strongSwan - Issue #403

v4 tunnel host-to-host "can't install route for 192.168.178.43/32 === 192.168.178.48/32 out, conflicts with IKE traffic"

07.09.2013 19:04 - Noel Kuntze

Status:	Rejected		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	charon		
Affected version:	5.1.0	**Resolution:**	Duplicate

Description

strongSwan 5.1.0
Both boxes run Arch Linux kernel 3.10.x.
Both hosts are connected over a switch and the LAN ports of a router.
I think this should work, but it doesn't.
192.168.178.43:

```
┌─[root][thermi-pc][/home/thermi]
└──╼ ipsec up server
initiating IKE_SA server[1] to 192.168.178.48
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) V ]
sending packet: from 192.168.178.43[500] to 192.168.178.48[500] (708 bytes)
received packet: from 192.168.178.48[500] to 192.168.178.43[500] (761 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
faking NAT situation to enforce UDP encapsulation
received cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN=Ther
miCorp ServerCA Layer 2"
received cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp Use
rCA Level 2"
received cert request for "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=Th
ermiCorp Root CA, E=noel.kuntze@googlemail.com"
sending cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=UserCA, CN=ThermiCorp User
CA Level 2"
sending cert request for "C=DE, ST=Baden-W??rttemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=The
rmiCorp Root CA, E=noel.kuntze@googlemail.com"
sending cert request for "C=DE, ST=Baden-W??rttemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN=Therm
iCorp ServerCA Layer 2"
authentication of '192.168.178.43' (myself) with pre-shared key
establishing CHILD_SA server
generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ IDr AUTH N(ESP_TFC_PAD_N) SA TSi TSr N
(MULT_AUTH) N(EAP_ONLY) ]
sending packet: from 192.168.178.43[4500] to 192.168.178.48[4500] (368 bytes)
received packet: from 192.168.178.48[4500] to 192.168.178.43[4500] (272 bytes)
parsed IKE_AUTH response 1 [ IDr AUTH SA TSi TSr N(AUTH_LFT) ]
authentication of '192.168.178.48' with pre-shared key successful
IKE_SA server[1] established between 192.168.178.43[192.168.178.43]...192.168.178.48[192.168.178.4
8]
scheduling reauthentication in 9888s
maximum IKE_SA lifetime 10428s
can't install route for 192.168.178.43/32 === 192.168.178.48/32 out, conflicts with IKE traffic
unable to install IPsec policies (SPD) in kernel
failed to establish CHILD_SA, keeping IKE_SA
received AUTH_LIFETIME of 3289s, scheduling reauthentication in 2749s
sending DELETE for ESP CHILD_SA with SPI 8d45370c
generating INFORMATIONAL request 2 [ D ]
sending packet: from 192.168.178.43[4500] to 192.168.178.48[4500] (96 bytes)
received packet: from 192.168.178.48[4500] to 192.168.178.43[4500] (96 bytes)
parsed INFORMATIONAL response 2 [ D ]
establishing connection 'server' failed
```

(Unnecessary parts redacted)

ipsec.conf

```
config setup
        # strictcrlpolicy=yes
        # uniqueids = no

conn %default
        leftupdown=/usr/lib/strongswan/sudo_updown

conn server
        mobike=no
        left=%defaultroute
        leftid=192.168.178.43
        leftauth=psk
        esp=aes256-sha512-modp4096!
        ike=aes256-sha512-modp4096!
        keyexchange=ikev2
        rightauth=psk
        right=192.168.178.48
        rightid=192.168.178.48
        auto=add
```

192.168.178.48:

```
config setup
        uniqueids=replace
        strictcrlpolicy=no
conn %default
        ikelifetime=60m
        marginbytes=3000000000
        marginpackets=150000
        inactivity=0s
        keylife=20m
        rekeymargin=3m
        keyingtries=3
        tfc=%mtu
        dpdaction=restart
        dpddelay=10
        dpdtimeout=60
        compress=yes
        left=192.168.178.48
        leftupdown=/usr/lib/strongswan/sudo_updown
conn desktop
        mobike=no
        keyexchange=ikev2
        ike=aes256-sha512-modp4096!
        esp=aes256-sha512-modp4096!
        leftauth=psk
        leftid=192.168.178.48
        right=%any
        rightid=192.168.178.43
        rightauth=psk
        auto=add
```

Related issues:

Is duplicate of Feature #380: Allow /32 remote subnet with kernel-libipsec pl...	**Closed**	**12.08.2013**

History

#1 - 10.09.2013 10:25 - Tobias Brunner

- Description updated

- Status changed from New to Rejected

- Assignee set to Tobias Brunner

- Resolution set to Duplicate

Files

charon_hosttohost.log	108 KB	07.09.2013	Noel Kuntze