Navigating the cloud with Azure Network Manager for scalable, secure, and centralised solutions

Adedeji Awolesi

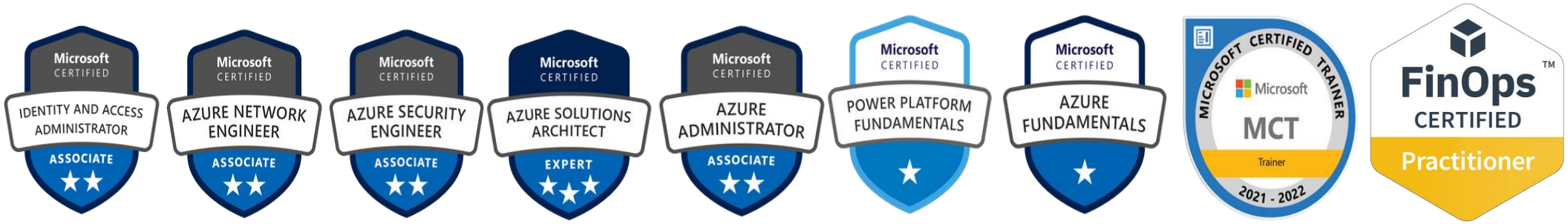
Agenda

- What is a Network
- Virtual Network
- Azure Virtual Network Manager (AVNM)
- Key Benefit
- Common Use Cases - AVNM
- How does AVNM works
- Network Group
- Connectivity Configuration
- Connected Groups
- Common Use Cases
- Deployments
- Security Configurations
- Security Admin rule vs NSG
- Common Use Cases – Security Rule
- Security Hierarchy
- Demo
- Conclusion

About ME

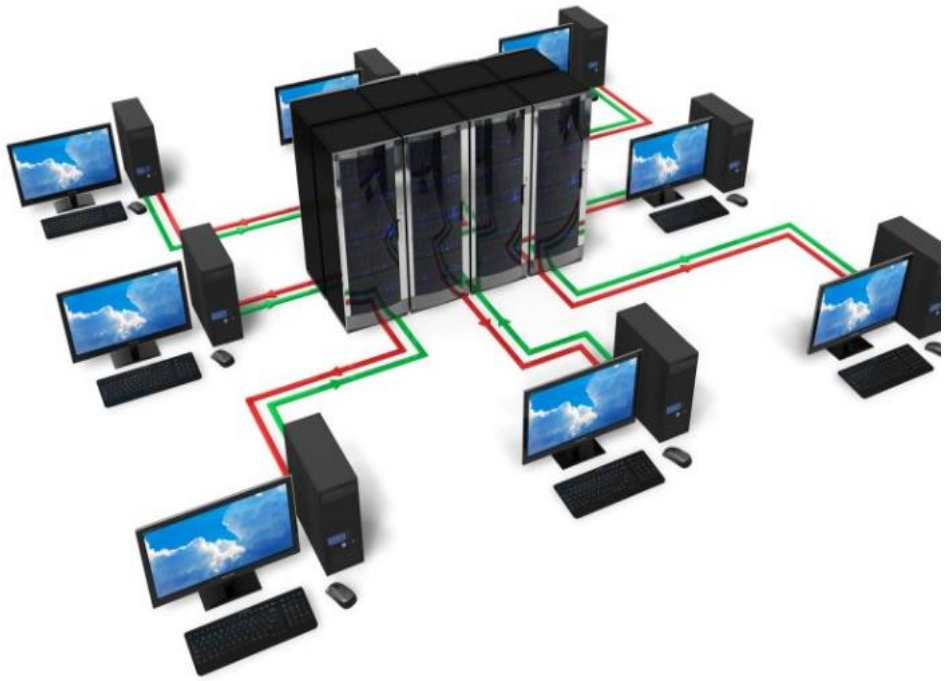
Adedeji Awolesi
Cloud Engineer - SS&C Blue Prism
BSc Management Information Systems
MBA Oil and Gas Management
10 years IT Experience
Azure Certified (8+), GCP (1), FinOps Certified Practitioner

