strongSwan - Issue #2678

Phase 1 issue

01.06.2018 12:40 - Jeff McKeon

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.6.1	**Resolution:**	

Description

Hello, I'm trying to get a system to connect to a Zyxel USG 60 IPSec L2TP Server.

Its failing on phase 1 somehow. I've double checked the PSK and settings on both sides but there must be something I'm missing.
NOTE: Actual public IP addresses have been changed for the sake of this post.

Verson: Linux strongSwan U5.6.1/K3.10.0-862.2.3.el7.x86_64

From the StrongSwan Side I see this:

```
peer not responding, trying again (3/3)
initiating Main Mode IKE_SA vpnconn1[1] to 47.21.145.234
generating ID_PROT request 0 [ SA V V V V V ]
sending packet: from 45.63.13.137[500] to 47.21.145.234[500] (240 bytes)
sending retransmit 1 of request message ID 0, seq 1
sending packet: from 45.63.13.137[500] to 47.21.145.234[500] (240 bytes)
sending retransmit 2 of request message ID 0, seq 1
sending packet: from 45.63.13.137[500] to 47.21.145.234[500] (240 bytes)
sending retransmit 3 of request message ID 0, seq 1
sending packet: from 45.63.13.137[500] to 47.21.145.234[500] (240 bytes)
sending retransmit 4 of request message ID 0, seq 1
sending packet: from 45.63.13.137[500] to 47.21.145.234[500] (240 bytes)
sending retransmit 5 of request message ID 0, seq 1
sending packet: from 45.63.13.137[500] to 47.21.145.234[500] (240 bytes)
```

The Zyxel shows it's sending responses and doing a TCPDump on the StrongSwan side shows they are being received:

```
[root@freepbx strongswan]# tcpdump udp port 500
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
06:32:29.274563 IP zyxel.net.isakmp > xx.xx.xx.xx.xxxx.com.isakmp: isakmp: phase 1 ? ident
06:32:37.802463 IP xx.xx.xx.xx.xxxx.com.isakmp > zyxel.net.isakmp.net.isakmp: isakmp: phase 1 I id
ent
06:32:37.855213 IP zyxel.net.isakmp.net.isakmp > xx.xx.xx.xx.xxxx.com.isakmp: isakmp: phase 1 R id
ent
06:32:45.177450 IP zyxel.net.isakmp.net.isakmp > xx.xx.xx.xx.xxxx.com.isakmp: isakmp: phase 1 R id
ent
```

ipsec.conf:

```
# ipsec.conf - strongSwan IPsec configuration file

config setup
        charondebug="ike 5"

conn vpnconn1
    type=tunnel
    authby=secret

    right=zyxel.net.isakmp
    rightsubnet=192.168.1.0/24                  #to connect only to one Client, use i.e. 192.168.1.
20/32
```

```
    rightid=server

    left=%defaultroute                                    #if ZyWall has a dynamic IP address,
 use zywall.dyndns.org
    leftsubnet=xx.xx.xx.xx/32                          #to connect only to one Server, use i.e. 10.
0.0.20/32
    rightid=client

    keyexchange=ikev1
    ike=aes256-sha512-modp1024
    esp=aes256-sha512-modp1024                          #change to "esp=aes256-sha512-modp1024" f
or version 5 compatibility!
#   auth=esp                                           #remove for version 5 compatibility!
    auto=add
```

History

#1 - 01.06.2018 14:31 - Tobias Brunner

- Description updated

- Category set to configuration

- Status changed from New to Feedback

- Affected version changed from 5.6.3 to 5.6.1

The daemon apparently does not receive the packet. Make sure you don't block UDP port 500 (and 4500 in case there is a NAT).

Also your config makes no sense if you actually want to use L2TP, which requires a host-to-host tunnel, usually limited to specific UDP ports (possibly even in transport mode), not a host-to-subnet tunnel (which is fine if you just use plain IPsec, but not if you want to use L2TP).

