Qual è l'algoritmo per la verifica dei certificati su Cisco Email Security Appliance (ESA)?

Sommario

Introduzione

Quando si utilizza TLS per recapitare la posta elettronica tramite Cisco Email Security Appliance (ESA), è possibile scegliere di eseguire la verifica del certificato utilizzando le opzioni 'Verifica' o 'Verifica ospitata'. Si tratta di una parte fondamentale per garantire la consegna delle e-mail tramite TLS ed è importante sapere come viene eseguita questa verifica.

Qual è l'algoritmo per la verifica dei certificati su Cisco Email Security Appliance (ESA)?

In realtà sono disponibili due algoritmi, uno per l'opzione 'Verifica' e l'altro per l'opzione 'Verifica ospitata'. In genere è consigliabile utilizzare l'opzione 'Hosted Verify', in quanto compatibile con una più ampia varietà di scenari.

Premesse

- Questa documentazione è basata su AsyncOS 8.0.1 e versioni successive. Le versioni precedenti di AsyncOS potrebbero avere un comportamento diverso.
- Se non diversamente specificato, sono supportate le corrispondenze con caratteri jolly
- Ogni algoritmo si arresta dopo una corrispondenza riuscita e i controlli successivi non vengono valutati
- Il comando CLI **tlsverify** usa l'algoritmo 'Verify'

Definizioni

- CN: Nome comune, parte dell'oggetto del certificato
- SAN: Estensione del nome soggetto alternativo a X.509. In questo documento si fa specifico riferimento a qualsiasi nome DNS incluso nel campo SAN.
- Dominio e-mail: Parte del dominio dell'indirizzo e-mail del destinatario. Ad esempio, per il recapito a 'user@example.com', il dominio e-mail è 'example.com'
- Nomi host MX: Questi sono i nomi host dei record MX del dominio e-mail

- Nome host PTR: Nome host restituito da una ricerca PTR DNS dell'indirizzo IP a cui si connette l'ESA
- Nomi host route SMTP: Se per la destinazione è configurata una route SMTP, si tratta del nome host utilizzato nella route SMTP

Algoritmo di verifica ospitato

1. Se il certificato contiene attributi SAN, verranno utilizzati *solo* questi e la CN verrà ignorata. La CN verrà utilizzata solo se nel certificato non sono presenti attributi SAN. È conforme alla RFC 6125.
2. Il certificato viene confrontato con il dominio di posta elettronica.
3. Il certificato viene confrontato con qualsiasi nome host di route SMTP esistente.
4. Il certificato viene confrontato con i nomi host MX.
5. Se nessuno dei controlli precedenti ha avuto esito positivo, la verifica ha esito negativo.

Verifica algoritmo

1. Gli attributi SAN vengono confrontati con il dominio e-mail.
2. La CN viene confrontata con il dominio e-mail. **Nota:** Le corrispondenze con caratteri jolly non sono supportate.
3. Gli attributi SAN vengono confrontati con il nome host PTR.
4. Se nessuno dei controlli precedenti ha avuto esito positivo, la verifica ha esito negativo.