Networking in Azure

Contents

- What is Networking?
- Basic Networking Concepts
- Ports
- Load Balancers
- Application Gateways
- Subnet
- Security Group
- IP Traffic
- Address Space (IPv4 & IPv6)

What is Networking?

Networking is the practice of connecting computers and other devices together to share resources and information.

It enables communication, data sharing, and resource utilization across devices.

Basic Networking Concepts

- **Network:** A collection of interconnected devices.
- **Node:** Any device connected to the network.
- **Router:** Directs data between networks.
- **Switch:** Connects devices within the same network.
- **Protocol:** A set of rules for data exchange.

Azure networking services

Azure Virtual Network (VNet) enables Azure resources to communicate with each other, the internet, and on-premises networks.

- Public endpoints, accessible from anywhere on the internet
- Private endpoints, accessible only from within your network
- Virtual subnets, segment your network to suit your needs
- Network peering, connect your private networks directly together

Ports

Logical endpoints for communication.

Helps in directing data to the correct application on a device.

Common Ports:

- **HTTP (80):** Used for web traffic.
- **HTTPS (443):** Used for secure web traffic.
- **FTP (21):** Used for file transfers.
- **SMTP (25):** Used for sending emails.
- **Telnet**: Port 23 (used for remote login to network devices)
- **POP3**: Port 110 (for receiving emails)
- **IMAP**: Port 143 (for retrieving emails)

Well-Known Ports

Service	Port	Function
HTTP	80	Web traffic
HTTPS	443	Secure web traffic
FTP	20, 21	File transfer
DNS	53	Name resolution
SMTP	25	Internet mail
POP3	110	Post Office Protocol (POP) mailbox
IMAP	143	Internet Message Access Protocol (IMAP) Mailbox
Telnet	23	Remote login
SSH	22	Secure remote logn

