コラボレーション エッジ(MRA)証明書の設定 とトラブルシューティング

内容	•
L J L	•

<u>はじめに</u>

<u>前提条件</u>

<u>要件</u>

<u>使用するコンポーネント</u>

<u>背景説明</u>

パブリック認証局(CA)とプライベート認証局(CA)

証明書チェーンの仕組み

<u>SSL ハンドシェイクの概要</u>

<u>設定</u>

Expressway-C および Expressway-E トラバーサル ゾーン/信頼

<u>CSRの生成と署名</u>

<u>Expressway-CとExpressway-Eが互いを信頼するように設定する</u>

<u>Cisco Unified Communications Manager (CUCM)と Expressway-C 間のセキュア通信</u>

<u>概要</u>

<u>CUCMとExpressway-C間の信頼の設定</u> 自己署名証明書を持つCUCMサーバ

<u>Expressway-C および Expressway-E クラスタの考慮事項</u> <u>クラスタ証明書</u> <u>信頼済み CA リスト</u>

<u>確認</u>

<u>現在の証明書情報の確認</u>

<u>Wiresharkでの証明書の読み取り/エクスポート</u>

<u>トラブルシュート</u>

<u>証明書がExpresswayで信頼されているかどうかをテストする</u>

<u>Synergy ライト エンドポイント (7800/8800 シリーズの電話機)</u>

<u>ビデオ リソース</u>

<u>MRAまたはクラスタ化ExpresswayのCSRの生成</u>

<u>Expresswayへのサーバ証明書のインストール</u>

<u>Expressway間の証明書信頼の設定方法</u>

はじめに

このドキュメントでは、モバイルリモートアクセス(MRA)導入に関する証明書について説明します。

前提条件

要件

このドキュメントに関する固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、クリアな(デフォルト)設定で作業を開始していま 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

パブリック認証局(CA)とプライベート認証局の比較

Expressway-C および E サーバでの証明書への署名では、いくつかのオプションがあります。証 明書署名要求(CSR)をGoDaddy、VerisignなどのパブリックCAで署名するように選択するか、ま たは独自の認証局(OpenSSLを使用して自己署名するか、Microsoft Windowsサーバなどの内部 エンタープライズCA)を使用している場合は、内部的に署名することができます。 これらの方 法で使用されるCSRの作成方法と署名方法の詳細については、『<u>Video Communication</u> <u>Server(VCS)証明書作成ガイド</u>』を参照してください。

実際にパブリック CA による署名を必要とするサーバは Expressway-E のみです。 これは、クラ イアントがMRA経由でサインインするときに証明書を参照する唯一のサーバです。したがって、 ユーザが手動で証明書を受け入れる必要がないことを保証するためにパブリックCAを使用します 。 Expressway-Eは内部CA署名付き証明書を使用できますが、初めて使用するユーザには信頼で きない証明書を受け入れるように求められます。7800および8800シリーズの電話機のMRA登録 は、証明書信頼リストを変更できないため、内部証明書では機能しません。 説明を簡単にするた め、Expressway-C証明書とExpressway-E証明書の両方を同じCAで署名することを推奨します。 ただし、両方のサーバで信頼済みCAリストを適切に設定していれば、これは必須ではありません。

証明書チェーンの仕組み

証明書は、サーバの証明書に署名した発行元の検証に使用される2つ以上の証明書のチェーンでリ ンクされます。 チェーンには、クライアント/サーバ証明書、中間証明書(場合によっては)、 ルート証明書(証明書に署名した最上位レベルの認証局であるため、ルートCAとも呼ばれます)の3種類の証明書があります。

証明書には、チェーンを構築する2つの主なフィールドであるサブジェクトと発行者が含まれます 。

サブジェクトは、この証明書によって表されるサーバまたは認証局の名前です。Expressway-CまたはExpressway-E(またはその他のユニファイドコミュニケーション(UC)デバイス)の場合、これ

は完全修飾ドメイン名(FQDN)から構築されます。

発行者は、その特定の証明書を検証する認証局です。 誰でも証明書(最初に証明書を作成したサ ーバーを含む、自己署名証明書とも呼ばれる)に署名できるため、サーバーおよびクライアント は、本物と信頼する発行者またはCAのリストを持ちます。

証明書チェーンは、常に自己署名のトップレベル証明書またはルート証明書で終わります。 証明 書階層を移動すると、各証明書にはサブジェクトに関連する異なる発行者が存在します。最終的 には、サブジェクトと発行者が一致するルートCAが検出されます。これは、それが最上位レベル の証明書であり、したがって、クライアントまたはサーバの信頼済みCAリストによって信頼され る必要がある証明書であることを示します。