https://www.linkedin.com/in/scopnat/



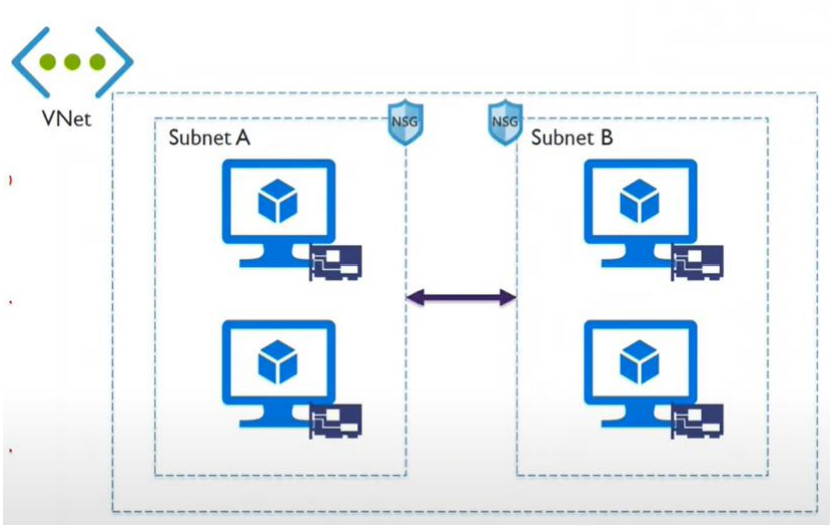
What is a Network?

A (Computer) network is a set of interconnected devices that communicate with each other and share resources.



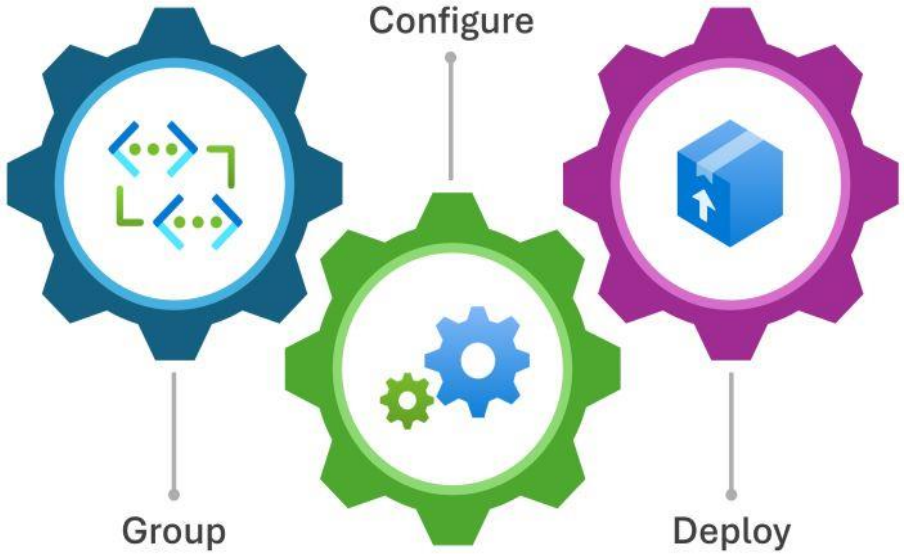
Virtual Network

An Azure Virtual Network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription



Azure Virtual Network Manager

- Is a centralised network management solution that helps you manage connectivity and security of your network resources.
- Simplifies and centrally manage azure networks at scale.
- Group → Configure →Deploy



