Microsoft

Azure Fundamentals

Networking

Abstract and learning objectives

In this whiteboard design session, you will look at the process of configuring an enterprise-class network within Azure. Your design will include technologies to connect multiple virtual networks, as well as using capabilities such as routing to deploy network virtual appliances such as firewalls to secure your deployment.

At the end of this whiteboard design session, you will be better able to design solutions using Azure Networking features and capabilities.

Step 1: Review the customer case study

Outcome

Analyze your customer needs.

Timeframe

15 minutes

Customer situation

Woodgrove Financial Services

- In business for over 75 years and is a well-known and respected name brand in the financial industry
- Historically risk-averse; helping them survive several financial downturns
- Started in the US, but expanded into Mexico 20 years ago
- Today they have 224 branches in the US and 64 in Mexico

Customer situation (continued)

- Headquartered in Chicago, IL
- US branches in several states over the north central US
- Mexico-based branches are in Mexico City and in the surrounding cities

Customer situation (continued)

- New president brought on to:
  - Modernize the image of the bank
  - Drive efficiencies through use of modern technologies
  - Lower capital costs
  - Refocus Woodgrove on its core business

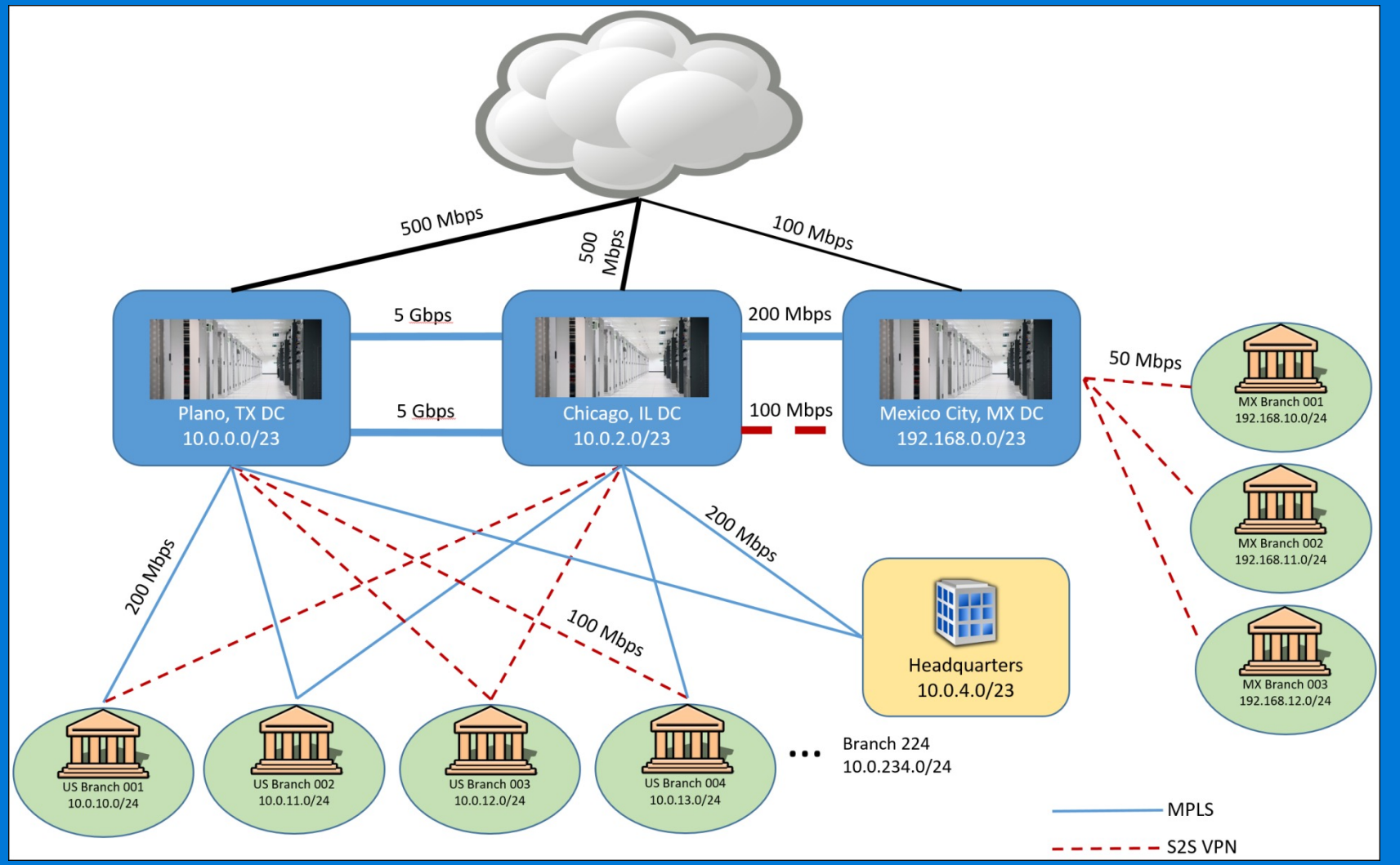
Customer situation (continued)

