Virtual Network Peering (version 1.0)

**Cloud Service Label: IaaS**

Description

Adversaries that have established a presence in one virtual network (VPC in AWS) will attempt to explore and access resources in other virtual networks owned by the same organization. By default, individual virtual networks have no routable paths between each other, so it is difficult to access one from another. Both Azure and AWS offer peering capabilities that enable virtual networks to communicate with each other seamlessly. Once peered, routing between the virtual networks is configured in the background and all resources in one virtual network are now reachable by default by the other.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Assigning Network Security Groups | In Azure assigning a Network Security Group (NSG) to subnets within a virtual network will protect all assets within the subnet from other virtual networks regardless of peering. |

Detection

NSG’s have netflow capture capabilities that can log all network connections that are attempted with a subnet. These logs can be saved to a storage account for analysis.

References