Determine if ESA is Using TLS for Delivery or Receiving

TAC **Document ID: 118500**

Contributed by Nasir Shakour and Robert Sherwin, Cisco TAC Engineers.

Oct 14, 2014

Contents

Introduction

This document describes how to determine if Transport Layer Security (TLS) is used for delivery or receiving on the Cisco Email Security Appliance (ESA).

Determine if ESA is Using TLS for Delivery or Receiving

TLS is an improved version of the Secure Socket Layer (SSL) technology. It is a widely−used mechanism for encrypting SMTP conversations over the Internet.

The ESA can establish connections to remote hosts using TLS or require TLS when remote hosts establish connections. TLS connections are recorded in the mail logs along with other significant actions related to messages such as filter actions, anti−virus and anti−spam verdicts, and delivery attempts. If there is a successful TLS connection, there will be a "TLS success" entry in the mail logs. Likewise, a failed TLS connection will produce a "TLS failed" entry. If a message does not have an associated TLS entry in the log file, that message was not delivered over a TLS connection.

Below are examples of successful and failed TLS connections. You are able to see the log entries from review of message tracking on the GUI, or using ***grep*** to parse the mail logs on the CLI. Please review the ESA Message Disposition Determination article for further assistance.

Successful TLS connection from remote host (Receiving):

```
Wed Jul 20 19:47:40 2005 Info: New smtp ICID 282204970 interface Management
(10.10.10.1) address 192.168.1.1 reverse dns host unknown verified no
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 ACCEPT SG None match  SBRS None
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 TLS success
Wed Jul 20 19:47:40 2005 Info: Start MID 200257070 ICID 282204970
```

Failed TLS connection from remote host (Receiving):

```
Tue Jun 28 19:08:49 2005 Info: New SMTP ICID 282204971 interface Management
(10.10.10.1) address 192.168.1.1 reverse dns host unknown verified no
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 ACCEPT SG None match  SBRS None
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS failed
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 lost
```

```
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS was required but remote host
did not initiate it
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 close
```

Successful TLS connection to remote host (Delivery):

```
Tue Jun 28 19:28:31 2005 Info: DCID 2386069 TLS success CN: <common>
Tue Jun 28 19:28:31 2005 Info: New SMTP DCID 2386069 interface 10.10.10.2
address 192.168.2.2
Tue Jun 28 19:28:31 2005 Info: Delivery start DCID 2386069 MID 200257075 to RID [0]
```

Failed TLS connection to remote host (Delivery):

```
Fri Jul 22 22:00:05 2005 Info: DCID 2386070 IP 192.168.2.2 TLS failed: STARTTLS
unexpected response
```

Related Information

- ***ESA Message Disposition Determination***
- ***Cisco Email Security Appliance − End−User Guides***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Oct 14, 2014 Document ID: 118500