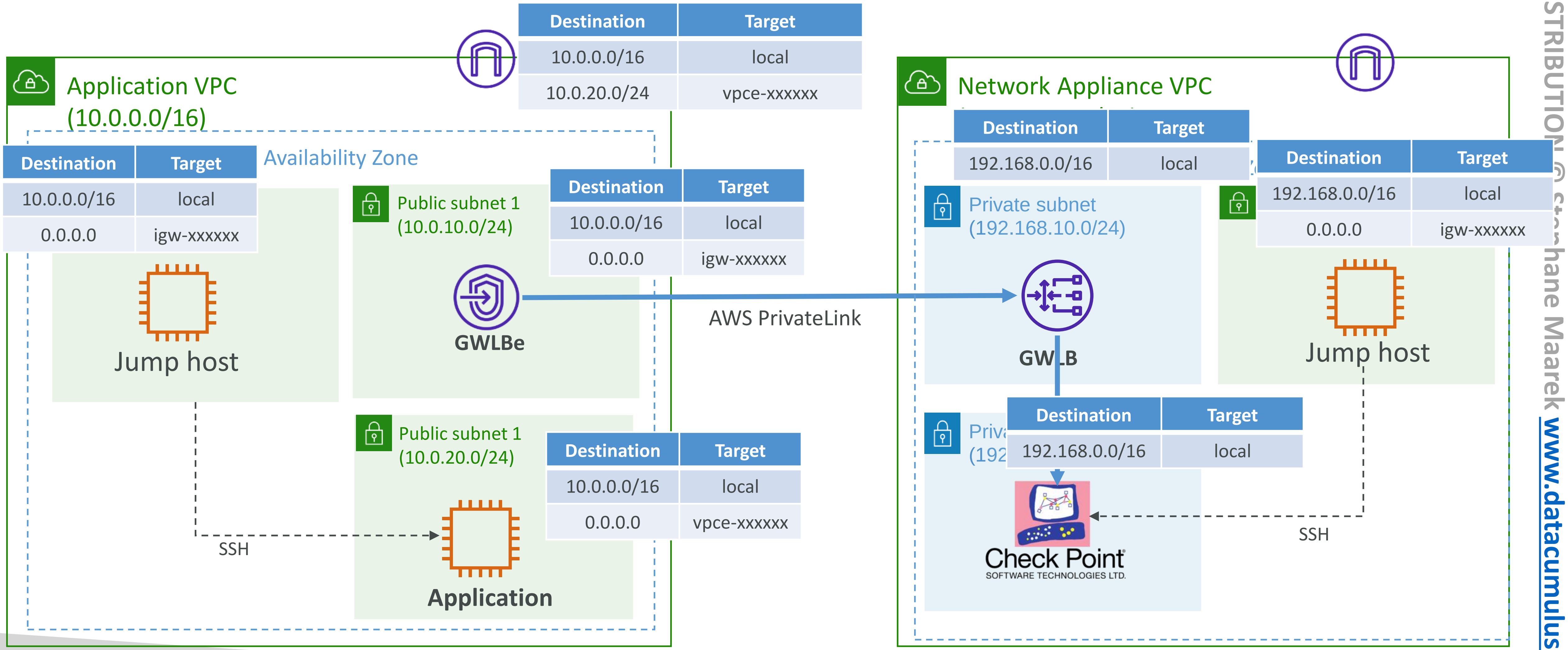
# Lab: Network setup



| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 10.0.20.0/24 | vpce-xxxxxx |

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0 | igw-xxxxxx |

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0 | igw-xxxxxx |

| Destination | Target |
|---|---|
| 10.0.0.0/16 | local |
| 0.0.0.0 | vpce-xxxxxx |

| Destination | Target |
|---|---|
| 192.168.0.0/16 | local |

| Destination | Target |
|---|---|
| 192.168.0.0/16 | local |
| 0.0.0.0 | igw-xxxxxx |

| Destination | Target |
|---|---|
| 192.168.0.0/16 | local |

# Steps - I

1. Create 2 VPCs – Application VPC and Network Appliance VPC
2. Create 3 subnets and corresponding 3 route tables in Application VPC
    1. Public subnet for jump host instance
    2. Public subnet for Application instance
    3. Public subnet for Gateway load balancer endpoint
3. Create 3 subnets and corresponding 3 route tables in Network VPC
    1. Public  subnet for Jump host instance
    2. Private subnet for Gateway load balancer (ideally we should use multiple AZs)
    3. Private subnet for the Network appliance instance (ideally we should have multiple appliance instances across multiple AZs)

# Steps - 2

4. Launch jumps hosts in both the VPCs public subnets
5. Launch an Application host in the Application VPC public subnet
6. Launch Checkpoint CloudGuard instance in Network Appliance VPC
    1. For this you need to first subscribe to the AWS marketplace AMI.
    2. SG should allow Traffic on GENEVE port 6081 from the GWLB IPs (192.168.10.0/24)
7. Create GWLB and Target group
    1. Add the Checkpoint instance as a target with healthcheck on TCP port 443
8. Create VPC endpoint service in Network Appliance VPC using GWLB
9. Create VPC endpoint in Application VPC for the GWLB service created above
10. Configure all the route tables as shown in the network diagram

# Steps - 3

10. SSH to jump host in Network Appliance VPC and from there SSH to Checkpoint instance (use the username: admin)
    - Get into the Expert mode: $expert
    - Run the tcpdump command: $tcpdump –nvv 'port 6081'
11. SSH to jump host in Application VPC and from there SSH to application host
    - From Application host: $ping www.amazon.com
12. You should see the ICMP traffic captured in the checkpoint instance tcpdump