strongSwan - Issue #3420

how to setup IP pool that will not go through the vpn tunneling ?

22.04.2020 11:48 - Royi Cohen

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.8.4	**Resolution:**	No change required

Description

is it possible to set IP addresses that when the client will try to connect to them, the connection will go directly and not go through the VPN tunneling?

I saw that I can define the destination IPs, but is it also support the ability to defined a list of IPs that will be bypass the VPN?

History

#1 - 22.04.2020 12:10 - Tobias Brunner

- Category set to configuration

- Status changed from New to Feedback

Have a look at passthrough policies, which clients can use to exclude certain traffic from VPN tunnels.

#2 - 28.04.2020 11:07 - Royi Cohen

something is not clear for me.

I have the following configuration in ipsec.conf:

```
conn ios
fragmentation=yes
keyexchange=ikev1
authby=xauthrsasig
xauth=server
left=%defaultroute
leftsubnet=0.0.0.0/0
leftfirewall=yes
leftcert=serverCert.pem
right=%any
rightsourceip=10.0.0.0/16
auto=add
dpdaction = clear
dpddelay = 3600s
```

Is it possible to add on the server configuration an IP address that the client will not send the traffic to it via the VPN tunneling, by adding in the IPsec the following configuration for example ?:

```
conn passthrough-2
left=127.0.0.1
leftsubnet=192.168.0.0/16
rightsubnet=10.0.0.0/8
type=passthrough
auto=route
```

#3 - 28.04.2020 11:40 - Royi Cohen

a better example for my question, if I want to bypass the VPN tunneling on the client-side for 2 destinations IPs like 1.1.1.1 and 2.2.2.2, is adding the following conf to the ipsec.conf on the server will do the job?

```
conn passthrough_base
left=127.0.0.1
right=127.0.0.1
type=passthrough
auto=route

conn passthrough_1
also=passthrough_base
leftsubnet=0.0.0.0/0
```

rightsubnet=1.1.1.1./32, 2.2.2.2/32

#4 - 28.04.2020 12:45 - Tobias Brunner

> Is it possible to add on the server configuration an IP address that the client will not send the traffic to it via the VPN tunneling

Only with IKEv1 and the proprietary [Cisco Unity]() attributes (*split-exclude*). With IKEv2 you could use narrowing (i.e. change *leftsubnet* so it includes only subnets to tunnel), but excluding single IP addresses could result in a lot of traffic selectors (possibly too many) and not all clients support this.

> is adding the following conf to the ipsec.conf on the server will do the job?

No, you have to configure such policies on the client. It's the one who decides what to tunnel.

#5 - 29.04.2020 13:20 - Royi Cohen

Tobias Brunner wrote:

> ... but excluding single IP addresses could result in a lot of traffic selectors (possibly too many) and not all clients support this.

Is this related to both options ? IKEv1 and IKEv2 ?

So there is not a good way for doing that ?

#6 - 29.04.2020 14:36 - Tobias Brunner

> > ... but excluding single IP addresses could result in a lot of traffic selectors (possibly too many) and not all clients support this.
>
> Is this related to both options ? IKEv1 and IKEv2 ?

No, only narrowing with IKEv2.

> So there is not a good way for doing that ?

Not from the server.

#7 - 25.09.2020 11:42 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required