Internal Proxy Behavior via Lateral Host-to-Host C2 Relay, Detection Strategy DET0075

Archived: 2026-04-05 15:09:29 UTC

AN0204

Anomalous process (e.g., `rundll32`, `svchost`, `cmd`) initiates connections to internal peer hosts not seen in typical communication baselines, used to proxy or forward traffic internally, often using SMB, RPC, or high ports.

Log Sources

Mutable Elements

Field	Description
InternalConnectionPattern	Tune based on known host-to-host communications that are rare (e.g., workstation-to-workstation).
DestinationPort	Focus on unusual internal traffic on ports like 1080, 8080, 4444, or SMB over non-standard ports.
TimeWindow	Correlate unusual traffic bursts with new process execution.

AN0205

`socat`, `ssh`, `iptables`, or `ncat` invoked from user space or cron jobs to create port forwarding, reverse shells, or inter-host tunnels between compromised Linux systems. Behavior is typically paired with socket activity and high entropy traffic.

Log Sources

Mutable Elements

Field	Description
UserContext	Alert on unexpected users executing inter-host relay tools (e.g., `www-data`, `backup`).
PortRange	Adjust to watch for commonly misused internal TCP/UDP ports.
ProcessPattern	Shell pipelines or wrapped invocations like `bash -c 'socat ...'`

AN0206

Execution of AppleScript or Automator services launching `ssh -L`, `socat`, or `launchctl` items that dynamically reroute traffic from one Mac endpoint to another. LaunchAgents used to establish permanent internal tunnels.

Log Sources

Mutable Elements

Field	Description
LaunchAgentPath	Directory where proxying LaunchDaemons may be dropped, e.g., `/Library/LaunchDaemons/`.
PortBindings	Dynamic port forwards often use ephemeral or non-standard service ports.
AppleScriptUsage	May trigger on less common scripting interfaces for traffic redirection.

AN0207

ESXi shell execution of tools/scripts (`nc`, `socat`, `perl`) relaying network traffic to other internal hosts, especially when initiated by unauthorized users or VMs.

Log Sources

Mutable Elements

Field	Description
CLICommandPattern	Watch for chained shell commands building local-to-local connections.
VMInitiator	Correlate to which VM initiated the traffic tunnel; unexpected VM behavior may be suspicious.
ConnectionDirectionality	Unusual east-west communication patterns among VMs.

AN0208

Configuration of internal NAT or proxy rules that redirect traffic between client segments internally (e.g., site-to-site port forwarding). Often used to relay internal beaconing or move traffic laterally through trust zones.

Log Sources

Mutable Elements

Field	Description
ProxyTarget	Internal subnets or endpoint roles allowed for port forwarding.
ConfigChangeUser	Detect changes made outside scheduled or authorized windows.
FlowThreshold	Volume of data relayed through proxy exceeds historical norms.
