証明書とキー

証明書とキー

TLS 証明書とキーは、Multicloud Defense Gateway によってプロキシシナリオで使用されます。入力（リバースプロキシ）の場合、ユーザーは Multicloud Defense Gateway を介してアプリケーションにアクセスし、サービス用に設定された証明書を提示します。出力（転送プロキシ）の場合、外部ホストの証明書が定義された証明書によって偽装され、署名されます。

証明書本文は Multicloud Defense Controllerにインポートされます。秘密キーは、次の方法で提供できます。

- 秘密キーのコンテンツをインポートします。
- AWS シークレットマネージャに保存し、シークレット名を指定します。
- AWS KMS に保存し、暗号テキストのコンテンツを提供します。
- GCP シークレットマネージャに保存し、シークレット名を指定します。
- Azure Key Vault とシークレットに保存し、Key Vault とシークレットの名前を指定します。

テスト用に Multicloud Defense Controllerで自己署名証明書を生成することもできます。これは、ローカル ファイル システムから秘密キーのコンテンツをインポートする場合と同様です。

（注） 証明書を作成した後で編集することは**できません**。既存の証明書を置き換える必要がある場合は、新しい証明書を作成し、新しい証明書を参照するように復号プロファイルを編集してから、古い証明書を削除する必要があります。

証明書と秘密キーをインポートするときに、Multicloud Defense Controller/UI は不一致があるかどうかを検出できます。ただし、他のインポートメソッドを使用する場合に、秘密キーがクラウド サービス プロバイダー内に保存されていると、Multicloud Defense Controller/UI は不一致があるかどうかを検出できません。これは、秘密キーの秘密が維持され、クラウド サービス プロバイダー内にとどまることを保証する設計によるものです。Multicloud Defense Gateway が秘密キーを必要とする場合は、アクセスして使用します。また、不一致がある場合はエラーが生成されます。

証明書のインポート

手順

ステップ 1 **[管理（Manage）] > [セキュリティポリシー（Security Policies）] > [証明書（Certificates）]**に移動します。
ステップ 2 [作成（Create）] をクリックします。
ステップ 3 [方法（Method）] のプロンプトが表示されたら、[証明書と秘密キーのインポート（Import your Certificate and Private Key）] を選択します。
ステップ 4 [証明書本文（Certificate Body）] に証明書ファイルの内容をコピーします。これには、証明書とチェーンを含めることができます。
ステップ 5 [証明書の秘密キー（Certificate Private Key）] に秘密キーの内容をコピーします。
ステップ 6 （任意）証明書とチェーンが異なるファイルにある場合は、[証明書チェーン（Certificate Chain）] にチェーンをインポートします。
ステップ 7 [保存（Save）] をクリックします。

AWS：KMS

手順

ステップ 1 **[管理（Manage）] > [セキュリティポリシー（Security Policies）] > [証明書（Certificates）]**に移動します。
ステップ 2 [作成（Create）] をクリックします。
ステップ 3 [メソッド（Method）] で、[AWS - KMSのインポート（Import AWS - KMS）] を選択します。
ステップ 4 クラウドアカウントおよびリージョンを選択します。

ステップ 5 [証明書本文（Certificate Body）] に証明書ファイルの内容をコピーします。これには、証明書とチェーンを含めることができます。

ステップ 6 [秘密キーの暗号テキスト（Private Key Cipher Text）] に AWK KMS で暗号化された暗号テキストをコピーします。。

ステップ 7 [保存（Save）] をクリックします。

AWS：Secrets Manager

手順

ステップ 1 **[管理（Manage）]** > **[セキュリティポリシー（Security Policies）]** > **[証明書（Certificates）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [メソッド（Method）] で、[AWS - シークレットのインポート（Import AWS - Secret）] を選択します。

