the tunneled traffic from the masquerading NAT rule (execute the command "iptables -t nat -I POSTROUTING -m policy --pol ipsec --dir out -j ACCEPT"), they can go online, just not go through VPN connection.

Hm, that rule should not affect traffic originating from source addresses other than the virtual IP (i.e. forwarded traffic). Did you change anything else? Maybe check all the rules with iptables-save (if available). Not directly related, but you probably also have to find a way to make that rule permanent in OpenWrt's config somehow.

#8 - 30.05.2020 14:46 - John YU

Tobias Brunner wrote:

> > All the devices connected to this router can't go online now.
> > Previously before I exclude the tunneled traffic from the masquerading NAT rule (execute the command "iptables -t nat -I POSTROUTING -m policy --pol ipsec --dir out -j ACCEPT"), they can go online, just not go through VPN connection.
>
> Hm, that rule should not affect traffic originating from source addresses other than the virtual IP (i.e. forwarded traffic). Did you change anything else? Maybe check all the rules with iptables-save (if available). Not directly related, but you probably also have to find a way to make that rule permanent in OpenWrt's config somehow.

I tried command "iptables-save". Please help me have a look. Thanks.

```
root@client:/tmp# iptables-save
# Generated by iptables-save v1.4.21 on Sat May 30 22:43:55 2020
*nat
:PREROUTING ACCEPT [182:39143]
```

```
:INPUT ACCEPT [12:2028]
:OUTPUT ACCEPT [41:3058]
:POSTROUTING ACCEPT [7:446]
:postrouting_lan_rule - [0:0]
:postrouting_rule - [0:0]
:postrouting_wan_rule - [0:0]
:prerouting_lan_rule - [0:0]
:prerouting_rule - [0:0]
:prerouting_wan_rule - [0:0]
:zone_lan_postrouting - [0:0]
:zone_lan_prerouting - [0:0]
:zone_wan_postrouting - [0:0]
:zone_wan_prerouting - [0:0]
-A PREROUTING -m comment --comment "!fw3: user chain for prerouting" -j prerouting_rule
-A PREROUTING -i br-lan -m comment --comment "!fw3" -j zone_lan_prerouting
-A PREROUTING -i eth0.2 -m comment --comment "!fw3" -j zone_wan_prerouting
-A POSTROUTING -m policy --dir out --pol ipsec -j ACCEPT
-A POSTROUTING -m comment --comment "!fw3: user chain for postrouting" -j postrouting_rule
-A POSTROUTING -o br-lan -m comment --comment "!fw3" -j zone_lan_postrouting
-A POSTROUTING -o eth0.2 -m comment --comment "!fw3" -j zone_wan_postrouting
-A zone_lan_postrouting -m comment --comment "!fw3: user chain for postrouting" -j postrouting_lan_rule
-A zone_lan_prerouting -m comment --comment "!fw3: user chain for prerouting" -j prerouting_lan_rule
-A zone_wan_postrouting -m comment --comment "!fw3: user chain for postrouting" -j postrouting_wan_rule
-A zone_wan_postrouting -m comment --comment "!fw3" -j MASQUERADE
-A zone_wan_prerouting -m comment --comment "!fw3: user chain for prerouting" -j prerouting_wan_rule
COMMIT
# Completed on Sat May 30 22:43:55 2020
# Generated by iptables-save v1.4.21 on Sat May 30 22:43:55 2020
*mangle
:PREROUTING ACCEPT [444:76506]
:INPUT ACCEPT [274:39391]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [196:25572]
:POSTROUTING ACCEPT [218:27989]
-A FORWARD -o eth0.2 -p tcp -m tcp --tcp-flags SYN,RST SYN -m comment --comment "!fw3: wan (mtu_fix)" -j TCPMS
S --clamp-mss-to-pmtu
COMMIT
# Completed on Sat May 30 22:43:55 2020
# Generated by iptables-save v1.4.21 on Sat May 30 22:43:55 2020
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:forwarding_lan_rule - [0:0]
:forwarding_rule - [0:0]
:forwarding_wan_rule - [0:0]
:input_lan_rule - [0:0]
:input_rule - [0:0]
:input_wan_rule - [0:0]
:output_lan_rule - [0:0]
:output_rule - [0:0]
:output_wan_rule - [0:0]
:reject - [0:0]
:syn_flood - [0:0]
:zone_lan_dest_ACCEPT - [0:0]
:zone_lan_forward - [0:0]
:zone_lan_input - [0:0]
:zone_lan_output - [0:0]
:zone_lan_src_ACCEPT - [0:0]
:zone_wan_dest_ACCEPT - [0:0]
:zone_wan_forward - [0:0]
:zone_wan_input - [0:0]
:zone_wan_output - [0:0]
:zone_wan_src_ACCEPT - [0:0]
-A INPUT -i lo -m comment --comment "!fw3" -j ACCEPT
-A INPUT -m comment --comment "!fw3: user chain for input" -j input_rule
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "!fw3" -j ACCEPT
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m comment --comment "!fw3" -j syn_flood
-A INPUT -i br-lan -m comment --comment "!fw3" -j zone_lan_input
-A INPUT -i eth0.2 -m comment --comment "!fw3" -j zone_wan_input
-A FORWARD -m comment --comment "!fw3: user chain for forwarding" -j forwarding_rule
