FORTINET

Public Cloud – 102
FortiGate Foundational

Course Goals

In this course you will learn how to deploy a FortiGate NGFW and secure an Azure Virtual Network to meet the security requirements of Company ABC as they move server workloads to Azure.

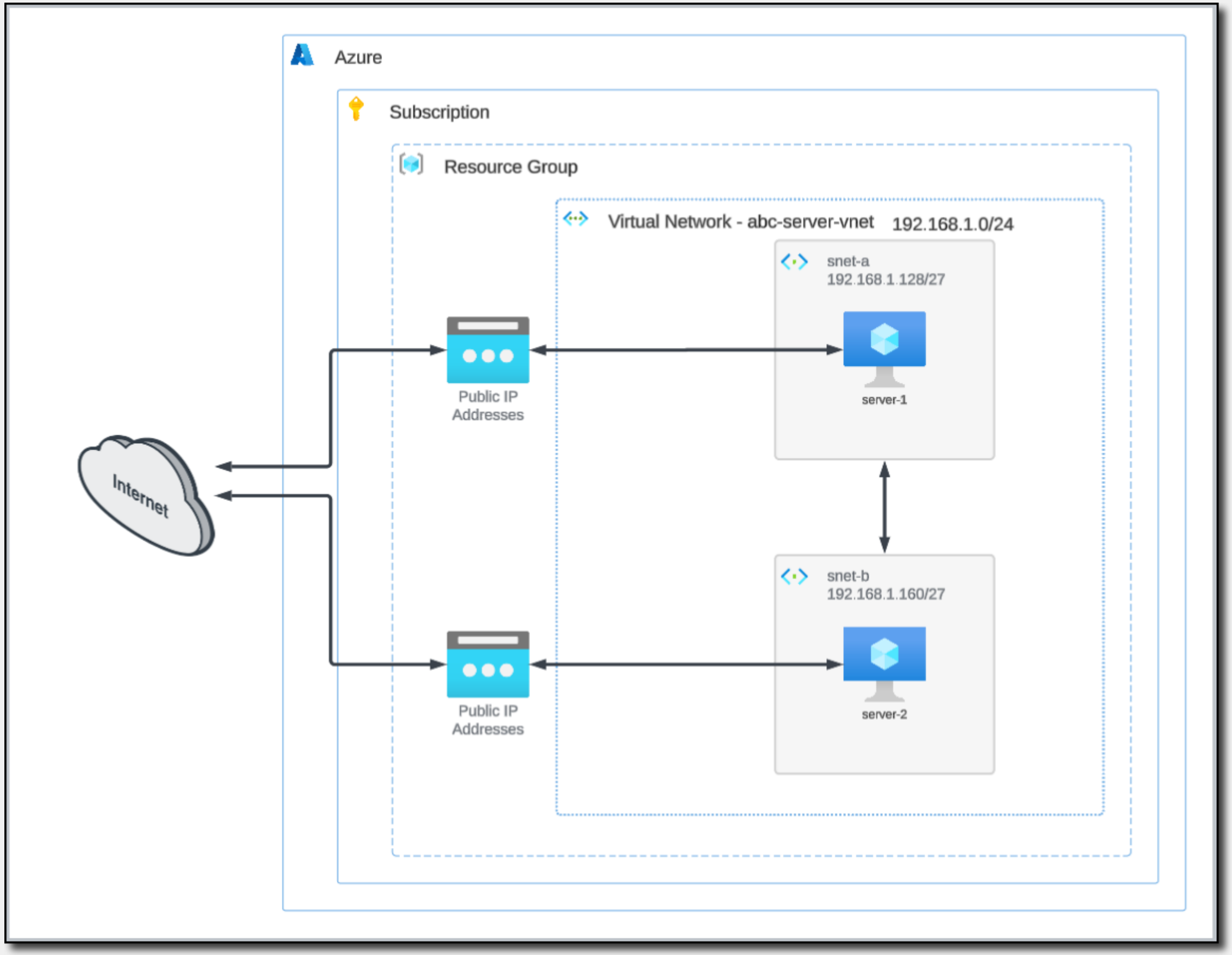
This course will start with understanding key services and terminology used in Azure when deploying public and private facing services in the public cloud. The course continues with the deployment of a FortiGate to secure the virtual network and the hosted services.

