Microsoft Cloud Workshop

Enterprise-class networking in Azure
Whiteboard design session student guide
June 2020

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

Contents

Enterprise-class networking in Azure whiteboard design session student guide

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's needs.

Timeframe: 15 minutes

Directions: With all participants in the session, the facilitator/SME presents an overview of the customer case study along with technical tips.

1. Meet your table participants and trainer.

2. Read all of the directions for steps 1-3 in the student guide.

3. As a table team, review the following customer case study.

Customer background

Woodgrove Financial Services has been in business for over 75 years and is a well-known and respected name brand in the financial industry. They are historically risk-averse, and it has served them well, enabling them to weather several financial storms that closed the doors on similarly sized institutions. While Woodgrove started in the United States, around 20 years ago, they branched out into the international arena by acquiring a bank headquartered in Mexico City. Today, they have 224 branches in the United States and 64 in Mexico.

Five years ago, a new president of Woodgrove Financial Services was brought onboard to help modernize the image of the bank and to drive efficiencies through use of modern technologies. The new president is under stiff pressure from the board to lower capital costs and help Woodgrove refocus on its core business. Woodgrove's mission is to promote its customer's well-being and secure their future through a broad range of financial services.

Woodgrove Financial Services headquarters is in Chicago, IL, and their United States branches exist in several states extending over the North Central United States. Their Mexico-based branches are in Mexico City and in the surrounding cities.

Customer situation

Ten years ago, Woodgrove went through a major upgrade of their Ethernet core and WAN connectivity between their two United States datacenters (located in Plano, TX and Chicago, IL). Today, the United States datacenters have redundant 5 Gbps connections between them. At the same time, they increased the bandwidth from their United States branch locations to no less than 100 Mbps with each branch having connectivity to both datacenters. Most United States branches have an MPLS-based connection to both datacenters but about forty percent have 1 MPLS connection to a datacenter and one Site-to-Site VPN connection to the other datacenter. About five percent of the United States branches have only Site-to-Site connections to both datacenters.

There is also a datacenter in Mexico, located in Mexico City. The Mexico datacenter has an MPLS connection to the Chicago datacenter with 200 Mbps bandwidth and a Site-to-Site VPN connection for redundancy that is 100 Mbps. All 64 of the Mexico-based branches have Site-to-Site VPN connections to this datacenter and the internet bandwidth for all branches was standardized recently at 50 Mbps up/down.

