ESAでのTLS用の証明書セットアップガイドの作成

内容

概要

このドキュメントでは、TLSで使用する証明書を作成する方法、着信/発信TLSをアクティブにする方法、およびCisco ESAの問題をトラブルシューティングする方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ESAのTLS実装は、暗号化を通じて電子メールのポイントツーポイント送信のプライバシーを提供します。管理者は、認証局(CA)サービスから証明書と秘密キーをインポートしたり、自己署名証明書を使用したりできます。

Cisco AsyncOS for Email Securityは、Simple Mail Transfer Protocol(SMTP)(*Secure SMTP over TLS*)に対する*STARTTLS*拡張をサポートしています。

> **ヒント**:TLSの詳細については、RFC 3207を参照してください。

> **注**：このドキュメントでは、ESAの*集中管理機能*を使用して、クラスタレベルで証明書をインストールする方法について説明します。証明書はマシンレベルでも適用できますが、マシンをクラスタから削除してから再び追加すると、マシンレベルの証明書は失われます。

機能の概要と要件

管理者は、次のいずれかの理由でアプライアンス上に自己署名証明書を作成する必要があります。

- TLSを使用する他のMTAとのSMTPカンバセーションを暗号化するため（着信カンバセーションと発信カンバセーションの両方）。
- アプライアンスでHTTPSサービスを有効にして、HTTPS経由でGUIにアクセスできるようにします。
- Lightweight Directory Access Protocol(LDAP)のクライアント証明書として使用するため（LDAPサーバにクライアント証明書が必要な場合）。
- アプライアンスとRivest-Shamir-Addleman(RSA)Enterprise Manager for Data Loss Protection(DLP)の間でセキュアな通信を可能にするため。
- アプライアンスとCisco Advanced Malware Protection(AMP)Threat Gridアプライアンス間の

セキュアな通信を可能にする。
ESAには、TLS接続を確立するために使用できるデモンストレーション証明書が事前に設定されています。

> **注意**：セキュアTLS接続を確立するにはデモンストレーション証明書で十分ですが、検証可能な接続は提供できないことに注意してください。

シスコでは、X.509またはPrivacy Enhanced Email(PEM)証明書をCAから取得することを推奨しています。これは*Apache*証明書とも呼ばれます。自己署名証明書は、検証可能な接続を提供できない前述のデモンストレーション証明書と類似しているため、自己署名証明書よりもCAの証明書の方が望ましいです。

> **注**:PEM証明書の形式は、RFC 1421 ~ RFC 1424でさらに定義されています。PEMは、公開キー、秘密キー、およびルート証明書を含めるために、(Apacheインストールおよび CA証明書ファイル*/etc/ssl/certs*などで)公開証明書のみ、または証明書チェーン全体を含めることができるコンテナ形式です。*PEM*という名前は、安全な電子メールの方法が失敗したことに由来しますが、使用したコンテナ形式は引き続きアクティブであり、X.509 ASN.1キーの64進数への変換です。

自分の証明書を持参する

独自の証明書をインポートするオプションはESAで使用できますが、必要なのは証明書が*PKCS#12*形式であることです。この形式には秘密キーが含まれます。管理者は、この形式で使用できる証明書を持っていないことがよくあります。このため、ESAで証明書を生成し、CAによって適切に署名することをお勧めします。

現在の証明書の更新

すでに存在する証明書の期限が切れている場合は、このドキュメントの「*自己署名証明書の展開*」セクションをスキップして、既存の証明書に再署名します。

> **ヒント**：詳細については、シスコのドキュメント『Renew a Certificate on an Email Security Appliance』を参照してください。

自己署名証明書の展開

このセクションでは、自己署名証明書と証明書署名要求(CSR)の生成、署名用のCAへの自己署名証明書の提供、署名付き証明書のESAへのアップロード、ESAサービスで使用する証明書の指定、アプライアンス設定と証明書のバックアップを行う方法について説明します。

