目录

简介

当使用TLS通过思科电子邮件安全工具(ESA)时传送电子邮件您能选择进行证书验证使用或者‘验证’或‘托管请验证’选项。 这是一个关键的部分保护电子邮件交付在TLS的，并且知道是重要的此验证如何进行。

什么是证书验证的算法在思科电子邮件安全工具(ESA) ？

实际上有两种算法，一个人的‘验证’选项，并且其他‘托管的验证’选项。 典型地，因为是与方案兼容，一个更加大的种类‘托管的验证’选项推荐。

背景信息

- 此文档根据AsyncOS 8.0.1及以后版本。 AsyncOS以前的版本可能有有些另外行为。
- 除非另外说明，支持通配符匹配
- 每种算法在成功的匹配以后终止，并且随后的检查没有被评估
- CLI命令**tlsverify**的用途‘验证算法’

定义

- CN ：这是公用名称，一部分的证书的主题
- SAN ：这是附属的替代名称分机对X.509。 当使用在本文，我们特别地是指在SAN字段包括的所有DNS名。
- 电子邮件域：这是收件人的电子邮件地址的域部分。 例如，当传送对‘user@example.com’，电子邮件域是‘example.com’时
- MX主机名：这些是电子邮件域的MX记录的主机名
- PTR主机名：这是ESA连接IP地址的DNS PTR查找返回的主机名
- SMTP路由主机名：如果SMTP路由为此目的地配置，这是用于SMTP路由的主机名

托管请验证算法

1. 如果证书包含SAN属性，*只有将*使用这些和CN将忽略。 CN，如果没有在证书的SAN属性只将使用。 这依照RFC 6125。
2. 证书根据电子邮件域核对。

3. 证书根据可能存在的所有SMTP路由主机名核对。
4. 证书根据MX主机名核对。
5. 如果上一个检查都未成功，验证发生故障。

验证算法

1. SAN属性根据电子邮件域核对。
2. CN根据电子邮件域核对。 **注意**：不支持通配符匹配。
3. SAN属性根据PTR主机名核对。
4. 如果上一个检查都未成功，验证发生故障。