WSTĘP DO AZURE NETWORK MANAGERA

Poznań 15.11.2022

Agenda

- Intro
- Obecne zmagania z sieciami
- Case Study
- Idea Azure Network Manager
- Demo
- Podziękowania

O mnie

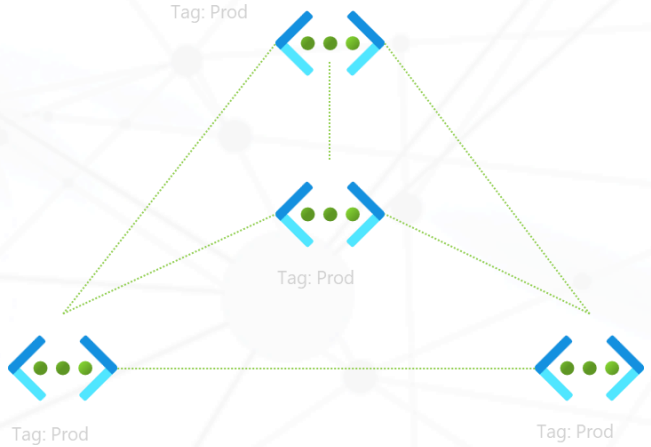
- Marek Serba
- Pracuje w IT od przeszło 14 lat
- Konsultant Azure w firmie Microsoft
- Links:
  - linkedin.com/in/techfellow
  - github.com/technicalflow
  - twitter.com/technicalflow
  - mysmall.cloud

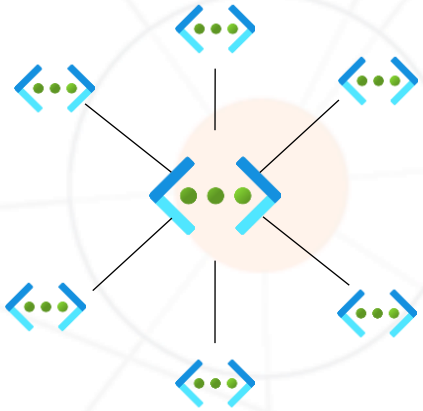
Azure Network Manager (Configuration)

*Preview

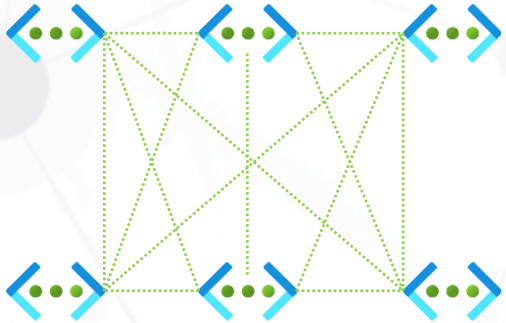
Problem z rozwiązaniami sieciowymi

- Budowa sieci w dużej skali
- Provisioning połączeń sieciowych
- Zarządzanie NSG staje się trudniejsze
- Praca operacyjna nad utrzymaniem sieci
- Komplikacja rozwiązań sieciowych