Key Benefits

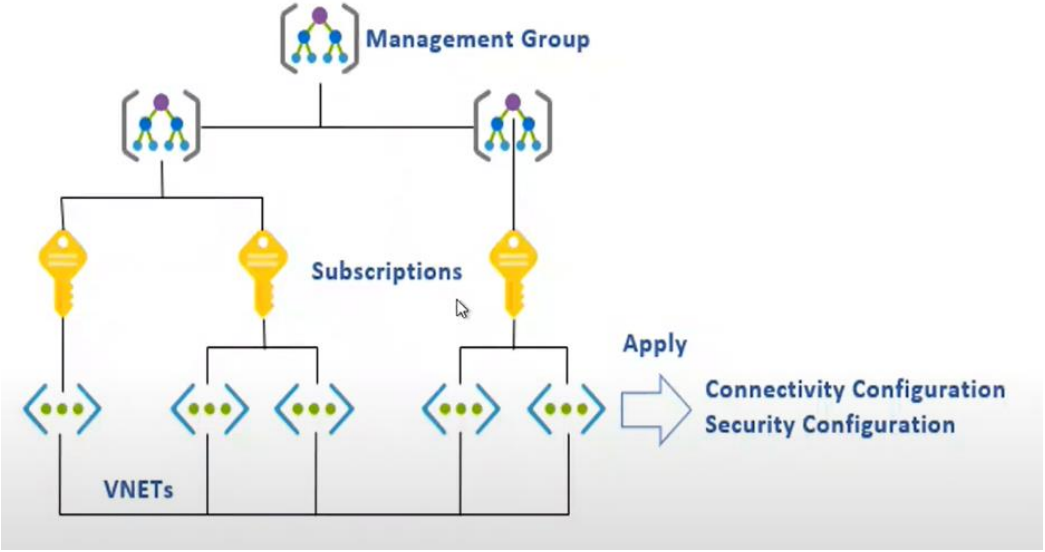
- Centralised Control – simplified global management across regions and subscription.
- Automatic configurations of application on network resources – Connectivity maintenance & day zero protection.
- Enforced security rules across your organisation new & existing network resources – Mitigate risk of changes or security holes.
- Regional deployment of configuration changes – Safely test in regions, fix and roll forward

Common use cases

Connectivity	Security
Create connectivity between subs, regions and tenant	Create org level standard rules that would be applied to new and existing VNET and not be modified.
Automatically create hub and spoke or Mesh topology	Create security boundaries and allow VNET owners manage NSG without breaking org policy.
Allow Vnet Spoke to directly connect to each other	Force allow traffic to & from critical services and not allow accidental block

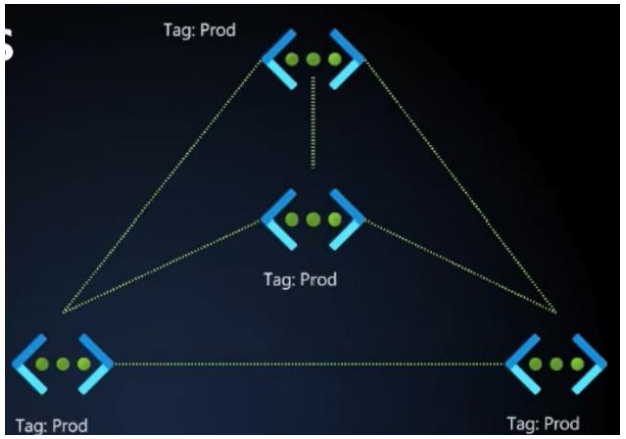
How does AVNM works?

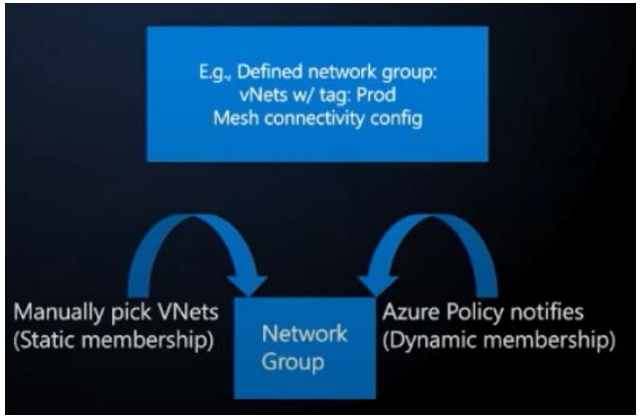
- Scope
- Network Group
- Connectivity configuration
- Security configuration
- Connected group



