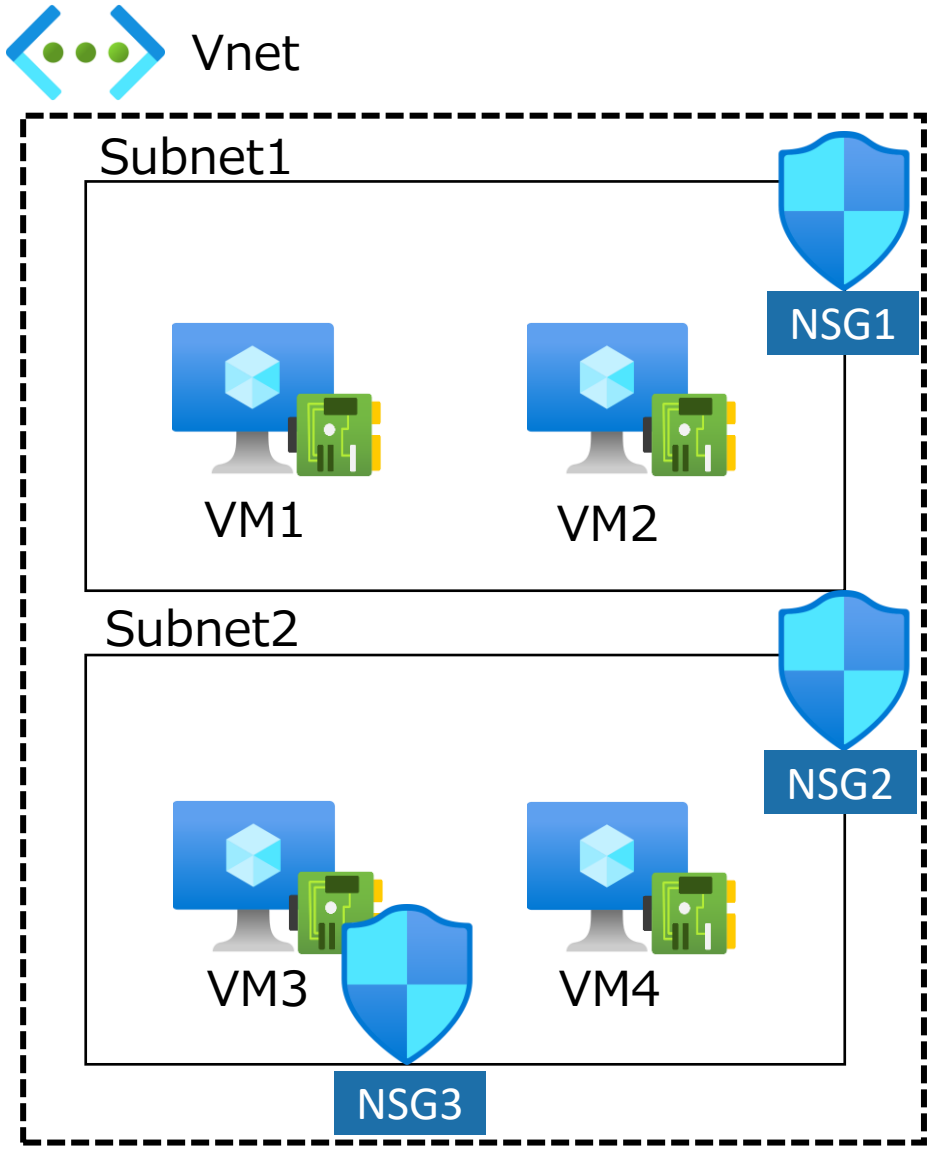
NSGまとめ



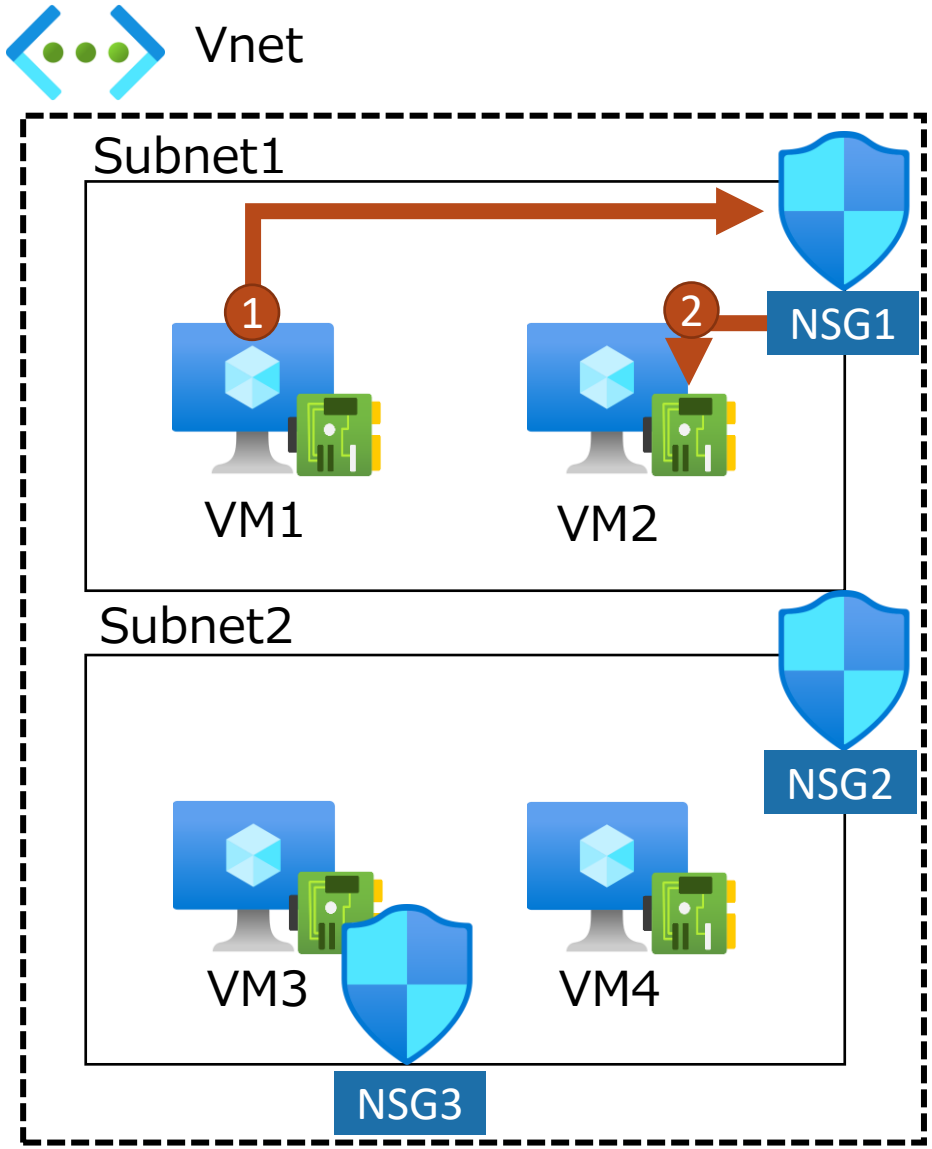
NSGはSubnet、NICに対して設定できる
→Vnetではない

考え方としては、VM主体で受信時はSubnet、NICに割り当てられているNSGを適用する。送信時はNIC、Subnetに割り当てられているNSGを適用する。

■受信トラフィック
受信トラフィックの場合、Azure は、サブネットに関連付けられているネットワーク セキュリティ グループがあれば、まずその規則を処理し、次にネットワーク インターフェイスに関連付けられているネットワーク セキュリティ グループがあれば、その規則を処理します。