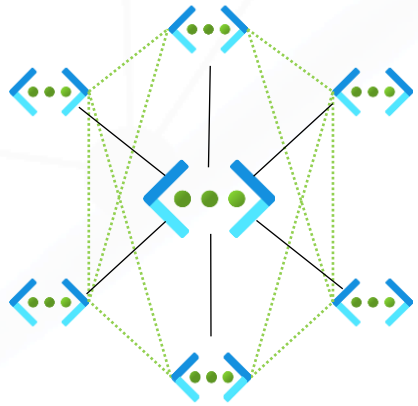




Hub and Spoke



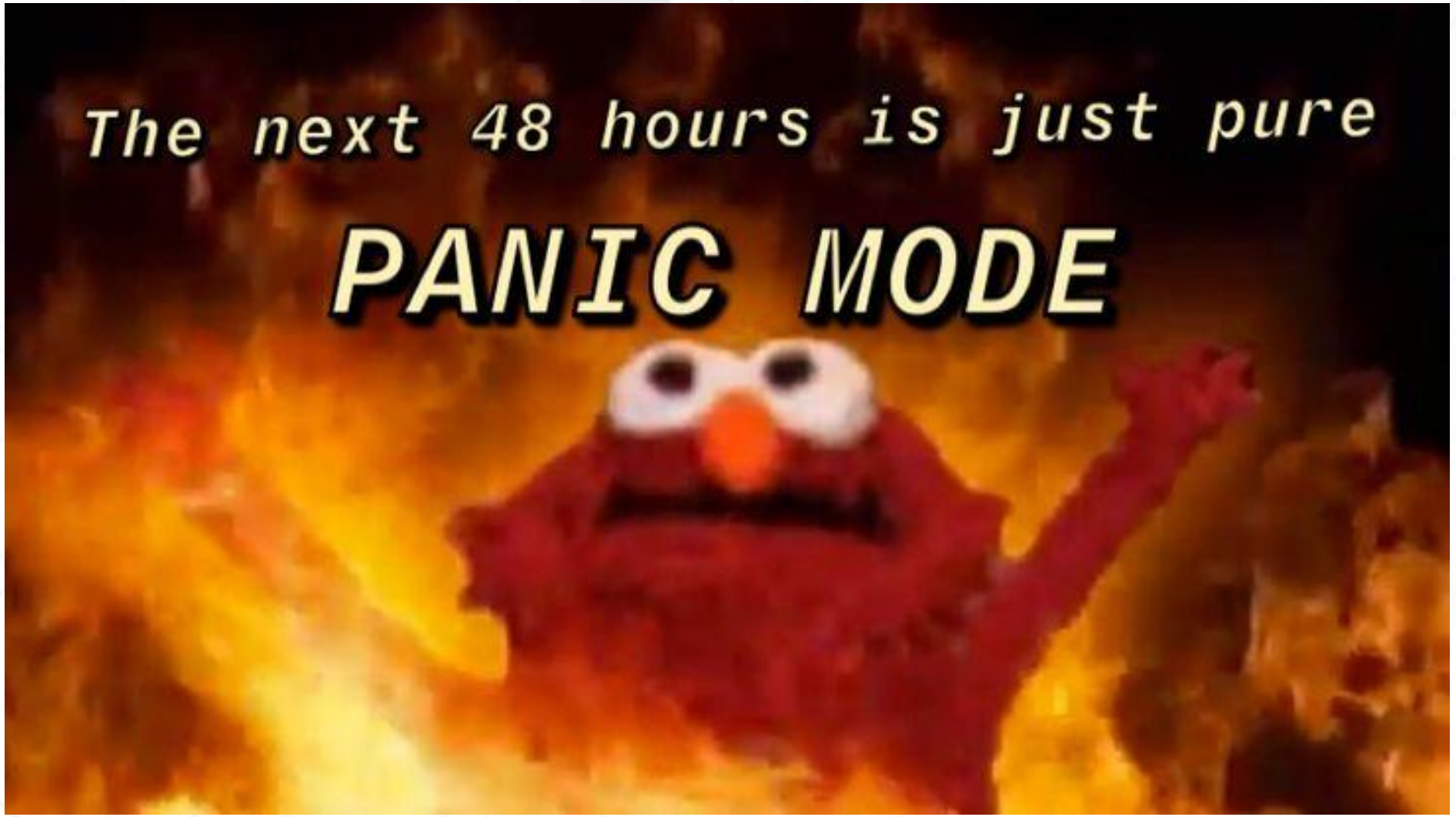
Mesh Network

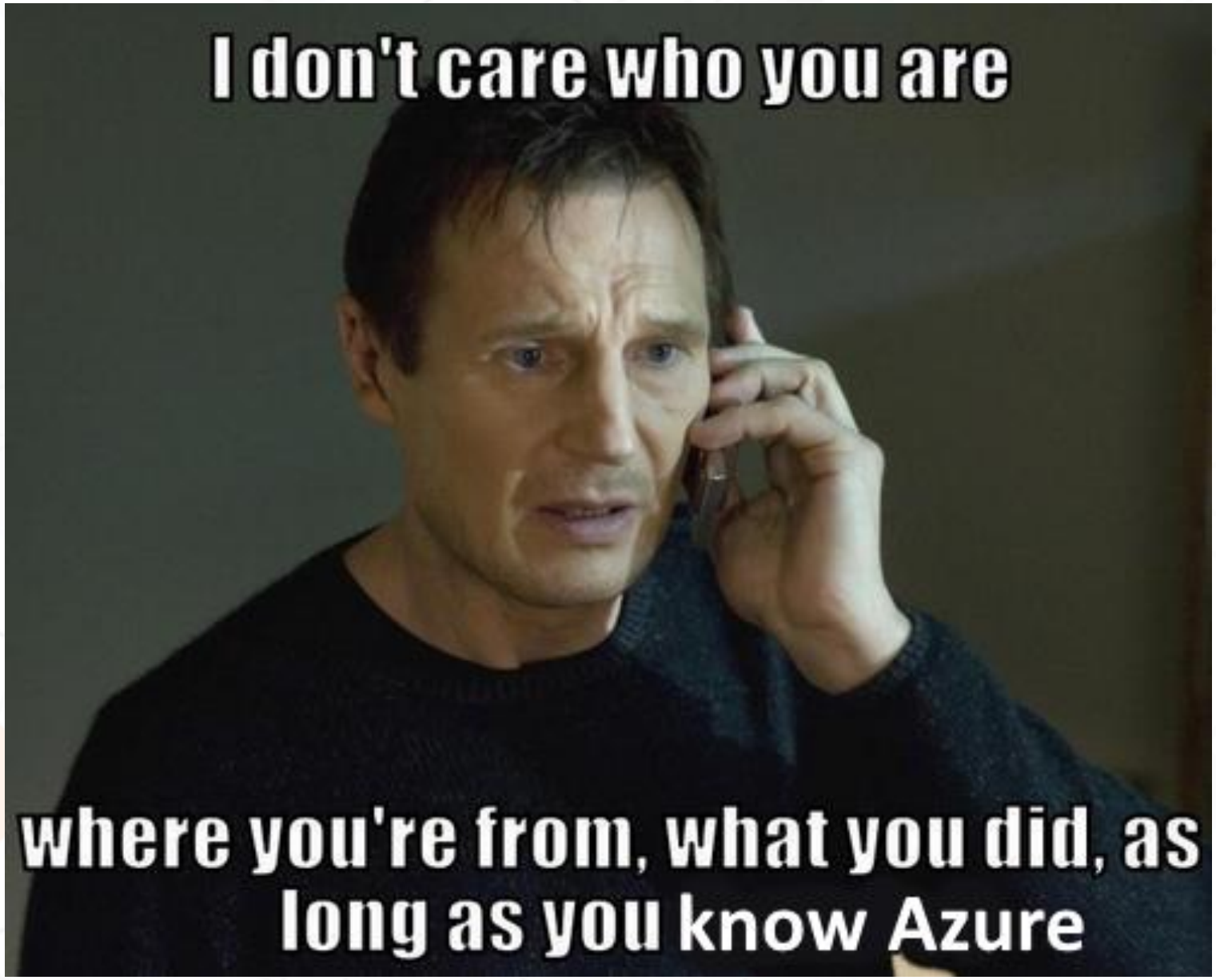


Hub and Spoke Mesh

CASE STUDY

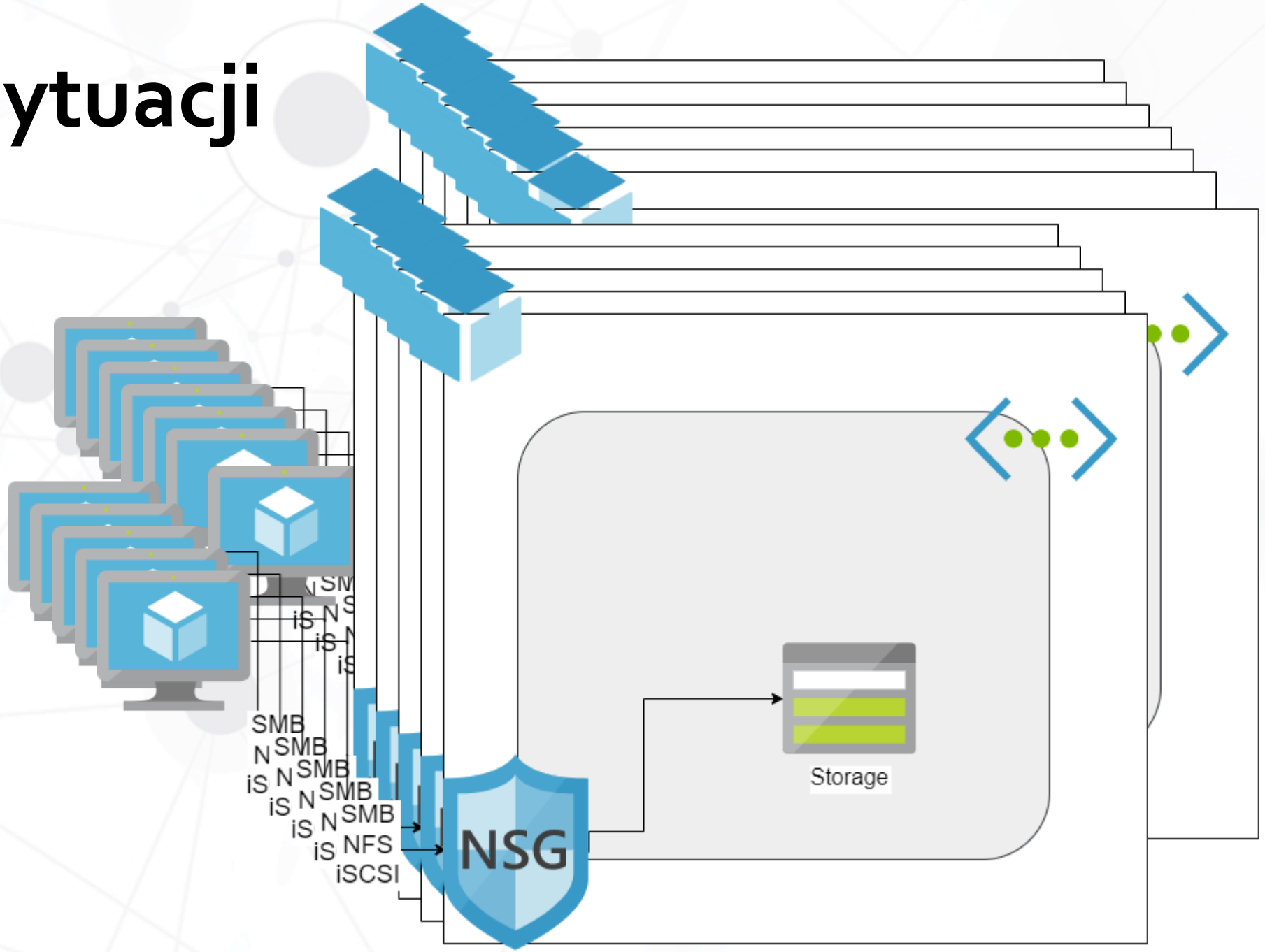

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost


The next 48 hours is just pure
PANIC MODE


I don't care who you are
where you're from, what you did, as long as you know Azure

