Solution to the Problem Statement

Answers to Planning questions –

1. What Azure locations will you use to host VNets?

   2 locations in North America, and 2 locations in Europe. You should pick those based on the physical location of your existing on-premises data centers. That way your connection from your physical locations to Azure will have a better latency.

2. Do you need to provide communication between these Azure locations?

   Yes. Since the databases must be replicated to all locations.

3. Do you need to provide communication between your Azure VNet(s) and your on-premises data center(s)?

   Yes. Since users connected to the on-premises data centers must be able to access the applications through an encrypted tunnel.

4. How many IaaS VMs do you need for your solution?

   200 IaaS VMs. App1, App2, App3, and App4 require 5 web servers each, 2 applications servers each, and 2 database servers each. That's a total of 9 IaaS VMs per application, or 36 IaaS VMs. App5 and App6 require 5 web servers and 2 database servers each. That's a total of 7 IaaS VMs per application, or 14 IaaS VMs. Therefore, you need 50 IaaS VMs for all applications in each Azure region. Since we need to use 4 regions, there will be 200 IaaS VMs.

   You will also need to provide DNS servers in each VNet, or in your on-premises data centers to resolve name between your Azure IaaS VMs and your on-premises network.

5. Do you need to isolate traffic based on groups of VMs (i.e. front end web servers and back end database servers)?

   Yes. Each application should be completely isolated from each other, and each application layer should also be isolated.

6. Do you need to control traffic flow using virtual appliances?

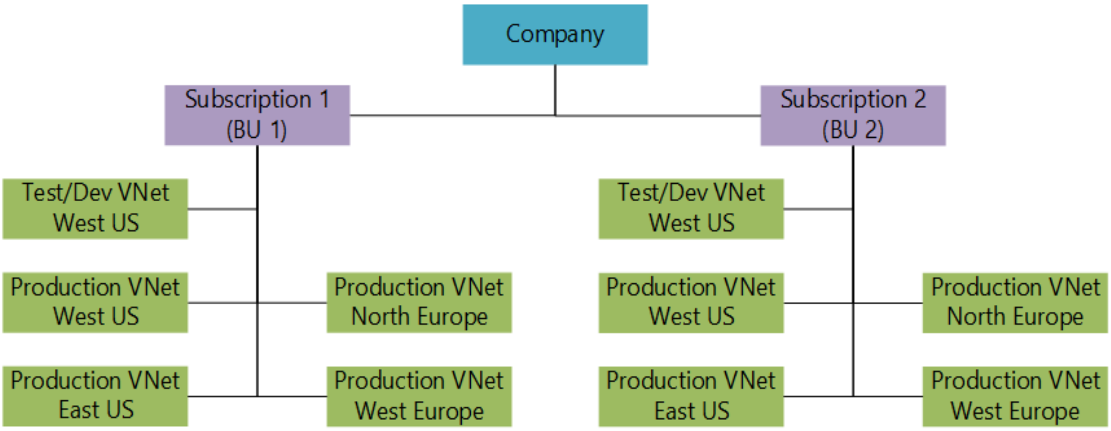
No. Virtual appliances can be used to provide more control over traffic flow, including more detailed data plane logging.

7. Do users need different sets of permissions to different Azure resources?

   Yes. The networking team needs full control on the virtual networking settings, while developers should only be able to deploy their VMs to pre-existing subnets.

Design Requirement Solution –

Based on those requirements, you need a subscription for each business unit. That way, consumption of resources from a business unit will not count towards limits for other business units. And since you want to minimize the number of VNets, you should consider using the **one subscription per business unit, two VNets per group of apps** pattern as seen below.



You also need to specify the address space for each VNet. Since you need connectivity between the on-premises data centers and the Azure regions, the address space used for Azure VNets cannot clash with the on-premises network, and the address space used by each VNet should not clash with other existing VNets. You could use the address spaces in the table below to satisfy these requirements.

