Create Certificates Setup Guide for TLS on ESA

Contents

Introduction

This document describes how to create a certificate for use with TLS, activate inbound / outbound TLS, and troubleshoot issues on the Cisco ESA.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The TLS implementation on the ESA provides privacy for point-to-point transmission of emails through encryption. It allows an administrator to import a certificate and private key from a Certificate Authority (CA) service, or use a self-signed certificate.

Cisco AsyncOS for Email Security supports the **STARTTLS** extension to Simple Mail Transfer Protocol (SMTP) (**Secure SMTP over TLS**).

Tip: For more information about TLS, refer to RFC 3207.

Note: This document describes how to install certificates at the cluster level with the use of the *Centralized Management* feature on the ESA. Certificates can be applied at the machine level as well; however, if the machine is ever removed from the cluster and then added back, the machine-level certificates are lost.

Functional Overview and Requirements

An administrator wants to create a self-signed certificate on the appliance for any of these reasons:

- In order to encrypt the SMTP conversations with other MTAs that use TLS (both inbound and outbound conversations).
- In order to enable the HTTPS service on the appliance for access to the GUI via HTTPS.
- For use as a client certificate for Lightweight Directory Access Protocols (LDAPs), if the LDAP server requires a client certificate.
- In order to allow secure communication between the appliance and the Rivest-Shamir-Addleman (RSA) Enterprise Manager for Data Loss Protection (DLP).
- In order to allow secure communication between the appliance and a Cisco Advanced Malware Protection (AMP) Threat Grid Appliance.

The ESA comes preconfigured with a demonstration certificate that can be used in order to establish TLS connections.

Caution: While the demonstration certificate is sufficient for the establishment of a secure TLS connection, be aware that it cannot offer a verifiable connection.

Cisco recommends that you obtain an X.509, or Privacy Enhanced Email (PEM) certificate from a CA. This is also referred to as an *Apache* certificate. The certificate from a CA is desirable over the self-signed certificate because a self-signed certificate is similar to the previously mentioned demonstration certificate, which cannot offer a verifiable connection.

Note: The PEM certificate format is further defined in RFC 1421 through RFC 1424. The PEM is a container format that can include only the public certificate (such as with Apache installs and CA certificate files */etc/ssl/certs*) or an entire certificate chain, to include public key, private key, and root certificates. The name *PEM* is from a failed method for secure email, but the container format that it used is still active and is a base-64 translation of the X.509 ASN.1 keys.

Bring Your Own Certificate

The option to import your own certificate is available on the ESA; however, the requirement is that the certificate be in PKCS#12 format. This format includes the private key. Administrators do not often have certificates that are available in this format. For this reason, Cisco recommends that you generate the certificate on the ESA and have it properly signed by a CA.

Update a Current Certificate

If a certificate that already exists has expired, skip the *Deploying Self-Signed Certificates* section of this document and re-sign the certificate that exists.

Tip: Refer to the Renew a Certificate on an Email Security Appliance Cisco document for more details.

Deploy Self-Signed Certificates

This section describes how to generate a self-signed certificate and Certificate Signing Request (CSR), provide the self-signed certificate to a CA for signing, upload the signed certificate to the ESA, specify the certificate for use with the ESA services, and back up the appliance configuration and certificate(s).

Generate a Self-Signed Certificate and CSR

To create a self-signed certificate via the CLI, enter the **certconfig** command.

To create a self-signed certificate from the GUI:

1. Navigate to **Network > Certificates > Add Certificate** from the appliance GUI.
2. Click the **Create Self-Signed Certificate** drop-down menu.

   When you create the certificate, ensure that the *Common Name* matches the hostname of the listening interface, or that it matches the hostname of the delivery interface.
   - The *listening* interface is the interface that is linked to the listener that is configured under **Network > Listeners**.
   - The *delivery* interface is automatically selected, unless explicitly configured from the CLI with the **deliveryconfig** command.
3. For a verifiable inbound connection, validate that these three items match:

- MX record (Domain Name System (DNS) hostname)
- Common Name
- Interface hostname

Note: The system hostname does not affect the TLS connections in regards to being verifiable. The system hostname is shown in the top-right corner of the appliance GUI, or from the CLI **sethostname** command output.

Caution: Remember to **submit** and **commit** your changes before you export the CSR. If these steps are not completed, the new certificate is not committed to the appliance configuration, and the signed certificate from the CA cannot sign, or be applied to, a certificate that already exists.

Provide the Self-Signed Certificate to a CA

To submit the self-signed certificate to a CA for signing:

1. Save the CSR to a local computer in PEM format **Network > Certificates > Certificate Name > Download Certificate Signing Request**.
2. Send the generated certificate to a recognized CA for signing.
3. Request an X.509/PEM/Apache formatted certificate, as well as the intermediate certificate.