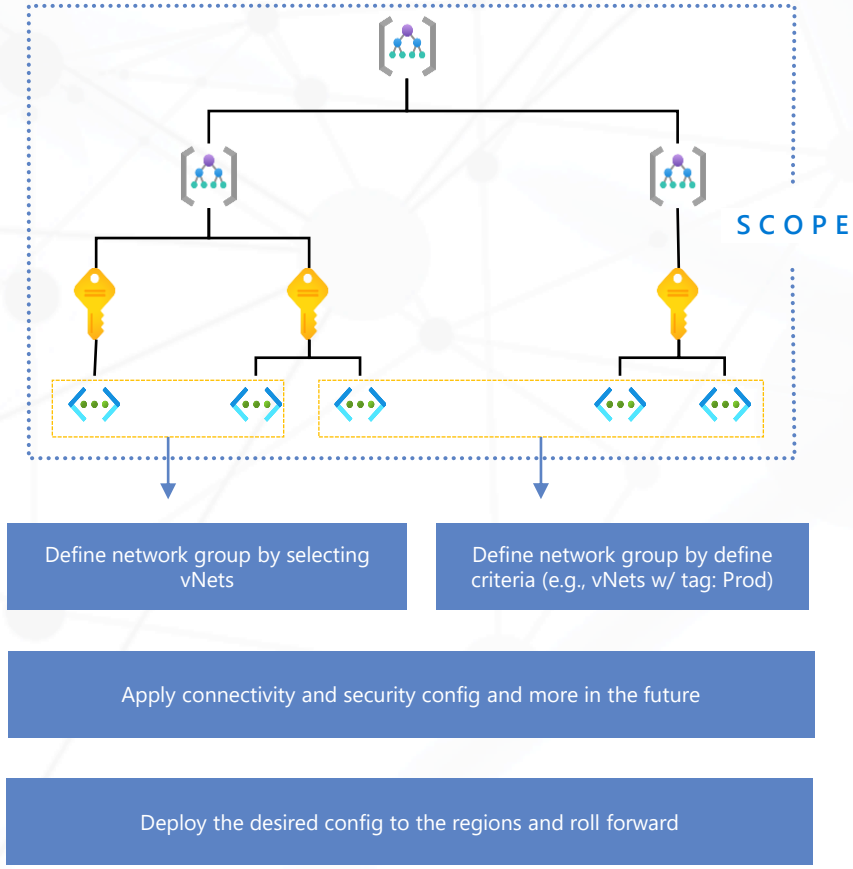
Analiza sytuacji

Analiza sytuacji



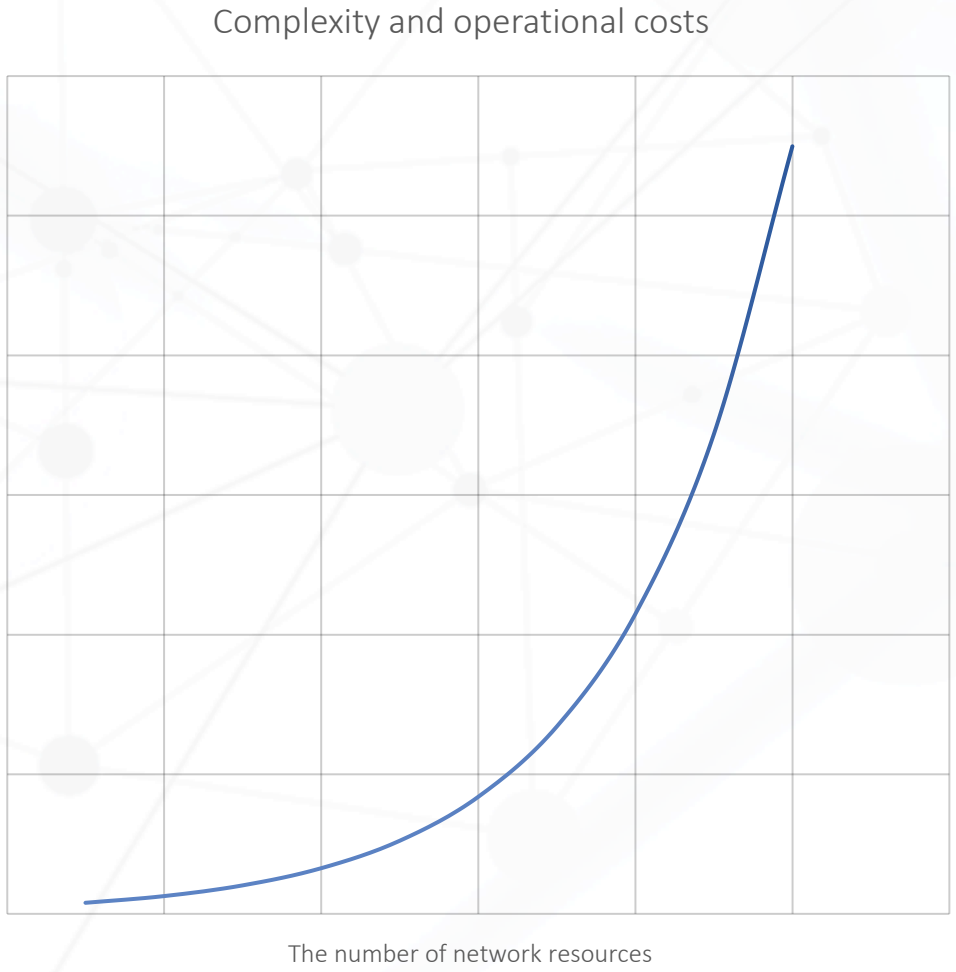
Idea Azure Network Manager

- Uproszczenie centralnego zarządzania sieciami w Azure
- Definiowanie zakresu (scope)
- Lepsza segmentacja sieci i zarządzanie nią
- Rozdzielenie konfiguracji i wdrożenia
- AVNM może stworzy grupy sieci w danym zakresie i zaaplikuje do nich konfigurację
- Dane funkcje mogą być zarządzane przez jedną instancje AVNM lub więcej, jednak nie mogą one mieć tych samych zakresów
- Network Grupa może zawierać kolekcję tych samych zasobów którym można przypisać konfigurację sieciową lub bezpieczeństwa. Obecnie są to VNETy, ale w przyszłości mają to być to grupy subnetów czy Network Interface.
- Przyszłość: Import reguł z NSG oraz integracja z Azure vWAN



