Quel est l'algorithme pour la vérification de certificat sur l'appliance de sécurité du courrier électronique de Cisco (ESA) ?

Contenu

Introduction

En employant le TLS pour fournir l'email par l'intermédiaire d'une appliance de sécurité du courrier électronique de Cisco (ESA) vous pouvez choisir d'exécuter la vérification de certificat utilisant ou « vérifiez » ou « a hébergé vérifient » des options. C'est une partie cruciale de sécuriser la livraison des emails au-dessus du TLS, et il est important de savoir cette vérification est exécutée.

Quel est l'algorithme pour la vérification de certificat sur l'appliance de sécurité du courrier électronique de Cisco (ESA) ?

Il y a réellement deux algorithmes, on pour « vérifient » l'option, et l'autre pour le « hébergé vérifient » l'option. Typiquement « a hébergé vérifient » l'option est recommandé car elle est compatible avec une plus grande variété de scénarios.

Informations générales

- Cette documentation est basée sur AsyncOS 8.0.1 et versions ultérieures. Les versions antérieures d'AsyncOS peuvent avoir le comportement quelque peu différent.
- Sauf indication contraire, des correspondances de masque sont prises en charge
- Chaque algorithme arrête après une concordance réussie et des contrôles ultérieurs ne sont pas évalués
- La commande CLI **tlsverify des** utilisations « vérifient l'algorithme »

Définitions

- NC : C'est le nom commun, une partie du sujet du certificat
- SAN : C'est l'extension soumise de nom secondaire à X.509. Une fois utilisés dans ce document, nous nous référons spécifiquement à tous les noms DNS inclus dans le SAN mettons en place.

- Domaine d'email : C'est la partie de domaine de l'adresse e-mail du destinataire. Par exemple, en livrant à « user@example.com », le domaine d'email est « example.com »
- Adresses Internet MX : Ce sont les adresses Internet des enregistrements MX du domaine d'email
- Adresse Internet PTR : C'est l'adresse Internet retournée par une consultation PTR de DN de l'adresse IP que l'ESA connecte à
- Adresses Internet d'artère de SMTP : Si une artère de SMTP est configurée pour cette destination, c'est l'adresse Internet utilisée dans l'artère de SMTP

Hébergé vérifiez l'algorithme

1. Si le certificat contient des attributs SAN, *seulement* ceux-ci seront utilisés et la NC sera ignorée. La NC sera seulement utilisée s'il n'y a aucun attribut SAN dans le certificat. Ceci se conforme à RFC 6125.
2. Le certificat est vérifié contre le domaine d'email.
3. Le certificat est vérifié contre toutes les adresses Internet d'artère de SMTP qui peuvent exister.
4. Le certificat est vérifié contre les noms d'hôte MX.
5. Si aucun des contrôles précédents n'a réussi, la vérification échoue.

Vérifiez l'algorithme

1. Des attributs SAN sont vérifiés contre le domaine d'email.
2. La NC est vérifiée contre le domaine d'email. Remarque: Des correspondances de masque ne sont pas prises en charge.
3. Les attributs SAN sont vérifiés contre l'adresse Internet PTR.
4. Si aucun des contrôles précédents n'a réussi, la vérification échoue.