strongSwan - Issue #3447

IPsec Multicast - Very close to getting it work OpenWRT to Vigor, Small problem.

15.05.2020 00:48 - Barry Jones

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.6.3	**Resolution:**	No feedback

Description

IPsec Multicast - Very close to getting it work OpenWRT to Vigor, Small problem.

I have the following set up.

OpenWRT router - 192.168.50.1 | Laptop 192.168.50.40
Vigor Router - 192.168.60.1 | Laptop 192.168.60.40

I have an IPsec VPN between these. The laptops on both ends can ping each other no problem.

The problem is with Multicast. I'm trying to send a packet UDP | port 40000 to 225.0.0.1

Laptop (Vigor) --> Laptop (OpenWRT) - No Issues
Laptop (OpenWRT) --> Laptop (Vigor) - Packet not received.

If I replace the OpenWRT router with another Vigor. So Vigor --> Vigor, Multicast works find on both ways.

Below is my config, is there anything you can see I am missing or anything to test further?

OpenWRT Firewall

```
iptables -t nat -I POSTROUTING -m policy --pol ipsec --dir out -j ACCEPT
iptables -t mangle -I PREROUTING -i br-lan -d 225.0.0.1/24 -p udp -j TTL --ttl-set 64
iptables -t mangle -I PREROUTING -i wwan0 -d 225.0.0.1/24 -p udp -j TTL --ttl-set 64
```

ipsec statusall

```
Listening IP addresses:
10.50.111.38
192.168.50.1
fd6d:d482:d664::1
Connections:
china-vigor: %any...2.97.90.173 IKEv1, dpddelay=30s
china-vigor: local: [10.50.111.38] uses pre-shared key authentication
china-vigor: remote: [2.97.90.173] uses pre-shared key authentication
china-vigor: child: 192.168.50.0/24 225.0.0.0/24 === 192.168.60.0/24 225.0.0.0/24 TUNNEL, dpdactio
n=restart
Security Associations (1 up, 0 connecting):
china-vigor[1]: ESTABLISHED 2 seconds ago, 10.50.111.38[10.50.111.38]...2.97.90.173[2.97.90.173]
china-vigor[1]: IKEv1 SPIs: d9c70d944986e34c_i* 10485e12e75b69e4_r, pre-shared key reauthenticatio
n in 43 minutes
china-vigor[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
china-vigor{1}: INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c5fbd313_i 910cca44_o
china-vigor{1}: AES_CBC_128/HMAC_SHA1_96, 72 bytes_i, 0 bytes_o, rekeying in 7 hours
china-vigor{1}: 192.168.50.0/24 === 192.168.60.0/24
```

ipsec.conf

```
conn china-vigor
authby=secret
```

```
aggressive=no
left=%any
leftsubnet=192.168.50.0/24,225.0.0.1/24
leftfirewall=yes
right=2.97.90.173
rightsubnet=192.168.60.0/24,225.0.0.1/24
mark=42
ike=aes128-sha1-modp1024
esp=aes128-sha1
keyingtries=0
ikelifetime=1h
keyexchange=ikev1
lifetime=8h
dpddelay=30
dpdtimeout=120
dpdaction=restart
auto=start
forceencaps=yes
closeaction=restart
```

forecast.conf

```
groups = 225.0.0.1,224.0.0.1,224.0.0.22,224.0.0.251,224.0.0.252,239.255.255.250
interface = br-lan
load = yes
reinject = china-vigor
```

smcroute.conf

```
mgroup from wwan0 group 225.0.0.1
mroute from wwan0 group 225.0.0.1 to br-lan
mgroup from br-lan group 225.0.0.1
mroute from br-lan group 225.0.0.1 to wwan0
```

Tcpdump - OpenWRT --> Vigor - Not received

```
tcpdump: listening on wwan0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:15:10.692982 IP (tos 0x0, ttl 63, id 19306, offset 0, flags [none], proto UDP (17), length 33)
    192.168.50.40.40000 > 225.0.0.1.40000: [udp sum ok] UDP, length 5
```

Tcpdump - Vigor --> OpenWRT - Received no issue.

```
tcpdump: listening on wwan0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:15:36.256191 IP (tos 0x0, ttl 1, id 19059, offset 0, flags [none], proto UDP (17), length 33)
    192.168.60.40.40000 > 225.0.0.1.40000: [udp sum ok] UDP, length 5
```

Forecast Log

```
Thu May 14 22:16:51 2020 daemon.info : 14[NET] forecast intercepted packet: 192.168.50.40 to 192.1
68.50.255
Thu May 14 22:16:51 2020 daemon.info : 15[NET] forecast intercepted packet: 192.168.50.40 to 192.1
68.50.255
Thu May 14 22:16:52 2020 daemon.info : 08[NET] forecast intercepted packet: 192.168.50.40 to 192.1
68.50.255
Thu May 14 22:16:53 2020 daemon.info : 06[NET] forecast intercepted packet: 192.168.60.40 to 225.0
.0.1
Thu May 14 22:16:53 2020 daemon.info : 09[NET] forecast intercepted packet: 192.168.60.40 to 225.0
.0.1
Thu May 14 22:16:53 2020 daemon.info : 07[NET] forecast intercepted packet: 192.168.60.40 to 225.0
.0.1
Thu May 14 22:16:54 2020 daemon.info : 10[NET] forecast intercepted packet: 192.168.60.40 to 255.2
55.255.255
```

```
Thu May 14 22:16:55 2020 daemon.info : 12[NET] forecast intercepted packet: 192.168.60.40 to 255.2
55.255.255
Thu May 14 22:16:56 2020 daemon.info : 13[NET] forecast intercepted packet: 192.168.60.40 to 255.2
55.255.255
Thu May 14 22:16:57 2020 daemon.info : 05[NET] forecast intercepted packet: 192.168.50.40 to 192.1
68.50.255
Thu May 14 22:16:57 2020 daemon.info : 14[NET] forecast intercepted packet: 192.168.50.40 to 192.1
68.50.255
Thu May 14 22:16:58 2020 daemon.info : 15[NET] forecast intercepted packet: 192.168.50.40 to 192.1
68.50.255
Thu May 14 22:17:02 2020 daemon.info : 04[NET] forecast intercepted packet: 192.168.50.40 to 225.0
.0.1
Thu May 14 22:17:02 2020 daemon.info : 08[NET] forecast intercepted packet: 192.168.50.40 to 225.0
.0.1
```

History

#1 - 15.05.2020 09:37 - Tobias Brunner

- Description updated

- Category set to configuration

- Status changed from New to Feedback

```
china-vigor{1}: 192.168.50.0/24 === 192.168.60.0/24
```

Apparently, your peer narrowed the traffic selectors and removed the multicast prefix you configured. Check the config and log on the peer to see why it did that. If it does not support multiple traffic selectors you might have to negotiate a separate CHILD_SA for the multicast traffic.

#2 - 30.09.2020 13:33 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No feedback