#2 - 05.06.2018 13:52 - Jeff McKeon

Ok, Makes sense. I do have the firewall ports open and it tcpdump shows that the packets are being received, just that they seem to be ignored by the daemon.

Is there a config example for the connection I'm trying to accomplish?

Essentially I want this linux host to connect to a VPN server via IPsec L2TP and have access to all devices on the remote subnet.

#3 - 05.06.2018 14:53 - Tobias Brunner

> I do have the firewall ports open and it tcpdump shows that the packets are being received, just that they seem to be ignored by the daemon.

Seeing a packet in tcpdump doesn't mean it is received by the userland, so make really sure your firewall rules don't block this traffic (post the output of iptables-save if you are unsure). If the response packets really are not blocked it would be rather strange that the daemon doesn't receive them (unless you e.g. configured *charon.interfaces_use*, or there is some other process that has a UDP socket open on the same port). You could also increase the log level for the *net* group to 2 to see if the socket receives a packet.

> Is there a config example for the connection I'm trying to accomplish?

No, we don't provide support for L2TP (but you might find configs by other users trying to do something similar, either in the archive of the user mailing list or the issue tracker).

#4 - 05.06.2018 15:25 - Jeff McKeon

```
# Generated by iptables-save v1.4.21 on Tue Jun  5 09:23:42 2018
*nat
:PREROUTING ACCEPT [1870:112284]
:INPUT ACCEPT [333:30438]
:OUTPUT ACCEPT [58944:3674928]
:POSTROUTING ACCEPT [52109:3126638]
:masq-input - [0:0]
:masq-output - [0:0]
-A POSTROUTING -j masq-input
-A POSTROUTING -j masq-output
-A POSTROUTING -m mark --mark 0x3/0x3 -j MASQUERADE
-A masq-input -j MARK --set-xmark 0x1/0xffffffff
-A masq-output -o eth0 -j MARK --set-xmark 0x2/0x2
```

```
COMMIT
# Completed on Tue Jun  5 09:23:42 2018
# Generated by iptables-save v1.4.21 on Tue Jun  5 09:23:42 2018
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1003415:2055947300]
:fpbx-rtp - [0:0]
:fpbxattacker - [0:0]
:fpbxblacklist - [0:0]
:fpbxfirewall - [0:0]
:fpbxhosts - [0:0]
:fpbxinterfaces - [0:0]
:fpbxknownreg - [0:0]
:fpbxlogdrop - [0:0]
:fpbxnets - [0:0]
:fpbxratelimit - [0:0]
:fpbxregistrations - [0:0]
:fpbxreject - [0:0]
:fpbxrfw - [0:0]
:fpbxshortblock - [0:0]
:fpbxsignalling - [0:0]
:fpbxsmarthosts - [0:0]
:fpbxsvc-chansip - [0:0]
:fpbxsvc-ftp - [0:0]
:fpbxsvc-http - [0:0]
:fpbxsvc-https - [0:0]
:fpbxsvc-iax - [0:0]
:fpbxsvc-isymphony - [0:0]
:fpbxsvc-nfs - [0:0]
:fpbxsvc-pjsip - [0:0]
:fpbxsvc-provis - [0:0]
:fpbxsvc-provis_ssl - [0:0]
:fpbxsvc-restapps - [0:0]
:fpbxsvc-restapps_ssl - [0:0]
:fpbxsvc-smb - [0:0]
:fpbxsvc-ssh - [0:0]
:fpbxsvc-tftp - [0:0]
:fpbxsvc-ucp - [0:0]
:fpbxsvc-vpn - [0:0]
:fpbxsvc-webrtc - [0:0]
:fpbxsvc-xmpp - [0:0]
:fpbxsvc-zulu - [0:0]
:rejsvc-nfs - [0:0]
:rejsvc-smb - [0:0]
:zone-external - [0:0]
:zone-internal - [0:0]
:zone-other - [0:0]
:zone-trusted - [0:0]
-A INPUT -j fpbxfirewall
-A fpbx-rtp -p udp -m udp --dport 10000:20000 -j ACCEPT
-A fpbx-rtp -p udp -m udp --dport 4000:4999 -j ACCEPT
-A fpbxattacker -m recent --set --name ATTACKER --mask 255.255.255.255 --rsource
-A fpbxattacker -j DROP
-A fpbxfirewall -i lo -j ACCEPT
