Microsoft

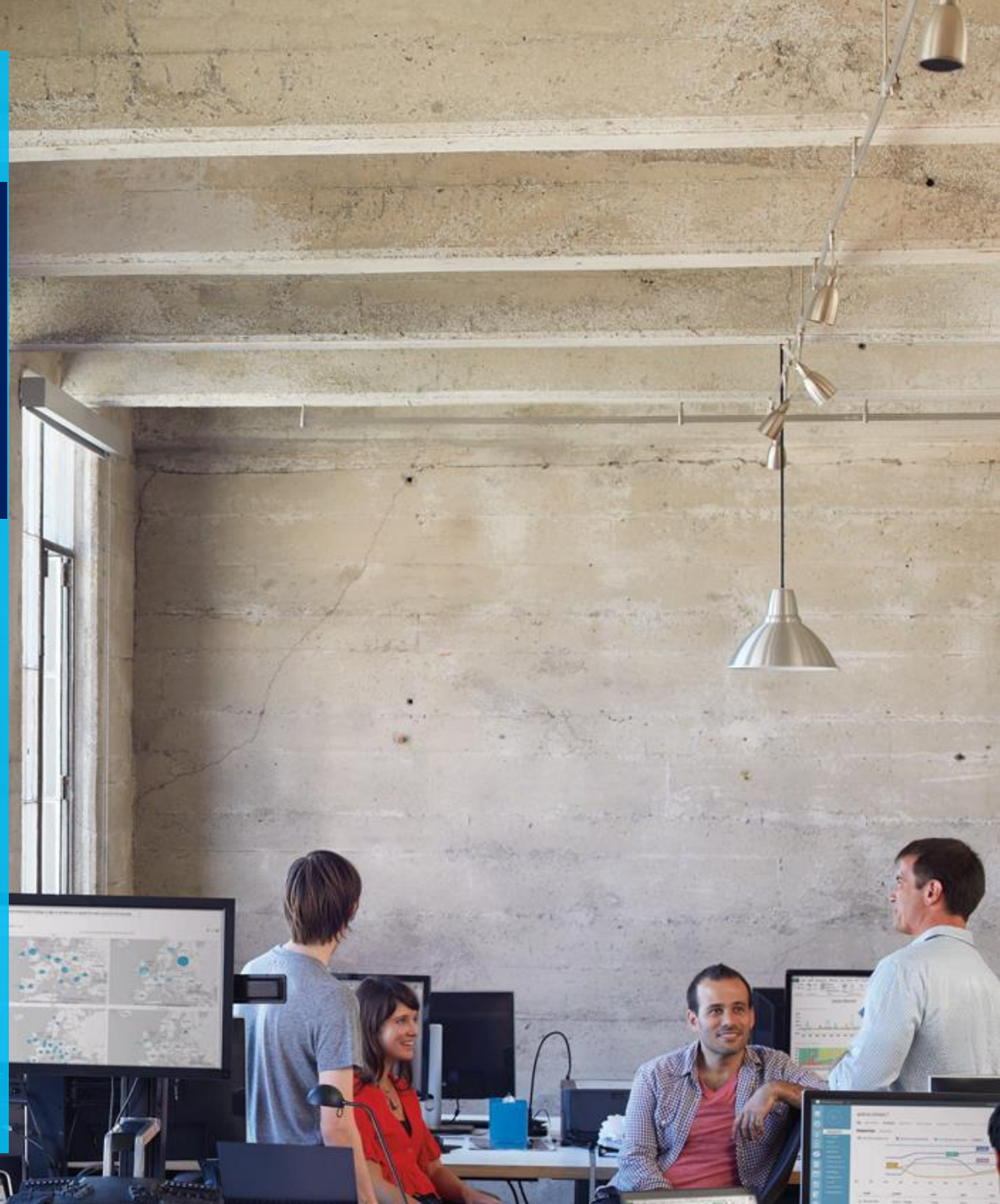
Date: 22nd Nov 2024

Microsoft Azure Power Lunch

Today's Topic:
Network Security Perimeter (Public Preview)

Series website: http://azurepowerlunch.com/

On-Demand Session Information (Recordings) are available here:
Azure Power Lunch YouTube Channel



