strongSwan - Issue #3687

Strongswan ipsec do not forward package to host

02.02.2021 01:20 - Jimmy Zhang

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	network / firewall		
Affected version:	5.7.2	**Resolution:**	

Description

Hi,

We have setup a VPN site to site IPSec tunnel between Juniper vSRX and Strongswan. We can see tunnel is up. However, we can't ping from the from host within source subnet to target host from the target subnet. Just wondering if I can get any help here?

Here is the Strongswan config:

```
[root@testfarm-uat-vpn ~]# swanctl -l
gw-gw: #2, ESTABLISHED, IKEv2, 00c43d5f587f83a5_i 910c55aafc68da88_r*
  local  '52.116.126.118' @ 10.128.2.177[4500]
  remote '52.117.245.227' @ 52.117.245.227[4500]
  AES_CBC-256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_384
  established 1866s ago, reauth in 81879s
  net-net: #3, reqid 2, INSTALLED, TUNNEL-in-UDP, ESP:AES_GCM_16-256/ECP_384
    installed 1848s ago, rekeying in 1481s, expires in 2112s
    in  c5ff6625,  27337 bytes,   330 packets,    85s ago
    out 6747d190,   3725 bytes,    16 packets,   937s ago
    local  10.128.2.128/26
    remote 10.36.6.0/26
[root@testfarm-uat-vpn ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[[root@testfarm-uat-vpn ~]# ip route list table 220
10.36.6.0/26 via 10.128.2.129 dev eth0 proto static src 10.128.2.177
[root@testfarm-uat-vpn ~]#
```

We opened all firewall from Juniper end. From tcpdump, we can see ping/ssh package from source IP reached to Strongswan, but the package does not reach to the target host.

Strongswan tcpdump:

```
[root@testfarm-uat-vpn conf.d]# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[root@testfarm-uat-vpn conf.d]# tcpdump -vv -i eth0 host 10.36.6.18
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes

18:00:47.768796 IP (tos 0x0, ttl 63, id 19381, offset 0, flags [DF], proto ICMP (1), length 84)
    10.36.6.18 > 10.128.2.132: ICMP echo request, id 3504, seq 1, length 64
18:00:47.768871 IP (tos 0x0, ttl 62, id 19381, offset 0, flags [DF], proto ICMP (1), length 84)
    10.36.6.18 > 10.128.2.132: ICMP echo request, id 3504, seq 1, length 64
```

tcpdump from target host is showing no package arrived.

```
[root@testfarm-uat-vpn conf.d]# cat swanctl.JimmyTest.conf
```

```
connections {

   gw-gw {
      local_addrs  = 10.128.2.177
      remote_addrs = 52.117.245.227

      local {
         auth = psk
      }
      remote {
         auth = psk
      }
      children {
         net-net {
            local_ts  = 10.128.2.128/26
            remote_ts = 10.36.6.0/26
            rekey_time = 3600
            rekey_bytes = 500000000
            rekey_packets = 1000000
            esp_proposals = aes256gcm128-ecp384
         }
      }
      version = 2
      mobike = no
      reauth_time = 86400
      proposals = aes256-sha256-ecp384
   }
}

secrets {
   ike{
      secret = ***********
   }
}
```

History

#1 - 02.02.2021 11:21 - Tobias Brunner

- Description updated

- Category set to network / firewall

- Status changed from New to Feedback

As the packet counters show you, packets are exchanged. So the tunnel seems to work. Might be a forwarding/firewall/NAT issue somewhere on or beyond the two IPsec gateways.

#2 - 02.02.2021 12:56 - Jimmy Zhang

So how do we check if the forwording setup is correct on this Strongswan node?
We don't use NAT on this config yet.
Also as showing, firewall iptables on this node is accepted for all.

#3 - 02.02.2021 14:40 - Tobias Brunner

Maybe your routing is messed up or there is some other problem in your network (e.g. another firewall/router) or the target device itself blocks the traffic. I really don't know, you have to debug that yourself.