Case-Study - 2019-0131-0694 Vrouter ACLs

Monday, April 1, 2019 3:20 PM

Problem Description:

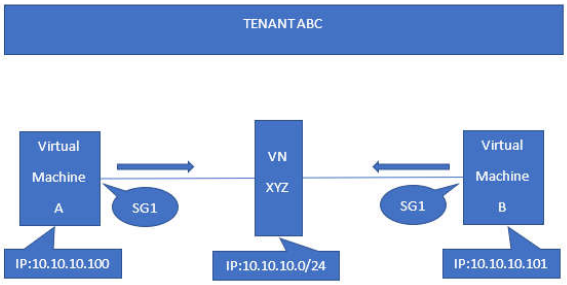
- SSH connections are timing out between VM instances in the same VN.
- Customer client VM application SSH into server VM and keeps the session idle.
- Customer notice that after 3mins of inactivity , the SSH session is unable to resume.
- The SSH flow on the vrouter ages out after 3 mins(180 secs flow aging) of inactivity and any new packets for that SSH session is dropped by the vrouter with action ":D(RevOutSG)".
- This issue is observed starting release 3.2.13 as a result of the fix introduced for Launchpad#1786924

```
    Index               Source:Port/Destination:Port                      Proto(V)
-----------------------------------------------------------------------------------
   187548<=>483032       10.10.10.100:55729                                 6 (22)
                         10.10.10.101:22
(Gen: 23, K(nh):242, Action:F, Flags:, TCP:SSrEEr, QOS:-1, S(nh):162,
 Stats:139/11311,  SPort 54974, TTL 0, Sinfo 172.18.101.104)

   483032<=>187548       10.10.10.101:22                                    6 (22)
                         10.10.10.100:55729
(Gen: 1, K(nh):242, Action:F, Flags:, TCP:SSrEEr, QOS:-1, S(nh):242,  Stats:565/143567,
 SPort 51505, TTL 0, Sinfo 32.0.0.0)
```

After 3 mins of Inactivity

```
    Index               Source:Port/Destination:Port                      Proto(V)
-----------------------------------------------------------------------------------
   187548<=>483032       10.10.10.100:55729                                 6 (22)
                         10.10.10.101:22
(Gen: 23, K(nh):242, Action:D(RevOutSG), Flags:, TCP:, QOS:-1, S(nh):162,
 Stats:24/1127,  SPort 54974, TTL 0, Sinfo 172.18.101.104)

   483032<=>187548       10.10.10.101:22                                    6 (22)
                         10.10.10.100:55729
(Gen: 1, K(nh):242, Action:F, Flags:, TCP:SSrEEr, QOS:-1, S(nh):242,  Stats:0/0,
 SPort 51505, TTL 0, Sinfo 32.0.0.0)
```

- For demonstration purposes, consider the following scenario where a security group 'SG1' is applied to the interfaces of both virtual machines A and B which are part of the same virtual network "XYZ"



- The security group 'SG1' is defined with following rules:

Security Group Details

Display Name	SG1
Security Group ID	Auto Configured (8000017)
UUID	731f3a0f-f83b-4990-a321-33b2abe21702
Rules	***egress IPv4*** network ***0.0.0.0/0*** protocol ***any*** ports ***any***
	ingress IPv4 network ***0.0.0.0/0*** protocol ***icmp*** ports type ***any*** code ***any***
	ingress IPv4 network ***0.0.0.0/0*** protocol ***tcp*** ports ***[22]***

- As seen in the above output, SG1 allows all traffic in the EGRESS direction and only accepts SSH and ICMP traffic in the INGRESS direction.
- At vrouter level, the same security groups are represented or mapped to a set of access-control lists(ACLs) which then dictate whether a traffic flow is permitted or denied by a vrouter.
- Once security-group 'SG1' is defined, the schema-transformer in Contrail will create necessary access-control-lists(ACLs) that represent the rules defined under security group 'SG1'.
- In this case, the schema-transformer will create two ACLs, one for each direction of traffic as shown below:

INGRESS DIRECTION

ACE Id	Action	Protocol	Source	Source Port	Destination	Destination Port
ACL UUID: f35ab6e3-089d-467a-8114-b203dc1106e1 (2 ACE)						
1	pass	1	0.0.0.0 / 0.0.0.0	any		any
2	pass	6	0.0.0.0 / 0.0.0.0	any		22

- Note that there are two access-list-entries(ACEs) for the ACL created in ingress direction, one for ICMP(protocol 1) and one for SSH(TCP port 22) traffic.

