

在ASA 上配置无客户端 SSL VPN (WebVPN)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[背景信息](#)

[配置](#)

[验证](#)

[故障排除](#)

[用于排除故障的步骤](#)

[用于排除故障的命令](#)

[常见问题](#)

[用户无法登录](#)

[无法将三个以上的 WebVPN 用户连接到 ASA](#)

[WebVPN 客户端无法点击书签且显示为灰色](#)

[通过 WebVPN 进行 Citrix 连接](#)

[如何避免需要对用户进行第二次身份验证](#)

[相关信息](#)

简介

本文档介绍思科自适应安全设备 (ASA) 5500 系列的简单配置，以支持通过无客户端安全套接字层 (SSL) VPN 访问内部网络资源。无客户端 SSL 虚拟专用网络 (WebVPN) 支持从任何位置对企业网络进行有限但有价值的安全访问。用户可以随时通过浏览器安全访问企业资源。无需其他客户端即可访问内部资源。使用基于 SSL 连接的超文本传输协议提供访问。

无客户端 SSL VPN 支持从几乎任何可以访问超文本传输协议 (HTTP) 互联网站点的计算机轻松访问各种 Web 资源以及支持 Web 的应用和传统应用。包括：

- 内部网站
- Microsoft SharePoint 2003、2007 和 2010
- Microsoft Outlook Web Access 2003、2007 和 2013
- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 和 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp 版本 5 至 6.5
- Citrix XenDesktop 版本 5 至 5.6 和版本 7.5

- VMware View 4

有关受支持软件的列表，请参见[思科 ASA 5500 系列支持的 VPN 平台](#)。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 支持 SSL 的浏览器
- 7.1 或更高版本的 ASA
- 颁发给 ASA 域名的 X.509 证书
- TCP 端口 443，在从客户端到 ASA 的路径中不得阻止该端口

有关完整的要求列表，请参见[思科 ASA 5500 系列支持的 VPN 平台](#)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA 版本 9.4(1)
- 自适应安全设备管理器 (ASDM) 版本 7.4(2)
- ASA 5515-X

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

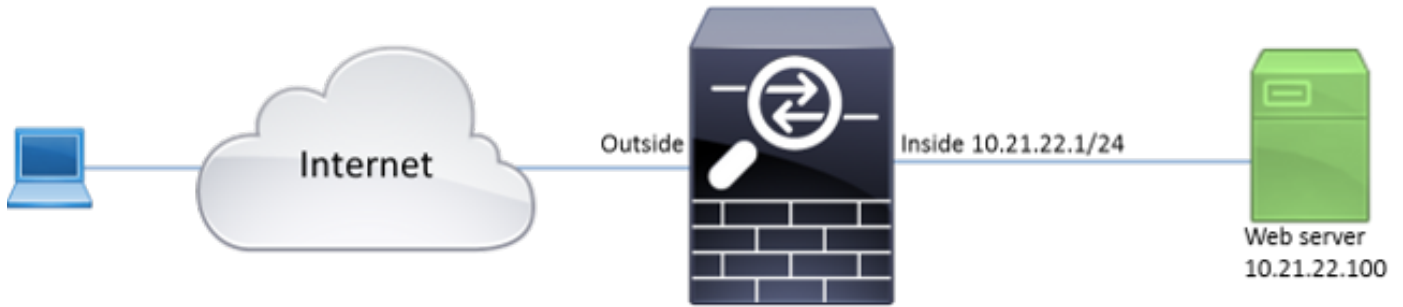
配置

本文介绍 ASDM 和 CLI 的配置过程。您可以选择使用这两种工具中的任何一种来配置 WebVPN，但某些配置步骤只能使用 ASDM 实现。

注意：使用命令[查找工具](#)(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



背景信息

WebVPN 使用 SSL 协议来保护在客户端和服务端之间传输的数据。当浏览器发起到 ASA 的连接时，ASA 会提供其证书以向浏览器验证身份。为了确保客户端和 ASA 之间的连接安全，您需要向 ASA 提供由客户端已信任的证书颁发机构签名的证书。否则，客户端将无法验证 ASA 的真实性，这可能会导致中间人攻击和用户体验不佳，因为浏览器会生成连接不受信任的警告。

注意：默认情况下，ASA 会在启动时生成自签名 X.509 证书。默认情况下，此证书用于客户端连接。不建议使用此证书，因为浏览器无法验证其真实性。此外，此证书会在每次重新启动时重新生成，因此它在每次重新启动后都会更改。