Funkcja połączeń

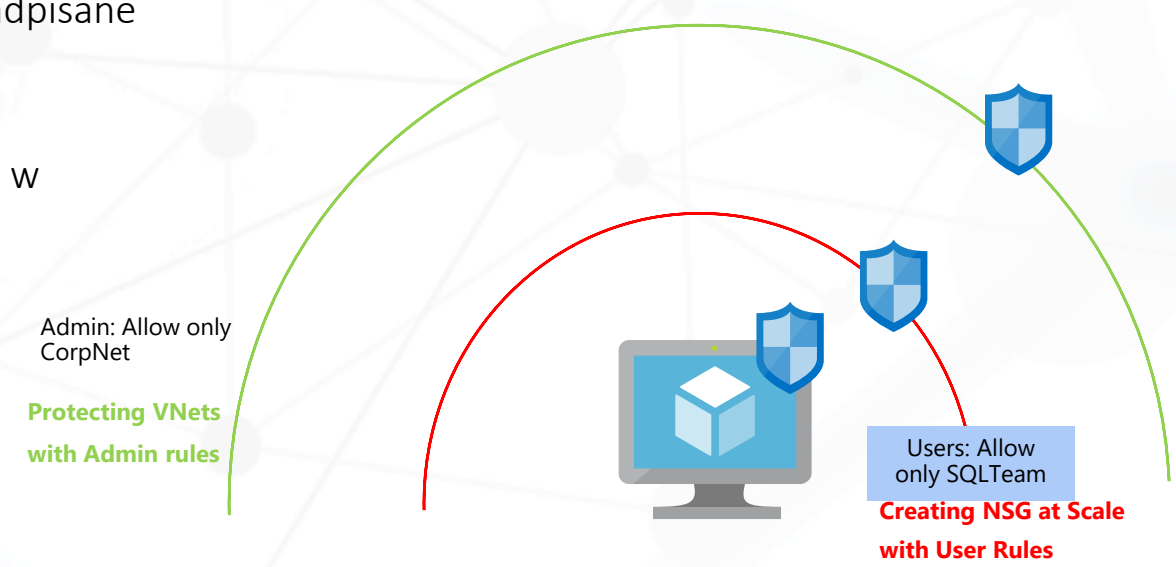
- Łatwe tworzenie nowych topologii sieciowych
- Łatwiejsze zarządzanie kompleksowymi konfiguracjami sieciowymi
- Opcje konfiguracji:
  - Hub and Spoke
  - Mesh (Nie ma peeringu – tylko connect group)
  - Hub and Spoke Mesh
- Skalowanie do 1000+ sieci Mesh
- Konfiguracja peeringów w jednym bądź wielu regionach
- Łatwa segmentacja sieci na Dev, Prod, Test itp.
- Grupowanie sieci na poziomie tenanta, management groupy lub subskrypcji
- Statyczne lub dynamiczne dodawanie sieci do group
- Zastosowanie konfiguracji na poziomie network groups



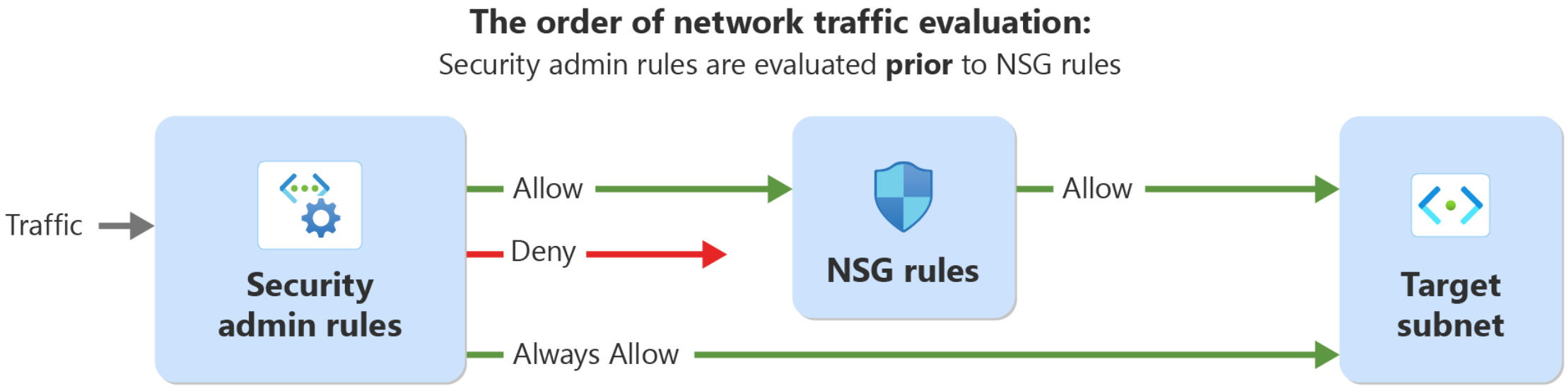
Funkcja bezpieczeństwa

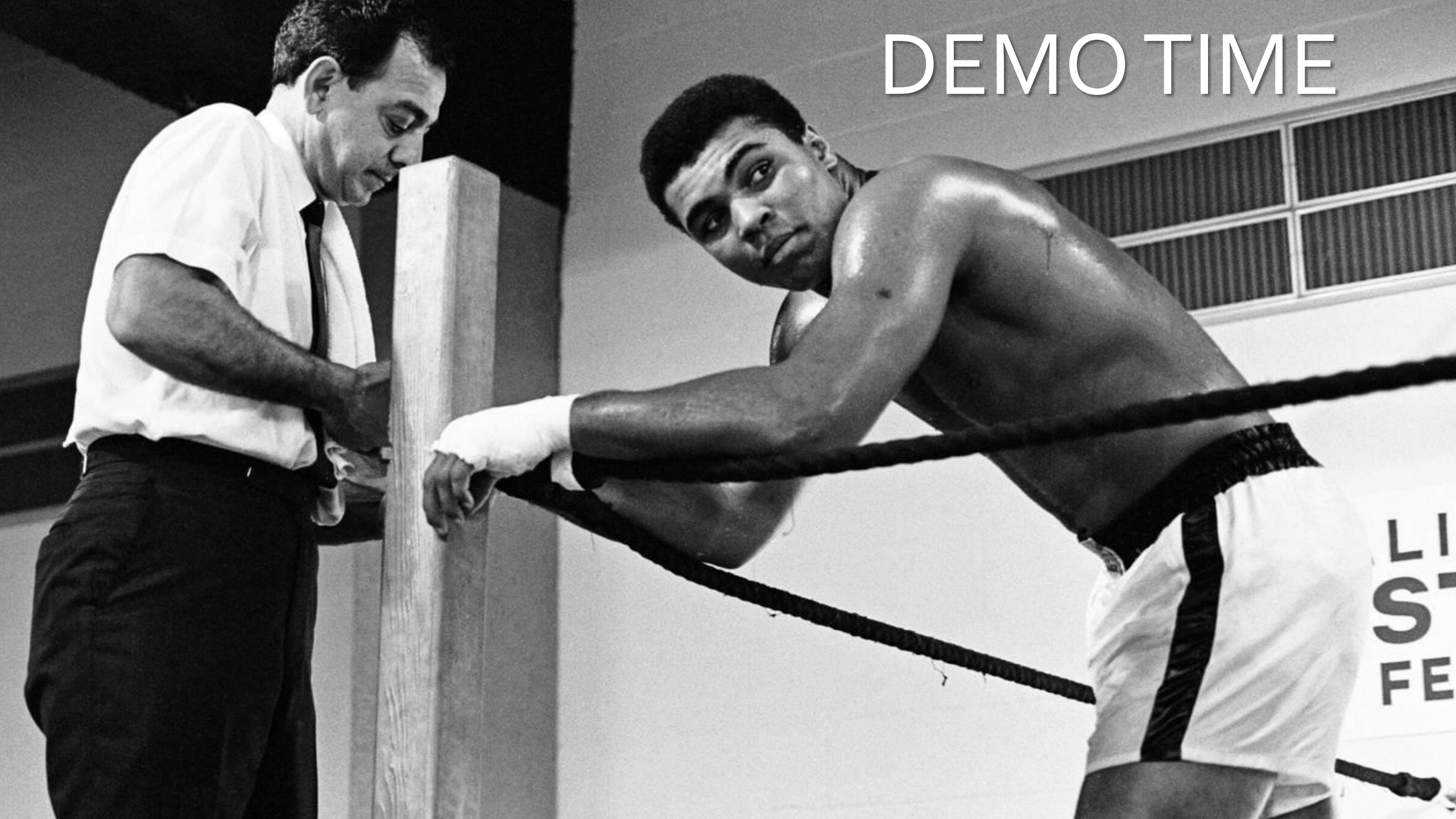
- Reguły Administratora – nowy koncept
  - Kompozycja podobna do reguł NSG (TO NIE NSG)
  - Opcje regulacji ruchu – Allow, Deny, Always Allow
  - Automatyczne dodawanie zasobów do polityk AVNM
  - Wymuszenie reguł organizacyjnych które nie mogą zostać nadpisane przez NSG
  - Target audience: Network admins, NetOps itp.
  - Reguły administratora są aplikowane do wszystkich zasobów w wyznaczonych grupach sieciowych
  - Prostsze zabezpieczenie ruchu na dużą skalę
  - Wdrożenie konfiguracji na wyznaczone region