-A fpbxfirewall -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A fpbxfirewall -p icmp -j ACCEPT
-A fpbxfirewall -d 255.255.255.255/32 -j ACCEPT
-A fpbxfirewall -m pkttype --pkt-type multicast -j ACCEPT
-A fpbxfirewall -p udp -m udp --sport 67:68 --dport 67:68 -j ACCEPT
-A fpbxfirewall -j fpbx-rtp
-A fpbxfirewall -j fpbxblacklist
-A fpbxfirewall -j fpbxsignalling
-A fpbxfirewall -j fpbxsmarthosts
-A fpbxfirewall -j fpbxregistrations
-A fpbxfirewall -j fpbxnets
-A fpbxfirewall -j fpbxhosts
-A fpbxfirewall -j fpbxinterfaces
-A fpbxfirewall -j fpbxreject
-A fpbxfirewall -m mark --mark 0x2/0x2 -j fpbxrfw
-A fpbxfirewall -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A fpbxfirewall -j fpbxlogdrop
-A fpbxhosts -s 127.0.0.1/32 -j zone-trusted
-A fpbxinterfaces -i eth0 -j zone-external
-A fpbxinterfaces -i tun0 -j zone-internal
```

```
-A fpbxknownreg -m recent --remove --name REPEAT --mask 255.255.255.255 --rsource
-A fpbxknownreg -m recent --remove --name ATTACKER --mask 255.255.255.255 --rsource
-A fpbxknownreg -m mark --mark 0x1/0x1 -j ACCEPT
-A fpbxknownreg -j fpbxsvc-ucp
-A fpbxknownreg -j fpbxsvc-zulu
-A fpbxknownreg -j fpbxsvc-restapps
-A fpbxknownreg -j fpbxsvc-restapps_ssl
-A fpbxknownreg -j fpbxsvc-provis
-A fpbxknownreg -j fpbxsvc-provis_ssl
-A fpbxlogdrop -j DROP
-A fpbxnets -s 47.21.145.234/32 -j zone-trusted
-A fpbxnets -s 47.21.145.0/24 -j zone-trusted
-A fpbxratelimit -m mark --mark 0x4/0x4 -j ACCEPT
-A fpbxratelimit -m recent --rcheck --seconds 90 --hitcount 1 --name WHITELIST --mask 255.255.255.255 --rsourc
e -j ACCEPT
-A fpbxratelimit -m state --state NEW -m recent --set --name REPEAT --mask 255.255.255.255 --rsource
-A fpbxratelimit -m state --state NEW -m recent --set --name DISCOVERED --mask 255.255.255.255 --rsource
-A fpbxratelimit -j LOG
-A fpbxratelimit -m recent --rcheck --seconds 86400 --hitcount 1 --name ATTACKER --mask 255.255.255.255 --rsou
rce -j fpbxattacker
-A fpbxratelimit -m recent --rcheck --seconds 86400 --hitcount 100 --name REPEAT --mask 255.255.255.255 --rsou
rce -j fpbxattacker
-A fpbxratelimit -m recent --rcheck --seconds 3600 --hitcount 50 --name REPEAT --mask 255.255.255.255 --rsourc
e -j fpbxattacker
-A fpbxratelimit -m recent --rcheck --seconds 60 --hitcount 10 --name REPEAT --mask 255.255.255.255 --rsource
-j fpbxshortblock
-A fpbxratelimit -j ACCEPT
-A fpbxregistrations -s 192.240.151.100/32 -j fpbxknownreg
-A fpbxregistrations -s 64.136.174.20/32 -j fpbxknownreg
-A fpbxregistrations -s 209.166.128.200/32 -j fpbxknownreg
-A fpbxregistrations -s 64.136.173.22/32 -j fpbxknownreg
-A fpbxregistrations -s 64.136.174.30/32 -j fpbxknownreg
-A fpbxregistrations -s 64.136.173.31/32 -j fpbxknownreg
-A fpbxregistrations -s 209.166.154.70/32 -j fpbxknownreg
-A fpbxregistrations -s 47.21.145.234/32 -j fpbxknownreg
-A fpbxreject -j rejsvc-nfs
-A fpbxreject -j rejsvc-smb
-A fpbxrfw -m recent --rcheck --seconds 90 --hitcount 1 --name WHITELIST --mask 255.255.255.255 --rsource -j A
CCEPT
-A fpbxrfw -m recent --set --name REPEAT --mask 255.255.255.255 --rsource
-A fpbxrfw -m recent --set --name DISCOVERED --mask 255.255.255.255 --rsource
-A fpbxrfw -m recent --rcheck --seconds 10 --hitcount 50 --name REPEAT --mask 255.255.255.255 --rsource -j fpb
