ASA 8.x： グループ エイリアスとグループ URL メソッドを使った、WebVPN ログイン時のグループ選択

目次

概要

SSL VPN ユーザ（AnyConnect/SVC およびクライアントレスの両方）は、次の異なるメソッドを使用して、アクセスするトンネル グループ [Adaptive Security Device Manager（ASDM）の接続プロファイルの用語] を選択できます。

- group-url
- group-alias（ログイン ページのトンネル グループ ドロップダウン リスト）
- certificate-maps（証明書を使用する場合）

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）を設定して、ユーザが WebVPN サービスにログインする際にドロップダウン メニューからグループを選択できるようにする方法を示します。 メニューに表示されるグループは、ASA に設定されている実際の接続プロファイル（トンネル グループ）のエイリアスまたは URL のいずれかです。 このドキュメントでは、接続プロファイル（トンネル グループ）のエイリアスと URL を作成し、表示するドロップダウン メニューを設定する方法を説明します。 この設定は、ソフトウェア バージョン 8.0(2) が稼働している ASA 上の ASDM 6.0(2) を使用して実行されます。

注: ASA バージョン 7.2.x は 2 つのメソッドをサポートします: グループ URL およびグループ エイリアス リスト。

注: ASA バージョン 8.0.x は 3 つのメソッドをサポートします: グループ URL、グループ エイリアスおよび認証 MAP。

前提条件

基本的な WebVPN 設定

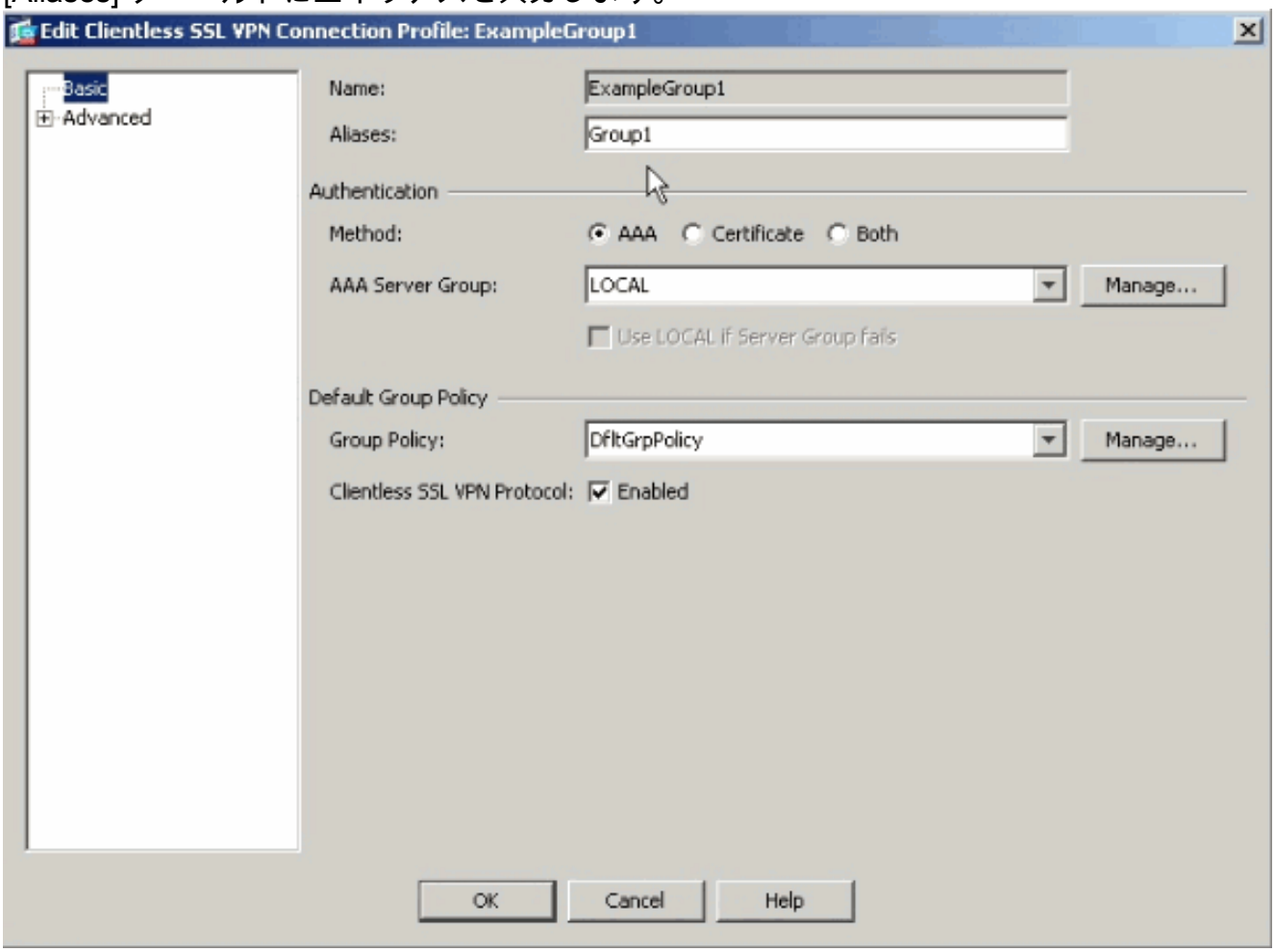
エイリアスの設定およびドロップダウンの有効化

このセクションでは、接続プロファイル（トンネル グループ）のエイリアスを設定し、それらのエイリアスが WebVPN ログイン ページの [Group] ドロップダウン メニューに表示されるように設定するための情報を提供しています。

