ASA 8.x: Allow Users to Select a Group at WebVPN Login via Group-Alias and Group-URL Method

Contents

Introduction

SSL VPN users (both AnyConnect/SVC and Clientless) can choose which tunnel group [Connection Profile in Adaptive Security Device Manager (ASDM) lingo] to access using these different methods:

- group-url
- group-alias (tunnel group drop-down list on login page)
- certificate-maps, if using certificates

This document demonstrates how to configure the Adaptive Security Appliance (ASA) to allow users to select a group via a drop-down menu when they login to the WebVPN service. The groups that appear in the menu are either aliases or URLs of real connection profiles (tunnel groups) configured on the ASA. This document illustrates how to create aliases and URLs for connection profiles (tunnel groups) and then configure the drop-down to appear. This configuration is performed using ASDM 6.0(2) on an ASA running software version 8.0(2).

Note: ASA version 7.2.x supports two methods: group-url and group-alias list.

Note: ASA version 8.0.x supports three methods: group-url, group-alias, and certificate-maps.

Prerequisites

Basic WebVPN configuration

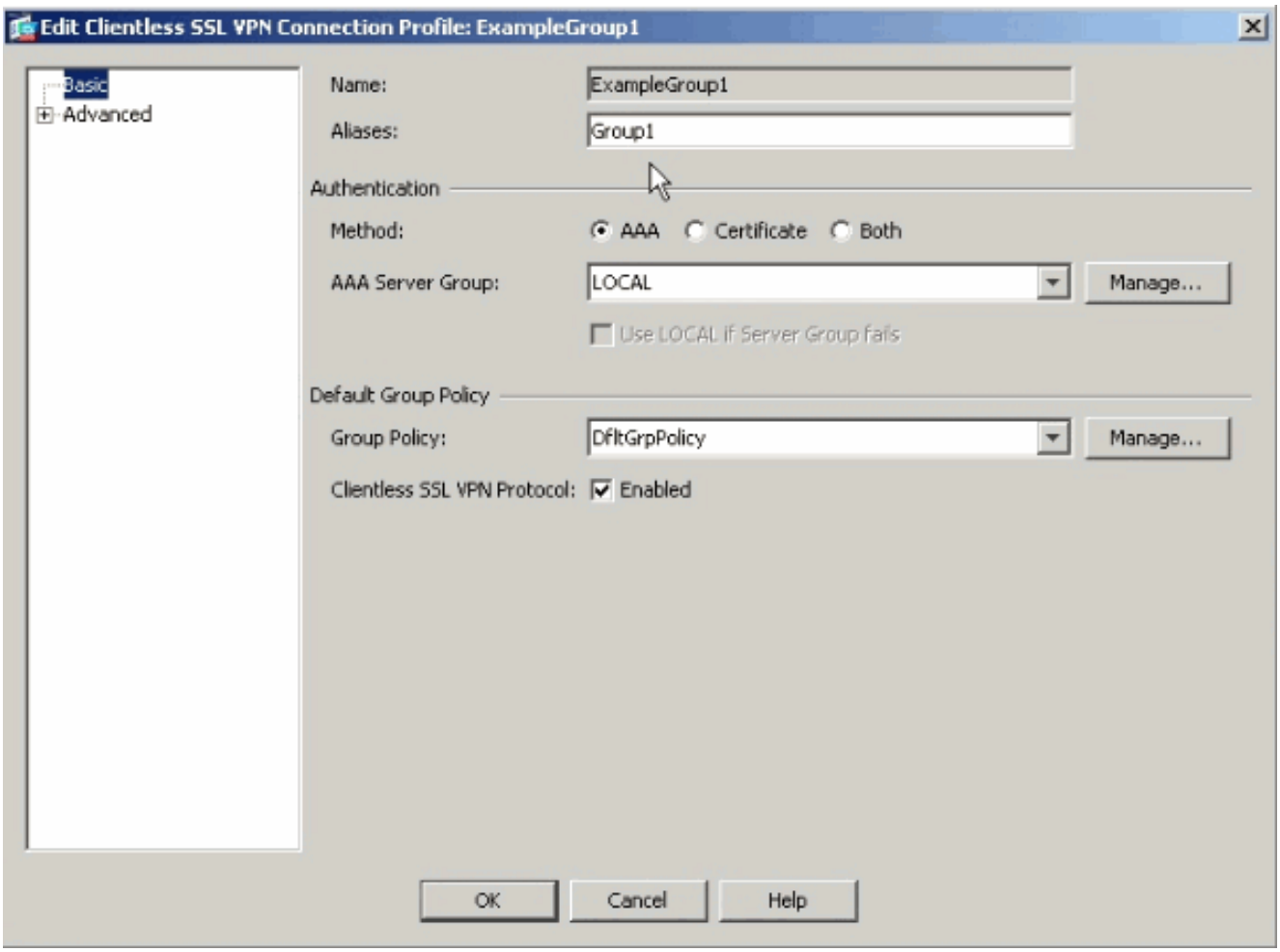
Configure an Alias and Enable the Drop-down

