# 什么是证书验证的算法在Cisco电子邮件安全工具(ESA)上？

## Contents



## Introduction

当使用TLS通过Cisco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‘验证’或‘主机请验证’选项。 这是获取电子邮件发运的一个关键的部分在TLS，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Cisco电子邮件安全工具(ESA)上？

实际上有两种算法，一个的‘验证’选项，并且其他‘主机的验证’选项。 典型地‘主机的验证’建议使用选项，因为是与方案兼容一个更大的种类。

## 背景信息

- 此文档根据AsyncOS 8.0.1及以后版本。 AsyncOS的以前的版本可能有有些另外工作情况。
- 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 ：这是普通的名字，一部分的认证的主题
- SAN ：这是附属的替代名称扩展名对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：这是接收人的电子邮件地址的域部分。 例如，当传送到‘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：这是主机名-返回由IP地址的DNS PTR查找ESA连接
- SMTP路由主机名：如果SMTP路由为此目的地被配置，这是用于SMTP路由-的主机名

## 主机请验证算法

1. 如果认证包含SAN属性，*只有将*使用这些和CN将被忽略。 CN，如果没有在认证的SAN属性只将使用。 这依照RFC 6125。
2. 认证根据电子邮件域核对。
3. 认证根据可能存在的所有SMTP路由主机名核对。
4. 认证根据MX主机名核对。
5. 如果早先检查都未成功，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。 **Note**:不支持通配符匹配。
3. SAN属性根据PTR主机名核对-。
4. 如果早先检查都未成功，验证发生故障。