Network Group

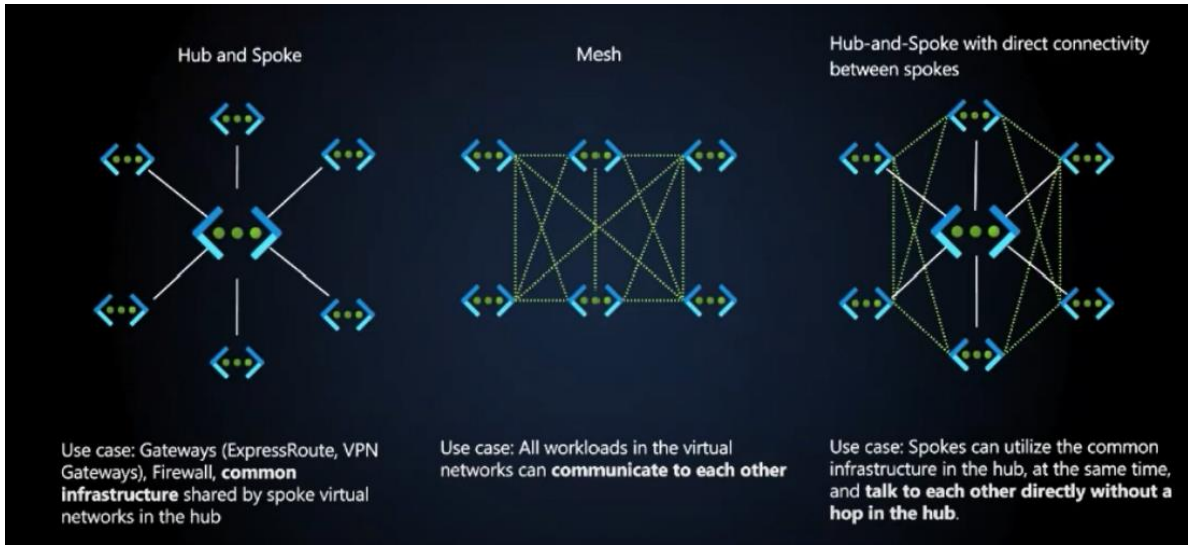
- Are containers/logical segment of your network
    - Eg Dev, Prod, Test or teams
- Group based on subscription, management group or tenant
- Static or Manual grouping
- Dynamic Grouping
    - Policies
        - Basic – ID/Tags/RG/Subs using GUI
        - Advanced – more flexible using JSON
- Any changes in membership will affect config automatically
- Apply the Config to Network Group