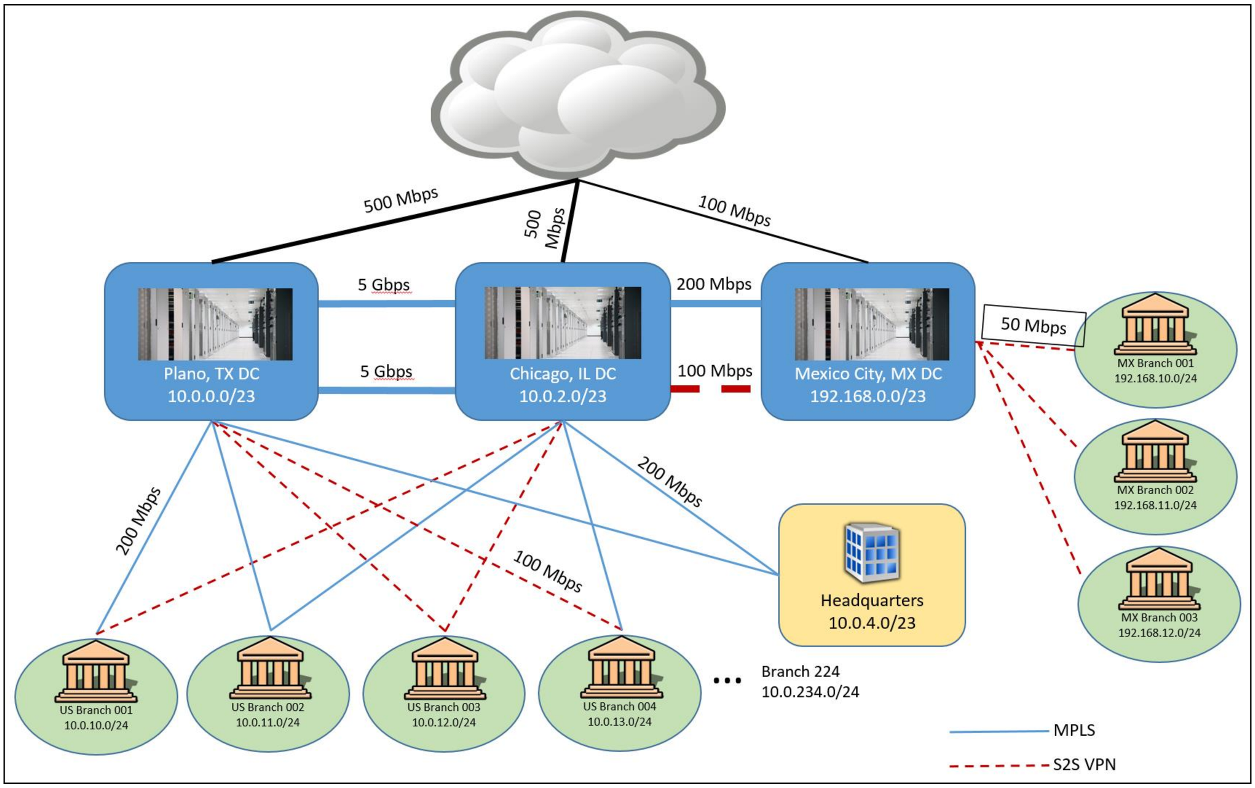


Figure 1 - Woodgrove current network configuration

Woodgrove leadership has been watching the emergence of hyper-scale public cloud offerings, and over the last several years, they have been discussing the adoption of public cloud. Through strong executive-level relationships with Microsoft, the organization has been predominantly a Microsoft shop for at least the last 15 years. Due in large part to this relationship, Woodgrove executives envision that over a five-year period they will transition 80-90% of their IT infrastructure to Microsoft Azure and will eventually decommission their Chicago datacenter altogether.

Woodgrove's business critical applications include:

- Their core banking application (a client-server application taking advantage of approximately 50 application servers and a SQL Server 2014-based data tier using Always on Availability Groups and In-Memory tables).

- Their website that enables online banking features (running on several web farms in the company's perimeter network and securely interacting with the banking application servers).

- Their HR system (a custom-written system taking advantage of several application servers and an Oracle-based data tier).

- Email (Exchange Server 2010 taking advantage of Database Availability Groups that span their two datacenters).

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

Woodgrove's pilot deployment of cloud-native applications will include:

- Implementing a simple marketing web application in Azure. The application should use PaaS rather than IaaS.

- Identifying an alternative to forced tunneling. To support the strategy of embracing cloud technologies, Network and security teams 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.

- Evaluating options for securing multi-tier business apps. Woodgrove IT is considering leveraging Azure Network Security Groups in combination with Application Security Groups.

- Securing connectivity to Azure PaaS. To minimize exposure of Azure PaaS services via public endpoints, Woodgrove's Information Security requested that communication between Azure IaaS and Azure PaaS services do not rely on public endpoints, whenever possible.

Customer needs

1. A detailed architecture and plan for providing robust, secure connectivity between their datacenters and Azure. The plan must support migration efforts and connectivity from the branch offices to Azure to allow connectivity to migrated applications. The solution should be able to continue to provide connectivity in the case of a severe connectivity partner outage.

2. A detailed architecture and plan for providing an enterprise-class networking scenario supporting secure data flow between tiers in the core banking application. All components of the design must be highly available.

3. The result of needs one and two should be a network design that allows applications to run both on-premises and in Azure.

4. For the time being, all internet traffic must be passed through an on-premises intrusion detection or prevention system to comply with company policy.

