strongSwan - Issue #848

updown script calls IPv4 hooks instead of IPv6 hooks for IPv6 peers

14.02.2015 19:13 - Noel Kuntze

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.2.2	**Resolution:**	

Description

Hello,

While building an updown script for special usage,
I noticed that only the following hooks are called
in the script:

- up-client
- down-client

In my scenario, the host this special script was running on, was only a responder.
The connection was made over IPv6.
I inserted the following code at line 155:

```
logger -t STRONGSWAN "DEBUG: $PLUTO_VERB:$1 : $PLUTO_ME $PLUTO_PEER"
```

It created the following output in the syslog:

```
Feb 14 05:08:51 thermi.strangled.net STRONGSWAN[21144]: DEBUG: up-client: : 2a03:4000:6:3064::1 2a
02:8071:9186:7d00:5054:ff:fe38:39ee
Feb 14 05:08:51 thermi.strangled.net STRONGSWAN[21155]: DEBUG: down-client: : 2a03:4000:6:3064::1
2a02:8071:9186:7d00:5054:ff:fe38:39ee
Feb 14 05:08:51 thermi.strangled.net STRONGSWAN[21166]: DEBUG: up-client: : 2a03:4000:6:3064::1 2a
02:8071:9186:7d00:5054:ff:fe38:39ee
```

It is completely fine that the IPv4 hooks are called for the defined IPv4 subnets, but as the peers
are connecting over IPv6, the following hooks should be called, too:

- up-host-v6
- down-host-v6

It would be nice that some light would be shed on this and whether this is intended behaviour
or a bug.
Following is the swanctl definition of the connection:

```
        home-active {
                version = 2
                remote_addrs = %any
                over_time = 3m
                keyingtries = 3
                dpd_delay = 10
                dpd_timeout = 60
                proposals = aes256gcm16-prfsha256-modp4096
                send_certreq = no
                rekey_time = 0s
                local {
                        id = thermi.strangled.net
                        auth = psk
                }

                remote {
                        id = thermi-home-gw-1
                        auth = psk
```

```
                }
                children {
                        home-active {
                                hostaccess = yes
                                local_ts = 0.0.0.0/0,::/0
                                remote_ts = 0.0.0.0/0
                                esp_proposals = aes256-aesxcbc-modp4096-esn
                                inactivity = 0s
                                dpd_action = clear
                                close_action = clear
                                rekey_time = 30m
                                mark_in = 0x1
                                mark_out = 0x1
                                updown = /usr/lib/strongswan/updown-active
                                tfc_padding = 0
                                ipcomp = yes
                                replay_window = 128
                         }
                }

        }
```

History

#1 - 16.02.2015 17:46 - Tobias Brunner

- Description updated

- Status changed from New to Feedback

The hooks to call are currently determined based on the address family of the traffic selectors not those of the endpoints (except for host-to-host tunnels, i.e. where the TS equals the endpoints and the -host hooks are called). So for the IPv4 subnets that are installed here this works as intended.

In the default script the -v6 suffix is mainly used to decide whether ip6tables should be used instead of iptables. So with nftables this could be less of an issue in the future and we could get by with only one set of hooks (flags that indicate the address families of the outer and inner addresses might be something to consider, though).

p.s. Could you please use <pre></pre> to format multi-line log/console output and files. Thanks!

#2 - 17.02.2015 20:53 - Noel Kuntze

Ah, okay. That makes sense. I will handle determining the peer IP address type in the hook itself then.
Thank you for the clarification.
I think having a flag or extra variable that tells you the IP address type directly would be nice.
Sure, I will try to keep this in mind when opening the next request.

#3 - 16.04.2015 10:30 - Tobias Brunner

- Category set to configuration

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner