Introduction to NSG and ASG

Introduction to Network Security Groups

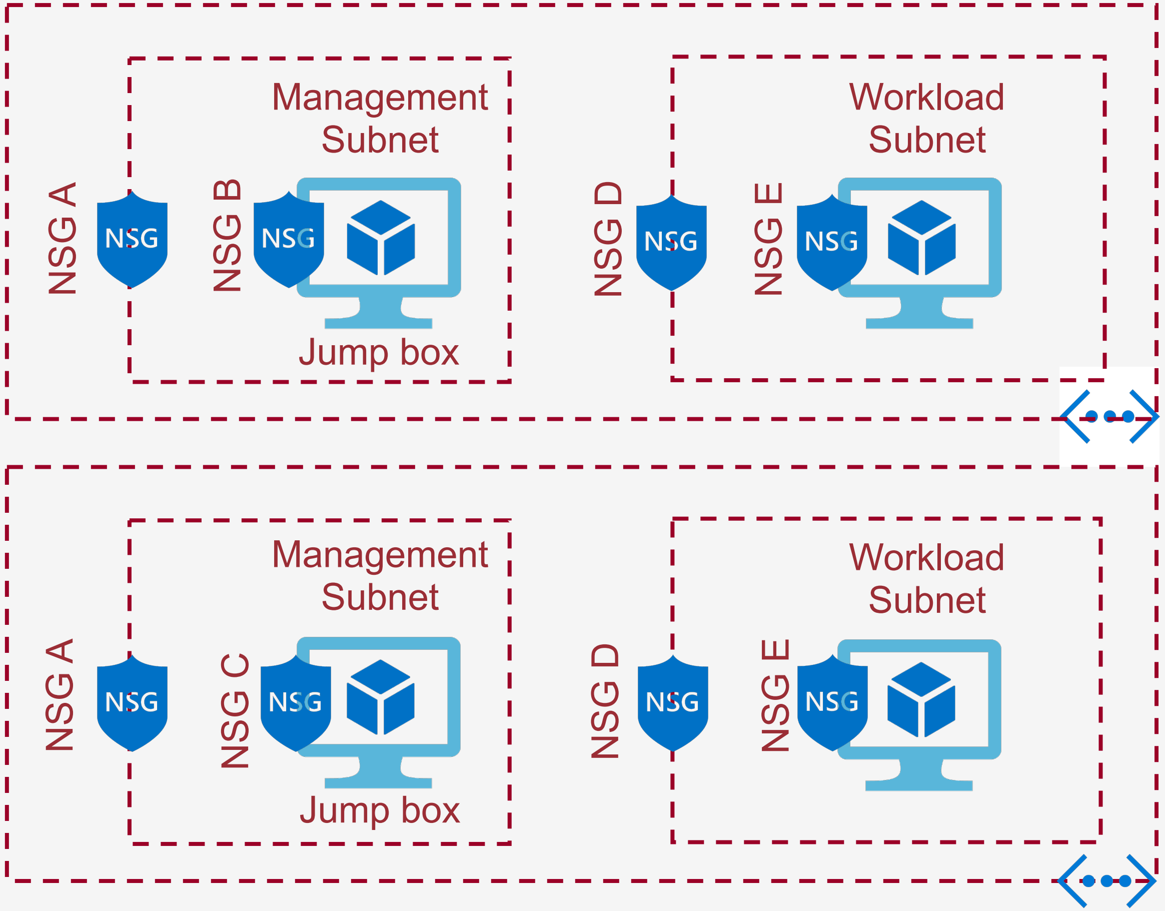
A network security group contains security rules that allow or deny Inbound / Outbound network traffic to or from several types of Azure resources.

NSG A

- Inbound rule – Allow RDP connections
- Outbound internet – Allow

NSG B

- Inbound rule – Allow RDP from specific IP address
- Outbound internet – Allow connection to Azure services



Security Rule properties

- Name - A unique name within the network security group.

- Priority - A number between 100 and 4096. Rules are processed in priority order with lower numbers has highest priority

- Source or Destination - Any, or an individual IP address, classless inter-domain routing (CIDR) block (10.0.0.0/24, for example), service tag, or application security group. The ability to specify multiple individual IP addresses and ranges (you cannot specify multiple service tags or application groups) in a rule is referred to as augmented security rules.