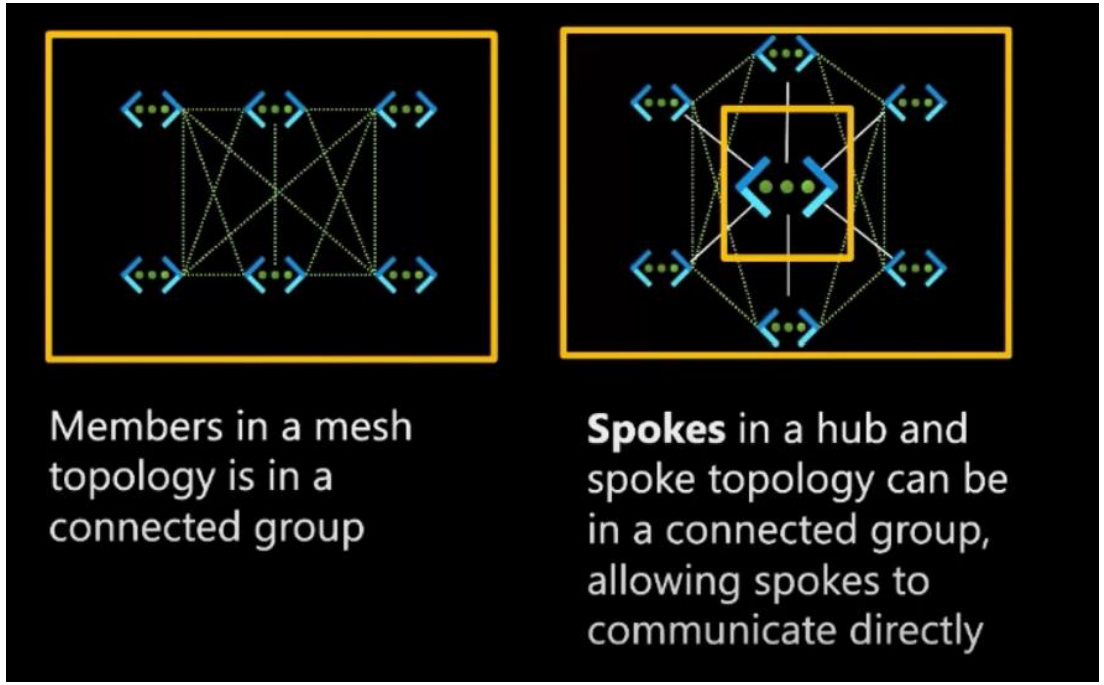
Connectivity Configurations

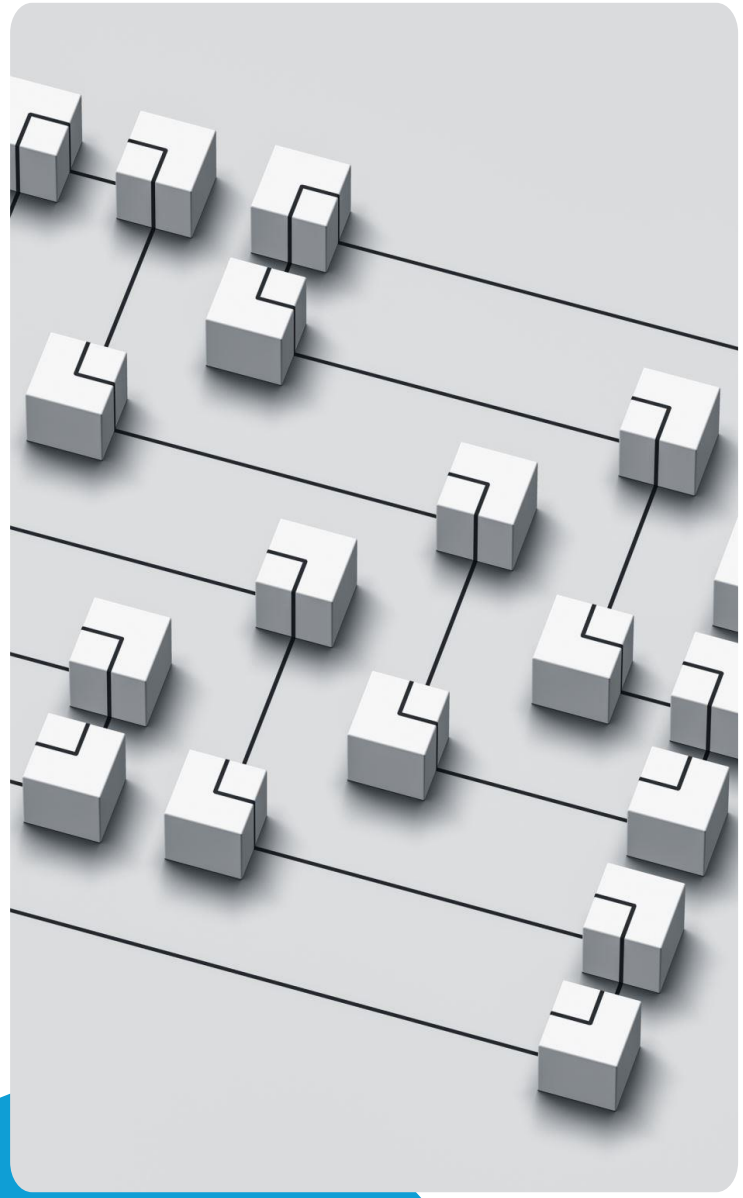
- Hub and Spoke
- Mesh Connectivity
- Hub and Spoke with direct connectivity
- Less hop and lower latency



Connected Groups

- Members in the connected group can communicate with each other
- This is not a peering relationship which is 1-1mapping instead a group.





