Firewall Disable, Data Component DC0043

Archived: 2026-04-05 17:45:56 UTC

The deactivation, misconfiguration, or complete stoppage of firewall services, either on a host or in a cloud control plane. Such activity may involve turning off firewalls, modifying rules to disable protection, or deleting firewall-related configurations and activity logs. Examples:

- Disabling Host-Based Firewalls: Stopping the Windows Defender Firewall service or using `iptables -F` to flush all rules on a Linux system.
- Cloud Firewall Modification or Deactivation: Modifying or deleting security group rules in AWS or disabling a network firewall in Azure.
- Activity Log Deletion: Writing or deleting entries in Azure Firewall Activity Logs to hide unauthorized firewall changes.
- Temporary Disable for Malicious Operations: Temporarily disabling a firewall to allow malicious files or traffic, then re-enabling it to avoid detection.
- Using Command-Line Tools to Stop Firewalls: Running commands like `Set-NetFirewallProfile -Enabled False on Windows or systemctl stop ufw` on Linux.

This data component can be collected through the following measures:

Cloud Control Plane

- Azure Activity Logs:
  - Enable logging of administrative actions, such as stopping or modifying Azure Firewall configurations.
  - Use Azure Monitor to track specific firewall-related actions, including disabling or rule deletion.
- AWS CloudTrail Logs:
  - Monitor `RevokeSecurityGroupIngress` or `RevokeSecurityGroupEgress` events to detect rule changes in AWS Security Groups.
- Google Cloud Platform Logs:
  - Collect logs from the Firewall Rules resource in Google Cloud Operations Suite to detect rule deletions or modifications.

Host-Level Firewalls

- Windows Firewall Event Logs:
  - Enable logging of firewall state changes:
    - Security Event ID 2004: Firewall service stopped.
    - Security Event ID 2005: Firewall service started.
  - Use Sysmon for process creation events tied to firewall commands or scripts (Sysmon Event ID 1).
- Linux Firewall Logs: Use auditd to track commands like iptables, firewalld, or ufw: `auditctl -a always,exit -F arch=b64 -S execve -k firewall_disable`

- macOS Firewall: Monitor changes to the macOS Application Firewall using the log show command.

Network-Level Monitoring

- IDS/IPS Alerts: Deploy IDS/IPS systems to monitor abnormal traffic flows that could indicate firewall disablement.
- NetFlow Data: Analyze NetFlow or packet capture data for traffic patterns inconsistent with firewall enforcement.

SIEM and CSPM Tools

- SIEM Integration: Use tools like Splunk or QRadar to centralize and analyze firewall disablement events from both hosts and cloud platforms.
- Cloud Security Posture Management (CSPM): Use CSPM solutions to monitor misconfigurations and track deactivation of critical cloud services like firewalls.
