Contents

Introduction

When using TLS to deliver email via a Cisco Email Security Appliance (ESA) you can choose to perform certificate verification using either the 'Verify' or 'Hosted Verify' options. This is a crucial part of securing the delivery of emails over TLS, and it is important to know how this verification is performed.

What is the algorithm for certificate verification on the Cisco Email Security Appliance (ESA)?

There are actually two algorithms, one for the 'Verify' option, and the other for the 'Hosted Verify' option. Typically the 'Hosted Verify' option is recommended as it is compatible with a larger variety of scenarios.

Background Information

- This documentation is based on AsyncOS 8.0.1 and later versions. Prior versions of AsyncOS may have somewhat different behavior.
- Unless otherwise specified, wildcard matches are supported
- Each algorithm stops after a successful match and subsequent checks are not evaluated
- The CLI command **tlsverify** uses the 'Verify Algorithm'

Definitions

- CN: This is the Common Name, part of the certificate's subject
- SAN: This is the Subject Alternate Name extension to X.509. When used in this document, we're specifically referring to any DNS names included in the SAN field.
- Email Domain: This is the domain portion of the recipient's email address. For example, when delivering to 'user@example.com', the email domain is 'example.com'
- MX Hostnames: These are the hostnames of the email domain's MX records
- PTR Hostname: This is the hostname returned by a DNS PTR lookup of the IP address the ESA is connecting to
- SMTP Route Hostnames: If an SMTP route is configured for this destination, this is the hostname used in the SMTP route

Hosted Verify Algorithm

1. If the certificate contains SAN attributes, *only* these will be used and the CN will be ignored. The CN will only be used if there are no SAN attributes in the certificate. This conforms to RFC 6125.
2. The certificate is checked against the email domain.
3. The certificate is checked against any SMTP route hostnames that may exist.
4. The certificate is checked against the MX hostname(s).
5. If none of the previous checks have succeeded, the verification fails.

Verify Algorithm

1. SAN attributes are checked against the email domain.
2. The CN is checked against the email domain. **Note**: Wildcard matches are not supported.
3. The SAN attributes are checked against the PTR hostname.
4. If none of the previous checks have succeeded, the verification fails.