ASA 8.x：允许用户在通过 Group-Alias 和 Group-URL 方法进行 WebVPN 登录时选择组

目录

简介

SSL VPN用户(AnyConnect/SVC和无客户端)使用这些不同的说法，能选择隧道组[Connection Profile in Adaptive Security Device Manager (ASDM) lingo]访问：

- group-url
- group-alias（登录页上的隧道组下拉列表）
- certificate-maps，如果使用证书

本文展示如何配置可适应安全工具(ASA)允许用户通过一个下拉菜单选择组，当他们登陆对WebVPN服务时。菜单中显示的组为在 ASA 上配置的实际连接配置文件（隧道组）的别名或 URL。本文档说明如何创建连接配置文件（隧道组）的别名和 URL，以及如何配置要显示的下拉菜单。在运行软件版本 8.0(2) 的 ASA 上使用 ASDM 6.0(2) 执行此配置。

注意： ASA 版本 7.2.x 支持两种方法：group-url 和 group-alias list。

注意： ASA 版本 8.0.x 支持三种方法：group-url、group-alias 和 certificate-maps。

先决条件

基本 WebVPN 配置

配置别名并启用下拉菜单

本部分提供有关如何配置连接配置文件（隧道组）的别名，以及如何配置这些别名以在 WebVPN 登录页上的“Group”下拉菜单中显示的信息。

ASDM

完成以下步骤，以在 ASDM 中配置连接配置文件（隧道组）的别名。根据需要，为要配置别名的每个组重复操作。

1. 选择 **Configuration > Clientless SSL VPN Access > Connection Profiles**。
2. 选择一个连接配置文件并单击 **Edit**。
3. 在“Aliases”字段中输入别名。
4. 单击 **OK** 并应用更改。
5. 在“Connection Profiles”窗口中，选中 **Allow user to select connection, identified by alias in the table above, at login page**。

CLI

在命令行中使用以下命令配置连接配置文件（隧道组）的别名，并启用隧道组下拉菜单。根据需要，为要配置别名的每个组重复操作。

```
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
```

配置 URL 并启用下拉菜单

本部分提供有关如何配置连接配置文件（隧道组）的 URL，以及如何配置这些 URL 以在 WebVPN 登录页上的“Group”下拉菜单中显示的信息。与 group-alias 相比，使用 group-url（组下拉菜单）的一个优点是，您不会像前一种方法那样暴露组名称。

ASDM

可使用两种方法在 ASDM 中指定 Group-URL：

- 配置文件方法 - 完全正常运行编辑 AC 配置文件并修改 <HostAddress> 字段。在 Windows 2000/XP 上，默认配置文件（例如，CiscoAnyConnectProfile.xml）位于以下目录下：C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile。对于 Vista，位置稍有不同：C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile。
- 在“Connect To”字段中输入组 URL 字符串。支持以下三种格式的组 URL 字符串：https://asa-vpn1.companyA.com/Employeesasa-vpn1.companyA.com/Employeesasa-vpn1.companyA.com（只有域，无路径）

完成以下步骤，以在 ASDM 中配置连接配置文件（隧道组）的 URL。根据需要，为要配置 URL 的每个组重复操作。

1. 选择 **Configuration > Clientless SSL VPN Access > Connection Profiles>Advanced>Clientless SSL VPN panel**。
2. 选择一个连接配置文件并单击 **Edit**。
3. 在“Group URLs”字段中输入 URL。
4. 单击 **OK** 并应用更改。

CLI

在命令行中使用以下命令配置连接配置文件（隧道组）的 URL，并启用隧道组下拉菜单。根据需要，为要配置 URL 的每个组重复操作。

```
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
```

问答

问题：

如果 ASA VPN 网关位于 NAT 设备后面，如何配置 group-url？

答案：

用户输入的主机/URL 将用于组映射。因此，必须在 ASA 的外部接口上使用 NAT'd 地址，而不是实际地址。最佳替代方法是为 group-url 映射使用 FQDN，而不是 IP 地址。

所有映射均是在 HTTP 协议级别上实施的（基于浏览器发送的信息），根据传入的 HTTP 标头中的信息组成 URL 以进行映射。主机名或 IP 取自主机标头，URL 的其余部分取自 HTTP 请求行。这意味着用户输入的主机/URL 将用于组映射。

验证

导航到 ASA 的 WebVPN 登录页，验证是否启用了下拉菜单以及是否显示别名。

导航到 ASA 的 WebVPN 登录页，验证是否启用了下拉菜单以及是否显示 URL。

故障排除

- 如果下拉列表未显示，请确保已启用该列表并配置了别名。用户常常执行了这两项操作中的一项操作，但未执行另一项。
- 确保正在连接到 ASA 的基本 URL。如果使用 group-url 连接到 ASA，则**不会显示**下拉列表，因为 group-url 的目的是执行组选择。

相关信息

- Cisco ASA 5500 系列自适应安全设备
- 技术支持和文档 - Cisco Systems