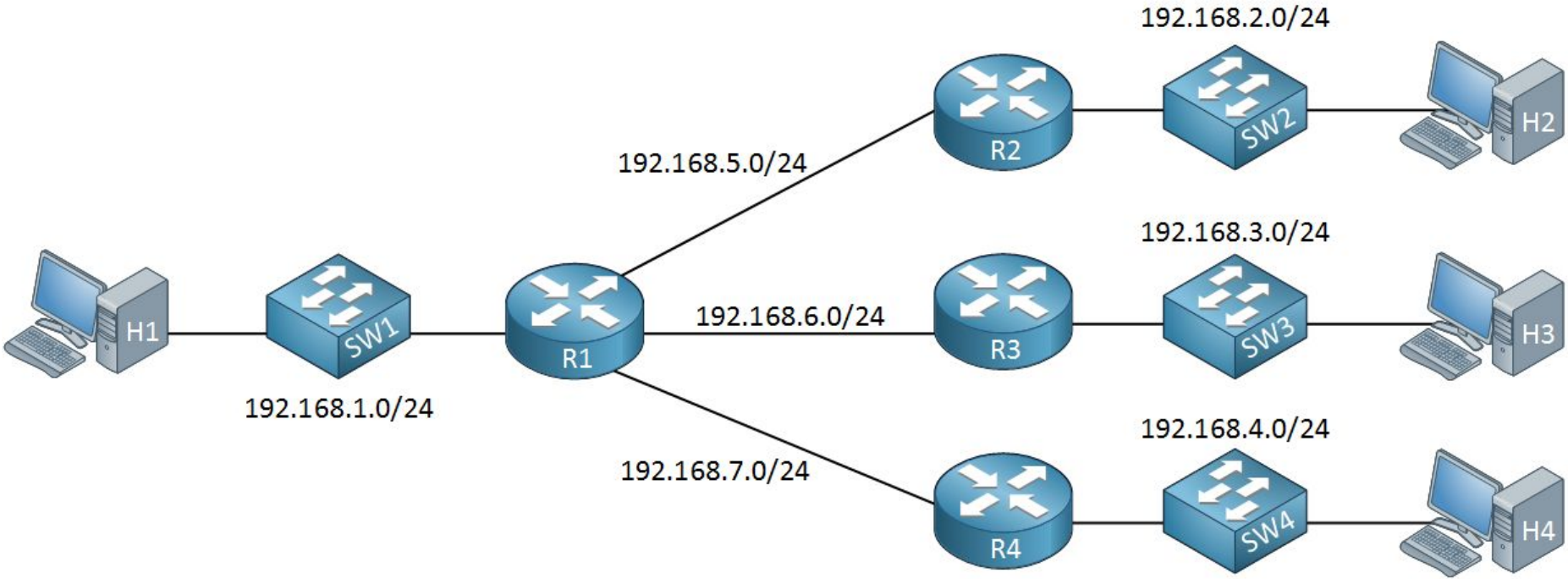
Subnets

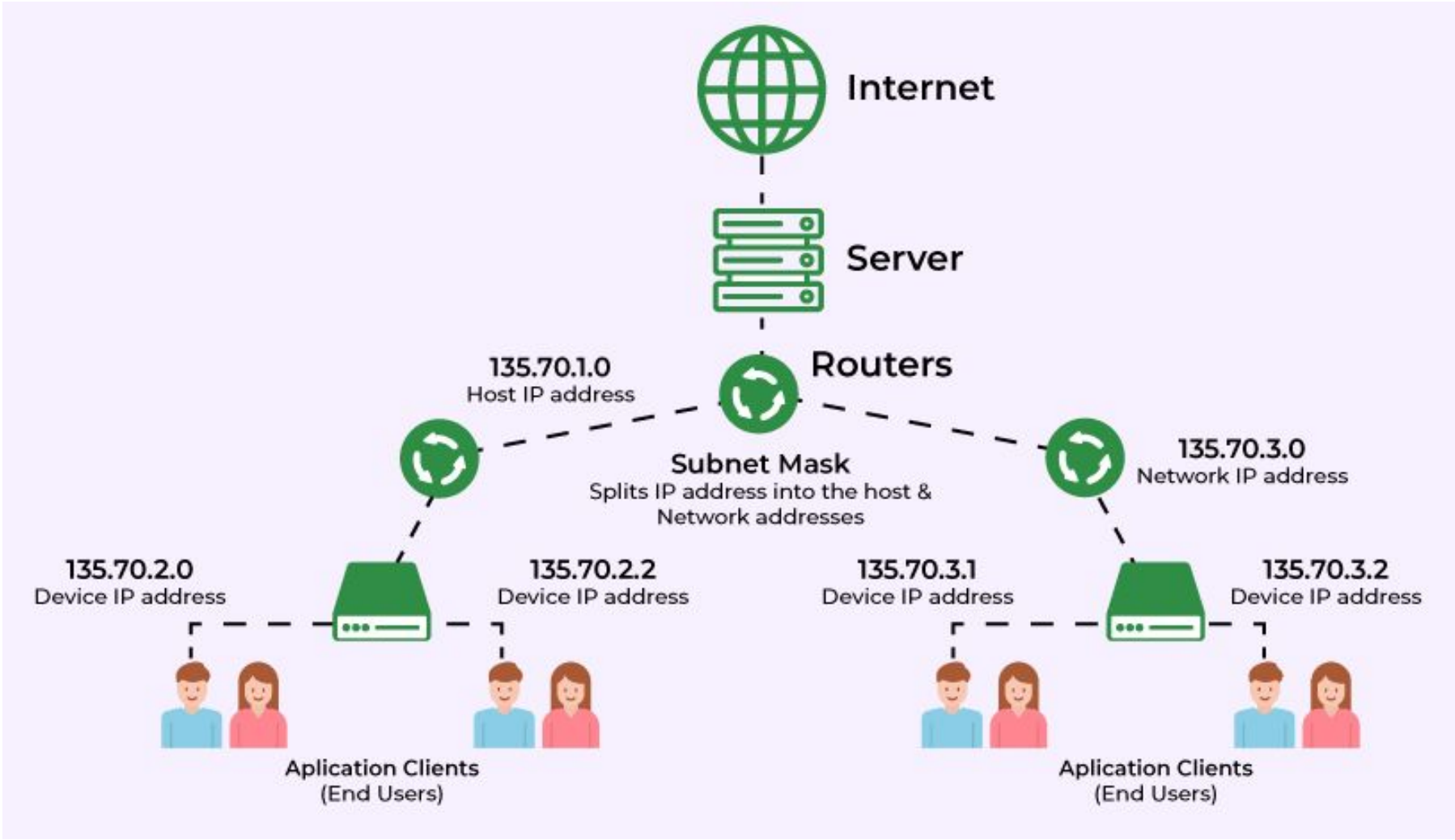
A segmented piece of a larger network.