ステップ 4 クラウドアカウントおよびリージョンを選択します。

ステップ 5 [証明書本文（Certificate Body）] に証明書ファイルの内容をコピーします。これには、証明書とチェーンを含めることができます。

ステップ 6 秘密キーが保存されているシークレット名を入力します。秘密キーの内容は、AWS Secrets Manager で [その他のタイプのシークレット（Other type of Secrets）]、[プレーンテキスト（Plain Text）] として保存する必要があります。

ステップ 7 [保存（Save）] をクリックします。

Azure Key Vault

手順

ステップ 1 **[管理（Manage）]** > **[セキュリティポリシー（Security Policies）]** > **[証明書（Certificates）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [メソッド（Method）] で、[Azure - Key Vaultシークレットのインポート（Import Azure - Key Vault Secret）] を選択します。

ステップ 4 クラウドアカウントおよびリージョンを選択します。

ステップ 5 [証明書本文（Certificate Body）] に証明書ファイルの内容をコピーします。これには、証明書とチェーンを含めることができます。

ステップ 6 秘密キーが保存されている Key Vault 名とシークレット名を入力します。

ステップ 7 [保存（Save）] をクリックします。

GCP：Secret Manager

手順

ステップ 1 **[管理（Manage）]** > **[セキュリティポリシー（Security Policies）]** > **[証明書（Certificates）]**に移動します。
ステップ 2 [Create] をクリックします。
ステップ 3 [メソッド（Method）] で、[GCP - シークレットのインポート（Import GCP - Secret）] を選択します。
ステップ 4 クラウドアカウントを選択します。
ステップ 5 シークレット名（フルパス）とシークレットのバージョンを入力します。
ステップ 6 [証明書本文（Certificate Body）] に証明書ファイルの内容をコピーします。これには、証明書とチェーンを含めることができます。
ステップ 7 [保存（Save）] をクリックします。

サーバー証明書の検証

ゲートウェイが転送プロキシとして機能する場合、サーバー証明書の検証は自動的にトラフィック処理に含まれます。サーバー証明書の検証**アクション**の指定は、トラフィックの処理に必須ではありませんが、セキュリティ全般を向上させることができます。デフォルトでは、サーバー証明書の検証は有効ではなく、サーバー証明書が無効な可能性があるサーバーへのトラフィックは通過します。サーバー証明書の検証アクションを有効にして、許可しないトラフィック、またはサーバー証明書の検証状態を問わず信頼する必要がある特定のトラフィックに関するルールに優先順位を付けます。

（注） この検証プロセスは、転送プロキシ環境で、**復号**が有効になっている場合に**のみ**適用されます。

一般的なルールアクションの場合は、主に TLS 復号プロファイルでサーバー証明書の検証アクションを有効にすることをお勧めします。TLS 復号の選択をオーバーライドする必要がある場合は、 FQDN サービスオブジェクトを変更して検証アクションを有効にすることができます。次の 2 つの方法で、サーバー証明書の検証を有効にできます。

- TLS 復号プロファイルでのサーバー証明書の検証
- FQDN サービスオブジェクトでのサーバー証明書の検証

TLS 復号プロファイルでのサーバー証明書の検証

TLS復号プロファイル内のサーバー証明書の検証アクションを選択すると、この復号プロファイルを使用するすべてのルールセットでこのアクションが使用されます。デフォルトでは、検証アクションは、サーバー証明書が有効かどうかに関係なくすべてのトラフィックを許可するように設定されており、 Multicloud Defense は HTTP ログ内にアラートを生成しません。

（注） 検証チェックの [記録（Log）] を有効にする場合、ログは**[調査（Investigate）] > [フロー分析（Flow Analytics）] > [HTTPSログ（HTTPS Logs）]**に配置してください。

TLS 復号プロファイルでサーバー証明書の検証を有効にするには、次の手順を実行します。

手順

ステップ 1 Multicloud Defense Controller から、**[管理（Manage）] > [プロファイル（Profiles）] > [復号（Decryption）]** に移動します。