EGRESS DIRECTION

ACE Id	Action	Protocol	Source	Source Port	Destination	Destination Port
ACL UUID: f49ce1ce-eadc-45f7-a26b-b6403dc230e1 (1 ACE)						
1	pass	any		any	0.0.0.0 / 0.0.0.0	any

- ACLs are created when the security group is defined, however they are not downloaded to all the vrouters at the time of SG creation.
- Once a security group is applied to any virtual-machine interface(VMI), the corresponding ACLs are then downloaded only to those vrouters which have the VMIs with corresponding Security groups.
- In the case of above security-group 'SG1' , the ACLs are downloaded on vrouters which hosts virtual-machines A and B.

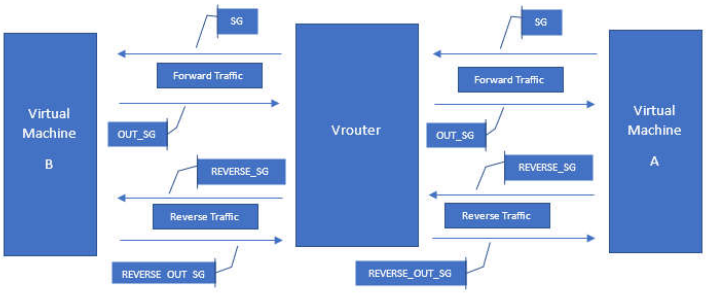
- Unlike traditional routers or switches where ACLs are applied on interfaces, in Contrail ACLs are applied to a flow rather than to a VMI port.

- To demonstrate, we are going to SSH from virtual-machine A to virtual-machine B and then take a look at ACLs applied to this SSH flow on the vrouter.

```
    Index                Source:Port/Destination:Port                      Proto(V)
-----------------------------------------------------------------------------------
   187548<=>483032       10.10.10.100:55729                                 6 (22)
                         10.10.10.101:22
(Gen: 23, K(nh):242, Action:F, Flags:, TCP:SSrEEr, QOS:-1, S(nh):162,
 Stats:139/11311,  SPort 54974, TTL 0, Sinfo 172.18.101.104)

   483032<=>187548       10.10.10.101:22                                    6 (22)
                         10.10.10.100:55729
(Gen: 1, K(nh):242, Action:F, Flags:, TCP:SSrEEr, QOS:-1, S(nh):242,  Stats:565/143567,
 SPort 51505, TTL 0, Sinfo 32.0.0.0)
```

ACL UUID	Protocol	Src Network	Src IP	Src Port	Dest Network	Dest IP	Dest Port
SG: f49ce1ce-eadc-45f7-a26b-b6403dc230e1	TCP	default-domain:aamonker:Test-VN-Right	10.10.10.100	55731	default-domain:aamonker:Test-VN-Right	10.10.10.101	22

- Shown above is the flow that is created on vrouter hosting virtual-machine A(10.10.10.100) for the outgoing SSH connection towards virtual-machine B(10.10.10.101)
- There are basically four directions in which the ACLs are applied on a flow depending on the direction of traffic
    - **SG**: Direction of traffic for the forward flow from source to destination
    - **OUT_SG** : Direction of traffic for the reverse flow from destination towards source
    - **REVERSE_SG** : Direction of traffic for the reverse flow from source towards destination
    - **REVERSE_OUT_SG**: Direction of traffic for the forward flow from destination towards source
- Here's is an image to illustrate the directions in which ACLs are applied per flow



- As shown previously, there are two ACLs that are created by the schema corresponding to the directions (INGRESS and EGRESS) defined at the time of security-group creation. For the sake of simplicity we will call them INGRESS ACL (ACL UUID: f35ab6e3-089d-467a-8114-b203dc1106e1) and EGRESS ACL(ACL UUID: f49ce1ce-eadc-45f7-a26b-b6403dc230e1)
- For the purpose of demonstration, we are using the outgoing flow shown above from VM-A(10.10.10.100:55730) to VM-B(10.10.10.101:22) on the vrouter hosting VM-A.
- We can view the ACLs applied on a vrouter flow in Contrail UI. Go to Dashboard --> Virtual Routers --> Select a vrouter --> Flows --> Select a flow
- For our case, following are the ACLs applied:
    - SG : EGRESS ACL

```
sg: - {
    FlowAclInfo: - {
        action: 32
        acl: - {
            list: - {
                FlowAclUuid: - {
                    uuid: f49ce1ce-eadc-45f7-a26b-b6403dc230e1
                }
            }
        }
```

    - OUT_SG: None

```
out_sg: - {
    FlowAclInfo: - {
        action: 32
        acl: - {
            list:
        }
```

    - REVERSE_SG: None

```
reverse_sg: - {
    FlowAclInfo: - {
        action: 32
        acl: - {
            list:
        }
```

    - REVERSE_OUT_SG: INGRESS ACL

```
reverse_out_sg: − {
    FlowAclInfo: − {
        action: 536870920
        acl: − {
            list: − {
                FlowAclUuid: − {
                    uuid: f35ab6e3-089d-467a-8114-b203dc1106e1
                }
            }
        }
```