xattacker
-A fpbxrfw -m recent --rcheck --seconds 86400 --hitcount 1 --name ATTACKER --mask 255.255.255.255 --rsource -j
 fpbxattacker
-A fpbxrfw -m recent --rcheck --seconds 60 --hitcount 10 --name SIGNALLING --mask 255.255.255.255 --rsource -j
 fpbxshortblock
-A fpbxrfw -m recent --set --name SIGNALLING --mask 255.255.255.255 --rsource
-A fpbxrfw -m recent --rcheck --seconds 86400 --hitcount 100 --name REPEAT --mask 255.255.255.255 --rsource -j
 fpbxattacker
-A fpbxrfw -j ACCEPT
-A fpbxshortblock -m recent --set --name CLAMPED --mask 255.255.255.255 --rsource
-A fpbxshortblock -j REJECT --reject-with icmp-port-unreachable
-A fpbxsignalling -p udp -m udp --dport 5160 -j MARK --set-xmark 0x1/0xffffffff
-A fpbxsignalling -p udp -m udp --dport 5060 -j MARK --set-xmark 0x1/0xffffffff
-A fpbxsmarthosts -s 64.136.174.30/32 -m mark --mark 0x1/0x1 -j ACCEPT
-A fpbxsmarthosts -s 64.136.173.31/32 -m mark --mark 0x1/0x1 -j ACCEPT
-A fpbxsmarthosts -s 192.240.151.100/32 -m mark --mark 0x1/0x1 -j ACCEPT
-A fpbxsmarthosts -s 209.166.154.70/32 -m mark --mark 0x1/0x1 -j ACCEPT
-A fpbxsmarthosts -s 209.166.128.200/32 -m mark --mark 0x1/0x1 -j ACCEPT
-A fpbxsmarthosts -s 64.136.173.22/32 -m mark --mark 0x1/0x1 -j ACCEPT
-A fpbxsmarthosts -s 64.136.174.20/32 -m mark --mark 0x1/0x1 -j ACCEPT
-A fpbxsvc-chansip -p udp -m udp --dport 5160 -j ACCEPT
-A fpbxsvc-ftp -p tcp -m tcp --dport 21 -j ACCEPT
-A fpbxsvc-http -p tcp -m tcp --dport 80 -j ACCEPT
-A fpbxsvc-https -p tcp -m tcp --dport 443 -j ACCEPT
-A fpbxsvc-iax -p udp -m udp --dport 4569 -j ACCEPT
-A fpbxsvc-pjsip -p udp -m udp --dport 5060 -j ACCEPT
-A fpbxsvc-pjsip -p tcp -m tcp --dport 8088 -j ACCEPT
-A fpbxsvc-provis -p tcp -m tcp --dport 84 -j ACCEPT
-A fpbxsvc-restapps -p tcp -m tcp --dport 82 -j ACCEPT
-A fpbxsvc-ssh -p tcp -m tcp --dport 22 -j ACCEPT
-A fpbxsvc-tftp -p udp -m udp --dport 69 -j ACCEPT
-A fpbxsvc-ucp -p tcp -m tcp --dport 81 -j ACCEPT
-A fpbxsvc-ucp -p tcp -m tcp --dport 8001 -j ACCEPT
```

```
-A fpbxsvc-ucp -p tcp -m tcp --dport 8003 -j ACCEPT
-A fpbxsvc-vpn -p udp -m udp --dport 1194 -j ACCEPT
-A fpbxsvc-webrtc -p tcp -m tcp --dport 8088 -j ACCEPT
-A fpbxsvc-webrtc -p tcp -m tcp --dport 8089 -j ACCEPT
-A fpbxsvc-xmpp -p tcp -m tcp --dport 5222 -j ACCEPT
-A fpbxsvc-zulu -p tcp -m tcp --dport 8002 -j fpbxratelimit
-A zone-external -m mark --mark 0x10/0x10
-A zone-external -j fpbxsvc-ucp
-A zone-external -j fpbxsvc-pjsip
-A zone-external -j fpbxsvc-chansip
-A zone-external -j fpbxsvc-zulu
-A zone-external -j fpbxsvc-vpn
-A zone-external -j fpbxsvc-xmpp
-A zone-internal -m mark --mark 0x4/0x4
-A zone-internal -j fpbxsvc-ssh
-A zone-internal -j fpbxsvc-http
-A zone-internal -j fpbxsvc-https
-A zone-internal -j fpbxsvc-ucp
-A zone-internal -j fpbxsvc-pjsip
-A zone-internal -j fpbxsvc-chansip
-A zone-internal -j fpbxsvc-iax
-A zone-internal -j fpbxsvc-webrtc
-A zone-internal -j fpbxsvc-provis
-A zone-internal -j fpbxsvc-vpn
-A zone-internal -j fpbxsvc-restapps
-A zone-internal -j fpbxsvc-xmpp
-A zone-internal -j fpbxsvc-ftp
-A zone-internal -j fpbxsvc-tftp
-A zone-other -m mark --mark 0x8/0x8
-A zone-other -j fpbxsvc-ucp
-A zone-other -j fpbxsvc-provis
-A zone-other -j fpbxsvc-vpn
-A zone-other -j fpbxsvc-xmpp
-A zone-trusted -j ACCEPT
COMMIT
```