In this section, you are presented with the information to configure an alias for a connection profile (tunnel group) and then configure those aliases to appear in the Group drop-down menu on the WebVPN login page.

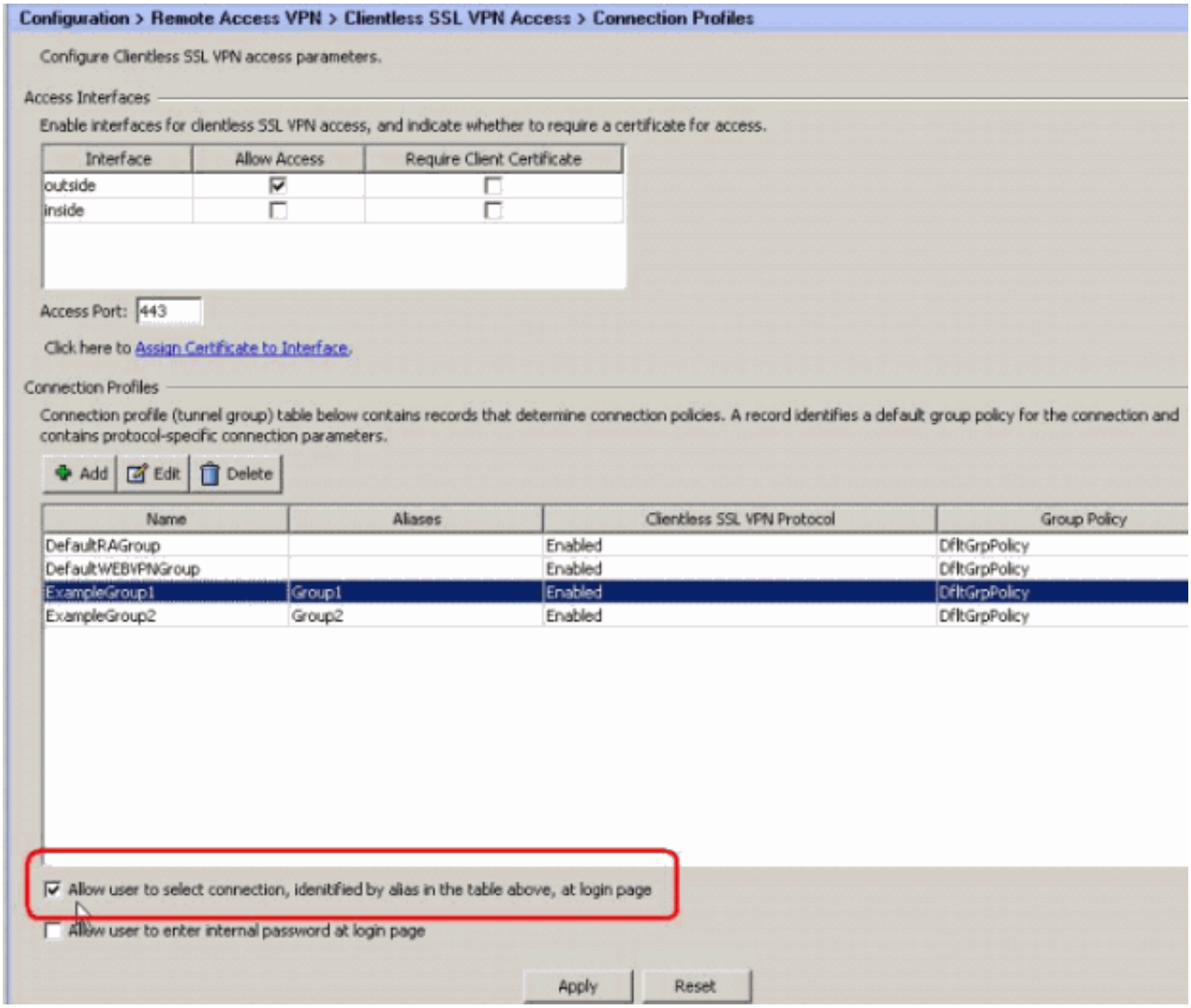
ASDM

Complete these steps in order to configure an alias for a connection profile (tunnel group) in the ASDM. Repeat as necessary for each group for which you want to configure an alias.

1. Choose **Configuration > Clientless SSL VPN Access > Connection Profiles**.
2. Select a connection profile and click **Edit**.
3. Enter an alias in the Aliases field.



4. Click **OK** and **Apply** the change.
5. In the Connection Profiles window, check **Allow user to select connection, identified by alias in the table above, at login page**.



CLI