The CA then generates a certificate in PEM format.

Note: For a list of CA providers, refer to the Certificate authority Wikipedia article.

Upload the Signed Certificate to the ESA

After the CA returns the trusted public certificate that is signed by a private key, upload the signed certificate to the ESA.

The certificate can then be used with a public or private listener, an IP interface HTTPS service, the LDAP interface, or all outbound TLS connections to the destination domains.

To upload the signed certificate to the ESA:

1. Ensure that the trusted public certificate that is received uses PEM format, or a format that can be converted to PEM before you upload it to the appliance.

   Tip: You can use the OpenSSL toolkit, a free software program, in order to convert the format.

2. Upload the signed certificate:

   a. Navigate to **Network > Certificates**.

   b. Click the name of the certificate that was sent to the CA for signing.

c. Enter the path to the file on the local machine or network volume.

Note: When you upload the new certificate, it overwrites the current certificate. An intermediate certificate that is related to the self-signed certificate can also be uploaded.

Caution: Remember to **submit** and **commit** the changes after you upload the signed certificate.

Specify the Certificate for Use with ESA Services

Now that the certificate is created, signed, and uploaded to the ESA, it can be used for the services that require certificate usage.

Inbound TLS

Complete these steps in order to use the certificate for the inbound TLS services:

1. Navigate to **Network > Listeners**.
2. Click the listener name.
3. Select the certificate name from the *Certificate* drop-down menu.
4. Click **Submit**.
5. Repeat Steps 1 through 4 as needed for any additional listeners.
6. **Commit** the changes.

Outbound TLS

Complete these steps in order to use the certificate for the outbound TLS services:

1. Navigate to **Mail Policies > Destination Controls**.
2. Click **Edit Global Settings...** in the *Global Settings* section.
3. Select the certificate name from the *Certificate* drop-down menu.
4. Click **Submit**.
5. **Commit** the changes.

HTTPS

Complete these steps in order to use the certificate for the HTTPS services:

1. Navigate to **Network > IP Interfaces**.
2. Click the interface name.
3. Select the certificate name from the *HTTPS Certificate* drop-down menu.

4. Click **Submit**.
5. Repeat Steps 1 through 4 as needed for any additional interfaces.
6. **Commit** the changes.

LDAPs

Complete these steps in order to use the certificate for the LDAPs:

1. Navigate to **System Administration > LDAP**.
2. Click **Edit Settings...** in the *LDAP Global Settings* section.
3. Select the certificate name from the *Certificate* drop-down menu.
4. Click **Submit**.
5. **Commit** the changes.

URL Filtering

To use the certificate for URL filtering:

1. Enter the **websecurityconfig** command into the CLI.
2. Proceed through the command prompts. Ensure that you select **Y** when you reach this prompt:

```
Do you want to set client certificate for Cisco Web Security Services Authentication?
```

3. Select the number that is associated with the certificate.
4. Enter the **commit** command in order to commit the configuration changes.

Back Up the Appliance Configuration and Certificate(s)

Ensure that the appliance configuration is saved at this time. The appliance configuration contains the completed certificate work that has been applied via the previously described processes.

Complete these steps in order to save the appliance configuration file:

1. Navigate to **System Administration > Configuration File > Download file to local computer to view or save**.
2. Export the certificate:
    a. Navigate to **Network > Certificates**.
    b. Click **Export Certificate**.

c. Select the certificate to export.

d. Enter the file name of the certificate.

e. Enter a password for the certificate file.

f. Click **Export**.

g. Save the file to a local or network machine.

h. Additional certificates can be exported at this time, or click **Cancel** in order to return to the **Network > Certificates** location.

Note: This process saves the certificate in PKCS#12 format, which creates and saves the file with password protection.

Activate Inbound TLS

In order to activate TLS for all inbound sessions, connect to the web GUI, choose **Mail Policies > Mail Flow Policies** for the configured inbound listener, and then complete these steps:

1. Choose a listener for which the policies must be modified.

2. Click the link for the name of the policy in order to edit it.

3. In the *Security Features* section, choose one of these *Encryption and Authentication* options in order to set the level of TLS that is required for that listener and mail flow policy:

   - **Off** – When this option is chosen, TLS is not used.

   - **Preferred** – When this option is chosen, TLS can negotiate from the remote MTA to the ESA. However, if the remote MTA does not negotiate (prior to the reception of a *220* response), the SMTP transaction continues *in the clear* (not encrypted). No attempt is made in order to verify whether the certificate originates from a trusted certificate authority. If an error occurs after the 220 response is received, then the SMTP transaction does not fall back to clear text.