##

logging level 2

```
[root@freepbx strongswan]# tail -f /var/log/charon.log
Jun  5 09:21:50 01[JOB] got event, queuing job for execution
Jun  5 09:21:50 01[JOB] no events, waiting
Jun  5 09:21:50 12[MGR] checkout IKEv1 SA with SPIs af6196bf777afbf6_i 0000000000000000_r
Jun  5 09:21:50 12[MGR] IKE_SA ikev1-l2tp-ipsec-userauth-in-l2tp[1] successfully checked out
Jun  5 09:21:50 12[IKE] <ikev1-l2tp-ipsec-userauth-in-l2tp|1> sending retransmit 2 of request message ID 0, se
q 1
Jun  5 09:21:50 12[NET] <ikev1-l2tp-ipsec-userauth-in-l2tp|1> sending packet: from xx.xx.13.137[500] to xx.xx.
145.234[500] (176 bytes)
Jun  5 09:21:50 12[MGR] <ikev1-l2tp-ipsec-userauth-in-l2tp|1> checkin IKE_SA ikev1-l2tp-ipsec-userauth-in-l2tp
[1]
Jun  5 09:21:50 12[MGR] <ikev1-l2tp-ipsec-userauth-in-l2tp|1> checkin of IKE_SA successful
Jun  5 09:21:50 04[NET] sending packet: from 45.63.13.137[500] to xx.xx.145.234[500]
Jun  5 09:21:50 01[JOB] next event in 12s 959ms, waiting
Jun  5 09:22:03 01[JOB] got event, queuing job for execution
Jun  5 09:22:03 01[JOB] no events, waiting
Jun  5 09:22:03 13[MGR] checkout IKEv1 SA with SPIs af6196bf777afbf6_i 0000000000000000_r
Jun  5 09:22:03 13[MGR] IKE_SA ikev1-l2tp-ipsec-userauth-in-l2tp[1] successfully checked out
```

#5 - 05.06.2018 19:25 - Tobias Brunner

I don't feel like going through all these rules, but you might want to simplify them (e.g. reduce their number, avoid marks and NAT and other special stuff) just to rule out that iptables causes this somehow.