自己署名証明書とCSRの生成

CLIを使用して自己署名証明書を作成するには、**certconfig**コマンドを入力します。

GUIから自己署名証明書を作成するには、次の手順を実行します。

1. アプライアンスのGUIから[Network] > [Certificates] > [Add Certificate] に移動します。

2. [Create Self-Signed Certificate] ドロップダウンメニューをクリックします。

   証明書を作成する際には、*共通名*がリスニングインターフェイスのホスト名と一致するか、または配信インターフェイスのホスト名と一致することを確認します。
   *listening*インターフェイスは、[Network] > [Listeners] で設定されたリスナーにリンクされたインターフェイスです。CLIで*deliveryconfig*コマンドを使用して明示的に設定されていない限り、*delivery*インターフェイスは自動的に選択されます。
3. 検証可能な着信接続の場合は、次の3つの項目が一致していることを検証します。

   MXレコード(ドメインネームシステム(DNS)ホスト名)

   共通名

   インターフェイスホスト名

   注：システムホスト名は、検証可能であることに関してTLS接続には影響しません。システムホスト名は、アプライアンスGUIの右上隅、またはCLIの**sethostname**コマンド出力に表示されます。

   注意:CSRをエクスポートする前に、必ず**送信**し、変更を**コミット**してください。これらの手順が完了しない場合、新しい証明書はアプライアンス構成にコミットされず、CAからの署名付き証明書はすでに存在する証明書に署名することも、その証明書に適用することもできません。

自己署名証明書をCAに提供する

自己署名証明書をCAに送信して署名するには、次の手順を実行します。

1. PEM形式でCSRをローカルコンピュータに保存します。[Network] > [Certificates] > [Certificate Name] > [Download Certificate Signing Request] の順に選択します。

2. 生成された証明書を署名用の認識されたCAに送信します。

3. X.509/PEM/Apache形式の証明書と中間証明書を要求します。

次に、CAはPEM形式で証明書を生成します。

注:CAプロバイダーのリストについては、Certificate authority Wikipediaの記事を参照してください。

署名付き証明書のESAへのアップロード

CAが秘密キーによって署名された信頼できる公開証明書を返した後、署名付き証明書をESAにアップロードします。

証明書は、パブリックまたはプライベートリスナー、IPインターフェイスHTTPSサービス、LDAPインターフェイス、または宛先ドメインへのすべての発信TLS接続で使用できます。

署名付き証明書をESAにアップロードするには、次の手順を実行します。

1. アプライアンスにアップロードする前に、受信した信頼できるパブリック証明書がPEM形式か、PEMに変換可能な形式を使用していることを確認します。 **ヒント**：形式を変換するには、フリーソフトウェアプログラムであるOpenSSLツールキットを使用できます。
2. 署名付き証明書をアップロードします。

   [Network] > [Certificates] に移動します。

   署名のためにCAに送信された証明書の名前をクリックします。

   ローカルマシンまたはネットワークボリューム上のファイルへのパスを入力します。

   注：新しい証明書をアップロードすると、現在の証明書が上書きされます。自己署名証明書に関連する中間証明書もアップロードできます。

   注意：署名付き証明書をアップロードした後は、必ず**送信**し、変更を**コミット**してください。

ESAサービスで使用する証明書の指定

証明書が作成され、署名され、ESAにアップロードされたので、証明書の使用を必要とするサービスに使用できます。

インバウンド TLS

インバウンドTLSサービスに証明書を使用するには、次の手順を実行します。

1. [Network] > [Listeners] に移動します。
2. リスナー名をクリックします。
3. [Certificate] ドロップダウンメニューから証明書名を選択します。
4. [Submit] をクリックします。
5. 必要に応じて、追加のリスナーに対してステップ1 ~ 4を繰り返します。
6. **変更を保存します。**

アウトバウンド TLS

アウトバウンドTLSサービスに証明書を使用するには、次の手順を実行します。

1. [Mail Policies] > [Destination Controls] に移動します。
2. [Global Settings] セクションで[Edit Global Settings...] をクリックします。

