Opis sytuacji:

Cześć Drogi Architekcie!

Sieć to jeden z podstawowych aspektów pracy w chmurze, nawet jeśli jesteś developerem i uważasz, że to przecież nie Twoje zabawki. Nawet jeśli faktycznie nie Twoje, dobrze wiedzieć, czym dysponujesz a czym nie. Warto też wiedzieć, co powiesz swoim kolegom z działu bezpieczeństwa.

Ale po kolei…

Pamiętasz kiedy planowałeś swoją migrację do Chmury?

Kiedy miałeś napisać plan migracji i zdecydować jak podejść do takiego wyzwania w dużej firmie o ogromnej skali przetwarzania?

Nadal pracujesz dla tej firmy i teraz poproszono Cię byś zbudował architekturę sieci dla rozwiązania po migracji. Nie martw się, jako architekt nie musisz znać szczegółów, ważne byś umiał zaplanować koncepcję, dobrać usługi i pokazać najlepsze praktyki, szczegółami zajmie się Twój zespół sieciowy oraz zespół od bezpieczeństwa.

Na razie przyjmij, że o sieci w chmurze to właśnie Ty wiesz najwięcej! I tak pewnie jeszcze chwilę pozostanie!

Zadanie:

#9.1 Dlatego teraz przed Tobą nie lada wyzwanie:

1. Przeczytaj poniższe dokumenty. Jeśli miałeś szansę je poznać czytając linki pod pracami domowymi to masz już ten etap z głowy. Materiał pomoże Ci w planowaniu migracji.

* <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/secure-vnet-dmz>
* <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke>
* <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/shared-services>

1. Przypomnij sobie wiedzę o usługach, które omówiliśmy. Szczególnie te podstawowe elementy oraz architektury sieci będą dla Ciebie ważne.
2. Wypisz od 5 do 10 rekomendacji dla osób od sieci jak powinna być zaprojektowana sieć w Azure.

Zwróć uwagę na takie elementy jak:

* Adresacja – jakie zakresy sieci wybrać i do czego
* Podział na Vnet’y i Subnet’y – pomyśl o segmentacji pod względem typów środowisk, ich wielkości i przeznaczeniu
* Zaplanuj wykorzystanie NSG oraz ASG lub też rozwiązań dedykowanych. Korzystaj śmiało z Service Tags i Service Endpoints ale ostrożnie ☺
* Pomyśl o usługach takich jak Azure Firewall czy DDoS

1. Na końcu powiedz, jakie limity usług zweryfikowałeś by zbudować taką architekturę. To ważne, chmura też ma swoje ograniczenia.

#9.2 A jeśli planowanie to nie twój żywioł to zrób proszę prostą architekturę i uruchom ją w Azure (jak masz zapał, to wykorzystaj do tego skrypty ARM).

Co ma powstać:

1. Sieć z podziałem na 3 subnety
2. W subnecie pierwszym niech stanie Application Gateway, w drugim dwa serwery z dowolnym serwerem aplikacyjnym w Availability Set, w 3 dowolna baza danych
3. Zrób odpowiednią segmentacje ruchu pomiędzy sieciami za pomocą NSG oraz ASG, tak by tylko ruch, który powinien wchodził i wychodził z danych segmenetów sieci
4. Przed całym rozwiązaniem postaw Azure Traffic Managera i skonfiguruj go w dowolnej opcji i sprawdź jak działa
5. Na koniec, ustaw logowanie wszystkich NSG do Azure Traffic Analytics i zobacz po 24h jaki ruch tam został zarejestrowany
6. Na koniec, sprawdź czy Twoje NSG i ASG poprawnie działają za pomocą narzędzie Network Watcher i dostępnych tam opcji.

Liczę na dobre zrzuty ekranu i opis rozwiązania.