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.

#TYDZIEN9.1

- Dobierz adresację prywatną w taki sposób, aby nie nachodziła na tą którą masz w on-premowym DC, tylko w ten sposób będziesz w stanie stworzyć środowisko hybrydowe i włączać nowe komponenty do twojej domeny

- Zestaw połączenie (VPN Gateway lub Express Route) pomiędzy chmurowym i on-premisowym DC. Przy planowaniu migracji decydowaliśmy się na przenoszenie do chmury systemu po systemie, więc na pewno nie uda się tego zrobić za jednym razem i funkcjonowanie hybrydowego środowiska przez jakiś czas jest konieczne. Zadbaj o to aby twoja on-premisowa usługa katalogowa była zsynchronizowana z AAD (np. AD z AAD za pomocą Active Directory Sync), aby Twoi użytkownicy mogli uwierzytelniać się z usługami świadczonymi przez chmurę

- Zastanów się w jaki sposób będziesz organizował swoje projekty i środowiska, rekomendowane podejście to architektura sieciowa Hub-Spoke, gdzie w Hubie (vnet) znajdą się subnety dla: gatewaya, DMZ, managementu (monitoring, audyt etc.) oraz bramka która pozwoli na połączenie z peered vnets. W Spokeach (vnety) znajdują się osobne środowiska i projekty.

- Zdefiniuj NSG w zależności od ruchu wchodzącego / wychodzącego na jaki chcesz pozwalać w ramach swojej sieci w chmurze. Dodatkowo jeżeli Twoja aplikacja jest hostowana przez VM-ki możesz użyć ASG, aby zdefiniować pomiędzy którymi tierami aplikacji (i w którą stronę) pozwalasz na ruch.

- VM które realizują funkcjonalności NVA zapnij w Scale Set i postaw przed nim Load Balancer, co pozwoli na monitorowanie ruchu z twojego on-premowego DC i dostosowywanie ilości VM w miarę obciążenia (tym samym trwały monitoring i niskie latency dla aplikacji)

Limity/usługi:

- jaki throughput ma VPN GW, który tier wybrać, czy może konieczny będzie ER

- jaka zakres adresów jest wymagany dla subnetów w których będą usługi potrzebne do połączenia DC, czy wymagają osobnych subnetów

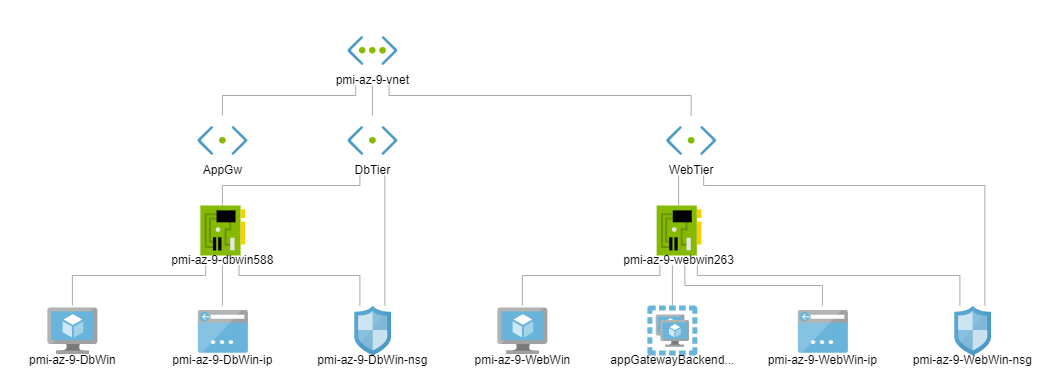
- ile sieci wirtualnych mogę stworzyć, subnetów, czy są ograniczenia dot. peeringu i jak organizowany jest ruch w przypadku peeringu

- generalnie skupiam się na dostępnej ilości, możliwości połączeń pomiędzy wszystkim co powyższe może się rozwijać w ramach migracji systemów do chmury

#TYDZIEN9.2

Bez ARM, nie ma faktycznie działającej apki ale wszystkie połączenia potestowane 😊

Topologia (1,2):