SSL ハンドシェイクの概要

トラバーサルゾーンの場合、Expressway-Cは常にクライアントとして機能し、Expressway-Eは 常にサーバとして機能します。 簡素化された交換は次のように機能します。

Expressway-C

Expressway-E

-----クライアントHello----->

<-----サーバHello------

<----サーバ証明書------

<----証明書要求 --

-----クライアント証明書----->

Expressway-Cは常に接続を開始し、常にクライアントであるため、ここでのキーは交換にありま す。Expressway-Eは、自身の証明書を最初に送信するルータです。Expressway-Cがこの証明書 を検証できない場合、ハンドシェイクを切断して自身の証明書をExpressway-Eに送信することは できません。

また、証明書に含まれている、 Transport Layer Security(TLS)Web クライアント認証および TLS Web サーバ認証の属性も重要です。これらの属性は、CSRに署名したCA上で決定され (Windows CAを使用する場合、選択したテンプレートによって決定されます)、証明書がクラ イアントまたはサーバ(あるいはその両方)の役割で有効であるかどうかが示されます。 VCSまたはExpresswayの場合は、状況に基づいて設定でき(トラバーサルゾーンの場合は常に同 じ)、証明書にクライアントとサーバの両方の認証属性が含まれている必要があります。

Expressway-CとExpressway-Eの両方が適用されていない場合、新しいサーバ証明書にアップロードするとエラーが表示されます。

証明書にこれらの属性があるかどうかわからない場合は、ブラウザまたはOSで証明書の詳細を開 き、「拡張キー使用法」セクションを確認します(図を参照)。 形式は、証明書の表示方法によ って異なる場合があります。

以下に例を挙げます。

Comment	Details
General	Decans

Certificate Hierarchy

ACTIVEDIRECTORY-CA	

Certificate Fields

Extended Key Usage	٠
Certificate Subject Alt Name	
Certificate Subject Key ID	
Certificate Authority Key Identifier	
CRL Distribution Points	_
Authority Information Access	=
Object Identifier (1 3 6 1 4 1 311 21 7)	
Object Identifier (1 3 6 1 4 1 311 21 10)	-

Field Value

```
Not Critical
TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)
```

Export...

設定

Expressway-C および Expressway-E トラバーサル ゾーン/信頼

CSR の生成と署名

前述のように、Expressway-CおよびExpressway-E証明書は、内部または外部CAによって、また は自己署名のためにOpenSSLによって署名される必要があります。

✤ 注:Expresswayサーバに付属する一時証明書はサポートされていないため、使用できません 。CA署名証明書があり、件名行が明確に定義されていないワイルドカード証明書を使用す

💊 る場合、その証明書はサポートされません。

最初のステップとして、CSR を生成し、優先する CA タイプによる署名を行います。このプロセスの詳細については、『証明書作成ガイド』を参照してください。CSRを作成する際には、証明書に含める必要があるサブジェクト代替名(SAN)を覚えておくことが重要です。SAN は証明書ガイドおよび『モバイル リモート アクセス導入ガイド』にも記載されています。新機能の追加が可能な最新バージョンのガイドを確認してください。使用されている機能に基づいて、含める必要がある一般的なSANのリスト:

Expressway-C

- ドメインリストに追加されたドメイン(内部または外部)。
- XMPPフェデレーションが使用されている場合は、すべての常設チャットノードのエイリアス。
- セキュアデバイスプロファイルを使用している場合は、CUCMでデバイスプロファイル名を 保護します。

Expressway-E

- Expressway-C で設定されたすべてのドメイン
- XMPPフェデレーションが使用されている場合は、すべての常設チャットノードのエイリアス。
- XMPP フェデレーション用にアドバタイズされたすべてのドメイン。
- ◆ 注:外部サービスレコード(SRV)ルックアップに使用されるベースドメインがExpressway-E証明書(xxx.comまたはcollab-edge.xxx.com)にSANとして含まれていない場合でも、 Jabberクライアントはエンドユーザに最初の接続で証明書を受け入れる必要があり、TCエ ンドポイントは接続に失敗します。

Expressway-CとExpressway-Eが互いを信頼するように設定する

ユニファイドコミュニケーションのトラバーサルゾーンで接続を確立するには、Expressway-Cと Expressway-Eが互いの証明書を信頼する必要があります。この例では、Expressway-E証明書が この階層を使用するパブリックCAによって署名されていると仮定します。

