

Usando TLSVERIFY para resolver problemas los problemas de la salida de TLS

Contenido

[Introducción](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo utilizar TLSVERIFY para resolver problemas los problemas de la salida de TLS.

En relación con el correo que procesa en el dispositivo de seguridad del correo electrónico de Cisco (ESA), usted puede ver que TLS es de entrega o de vuelta del error o de la alerta.

Del CLI en el dispositivo, el uso **tlsverify** para probar la comunicación de TLS de su dispositivo al dominio externo.

```
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]> mx.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 mx.example.com.
```

```
TLS certificate match mx.example.com
```

```
TLS certificate verified.
```

```
TLS connection to 1.1.1.1 succeeded.
```

```
TLS successfully connected to mx.example.com.
```

```
TLS verification completed.
```

La salida antedicha de **tlsverify** la verificación de TLS de las demostraciones del comando de este dispositivo al destino con la dirección IP 1.1.1.1.

Información Relacionada

- [Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)