Welcher Algorithmus dient zur Zertifikatsverifizierung auf der Cisco E-Mail Security Appliance (ESA)?

Inhalt

Einführung

Wenn Sie mit TLS E-Mails über eine Cisco E-Mail Security Appliance (ESA) versenden, können Sie die Zertifikatsüberprüfung entweder mithilfe der Optionen 'Verify' (Überprüfen) oder 'Hosted Verify' (Gehostete Überprüfung) durchführen. Dies ist ein wichtiger Teil der Absicherung der E-Mail-Zustellung über TLS, und es ist wichtig zu wissen, wie diese Verifizierung durchgeführt wird.

Welcher Algorithmus dient zur Zertifikatsverifizierung auf der Cisco E-Mail Security Appliance (ESA)?

Es gibt tatsächlich zwei Algorithmen, einen für die Option "Überprüfen" und einen für die Option "Gehostete Überprüfung". In der Regel wird die Option "Gehostete Überprüfung" empfohlen, da sie mit einer größeren Anzahl von Szenarien kompatibel ist.

Hintergrundinformationen

- Diese Dokumentation basiert auf AsyncOS 8.0.1 und höheren Versionen. Frühere Versionen von AsyncOS können etwas anderes Verhalten aufweisen.
- Sofern nicht anders angegeben, werden Platzhalterabgleiche unterstützt.
- Jeder Algorithmus wird beendet, nachdem eine erfolgreiche Übereinstimmung gefunden wurde, und die nachfolgenden Prüfungen werden nicht ausgewertet.
- Der CLI-Befehl **tlsverify** verwendet den 'Verify Algorithm'

Definitionen

- KN: Dies ist der Common Name, Teil des Zertifikats.
- SAN: Dies ist die Erweiterung Betreff Alternate Name zu X.509. Bei Verwendung in diesem Dokument beziehen wir uns speziell auf DNS-Namen, die im SAN-Feld enthalten sind.
- E-Mail-Domäne: Dies ist der Domänenteil der E-Mail-Adresse des Empfängers. Bei der

Übermittlung an 'user@example.com' lautet die E-Mail-Domäne beispielsweise 'beispiel.com'.
- MX-Hostnamen: Dies sind die Hostnamen der MX-Datensätze der E-Mail-Domäne.
- PTR-Hostname: Dies ist der Hostname, der von einer DNS-PTR-Suche der IP-Adresse zurückgegeben wird, mit der die ESA eine Verbindung herstellt.
- SMTP-Routen-Hostnamen: Wenn für dieses Ziel eine SMTP-Route konfiguriert ist, ist dies der Hostname, der für die SMTP-Route verwendet wird.

Hosted Verification-Algorithmus

1. Wenn das Zertifikat SAN-Attribute enthält, werden *nur* diese verwendet, und die CN wird ignoriert. Die CN wird nur verwendet, wenn das Zertifikat keine SAN-Attribute enthält. Dies entspricht RFC 6125.
2. Das Zertifikat wird mit der E-Mail-Domäne abgeglichen.
3. Das Zertifikat wird mit allen Hostnamen für SMTP-Routen abgeglichen, die vorhanden sein können.
4. Das Zertifikat wird mit dem/den MX-Hostnamen(n) abgeglichen.
5. Wenn keine der vorherigen Prüfungen erfolgreich durchgeführt wurde, schlägt die Überprüfung fehl.

Algorithmus überprüfen

1. SAN-Attribute werden mit der E-Mail-Domäne abgeglichen.
2. Der CN wird mit der E-Mail-Domäne abgeglichen. **Hinweis**: Wildcard-Übereinstimmungen werden nicht unterstützt.
3. Die SAN-Attribute werden mit dem PTR-Hostnamen abgeglichen.
4. Wenn keine der vorherigen Prüfungen erfolgreich durchgeführt wurde, schlägt die Überprüfung fehl.