3. [Certificate] ドロップダウンメニューから証明書名を選択します。
4. [Submit] をクリックします。
5. **変更を保存します。**

HTTPS

HTTPSサービスに証明書を使用するには、次の手順を実行します。

1. [Network] > [IP Interfaces] に移動します。
2. インターフェイス名をクリックします。
3. [HTTPS Certificate] ドロップダウンメニューから証明書名を選択します。
4. [Submit] をクリックします。
5. 必要に応じて、追加のインターフェイスに対してステップ1 ~ 4を繰り返します。
6. **変更を保存します。**

LDAPS

LDAPの証明書を使用するには、次の手順を実行します。

1. [System Administration] > [LDAP] に移動します。
2. [LDAP Global Settings] セクションで[Edit Settings...] をクリックします。
3. [Certificate] ドロップダウンメニューから証明書名を選択します。
4. [Submit] をクリックします。
5. **変更を保存します。**

URL フィルタリング

URLフィルタリングに証明書を使用するには、次の手順を実行します。

1. CLIに**websecurityconfig**コマンドを入力します。
2. コマンドプロンプトに進みます。次のプロンプトが表示されたら、必ず**Y**を選択してください。

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

3. 証明書に関連付けられている番号を選択します。

4. commitコマンドを入力して、設定変更を確定します。

アプライアンスの設定と証明書のバックアップ

この時点でアプライアンスの設定が保存されていることを確認します。アプライアンスの設定には、前述のプロセスを通じて適用された、完了した証明書作業が含まれます。

アプライアンス設定ファイルを保存するには、次の手順を実行します。

1. [System Administration] > [Configuration File] > [Download file to local computer to view or save] に移動します。

2. 証明書をエクスポートします。

   [Network] > [Certificates] に移動します。

   [Export Certificate] をクリックします。

   エクスポートする証明書を選択します。

   証明書のファイル名を入力します。

   証明書ファイルのパスワードを入力します。

   [Export] をクリックします。

   ファイルをローカルマシンまたはネットワークマシンに保存します。

   この時点で追加の証明書をエクスポートできます。または、[Cancel] をクリックして [Network] > [Certificates] の場所に戻ることもできます。

   注：このプロセスでは、証明書をPKCS#12形式で保存します。これにより、ファイルが作成され、パスワードで保護された状態で保存されます。

インバウンドTLSの有効化

すべての着信セッションのTLSをアクティブにするには、Web GUIに接続し、設定された着信リスナーに対して[Mail Policies] > [Mail Flow Policies] を選択し、次の手順を実行します。

1. ポリシーを変更する必要があるリスナーを選択します。

2. ポリシーを編集するには、ポリシーの名前のリンクをクリックします。

3. [Security Features] セクションで、次のいずれかの[Encryption and Authentication] オプションを選択して、そのリスナーとメールフローポリシーに必要なTLSのレベルを設定します。

   Off：このオプションを選択すると、TLSは使用されません。

Preferred：このオプションを選択すると、TLSはリモートMTAからESAにネゴシエートできます。ただし、リモートMTAが(*220*応答の受信前に)ネゴシエートしない場合、SMTPトランザクションは*clear*(暗号化されていない)状態で続行されます。証明書が信頼できる認証局から発行されたものかどうかを確認する試みは行われません。220応答の受信後にエラーが発生した場合、SMTPトランザクションはクリアテキストにフォールバックしません。

Required：このオプションを選択すると、リモートMTAからESAにTLSをネゴシエートできます。ドメインの証明書を確認する試みは行われません。ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。ネゴシエーションが成功すると、暗号化されたセッションを介してメールが配信されます。