- Reguły użytkownika (Nie zaimplementowane jeszcze)
  - Użycie tylko reguł Allow dla ruchu http, https oraz ssh
  - Łatwość zarządzania dostępem
  - Target audience: teamy produktowe i usługowe
  - Reguły powinny być conflict-free



Zasada działania Reguł Administratora




DEMO TIME

Demo for online readers

- 3 groups of 10 test VNETs, each with a small VM running IIS
  - Template: mddazure/multiple-vnets-with-vms (github.com)
  - Terraform Network Manager code: https://github.com/technicalflow/myterraform/tree/main/NetworkManagerAzAPI

Home > Network Managers >

Create an Azure Network Manager resource

Azure Network Manager | PREVIEW

Basics Tags Review + create

Create an Azure Network Manager to create and apply configurations across your network environments.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Internal MdD 1

Resource group * anm

Create new

Instance details

Name * demo-anm

Region * (US) East US

Description

Scope and Features

Azure Network Manager lets you create groups of networks within the scope you define below, and apply configurations based on the features you select. The selected features can be managed by one instance of Azure Network Manager, or by seperate instances. However, multiple instances can't overlap on one selected scope. For example, two instances of Azure Network Manager can't manage security for the same management group.

Scope * Internal MdD 1

Select scopes

Features * 2 selected

Select scopes

PREVIEW

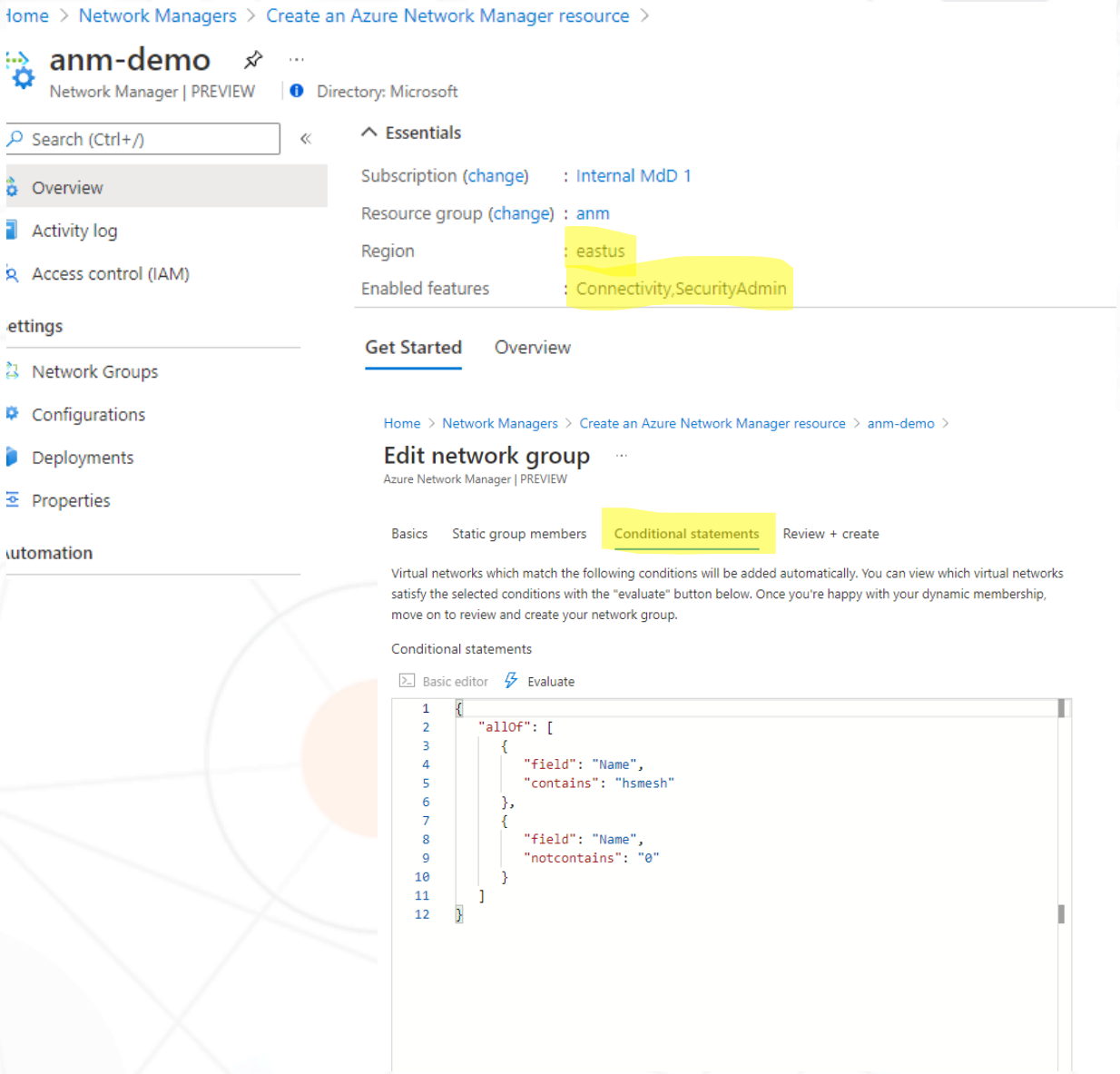
SCOPES

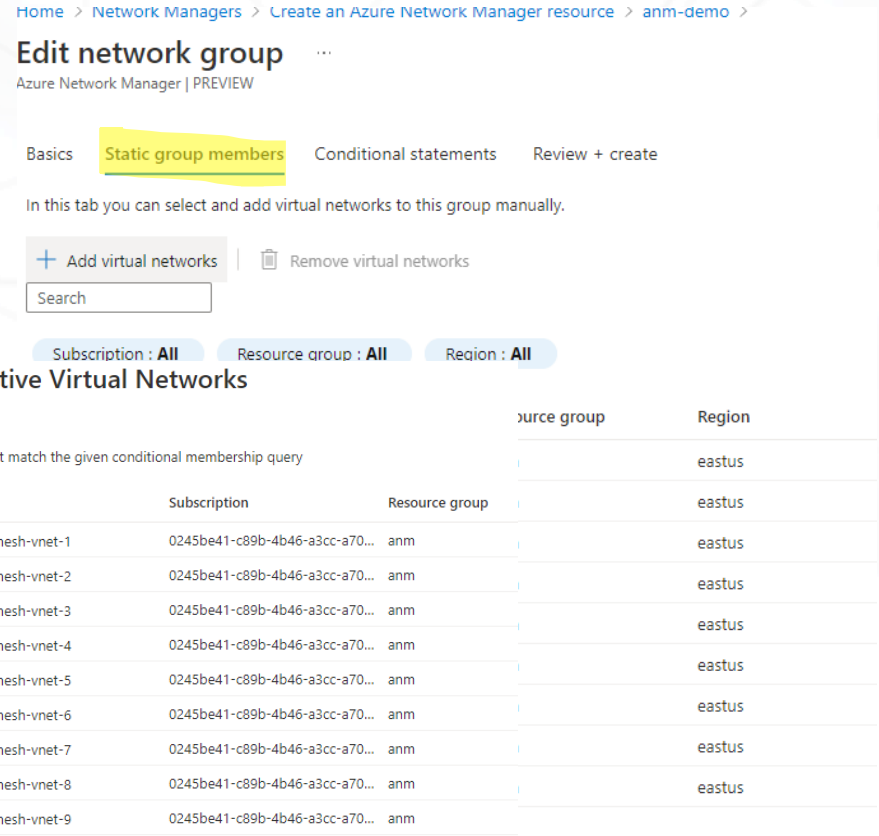
- 72f988bf-86f1-41af-91ab-2d7cd011db47
  - CnAI Orchestration Service Public Corp prod
    - Non Production
      - NonProd Ring1
        - ASC DEMO
    - WCBMG
      - MicrosoftSolutionsMG
        - Internal MdD 1
        - Internal MdD 2
      - ServicesMG
        - ProjectPurposeMG
          - InternalProjectsMG
            - DevTestEnvironmentMG
              - ES-CUS-PwCECDWAssist-DEV-Asodemo
    - Contoso IT - Retail - Prod

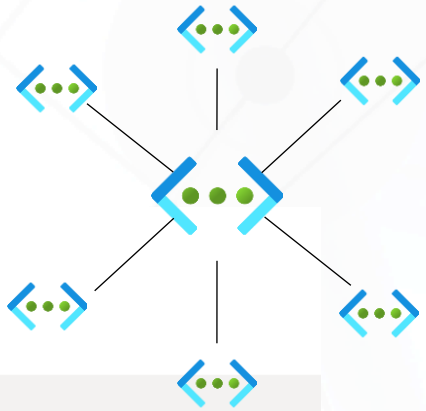
Add to selected scope

SELECTED SCOPES

Internal MdD 1


Home > Network Managers > Create an Azure Network Manager resource >
anm-demo
Network Manager | PREVIEW
Directory: Microsoft
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
ettings
Network Groups
Configurations
Deployments
Properties
utomation
Essentials
Subscription (change) : Internal MdD 1
Resource group (change) : anm
Region : eastus
Enabled features : Connectivity,SecurityAdmin
Get Started
Overview
Home > Network Managers > Create an Azure Network Manager resource > anm-demo >
Edit network group
Azure Network Manager | PREVIEW
Basics
Static group members
Conditional statements
Review + create
Virtual networks which match the following conditions will be added automatically. You can view which virtual networks satisfy the selected conditions with the "evaluate" button below. Once you're happy with your dynamic membership, move on to review and create your network group.