Use these commands at the command line to configure an alias for a connection profile (tunnel group) and enable the tunnel group drop-down. Repeat as necessary for each group for which you want to configure an alias.

```
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
```

Configure a URL and Enable the Drop-down

In this section, you are presented with the information to configure a URL for a connection profile (tunnel group) and then configure those URLs to appear in the Group drop-down menu on the WebVPN login page. One advantage of using group-url over group-alias (group drop-down) is that you do not expose the group names as the latter method does.

ASDM

There are two methods used to specify the Group-URL in ASDM:

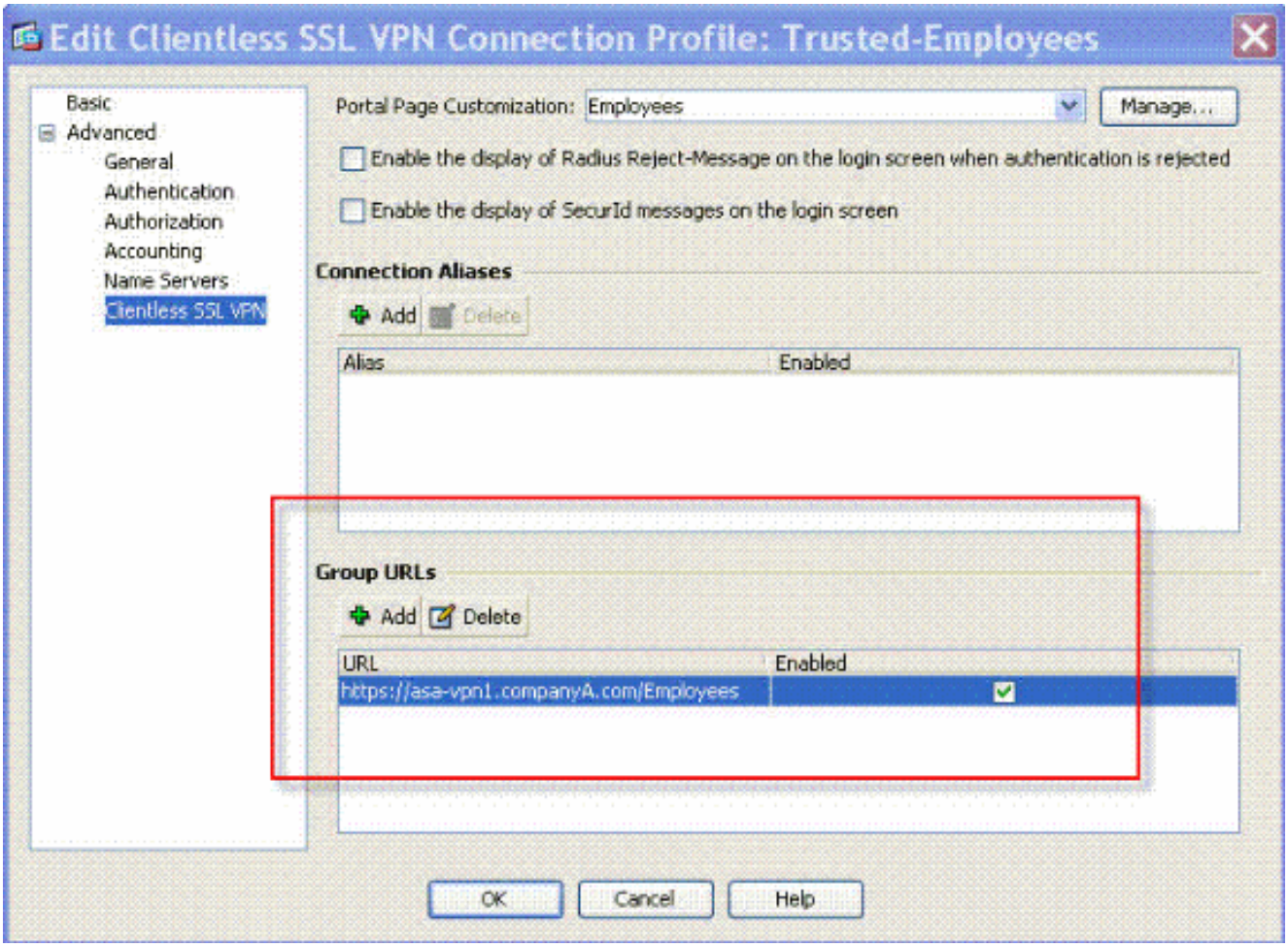
- Profile Method - fully operationalEdit the AC Profile and modify the <HostAddress> field.On