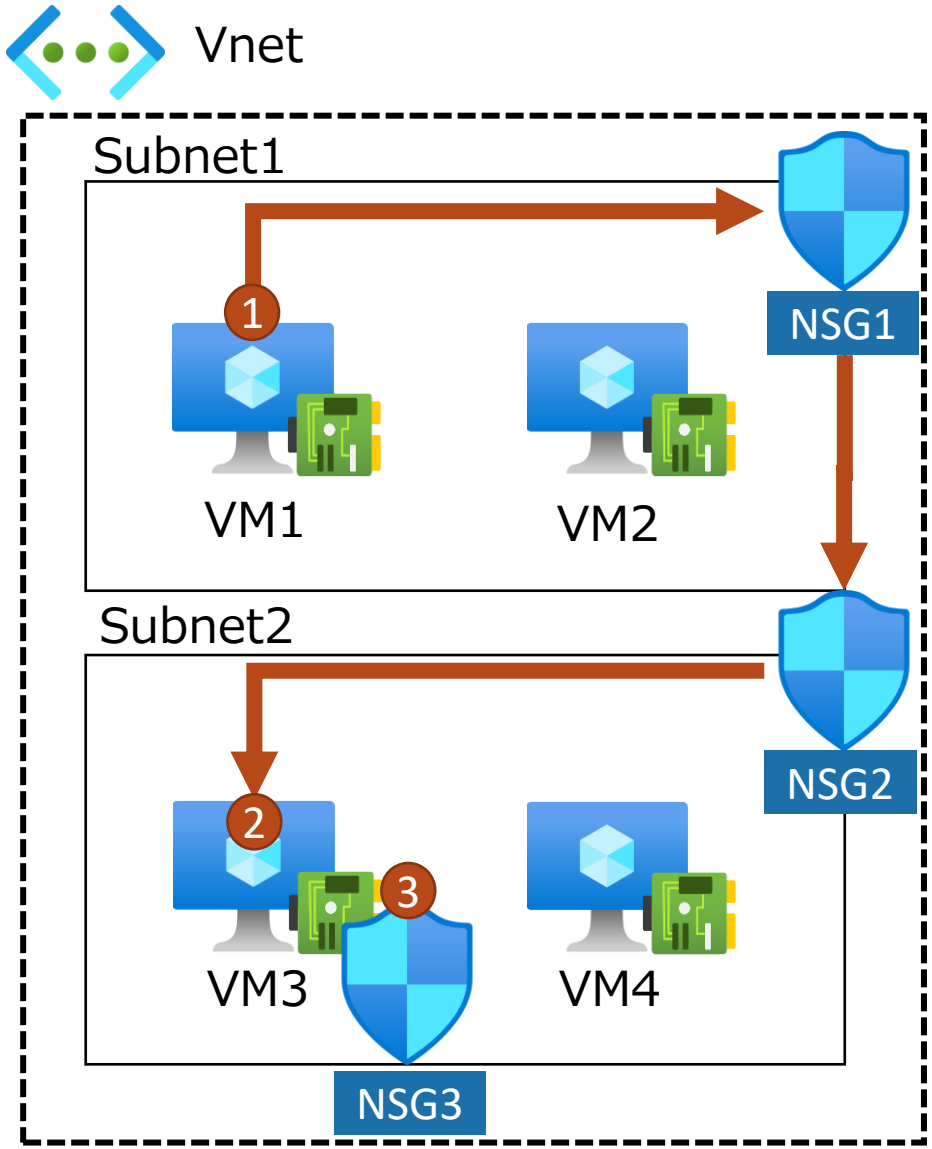
■送信トラフィック
送信トラフィックの場合、Azure はネットワーク インターフェイスに関連付けられているネットワーク セキュリティ グループがあれば、まずその規則を処理し、次にサブネットに関連付けられているネットワーク セキュリティ グループがあれば、その規則を処理します。

