strongSwan - Issue #3576

strongswan on openwrt virtual ip inside ipsec tunnel

24.09.2020 10:37 - Francesco Galletti

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	network / firewall		
Affected version:	5.9.0	**Resolution:**	

Description

Hello, we have an ipsec vpn beetween many Mikrotik routers and one central firewall in a datacenter. All this mikrotik routers that have openwrt operating system have the same LAN ip adress 192.168.8.1 and one device connected in the LAN 192.168.8.10
we decided to split all the Mikrotik routers in many small lans in the 11.0.0.0 subnet and the central firewall have the local network 172.16.0.0/16
so all Mikrotik starts a connection having a fake local lan someting like this:

MIKROTIK1 eth0 real 192.168.8.1 - fake 11.0.0.16/28 -> ipsec to datacenter 172.16.0.0/16
MIKROTIK2 eth0 real 192.168.8.1 - fake 11.0.0.27/28 -> ipsec to datacenter 172.16.0.0/16
MIKROTIK3 eth0 real 192.168.8.1 - fake 11.0.0.38/28 -> ipsec to datacenter 172.16.0.0/16

Using the real lan 192.168.8.0/24 everything works fine, now i just need to make the fake lan to work, this is my ipsec.conf - but i have no idea how to let the Mikrotik to NAT the request received from 172.16.0.0 on 11.0.0.0.26 to 192.168.8.10

1. ipsec.conf - strongSwan IPsec configuration file
2. basic configuration
   config setup
   charondebug="all"
   strictcrlpolicy=no

1. Add connections here.
   conn client-to-datacenter
   authby=secret
   left=%defaultroute
   leftauth=psk
   leftid=test2@test.local
   leftsubnet=11.0.0.16/28 (this must be translated in the real network 192.168.8.0/24)
   right=66.66.6.106
   rightauth=psk
   rightsubnet=172.16.0.0/16
   ike=aes256-sha2_256-modp1024!
   esp=aes256-sha2_256!
   keyingtries=3
   ikelifetime=6h
   lifetime=1h
   leftauth=psk
   dpddelay=30
   dpdtimeout=120
   dpdaction=restart
   auto=route

Thank you very much for your help

History

#1 - 24.09.2020 11:10 - Tobias Brunner

- Status changed from New to Feedback

Mikrotik to NAT the request received from 172.16.0.0 on 11.0.0.0.26 to 192.168.8.10

Use SNAT/DNAT rules (how you do that on Mikrotik boxes I have no idea).

#2 - 24.09.2020 14:22 - Francesco Galletti

Thank you very much, Mikrotik uses OPENWRT (Linux) and NAT is managed on iptables, could you please be so kind to write the example of the NAT rule you would use in this case? and in ipsec.conf wich value shoul leftsubnet= have?

Thank you

#3 - 24.09.2020 15:09 - Tobias Brunner

- Category set to network / firewall

> could you please be so kind to write the example of the NAT rule you would use in this case?

To allow traffic from any host in 192.168.8.0/24 maybe something like this:

```
iptables -t nat -A POSTROUTING -s 192.168.8.0/24 -j SNAT --to-source 11.0.0.16
```

If you also want to explicitly NAT inbound traffic to 192.168.8.1 (i.e. if traffic can be initiated by the remote end), you also need something like this:

```
iptables -t nat -A PREROUTING -d 11.0.0.16 -j DNAT --to-destination 192.168.8.1
```

> and in ipsec.conf wich value shoul leftsubnet= have?

The IP address from/to which you actually want to tunnel traffic (in this example 11.0.0.16/32).

#4 - 25.09.2020 14:26 - Francesco Galletti

Great! is perfectly working. I just have a question: how can i keep tunnel up? like a keep alive. Because Mikrotik should initiate the tunnel but i have to manually do it via ipsec up connection
if tunnel is down and ping 172.16.0.1 tunnel not going up automatically.

#5 - 25.09.2020 17:01 - Tobias Brunner

> Because Mikrotik should initiate the tunnel but i have to manually do it via ipsec up connection
> if tunnel is down and ping 172.16.0.1 tunnel not going up automatically.

With *auto=route*, trap policies (based on the configured *left*|*rightsubnet*) are installed in the kernel (this should be combined with *dpdaction=clear*, because *restart* could cause duplicate SAs), which should cause acquires from the kernel that in turn should trigger the initiation of SAs when matching traffic hits them. So after the SNAT is applied, the packets should theoretically match those policies and cause an acquire. Check the status output and the log for details.