Utilisant TLSVERIFY pour dépanner des questions de la livraison de TLS

Contenu

Introduction

Ce document décrit comment employer TLSVERIFY pour dépanner des questions de la livraison de TLS.

Par rapport à la messagerie traitant sur l'appliance de sécurité du courrier électronique de Cisco (ESA), vous pouvez voir que le TLS est ne fournissant pas ou renvoyant l'erreur ou l'alerte.

Du CLI sur l'appliance, l'utilisation **tlsverify** pour tester la transmission de TLS de votre appliance au domaine externe.

```
mail3.example.com> tlsverify

Enter the TLS domain to verify against:
[]> example.com

Enter the destination host to connect to. Append the port
(example.com:26) if you are not connecting on port 25:
[example.com]> mxe.example.com:25

Connecting to 1.1.1.1 on port 25.
Connected to 1.1.1.1 from interface 10.10.10.10.
Checking TLS connection.
TLS connection established: protocol TLSv1, cipher RC4-SHA.
Verifying peer certificate.
Verifying certificate common name mxe.example.com.
TLS certificate match mxe.example.com
TLS certificate verified.
TLS connection to 1.1.1.1 succeeded.

TLS successfully connected to mxe.example.com.
TLS verification completed.
```

La sortie ci-dessus de **tlsverify la** vérification de TLS d'expositions de commande de cette appliance à la destination avec l'adresse IP 1.1.1.1.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur

- Support et documentation techniques - Cisco Systems