strongSwan - Issue #3332

Block traffic on only one way

06.02.2020 15:04 - Alexis Fischer

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.5.1	**Resolution:**	

Description

I am kinda new to IPSEC. I've set up a working Site to Site IPSEC Tunnel with strongswan on a debian 9 machine. However I have a requirement about how the traffic should work : The network on Site A can send packets to Site B Network and receive acks. Site B can only communicate with Site A when a connection is open. Basically, Site A can access Site B but Site B can't access site A. The infrastructure schema is like so :

```
        SITE A                                                  SITE B
NetA--------------GatewayA------Internet------GatewayB-----------------NetB
A.A.A.A/24  A.A.A.254  pub.lic.ip.A   pub.lic.ip.B  B.B.B.254     B.B.B.B/24
```

I only have access to Site A. Site B is on client side.

Now I need to restrict access from Site B to Site A. My first go was to put iptables on GatewayA to basically accept ESTABLISHED and RELATED packets from Site B and DROP everything else. Here are my iptables :

```
sudo iptables -L FORWARD
Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        state RELATED
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        state ESTABLISHED
DROP       all  --  B.B.B.B/24        A.A.A.A/24        policy match dir in pol ipsec proto esp
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        policy match dir in pol ipsec reqid 2 prot
o esp
ACCEPT     all  --  A.A.A.A/24        B.B.B.B/24        policy match dir out pol ipsec reqid 2 pro
to esp

sudo iptables -L INPUT
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        state RELATED
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        state ESTABLISHED
DROP       all  --  B.B.B.B/24        A.A.A.A/24        policy match dir in pol ipsec proto esp
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        policy match dir in pol ipsec reqid 2 prot
o esp
```

Here, the 3 first rules on each table are manually edited and the next ones are set up by strongswan/ipsec. On a test environment, i can ping from site A to Site B but not from Site B to Site A, which is what I want.

```
me@gatewayA:~$ ping A.A.A.1
PING A.A.A.1 (A.A.A.1) 56(84) bytes of data.
64 bytes from A.A.A.1: icmp_seq=1 ttl=63 time=2.25 ms
64 bytes from A.A.A.1: icmp_seq=2 ttl=63 time=1.32 ms
64 bytes from A.A.A.1: icmp_seq=3 ttl=63 time=1.28 ms
64 bytes from A.A.A.1: icmp_seq=4 ttl=63 time=1.56 ms
64 bytes from A.A.A.1: icmp_seq=5 ttl=63 time=1.45 ms

me@gatewayB:~$ ping B.B.B.1
PING B.B.B.1 (B.B.B.1) 56(84) bytes of data.
```

Now, for some reason, I need to restart ipsec :

```
sudo ipsec restart
```

Now i check my iptables :

```
sudo iptables -L FORWARD
Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        policy match dir in pol ipsec reqid 2 prot
o esp
ACCEPT     all  --  A.A.A.A/24        B.B.B.B/24        policy match dir out pol ipsec reqid 2 pro
to esp
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        state RELATED
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        state ESTABLISHED
DROP       all  --  B.B.B.B/24        A.A.A.A/24        policy match dir in pol ipsec proto esp

sudo iptables -L INPUT
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        policy match dir in pol ipsec reqid 2 prot
o esp
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        state RELATED
ACCEPT     all  --  B.B.B.B/24        A.A.A.A/24        state ESTABLISHED
DROP       all  --  B.B.B.B/24        A.A.A.A/24        policy match dir in pol ipsec proto esp
```

As you can see, restarting ipsec changed the iptables and now I can ping in both ways.

So I was wondering if there was any way to achieve what I want, which is to restrict access from Site B to Site A without affecting communications that goes from Site A to Site B. Maybe there is a way to define iptables within the strongswan configuration, or maybe change the priority of iptables rules so that they keep their order at reboot.

History

#1 - 06.02.2020 15:13 - Tobias Brunner

- Category set to configuration

- Status changed from New to Feedback

Please don't cross-post. As I wrote there, just disable *leftfirewall*.