strongSwan - Issue #3425

Encryption happens in only one direction for bi-directional traffic.

24.04.2020 15:04 - Nagendra E S

Status: New
Priority: Normal
Assignee: 
Category: 
Affected version: 5.7.2
Resolution: 

Description
Topology:
Servers run Ubuntu 18.04 and Linux 4.15.0-29-generic

Two servers connected over network hosting VMs on each server. Host(hypervisor) OS is having custom datapath. This datapath sends packets that have to be encrypted to a "crypt0" interface which interfaces with linux kernel IP stack. There is another interface "decrypt0" interface which is used to receive packets decrypted by kernel back to the custom datapath.

Problem Description:
ping is originating on VM1 on Server-1 (10.204.216.39). The ping packets are encapsulated over VxLan (UDP) by custom datapath with src-ip 10.204.216.39 and dst-ip 10.204.216.46, and sent to crypt0 interface. The kernel encrypts and sends to other server Server-2 (10.204.216.46) using the linux ip stack forwarding tables. On Server-2, decryption happens and packets are sent to VM2 on Server-2 after removing VxLan header in custom datapath.

Now, the ping replies from VM2 on Server-2 are going to the linux kernel stack via the custom datapath and crypt0 interface. However, the packets are not getting encrypted and forwarded as plain-text on to the network physical interface.

To summarise, packets originating from Server-1 are getting encrypted but packets originating from Server-2 are not getting encrypted and going as plain-text.

Decryption happens properly on Server-2 (for packets received from Server-1).

Now, if ping is done from VM2, still the encryption doesn't happen on Server-2 but the ping response from Server-1 is encrypted.

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>server_1.tar</td>
<td>30 KB</td>
<td>24.04.2020</td>
<td>Nagendra E S</td>
</tr>
<tr>
<td>server_2.tar</td>
<td>30 KB</td>
<td>24.04.2020</td>
<td>Nagendra E S</td>
</tr>
</tbody>
</table>