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "!fw3" -j ACCEPT
-A FORWARD -i br-lan -m comment --comment "!fw3" -j zone_lan_forward
-A FORWARD -i eth0.2 -m comment --comment "!fw3" -j zone_wan_forward
-A OUTPUT -o lo -m comment --comment "!fw3" -j ACCEPT
```

```
-A OUTPUT -m comment --comment "!fw3: user chain for output" -j output_rule
-A OUTPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "!fw3" -j ACCEPT
-A OUTPUT -o br-lan -m comment --comment "!fw3" -j zone_lan_output
-A OUTPUT -o eth0.2 -m comment --comment "!fw3" -j zone_wan_output
-A reject -p tcp -m comment --comment "!fw3" -j REJECT --reject-with tcp-reset
-A reject -m comment --comment "!fw3" -j REJECT --reject-with icmp-port-unreachable
-A syn_flood -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m limit --limit 25/sec --limit-burst 50 -m comment
 --comment "!fw3" -j RETURN
-A syn_flood -m comment --comment "!fw3" -j DROP
-A zone_lan_dest_ACCEPT -o br-lan -m comment --comment "!fw3" -j ACCEPT
-A zone_lan_forward -m comment --comment "!fw3: user chain for forwarding" -j forwarding_lan_rule
-A zone_lan_forward -m comment --comment "!fw3: forwarding lan -> wan" -j zone_wan_dest_ACCEPT
-A zone_lan_forward -m conntrack --ctstate DNAT -m comment --comment "!fw3: Accept port forwards" -j ACCEPT
-A zone_lan_forward -m comment --comment "!fw3" -j zone_lan_dest_ACCEPT
-A zone_lan_input -m comment --comment "!fw3: user chain for input" -j input_lan_rule
-A zone_lan_input -m conntrack --ctstate DNAT -m comment --comment "!fw3: Accept port redirections" -j ACCEPT
-A zone_lan_input -m comment --comment "!fw3" -j zone_lan_src_ACCEPT
-A zone_lan_output -m comment --comment "!fw3: user chain for output" -j output_lan_rule
-A zone_lan_output -m comment --comment "!fw3" -j zone_lan_dest_ACCEPT
-A zone_lan_src_ACCEPT -i br-lan -m conntrack --ctstate NEW,UNTRACKED -m comment --comment "!fw3" -j ACCEPT
-A zone_wan_dest_ACCEPT -o eth0.2 -m conntrack --ctstate INVALID -m comment --comment "!fw3: Prevent NAT leaka
ge" -j DROP
-A zone_wan_dest_ACCEPT -o eth0.2 -m comment --comment "!fw3" -j ACCEPT
-A zone_wan_forward -m comment --comment "!fw3: user chain for forwarding" -j forwarding_wan_rule
-A zone_wan_forward -p esp -m comment --comment "!fw3: Allow-IPSec-ESP" -j zone_lan_dest_ACCEPT
-A zone_wan_forward -p udp -m udp --dport 500 -m comment --comment "!fw3: Allow-ISAKMP" -j zone_lan_dest_ACCEP
T
-A zone_wan_forward -m conntrack --ctstate DNAT -m comment --comment "!fw3: Accept port forwards" -j ACCEPT
-A zone_wan_forward -m comment --comment "!fw3" -j zone_wan_dest_ACCEPT
-A zone_wan_input -m comment --comment "!fw3: user chain for input" -j input_wan_rule
-A zone_wan_input -p udp -m udp --dport 68 -m comment --comment "!fw3: Allow-DHCP-Renew" -j ACCEPT
-A zone_wan_input -p icmp -m icmp --icmp-type 8 -m comment --comment "!fw3: Allow-Ping" -j ACCEPT
-A zone_wan_input -p igmp -m comment --comment "!fw3: Allow-IGMP" -j ACCEPT
-A zone_wan_input -p esp -m comment --comment "!fw3: @rule[9]" -j ACCEPT
-A zone_wan_input -p udp -m udp --dport 500 -m comment --comment "!fw3: @rule[10]" -j ACCEPT
-A zone_wan_input -p udp -m udp --dport 4500 -m comment --comment "!fw3: @rule[11]" -j ACCEPT
-A zone_wan_input -p ah -m comment --comment "!fw3: @rule[12]" -j ACCEPT
-A zone_wan_input -m conntrack --ctstate DNAT -m comment --comment "!fw3: Accept port redirections" -j ACCEPT
-A zone_wan_input -m comment --comment "!fw3" -j zone_wan_src_ACCEPT
-A zone_wan_output -m comment --comment "!fw3: user chain for output" -j output_wan_rule
-A zone_wan_output -m comment --comment "!fw3" -j zone_wan_dest_ACCEPT
-A zone_wan_src_ACCEPT -i eth0.2 -m conntrack --ctstate NEW,UNTRACKED -m comment --comment "!fw3" -j ACCEPT
COMMIT
# Completed on Sat May 30 22:43:55 2020
```

#9 - 02.06.2020 10:29 - Tobias Brunner

As I said before, the inserted rule should only affect traffic that matches the policy, which is not the case for source IPs other than the virtual IP. So unless the MASQUERADE rule maps the packets to the virtual IP, there shouldn't be an issue. Are packets from the LAN natted to the virtual IP and sent to the VPN server? (Check on the server or via traffic counters.) If so, you could try the *charon.install_virtual_ip_on* option to install the virtual IP on e.g. *lo* so the MASQUERADE rule is not tempted to use it.

#10 - 30.09.2020 13:43 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No feedback