Detection Strategy for Network Address Translation Traversal, Detection Strategy DET0163

Archived: 2026-04-05 13:58:52 UTC

AN0465

Defenders may observe unauthorized or anomalous changes to NAT configurations, including the addition of new translation rules or modifications to existing ones. Suspicious behaviors include sudden introduction of NAT mappings bridging segmented networks, new port address translation rules that obscure true source IPs, or traffic flows inconsistent with expected network design. Multi-event correlation includes detecting configuration changes on routers/firewalls, followed by traffic traversing unexpected internal/external address pairs.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time correlation window between NAT rule change and unexpected traffic; adjustable to align with change management practices.
AuthorizedNATRules	Whitelist of approved NAT policies and rules; prevents false positives from legitimate operations.
TrafficVolumeThreshold	Threshold for abnormal traffic across NAT; tuned to differentiate testing from large-scale exfiltration or bridging.
InterfaceScope	Specific interfaces or zones monitored for NAT translation; allows tuning for internal vs. external-facing boundaries.