- Ten years ago went through a major upgrade of their Ethernet core and WAN between two US datacenters:
  - Plano, TX
  - Chicago, IL
- Mexico datacenter located in Mexico City

Customer situation (continued)

- Woodgrove Financial Services want to run a marketing web application on the cloud as a pilot basis.
- To support the strategy of embracing cloud technologies, Network and security team are considering alternatives to redirecting internet traffic via an on-premises security gateway for this deployment. They are looking for a Cloud-native security solution.

Customer situation (continued)



Customer situation (continued)

Business-critical applications

- Core banking application
  - Client-server applications
  - 50 application servers and a SQL Server 2014-based data tier (always-on availability groups and in-memory tables).
- Banking website
  - Enables online banking
  - Running on web farm in the company's perimeter network and securely interacting with the banking application servers.

Customer situation (continued)

Business-critical applications

- HR system
  - Custom-written; capitalizing on several application servers and an Oracle-based data tier.
- Email
  - Exchange Server 2010; capitalizing on DAGs that span their 2 datacenters.

Customer situation (continued)

Additional applications requirements

- A large number of multi-tier custom business apps that, due to their legacy dependencies, will likely be migrated to Azure IaaS.

Customer situation (continued)

Pilot application running on cloud

- A new application running fully on cloud will be used as their new marketing site.
- A cloud-native security solution is required.
- The application must be fully isolated from their business-critical applications.
- The application should use PaaS rather than IaaS.

Customer needs

- Detailed architecture and plan for providing robust, secure connectivity between their datacenters and Azure.
- Azure Virtual Networking architecture and plan for providing an enterprise-class networking scenario, supporting secure data flow between tiers in an n-tier application.

Customer needs (continued)

- End result is a network design that allows applications to run both on-premises and in Azure.
- All the incoming traffic must be inspected in order to ensure protection against SQL injections, cross-site scripting and other web attacks such as http protocol violation.

Customer needs (continued)

- For the new cloud application, related PaaS services need to be deployed in order to run the application.
- Traffic going to the new application will not be redirected to the on-premises corporate network.
- Instead, Woodgrove are looking to deploy a cloud-native security solution for this pilot.
- The web app architecture requires URL-based routing, redirection, and SSL termination.

Customer objections

- Tight regulatory compliance requirements:
  - Security must be a key tenant of all operations including those related to technology.
  - CSO is opposed to using services solely accessible over the public internet (Office 365, CRM, and other Microsoft SaaS are off limits).
  - PaaS services accessible over the internet are also unusable.
  - Relegated Woodgrove to “private” Azure services such as IaaS.

Customer objections (continued)

- Director of Network Operations believes complex "Enterprise-grade" networking scenarios cannot be deployed in hyper-scale public clouds.
- Director of Network Operations requires that engineers have the ability to analyze traffic flows and capture packets when needed.
- Need to provide detailed solution plans, case studies, and customer testimonials to help better understand.

Common scenarios

Azure Infrastructure as a Service (IaaS)

- Virtual machines
- Virtual networks
- VPN gateway
- Virtual appliances
- Hybrid connectivity
- Load balancers
- Storage
- Web Application firewall
- Azure Firewall

Preferred solution

- The solution for Woodgrove involves several technologies, including:
  - ExpressRoute with private and Microsoft peering with route filters, enabling connectivity to VMs and Vnets.
  - Azure Bastion service for secure remote administration with Just-in-time (JIT) virtual machine access for RDP port security.
  - Azure Firewall for protecting connections between on-premises and Azure.
  - Virtual Network Service endpoints to further secure access to PaaS services such as storage and Azure SQL.