NSGまとめ



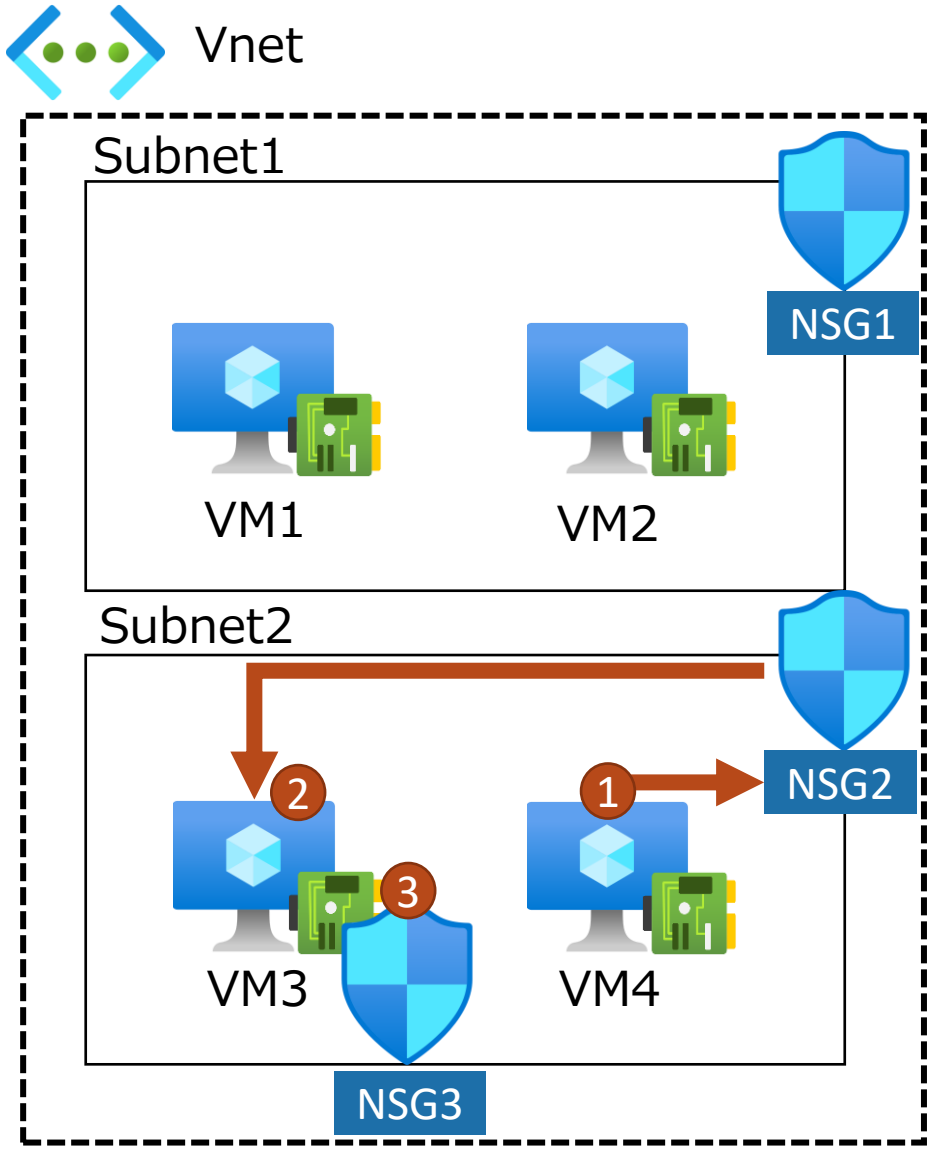
VM1 to VM2
①NSG1の送信ルール（Subnet1に紐づいている）
②NSG1の受信ルール（Subnet1に紐づいている）
が評価される
→同じサブネット内であれば、隣のサーバにはフリーで繋がるわけではない。デフォルトルールで仮想ネットワーク間の通信は全ポート送受信ともに「許可」設定になっているため自在に接続ができているように見えている。

NSGまとめ



VM1 to VM3
・NSG1の送信ルール（Subnet1に紐づいている）
・NSG2の受信ルール（Subnet2に紐づいている）
・NSG3の受信ルール（VM3のNICに紐づいている）
が評価される

NSGまとめ



VM4 to VM3
①NSG2の送信ルール（Subnet1に紐づいている）
②NSG2の受信ルール（Subnet1に紐づいている）
②NSG3の受信ルール（VM3のNICに紐づいている）
が評価される