Windows 2000/XP the default profile file (for example, CiscoAnyConnectProfile.xml) is in the directory: C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile.The location for Vista is slightly different: C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile.

- Enter the group URL string in the Connect To field.Three formats of group URL strings are supported:https://asa-vpn1.companyA.com/Employeesasa-vpn1.companyA.com/Employeesasa-vpn1.companyA.com (domain-only, no path)

Complete these steps in order to configure a URL for a connection profile (tunnel group) in the ASDM. Repeat as necessary for each group for which you want to configure a URL.

1. Choose **Configuration > Clientless SSL VPN Access > Connection Profiles>Advanced>Clientless SSL VPN panel**.
2. Select a connection profile and click **Edit**.
3. Enter a URL in the Group URLs field.



4. Click **OK** and **Apply** the change.

CLI

Use these commands at the command line to configure a URL for a connection profile (tunnel group) and enable the tunnel group drop-down. Repeat as necessary for each group for which you want to configure a URL.

```
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 and A

Question:

How do you configure the group-url if the ASA VPN gateway is behind a NAT device?

Answer:

The host/URL that the user enters will be used for the group mapping. Therefore, you have to use the NAT'd address, not the actual address on the ASA's outside interface. The best alternative is to use FQDN instead of IP address for group-url mapping.

All mapping is implemented on HTTP protocol level (based on information the browser sends) and a URL is composed to map from information in incoming HTTP headers. The host name or IP is taken from the host header and the rest of the URL from the HTTP request line. This means that the host/URL the user enters will be used for the group mapping.

Verify

Navigate to the WebVPN login page of the ASA to verify that the drop-down is enabled and that the aliases appear.

Navigate to the WebVPN login page of the ASA to verify that the drop-down is enabled and that

the URL appears.

Troubleshoot

- If the drop-down list does not appear, be certain that you have enabled it and that aliases are configured. Users often do one of these things, but not the other.
- Be sure that you are connecting to the base URL of the ASA. The drop-down list **does not appear** if you connect to the ASA using a group-url, as the purpose of the group-url is to perform the group selection.

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Technical Support & Documentation - Cisco Systems**