Detection Strategy for Protocol Tunneling accross OS platforms., Detection Strategy DET0538

Archived: 2026-04-05 14:46:03 UTC

AN1483

Processes such as plink.exe, ssh.exe, or netsh.exe establishing outbound network connections where traffic patterns show encapsulated protocols (e.g., RDP over SSH). Defender observations include anomalous process-to-network relationships, large asymmetric data flows, and port usage mismatches.

Log Sources

Mutable Elements

Field	Description
AllowedTools	Whitelist legitimate tunneling tools (e.g., used by admins).
DataAsymmetryThreshold	Ratio of sent vs received bytes that indicates tunneling activity.
TimeWindow	Correlate process creation with network connection within N seconds.

AN1484

sshd, socat, or custom binaries initiating port forwarding or encapsulating traffic (e.g., RDP, SMB) through SSH or HTTP. Defender sees abnormal connect/bind syscalls, encrypted traffic on ports typically used for non-encrypted services, and outlier traffic volume patterns.

Log Sources

Mutable Elements

Field	Description
ForwardingFlags	Specific sshd config flags indicating port forwarding.
ProtocolBaseline	Define expected application protocols by port to catch tunneling mismatches.

AN1485

launchd or user-invoked processes (ssh, socat) encapsulating traffic via SSH tunnels, VPN-style tooling, or DNS-over-HTTPS clients. Defender sees outbound TLS traffic with embedded DNS or RDP payloads.

Log Sources

Mutable Elements

Field	Description
ExpectedDoHResolvers	Known legitimate DoH resolvers used in environment.
PayloadEntropyThreshold	Flag excessive randomness in payloads on standard ports.

AN1486

VMware daemons or user processes encapsulating traffic (e.g., guest VMs tunneling via hostd). Defender sees network services inside ESXi creating flows inconsistent with management plane traffic, such as SSH forwarding or DNS-over-HTTPS from management interfaces.

Log Sources

Mutable Elements

Field	Description
ESXiServiceProfiles	Baseline allowed services and expected ports for ESXi management.
