Metodické usmernenie – Azure Firewall a RBAC Template

1. Úvod

Toto metodické usmernenie slúži ako podpora pre správne a jednotné vyplňovanie šablón „Azure Firewall Policy“ a „Azure RBAC Template“, ktoré sa používajú pri návrhu a dokumentácii sieťových a prístupových pravidiel v prostredí Microsoft Azure. Cieľom je zjednotiť správu bezpečnostných nastavení, zvýšiť prehľadnosť a zabezpečiť konzistentný prístup v rámci projektov verejnej správy.

2. Metodika k Azure Firewall Policy

Záznamy v tomto liste popisujú konkrétne pravidlá sieťového prístupu cez firewall. Každé pravidlo musí byť špecifikované detailne a jasne.

2.1 Source IP

Zdrojová IP adresa, rozsah (napr. 10.0.0.1, 10.0.0.0/24) alebo viacero hodnôt oddelených čiarkou.

2.2 Protocol

Typ sieťového protokolu. Možnosti:
- TCP – spoľahlivý protokol (napr. HTTPS, SSH)
- UDP – rýchly protokol, bez zaručenia (napr. DNS, VoIP)
- ICMP – diagnostika (napr. ping)
Nepoužívať hodnotu 'Any'.

2.3 Destination Port

Port alebo portový rozsah (napr. 443, 80, alebo 1000-2000).

2.4 Destination IP/FQDN

Cieľová IP adresa alebo FQDN (napr. mirri.gov.sk). FQDN sa odporúča pri cloudových a dynamických cieľoch.

2.5 RuleType

Typ pravidla – NetworkRule (IP/port), ApplicationRule (FQDN/web služby).

2.6 Action

Definuje akciu – Allow alebo Deny.

2.7 Comment

Poznámka k pravidlu, napr. 'Dočasné', 'Presunúť pod ApplicationRule'.

3. Metodika k Azure RBAC Template

Táto šablóna definuje priradenie rolí používateľom alebo skupinám v rámci prostredia Azure.

3.1 Role

- Owner – úplný prístup
- Contributor – úplný prístup bez správy prístupov
- Reader – len čítanie

Odporúča sa princíp minimálnych oprávnení.

3.2 Email

Pracovný e-mail používateľa alebo skupiny.

3.3 First/Last Name

Meno a priezvisko používateľa na účely identifikácie.

3.4 Company

Organizácia, ku ktorej používateľ patrí (napr. MIRRI, NASES, Dodávateľ).

4. Doplnkové sheety: VPN P2S, VPN S2S

- **VPN P2S (Point-to-Site)**: Evidencia prístupov jednotlivcov do Azure prostredníctvom VPN.
- **VPN S2S (Site-to-Site)**: Zaznamenanie parametrov pre site-to-site VPN spojenia medzi organizáciami.

5. Naming konvencia súborov

Používajte nasledujúcu štruktúru názvu pre každý typ šablóny:

Azure_Firewall_Policy_{OVM}_{projekt}_{date}.xlsx

Azure_RBAC_Template_{OVM}_{projekt}_{date}.xlsx

- {OVM} – skratka organizácie
- {projekt} – názov informačného systému/projektu
- {date} – dátum v tvare YYYYMMDD

6. Záver

Táto metodika pomáha udržať štandardizovaný prístup k sieťovej a prístupovej politike v prostredí Azure. Odporúča sa pravidelná kontrola týchto šablón a ich zosúladenie s bezpečnostnými požiadavkami a audítorskými odporúčaniami.