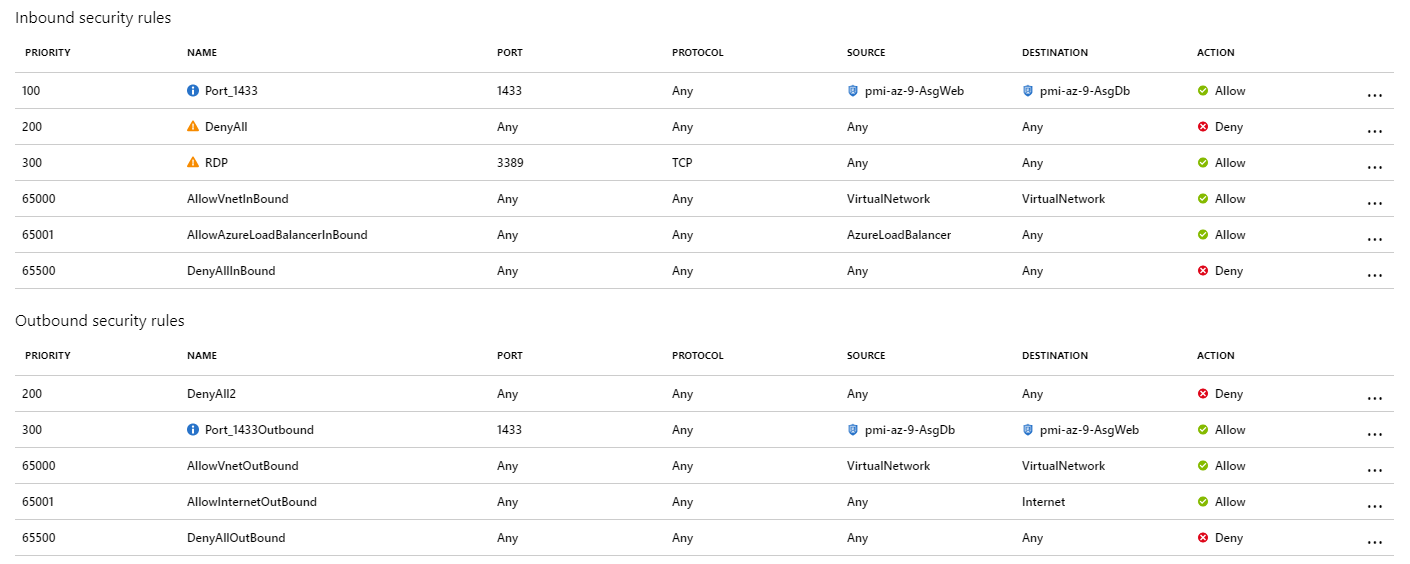
DbWin – maszynka windowsa z SQL Serverem

WebWin - maszynka z IIS. Nie robiłem w końcu VMSS ze względu na to, że nie dało się przypisać ASG na VMSS.

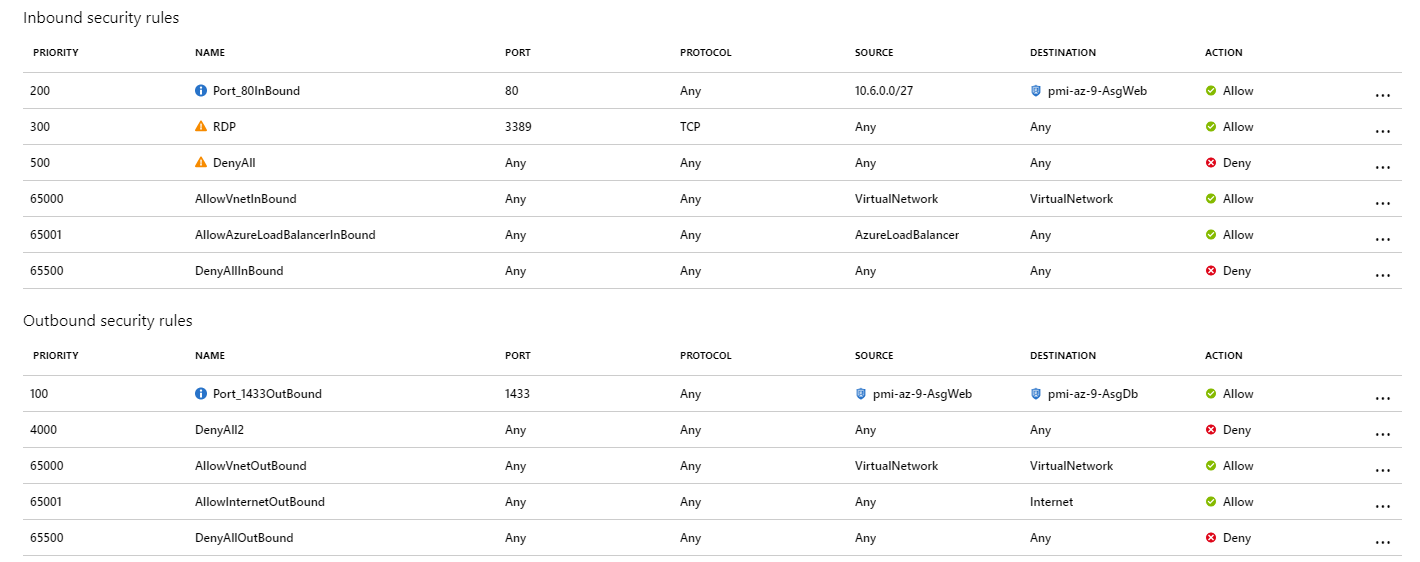
Subnety chyba jasne, w AppGw mam Application Gateway.