Common use cases

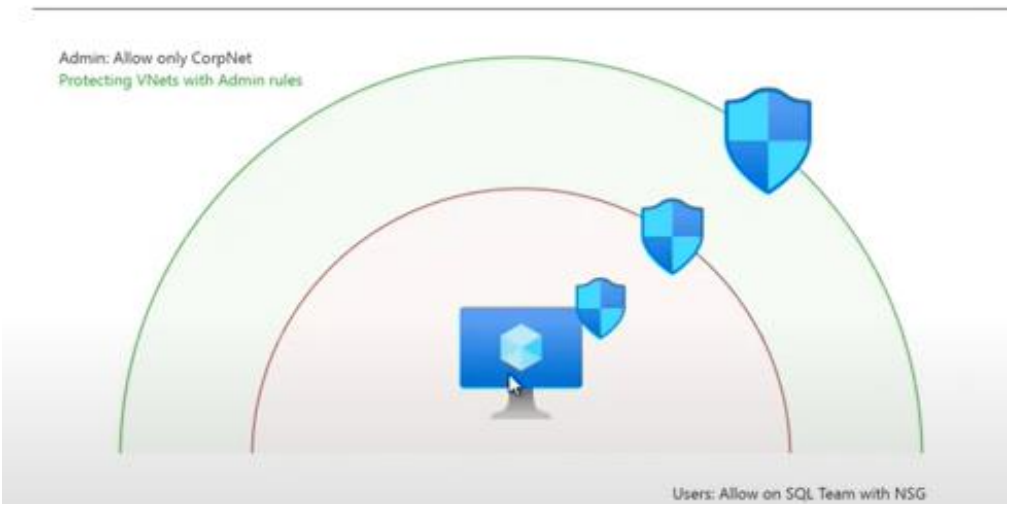
- Connect Vnets across subscriptions and region within a click
- Leverage central infrastructure services in a Hub Vnet with others
  - Establish direct connectivity among Vnets to reduce latency
  - Connect all Prod & Dev Vnets to a Hub and only allow direct connectivity among only Dev or Prod all in the same config
- Automatically maintain connectivity at scale even with addition of new network resources
  - Define NG membership with Policy which removes overhead of ensuring new/existing Vnets are connected as intended

Deployment

- Safely deploy across all regions
- Fix and roll forward

Security Configurations

- Admin Rules - This is not NSG
- This is applied to all resources in a network group.
- Overwrite any conflicting rules
- Enforced Rules
- Input: Security policy →Output: Admin rules