4. [Submit] をクリックします。

5. [Commit Changes] **ボタンをクリックします。**必要に応じて、この時点でオプションのコメントを追加できます。

6. [Commit Changes] をクリックして変更を保存します。

リスナーのメールフローポリシーが、選択したTLS設定で更新されます。

選択したドメインセットから着信する着信セッションのTLSをアクティブにするには、次の手順を実行します。

1. Web GUIに接続し、[Mail Policies] > [HAT Overview] を選択します。

2. 送信者のIP/FQDNを適切な送信者グループに追加します。

3. 前の手順で変更した送信者グループに関連付けられているメールフローポリシーのTLS設定を編集します。

4. [Submit] をクリックします。

5. [Commit Changes] **ボタンをクリックします。**必要に応じて、この時点でオプションのコメントを追加できます。

6. [Commit Changes] をクリックして変更を保存します。

送信者グループのメールフローポリシーが、選択したTLS設定で更新されます。

ヒント:ESAがTLS検証を処理する方法の詳細については、この記事を参照してください。[ESAでの証明書検証のアルゴリズムは何ですか。]

アウトバウンドTLSの有効化

発信セッションのTLSをアクティブにするには、Web GUIに接続し、[Mail Policies] > [Destination Controls] を選択してから、次の手順を実行します。

1. [Add Destination...] をクリックします。.

2. 宛先ドメインを追加します。

3. [TLS Support] セクションで、ドロップダウンメニューをクリックし、次のいずれかのオプションを選択して、設定するTLSのタイプを有効にします。

   None：このオプションを選択すると、インターフェイスからドメインのMTAへのアウトバウンド接続に対してTLSがネゴシエートされません。

   Preferred：このオプションを選択すると、ESAインターフェイスからドメインのMTAにTLSがネゴシエートされます。ただし、（220応答の受信前に）TLSネゴシエーションが失敗した場合、SMTPトランザクションは暗号化されずに*クリア*状態で続行されます。証明書が信頼できるCAから発信されているかどうかを確認する試みは行われません。220応答の受信後にエラーが発生した場合、SMTPトランザクションはクリアテキストにフォールバックしません。

   Required：このオプションを選択すると、ESAインターフェイスからドメインのMTAへのTLSがネゴシエートされます。ドメインの証明書を確認する試みは行われません。ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。ネゴシエーションが成功すると、暗号化されたセッションを介してメールが配信されます。

   Preferred-Verify：このオプションを選択すると、ESAからドメインのMTAにTLSがネゴシエートされ、アプライアンスはドメイン証明書の確認を試みます。この場合、次の3つの結果が考えられます。

   TLSがネゴシエートされ、証明書が検証されます。暗号化されたセッションによってメールが配信される。

   TLSはネゴシエートされますが、証明書は検証されません。暗号化されたセッションによってメールが配信される。

   TLS接続は確立されず、証明書は検証されません。電子メール メッセージがプレーン テキストで配信される。**Required-Verify**：このオプションを選択すると、ESAからドメインのMTAにTLSがネゴシエートされ、ドメイン証明書の検証が必要になります。この場合、次の3つの結果が考えられます。

   TLS接続がネゴシエートされ、証明書が検証されます。暗号化されたセッションによって電子メール メッセージが配信される。

   TLS接続はネゴシエートされますが、証明書は信頼できるCAによって検証されません。メールは配信されない。

   TLS接続はネゴシエートされませんが、メールは配信されません。
4. 宛先ドメインの*宛先制御*に必要な変更をさらに行います。

5. [Submit] をクリックします。

6. [Commit Changes] **ボタンをクリックします。**必要に応じて、この時点でオプションのコメントを追加できます。

7. [Commit Changes] をクリックして変更を保存します。

ESA証明書の設定ミスの症状

TLSは自己署名証明書で動作しますが、送信側でTLS検証が必要な場合は、CA署名付き証明書をインストールする必要があります。

ESAにCA署名付き証明書がインストールされていても、TLS検証が失敗する可能性があります。

このような場合は、「確認」セクションの手順で証明書を確認することを推奨します。

確認

Webブラウザを使用したTLSの確認

CA署名付き証明書を確認するには、証明書をESA GUI HTTPSサービスに適用します。

次に、WebブラウザでESAのGUIに移動します。https://youresaに移動するときに警告が表示される場合は、中間証明書が欠落しているなど、証明書が不適切にチェーン接続されている可能性があります。

