リモートアクセス VPN の移行

AAA サーバーキーの取得の自動化

Firewall 移行ツール 3.0 は、ローカルユーザー、Radius、および Live Connect ASA の LDAP/LDAPS/AD サーバーに使用されるキーの取得を自動化するか、または **more system: running-config** コマンドをアップロードする場合。また、すべてのキーを手動で取得し、**[確認と検証（Review and Validate）] > [リモートアクセス （Remote Access VPN）]** の下の [AAA] セクションに入力することもできます。

ASA 構成からのクリアテキスト形式での AAA サーバーキーの取得

始める前に

ASA では、構成したキーは暗号化されたハッシュとして保存されます。ただし、*showrun* コマンドを使用すると、実行構成でキーがクリアテキストで表示されることはありません。キーは、ローカルユーザー、Radius と LDAP、LDAPS、または AD サーバーに使用されます。クリアテキスト形式でキーを取得するには、次の手順を実行します。

手順

ステップ 1 SSH コンソールを介して ASA に接続します。

ステップ 2 *more system:running-config* コマンドを入力します。

ステップ 3 **aaa-server and local user** セクションに移動してクリアテキスト形式のすべての AAA 構成と対応するキー値を見つけます。

```
ciscoASA#more system:running-config

!

aaa-server Test-RADIUS (inside) host 2.2.2.2

 key <key in clear text>     <-----The radius key is now displayed in clear text format.

aaa-server Test-LDAP (inside) host 3.3.3.3

ldap-login-password <クリアテキストのパスワード> <-----LDAP/AD/LDAPS パスワードがクリアテキスト形式で表示されるようになりました。

username Test_User password <Password in clear text> <-----The Local user
        password is shown in clear text.
```

（注） ローカルユーザーのパスワードが暗号化されている場合は、パスワードを内部で確認するか、または Firewall 移行ツールで新しいパスワードを構成できます。

ASA からの PKI 証明書のエクスポートと管理センターへのインポート

始める前に

リモートアクセス VPN には、次の証明書が必要です。

- グローバル SSL プロトコル
- IKEv2 プロトコル
- インターフェイス証明書
- SAML

ASAASA では、トラストポイントモデルを使用して、証明書を構成に保存します。トラストポイントは、証明書が保存されるコンテナです。ASAASA トラストポイントは最大2つの証明書を保存できます。

ASAASA 構成ファイルの ASAASA トラストポイントまたは証明書にはハッシュ値が含まれています。したがって、それらを管理センターに直接インポートすることはできません。

インポート先の管理センターで、移行前アクティビティの一環として、ASAASA トラストポイントまたは VPN 証明書を PKI オブジェクトとして手動で移行します。

手順

ステップ 1 次のコマンドを使用し、CLI を介してインポート元の ASAASA 構成から PKI 証明書をキーとともに PKCS12 ファイルにエクスポートします。

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

ステップ 2 PKI 証明書を管理センターにインポートします（[オブジェクト管理（Object Management）] [PKI オブジェクト（PKI Objects）]。

詳細については、『Firewall Management Center Configuration Guide』[英語] を参照してください。

手動で作成した PKI オブジェクトは、[リモートアクセス VPN（Remote Access VPN）] の [トラストポイント（Trustpoint ）] セクションにある [確認と検証（Review and Validate ）] ページの Firewall 移行ツールで使用できるようになりました。

AnyConnect パッケージとプロファイルの取得

AnyConnectプロファイルはオプションであり、管理センターまたはFirewall移行ツールを介してアップロードできます。

始める前に

- 管理センターのリモートアクセス VPN には、1 つ以上の AnyConnect パッケージが必要です。
- 構成が Hostscan と外部ブラウザパッケージで構成されている場合は、これらのパッケージをアップロードする必要があります。
- 移行前のアクティビティの一環として、すべてのパッケージを管理センターに追加する必要があります。
- Dap.xml と Data.xml は、Firewall 移行ツールを介して追加する必要があります。

手順

ステップ 1 次のコマンドを使用して、必要なパッケージを送信元 ASA から FTP または TFTP サーバーにコピーします。

```
Copy <source file location:/source file name> <destination>
ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Example
 of copying Anyconnect Package.
ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Example
 of copying External Browser Package.
ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Example of copying
Hostscan Package.
ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Example of copying Dap.xml
```

```
ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Example of copying Data.xml
ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Example of copying Anyconnect
Profile.
```

ステップ 2 ダウンロードしたパッケージを管理センターにインポートします（**[オブジェクト管理（Object Management）] > [VPN] > [AnyConnect ファイル（AnyConnect File）]**）。

1. Dap.xml と Data.xml は、**[確認と検証（Review and Validate）] > [リモートアクセス VPN（Remote Access VPN）] > [AnyConnect ファイル（AnyConnect File）]** セクションの Firewall 移行ツールから管理センターにアップロードする必要があります。
2. AnyConnect プロファイルは、管理センターに直接アップロードするか、または **[確認と検証（Review and Validate）] > [リモートアクセス VPN（Remote Access VPN）] > [AnyConnect ファイル（AnyConnect File）]** セクションの Firewall 移行ツールを介してアップロードできます。

手動でアップロードされたファイルが Firewall 移行ツールで使用できるようになりました。

ドメインと AD プライマリドメインの取得

暗号化が LDAPS に設定されている AAA サーバーの場合、ASA は IP とホスト名またはドメインをサポートしますが、管理センターはホスト名またはドメインのみをサポートします。ASA 構成にホスト名またはドメインが含まれている場合、それらが取得されて表示されます。ASA 構成に LDAPS の IP アドレスが含まれている場合は、[リモートアクセス VPN（Remote Access VPN）] の下の [AAA] セクションにドメインを入力します。AAA サーバーの IP アドレスに解決できるドメインを入力する必要があります。

タイプが AD の AAA サーバー（サーバータイプは ASA 構成で Microsoft）の場合、[AD プライマリドメイン（AD Primary Domain）] は管理センターで構成する必須フィールドです。このフィールドは ASA では個別に構成されず、ASA の LDAP-base-dn 構成から抽出されます。

```
If the ldap-base-dn is: ou=Test-Ou,dc=gcevpn,dc=com
```

[AD プライマリドメイン（AD Primary Domain）] は、プライマリドメインを形成する dc、dc=gcevpn、dc=com で始まるフィールドです。AD プライマリドメインは gcevpn.com になります。

LDAP-base-dn のサンプルファイル：

```
cn=asa,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:
```

ここで、dc=abc と dc=com が abc.com として結合され、AD プライマリドメインが形成されます。

```
cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:
```

AD プライマリドメインは fwsecurity.cisco.com です。

AD プライマリドメインは自動的に取得され、Firewall 移行ツールに表示されます。

リモートアクセス VPN の移行

（注） AD プライマリドメインの値は、レルムオブジェクトごとに一意である必要があります。競合が検出された場合か、または Firewall 移行ツールが ASA 構成で値を見つけられない場合は、特定のサーバーの AD プライマリドメインを入力するように求められます。AD プライマリドメインを入力して構成を検証します。

リモートアクセス VPN の移行