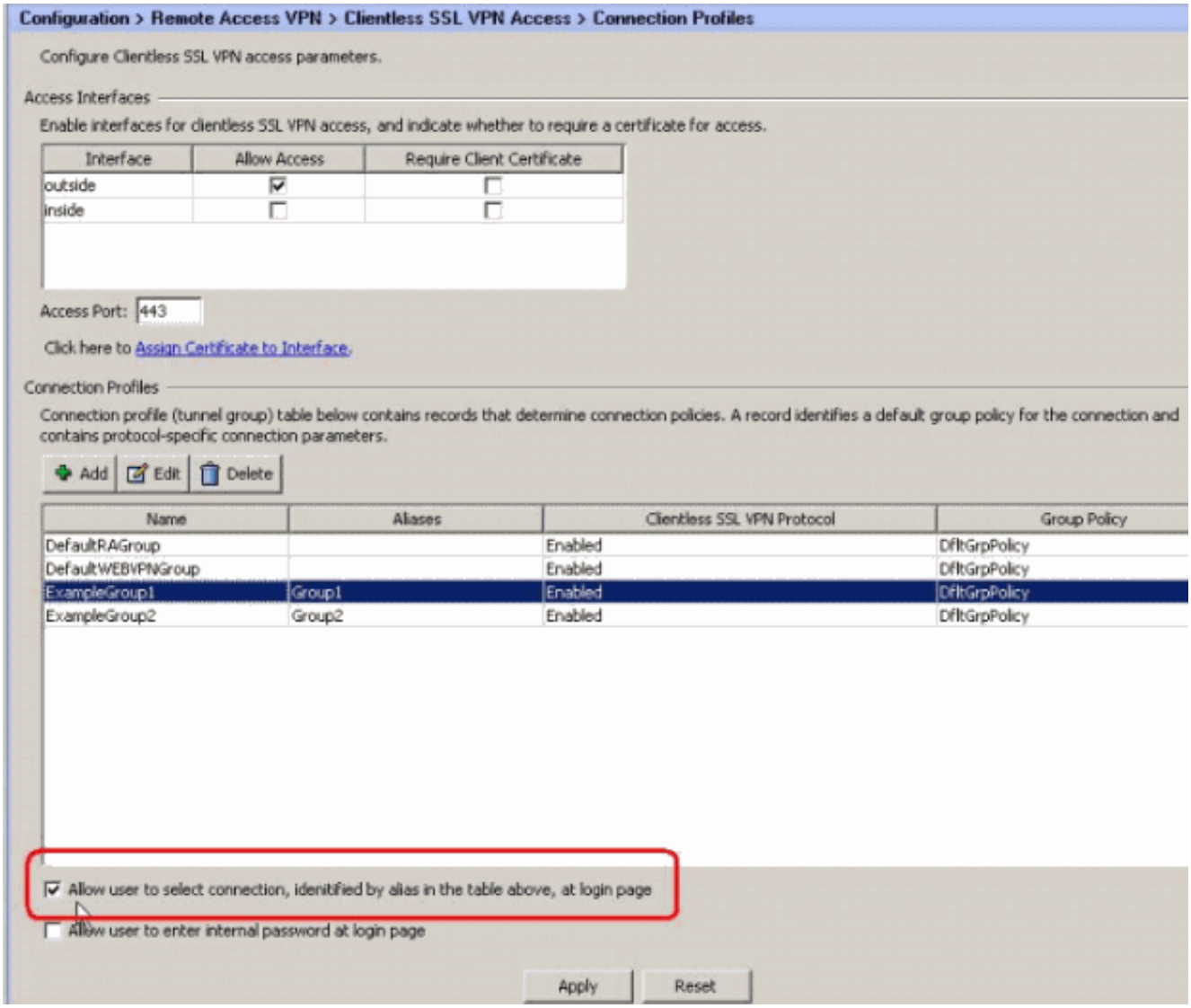
ASDM

ASDM で接続プロファイル（トンネル グループ）のエイリアスを設定するには、次の手順を実行します。 エイリアスを設定するグループごとに、必要に応じて同じ手順を繰り返します。

1. [Configuration] > [Clientless SSL VPN Access] > [Connection Profiles] の順に選択します。
2. 接続プロファイルを選択し、[Edit] をクリックします。
3. [Aliases] フィールドにエイリアスを入力します。



4. [OK] をクリックして変更を**適用**します。
5. [Connection Profiles] ウィンドウで [Allow user to select connection, identified by alias in the table above, at login page] にチェックマークを入れます。



CLI

コマンド ラインで次の各コマンドを使用して接続プロファイル（トンネル グループ）のエイリアスを設定し、トンネル グループ ドロップダウンを有効にします。 エイリアスを設定するグループごとに、必要に応じて同じ手順を繰り返します。

```
ciscoasa#configure terminal ciscoasa(config)#tunnel-group ExampleGroup1 webvpn-att
ciscoasa(config-tunnel-webvpn)#group-alias Group1 enable ciscoasa(config-tunnel-webvpn)#exit
ciscoasa(config)#webvpn ciscoasa(config-webvpn)#tunnel-group-list enable
```

URL の設定およびドロップダウンの有効化

このセクションでは、接続プロファイル（トンネル グループ）の URL を設定し、それらの URL が WebVPN ログイン ページの [Group] ドロップダウン メニューに表示されるように設定するための情報を提供しています。 group-url を使用すると、group-alias メソッド（グループ ドロップダウン）の場合と異なり、グループ名を公開しないでよいという利点があります。