Preferred solution (continued)

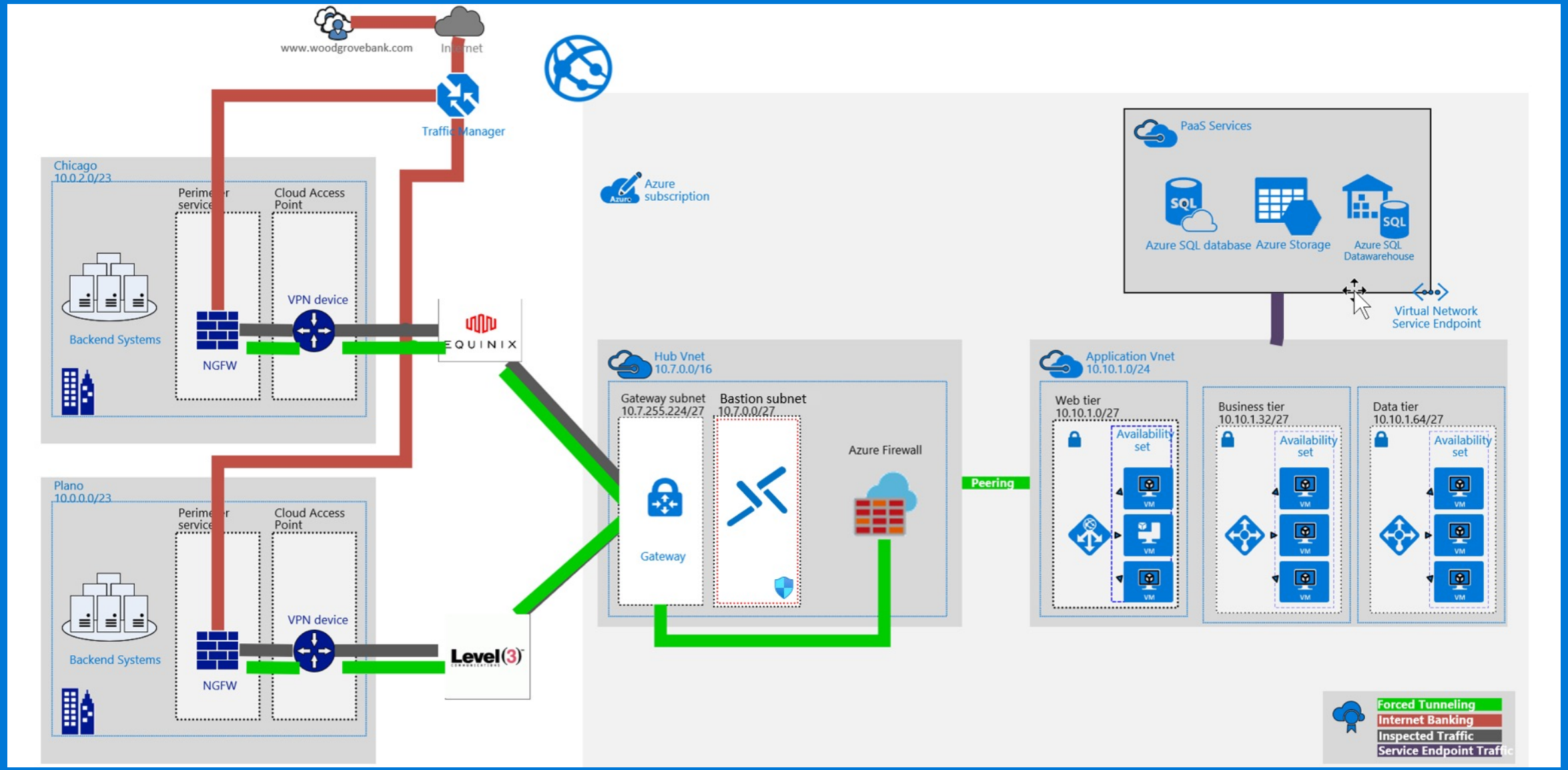
An enterprise-class configuration within an Azure Virtual Network to support a 3-tier application. Components of this solution include:

- Multiple Virtual Networks configured in a hub-spoke topology.
- Multiple subnets for the hub and spoke
  - Hub – Gateway, Perimeter, Bastion
  - Spoke – Web tier, Business tier, Data tier
- Azure Firewall configured with rules that define allowed and denied network traffic between on-premises and Azure workloads

Preferred solution (continued)

- Five Route Tables associated with their corresponding subnets, each with specific user-defined routes configured.
- Five network security groups associated with their respective subnets, each with specific allow/deny rules configured.
- Application Security Groups (three per each multi-tier legacy business app) to secure traffic within the same subnet, along with the corresponding Network Security Groups.
- One Azure web application firewall that will protect and inspect incoming traffic.

Preferred solution (continued)

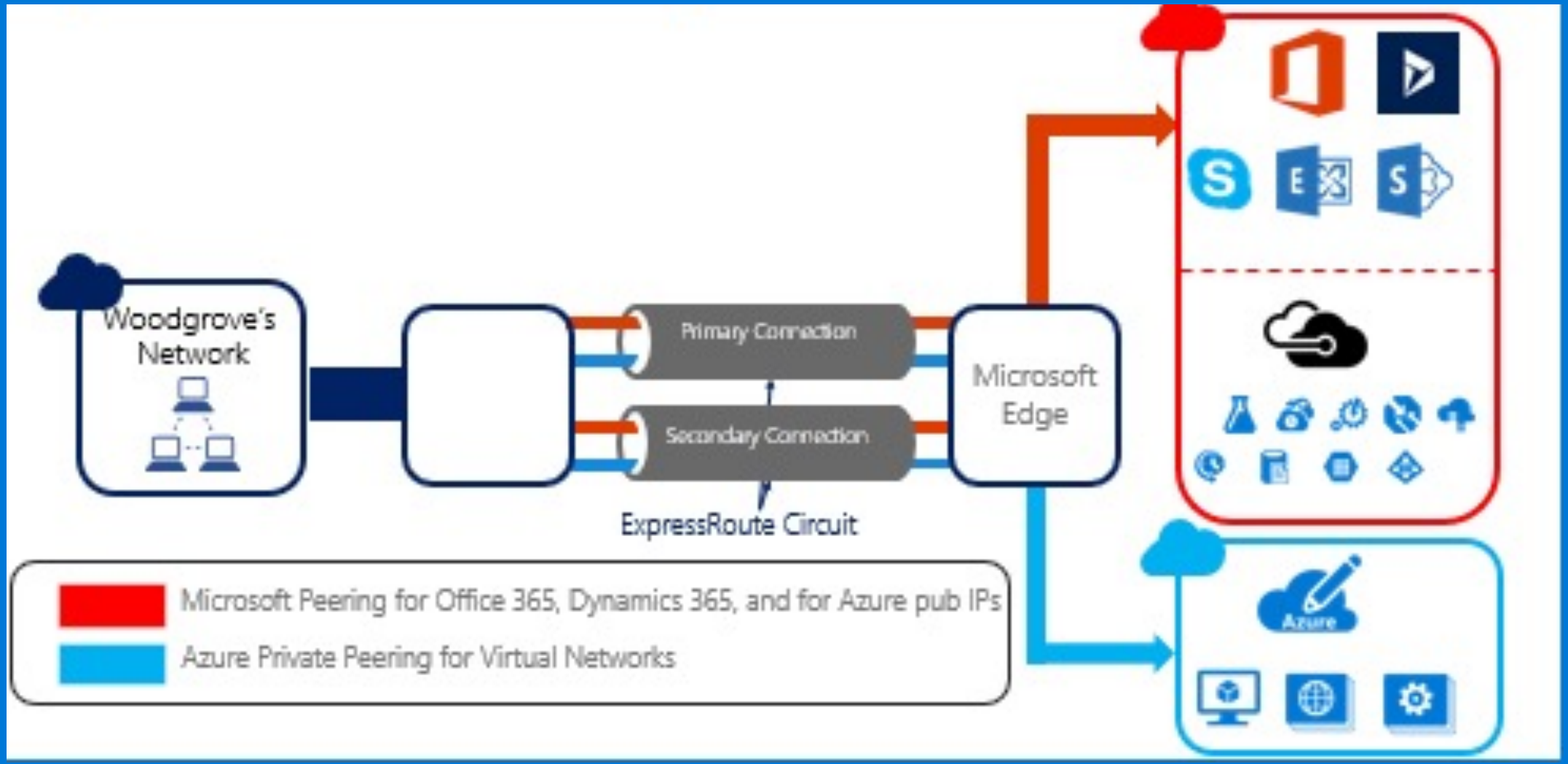


Preferred solution (continued)