Purpose: Improves network performance and security by isolating groups of devices.

Types:

- **Public Subnet:** Accessible from the internet.
- **Private Subnet:** Not accessible from the internet, only within the network


192.168.2.0/24
192.168.5.0/24
R2
SW2
H2
192.168.3.0/24
H1
SW1
R1
192.168.6.0/24
R3
SW3
H3
192.168.1.0/24
192.168.4.0/24
192.168.7.0/24
R4
SW4
H4


Internet
Server
Routers
135.70.1.0
Host IP address
Subnet Mask
Splits IP address into the host &
Network addresses
135.70.3.0
Network IP address
135.70.2.0
Device IP address
135.70.2.2
Device IP address
135.70.3.1
Device IP address
135.70.3.2
Device IP address
Aplication Clients
(End Users)
Aplication Clients
(End Users)

Address Space

The address space for a virtual network in Azure comprises one or more addresses that do not overlap. Classless Inter-Domain Routing notations specify these address ranges

IP Address: Unique identifier for a device on a network.

IPv4:

- **Format:** 32-bit address (e.g., 192.168.1.1).
- **Address Range:** Approximately 4.3 billion addresses.

IPv6:

- **Format:** 128-bit address (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- **Address Range:** Vastly larger than IPv4, solving address exhaustion.

IPv4

Address Size:
32-bit number

Address Format:
Dotted Decimal Notation:
192.168.1.1

Prefix Notation:
255.255.255.0
/24

Number of addresses:
2**32 = 4,294,967,296

IPv6

Address Size:
128-bit number

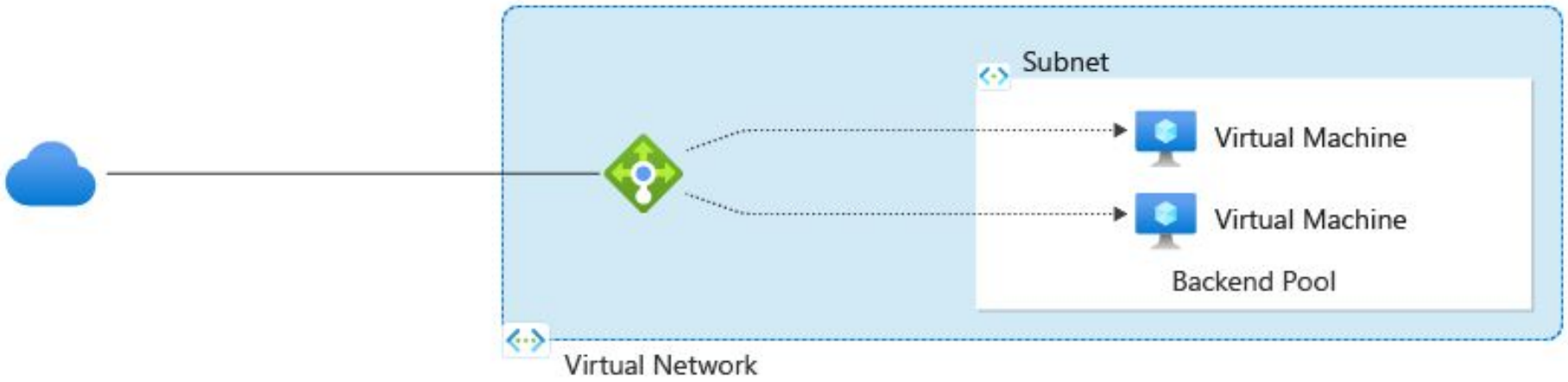
Address Format:
Hexadecimal Notation:
fe80::94db:946e:8d4e:129e