ASDM

ASDM でグループ URL を指定するには次の 2 つの方法を使用できます。

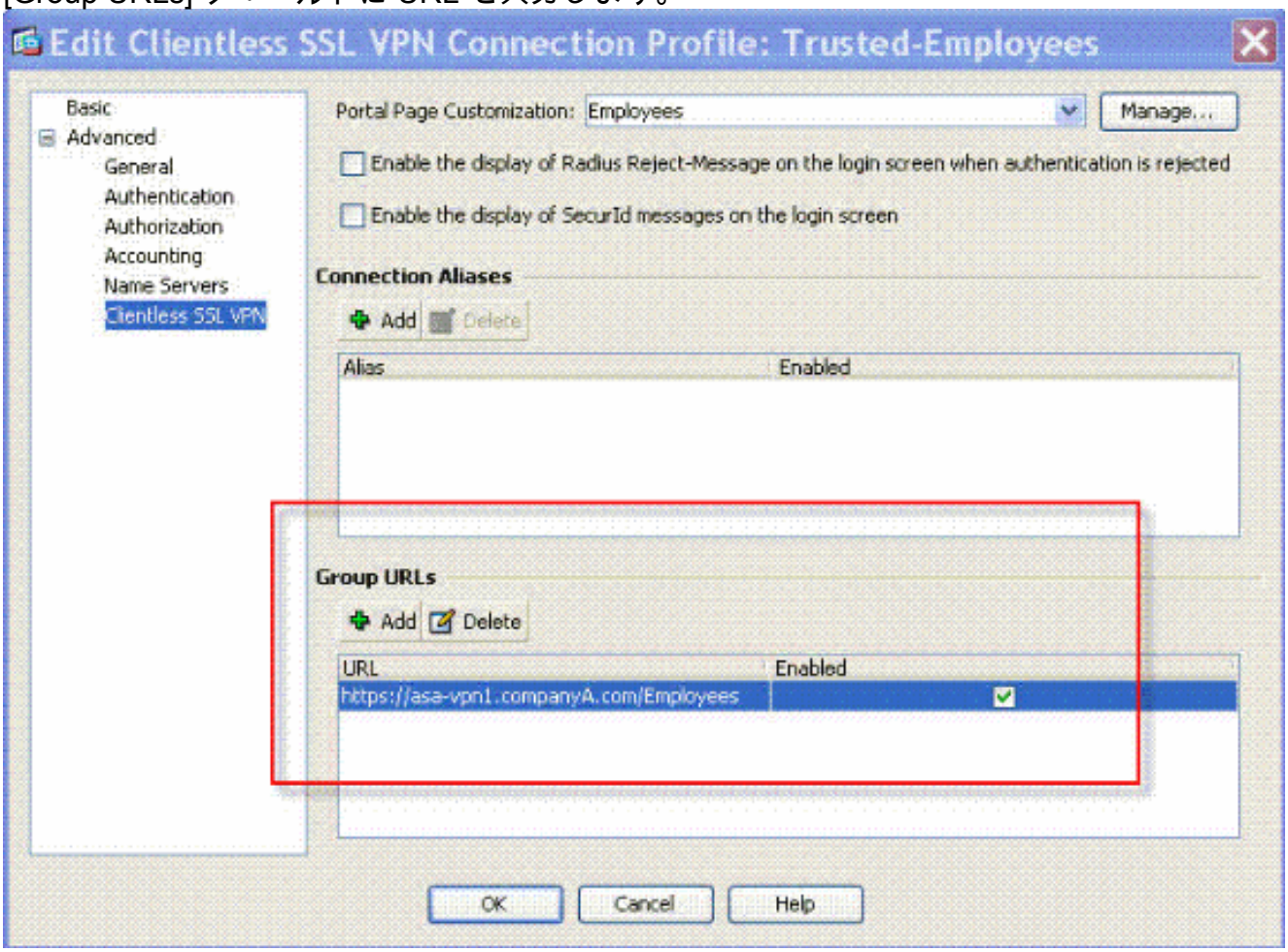
- プロファイルを使用する方法：完全に動作可能AC プロファイルを編集し、[<HostAddress>]

フィールドを変更します。Windows 2000/XP では、デフォルトのプロファイル ファイル（たとえば、CiscoAnyConnectProfile.xml）は、 C:\Documents and Settings\All ユーザ\適用業務 データ\ Cisco \ Cisco AnyConnect VPN Client \プロファイル。Vista の場所は少し異なり、 C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile です。

- [Connect To] フィールドにグループ URL 文字列を入力します。グループ URL 文字列は、次の 3 つの形式がサポートされています。https://asa-vpn1.companyA.com/Employeesasa-vpn1.companyA.com/Employeesasa-vpn1.companyA.com（ドメインのみ、パスはなし）