証明書 3

- 発行者: GoDaddyルートCA
- 件名:GoDaddyルートCA

証明書 2

- 発行者: GoDaddyルートCA
- 件名:GoDaddy中間認証局

証明書 1

発行者:GoDaddy中間認証局

件名:Expressway-E.lab

Expressway-Cは、信頼証明書1を使用して設定する必要があります。ほとんどの場合、サーバに 適用された信頼できる証明書に基づいて、サーバは最も低いレベルのサーバ証明書のみを送信し ます。 つまり、Expressway-Cが証明書1を信頼するためには、証明書2と3の両方をExpressway-Cの信頼済みCAリスト(メンテナンス>セキュリティ>信頼済みCAリスト)にアップロードする必要 があります。 Expressway-CがExpressway-E証明書を受信するときに中間証明書2を省略すると 、信頼されたGoDaddyルートCAに関連付ける方法がないため、拒否されます。

証明書 3

発行者: GoDaddyルートCA

件名:GoDaddyルートCA

証明書 1

発行者: GoDaddy中間認証局 – 信頼されていません!

件名:Expressway-E.lab

さらに、ルートのない中間証明書のみをExpressway-Cの信頼されたCAリストにアップロードす ると、GoDaddy中間認証局は信頼されているようですが、より高い認証局によって署名されてい ます。この場合、信頼されていないGoDaddyルートCAは失敗します。

証明書 2

発行者: GoDaddyルートCA – 信頼されていません!

件名:GoDaddy中間認証局

証明書 1

発行者:GoDaddy中間認証局

件名:Expressway-E.lab

```
すべての中間認証局とルートが信頼済み CA リストに追加されると、証明書を検証できます。
```

証明書 3

発行者: GoDaddyルートCA – 自己署名トップレベル証明書が信頼され、チェーンが完了しました。

件名: GoDaddyルートCA

証明書 2

発行者: GoDaddyルートCA

件名:GoDaddy中間認証局

証明書 1

発行者:GoDaddy中間認証局

件名:Expressway-E.lab

証明書チェーンが不明な場合は、特定のExpresswayのWebインターフェイスにログインしたとき にブラウザを確認できます。 プロセスはブラウザによって若干異なりますが、Firefoxでは、ア ドレスバーの左端にあるロックアイコンをクリックできます。 表示されるポップアップで、[詳 細情報(More Information)]>[証明書の表示(View Certificate)]>[詳細(Details)]をクリック します。 ブラウザでチェーン全体を結合できる場合は、チェーンを上から下に表示できます。 トップレベル証明書に一致するサブジェクトと発行者がない場合、チェーンは完了していません 。 必要な証明書を強調表示した状態でexportをクリックすると、チェーン内の各証明書を単独で エクスポートすることもできます。 これは、正しい証明書を CA の信頼リストに確実にアップロ ードしたかどうかわからない場合に役立ちます。

	. – • ×
General Media Permissions Security	
Website Identity	
Website:	
Owner: This website does not supply ownersh	ip information.
Verified by: DigiCert Inc	
	<u>V</u> iew Certificate
Privacy & History	
Have I visited this website prior to today?	Yes, 622 times
Is this website storing information (cookies) on my computer?	Yes View Coo <u>k</u> ies
Have I saved any passwords for this website?	No Vie <u>w</u> Saved Passwords
Technical Details	
Connection Encrypted (TLS_RSA_WITH_AES_128_CB	C_SHA, 128 bit keys, TLS 1.2)
The page you are viewing was encrypted before being	transmitted over the Internet.
Encryption makes it difficult for unauthorized people to therefore unlikely that anyone read this page as it trave	o view information traveling between computers. It is led across the network.