- Protocol – TCP, UDP or Any

- Port range - You can specify an individual or range of ports

- Action – Allow or Deny

Service Tags

A service tag represents a group of IP address prefixes to help minimize complexity for security rule creation. You cannot create your own service tag, nor specify which IP addresses are included within a tag. Microsoft manages the address prefixes encompassed by the service tag, and automatically updates the service tag as addresses change.

01 ***Storage -*** This tag denotes the IP address space for the Azure Storage service. If you specify Storage for the value, traffic is allowed or denied to storage.

02 ***Sql -*** This tag denotes the address prefixes of the Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure SQL Data Warehouse services.

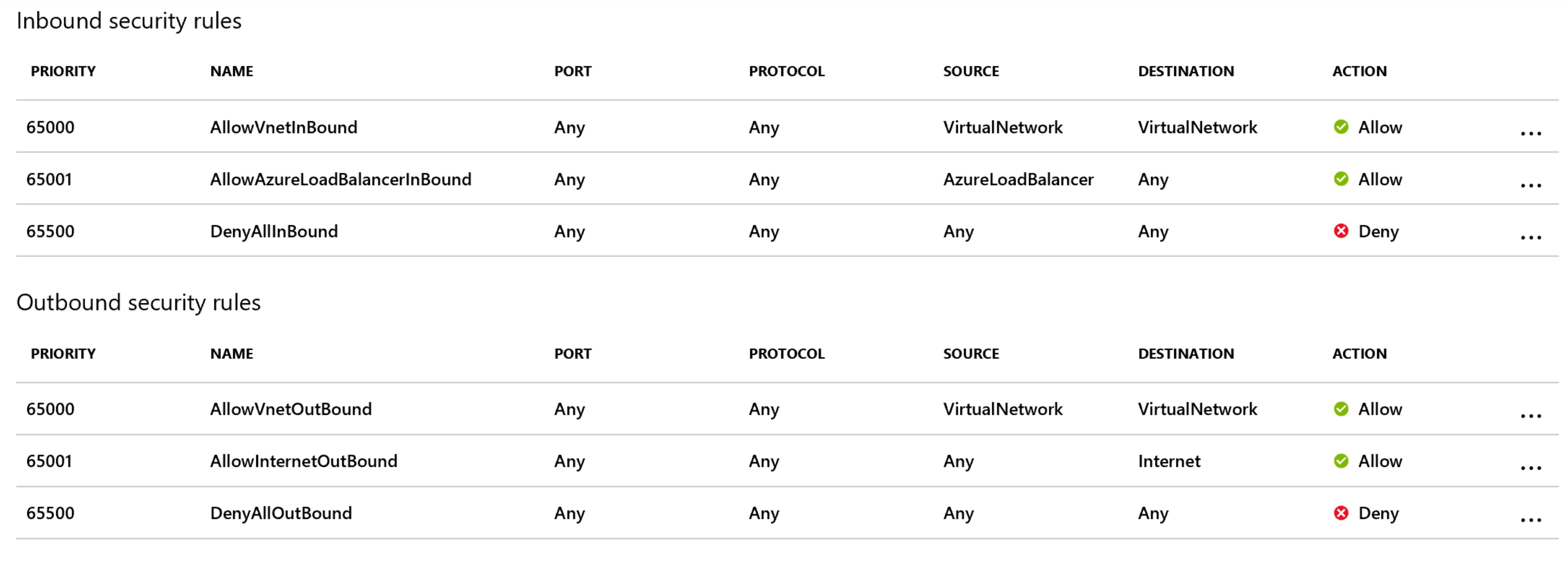
03 ***Azure CosmosDB -*** This tag denotes the address prefixes of the Azure Cosmos Database service.

04 ***AzureKeyVault -*** This tag denotes the address prefixes of the Azure KeyVault service. If you specify Azure KeyVault for the value, traffic is allowed or denied to AzureKeyVault.

05 ***EventHub -*** This tag denotes the address prefixes of the Azure EventHub service. If you specify EventHub for the value, traffic is allowed or denied to EventHub..