Segmentacja ruchu (3):

* pmi-az-9-DbWin-nsg – wpuszcza tylko ruch po 1433 (SQL Server) z ASG pmi-az-9-AsgWeb (ASG przypisane do VM z IIS)



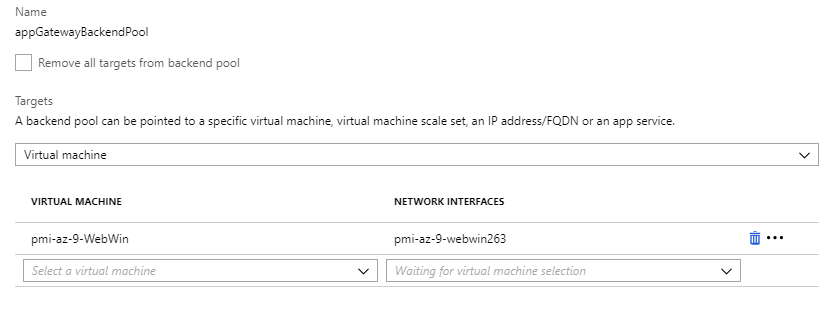
* pmi-az-9-WebWin-nsg – wpuszcza tylko ruch po 80 z subnetu Application Gateway



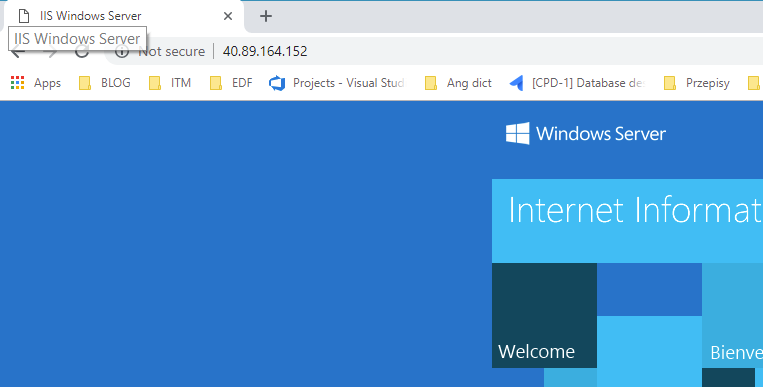
Zrzut z logów IIS, 10.6.0.4/27 to przestrzeń adresowa subnetu AppGw:

2018-11-29 14:18:02 10.6.0.39 GET / - 80 - **10.6.0.4** Azure+Traffic+Manager+Endpoint+Monitor - 200 0 0 17

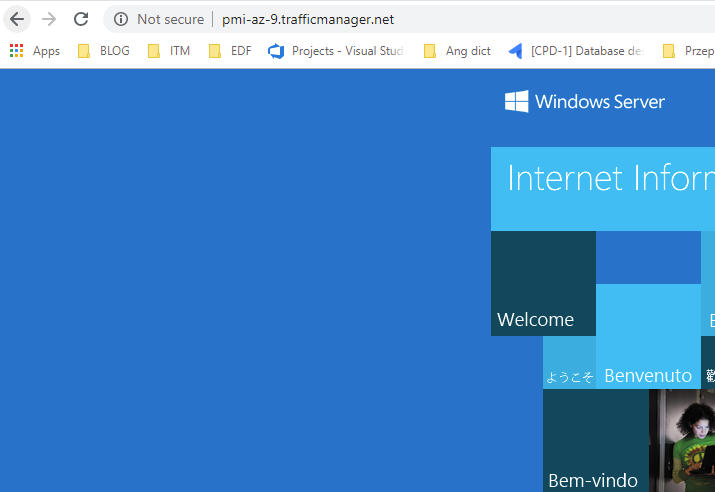
Application Gateway:



Website z IIS dostępny po publicznym IP



Traffic Manager:



Logi z Traffic Analytics:

**Nie mam bo wszystko robiłem na France Central, a Traffica Analytics nie jest wspierany w tym regionie :<**