SSL Client Certificate	en verified for the following uses:	
SSL Server Certificate		
Issued To		
Organization (O)		
Organizational Unit (OL	J)	
Serial Number		
Issued By		
Common Name (CN)	DigiCert SHA2 High Assurance Server CA	
Organization (O)	DigiCert Inc	
Organizational Unit (OL	J)	
Period of Validity		
Begins On	3/25/2015	
Expires On	4/12/201/	
Fingerprints	38.37.23.04.85.02.00.55.20.48.08.52.07.50.05.08.	
SHA-250 Fingerprint	F3:75:F6:0D:43:98:8B:73:22:A4:ED:A8:E6:D7:2A:23	
SHA1 Fingerprint	CE:7B:79:41:94:9E:07:48:F3:A4:B4:07:03:76:D3:52:12:5D:A9:42	

	l
eral Details	
Certificate <u>H</u> ierarchy	
▲DigiCert High Assurance EV Root CA	
Certificate <u>F</u> ields	
Builtin Object Token:DigiCert High Assurance EV Root CA	
▶ Certificate	
Certificate Signature Algorithm	
Certificate Signature Value	
Field <u>V</u> alue	
_	
E <u>x</u> port	

Expressway-CがExpressway-Eからの証明書を信頼するようになったので、反対方向で動作する ことを確認します。Expressway-C証明書がExpressway-Eに署名したのと同じCAによって署名さ れている場合、プロセスは簡単です。Expressway-Eの信頼済みCAリストに、Cで実行したのと同 じ証明書をアップロードします。 Cが別のCAによって署名されている場合は、図に示すように 同じプロセスを使用する必要がありますが、代わりにExpressway-C証明書に署名したチェーンを 使用します。

Cisco Unified Communications Manager (CUCM)と Expressway-C 間のセキュア 通信

概要

Expressway-CとExpressway-E間のトラバーサルゾーンとは異なり、Expressway-CとCUCM間の セキュアなシグナリングは必要ありません。内部セキュリティポリシーで許可されていない場合 を除き、この手順を続行する前に、最初にMRAをCUCM上の非セキュアなデバイスプロファイル で動作するように設定する必要があります。

CUCMとExpressway-Cの間で有効にできる主なセキュリティ機能は、TLS検証とセキュアデバイ ス登録の2つです。 SSL ハンドシェイクにおいて CUCM 側からの 2 つの異なる証明書を使用す るため、これら 2 つの機能には重要な違いがあります。

TLS 検証 - tomcat 証明書

セキュア SIP 登録 - callmanager 証明書

CUCMとExpressway-C間の信頼の設定

この場合の概念は、Expressway-CとExpressway-Eの間とまったく同じです。 最初に、CUCM が Expressway-C のサーバ証明書を信頼する必要があります。 つまり、CUCMでは、 Expressway-Cの中間証明書とルート証明書を、TLS検証機能の場合はtomcat-trust証明書、セキュ アなデバイス登録の場合はCallManager-trust証明書としてアップロードする必要があります。 こ れを行うには、CUCM Web GUIの右上にあるCisco Unified OS Administrationに移動し、 Security> Certificate Managementの順に選択します。 ここでは、[証明書/証明書チェーンをアッ プロード(Upload Certificate/Certificate Chain)]をクリックして正しい信頼形式を選択するか、 [検索(Find)]をクリックして現在アップロードされている証明書のリストを表示することがで きます。

🥹 Upload Certificate/Certificate chain - Mozilla Firefox				
https://	https://			
Upload Certificate/Certifica	ite chain			
Dipload 🖳 Close				
Status Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster				
└ Upload Certificate/Certific	ate chain			
Certificate Purpose*	CallManager-trust			
Description(friendly name)	Expressway Root Cert			
Upload File	Browse_ No file selected.			
Upload Close				
(i) *- indicates required item.				

Expressway-CがCUCM証明書に署名したCAを信頼していることを確認する必要があります。こ れを行うには、信頼済みCAリストにこれらの証明書を追加します。 ほとんどの場合、CAを使用 してCUCM証明書に署名した場合、tomcat証明書とCallManager証明書は同じCAによって署名さ れる必要があります。これらが異なる場合は、TLS検証とセキュア登録を使用する場合に両方を 信頼する必要があります。

セキュアSIP登録の場合、デバイスに適用されるCUCMのセキュアデバイスプロファイル名が Expressway-C証明書にSANとしてリストされていることを確認する必要もあります。これがセキ ュア登録メッセージを含まない場合、CUCMからの403で失敗し、TLSの失敗を示します。

注:セキュアなSIP登録のためにCUCMとExpressway-Cの間でSSLハンドシェイクが発生す る場合、2つのハンドシェイクが発生します。まず、Expressway-Cがクライアントとして動 作し、CUCMとの接続を開始します。これが正常に完了すると、CUCMは応答するクライア ントとして別のハンドシェイクを開始します。 つまり、Expressway-C の場合とまったく 同様に、CUCM 上の callmanager 証明書で TLS Web クライアントと TLS Web サーバの両 方の認証属性が適用されている必要があります。 違いは、CUCMではこれらの証明書を両 方なしでアップロードでき、CUCMにサーバ認証属性しかない場合は、内部のセキュア登録 が正常に動作することです。リストでCallManager証明書を探して選択すると、CUCMでこ れを確認できます。 ここでは、Extensionセクションの下のUsage OIDを確認できます。 Client Authenticationには1.3.6.1.5.5.7.3.2、Server Authenticationには1.3.6.1.5.5.7.3.1が表 示されています。このウィンドウから証明書をダウンロードすることもできます。