Subscription	VNet	Azure region	Address space
BU1	ProdBU1US1	West US	172.16.0.0/16
BU1	ProdBU1US2	East US	172.17.0.0/16
BU1	ProdBU1EU1	North Europe	172.18.0.0/16
BU1	ProdBU1EU2	West Europe	172.19.0.0/16
BU1	TestDevBU1	West US	172.20.0.0/16
BU2	TestDevBU2	West US	172.21.0.0/16
BU2	ProdBU2US1	West US	172.22.0.0/16
BU2	ProdBU2US2	East US	172.23.0.0/16
BU2	ProdBU2EU1	North Europe	172.24.0.0/16
BU2	ProdBU2EU2	West Europe	172.25.0.0/16

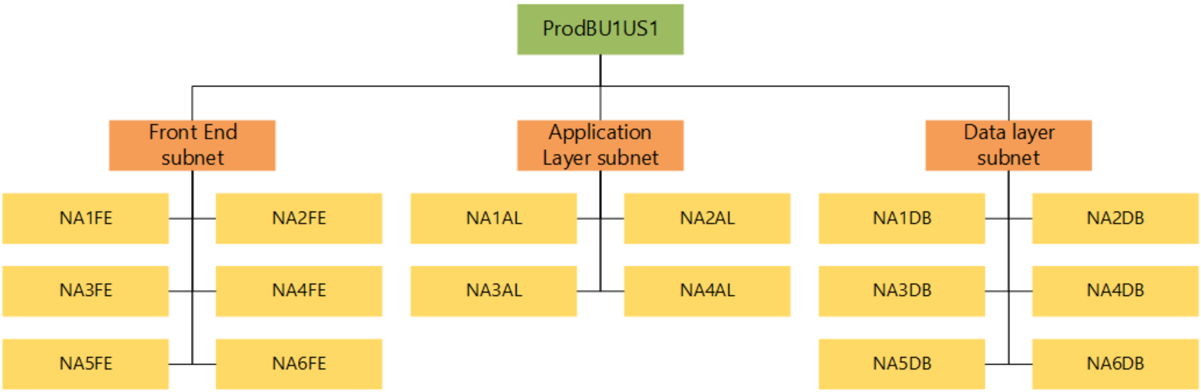
Requirement for Subnets and Network Security Groups - Solution

Number of subnets and NSGs

The following requirements are related to subnets and NSGs:

- You should minimize the amount of VNets and subnets.
- Each application is completely isolated from each other.
- Each application can be accessed by customers over the Internet using HTTP.
- Each application can be accessed by users connected to the on-premises data centers by using an encrypted tunnel.
- Connection to on-premises data centers should use existing VPN devices.
- The databases in each location should replicate to other Azure locations once a day.

Based on those requirements, you could use one subnet per application layer, and use NSGs to filter traffic per application. That way, you only have 3 subnets in each VNet (front end, application layer, and data layer) and one NSG per application per subnet. In this case, you should consider using the **one subnet per application layer, NSGs per app** design pattern. The figure below shows the use of the design pattern representing the **ProdBU1US1** VNet.



However, you also need to create an extra subnet for the VPN connectivity between the VNets, and your on-premises data centers. And you need to specify the address space for each subnet. The figure below shows a sample solution for **ProdBU1US1** VNet. You would replicate this scenario for each VNet. Each color represents a different application.