ステップ 2 サーバー証明書の検証を追加する TLS 復号プロファイルを選択します。プロファイルが用意できていない場合は、ここで作成します。詳細については、復号プロファイルを参照してください。

ステップ 3 [編集（Edit）] をクリックして復号プロファイルを編集します。

ステップ 4 [プロファイルのプロパティ（Profile Properties）] セクションで、[無効なサーバー証明書アクション（Invalid Server Certificate Action）] ドロップダウンを展開します。

ステップ 5 次のオプションのいずれかを選択します。

- [拒否/ログ（Deny Log）]：このオプションは、検証済みのサーバー証明書を提供しない接続を自動的にドロップし、インシデントをログに記録します。
- [拒否/ログなし（Deny No Log）]：このオプションは、検証済みのサーバー証明書を提供しない接続を自動的にドロップし、インシデントをログに記録**しません**。
- [許可/ログ（Allow Log）]：このオプションは、検証済みのサーバー証明書を提供しない接続の通過を許可し、インシデントをログに記録します。
- [許可/ログなし（Allow No Log）]：このオプションは、検証済みのサーバー証明書を提供しない接続の通過を許可し、インシデントをログに記録**しません**。これはデフォルトで選択されているアクションです。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

TLS 復号プロファイルが転送プロキシ サービス オブジェクトに正しく関連付けられていることを確認します。詳細については、転送サービスオブジェクト（出力/East-West）を参照してください。

TLS復号プロファイルがサービスオブジェクトに含まれたら、ポリシー内のルールの順序が、希望するトラフィックの処理方法に対応するように順序付けされていることを確認します。

FQDN サービスオブジェクトでのサーバー証明書の検証

FQDN サービスオブジェクト内の**無効なサーバー証明書の検証**は任意です。これを指定すると、TLS 復号プロファイルで指名された動作が上書きされます。ここで選択を指定しない場合、追加のアクションまたは上書きアクションは実行されません。FQDNサービスオブジェクト内の無効なサーバー証明書の検証を使用することで、TLS復号プロファイルによってブロックまたは許可されていた可能性のある特定のサーバーのトラフィックをブロックまたは許可できます。

検証チェックの [記録（Log）] を有効にする場合、これらのログは**[調査（Investigate）] > [フロー分析（Flow Analytics）] > [HTTPSログ（HTTPS Logs）]**に配置されることに注意してください。

FQDNサービスオブジェクトのサーバー証明書の検証アクションを含めるには、次の手順を実行します。

手順

ステップ 1 Multicloud Defense Controller から、**[管理（Manage）] > [セキュリティプロファイル（Security Profile）] > [FQDNs]**に移動します。

ステップ 2 変更する FQDN サービスオブジェクトを選択します。

ステップ 3 選択した FQDN サービスオブジェクトを [編集（Edit）] します。

ステップ 4 ルールセットに含まれる FQDN サービスオブジェクトのリストで、[無効なサーバー証明書のアクション（Invalid Server Certificate Action）] ドロップダウンメニューを展開し、次のいずれかのオプションを選択します。

- [拒否/ログ（Deny Log）]：検証済みのサーバー証明書を提供しない接続を自動的にドロップし、インシデントをログに記録します。
- [拒否/ログなし（Deny No Log）]：検証済みのサーバー証明書を提供しない接続を自動的にドロップし、インシデントをログに記録**しません**。
- [許可/ログ（Allow Log）]：検証済みのサーバー証明書を提供しない接続の通過を許可し、インシデントをログに記録します。
- [許可/ログなし（Allow No Log）]：検証済みのサーバー証明書を提供しない接続の通過を許可し、インシデントをログに記録**しません**。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

FQDN サービスオブジェクトがルールまたはルールセットに正しく関連付けられていることを確認します。詳細については、ルールセットとルールセットグループを参照してください。

FQDN サービスオブジェクトがポリシーのルールまたはルールセットに正常に関連付けられたら、ポリシー内のルールの順序が、希望するトラフィックの処理方法に対応するように順序付けされていることを確認します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。