🥑 Certificate Details(CA-signed) - Mozilla Firefox	25	
https:///////cmplatform/certificateEdit.do?cert=/usr/local/cm/.security/CallManager/certs/CallManage	r.per	
Certificate Details for cucm10-lab-pub.tkratzke.local, CallManager	-	
Regenerate 🔍 Generate CSR 👔 Download .PEM File 👔 Download .DER File		
_ Status	ן ר	
i Status: Ready		
Certificate Settings		
Locally Uploaded 01/04/15		
File Name CallManager.pem		
Certificate Purpose CallManager		
Certificate Type certs		
Certificate Group product-cm		
Description(friendly name) Certificate Signed by tkratzke-ACTIVEDIRECTORY-CA		
Description(friendly name) Certificate Signed by tkratzke-ACTIVEDIRECTORY-CA Certificate File Data Key: RSA (1.2.840.113549.1.1.1) Key value: 3082010a0282010100c3f0061dafbffa97cd781c9627134664cae9f55d5d92871b60ce17ddf78972963a4 Idb705c43c97046df73897748e2a2459c96f7cd3cc849c71055b27ffd30dc6d4ebc727beb7a96e98ab78 01d25eb0e354086e318df242d4039004f2c569308c875697ecdf2b9040d4aa22da5b7a82f667abbd2342 0fe820dd157a648ee4c611ca8612cef49f35dd8e01677b18edca260c5aa3920da979e4adadb7ed4c776e e1c9a28d9eaf90648cafaf757a7050ec0fc383eccbb227d0947e3265737f640e7db4d280e477689ba395 60a6a39db010fadb4e2da05beea5c8f47357726d90e56c1415c499e8d09ab36357c1223f1bae52baa82 32ba70485bd745407b354bd09d0203010001 Extensions: 9 present [Extension: ExtKeyUsageSyntax (OID.2.5.29.37) Critical: false Usage oids: 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1,]		
Regenerate Generate CSR Download .PEM File Download .DER File		

✤ 注:クラスタ内のパブリッシャに適用される信頼証明書は、サブスクライバに複製する必要 があります。新しい設定で個別にログインして確認することをお勧めします。

◆ 注:Expressway-CがCUCMからの証明書を正しく検証するには、CUCMサーバをIPアドレスではなくFQDNを使用してExpressway-Cに追加する必要があります。 IPアドレスが機能する唯一の方法は、各CUCMノードのIPが証明書にSANとして追加されている場合です。これは、ほとんど行われません。

デフォルトでは、CUCMサーバには自己署名証明書が付属しています。 これらが設定されている 場合、TLS検証とセキュアデバイス登録の両方を同時に使用することはできません。 どちらの機 能も単独で使用できますが、証明書は自己署名であるため、自己署名Tomcat証明書と自己署名 CallManager証明書の両方をExpressway-Cの信頼済みCAリストにアップロードする必要がありま す。 Expressway-Cが自身の信頼リストを検索して証明書を検証する場合、サブジェクトが一致 する証明書が見つかると停止します。このため、信頼リストでtomcatまたはCallManagerのどち らか上位にある機能が動作します。 低い方のAPは、存在しないかのように失敗します。 この問 題を解決するには、CA(パブリックまたはプライベート)を使用して CUCM 証明書に署名し、 その CA のみを信頼します。

Expressway-C および Expressway-E クラスタの考慮事項

クラスタ証明書

冗長化の目的で Expressway-C サーバまたは Expressway-E サーバのクラスタを使用している場合は、サーバごとに個別の CSR を生成して CA による署名を行うことを強くお勧めします。前のシナリオでは、図に示すように、各ピア証明書の共通名(CN)は同じクラスタの完全修飾ドメイン名(FQDN)になり、SANはクラスタのFQDNとそれぞれのピアのFQDNになります。



クラスタFQDNをCNとして使用し、SAN内の各ピアのFQDNとクラスタFQDNを使用することで 、クラスタ内のすべてのノードで同じ証明書を使用できるため、パブリックCAによって署名され る複数の証明書のコストを回避できます。



