Firewall Rule Modification, Data Component DC0051

Archived: 2026-04-05 16:35:45 UTC

The creation, deletion, or alteration of firewall rules to allow or block specific network traffic. Monitoring changes to these rules is critical for detecting misconfigurations, unauthorized access, or malicious attempts to bypass network protections. Examples:

- Rule Creation: Adding a new rule to allow inbound traffic on port 3389 (RDP).
- Rule Deletion: Deleting a rule that blocks inbound traffic from untrusted IP ranges.
- Rule Modification: Changing a rule to allow traffic from "any" source IP instead of a specific trusted range.
- Audit Log Metadata: Logs indicating "Firewall rule modified by admin@domain.com."
- Platform-Specific Scenarios
    - Azure: Altering rules in an Azure Network Security Group (NSG).
    - AWS: Modifying Security Group rules to allow traffic.
    - Windows: Changes tracked in Security Event Logs (EID 4950 or 4951).

This data component can be collected through the following measures:

Cloud Control Plane

- Azure: Collect rule modification logs from Azure Firewall Activity Logs.
    - Example Command: `az network firewall policy rule-collection-group rule-collection list --policy-name <policy-name>`
- AWS: Use CloudTrail to track `AuthorizeSecurityGroupIngress` or `RevokeSecurityGroupIngress` actions.
  Example: `aws ec2 describe-security-groups`
- Google Cloud: Use gcloud commands to extract firewall rules: `gcloud compute firewall-rules list --format=json`

Host-Based Firewalls

- Windows:
    - Collect events from the Windows Security Event Log (EID 4950: A rule has been modified).
    - Use PowerShell to track rule changes: `Get-NetFirewallRule -PolicyStore PersistentStore`
- Linux:
    - Monitor iptables or nftables rule modifications: `iptables -L -v`
    - Use auditd for real-time monitoring: `auditctl -w /etc/iptables.rules -p wa`
- macOS: Use pfctl to monitor rule changes: `sudo pfctl -sr`

SIEM Integration

- Collect logs from cloud platforms, host systems, and network appliances for centralized monitoring.

API Monitoring

- Monitor API calls for firewall rule modifications.

Source: https://attack.mitre.org/datacomponents/DC0051