Conditional statements
Basic editor
Evaluate
{
"allOf": [
{
"field": "Name",
"contains": "hsmesh"
},
{
"field": "Name",
"notcontains": "0"
}
]
}


Home > Network Managers > Create an Azure Network Manager resource > anm-demo >
Edit network group
Azure Network Manager | PREVIEW
Basics
Static group members
Conditional statements
Review + create
In this tab you can select and add virtual networks to this group manually.
Add virtual networks
Remove virtual networks
Search
Subscription : All
Resource group : All
Region : All
Effective Virtual Networks
PREVIEW
Vnets that match the given conditional membership query
Name
Subscription
Resource group
Region
hsmesh-vnet-1 0245be41-c89b-4b46-a3cc-a70... anm eastus
hsmesh-vnet-2 0245be41-c89b-4b46-a3cc-a70... anm eastus
hsmesh-vnet-3 0245be41-c89b-4b46-a3cc-a70... anm eastus
hsmesh-vnet-4 0245be41-c89b-4b46-a3cc-a70... anm eastus
hsmesh-vnet-5 0245be41-c89b-4b46-a3cc-a70... anm eastus
hsmesh-vnet-6 0245be41-c89b-4b46-a3cc-a70... anm eastus
hsmesh-vnet-7 0245be41-c89b-4b46-a3cc-a70... anm eastus
hsmesh-vnet-8 0245be41-c89b-4b46-a3cc-a70... anm eastus
hsmesh-vnet-9 0245be41-c89b-4b46-a3cc-a70... anm



Home > Network Managers > Create an Azure Network Manager resource > anm-demo >

Edit a connectivity configuration

Azure Network Manager | PREVIEW

Name: hubspoke

Description:

Topology
- ○ Mesh
- ◉ Hub and Spoke

Hub: hs-vnet-0

Select a hub

Existing peerings

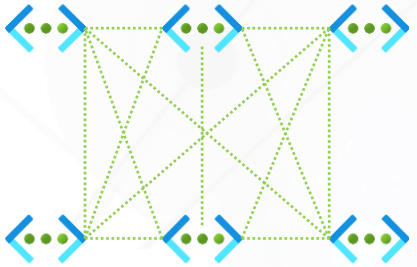
☑ Delete existing peerings

Spoke network groups

Within each network group, all virtual networks are peered to the hub. Check the box for transitivity to peer virtual networks within the same group and region. Check the box for global mesh to peer virtual networks within the same group across a

+ Add network groups | Remove network groups

Network group name	Transitivity	Global Mesh	Gateway
hubspoke	☐ Enable peering within network group	☐ Enable mesh connectivity across regions	☑ Use hub as a gateway



Home > Network Managers > anm-demo >

Add a connectivity configuration

Azure Network Manager | PREVIEW

Name *: mesh

Description:

Topology: (•) Mesh ( ) Hub and Spoke

Global Mesh

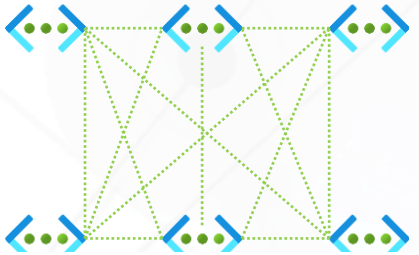
[ ] Enable mesh connectivity across regions

Network Groups

The virtual networks that are in the same region will be peered across all network groups selected below. Check the box for global mesh to peer virtual networks across regions.

+ Add network groups | Remove network groups

Network Groups	Static Group Members	Dynamic Membership Enabled
mesh		Yes



mesh-VMNic-1 | Effective routes

Network interface | Directory: Microsoft

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags

Settings

- IP configurations
- DNS servers
- Network security group
- Properties
- Locks

Download | Refresh | Give feedback

Showing only top 200 records, click Download above to see all.

