Using TLSVERIFY to Troubleshoot TLS Delivery Issues

Document ID: 118581

Contributed by Cisco TAC Engineers.

Oct 14, 2014

Contents

Introduction

This document describes how to use TLSVERIFY to troubleshoot TLS delivery issues.

In relation to mail processing on the Cisco Email Security Appliance (ESA), you may see that TLS is not delivering or returning error or alert.

From the CLI on the appliance, use ***tlsverify*** to test TLS communication from your appliance to the external domain.

```
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.
```

The above output from ***tlsverify*** command shows TLS verification from this appliance to the destination with IP address 1.1.1.1.

Related Information

- ***Cisco Email Security Appliance − End−User Guides***
- ***Technical Support & Documentation − Cisco Systems***