AWS Best Practices:

Assigning Multiple Public IPs to the Same Interface

Q1 2016

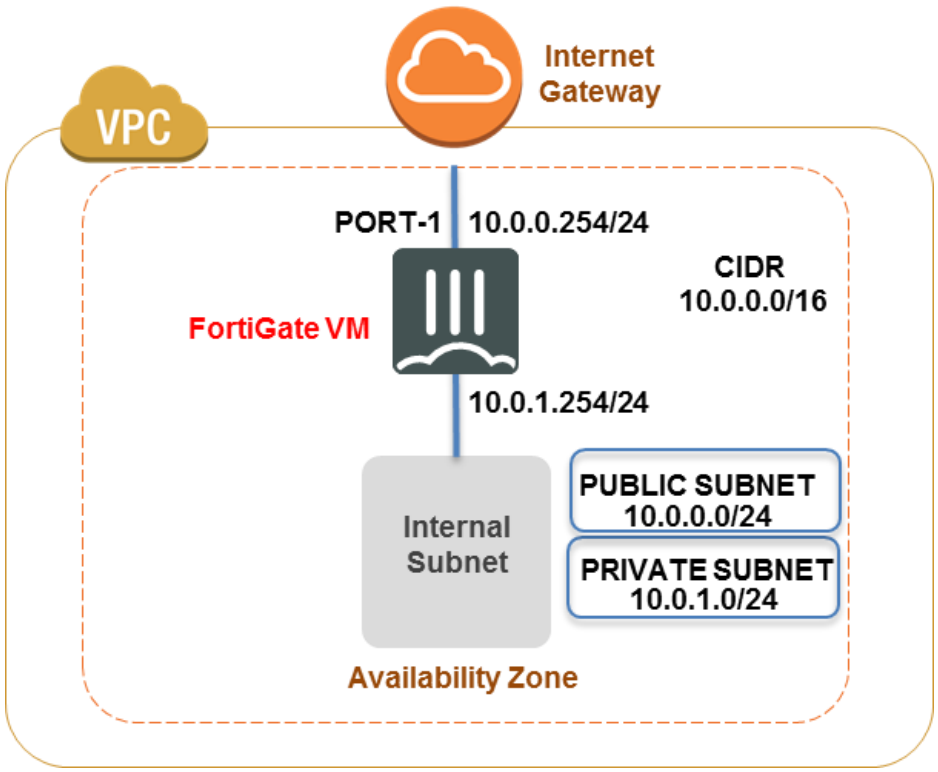
Problem Statement

- In AWS, FortiGate-VM's Port-1 is mapped to the Elastic Network Interface (ENI) eth0 of the instance. Once you have a FortiGate firewall in your VPC that is functioning as your Internet Gateway, the FortiGate's Port-1 is the internet-facing interface by default. This behavior is because AWS enforces the Elastic Network Interface eth0 as the dedicated interface for passing internet traffic.

  The Port-1 of the FortiGate gets the IP address through DHCP in FortiOS. With this setting, we will not be able to set secondary IP for Port-1 and thus no more than one elastic IP for Port-1 as well.

Solution

- We will be using this example VPC:



- In AWS, all the traffic within the VPC is handled by an Intrinsic Router. The IP address for the Intrinsic Router is always the first usable IP address in the subnet. For example, if your subnet is 10.0.0.0/24, the intrinsic router is at 10.0.0.1. Having known that, we are going to workaround the issue in the problem statement above using the following steps.

Step 1: Create a Static Route

- Since we know that the AWS Intrinsic Router sits at the first usable IP in the subnet, we are going to create a static default route pointed at this IP address.

From FortiOS CLI

```
config router static
   edit 1
      set dst 0.0.0.0 0.0.0.0
      set gateway 10.0.0.1
      set device "Port-1"
   next
End
```

