Traffic Signaling (Port-knock / magic-packet → firewall or service activation) – T1205, Detection Strategy DET0524

Archived: 2026-04-05 16:54:31 UTC

AN1448

A remote host sends a short sequence of failed connection attempts (RST/ICMP unreachable) to a set of closed ports. Within a brief window the endpoint (a) adds/enables a firewall rule or (b) a sniffer-backed process begins listening or opens a new socket, after which a successful connection occurs. Also detects Wake-on-LAN magic packets seen on local segment.

Log Sources

Mutable Elements

Field	Description
TimeWindowKnock	Window to correlate knock sequence → rule change → successful connect (e.g., 120s).
PortSequenceMinLen	Minimum number of distinct closed ports hit before success (e.g., 3).
SuspiciousProcesses	List of binaries that commonly toggle firewall/sniff (netsh.exe, powershell.exe, npcapservice.exe, windivert, rawsock tools).
AllowedFirewallChangers	Service accounts or software update agents allowed to change firewall.
WoLAllowedWindows	Maintenance windows when magic packets are expected.

AN1449

Closed-port knock sequence from a remote IP followed by on-host firewall change (iptables/nftables) or daemon starts listening (socket open) and a successful TCP/UDP connect. Optional detection of libpcap/raw-socket sniffers spawning to watch for secret values.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve: Commands altering firewall or enabling listeners (iptables, nft, ufw, firewall-cmd, systemctl start *ssh*/*telnet*, ip route add, tcpdump, tshark)

Data Component	Name	Channel
Network Connection Creation (DC0082)	auditd:SYSCALL	socket/bind: Process binds to a new local port shortly after knock
Network Traffic Flow (DC0078)	NSM:Flow	Knock pattern: multiple REJ/S0 to distinct closed ports then successful connection to service_port
Network Traffic Content (DC0085)	NSM:Flow	Packets with unusual flags or payloads outside established flows (e.g., WoL magic FF×6 + 16×MAC)

Mutable Elements

Field	Description
ServicePort	Port that becomes available post-knock (e.g., 22/8022/2323).
KnockResetRatio	Percentage of failed attempts with RST/ICMP vs SYN/SYN-ACK to qualify as closed-port probing.
ProcessAllowList	Automation expected to touch firewall/daemon configs (config-mgmt agents).

AN1450

Remote knock sequence followed by PF/socketfilterfw rule update or a background process listening on a new port; then a successful TCP session. Also flags WoL magic packets on local segment.

Log Sources

Mutable Elements

Field	Description
PFAnchorPaths	Anchors or conf files monitored for change (/etc/pf.conf, /etc/pf.anchors/*).
DeveloperMode	Reduce noise on dev endpoints compiling or testing PF rules.

AN1451

Crafted ‘synful knock’ patterns toward routers/switches (same src hits interface/broadcast/network address on same port in short order) followed by ACL/telnet/SSH enablement or module change. Detect device image/ACL updates then a new mgmt session.

Log Sources

Mutable Elements

Field	Description
MgmtPortSet	Ports whose sudden enablement should alert (23, 22, 2323, 80/443, 4786).
DeviceRole	Applies different thresholds to core/edge/branch devices.