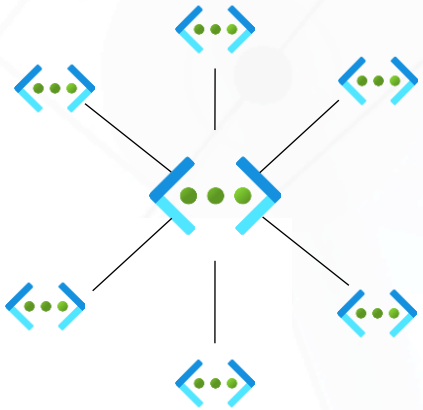
Scope: Network interface (mesh-VMNic-1)

Associated route table: -

Effective routes

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address	User Defined Route Name
Default	Active	10.0.1.0/24	Virtual network	-	-
Default	Active	10.0.9.0/24, 8 more	ConnectedGroup	-	-
Default	Active	0.0.0.0/0	Internet	-	-

A	B	C	D	E	F	G	H	I
Column1	Column2	Column3	Column4	Column5	Column6	Column7	Column8	Column9
Source,"State","Address Prefixes","Next Hop Type","Next Hop IP Address","User Defined Route Name"								
Default,"Active","10.0.1.0/24","Virtual network","",""								
Default,"Active","10.0.9.0/24	10.0.8.0/24	10.0.7.0/24	10.0.6.0/24	10.0.5.0/24	10.0.4.0/24	10.0.3.0/24	10.0.2.0/24	10.0.0.0/24","ConnectedGroup","",""
Default "Active" "0.0.0.0/0" "Internet" "" ""								



hs-vnet-0 | Peerings

Virtual network | Directory: Microsoft

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

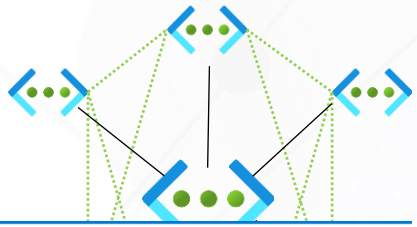
Settings

- Address space
- Connected devices
- Subnets
- DDoS protection
- Firewall
- Security
- Network manager
- DNS servers
- Peerings
- Service endpoints

Add | Refresh | Sync

Filter by name... | Peering status == **all**

Name	Peering status	Peer	Gateway transit
ANM_22740FFA83EB4B03043CC7E_hs-vn...	Deleting	hs-vnet-6	Enabled
ANM_22740FFA83EB4B03043CC7E_hs-vn...	Connected	hs-vnet-5	Enabled
ANM_22740FFA83EB4B03043CC7E_hs-vn...	Connected	hs-vnet-8	Enabled
ANM_22740FFA83EB4B03043CC7E_hs-vn...	Connected	hs-vnet-7	Enabled
ANM_22740FFA83EB4B03043CC7E_hs-vn...	Connected	hs-vnet-2	Enabled
ANM_22740FFA83EB4B03043CC7E_hs-vn...	Connected	hs-vnet-9	Enabled
ANM_22740FFA83EB4B03043CC7E_hs-vn...	Connected	hs-vnet-1	Enabled



Home > Network Managers > anm-demo >

Add a connectivity configuration

Azure Network Manager | PREVIEW

Name *: hubspokemesh

Description:

Topology: (•) Hub and Spoke ( ) Mesh

Hub: hsmesh-vnet-0

Select a hub

Existing peerings

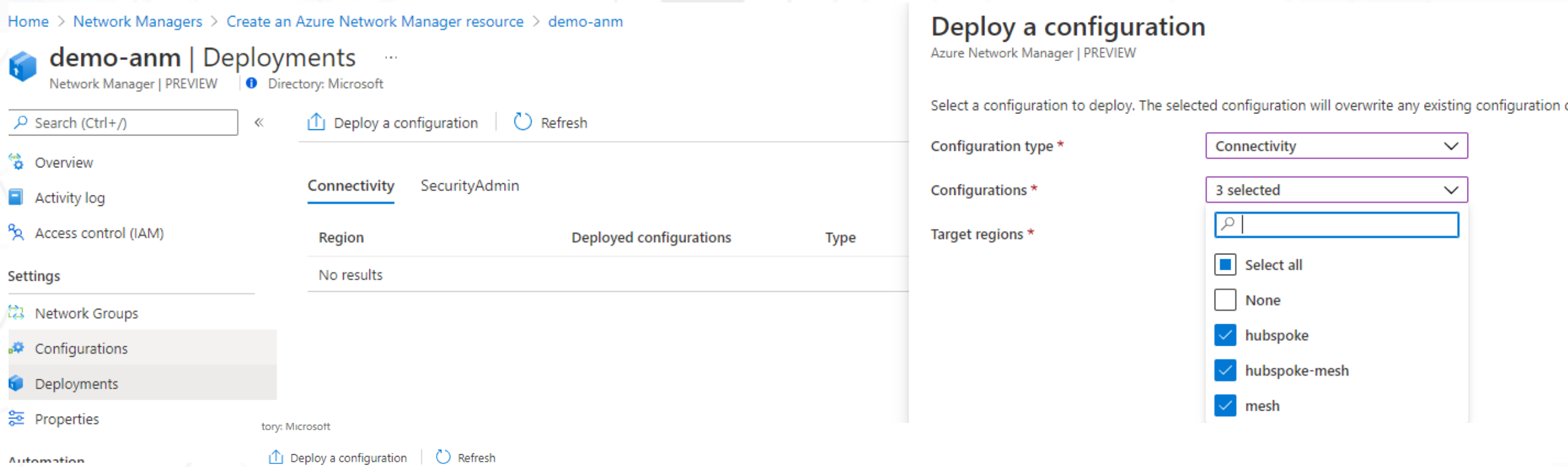
[x] Delete existing peerings

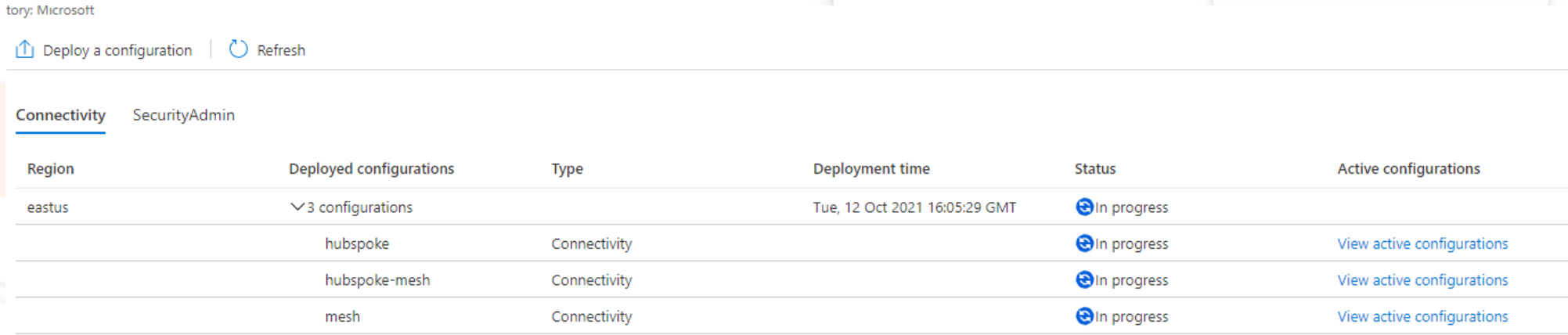
Spoke network groups

Within each network group, all virtual networks are peered to the hub. Check the box for transitivity to peer virtual networks within the same group and region. Check the box for global mesh to peer virtual networks within the same group across all regions.

