strongSwan - Feature #2138

IKEv2 IPv6 source address selection algorithm should take labels into account

08.10.2016 18:36 - Carl-Daniel Hailfinger

Status:	Closed	**Start date:**	08.10.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	kernel-interface		
Target version:	5.5.2		
Resolution:	Fixed		

Description

I have a strongswan server and strongswan road warrior client with the following configuration:

Server: global+local IPv6 addresses, global+local IPv4 addresses, DNS A record for openwrt.myorg.org points to global v4 address, DNS AAAA record for openwrt.myorg.org points to global v6 address
Client: global+local IPv6 addresses, local IPv4 address, no DNS records

ipsec.conf on the client has (sanitized):

```
conn %default
        ikelifetime=3h
        lifetime=1h
        margintime=9m
        keyingtries=%forever
        keyexchange=ikev2
        left=%any
        leftauth=pubkey
        leftcert=mobile-pi3Cert.der
        leftid="C=DE, O=myorg, CN=mobile-pi3"
        leftsourceip=192.168.3.5
        leftfirewall=yes
        lefthostaccess=yes

conn openwrt
        auto=start
        #dpdaction=restart should only be set at a client, not at the central server
        dpdaction=restart
        closeaction=restart
        right=%openwrt.myorg.org
        rightsubnet=0.0.0.0/0
        rightauth=pubkey
        rightcert=openwrtCert.der
        rightid="C=DE, O=myorg, CN=openwrt"
        rightdns=192.168.2.1
```

Given that openwrt.myorg.org has an A and AAAA record, sometimes the IKEv2 happens via IPv4, sometimes via IPv6. IPv4 always works fine, but the IKEv2 source address selection for IPv6 seems to be somewhat random.

Performing IKEv2 from client global IPv6 address to server global IPv6 address works fine, but sometimes the client attempts to use its unique local address (in the range fc00::/7) as source address for IKEv2. That obviously can't work over the public internet unless some IPv6 NAT is involved.

Suggestion: For IKEv2 IPv6 source address selection (initial connection as well as MOBIKE associated reconnect), the source address selection algorithm should check if the IPv6 destination address is a global address, and prefer an IPv6 global address as source address as well. If the IPv6 destination address is unique local, the source address selection algorithm should prefer an unique local address as well.

Associated revisions

Revision f1257277 - 25.01.2017 17:33 - Tobias Brunner

kernel-netlink: Prefer matching label when selecting IPv6 source addresses

This implements rule 6 of RFC 6724 using the default priority table,
so that e.g. global addresses are preferred over ULAs (which also have
global scope) when the destination is a global address.

Fixes #2138.

Revision 7a40162c - 06.02.2017 11:06 - Tobias Brunner

kernel-netlink: Prefer matching label when selecting IPv6 source addresses

This implements rule 6 of RFC 6724 using the default priority table,
so that e.g. global addresses are preferred over ULAs (which also have
global scope) when the destination is a global address.

Fixes #2138.

History

#1 - 10.10.2016 10:11 - Tobias Brunner

- Tracker changed from Issue to Feature

- Subject changed from IKEv2 IPv6 source address selection algorithm should take scope into account to IKEv2 IPv6 source address selection algorithm should take labels into account

- Description updated

- Category set to kernel-interface

- Status changed from New to Feedback

The scope of these addresses is actually the same (global). But we currently don't implement rule 6 of RFC 6724 which uses a policy table to determine matching labels for addresses (so ULAs are depreferenced when not reaching an ULA). The patch in the *2138-kernel-netlink-ula* branch adds that (but doesn't make the policy table configurable).

As a workaround you could try to use the native source address lookup by setting *charon.plugins.kernel-netlink.fwmark* (see Routing).

#2 - 10.10.2016 16:00 - Carl-Daniel Hailfinger

Wow, that was quick. Thank you! Will test ASAP.

#3 - 10.03.2017 13:42 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.5.2

- Resolution set to Fixed