Wat is het algoritme voor certificaatverificatie op Cisco e-mail security applicatie (ESA)?

Inhoud

Inleiding

Wanneer u TLS gebruikt om e-mail te verzenden via een Cisco e-mail security applicatie (ESA), kunt u ervoor kiezen om certificatie uit te voeren met behulp van de opties 'Verifiëren' of 'Hosted verify'. Dit is van cruciaal belang om de levering van e-mails via TLS te waarborgen en het is belangrijk te weten hoe deze verificatie wordt uitgevoerd.

Wat is het algoritme voor certificaatverificatie op Cisco e-mail security applicatie (ESA)?

Er bestaan eigenlijk twee algoritmen, één voor de optie 'Verifiëren' en één voor de optie 'Hosted verify'. Meestal wordt de optie 'Hosted verify' aanbevolen, omdat deze compatibel is met een groter aantal scenario's.

Achtergrondinformatie

- Deze documentatie is gebaseerd op AsyncOS 8.0.1 en latere versies. Eerdere versies van AsyncOS kunnen enigszins verschillend gedrag hebben.
- Tenzij anders gespecificeerd worden overeenkomsten met jokerteken ondersteund
- Elk algoritme stopt na een succesvolle match en de daaropvolgende controles zijn niet geëvalueerd
- De CLI-opdracht **tlsverify** gebruikt het 'verify-algoritme'

Definities

- GN: Dit is de gewone naam, een deel van het certificaat
- SAN: Dit is de Onderwerp Alternate Name extensie tot X.509. Wanneer gebruikt in dit document, verwijzen we specifiek naar DNS-namen die in het SAN-veld staan.
- E-maildomein: Dit is het domeingedeelte van het e-mailadres van de ontvanger. Bijvoorbeeld wanneer het aanbieden aan 'user@example.com', is het e-maildomein 'voorbeeld.com'
- MX Hostname: Dit zijn de hostnamen van de MX records van het e-maildomein

- PTR Hostname: Dit is de hostname die wordt teruggegeven door een DNS PTR-raadpleging van het IP-adres waarop het ESA een verbinding maakt
- MTP-routeswitchnamen: Als een route wordt gevormd voor deze bestemming, is dit de hostname die in de route mtp wordt gebruikt

Hosted verify-algoritme

1. Indien het certificaat SAN-eigenschappen bevat, worden *alleen* deze gebruikt en wordt de GN genegeerd. De GN wordt alleen gebruikt indien het certificaat geen SAN-eigenschappen bevat. Dit komt overeen met RFC 6125.
2. Het certificaat wordt afgevinkt tegen het e-maildomein.
3. Het certificaat wordt afgevinkt tegen elke mogelijke naam van een smTP-route.
4. Het certificaat wordt gecontroleerd aan de hand van de MX hostname(en).
5. Als geen van de vorige controles is geslaagd, is de verificatie mislukt.

Algoritme controleren

1. SAN-eigenschappen worden afgevinkt tegen het e-maildomein.
2. De GN wordt gecontroleerd aan de hand van het e-maildomein. Opmerking: Wildkaartovereenkomsten worden niet ondersteund.
3. De SAN eigenschappen worden afgevinkt tegen de PTR hostname.
4. Als geen van de vorige controles is geslaagd, is de verificatie mislukt.