Overview

Contoso are a manufacturer of car components with a headquarters in London and satellite offices in Amsterdam and Munich. Contoso are going through a large digital transformation program at the moment where they are rationalising their data centre estate and moving much of their enterprise infrastructure to Azure.

The London office has 2,000 users. The Amsterdam office has 500 users. The Munich office has 500 users. All existing resources within Contoso's enterprise estate are hosted in data centre facilities in either London or Amsterdam.

Contoso are already using Microsoft 365 for modern workplace services therefore already have an existing Azure AD tenant. They have no active Azure subscriptions.

Existing Environment

The existing network contains an Active Directory with the primary domain name of contoso.com. All Domain Controllers have integrated DNS and host the contoso.com DNS zone. Domain Controllers are deployed in pairs in both the London and Amsterdam data centres.

Contoso's business is dividend into departments which are:

- Finance
- Human Resources
- Supply Chain
- Sales

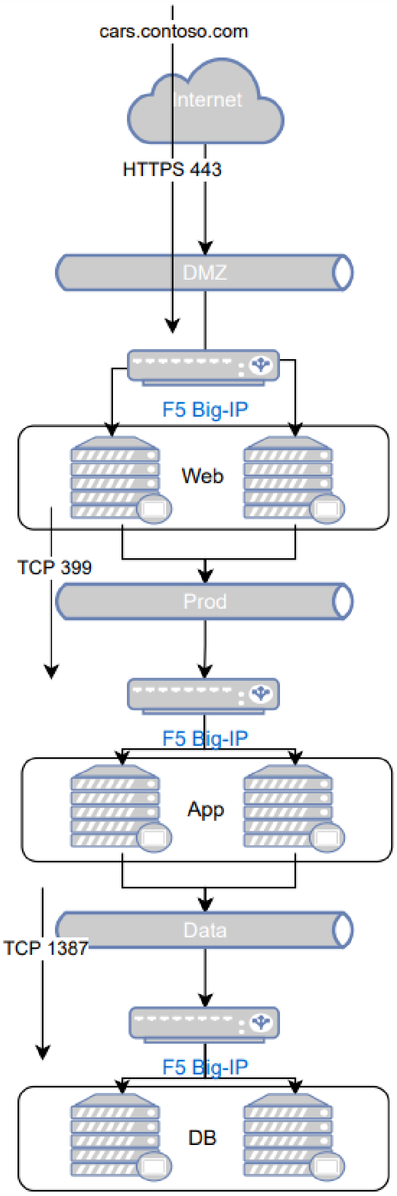
Each department has its own organisational unit within the existing Active Directory. Each user account within the Active Directory has the department attribute set to match the users main working area within the business.

The existing data centre facilities are managed by different service providers. They facilities at London and Amsterdam are connected via an MPLS circuit provided by British Telecom. In addition to this MPLS circuit, there is also S2S VPNs between London and Amsterdam provisioned as a backup route to the MPLS circuit. These VPNs are terminated into Cisco ASA firewalls which sit within the management boundary of Contoso in each of the data centres.

A production application known as CarPartsSystem has been selected as the first application to be migrated to Azure as part of the initial POC. This application is currently running on a Hyper-V Cluster which sits within London. Hyper-V Replica is configured to replicate the application servers to Amsterdam for a warm failover capability. Contoso has F5 Big-IP Load Balancers to load balance and ensure high availability of the multiple tiers within the application. The application is built on Windows Server and SQL. It is a traditional 3-tier application architecture.

- Web tier – this is Windows Server 2016 with IIS installed and ASP.net webforms
    - The web tier is presented over port 443 (HTTPS).
- Application tier – this is Windows Server 2016 with C# class libraires and middleware
    - The web and application tier communicate over port TCP 399
    - The application tier and database tier communicate over port TCP 1387
- Database tier – this is Windows Server 2019 with SQL 2018 and a large scale 1TB database
    - No communication is currently open between the web and database tier Web

The following diagram outlines the high-level architecture of the application.



You have successfully won a consulting project with Contoso and their internal IT Manager has been reading up on Azure. During a discovery workshop with the IT Manager a number of functional and non-functional requirements have been gathered.

Requirements

	Problem Statement	Solution
1	The customer requires that all on prem Active Directory users are available in AAD.	
2	The custom requires that all user logins to AAD are met with a second authentication challenge.	

3	The customer requires the ability to give each business unit its own Azure subscription to help manage costs.	
4	The customers central IT department must be able to enforce central governance and control across the entire tenant.	
5	The customer requires a central hub and spoke architecture managed by IT.	
6	The customer requires dedicated and SLA backed connectivity from the London HQ.	
7	The customer requires private and encrypted connectivity from Amsterdam and Munich into Azure.	
8	The custom requires that all data stored within Azure must be hosted physically in either the UK or Europe.	
9	The customer requires the ability to create new Virtual Machines in Azure.	
10	The customer requires the ability to set metadata against each Azure resource to ensure cross charging to business units is possible.	
11	The customer requires the ability to allow employees access to their own email accounts whilst maintaining a company security posture on their BYOD devices.	
12	The customer must be able to control rights and access levels inside AAD which might not fit the default role offerings.	
13	The customer requires users to have the ability to reset their own on prem AAD passwords directly from the cloud to cut ops tickets.	
14	The customer requires the ability to collaborate with users who are	

	members of another AAD tenant on a cross purposes project.	
15	The customer wants to be able to automate and streamline the process of creating new Windows VMs in Azure.	
16	The customer must be able to control all inbound and outbound network access centrally from Azure.	
17	The customer must be able to ingest a huge amount of encrypted data offline via a hard disk.	
18	The customer requires that all VMs which run on Azure are encrypted at the operating system level.	
19	The customer has an application which requires high IOPS, high throughput data disks for a SQL application.	
20	The customer requires the ability to dynamically scale a collection of application VMs based on incoming demand.	
21	The customer must be able to define a set of ideal configurations which must be applied against VMs in Azure.	
22	The customer wants to host their public DNS domains in Azure.	
23	The customer must have a blob storage area inside Azure which is accessible only over a private connection.	
24	The customer wants to remotely manage their Azure VMs using the most secure method possible without establishing cross site connectivity.	
25	The customer must be able to replace their F5 Big-IP load balancers with a suitable L4 solution.	

26	The customer requires the ability to apply WAF rules against an internet facing application.	
27	The customer requires the ability to configure SSL offloading for a public facing internet application.	
28	The customer must be able to control network flow within Azure to increase the security of the CarSystem application.	
29	The customer must be able to backup files and folders from on premise servers to Azure.	
30	The customer must be able to backup Azure VMs and retain a month end backup for the period of 12 months.	
31	The customer requires the ability to run a simple containerised web application with a low management foot print.	
32	The customer must be able to do self-diagnosis and troubleshooting of Azure VMs to understand networking faults.	
33	The customer requires the ability to connect two Azure Virtual Networks together without the presence of a VPN.	
34	The customer must be able to run a containerised application at scale on Azure.	
35	The customer must be able to replicate production systems from on region of Azure to another for BCDR.	
36	The customer must be able to configure Azure VM high availability to survive a single rack outage.	
37	The customer must be able to configure Azure VM high availability to survive a DC within a region outage.	

38	The customer must be able to storage a large quantity of unstructured and unrelated data on Azure.	
39	The customer must be able to replace existing SMB file shares with an Azure native solution.	
40	The customer requires the ability to interact with Azure storage using a time-based authentication key for vendor access.	