Naveed Zaheer – Cloud Solution Architect



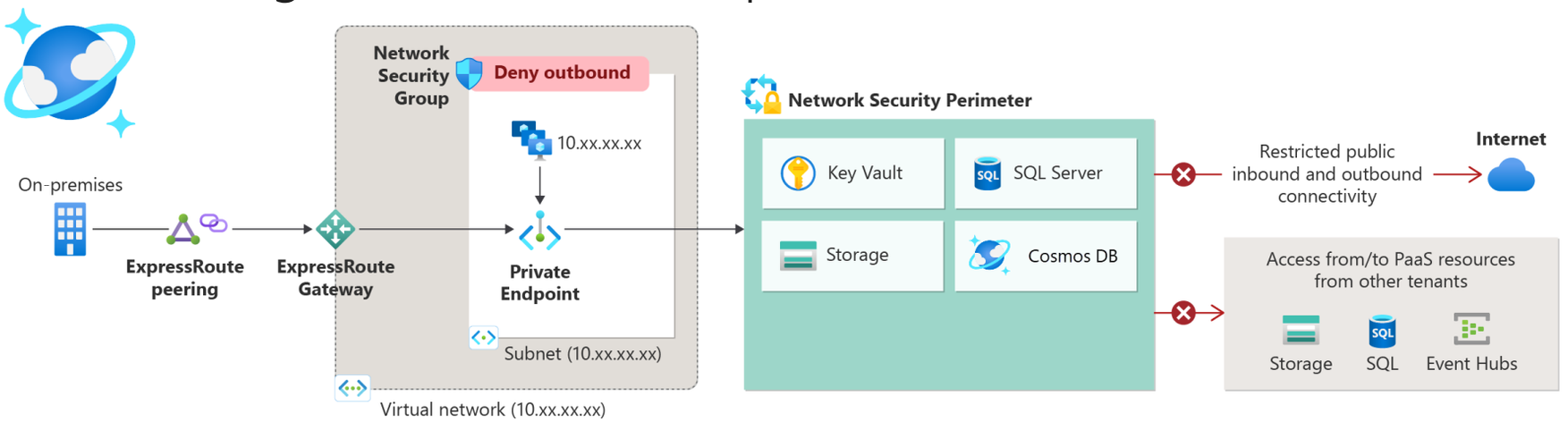
- Been with Microsoft for more than 19 years and in software industry for more than 28 years
- Spent 10+ years with Microsoft Consulting Services in areas such as AppDev, Distributed Applications, SOA and Cloud Applications
- Working with Azure since its inception
- Currently in a Cloud Solution Architect role

Agenda

- What is Network Security Perimeter?
- Network Security Perimeter – Components, Properties and Use Cases
- Demo
- Q & A

What is Network Security Perimeter?

- Allows organizations to define a logical network isolation boundary for PaaS resources that are deployed outside your organization's virtual networks.
- Restricts public network access to PaaS resources outside of the perimeter; access can be exempted by using explicit access rules for public inbound and outbound.
- Control resource to resource access communication within perimeter members, preventing data exfiltration to non-authorized destinations.
- Manages external public access with explicit rules for PaaS resources associated with the perimeter.
- Generate access logs for audit and compliance.



Components of Network Security Perimeter

Component	Description
Network security perimeter	Top level resource defining logical network boundary to secure PaaS resources.
Profile	Collection of access rules that apply on resources associated with the profile.
Access rule	Inbound and outbound rules for resources in a perimeter to allow access outside the perimeter.
Resource association	Perimeter membership for a PaaS resource.
Diagnostics settings	Extension resource hosted by Microsoft Insights to collect logs & metrics for all resources in the perimeter.

Access modes in network security perimeter

Mode	Description
Learning mode	- Default access mode. - Helps network administrators to understand the existing access patterns of their PaaS resources. - Advised mode of use before transitioning to enforced mode.
Enforced mode	- Must be set by the administrator. - By default, all traffic except intra perimeter traffic is denied in this mode unless an Allow access rule exists.

Network Security Perimeter – Common Use Cases

- Create a secure boundary around PaaS resources.
- Prevent data exfiltration by associating PaaS resources to the perimeter.
- Enable access rules to grant access outside the secure perimeter.
- Manage access rules for all the PaaS resources within the network security perimeter in a single pane of glass.
- Enable diagnostic settings to generate access logs of PaaS resources within the perimeter for Audit and Compliance.
- Allow private endpoint traffic without other access rules.

Network Security Perimeter – Access Behavior

Association access mode	Not associated	Learning mode	Enforced mode
Public network access			
Enabled	**Inbound:** Resource rules **Outbound** Allowed	**Inbound:** Network security perimeter + Resource rules **Outbound** Network security perimeter rules + Allowed	**Inbound:** Network security perimeter rules **Outbound** Network security perimeter rules
Disabled	**Inbound:** Denied **Outbound:** Allowed	**Inbound:** Network security perimeter rules **Outbound:** Network security perimeter rules + Allowed	**Inbound:** Network security perimeter rules **Outbound:** Network security perimeter rules
SecuredByPerimeter	**Inbound:** Denied **Outbound:** Denied	**Inbound:** Network security perimeter rules **Outbound:** Network security perimeter rules	- **Inbound:** Network security perimeter rules - **Outbound:** Network security perimeter rules

Network Security Perimeter – Onboarded Resources

Resource Name	Resource type	Resources
Azure Monitor	Microsoft.Insights/dataCollectionEndpoints Microsoft.Insights/ScheduledQueryRules Microsoft.Insights/actionGroups Microsoft.OperationalInsights/workspaces	Log Analytics Workspace, Application Insights, Alerts, Notification Service
Azure AI Search	Microsoft.Search/searchServices	-
Cosmos DB	Microsoft.DocumentDB/databaseAccounts	-
Event Hubs	Microsoft.EventHub/namespaces	-
Key Vault	Microsoft.KeyVault/vaults	-
SQL DB	Microsoft.Sql/servers	-
Storage	Microsoft.Storage/storageAccounts	-

Microsoft

Demo

Resources

- What is Network Security Perimeter?

Q & A