#6 - 07.06.2018 17:05 - Jeff McKeon

Ok, I dialed it back and dropped the L2TP. I have successfully set up a IPsec VPN between my linux box (StrongSwan) and my Zyxel USG60 firewall.

eht1 10.1.96.4 <Linux> eth0 XXX.XXX.13.137 <<----IPSEC---->> XXX.XXX.145.234 <ZyXel USG60> eth1 192.168.1.1

ipsec.conf:

1. /etc/ipsec.conf - strongSwan IPsec configuration file

config setup

conn %default
ikelifetime=60m
keylife=20m
rekeymargin=3m
keyingtries=1
keyexchange=ikev1
authby=secret

conn net-net
left=XXX.XXX.13.137
leftsubnet=10.1.96.0/20
leftid=XXX.XXX.13.137
leftfirewall=yes
right=XXX.XXX.145.234
rightsubnet=192.168.1.0/24
rightid=XXX.XXX.145.234
ike=aes256-sha1-modp1024!
esp=aes256-sha1-modp1024!
auto=add

IPTABLES:

Chain FORWARD (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 192.168.1.0/24 10.1.96.0/20 policy match dir in pol ipsec reqid 1 proto esp
ACCEPT all -- 10.1.96.0/20 192.168.1.0/24 policy match dir out pol ipsec reqid 1 proto esp

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

Chain fail2ban-BadBots (1 references)
target prot opt source destination
RETURN all -- anywhere anywhere

Chain fail2ban-FTP (1 references)
target prot opt source destination
RETURN all -- anywhere anywhere

Chain fail2ban-SIP (2 references)
target prot opt source destination
RETURN all -- anywhere anywhere
RETURN all -- anywhere anywhere

Chain fail2ban-SSH (1 references)
target prot opt source destination
RETURN all -- anywhere anywhere

Chain fail2ban-apache-auth (1 references)
target prot opt source destination
RETURN all -- anywhere anywhere

Chain fail2ban-recidive (1 references)
target prot opt source destination
RETURN all -- anywhere anywhere

ROUTE:
[root@freepbx strongswan]# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default gateway 0.0.0.0 UG 0 0 0 eth0
10.1.96.0 0.0.0.0 255.255.240.0 U 0 0 0 eth1
10.8.0.0 0.0.0.0 255.255.255.0 U 0 0 0 tun0
XXX.XXX.12.0 0.0.0.0 255.255.254.0 U 0 0 0 eth0
link-local 0.0.0.0 255.255.0.0 U 1002 0 0 eth0
link-local 0.0.0.0 255.255.0.0 U 1003 0 0 eth1

THE PROBLEM:

I can ping from the linux box to 192.168.1.1 (Zyxel LAN interface) and get responses no problem.
if I try to ping any other IP on the 192.168.1.0 subnet I see them coming in to my Zyxel and being forwarded to the inside device but the linux box receives nothing back.

if I try to ping from the 192.168.1.0 subnet to 10.1.96.4 (linux eth1) the Zyxel firewall is sending the traffic down the tunnel but not getting any

response back.

I suspect this is a route issue on the Linux side?

#7 - 07.06.2018 18:25 - Noel Kuntze

Hi,

You need to fix your nat rules.
And please provide the outputs ip address, ip rule and ip route show table all.

The net-tools are insufficient to deal with modern Linux. They're fine on *BSD, but not on Linux.