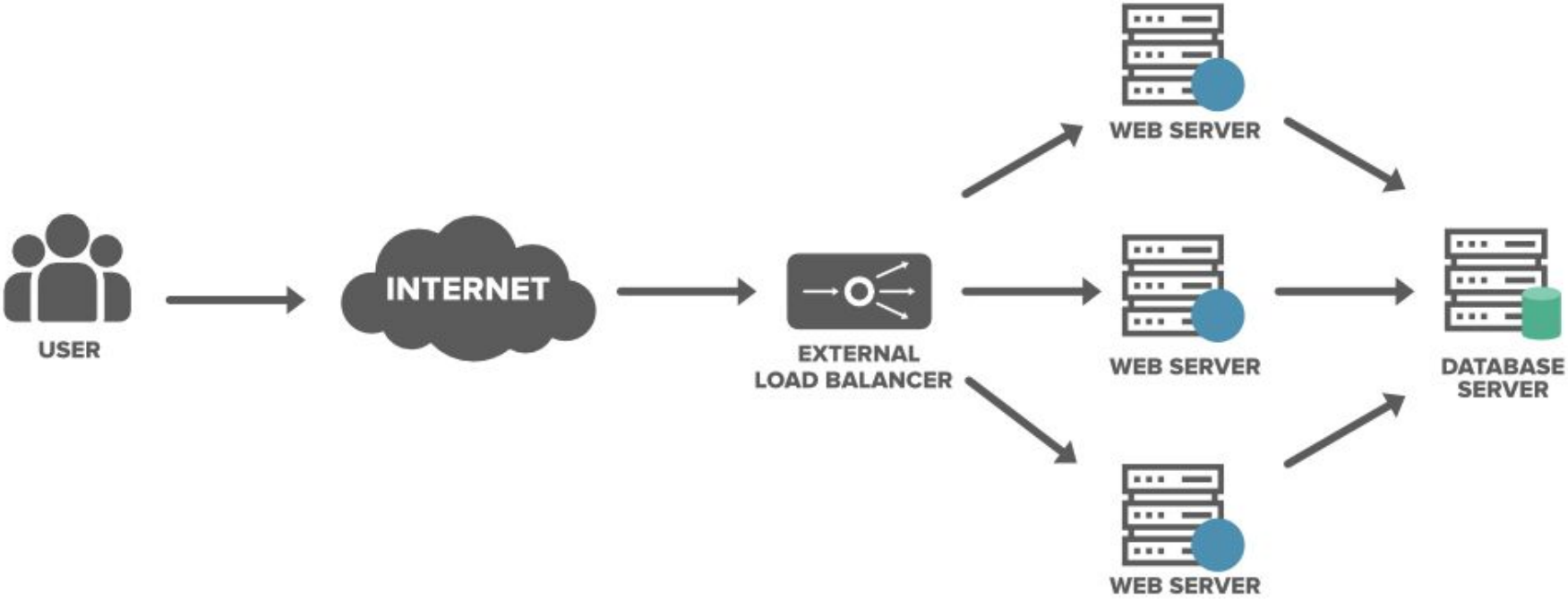
Prefix Notation:
/64

Number of addresses:
2**128 =
340,282,366,920,938,463,463,374,607,
431,768,211,456

Load Balancers

Distributes incoming network traffic across multiple servers. It enhances the availability and reliability of applications.