Step 2: Change the Addressing Mode to Static for Port-1

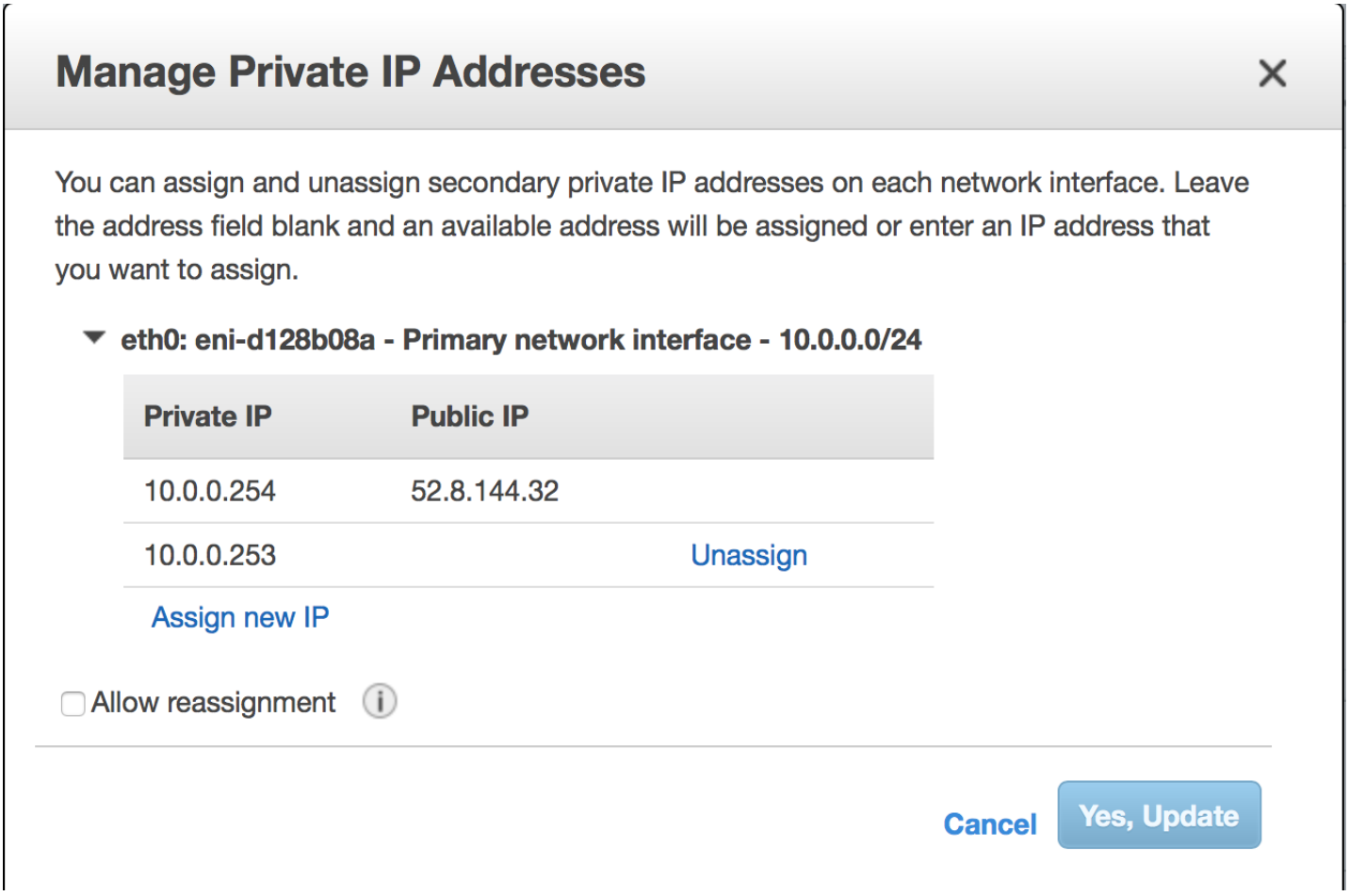
- Change the addressing mode for Port-1 from DHCP to static and enable the ability to assign Secondary IPs here.

From the FortiOS CLI

```
config system interface
   edit "Port-1"
      set vdom "root"
      set mode static
      set ip 10.0.0.254 255.255.255.0
      set allowaccess ping https ssh http fgfm
      set vlanforward enable
      set type physical
      set alias "Wan1"
      set snmp-index 1
      set secondary-IP enable
   next
end
```