#8 - 07.06.2018 20:06 - Jeff McKeon

IP ROUTE SHOW TABLE ALL

192.168.1.0/24 via XXX.XXX.12.1 dev eth0 table 220 proto static src 10.1.96.4
default via XXX.XXX.12.1 dev eth0
10.1.96.0/20 dev eth1 proto kernel scope link src 10.1.96.4
10.8.0.0/24 dev tun0 proto kernel scope link src 10.8.0.1
XXX.XXX.12.0/23 dev eth0 proto kernel scope link src XXX.XXX.13.137
169.254.0.0/16 dev eth0 scope link metric 1002
169.254.0.0/16 dev eth1 scope link metric 1003
broadcast 10.1.96.0 dev eth1 table local proto kernel scope link src 10.1.96.4
local 10.1.96.4 dev eth1 table local proto kernel scope host src 10.1.96.4
broadcast 10.1.111.255 dev eth1 table local proto kernel scope link src 10.1.96.4
broadcast 10.8.0.0 dev tun0 table local proto kernel scope link src 10.8.0.1
local 10.8.0.1 dev tun0 table local proto kernel scope host src 10.8.0.1
broadcast 10.8.0.255 dev tun0 table local proto kernel scope link src 10.8.0.1
broadcast XXX.XXX.12.0 dev eth0 table local proto kernel scope link src XXX.XXX.13.137
local XXX.XXX.13.137 dev eth0 table local proto kernel scope host src XXX.XXX.13.137
broadcast XXX.XXX.13.255 dev eth0 table local proto kernel scope link src XXX.XXX.13.137
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
unreachable default dev lo proto kernel metric 4294967295 error -101 pref medium
unreachable ::/96 dev lo metric 1024 error -113 pref medium
unreachable ::ffff:0.0.0.0/96 dev lo metric 1024 error -113 pref medium
unreachable 2002:a00::/24 dev lo metric 1024 error -113 pref medium
unreachable 2002:7f00::/24 dev lo metric 1024 error -113 pref medium
unreachable 2002:a9fe::/32 dev lo metric 1024 error -113 pref medium
unreachable 2002:ac10::/28 dev lo metric 1024 error -113 pref medium
unreachable 2002:c0a8::/32 dev lo metric 1024 error -113 pref medium
unreachable 2002:e000::/19 dev lo metric 1024 error -113 pref medium
unreachable 3ffe:ffff::/32 dev lo metric 1024 error -113 pref medium
fe80::/64 dev tun0 proto kernel metric 256 pref medium
fe80::/64 dev eth0 proto kernel metric 256 pref medium
fe80::/64 dev eth1 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 unspec metric 0 pref medium
local fe80::5400:1ff:fe76:2c5 dev lo table local proto unspec metric 0 pref medium
local fe80::5800:1ff:fe76:2c5 dev lo table local proto unspec metric 0 pref medium
local fe80::dc44:87b6:9003:bab9 dev lo table local proto unspec metric 0 pref medium
ff00::/8 dev tun0 table local metric 256 pref medium
ff00::/8 dev eth0 table local metric 256 pref medium
ff00::/8 dev eth1 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 1000
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 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 56:00:01:76:02:c5 brd ff:ff:ff:ff:ff:ff
inet XXX.XXX.13.137/23 brd XXX.XXX.13.255 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::5400:1ff:fe76:2c5/64 scope link
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000

link/ether 5a:00:01:76:02:c5 brd ff:ff:ff:ff:ff:ff
inet 10.1.96.4/20 brd 10.1.111.255 scope global eth1
valid_lft forever preferred_lft forever
inet6 fe80::5800:1ff:fe76:2c5/64 scope link
valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 100
link/none
inet 10.8.0.1/24 brd 10.8.0.255 scope global tun0
valid_lft forever preferred_lft forever
inet6 fe80::dc44:87b6:9003:bab9/64 scope link flags 800
valid_lft forever preferred_lft forever

IP RULE:

0: from all lookup local
220: from all lookup 220
32766: from all lookup main
32767: from all lookup default