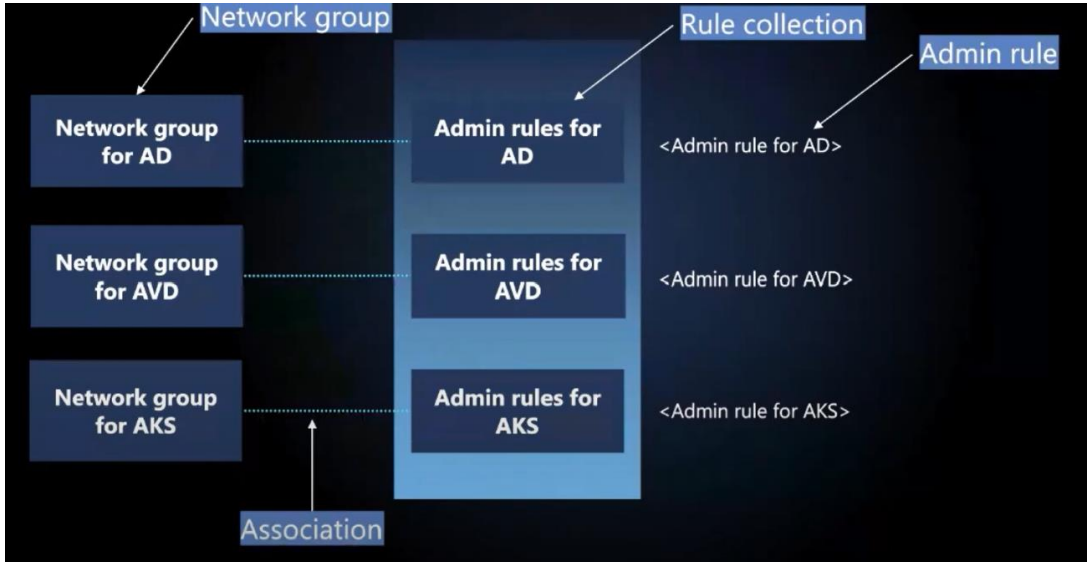
Security Admin rules vs NSG

- The order of network traffic evaluation:
  - Security admin rules are evaluated prior to NSG

- Three types of Rules
  - Allow: Non-terminating
  - Always Allow: Terminating
  - Always Deny: Terminating

Security admin rule construct

- Easily create admin rules for different workloads



Common use for security rules

Apply guardrails security rules – blocking high risk ports.

Enforce standard security rules on all existing and new vnet without risk of change by non admin users.

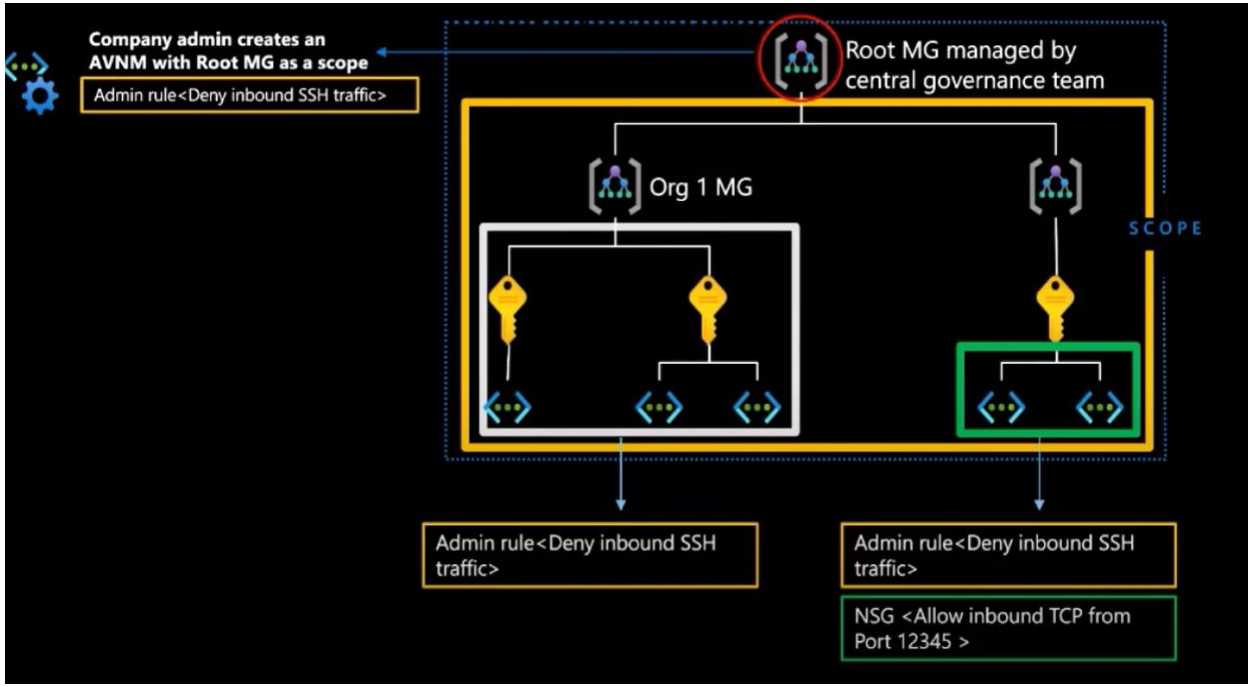
Ensure essential traffic such as monitoring services or program updates is not accidentally blocked.

