Open Infrastructure - Task #6681

Create a distributed firewall PoC based on uncloud/nft

05/13/2019 05:35 PM - Nico Schottelius

Status:	Rejected	**Start date:**	05/13/2019
Priority:	Normal	**Due date:**	
Assignee:	Nico Schottelius	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
PM Check date:			

Description

Design

- uncloud needs to know about opennebula VMs
  - we have an importer for this one
- uncloud needs to be able to extract mappings for
  - mac <-> nic
  - ip address <-> nic
  - VM <-> host (?)
- uncloud needs to be able to configure nft on all hosts
  - ssh keys need to be configured

History

#1 - 05/13/2019 05:49 PM - Nico Schottelius

- Description updated

- Status changed from New to In Progress

- testing consul kv

```
[17:33:14] server2.place6:~# consul  kv put vm-firewall/a-vm-id/allow-one-23654-0 "2a09:2947::42/64"
Success! Data written to: vm-firewall/a-vm-id/allow-one-23654-0
[17:36:57] server2.place6:~# consul  kv put vm-firewall/a-vm-id/allow-one-23654-0-ether "20:c9:d0:43:12:d9"
Success! Data written to: vm-firewall/a-vm-id/allow-one-23654-0-ether
[17:38:56] server2.place6:~# consul kv get vm-firewall/a-vm-id/allow-one-23654-0-ether
20:c9:d0:43:12:d9
[17:39:03] server2.place6:~#
```

- consul can have watches: https://www.consul.io/docs/agent/watches.html
  - could be used for updating the firewall

```
{
  "type": "key",
  "key": "foo/bar/baz",
  "handler_type": "script",
  "args": ["/usr/bin/my-service-handler.sh", "-redis"]
}
```

- nft rules / hints
  - ether saddr 20:c9:d0:43:12:d9

#2 - 05/13/2019 05:51 PM - Nico Schottelius

Checking mac addresses, inside != outside:

```
[17:49:56] server2.place6:~# ip l | grep -i -e 02:00:f0:a9:c4:09 -e 24181
251: one-24181-0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9200 qdisc htb master br-vm-place6 state UNKNOWN mode
DEFAULT group default qlen 1000
[17:50:11] server2.place6:~# ip l sh dev one-24181-0
251: one-24181-0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9200 qdisc htb master br-vm-place6 state UNKNOWN mode
DEFAULT group default qlen 1000
    link/ether fe:00:f0:a9:c4:09 brd ff:ff:ff:ff:ff:ff
[17:50:21] server2.place6:~#
```

=> need mac address in database

#3 - 05/13/2019 05:55 PM - Nico Schottelius

Watching on different servers nicely works:

```
[17:54:10] server2.place6:~# consul  kv put vm-firewall/a-vm-id/allow-one-23654-1 "2a09:2947::43/64"
Success! Data written to: vm-firewall/a-vm-id/allow-one-23654-1
[17:53:17] server3.place6:~# consul watch -type=keyprefix -prefix=vm-firewall/ "/bin/echo updating firewall"
updating firewall
updating firewall
```

#4 - 05/14/2019 09:24 PM - Nico Schottelius

- Description updated

#5 - 05/17/2019 09:14 PM - Nico Schottelius

- Description updated

#6 - 05/18/2019 11:20 AM - Nico Schottelius

- Description updated

#7 - 05/18/2019 09:30 PM - Nico Schottelius

- Description updated

#8 - 06/23/2019 05:47 PM - Nico Schottelius

- Assignee changed from Nico Schottelius to ll nu

Balazs,

please read and close afterwards -- this is a duplicate ticket of ucloud-firewall.

#9 - 07/02/2019 09:47 PM - ll nu

- Status changed from In Progress to Closed

#10 - 07/02/2019 09:56 PM - Nico Schottelius

- Status changed from Closed to Seen

Poing - if you close, please document where the solution
can be found ;-)

redmine@ungleich.ch writes:

#11 - 07/03/2019 02:12 PM - ll nu

You wrote that i should read it and close afterwards.

You mean link the duplicate issue?
https://redmine.ungleich.ch/issues/6857 - ucloud-firewall

#12 - 09/04/2019 03:44 PM - ll nu

- Status changed from Seen to Closed

#13 - 05/17/2020 10:29 PM - Nico Schottelius

- Status changed from Closed to In Progress

- Assignee changed from ll nu to Nico Schottelius

Reopening - as prod is now needed

#14 - 05/17/2020 10:29 PM - Nico Schottelius

- Subject changed from Create a distributed firewall PoC based on nft/consul to Create a distributed firewall PoC based on uncloud/nft

#15 - 05/17/2020 10:34 PM - Nico Schottelius

- Description updated

#16 - 12/06/2021 11:55 PM - Nico Schottelius

- Status changed from In Progress to Rejected