strongSwan - Issue #3534

use of strongswan, ipvlan L2 and kernel ipsec

04.08.2020 18:49 - Harshal Haridas

Status:	New		
Priority:	Urgent		
Assignee:			
Category:	libstrongswan		
Affected version:	5.3.5	**Resolution:**	

Description

We have a situation where we cannot get strongswan and ipsec on a host to work with docker containers configured using ipvlans l2 mode and which have ip address configured different from host ip address. We are using linux kernel version 4.18 and strongswan version 5.3.5. Question is whether it is possible to use host deployed libstrongswan and libipsec to encrypt traffic from docker containers configured using ipvlan l2?

Example:
Host1 ip address: 192.168.1.1
Docker container1 ip address configured: 192.168.1.2
External target host2 ip address: 192.168.1.3
External target container2 ip address configured: 192.168.1.4

container1 executes on host1
container2 executes on host2

policies deployed on host 1 and host 2:
192.168.1.1-192.168.1.3 encrypt (aes128-gcm)
192.168.1.2-192.168.1.4 encrypt (aes128-gcm)

strongswan and ipsec/kernel implemented outside container on host
traffic from .1-.3

Policies work (traffic encrypted) between hosts but traffic from containers is not seen on the wire at all.

When we use the containers with docker bridged networking (i.e. no external ip address assigned), we can see encrypted traffic on the wire between two containers.

Is the above expected to work? And if yes, are there good references to look at to see how to get this to work?

History

#1 - 04.08.2020 20:59 - Harshal Haridas

Harshal Haridas wrote:

> We have a situation where we cannot get strongswan and ipsec on a host to work with docker containers configured using ipvlans l2 mode and which have ip address configured different from host ip address. We are using linux kernel version 4.18 and strongswan version 5.3.5. Question is whether it is possible to use host deployed libstrongswan and libipsec to encrypt traffic from docker containers configured using ipvlan l2?
>
> Example:
> Host1 ip address: 192.168.1.1
> Docker container1 ip address configured: 192.168.1.2
> External target host2 ip address: 192.168.1.3
> External target container2 ip address configured: 192.168.1.4
>
> container1 executes on host1
> container2 executes on host2
>
> policies deployed on host 1 and host 2:
> 192.168.1.1-192.168.1.3 encrypt (aes128-gcm)
> 192.168.1.2-192.168.1.4 encrypt (aes128-gcm)
>
> strongswan and ipsec/kernel implemented outside container on host
> traffic from .1-.3
>
> Policies work (traffic encrypted) between hosts but traffic from containers is not seen on the wire at all.

Not seeing on the wire primarily happens when using ipvlan l3 mode. with use of ipvlan l2, we see cleartext traffic all the time.

> When we use the containers with docker bridged networking (i.e. no external ip address assigned), we can see encrypted traffic on the wire between two containers.
>
> Is the above expected to work? And if yes, are there good references to look at to see how to get this to work?