サードパーティツールを使用したTLSの確認

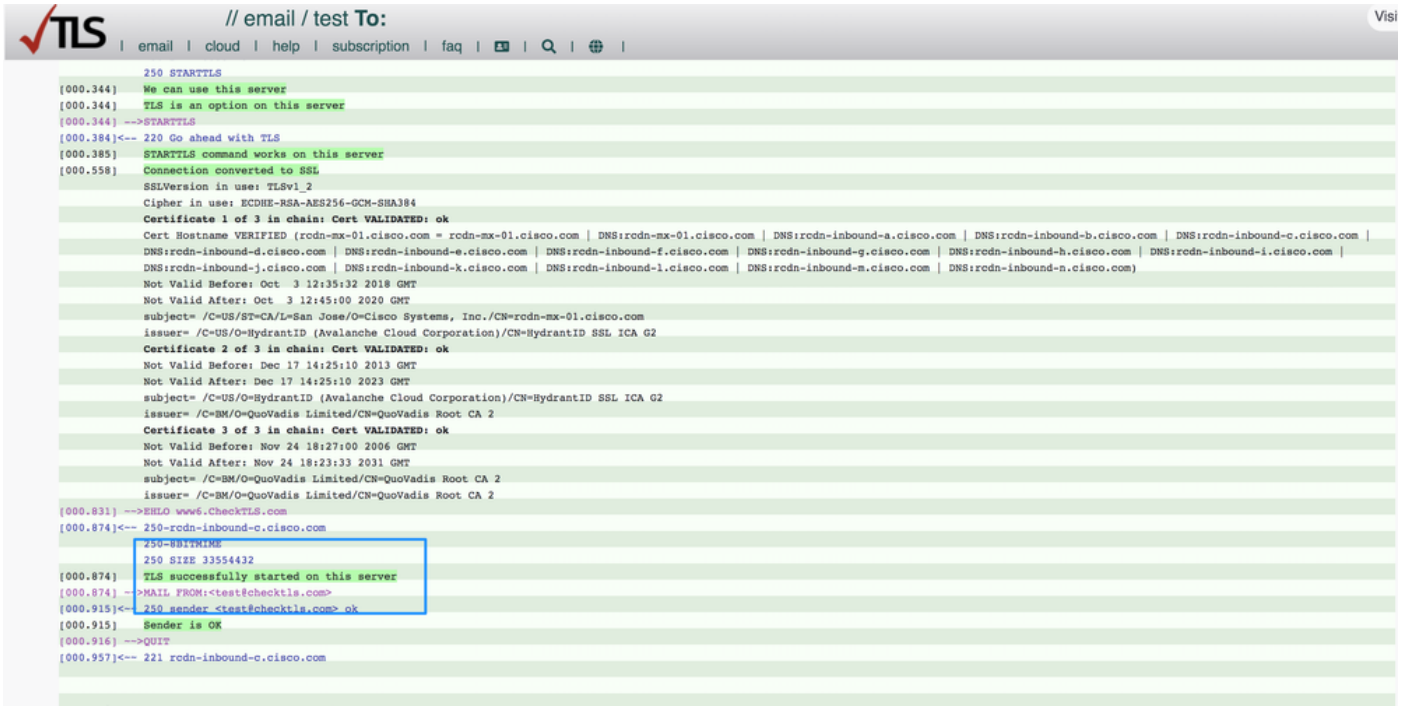
テストを行う前に、アプライアンスが受信メールを受信するリスナーにテスト対象の証明書が適用されていることを確認します。

CheckTLS.comやSSL-Tools.netなどのサードパーティツールを使用して、証明書の正しいチェーンを確認できます。

TLS-Verify SuccessのCheckTLS.com出力の例

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%



TLS検証の失敗に対するCheckTLS.comの出力例

証明書ホスト名が確認されない(mailC.example.com != gvsvipa006.example.com)

