Detection of Disabled or Modified System Firewalls across OS Platforms., Detection Strategy DET0145

Archived: 2026-04-05 13:17:58 UTC

AN0406

Detection of firewall tampering by monitoring processes executing netsh, PowerShell Set-NetFirewallProfile, or sc stop mpssvc. Registry modifications under HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy also indicate adversarial actions.

Log Sources

Mutable Elements

Field	Description
MonitoredCommands	List of admin tools and scripts allowed to legitimately modify firewall settings.
AlertThreshold	Number of firewall rule changes within a time window before triggering alert.

AN0407

Detection of iptables, nftables, or firewalld rule modifications. Correlation of sudden drops in active firewall rules with suspicious processes suggests adversarial evasion.

Log Sources

Mutable Elements

Field	Description
AllowedScripts	Baseline admin scripts allowed to make firewall modifications.

AN0408

Detection of PF firewall rule modifications via pfctl, socketfilterfw, or defaults write to com.apple.alf. Adversaries often disable firewall profiles entirely or whitelist malicious processes.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	macos:unifiedlog	pfctl -d, socketfilterfw --setglobalstate off, or modifications to com.apple.alf

Mutable Elements

Field	Description
PFConfigFiles	Monitor for baseline pf.conf and custom rule file modifications.

AN0409

Detection of firewall changes using esxcli network firewall set or vSphere API modifications. Sudden disabling of firewall rules across management interfaces is a strong adversarial signal.

Log Sources

Mutable Elements

Field	Description
APIMethods	Whitelist of authorized vSphere API methods for firewall configuration.

AN0410

Detection of firewall ACL or rule base changes through CLI (e.g., no access-list, permit any any). Monitor configuration commits from unusual users or sessions.

Log Sources

Mutable Elements

Field	Description
AuthorizedAdmins	List of approved admin accounts allowed to modify firewall ACLs.
