Impair Defenses: Disable or Modify Cloud Firewall, Sub-technique T1562.007 - Enterprise

Archived: 2026-04-05 18:00:23 UTC

Adversaries may disable or modify a firewall within a cloud environment to bypass controls that limit access to cloud resources. Cloud firewalls are separate from system firewalls that are described in Disable or Modify System Firewall.

Cloud environments typically utilize restrictive security groups and firewall rules that only allow network activity from trusted IP addresses via expected ports and protocols. An adversary with appropriate permissions may introduce new firewall rules or policies to allow access into a victim cloud environment and/or move laterally from the cloud control plane to the data plane. For example, an adversary may use a script or utility that creates new ingress rules in existing security groups (or creates new security groups entirely) to allow any TCP/IP connectivity to a cloud-hosted instance.[1] They may also remove networking limitations to support traffic associated with malicious activity (such as cryptomining).[2][1]

Modifying or disabling a cloud firewall may enable adversary C2 communications, lateral movement, and/or data exfiltration that would otherwise not be allowed. It may also be used to open up resources for Brute Force or Endpoint Denial of Service.

Source: https://attack.mitre.org/techniques/T1562/007