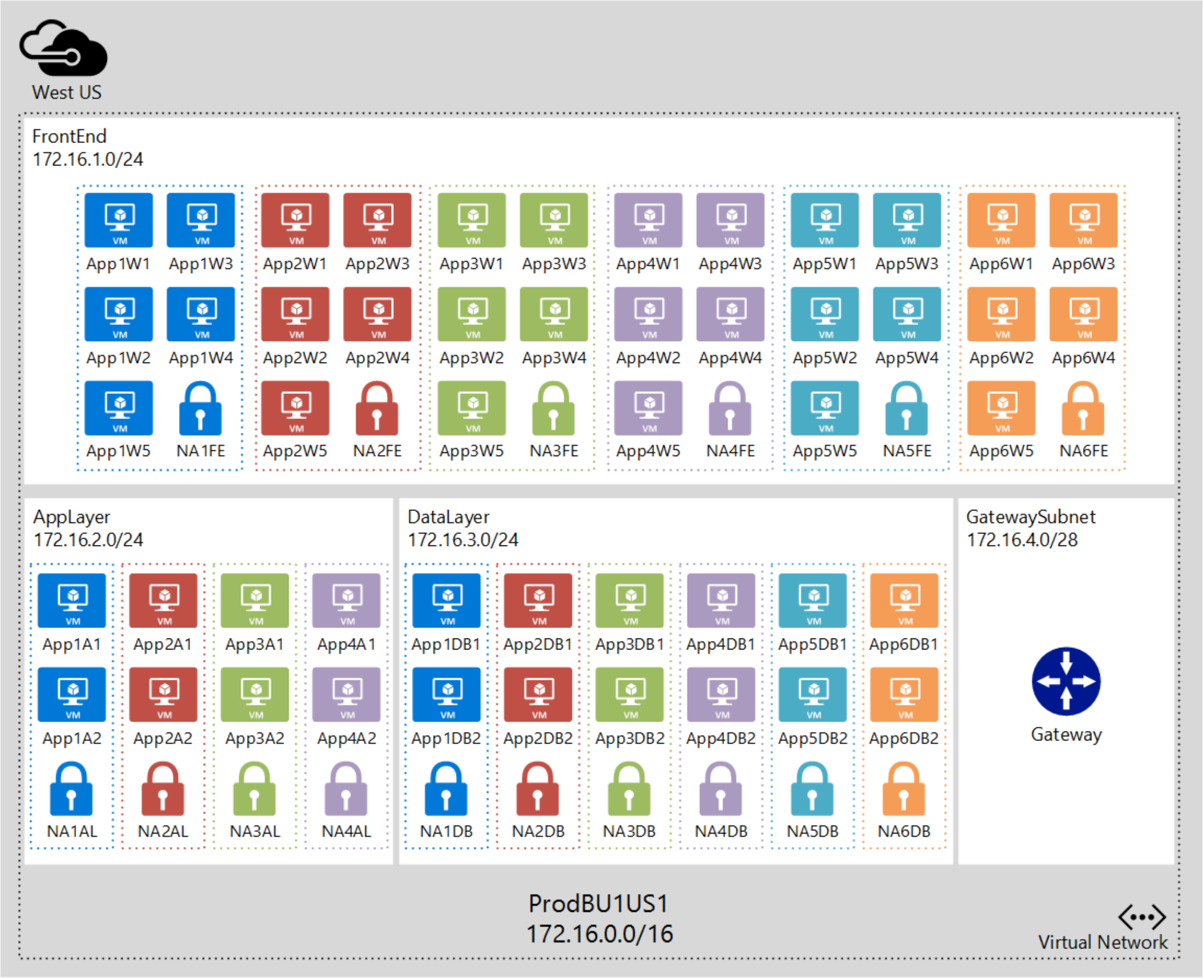
Access Control

The following requirements are related to access control:

- The company's networking group should have full control over the VNet configuration.
- Developers in each business unit should only be able to deploy VMs to existing subnets.

Based on those requirements, you could add users from the networking team to the built-in **Network Contributor** role in each subscription; and create a custom role for the application developers in each subscription giving them rights to add VMs to existing subnets.

Final Architecture of Virtual Network in Azure


West US
FrontEnd
172.16.1.0/24
App1W1
App1W3
App1W2
App1W4
App1W5
NA1FE
App2W1
App2W3
App2W2
App2W4
App2W5
NA2FE
App3W1
App3W3
App3W2
App3W4
App3W5
NA3FE
App4W1
App4W3
App4W2
App4W4
App4W5
NA4FE
App5W1
App5W3
App5W2
App5W4
App5W5
NA5FE
App6W1
App6W3
App6W2
App6W4
App6W5
NA6FE
AppLayer
172.16.2.0/24
App1A1
App1A2
NA1AL
App2A1
App2A2
NA2AL
App3A1
App3A2
NA3AL
App4A1
App4A2
NA4AL
DataLayer
172.16.3.0/24
App1DB1
App1DB2
NA1DB
App2DB1
App2DB2
NA2DB
App3DB1
App3DB2
NA3DB
App4DB1
App4DB2
NA4DB
App5DB1
App5DB2
NA5DB
App6DB1
App6DB2
NA6DB
GatewaySubnet
172.16.4.0/28
Gateway
ProdBU1US1
172.16.0.0/16
Virtual Network