Firewall Metadata, Data Component DC0053

Archived: 2026-04-02 11:29:35 UTC

Contextual information about firewalls, including their configurations, policies, status, and other details such as names and associated rules. This metadata provides valuable insights into the operational state and configurations of firewalls, both in cloud control planes and host systems. Examples:

- Firewall Name and Configuration: The name, type, and purpose of a firewall such as "Azure Firewall - Production Environment."
- Policy Details: Capturing firewall policy details, such as "Allow inbound TCP 443 to web servers."
- Firewall Status: Status indicators like "Active," "Disabled," or "Pending Updates."
- Audit Log Metadata: Log entries showing administrative changes, such as "Policy modified by admin@domain.com."
- Rules Associated with Firewalls: Rules specifying source/destination IP ranges, protocols, and ports.
- Tagging Information: Tags like "Environment: Production" or "Owner: NetworkOps."

This data component can be collected through the following measures:

Cloud Control Plane

- Azure: Use Azure Activity Logs and Network Watcher to collect metadata for Azure Firewall.
  - Example: `az network firewall show --name <firewall-name>`
- AWS: Use AWS CloudTrail and describe commands: `aws ec2 describe-security-groups`
- Google Cloud: Use gcloud commands to extract metadata: `gcloud compute firewall-rules list --format=json`

Host-Based Firewalls

- Windows: Use PowerShell to gather metadata: `Get-NetFirewallRule -PolicyStore PersistentStore`
- Linux: Query iptables or nftables rulesets: `iptables -S`
- macOS: Use pfctl to extract metadata: `sudo pfctl -sr`

SIEM Integration

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

API Monitoring

- Monitor API calls for metadata requests. Example (AWS): `Capture DescribeSecurityGroups or DescribeNetworkAcls` calls via CloudTrail.

Endpoint Detection and Response (EDR)

- Use EDR solutions to monitor firewall management tools for configuration changes or queries.

Source: https://attack.mitre.org/datacomponents/DC0053