证书安装不在本文档的讨论范围内。

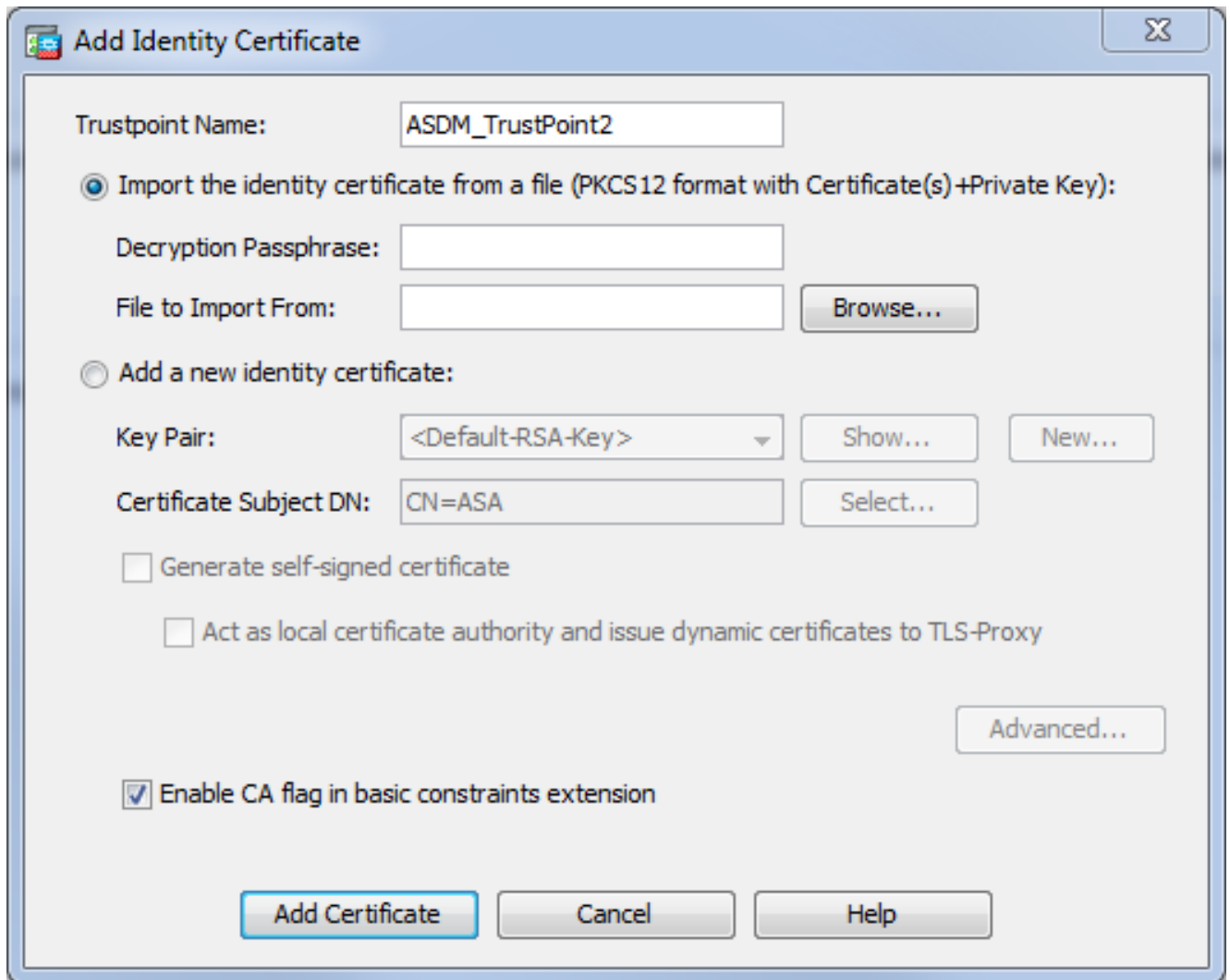
配置

在 ASA 上配置 WebVPN 包括五个主要步骤：

- 配置 ASA 将使用的证书。
- 在 ASA 接口上启用 WebVPN。
- 创建用于 WebVPN 访问的服务器和/或统一资源定位符 (URL) 列表。
- 为 WebVPN 用户创建一个组策略。
- 将这一新的组策略应用于隧道组。

注意：在版本 9.4 之后的 ASA 版本中，用于选择 SSL 密码的算法已更改（请参阅思科 ASA 系列版本说明，版本 9.4(x)）。如果只使用支持椭圆曲线加密的客户端，则对证书使用椭圆曲线私钥是安全的。否则，应使用自定义加密套件，以避免让 ASA 提供自签名临时证书。您可以将 ASA 配置为仅将基于 RSA 的密码与 `ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5"` 命令一起使用。

