目次

概要

この資料は Cisco Web セキュリティ アプライアンス（WSA）の HTTPS 復号化のために使用する必要がある認証の種類を記述したものです。

認証 外観

WSA に HTTPS 復号化と併用するため現在の認証およびプライベートキーを使用する機能があります。 ただしすべての x.509 認証がはたらかないので、使用する必要がある認証の種類についての混合があるかもしれません。

認証には 2 つの主要 な タイプがあります: **サーバ証明**および**原証明**。 すべての x.509 認証は基本制約フィールドが含まれています、認証の種類を識別する:

- **Type=End 認証対象エンティティ**-サーバ証明
- **認証対象 Type=CA** -原証明

> **注** WSA の HTTPS 復号化のためにまた認証局 （CA）署名証明書と言われる原証明を、使用して下さい。

原証明

原証明はとりわけサーバ証明に署名するために作成されます。 作成し、あなた自身の CA を操作し、あなた自身のサーバ証明に署名できます。

> **注** 原証明は他の認証だけに署名するので HTTPS 暗号化および復号化を行うために、Webサーバで使用することができません。

WSA はアクティブに HTTPS 復号化のためのサーバ証明を生成するのに原証明を使用する必要があります。 原証明 使用方法のために利用可能 な 2 つのオプションがあります:

- WSA で原証明を生成して下さい。 WSA は自身の原証明およびプライベートキーを作成し、サーバ証明に署名するためにこのキーペアを使用します。

- WSA に現在の原証明およびプライベートキーをアップロードできます。 原証明の Common Name （ CN ） フィールドはその エンティティ（ 一般的に株式会社名前 ）を信頼シグニチャが含まれているあらゆるサーバ証明識別します。

  注 サーバ証明は信頼される場合がある前に Webブラウザで現在の公開キーがある原証明によって署名する必要があります。

サーバ証明書

サーバ証明はとりわけおよび特定のサーバの信頼性を確認するために HTTPS 暗号化および復号化で使用されるために作成されます。 サーバ証明は CA 原証明の使用の CA によって署名します。 CA の一般的な例は VeriSign または Thawte です。

注 サーバ証明は他の認証に署名するために使用することができません; 従って、HTTPS 復号化はサーバ証明が WSA でインストールされている場合はたらきません。

サーバ証明の CN フィールドは認証が使用されるように意図されているホストを規定 します。 たとえば、**https://www.verisign.com は www.verisign.com** の CN とサーバ証明を使用します。

関連情報

- Web セキュリティ アプライアンス (WSA) 認証 使用方法 (HTTPS 復号化、GUI ログオン、クレデンシャル暗号化)
- WSA 及び証明書署名要求 (CSR) オプションの HTTPS プロキシを有効に するステップ
- HTTPS プロキシを有効に するステップ (WSA) 及びルート/中間認証 オプションをアップロードします
- テクニカルサポートとドキュメント - Cisco Systems