   - **Required** – When this option is chosen, TLS can be negotiated from the remote MTA to the ESA. No attempt is made in order to verify the certificate of the domain. If the negotiation fails, no email is sent through the connection. If the negotiation succeeds, then the mail is delivered via an encrypted session.

4. Click **Submit**.

5. Click the **Commit Changes** button. You can add an optional comment at this time, if desired.

6. Click **Commit Changes** in order to save the changes.

The mail flow policy for the listener is now updated with the TLS settings that you have chosen.

Complete these steps in order to activate TLS for inbound sessions that arrive from a select set of domains:

1. Connect to the web GUI and choose **Mail Policies > HAT Overview**.

2. Add the sender(s) IP/FQDN to the appropriate Sender Group.
3. Edit the TLS settings of the mail flow policy that is associated with the Sender Group that you modified in the previous step.
4. Click **Submit**.
5. Click the **Commit Changes** button. You can add an optional comment at this time, if desired.
6. Click **Commit Changes** in order to save the changes.

The mail flow policy for the Sender Group is now updated with the TLS settings that you have chosen.

Tip: Refer to this article for further information on how the ESA handles TLS verification : What is the algorithm for certificate verification on the ESA?

Activate Outbound TLS

In order to activate TLS for outbound sessions, connect to the web GUI, choose **Mail Policies** > **Destination Controls**, and then complete these steps:

1. Click **Add Destination...**.
2. Add the destination domain.
3. In the *TLS Support* section, click the drop-down menu and choose one of these options in order to enable the type of TLS that is to be configured:
    - **None** – When this option is chosen, TLS is not negotiated for outbound connections from the interface to the MTA for the domain.
    - **Preferred** – When this option is chosen, TLS is negotiated from the email gateway interface to the MTA(s) for the domain. However, if the TLS negotiation fails (prior to receiving a 220 response), the SMTP transaction does not fall back to clear text. No attempt is made to verify if the certificate originates from a trusted certificate authority. If an error occurs and the TLS negotiation fails after the 220 response is received, the SMTP transaction can continue "in the clear" (not encrypted).
    - **Required** – When this option is chosen, TLS is negotiated from the ESA interface to MTA(s) for the domain. No attempt is made in order to verify the certificate of the domain. If the negotiation fails, no email is sent through the connection. If the negotiation succeeds, then the mail is delivered via an encrypted session.
    - **Preferred-Verify** – When this option is chosen, TLS is negotiated from the ESA to the MTA(s) for the domain, and the appliance attempts to verify the domain certificate. In this case, these three outcomes are possible:
        - The TLS is negotiated and the certificate is verified. The mail is delivered via an encrypted session.
        - The TLS is negotiated, but the certificate is not verified. The mail is delivered via an encrypted session.

        - No TLS connection is made, and the certificate is not verified. The email message is delivered in plain text.
    - **Required-Verify** – When this option is chosen, TLS is negotiated from the ESA to the MTA(s) for the domain, and verification of the domain certificate is required. In this case, these three outcomes are possible:
        - A TLS connection is negotiated, and the certificate is verified. The email message is delivered via an encrypted session.
        - A TLS connection is negotiated, but the certificate is not verified by a trusted CA. The mail is not delivered.
        - A TLS connection is not negotiated, but the mail is not delivered.
4. Make any further changes that are needed to the *Destination Controls* for the destination domain.
5. Click **Submit**.
6. Click the **Commit Changes** button. You can add an optional comment at this time, if desired.
7. Click **Commit Changes** in order to save the changes.

ESA Certificate Misconfiguration Symptoms

TLS works with a self-signed certificate, however if TLS verification is required by the sender, a CA signed certificate would need to be installed.

TLS Verification can fail even though a CA signed certificate was installed on the ESA.

In these cases, it is recommended to verify the certicate via the steps in the Verify section.

Verify

Verify TLS with a Web Browser

In order to verify the CA signed certificate, apply the certificate to the ESA GUI HTTPS service.

Then, navigate to the GUI of your ESA in your web browser. If there are warnings when you navigate to https://youresa, then the certificate is likely improperly chained, like missing an intermediate certificate.

