ASAでのUnified Mobility Advantageサーバ証明書の問題

内容

概要

このドキュメントでは、適応型セキュリティアプライアンス(ASA)とCisco Unified Mobility Advantage(CUMA)サーバの間で自己署名証明書を交換する方法、およびその逆の方法について説明します。また、証明書のインポート中に発生する一般的な問題のトラブルシューティング方法についても説明します。

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情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ASA 5500 シリーズ
- Cisco Unified Mobility Advantageサーバ7

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

導入シナリオ

Cisco Mobility Advantageソリューションで使用されるTLSプロキシの導入シナリオは2つあります。

注：どちらのシナリオでも、クライアントはインターネットから接続します。

1. 適応型セキュリティアプライアンスは、ファイアウォールとTLSプロキシの両方として機能します。
2. 適応型セキュリティアプライアンスは、TLSプロキシとしてのみ機能します。

どちらのシナリオでも、**Cisco UMAサーバ証明書**と**キーペア**を**PKCS-12**形式でエクスポートし、適応型セキュリティアプライアンスにインポートする必要があります。証明書は、Cisco UMAクライアントとのハンドシェイク中に使用されます。

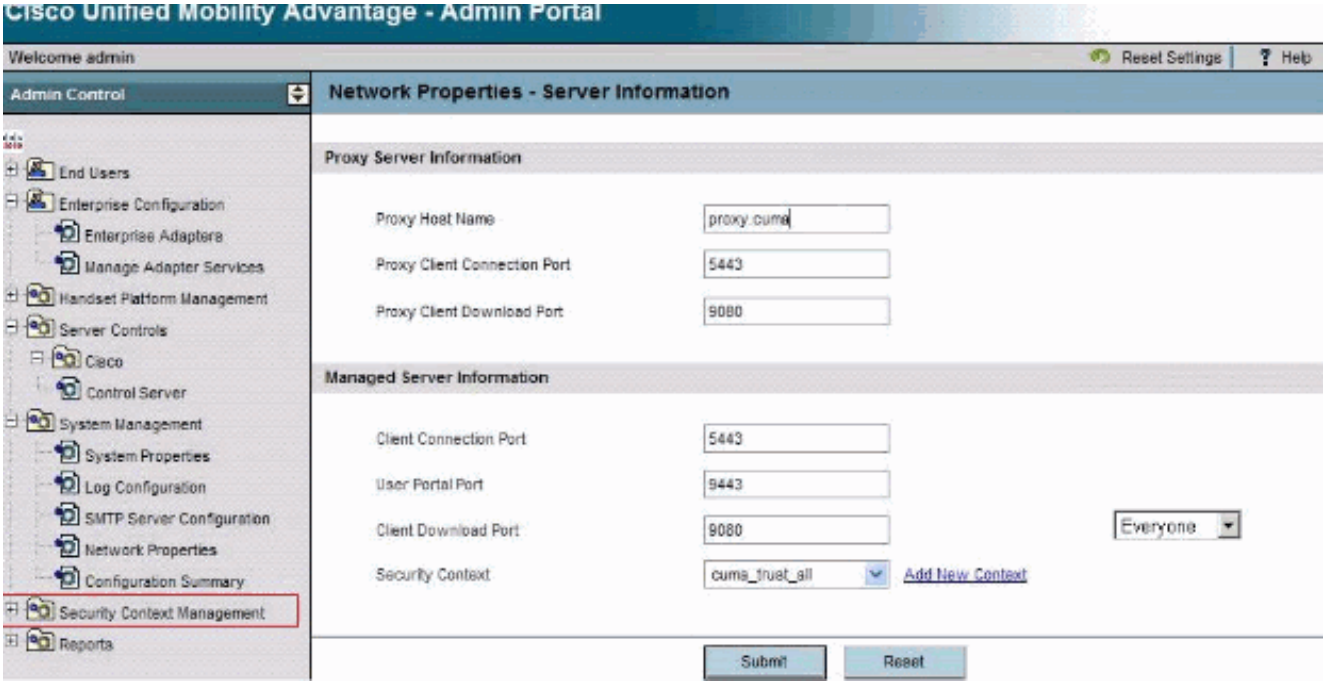
適応型セキュリティアプライアンス(ASA)のトラストストアにCisco UMAサーバ自己署名証明書をインストールすると、適応型セキュリティアプライアンスが適応型セキュリティアプライアンスプロキシとCisco UMAサーバ間のハンドシェイク中にCisco UMAサーバを認証する必要があります。

Cisco UMAサーバ自己署名証明書のインストール

CUMAサーバで実行するタスク

これらの手順は、CUMAサーバで実行する必要があります。次の手順を使用して、CUMAに自己署名証明書を作成し、CN=portal.aipc.comでASAと交換します。これは、ASA信頼ストアにインストールする必要があります。次のステップを実行します。

1. CUMAサーバに自己署名証明書を作成します。Cisco Unified Mobility Advantage Adminポータルにサインインします。[Security Context Management]**の横にある[+]**を選択します。



「セキュリティ・コンテキスト」を選択します。「コンテキストの追加」を選択します。次の情報を入力します。

```
Do you want to create/upload a new certificate? create
Context Name "cuma"
Description "cuma"
Trust Policy "Trusted Certificates"
Client Authentication Policy "none"
Client Password "changeme"
Server Name cuma.ciscodom.com
Department Name "vsec"
Company Name "cisco"
City "san jose"
State "ca"
Country "US"
```