Default NSG rules

RUDRA
PRODUCTS & SERVICES



Inbound security rules

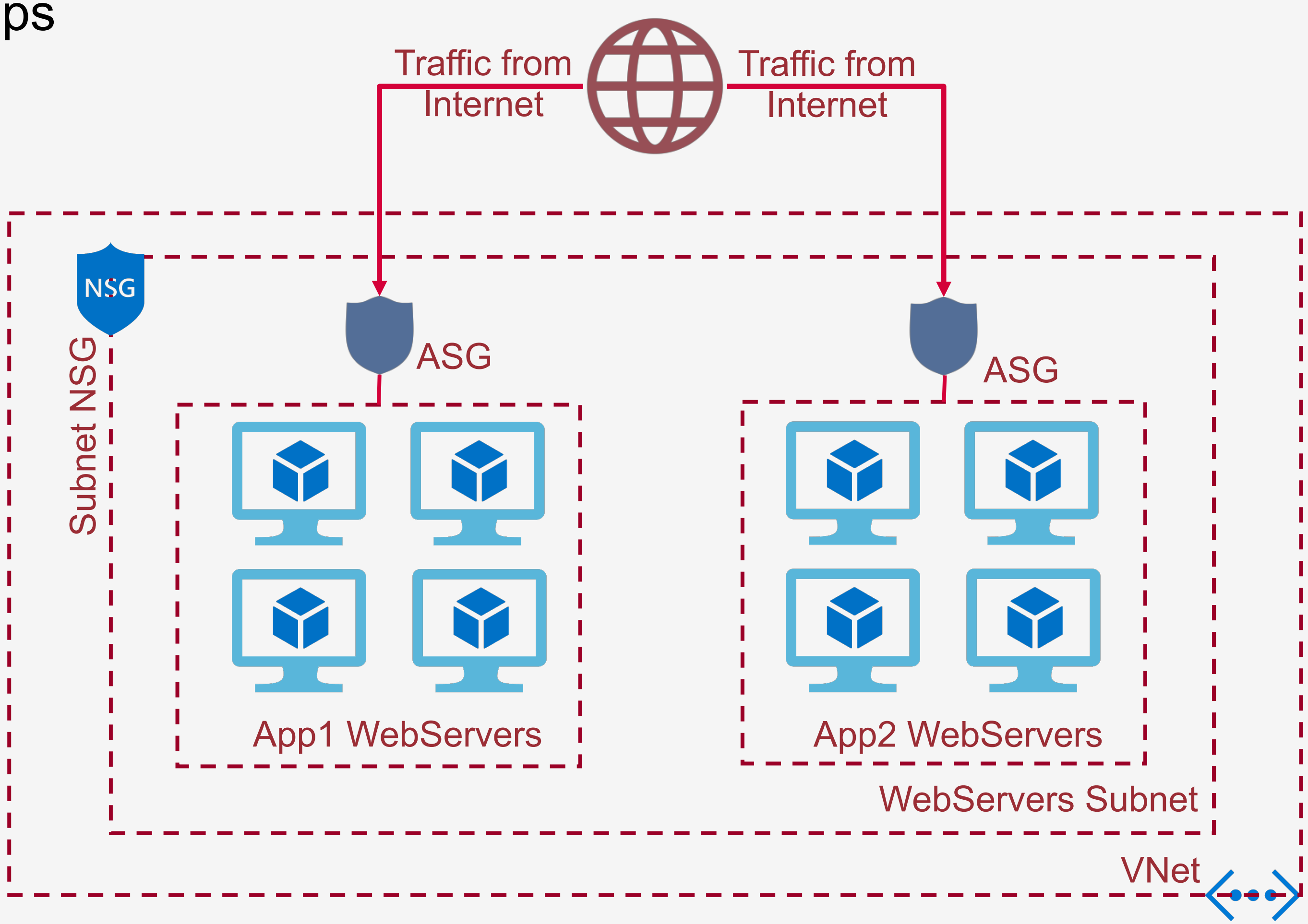
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny	...

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow	...
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow	...
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny	...

Application Security Group

Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups


Traffic from Internet
Traffic from Internet
NSG
Subnet NSG
ASG
ASG
App1 WebServers
App2 WebServers
WebServers Subnet
VNet