Verify TLS with Third-Party Tools

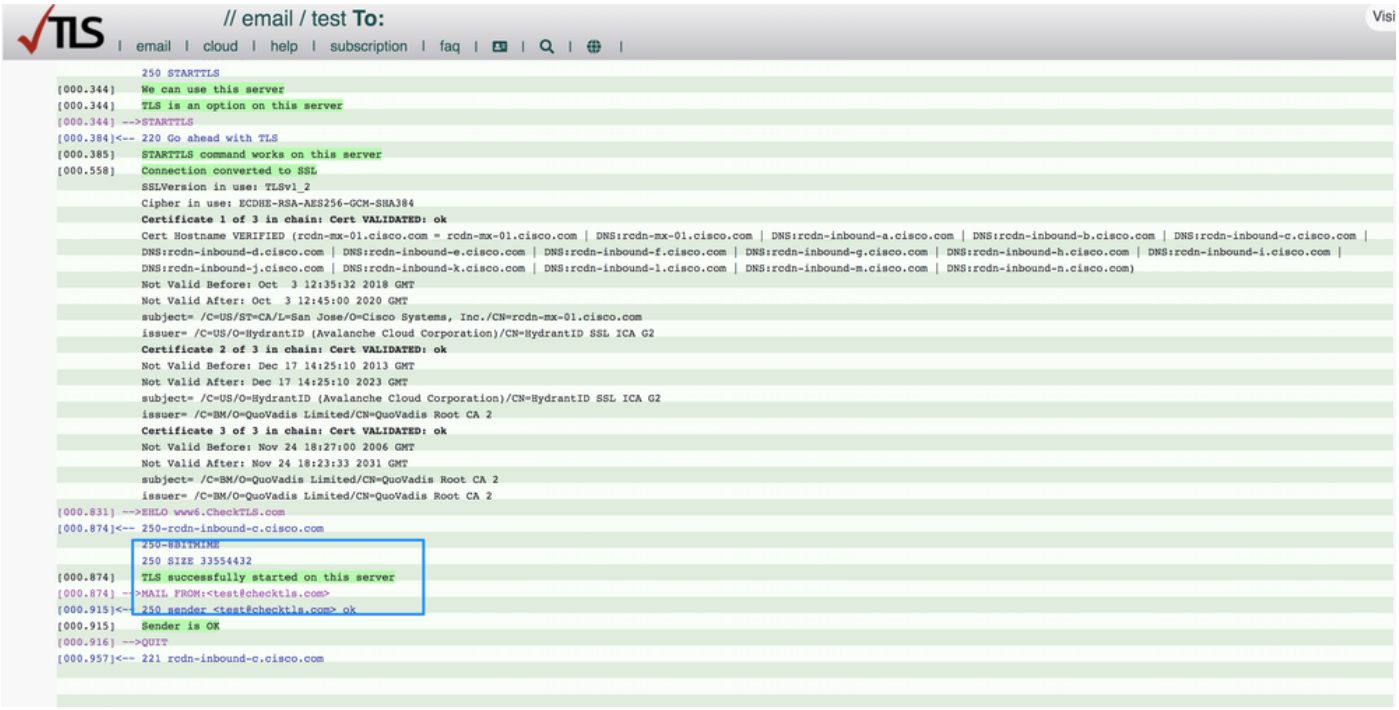
Before test, ensure the certificate to be tested is applied at the listener where your appliance receives Inbound mail.

Third-party tools such as CheckTLS.com and SSL-Tools.net can be used to verify the proper chaining of the certificate.

Example of CheckTLS.com Output for TLS-Verify Success

CheckTLS Confidence Factor for "postmaster@cisco.com": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
alln-mx-01.cisco.com [173.37.147.230:25]	10	OK (41ms)	OK (422ms)	OK (50ms)	OK (48ms)	OK (450ms)	OK (58ms)	OK (41ms)
rcdn-mx-01.cisco.com [72.163.7.166:25]	20	OK (41ms)	OK (260ms)	OK (42ms)	OK (41ms)	OK (446ms)	OK (43ms)	OK (42ms)
aer-mx-01.cisco.com [173.38.212.150:25]	30	OK (80ms)	OK (484ms)	OK (81ms)	OK (79ms)	OK (548ms)	OK (80ms)	OK (81ms)
Average		100%	100%	100%	100%	100%	100%	100%



Example of CheckTLS.com Output for TLS-Verify Failure

TestReceiver

CheckTLS Confidence Factor for "i[redacted]": 90

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
[redacted]	5	OK (121ms)	OK (683ms)	OK (407ms)	OK (236ms)	FAIL	OK (2,122ms)	OK (122ms)	OK (122ms)
[redacted]	5	OK (125ms)	OK (715ms)	OK (130ms)	OK (125ms)	FAIL	OK (1,608ms)	OK (125ms)	OK (127ms)
Average		100%	100%	100%	100%	0%	100%	100%	100%

Cert Hostname DOES NOT VERIFY (mailC.example.com != gvsvipa006.example.com)

Resolution

Note: If a self-signed certifcate is in use, the expected result in "Cert OK" column is "FAIL".