◆ 注:Cs証明書の電話セキュリティプロファイル名が必要になるのは、UCMでセキュア電話セキュリティプロファイルを使用する場合だけです。外部ドメインまたはcollab-edge.example.com(example.comはユーザのドメイン)は、IP PhoneおよびTCエンドポイントをMRA経由で登録する場合にのみ必要です。これは、MRA経由のJabber登録ではオプションです。存在しない場合、JabberはMRA経由でログインするときに証明書を受け入れるように求めます。

どうしても必要な場合は、次のプロセスでこれを実行するか、OpenSSLを使用して秘密キーと CSRの両方を手動で生成できます。

手順1:クラスタのプライマリでCSRを生成し、クラスタエイリアスをCNとしてリストするよう に設定します。クラスタ内のすべてのピアを、他のすべての必要なSANとともに代替名として追 加します。

ステップ2:このCSRに署名し、プライマリピアにアップロードします。

ステップ3:プライマリにrootとしてログインし、/Tandberg/persistent/certsにある秘密キーをダウンロードします。

ステップ4:署名付き証明書と一致した秘密キーの両方をクラスタ内の他のピアにアップロードします。

- 💊 注:これは次の理由から推奨されません。
 - 1.すべてのピアが同じ秘密キーを使用するため、セキュリティ上のリスクがあります。 何 らかの方法で侵害された場合、攻撃者は任意のサーバからのトラフィックを復号化できます 。

2.証明書を変更する必要がある場合は、単純なCSRの生成と署名ではなく、このプロセス全体を繰り返す必要があります。

信頼済み CA リスト

クラスタ内の CUCM サブスクライバとは異なり、Expressway または VCS クラスタ内のピア間 で信頼済み CA リストは複製されません。 つまり、クラスタがある場合は、信頼できる証明書を 各ピアのCAリストに手動でアップロードする必要があります。

確認

このセクションでは、設定が正常に動作していることを確認します。

現在の証明書情報の確認

既存の証明書の情報を確認するにはいくつかの方法があります。 最初のオプションは、Webブ ラウザを使用することです。前のセクションで説明した方法を使用します。この方法は、チェー ン内の特定の証明書のエクスポートにも使用できます。 SAN、またはExpresswayサーバ証明書 に追加されたその他の属性を確認する必要がある場合は、Web Graphical User Interface (GUI; グラフィカルユーザインターフェイス)を使用して直接確認できます。確認す るには、Maintenance > Security Certificates > Server Certificateの順に移動し、Show Decodedを クリックします。

Show (decoded) Show (PEM file) _ 0 23 📵 Mozilla Firefox E' https:// /viewcert?cert=SERVER_CERTIFICATE A Certificate: Data: Version: 3 (0x2) Serial Number: Signature Algorithm: sha1WithRSAEncryption Issuer: DC=local, DC= -ACTIVEDIRECTORY-CA CN= Validity Not Before: May 11 15:40:03 2015 GMT Not After : May 10 15:40:03 2017 GMT Subject: C=US, ST=NC, L=RTP, O=Cisco, OU=TAC, CN= Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit) Modulus: 00:95:ed:09:0f:99:7a:f9:82:41:e8:23:09:15:e0: 0d:7b:84:bc:97:52:35:19:e6:5f:81:be:62:bc:eb: 8b:ad:9f:ea:e3:13:a0:61:ca:db:bc:7c:da:31:7e: f8:49:1d:75:2f:75:45:74:f0:5b:87:3c:5b:5f:12: 06:d5:c3:ab:2c:d5:02:a4:b4:01:2c:f8:94:d0:05: 27:1f:b7:4c:7d:3c:a2:a7:97:ae:fc:5a:bd:93:ce: 75:60:7c:53:2a:06:e7:7a:97:2e:0d:99:cf:d8:1e: Ob:ce:af:e8:5d:fc:67:24:6e:65:92:12:5a:1e:b6: 5f:3e:ca:90:b3:ed:50:ba:61:1e:64:92:43:70:f1: 77:bf:14:b7:31:af:6f:93:9b:a6:6c:a3:2e:60:bb: e7:45:4e:f6:02:30:40:b0:35:2a:6b:b9:cd:73:93: 01:74:f4:b3:cd:2e:5d:8a:af:c4:4a:c5:58:36:cc: 18:88:3c:9f:21:e6:65:83:14:8c:b3:7e:73:b0:ce: 31:74:b2:c0:f6:19:45:b6:ec:2e:f4:e5:af:6c:56: ff:74:23:00:80:45:f1:f7:a9:3e:7e:8a:9c:71:7e: 72:d4:e8:ad:b9:f4:bc:6f:e5:57:45:4e:56:c9:f7: ac:f0:98:a8:4a:91:66:7b:db:9f:ef:91:df:11:59: 8f:8f Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Kev Usage: critical Digital Signature, Key Encipherment, Data Encipherment X509v3 Extended Key Usage: <. 111

