

## Impair Defenses: Disable or Modify Network Device Firewall, Sub-technique T1562.013 - Enterprise

Archived: 2026-04-05 15:00:21 UTC

Adversaries may disable network device-based firewall mechanisms entirely or add, delete, or modify particular rules in order to bypass controls limiting network usage.

Modifying or disabling a network firewall may enable adversary C2 communications, lateral movement, and/or data exfiltration that would otherwise not be allowed. For example, adversaries may add new network firewall rules to allow access to all internal network subnets without restrictions.<sup>[1]</sup>

Adversaries may gain access to the firewall management console via [Valid Accounts](#) or by exploiting a vulnerability. In some cases, threat actors may target firewalls that have been exposed to the internet [Exploit Public-Facing Application](#).<sup>[2]</sup>

---

Source: <https://attack.mitre.org/techniques/T1562/013>