2. Cisco Unified Mobility Advantageから自己署名証明書をダウンロードします。この作業を行うには、次の手順を実行します。[Security Context Management]の横にある[+]を選択します。「セキュリティ・コンテキスト」を選択します。ダウンロードする証明書を保持するセキュリティ・コンテキストの横にある「コンテキストの管理」を選択します。Download Certificateを選択します。注：証明書がチェーンであり、ルート証明書または中間証明書が関連付けられている場合、チェーン内の最初の証明書だけがダウンロードされます。これは、自己署名証明書に十分です。ファイルを保存します。
3. 次の手順では、Cisco Unified Mobility AdvantageからASAに自己署名証明書を追加します。ASAで次の手順を実行します。テキストエディタでCisco Unified Mobility Advantageから自己署名証明書を開きます。Cisco適応型セキュリティアプライアンス(ASA)信頼ストアに証明書をインポートします。

```
cuma-asa(config)# crypto ca trustpoint cuma-server-id-cert
cuma-asa(config-ca-trustpoint)# enrollment terminal
cuma-asa(config-ca-trustpoint)# crypto ca authenticate
cuma-server-id-cert
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

----BEGIN CERTIFICATE----
** paste the contents from wordpad **
----END CERTIFICATE----
```

4. CUMAサーバ上のASA自己署名証明書をエクスポートします。Cisco Adaptive Security Applianceからの証明書を要求するようにCisco Unified Mobility Advantageを設定する必要が

あります。必要な自己署名証明書を提供するには、次の手順を実行します。次の手順は、ASAで実行する必要があります。新しいキーペアを生成します。

```
cuma-asa(config)# crypto key generate rsa label asa-id-key mod 1024

INFO: The name for the keys will be: asa-id-key

Keypair generation process begin. Please wait...
```

新しいトラストポイントを追加します。

```
cuma-asa(config)# crypto ca trustpoint asa-self-signed-id-cert

cuma-asa(config-ca-trustpoint)# keypair asa-id-key

cuma-asa(config-ca-trustpoint)# enrollment self
```

トラストポイントを登録します。

```
cuma-asa(config-ca-trustpoint)# crypto ca enroll asa-self-signed-id-cert
% The fully-qualified domain name in the certificate will be:
cuma-asa.cisco.com
% Include the device serial number in the subject name? [yes/no]: n
Generate Self-Signed Certificate? [yes/no]: y
```

証明書をテキストファイルにエクスポートします。

```
cuma-asa(config)# crypto ca export asa-self-signed-id-cert
identity-certificate
The PEM encoded identity certificate follows:

-----BEGIN CERTIFICATE-----

Certificate data omitted

-----END CERTIFICATE-----
```

5. 前の出力をテキストファイルにコピーし、CUMAサーバ信頼ストアに追加して、次の手順を実行します。[Security Context Management]**の横にある[+]**を選択します。「セキュリティ・コンテキスト」**を選択します**。署名付き証明書を**インポートする**セキュリティコンテキストの横にある[Manage Context]を選択します。[Trusted Certificates]**バーで[Import]**を選択します。証明書テキストを貼り付けます。証明書に名前を付けます。「インポート」**を選択します。注：リモート**接続先の設定では、携帯電話が同時に鳴るかどうかを判断するためにデスクの電話機にコールします。これにより、モバイルコネクトが動作し、リモート接続先の設定に問題がないことを確認できます。

他の証明機関にCUMA証明書要求を追加するときに問題が発生しました

問題 1

CUMC/CUMAソリューションが信頼できる証明書と連携する場合に役立つデモ/プロトタイプインストールの多くは、自己署名または他の認証局から取得されます。Verisign証明書は高価で、取得に時間がかかります。ソリューションが他のCAからの自己署名証明書と証明書をサポートしている場合は有効です。

現在サポートされている証明書は、GeoTrustおよびVerisignです。この問題は、Cisco Bug ID CSCta62971(登録ユーザ専用)に記載されています。

エラー:接続できません

https://<host>:8443などのユーザポータルページにアクセスしようとすると、「Unable to connect メッセージが表示されます。

解決方法

この問題は、Cisco Bug ID CSCsm26730(登録ユーザ専用)に記載されています。 ユーザポータルページにアクセスするには、次の回避策を実行します。

この問題の原因はドル文字であるため、管理対象サーバーの**server.xmlファイル**にドル文字が含まれている場合は、ドル文字を**エスケープします**。たとえば、/opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xmlを編集します。

インライン：**keystorePass="pa$word"** maxSpareThreads="15"

$文字を$$に置。**keystorePass="pa$$word" maxSpareThreads="**15"のように表示されます。

CUMA管理ポータルの一部のページにアクセスできません

次のページは**CUMA**管理ポータルでは表示**できません**。

- ユーザのアクティブ化/非アクティブ化
- 検索/メンテナンス

ユーザが左側のメニューの上記2つのページのいずれかをクリックすると、ブラウザはページのロードを示しているように見えますが、何も起こりません（ブラウザに表示されていた前のページだけが表示されます）。

解決方法

ユーザページに関連するこの問題を解決するには、Active Directoryに使用するポートを**3268に変更**し、CUMAを再起動します。

関連情報

- ASA-CUMAプロキシの段階的な設定
- ASR5000 v1の概要
- Cisco Unified Mobility Advantageのアップグレード
- 音声に関する技術サポート
- 音声とユニファイド コミュニケーションに関する製品サポート
- テクニカル サポートとドキュメント – Cisco Systems