ここでは、証明書をダウンロードしなくても、証明書の特定の詳細をすべて確認できます。 アク ティブな CSR についても、関連する署名済み証明書をまだアップロードしていなければ、同じ 手順を実行できます。

Wiresharkでの証明書の読み取り/エクスポート

証明書交換を含むSSLハンドシェイクのWiresharkキャプチャがある場合、Wiresharkは実際に証 明書を復号化でき、チェーン内のすべての証明書を内部からエクスポートできます(チェーン全 体が交換されている場合)。 証明書の交換における特定のポート(トラバーサル ゾーンの場合 は一般に 7001)について、パケット キャプチャをフィルタで絞り込みます。 次に、クライアン トとサーバのhelloパケットがSSLハンドシェイクとともに表示されない場合、TCPストリーム内 のパケットの1つを右クリックして、decode asを選択します。 ここで、SSLを選択して、 applyをクリックします。 ここで、正しいトラフィックをキャプチャした場合は、証明書交換を 確認する必要があります。 ペイロードに証明書が含まれている正しいサーバからのパケットを見 つけます。 図に示すように、証明書のリストが表示されるまで、下部ペインのSSLセクションを

展開します。

Filte	tcp.stream eq 19	▼ Expression Clear Ap	ply Save Filter
No.	Time Sour	ce Destination	Protocol Length Info
1	803 2015-06-03 18:01:07.522714		TCP 74 25018+7001 [SYN] S
1	806 2015-06-03 18:01:07.522835		TCP 74 7001→25018 [SYN, A
1	807 2015-06-03 18:01:07.522855		TCP 66 25018-7001 [ACK] 5
1	808 2015-06-03 18:01:07.523594		TLSv1.2 266 Client Hello
1	809 2015-06-03 18:01:07.523846		TCP 66 7001-25018 [ACK] 5
1	811 2015-06-03 18:01:07.538935		TLSv1.2 1514 Server Hello
1	812 2015-06-03 18:01:07.538970		TCP 66 25018-7001 [ACK] 5
1	813 2015-06-03 18:01:07.539008		TLSv1.2 1514 Certificate
•			III
E E	ame 1813: 1514 bytes on wire (121)	12 bits), 1514 bytes captured (1211	2 hits)
	thernet II, Src: Vmware_a1:14:46 (), Dst: Vmware_a1:	:1e:e1 ()
+ I	ternet Protocol Version 4, Src:	,, <u>-</u>	····· · · · · · · · · · · · · · · · ·
± TI	ansmission Control Protocol, Src	Port: 7001 (7001),	
±Ε	Reassembled TCP Segments (2541 b	ytes): #1811(1390), #1813(1151)]	
E 5	ecure Sockets Layer		
	TLSv1.2 Record Laver: Handshake P	rotocol: Certificate	
	Content Type: Handshake (22)		
	Version: TLS 1.2 (0x0303)		
	Length: 2536		
	Handshake Protocol: Certificate		
	Handshake Type: Certificate (11)		
	landh - 552		
	Certificates Length: 2529		
	Certificates (2529 bytes)		
	Certificate Length: 1612		
	Certificate (id-at-commonNat	me= id_s	at-organizationalUnitName= id-at-organizationNa
	Certificate Length: 011	,10-8	te or garrizacionaron enance, ru-ac-or garrizacionna
	ceren reace Lengen. 511		

証明書を展開すると、すべての詳細を確認できます。 証明書をエクスポートする場合は、チェーン内の目的の証明書を右クリックし(複数ある場合)、Export Selected Packet Bytesを選択します。 証明書の名前を入力し、[保存(Save)]をクリックします。 ここで、Windows証明書ビューアで証明書を開くか(.cer拡張子を付けた場合)、他の分析ツールにアップロードする必要があります。