5. 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 etc.

6. All traffic targeting the cloud-based marketing web app will not be passed through on premises network. An alternative cloud-native security solution is required.

7. URL based routing, redirection, SSL termination will need to be implemented on the FW/LB level for the new cloud web apps.

8. DDoS protection plan must be configured for the Virtual Network which will host the Data and Web tiers of the core banking application.

9. All traffic that goes in and out of Azure virtual networks must be filtered and passed through a firewall appliance.

10. All traffic that goes through ExpressRoute circuit needs to be distributed based on business units and will have granular control of circuit distributions.

11. ExpressRoute circuits need to be link together to make a private network so that data can directly exchange between offices.

Customer objections

1. 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 tenet 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.

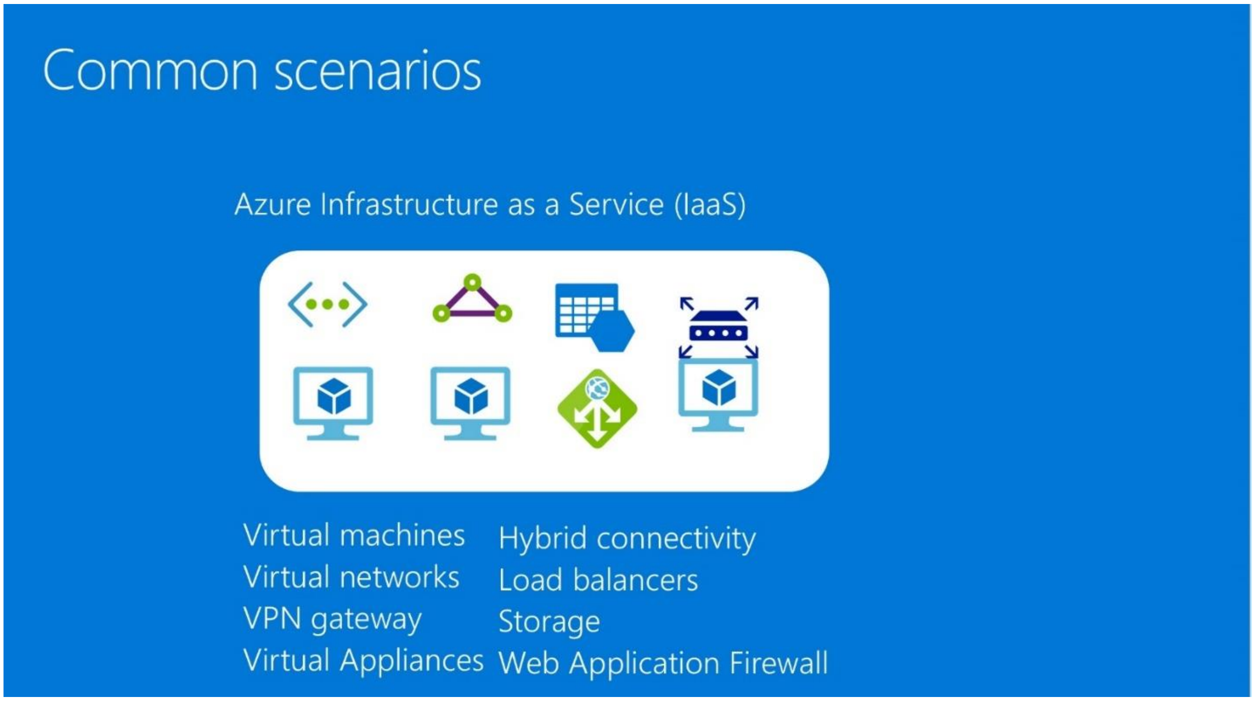
2. The director of Network Operations is under the impression that complex enterprise-grade networking scenarios, such as those that support n-tier applications, cannot be configured in

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.

3. 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.

4. 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."