ASDM で接続プロファイル（トンネル グループ）の URL を設定するには、次の手順を実行します。 URL を設定するグループごとに、必要に応じて同じ手順を繰り返します。

1. [Configuration] > [Clientless SSL VPN Access] > [Connection Profiles] > [Advanced] > [Clientless SSL VPN] パネルの順に選択します。
2. 接続プロファイルを選択し、[Edit] をクリックします。
3. [Group URLs] フィールドに URL を入力します。



4. [OK] をクリックして変更を**適用**します。

CLI

コマンド ラインで次の各コマンドを使用して接続プロファイル（トンネル グループ）の URL を設定し、トンネル グループ ドロップダウンを有効にします。 URL を設定するグループごとに、必要に応じて同じ手順を繰り返します。

```
ciscoasa#configure terminal ciscoasa(config)#tunnel-group Trusted-Employees type remote-access
ciscoasa(config)#tunnel-group Trusted-Employees general-attributes
ciscoasa(config)#authentication-server-group (inside) LDAP-AD11 ciscoasa(config)#accounting-
server-group RadiusACS12 ciscoasa(config)#default-group-policy Employees
```

```
ciscoasa(config)#tunnel-group Trusted-Employees webvpn-attributes ciscoasa(config)#group-url
https://asa-vpn1.companyA.com/Employees enable ciscoasa(config)#webvpn ciscoasa(config-
webvpn)#tunnel-group-list enable
```

Q&A

質問：

ASA VPN ゲートウェイが NAT デバイスの背後にある場合、group-url をどのように設定しますか。

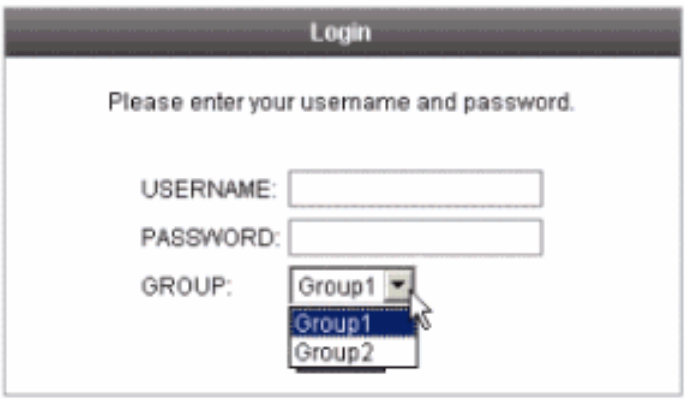
回答：

ユーザが入力するホスト/URL はグループ マッピングに使用されます。 そのため、ASA の外部インターフェイスの実際のアドレスではなく、NAT のアドレスを使用する必要があります。 これに代わる最適な方法は、group-url マッピングに IP アドレスではなく FQDN を使用することです。

すべてのマッピングは (ブラウザが送信する情報に基づいて) HTTP プロトコル レベルで実装され、URL は着信 HTTP ヘッダーの情報をマップ元とするように構成されます。 ホスト名または IP はホスト ヘッダーから取得され、URL の残りの部分は HTTP の要求行から取得されます。 これは、ユーザが入力するホスト/URL がグループ マッピングに使用されることを意味します。

確認

ASA の WebVPN ログイン ページに移動して、ドロップダウンが有効でエイリアスが表示されていることを確認します。



ASA の WebVPN ログイン ページに移動して、ドロップダウンが有効で URL が表示されていることを確認します。

トラブルシューティング

- ドロップダウン リストが表示されない場合、ドロップダウン リストを有効にしてエイリアスを設定したことを確認します。 どちらか一方を行い、もう一方を行っていないことがよくあります。
- ASA のベース URL に接続していることを確認します。 group-url の目的はグループ選択を行うことであるため、group-url を使用して ASA に接続している場合、ドロップダウン リストは**表示されません**。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- テクニカルサポートとドキュメント - Cisco Systems