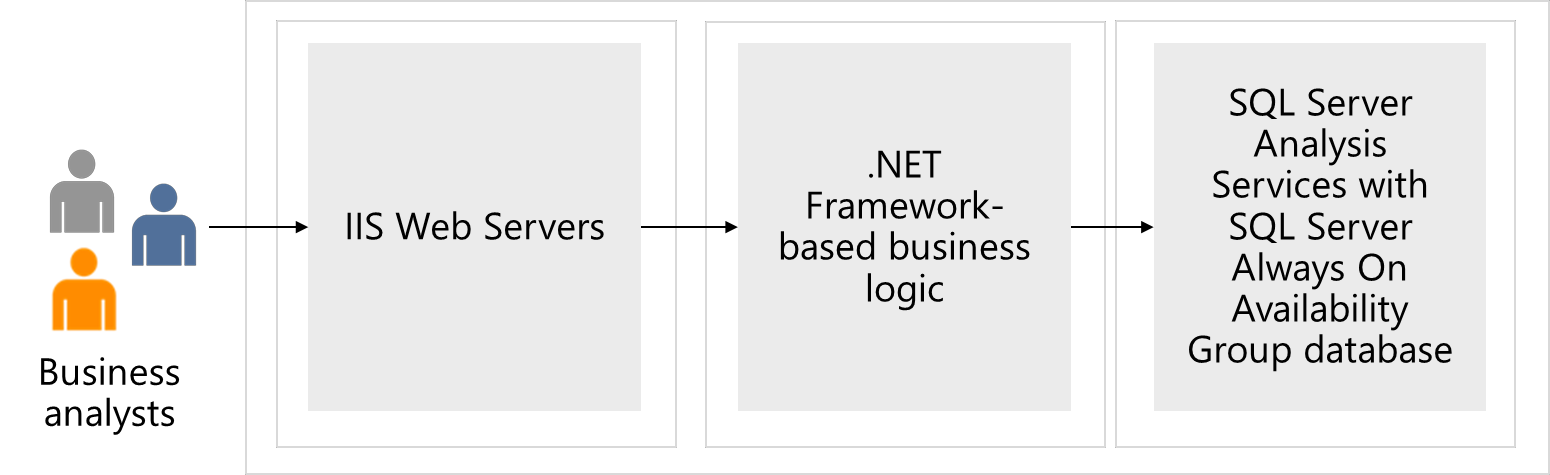
Networking

Estimated time: 120 minutes  
Requirements

As the Tailwind Traders Enterprise IT team prepares to define the strategy to migrate some of company’s workloads to Azure, it must identify the required networking components and  
design a network infrastructure necessary to support them. Considering the global scope of its operations, Tailwind Traders will be using multiple Azure regions to host its applications. Most of these applications have dependencies on infrastructure and data services, which will also reside in Azure. Internal applications migrated to Azure must remain accessible to Tailwind Traders users. Internet-facing applications migrated to Azure must remain accessible to any external customer.

To put together the initial networking design, the Tailwind Traders Enterprise IT team chose a key application, which is representative of the most common categories of workloads that are expected to be migrated to Azure:

**BI enterprise application**



* An internal, Windows-based, three-tier business intelligence (BI) enterprise application with the front-end tier running IIS web servers, the middle tier hosting .NET Framework based business logic, and the back-end tier implemented as a SQL Server Always On Availability Group database.
* This application is categorized as mission-critical and requires high availability provisions with the availability SLA of 99.99% and disaster recovery provisions, with 10-minute RPO and 2-hour RTO.
* To provide connectivity to internal apps migrated to Azure, Tailwind Traders will need to establish hybrid connectivity from their on-premises datacenters. The Enterprise IT group already established that such connectivity will be implemented by using ExpressRoute circuit from its main Seattle datacenter, however, at this point it is not clear yet what would be failover solution in case that circuit becomes unavailable. The Tailwind Traders CFO wants to avoid paying for another, redundant ExpressRoute circuit.
* There are additional considerations that apply to on-premises connectivity to internal apps migrated to Azure. Since the Tailwind Traders Azure environment will consist of multiple subscriptions and, effectively, multiple virtual networks, to minimize cost, it is important to minimize the number of Azure resources required to implement core networking capabilities. Such capabilities include hybrid connectivity to on-premises locations as well as traffic filtering. Incidentally, this need to minimize cost aligns with the Information Security and Risk requirements, which state that all traffic between on premises locations and Azure virtual networks must flow via a single virtual network, which will be hosting components responsible for hybrid connectivity and traffic filtering.
* As per requirements defined by the Tailwind Traders Information Security and Risk  
  teams, all communication between Azure VMs in different tiers that are part of the  
  same application must allow only the ports required to run and maintain the  
  application. However, due to IP address space limitations, it might not be possible to  
  allocate dedicated subnets to each tier. Enterprise IT group needs to identify the  
  optimal way to configure source and destination for traffic filtering that would not  
  require directly referencing IP addresses or IP address ranges.

Tasks

* Design a 3-tier network solution for the BI Application. Your design could include  
  Azure ExpressRoute, VPN Gateways, Application Gateways, Azure Firewall, and  
  Azure Load Balancers. Your networking components should be grouped into virtual networks and network security groups should be considered. Be prepared to explain why you chose each component of the solution.
* Based on your architect solution from the compute case study how would this  
  impact the network design? Would you need any additional networking resources to secure access to the modernized application? Would you no longer need some of the recommended solutions implemented in your original network design?
* Based on your storage (relational) case study how would you update the network  
  design to secure access to the storage account and ensure only select users have  
  access to the storage account?  
  • Based on the modernizing of the SQL backend how do you plan to enable pragmatic access to the data base so that the front end has no hard coded secrets in its code base?