+ Add network groups | Remove network groups

Network group name	Transitivity	Global Mesh	Gateway
[ ] hsmesh	[x] Enable peering within network group	[ ] Enable mesh connectivity across regions	[x] Use hub as a gateway


Home > Network Managers > Create an Azure Network Manager resource > demo-anm
demo-anm | Deployments
Network Manager | PREVIEW
Directory: Microsoft
Search (Ctrl+/)
Deploy a configuration
Refresh
Overview
Activity log
Access control (IAM)
Settings
Network Groups
Configurations
Deployments
Properties
Connectivity
SecurityAdmin
Region
Deployed configurations
Type
No results
Deploy a configuration
Azure Network Manager | PREVIEW
Select a configuration to deploy. The selected configuration will overwrite any existing configuration
Configuration type *
Connectivity
Configurations *
3 selected
Target regions *
Select all
None
hubspoke
hubspoke-mesh
mesh


Deploy a configuration
Refresh
Connectivity
SecurityAdmin
Region
Deployed configurations
Type
Deployment time
Status
Active configurations
eastus
3 configurations
Tue, 12 Oct 2021 16:05:29 GMT
In progress
hubspoke
Connectivity
In progress
View active configurations
hubspoke-mesh
Connectivity
In progress
View active configurations
mesh
Connectivity
In progress
View active configurations

Edit a rule collection

Azure Virtual Network Manager | PREVIEW

Name: testrulecoll

Target network groups *: hubspoke

Rules

+ Add a rule | Delete

Rule name	Priority	Direction	Protocc
allwRDPin	45	Inbound	Tcp

Edit a rule

Azure Virtual Network Manager | PREVIEW

Name	allwRDPin
Description	
Priority *	45
Action *	Always Allow
Direction *	Inbound
Protocol *	Tcp
Source type	IP address
Source IP addresses	*
Source port	0-65535
Destination type	IP address
Destination IP addresses	10.0.0.0/24, 104.45.135.185
Destination port	3389

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)

Settings
Network Groups
Configurations
Deployments
Properties

Automation
Tasks (preview)

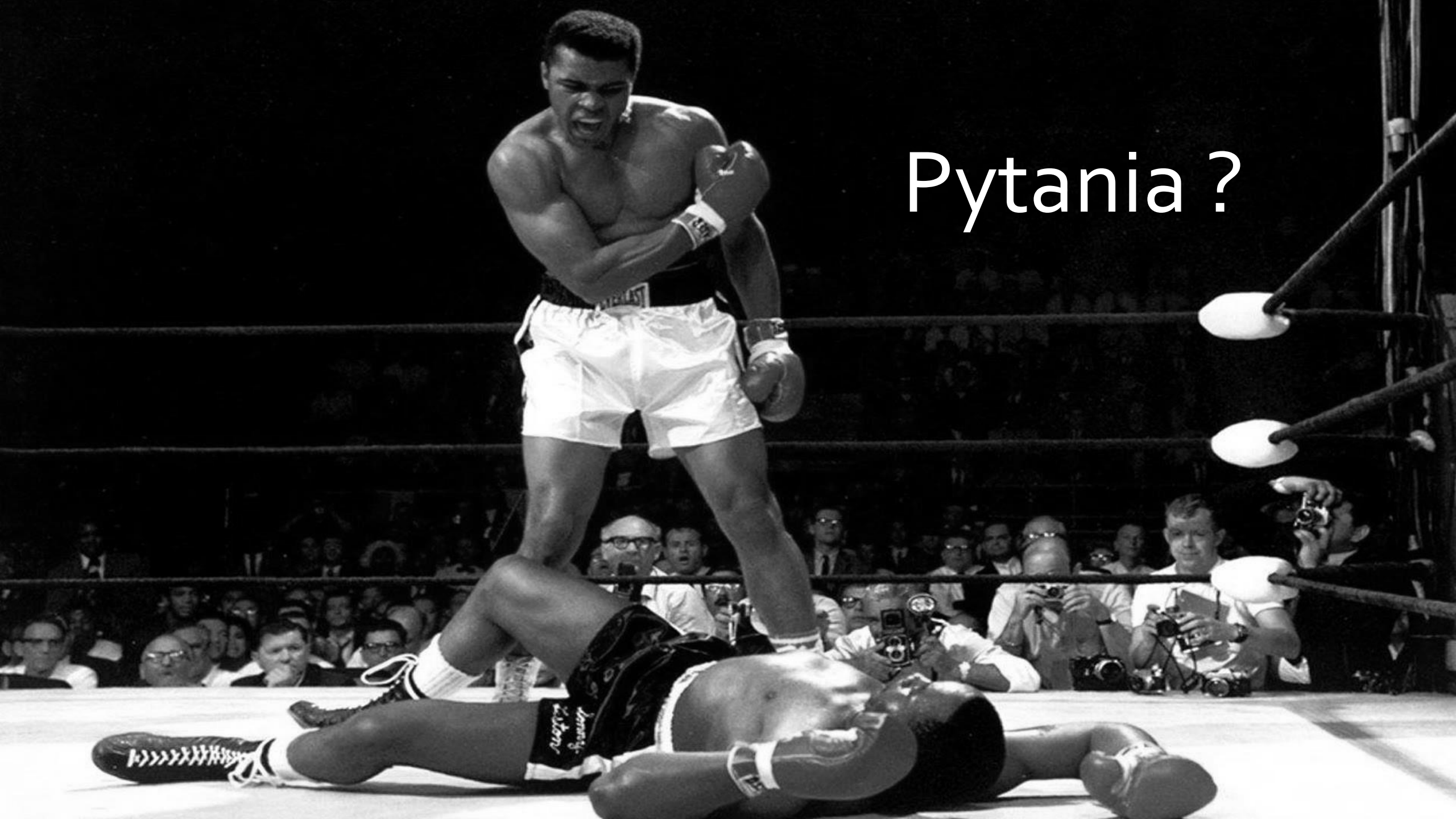
Support + troubleshooting
New Support Request

Deploy a configuration

Azure Virtual Network Manager | PREVIEW

The selected configuration for deployment will overwrite any existing configuration of the same type in the target region. This is because when you commit your configuration, you are defining your overall desired state of your configuration. Azure Virtual Network Manager w make the necessary changes to honor this state. The target regions selected are where the configurations will be applied.

Configuration type *	SecurityAdmin
Configurations *	SecurirtyDemoConfig
Target regions *	East US


Pytania ?

Podsumowanie

Czy jest Network Manager …

- Rozwiązaniem na problemy skali sieci
- Ułatwienie zarządzania połączeniami sieci
- Ułatwienie zarządzania bezpieczeństwem sieci
- Ułatwienie regulacji dostępu

… a czym nie jest

- One to rule them all tool
- Zastępstwem dla NSGs
- Zastępstwem dla ustawiania Peeringów

Future:

- Reguły użytkownika
- Grupy Subnetów
- Grupy interfejsów sieciowych - NIC
- Import reguł NSG
- Integracja z vWAN Hub

Dziękuję

- Kod:

  https://github.com/technicalflow/myTerraform

- Network Manager
  - https://learn.microsoft.com/en-us/azure/virtual-network-manager
  - https://www.youtube.com/watch?v=qNn83S55WHQ

- Więcej ciekawych informacji o sieciach:
  - https://www.youtube.com/c/AdamStuart1