Day 0 protection for newly provision network resources.

Flexible allow downstream teams to configure NSG as needed for more specific traffic dictation.

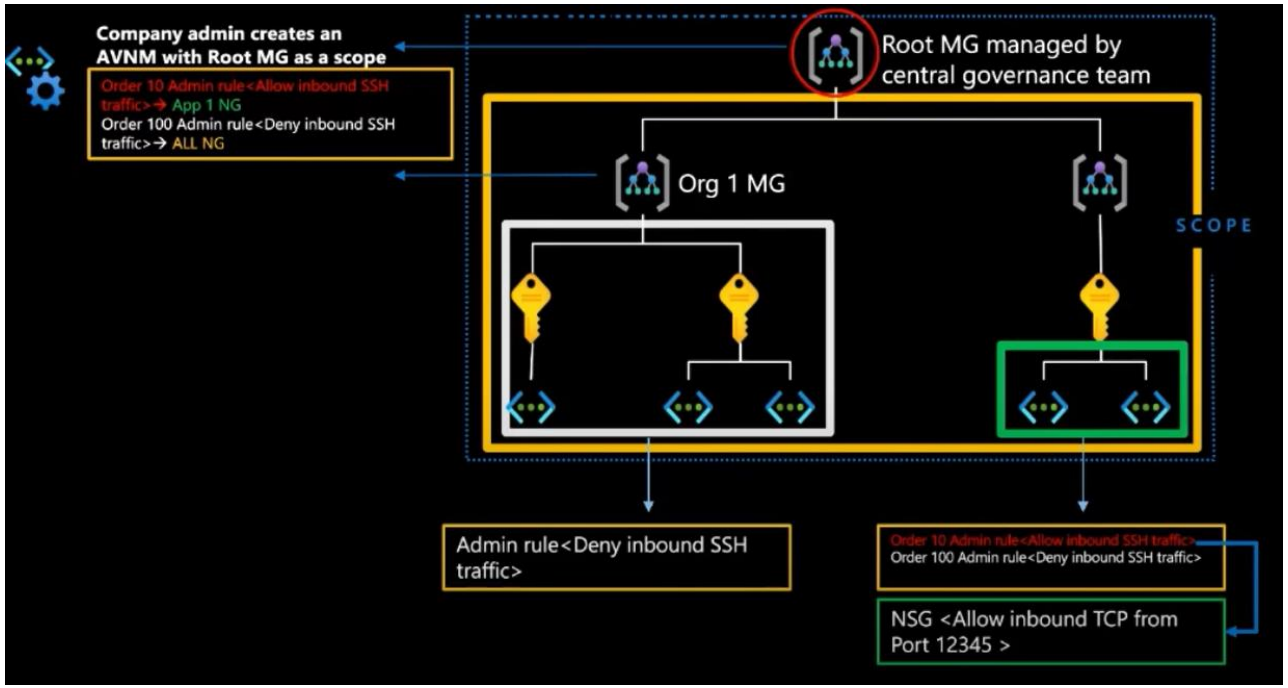
Security hierarchy

- Allows different teams to work together



Security hierarchy - exception

- What if some teams need security admin rule exception



Demo

In conclusion

- AVMN is a highly scalable network management solution.
- Global Management of VNet across region, subs & tenant.
- Automated management and deployment of VNet topology
- High-priority security rule enforcement at scale to protect
- Safe deployment of network configuration across desired regions.

Documentation

https://learn.microsoft.com/en-us/azure/virtual-network-manager/

Azure Virtual Network Manager | Microsoft Azure

https://www.youtube.com/watch?v=hSczkhJuV5Y

THANK YOU