Infographic for common scenarios



Common scenarios

Azure Infrastructure as a Service (IaaS)

Virtual machines
Virtual networks
VPN gateway
Virtual Appliances

Hybrid connectivity
Load balancers
Storage
Web Application Firewall

Step 2: Design a proof of concept solution

Outcome

Design a solution and prepare to present the solution to the target customer audience in a 15-minute chalk-talk format.

Timeframe: 60 minutes

Business needs

Directions: With all participants at your table, answer the following questions and list the answers on a flip chart:

1. Who should you present this solution to? Who is your target customer audience? Who are the decision makers?

2. What customer business needs do you need to address with your solution?

Design

Directions: With all participants at your table, respond to the following questions on a flip chart.

The desired outcome is a network architecture that meets the needs of a modern financial services organization. This design will not have single points of failure and will include concepts such as a perimeter network with redundant firewalls protecting the internal subnets containing the application tiers. A simple network design will most likely confirm the director of Network Operation's beliefs that Azure cannot support real-world, enterprise-class networking (see customer objections)---*prove her wrong!*

High-Level architecture

1. Create a high-level architecture diagram and explanation of the components of your solution.

Address the following customer requirements

1. Explain the approach you would take to deploying ExpressRoute Circuits including location and circuit size.

2. What ExpressRoute peering options you would enable and what workloads would use them? Diagram your peering configuration including subnet, IP and autonomous system number configuration needed.

3. What are the NAT requirements for ExpressRoute integration?

4. How does your design address availability at the network layer?

5. How is routing configured in your overall design?

6. Identify where Network Security Groups are used in your design.

Prepare

Directions: With all participants at your table:

1. Identify any customer needs that are not addressed with the proposed solution.

2. Identify the benefits of your solution.

3. Determine how you will respond to the customer's objections.

Prepare a 15-minute chalk-talk style presentation to the customer.

Step 3: Present the solution

Outcome

Present a solution to the target customer audience in a 15-minute chalk-talk format.

Timeframe: 30 minutes

Presentation

Directions:

1. Pair with another table.
2. One table is the Microsoft team and the other table is the customer.
3. The Microsoft team presents their proposed solution to the customer.
4. The customer makes one of the objections from the list of objections.
5. The Microsoft team responds to the objection.
6. The customer team gives feedback to the Microsoft team.
7. Tables switch roles and repeat Steps 2-6.

Wrap-up

Timeframe: 15 minutes

Directions: Tables reconvene with the larger group to hear the facilitator/SME share the preferred solution for the case study.

Additional references

Description	Links
IP Addressing and Subnetting for New Users	http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

CIDR / VLSM Supernet Calculator	http://www.subnet-calculator.com/cidr.php
ExpressRoute documentation	https://azure.microsoft.com/en-us/documentation/services/expressroute/
ExpressRoute Routing requirements	https://azure.microsoft.com/en-us/documentation/articles/expressroute-routing/
ExpressRoute NAT requirements	https://azure.microsoft.com/en-us/documentation/articles/expressroute-nat/
ExpressRoute workflows	https://azure.microsoft.com/en-us/documentation/articles/expressroute-workflows/
ExpressRoute Global Reach	https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach
Site-to-Site VPN documentation	https://azure.microsoft.com/en-us/documentation/services/vpn-gateway/
Virtual Network documentation	https://azure.microsoft.com/en-us/documentation/services/virtual-network/
Network Security Group documentation	https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/
User-Defined Routing and IP Forwarding	https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-udr-overview/
Load Balancer	https://azure.microsoft.com/en-us/documentation/articles/load-balancer-overview/
Microsoft Azure Virtual Datacenter: A Network Perspective	https://docs.microsoft.com/en-us/azure/networking/networking-virtual-datacenter
Deploy highly available network virtual appliances	https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/nva-ha
Azure Firewall Documentation	https://docs.microsoft.com/en-us/azure/firewall/
Virtual Network Service Endpoints	https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview
Azure Bastion	https://docs.microsoft.com/en-us/azure/bastion/bastion-overview