Multi-hop Proxy Behavior via Relay Node Chaining, Onion Routing, and Network Tunneling, Detection Strategy DET0359

Archived: 2026-04-05 17:52:16 UTC

AN1020

Suspicious processes (e.g., Tor clients, relays, unknown binaries) launch with sustained encrypted outbound traffic to known anonymity infrastructure (e.g., Tor, I2P), and may relay to additional internal systems via reverse proxying, ICMP tunneling, or socket forwarding.

Log Sources

Mutable Elements

Field	Description
DomainCategory	Can be tuned to `.onion`, I2P, or suspicious CDN domains.
ProcessParent	Detect known-good vs. abnormal launching binaries (e.g., mshta spawning Tor).
ConnectionDuration	Threshold for persistent connections over known relay ports (e.g., 9050).

AN1021

Tools such as `tor`, `nglite`, `proxychains`, `chisel`, or custom daemons repeatedly initiate outbound sessions to multiple nodes before final destination. This behavior is abnormal for Linux services outside of VPN, monitoring, or CDN relay contexts.

Log Sources

Mutable Elements

Field	Description
ExecutablePath	Match known proxy tools, tuned for environment.
RelayCount	Detect outbound chaining behavior through >2 IPs in short succession.
ProtocolType	Allow filtering by ICMP, TCP/443, UDP for obfuscation channels.

AN1022

LaunchAgents or LaunchDaemons initiate persistent Tor or relay processes that make encrypted outbound connections. May be paired with sandbox bypasses or unsigned executables communicating over SOCKS proxies.

Log Sources

Mutable Elements

Field	Description
LaunchdLabel	Regex for masking patterns in LaunchAgents with proxy behavior.
UnsignedBinary	Allow for exceptions for known unsigned binaries.
SOCKSPortUsage	Monitor local 9050/9150 activity and rerouted system traffic.

AN1023

Outbound encrypted traffic initiated from hypervisor shell or via VM backdoor mechanisms to relays in VPS infrastructure, especially if traversing multiple nodes before reaching Internet destination. Packet captures or firewall logs show non-VM communication paths.

Log Sources

Mutable Elements

Field	Description
HopCount	Threshold on number of IPs contacted in sequence without DNS resolution.
ShellAccess	Flag if relay communication initiated by ESXi shell or unknown VM agent.
VPSIPRange	Filter for known Tor/VPS egress networks.

AN1024

Encrypted traffic or ICMP tunneling from border routers to internal routers or unknown external IPs. Forwarded traffic shows consistent hop-to-hop relaying without matching configured VPN or expected network topology.

Log Sources

Mutable Elements

Field	Description
VPNConfigWhitelist	Define allowed internal router communication paths.
ICMPPayloadEntropy	High entropy ICMP payloads may indicate tunneling activity.

Field	Description
RelayChainSignature	Track known multi-hop pattern signatures or port hopping techniques.

Source: https://attack.mitre.org/detectionstrategies/DET0359#AN1020