If a CA signed certificate is in use and TLS-verify still fails, verify that these items match:

- Certificate common name.
- Hostname (at GUI > Network > Interface).
- MX record hostname: this is the MX Server column in the TestReceiver table.

If a CA signed certificate was installed and you see errors, continue to the next section for information on how to troubleshoot the issue.

Troubleshoot

This section describes how to troubleshoot basic TLS issues on the ESA.

Intermediate Certificates

Look for duplicate intermediate certificates, especially when current certificates are updated instead of a new certificate creation. The intermediate certificate(s) have possibly changed, or have been improperly chained, and the certificate possibly uploaded multiple intermediate certificates. This can introduce certificate chaining and verification issues.

Enable Notifications for Required TLS Connection Failures

You can configure the ESA in order to send an alert if the TLS negotiation fails when messages are delivered to a domain that requires a TLS connection. The alert message contains the name of the destination domain for the failed TLS negotiation. The ESA sends the alert message to all of the recipients that are set to receive warning severity level alerts for *System* alert types.

Note: This is a global setting, so it cannot be set on a per-domain basis.

Complete these steps in order to enable TLS connection alerts:

1. Navigate to **Mail Policies > Destination Controls**.
2. Click **Edit Global Settings**.
3. Check the **Send an alert when a required TLS connection fails** check box.

Tip: You can also configure this setting with the **destconfig > setup** CLI command.

The ESA also logs the instances for which TLS is required for a domain, but could not be used in the appliance mail logs. This occurs when any of these conditions are met:

- The remote MTA does not support ESMTP (for example, it did not understand the *EHLO* command from the ESA).
- The remote MTA supports ESMTP, but the *STARTTLS* command was not in the list of extensions that it advertised in its *EHLO* response.
- The remote MTA advertised the *STARTTLS* extension, but responded with an error when the ESA sent the *STARTTLS* command.

Locate Successful TLS Communication Sessions in the Mail Logs

The TLS connections are recorded in the mail logs, along with other significant actions that are related to messages, such as filter actions, anti-virus and anti-spam verdicts, and delivery attempts. If there is a successful TLS connection, there is a resulting TLS *success* entry in the mail logs. Likewise, a failed TLS connection produces 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.

Tip: In order to understand the mail logs, refer to the ESA Message Disposition Determination Cisco document.

Here is an example of a successful TLS connection from the remote host (reception):

```
Tue Apr 17 00:57:53 2018 Info: New SMTP ICID 590125205 interface Data 1 (192.168.1.1) address 10.0.0.1
Tue Apr 17 00:57:53 2018 Info: ICID 590125205 ACCEPT SG SUSPECTLIST match sbrs[-1.4:2.0] SBRS -1.1
Tue Apr 17 00:57:54 2018 Info: ICID 590125205 TLS success protocol TLSv1 cipher DHE-RSA-AES256-SHA
Tue Apr 17 00:57:55 2018 Info: Start MID 179701980 ICID 590125205
```

Here is an example of a failed TLS connection from the remote host (reception):

```
Mon Apr 16 18:59:13 2018 Info: New SMTP ICID 590052584 interface Data 1 (192.168.1.1) address 10.0.0.1
Mon Apr 16 18:59:13 2018 Info: ICID 590052584 ACCEPT SG UNKNOWNLIST match sbrs[2.1:10.0] SBRS 2.7
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 TLS failed: (336109761, 'error:1408A0C1:SSL routines:SSL3
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 lost
```

```
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 close
```

Here is an example of a successful TLS connection to the remote host (delivery):

```
Tue Apr 17 00:58:02 2018 Info: New SMTP DCID 41014367 interface 192.168.1.1 address 10.0.0.1 port 25
Tue Apr 17 00:58:02 2018 Info: DCID 41014367 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-S
Tue Apr 17 00:58:03 2018 Info: Delivery start DCID 41014367 MID 179701982 to RID [0]
```

Here is an example of a failed TLS connection to the remote host (delivery):

```
Mon Apr 16 00:01:34 2018 Info: New SMTP DCID 40986669 interface 192.168.1.1 address 10.0.0.1 port 25
Mon Apr 16 00:01:35 2018 Info: Connection Error: DCID 40986669 domain: domain IP:10.0.0.1 port: 25 deta
 temporary reason' interface: 192.168.1.1 reason: unexpected SMTP response
Mon Apr 16 00:01:35 2018 Info: DCID 40986669 TLS failed: STARTTLS unexpected response
```

Related Information

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