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。

証明書がExpresswayで信頼されているかどうかをテストする

最良の方法は、証明書チェーンを手動で確認し、すべてのメンバーがExpresswayの信頼済み CAリストに含まれていることを確認することですが、Web GUIのメンテナンス> [セキュリティ 証明書]の下にあるクライアント証明書テストを使用して、Expresswayが特定のクライアントの 証明書を信頼しているかどうかをすばやく確認できます。すべてのデフォルト設定を同じにして ください。ドロップダウンからUpload Test File (pem形式)を選択し、検証するクライアント証 明書を選択します。 証明書が信頼されていない場合、図に示すように、拒否された理由を説明す るエラーが表示されます。表示されるエラーは、参照用にアップロードされた証明書のデコード された情報です。

Client certificate testing	
Client certificate	
Certificate source Select the file you want to test Currently uploaded test file	This tests whether a client certificate is valid wh Uploaded test file (PEM format) v BrowseNo file selected.
Certificate-based authentication pattern	
Regex to match against certificate	This section applies only if your certificate conta username format combinations to the nominated /Subject*CN=(? <capturecommonname>([^,\\]](\</capturecommonname>
Username format	#captureCommonName#
	Make these settings permanent
Check certificate	
Certificate test results	

Valid certificate:

Invalid: The client certificate is not signed by a CA in the trusted CA list.

Expresswayが証明書CRLを取得できないことを示すエラーが表示されても、Expresswayが CRLチェックを使用しない場合は、証明書が信頼され、他のすべての検証チェックに合格するこ とを意味します。

Client certificate testing	
Client certificate	
	This tests whether a client certificate is valid when checked against the Exp
Certificate source	Uploaded test file (PEM format) 👻 🤃
Select the file you want to test	Browse No file selected.
Currently uploaded test file	vcs.cer
Certificate-based authentication pattern	
	This section applies only if your certificate contains authentication credentia
	username format combinations to the nominated certificate to see if the certi
Regex to match against certificate	/Subject.*CN=(? <capturecommonname>([^,\\](\))*)/m</capturecommonname>
Username format	#captureCommonName#
	Make these settings permanent

Check certificate

Certificate test results Valid certificate:

Invalid: unable to get certificate CRL, please ensure that you have uploaded a CRL for the CA that signed this client certificate

Synergy ライト エンドポイント(7800/8800 シリーズの電話機)

これらの新しいデバイスには、事前に入力された証明書信頼リストが付属しています。このリストには、既知のパブリックCAが多数含まれています。 この信頼リストは変更できません。つまり、これらのデバイスを使用するには、Expressway-E証明書をこれらの一致したパブリックCAのいずれかによって署名する必要があります。 内部CAまたは別のパブリックCAによって署名されている場合、接続は失敗します。 Jabber クライアントのようにユーザが手動で証明書を承諾するオプションはありません。

- ◆ 注:一部の導入では、Expressway-Eが内部CAを使用する場合でも、7800/8800シリーズの 電話機に含まれるリストからCAを使用するCitrix NetScalerなどのデバイスを使用して MRA経由で登録できることが判明しています。SSL認証を機能させるには、NetScalerのル ートCAをExpressway-Eにアップロードし、内部のルートCAをNetscalerにアップロードす る必要があります。これは動作することが実証されており、ベストエフォート型のサポート です。
- 注:信頼されたCAリストにすべての正しい証明書が含まれているように見えても、拒否される場合は、リストの上位に、同じサブジェクトを持ち、正しい証明書と競合する可能性がある別の証明書が存在しないことを確認してください。他のすべてが失敗した場合は、ブラウザまたはWiresharkからチェーンを直接エクスポートし、すべての証明書を反対側のサーバのCAリストにアップロードできます。これにより、信頼できる証明書であることが保証されます。
- 注:トラバーサルゾーンの問題をトラブルシューティングする際に、証明書に関連した問題のように見える場合がありますが、実際にはソフトウェア側の問題です。 トラバーサルに使用しているアカウントのユーザ名とパスワードが正しいか確認してください。
- ➢ 注:VCSまたはExpresswayでは、証明書のSANフィールドで999文字を超える文字はサポートされていません。この制限を超えているSAN(多くの代替名が必要)は、存在しないものとして無視されます。

ビデオ リソース

このセクションでは、すべての証明書設定プロセスを説明するビデオ情報を提供します。

<u>MRAまたはクラスタ化ExpresswayのCSRの生成</u>

<u>Expresswayへのサーバ証明書のインストール</u>

<u>Expressway間の証明書信頼の設定方法</u>

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。