Unauthorized Network Firewall Rule Modification (T1562.013), Detection Strategy DET0306

Archived: 2026-04-05 17:46:37 UTC

AN0855

Defender observes configuration changes on firewall/network appliance involving rule creation, modification, or deletion from abnormal management IPs or non-console channels (e.g., remote CLI, API). These are often correlated with a spike in previously blocked outbound traffic, unexpected allow-all rules, or bulk rule deletions. Behavior often follows unauthorized login, privilege escalation, or API abuse.

Log Sources

Mutable Elements

Field	Description
TrustedAdminIPs	Allowlisted IPs/subnets where administrative access is expected (e.g., jump box, VPN mgmt)
ConfigChangeWindow	Expected maintenance window (e.g., 02:00–04:00 UTC) to filter benign changes
RuleScopeThreshold	Number of rules affected or port ranges modified to determine severity
NewUserPrivilegeThreshold	Flag new users making changes without observed privilege elevation path

---