USER
INTERNET
EXTERNAL
LOAD BALANCER
WEB SERVER
WEB SERVER
WEB SERVER
DATABASE
SERVER

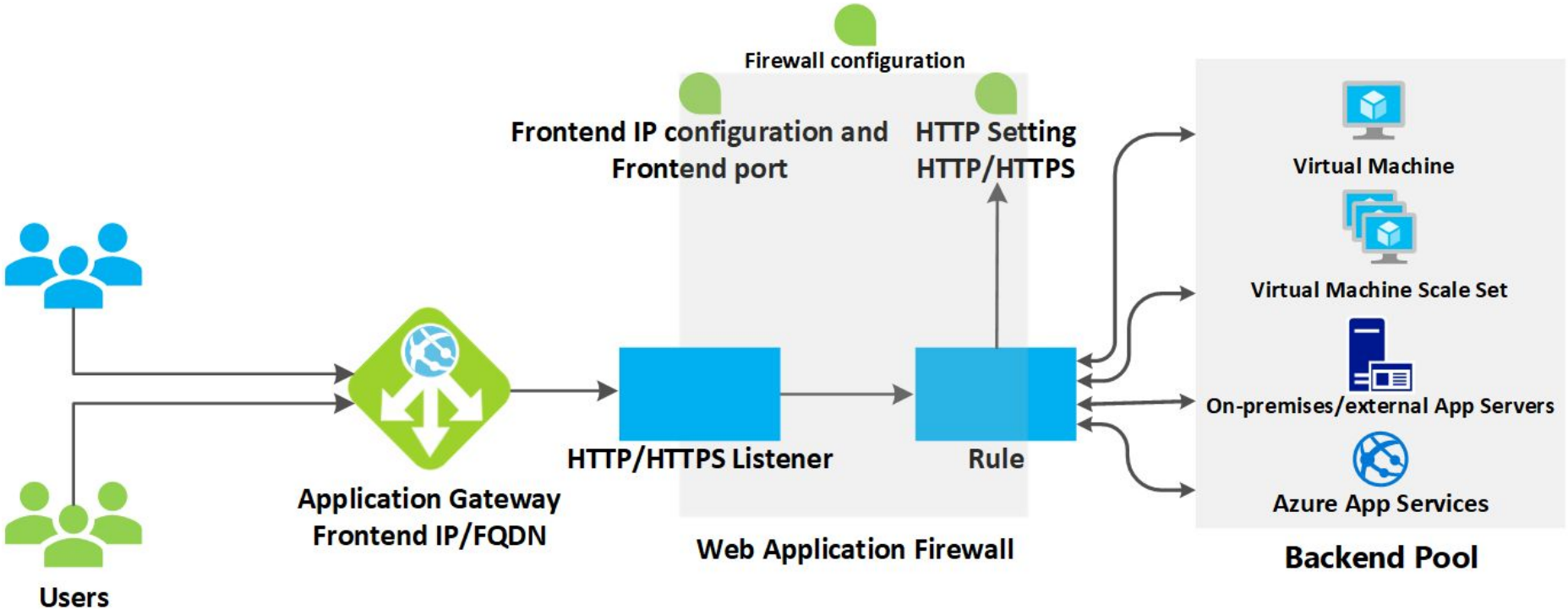
Application Gateways

Acts as an intermediary that controls communication between clients and servers.

It provides enhanced security, monitoring, and performance optimization.

Functions:

- **Firewall:** Filters traffic based on predefined security rules.
- **Proxy:** Acts on behalf of clients to fetch data from servers.


Firewall configuration
Frontend IP configuration and
Frontend port
HTTP Setting
HTTP/HTTPS
Virtual Machine
Virtual Machine Scale Set
On-premises/external App Servers
Azure App Services
Backend Pool
Users
Application Gateway
Frontend IP/FQDN
HTTP/HTTPS Listener
Rule
Web Application Firewall