解決方法

> **注：自**己署名証明書が使用されている場合、[Cert OK]列の予想される結果は[FAIL]です。

CA署名付き証明書が使用中でもTLS検証が失敗する場合は、次の項目が一致していることを確認します。

- 証明書の共通名。
- ホスト名（[GUI] > [Network] > [Interface]で指定）。
- MXレコードホスト名：これはTestReceiverテーブルのMX Server列です。

CA署名付き証明書がインストールされていて、エラーが表示された場合は、次のセクションに進み、問題のトラブルシューティング方法に関する情報を参照してください。

トラブルシュート

このセクションでは、ESAの基本的なTLSの問題をトラブルシューティングする方法について説明します。

中間証明書

特に、新しい証明書を作成する代わりに現在の証明書を更新する場合は、重複する中間証明書を探します。中間証明書が変更されたか、不適切にチェーンされ、証明書が複数の中間証明書をアップロードした可能性があります。これにより、証明書チェーンと検証の問題が発生する可能性があります。

必要なTLS接続障害の通知を有効にする

TLS接続を必要とするドメインにメッセージが配信されるときにTLSネゴシエーションが失敗した場合にアラートを送信するようにESAを設定できます。アラートメッセージには、失敗したTLSネゴシエーションの宛先ドメインの名前が含まれています。ESAは、システムアラートタイプの警告重大度レベルのアラートを受信するように設定されているすべての受信者にアラートメッセージを送信します。

> **注**：これはグローバル設定であるため、ドメイン単位で設定することはできません。

TLS接続アラートを有効にするには、次の手順を実行します。

1. [Mail Policies] > [Destination Controls] に移動します。
2. [Edit Global Settings] をクリックします。
3. [Send an alert when a required TLS connection fails] チェックボックスをオンにします。

> **ヒント**：この設定は、**destconfig > setup** CLIコマンドを使用して設定することもできます。

また、ESAは、ドメインにTLSが必要であるが、アプライアンスのメールログでは使用できなかったインスタンスも記録します。これは、次のいずれかの条件が満たされた場合に発生します。

- リモートMTAはESMTPをサポートしていません(たとえば、ESAからの*EHLO*コマンドを認識していません)。
- リモートMTAはESMTPをサポートしていますが、*STARTTLS*コマンドが*EHLO*応答でアドバタイズした内線番号のリストに含まれていませんでした。
- リモートMTAは*STARTTLS*拡張をアドバタイズしましたが、ESAが*STARTTLS*コマンドを送信したときにエラーで応答しました。

メールログでの成功したTLS通信セッションの特定

TLS接続は、メッセージに関連する他の重要なアクション (フィルタアクション、ウイルス対策とスパム対策の判定、配信試行など) とともに、メールログに記録されます。TLS接続が成功し

た場合、メールログにTLS *success*エントリが生成されます。同様に、TLS接続が失敗すると、TLS *failed*エントリが生成されます。メッセージに関連付けられた TLS エントリがログ ファイルにない場合、そのメッセージは TLS 接続経由で配信されていません。

> **ヒント**：メールログを理解するには、シスコのドキュメント『ESAメッセージの破棄の判別』を参照してください。

リモートホスト（受信）からの正常なTLS接続の例を次に示します。

```
Tue Apr 17 00:57:53 2018 Info: New SMTP ICID 590125205 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
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
```

リモートホスト（受信）からのTLS接続の失敗の例を次に示します。

```
Mon Apr 16 18:59:13 2018 Info: New SMTP ICID 590052584 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
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_GET_CLIENT_HELLO:no shared cipher')
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 lost
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 close
```

リモートホスト（配信）への正常なTLS接続の例を次に示します。

```
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-SHA384
Tue Apr 17 00:58:03 2018 Info: Delivery start DCID 41014367 MID 179701982 to RID [0]
```

リモートホスト（配信）へのTLS接続の失敗の例を次に示します。

```
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 details: 454-'TLS not available due to
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
```

関連情報

- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド
- Ciscoコンテンツセキュリティ管理アプライアンス – エンドユーザガイド
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。