

# Detecting Protocol or Service Impersonation via Anomalous TLS, HTTP Header, and Port Mismatch Correlation, Detection Strategy DET0470

Archived: 2026-04-02 10:55:53 UTC

## AN1294

Untrusted processes creating outbound TLS/HTTPS connections with malformed certificates or header fields, often mismatched with target service behavior. Detects protocol impersonation attempts via traffic metadata analysis and host process lineage.

### Log Sources

### Mutable Elements

Field	Description
IssuerOrgFilter	Organizations in certificate issuer fields to allowlist or monitor.
UserContext	Restrict detection to non-system users or external-facing applications.
HeaderSignatureMatch	Specific HTTP header anomalies or patterns (e.g., missing User-Agent).

## AN1295

Detection of binaries spawning encrypted sessions using OpenSSL or curl to external services with mismatched ports/protocols. Identifies behavior where internal services simulate trusted cloud service traffic patterns.

### Log Sources

### Mutable Elements

Field	Description
ProtocolMatchConfidence	Threshold for header-field mismatch against expected service behavior.
TimeWindow	Correlation window between process spawn and encrypted session.

## AN1296

Unsigned or suspicious applications initiating network traffic claiming to be browser, mail, or cloud clients. Detects impersonation via TLS fingerprint and User-Agent string deviation.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
ParentProcessFilter	Limit detections to children of suspicious binaries.
HeaderAnomalyScore	Threshold for deviation from expected headers (User-Agent, Host).

**AN1297**

ESXi hosts initiating connections from non-standard daemons mimicking HTTP/HTTPS or SNMP traffic, but with irregular payload formats or expired/unsigned TLS certificates.

**Log Sources**

**Mutable Elements**

<b>Field</b>	<b>Description</b>
TLSFingerprintMatch	Allows matching against known-good or known-bad JA3/JA3S hashes.
AllowedServicePorts	Tune for expected network ports per ESXi role.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0470>