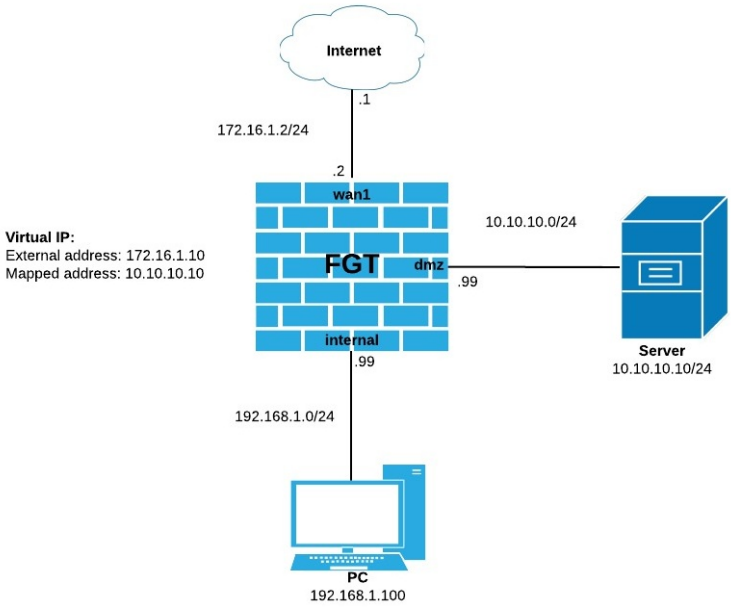
Fortigate Hairpin NAT

Article Number: 120 | Rating: 4.3/5 from 3 votes | Last Updated: Fri, Aug 4, 2017 at 4:35 PM

This article describes the configuration needed for Hairpin NAT.

Scenario: Internal user ("PC" in the follow diagram) needs to access Server (10.10.10.10)



In this scenario, both PC and Server are behind FortiGate and PC wants to connect to Server by pointing to its external address (172.16.1.10) instead of its real one (10.10.10.10). This is called Hairpin NAT.

Solution

The solution will depend on how the Virtual IP (VIP) has been configured in first place, specifically the value set to the external interface option set in the VIP.

=> External interface set to a particular interface, for instance wan1:

```
config firewall vip
   edit "VIP"
      set extip 172.16.1.10
      set extintf "wan1"
      set mappedip 10.10.10.10
   next
end
```

Two policies are needed:

1. An incoming policy with VIP object as destination address and dmz as outgoing interface (interface server is behind). This would be the typical policy needed for making a device accessible from Internet.

```
config firewall policy
   edit 1
      set srcintf "wan1"
      set dstintf "dmz"
      set srcaddr "all"
      set dstaddr "VIP"   <--- VIP object
      set action accept
      set schedule "always"
      set service "ALL"
   next
end
```

2. An outgoing policy having as outgoing interface the same one defined as external interface in VIP object. In this case this would be wan1.

```
config firewall policy
   edit 2
      set srcintf "internal"
      set dstintf "wan1"  <-- Same as external interface defined in VIP
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set nat enable
   next
end
```

=> External interface set to any:

```
config firewall vip
   edit "VIP"
      set extip 172.16.1.10
      set extintf "any"
      set mappedip 10.10.10.10
   next
end
```

One policy is needed:

1) An outgoing policy with VIP object as destination address and dmz as outgoing interface (interface server is behind)

```
config firewall policy
   edit 3
      set srcintf "internal"
      set dstintf "dmz"
      set srcaddr "all"
      set dstaddr "VIP"   <--- VIP object
      set action accept
      set schedule "always"
      set service "ALL"
   next
end
```

Or you can also create the same policy as above but with "match-vip" enabled and "all" as destination address instead:

```
config firewall policy
   edit 3
      set srcintf "internal"
      set dstintf "dmz"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
```

```
        set schedule "always"
        set service "ALL"
        set match-vip enable
    next
end
```

Notes:
- Even though packet is destined to an external address, it is never forwarded to the Internet. This is, packet always remains on the inside network since FortiGate will forward and translate it between interfaces.
- If both PC and Server are behind the same interface, same rules apply. In this case, outgoing and incoming interfaces will be the same in policy #3.