ExpressRoute configuration details:

- Two ExpressRoute circuits will be provisioned:
  - First in Dallas, TX (corresponding to the Plano, TX datacenter)
    - Level 3 is the communications provider
  - Second in Chicago, IL (corresponding to Chicago, IL datacenter)
    - Equinix is the connectivity provider
- Capitalizing on different providers will enable Woodgrove to maintain connectivity to Azure even in the case of a catastrophic provider issue.
- After study, the unlimited licensing option with 1 Gbps was chosen for both ExpressRoute circuits. The use of a Microsoft peering path necessitates an ExpressRoute standard SKU at minimum.

Preferred solution (continued)



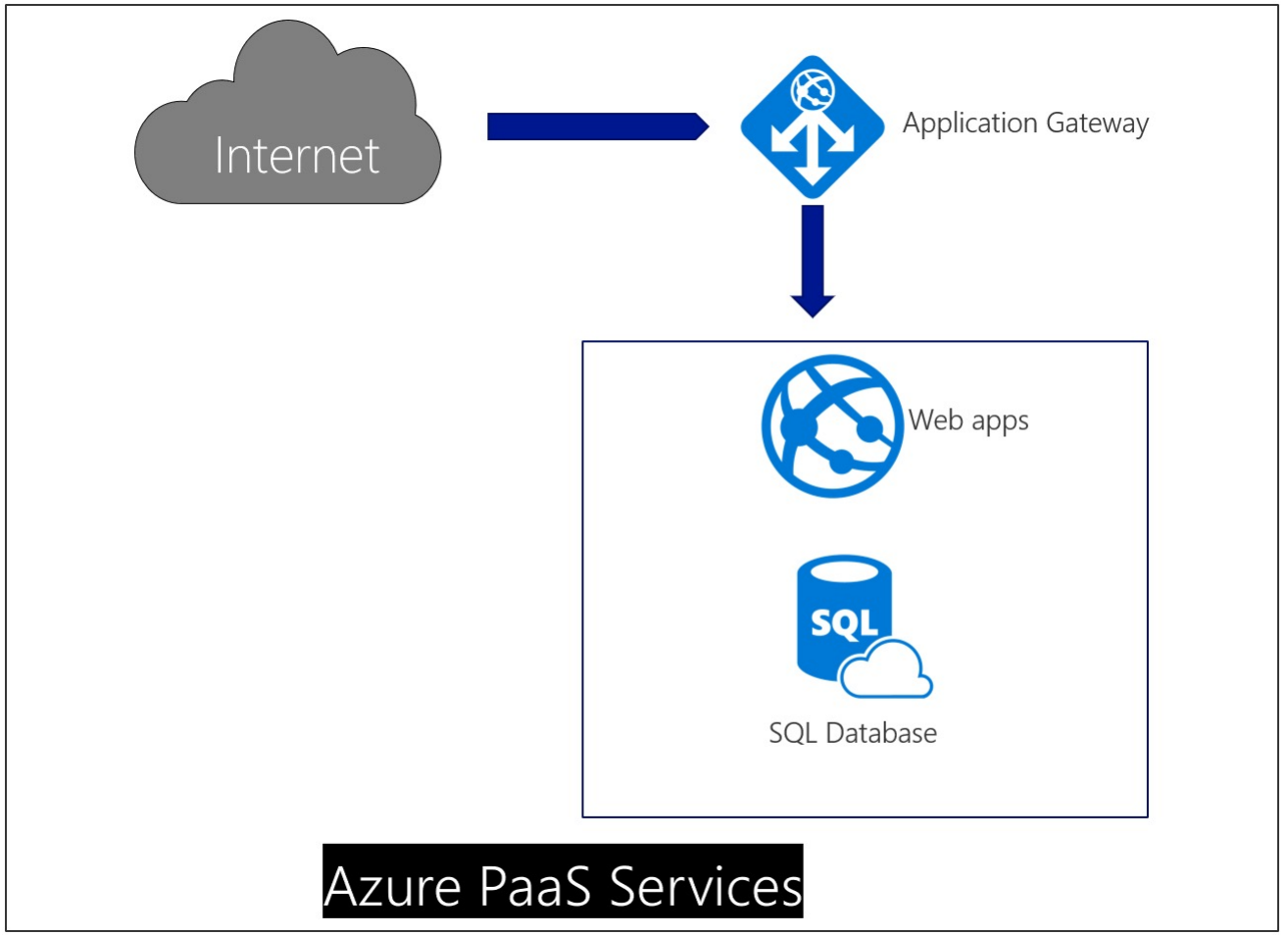
Preferred solution (continued)
Azure Firewall