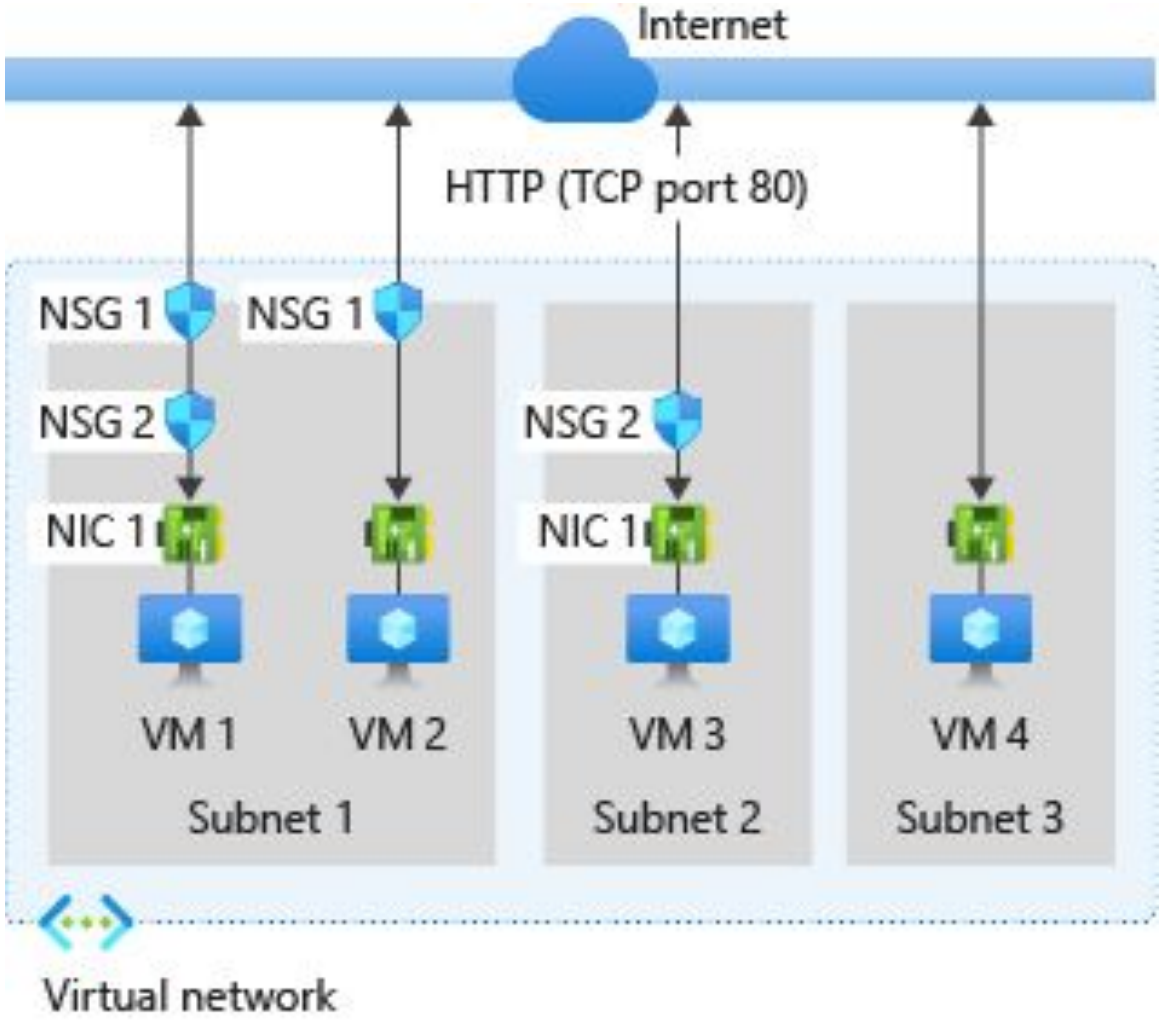
Security Groups

A virtual firewall for controlling inbound and outbound traffic to resources.

It enhances security by specifying allowed traffic.

Rules:

- **Inbound Rules:** Define what traffic is allowed to enter the network.
- **Outbound Rules:** Define what traffic is allowed to leave the network.


Internet
HTTP (TCP port 80)
NSG 1
NSG 1
NSG 2
NSG 2
NIC 1
NIC 1
VM 1
VM 2
VM 3
VM 4
Subnet 1
Subnet 2
Subnet 3
Virtual network

Quiz Time

https://quizizz.com/admin/quiz/6686da9185ed971bc9a53956?source=admin&trigger=quizPage

Get Certified!

- Configure secure access to workloads with Azure virtual networking services:

  https://learn.microsoft.com/en-us/credentials/applied-skills/configure-secure-workloads-use-azure-virtual-networking/

  Guided Project - https://microsoftlearning.github.io/Configure-secure-access-to-workloads-with-Azure-virtual-networking-services/

Assignment

- Create an Azure virtual network with four subnets with this address space 192.148.30.0/26
- Configure secure access to workloads with Azure virtual networking services:

  https://learn.microsoft.com/en-us/credentials/applied-skills/configure-secure-workloads-use-azure-virtual-networking/

  Submission Link - https://forms.gle/XsZRVRiGDCo9YVhx7