- Learn key Azure services and terms
- Deploy and configure an Azrue Virtual Network (VNET)
- Deploy server Virtual Machines (VM) in a VNET
- Deploy and configure a FortiGate Network Virtual Appliance (NVA)
- Deploy an Azure Route Table and create User Define Routes (UDR)
- Secure the VNET and hosted services utilizing FortiGate policies

Deployment Architectures – Unsecured Virtual Network

Default Virtual Network Deployment

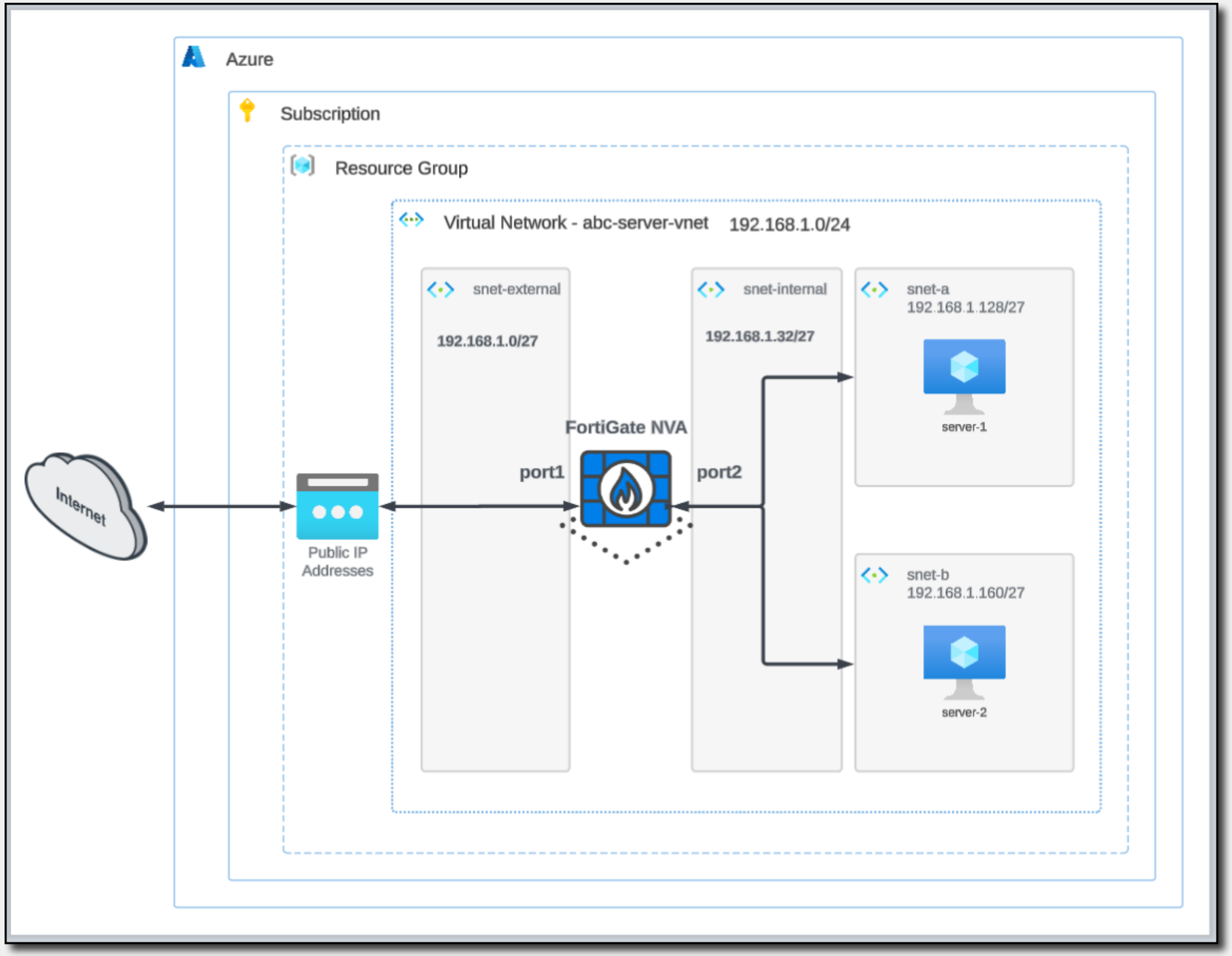
- Default traffic flow from VMs
- Direct access to other subnets
- Public IP Address ties directly to VMs
- Direct access to the Internet
- Direct access from the Internet
- Basic traffic filtering
- Multiple Public IPs
- No UTM traffic management
- No traffic security logs



Deployment Architectures – Secured Virtual Network

Secured Virtual Network Deployment

- Managed traffic flow from VMs (UDRs)
- Managed access to other subnets
- Public IP Address tied to FortiGate NVA
- Managed access to/from the Internet
- Firewall - VIPs, NAT, UTM profiles
- Additional services - IPSEC / SD-WAN
- Cost savings:
  - PIPs, VPN Gateway, Azure firewall
- Logging – FortiAnalyzer, SYSLOG, local
- FortiManager management



Fortinet Products in Azure Marketplace

Fortinet Public Cloud Deployment Guides

Questions

Moderated

Check in every 30 Minutes
Environments Available for 5 hours

Guide: https://fortinetcloudcse.github.io/azure-102-foundational

FORTINET