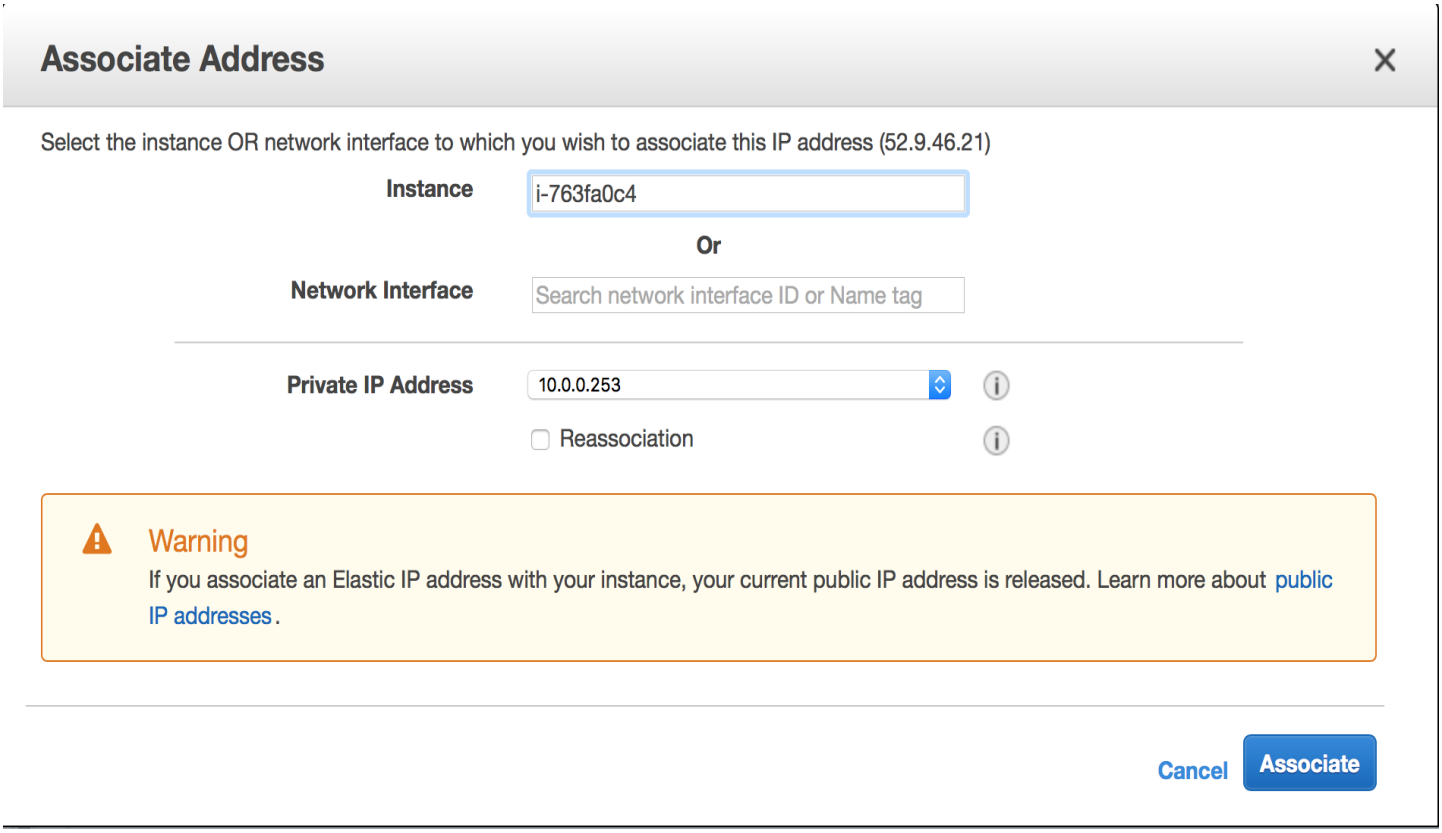
Step3: Assign the IP Address from AWS Management Console

- Assign the secondary IP address from the AWS Management Console. From the EC2 panel, navigate to the Network Interfaces and choose the ENI in question and click on Assign new IP and set the IP here.



Step4: Assign the Elastic IP to the Secondary IP Address

- Now that we have the Secondary IP address set up for the interface, we can assign an Elastic IP for the IP from the AWS Management Console. Navigate to Elastic IPs section under EC2 and then assign the Elastic IP to the newly created Secondary IP address in the step above.



Step5: Assign the Secondary IP Address in FortiOS

- In the final step, set the IP address in FortiOS. Use the following CLI commands to do the same. At this time, we should be able to use the secondary IP in Virtual IP configurations and in policies.

```
config system interface
   edit "Port-1"
      set vdom "root"
      set mode static
      set ip 10.0.0.254 255.255.255.0
      set allowaccess ping https ssh http fgfm
      set vlanforward enable
      set type physical
      set alias "Wan1"
      set snmp-index 1
      set secondary-IP enable
         config secondaryip
            edit 1
               set ip 10.0.0.253 255.255.255.0
               set allowaccess https http
            next
         end
   next
end
```