- Built-in high availability (no load balancers required)
- Deployed into a hub virtual network perimeter subnet.
- Filter traffic coming in from the internet and from the on-premises environment.
- User-defined routes are leveraged to forward traffic through the firewall for inspection.

Preferred solution for cloud-based application

- Azure web apps will be configured and used, to run the marketing application pilot.
- Application GW running as a WAF will be used as the security solution. It will also provide URL-based routing, redirection, and SSL termination .
- The Azure Web App will be configured as backend back-end pool member of Application Gateway.
- To ensure end users will hit the gateway, a CNAME record can be used to point to the public endpoint of the application gateway.
- To create the alias, it needs Public IP address and DNS name attached to the App Gateway.

Cloud Web App Deployment



Preferred objections handling

Objection

As a financial institution, Woodgrove is under tight regulatory compliance requirements. Security is a key aspect of compliance and as such, it must be a key tenant of all operations including those related to technology. The corporate security officer is generally opposed to using services solely accessible over the public internet. Services like Office 365, CRM, and other Microsoft SaaS offerings are off limits. Additionally, PaaS services accessed over the internet are also unusable. It has relegated Woodgrove to private Azure services such as IaaS.

Potential answer

Using ExpressRoute, Woodgrove can access and use Azure private and public services without traversing the internet. This secure connectivity, in addition to the business-class SLAs and greater bandwidth, make ExpressRoute a compelling offering that addresses this objection.

This can be further refined with the use of Virtual Network Service endpoints with offerings such as Azure SQL

Preferred objections handling

Objection

The director of Network Operations is under the impression that complex enterprise-grade networking scenarios, such as those that support n-tier applications, cannot be configured in hyper-scale public clouds. Trust comes slowly with this director. She will most likely need detailed solution plans, case studies, and even customer testimonials to help convince her of the viability of anything other than simple networking scenarios in Azure.

Potential answer

Azure supports many critical enterprise-grade scenarios, including scenarios that require hybrid connectivity and high availability such as Woodgrove. Many of these scenarios are documented in the Azure Architecture Center with reference architectures that cover best practices.

Preferred objections handling

Objection

The director of Network Operations also does not trust cloud security. She will need a strategy in place which allows Network Engineers the ability to analyze traffic flows and capture packets when needed for cloud-hosted resources.

Potential answer

Azure fully supports forced tunneling ensuring that all internet traffic is directed to the desired site, be that in an Azure Virtual Network or on-premises.

All internet traffic can easily be routed from Azure to an on-premises appliance for intrusion detection/prevention and logging.

Preferred objections handling

Objection

The corporate compliance officer of Woodgrove must ensure compliance with many requirements to ensure his organization passes audits from both internal and external entities. One requirement is all outbound internet requests must pass through an on-premises system that inspects and logs this traffic. The CCO is skeptical of IaaS solutions in Azure since "those VMs in the cloud can access the internet directly."

Potential answer

Azure fully supports forced tunneling ensuring that all internet traffic is directed to the desired site, be that in an Azure Virtual Network or on-premises. For example, all internet traffic can easily be routed from Azure to an on-premises appliance for intrusion detection/prevention and logging.

Customer quote

Quote from the Network Director:

"Azure's advanced networking capabilities and support for partner solutions are a welcome surprise. Your proof of concept has clearly demonstrated the platform's ability to more than satisfy our complex requirements."