1. 选项 1 - 使用 pkcs12 文件导入证书。依次选择配置 > 防火墙 > 高级 > 证书管理 > 身份证书 > 添加。您可以使用 pkcs12 文件进行安装，也可以采用隐私增强型邮件 (PEM) 格式粘贴内容。



CLI :

```
ASA(config)# crypto ca import TrustPoint-name pkcs12 "password"
```

```
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJUQIBAzCCCRCGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCaggAgIIFuHFrV6enVflNv3sBBYB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x30zo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbils1ioe4Dplx1b
```

--- output ommited ---

```
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJUQIBAzCCCRCGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCaggAgIIFuHFrV6enVflNv3sBBYB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x30zo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbils1ioe4Dplx1b
```

```
quit
```

INFO: Import PKCS12 operation completed successfully

选项 2 - 创建自签名证书。依次选择配置 > 防火墙 > 高级 > 证书管理 > 身份证书 > 添加。单击 Add a new identity certificate 单选按钮。选中“生成自签名证书”复选框。选择与 ASA 的域名匹配的通用名称 (CN)。

The screenshot shows the 'Add Identity Certificate' dialog box. The 'Trustpoint Name' field contains 'ASDM_TrustPoint1'. There are two radio buttons: 'Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):' (unselected) and 'Add a new identity certificate:' (selected). Under the first option, there are fields for 'Decryption Passphrase:' and 'File to Import From:' with a 'Browse...' button. Under the second option, there is a 'Key Pair:' dropdown menu showing '<Default-RSA-Key>', a 'Show...' button, and a 'New...' button. Below that is a 'Certificate Subject DN:' field containing 'CN=ASA' and a 'Select...' button. There are two checkboxes: 'Generate self-signed certificate' (checked) and 'Act as local certificate authority and issue dynamic certificates to TLS-Proxy' (unchecked). An 'Advanced...' button is located at the bottom right. At the very bottom, there are three buttons: 'Add Certificate', 'Cancel', and 'Help'.

点击新建以创建证书的密钥对。选择密钥类型、名称和大小。

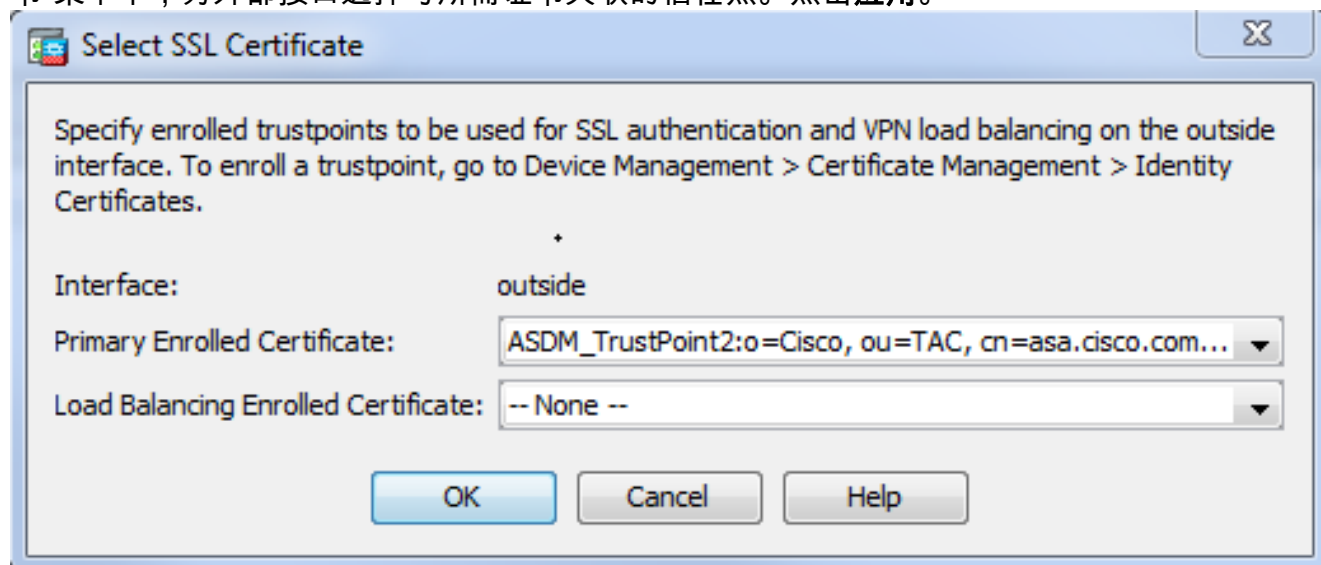
The screenshot shows the 'Add Key Pair' dialog box. The 'Key Type' has two radio buttons: 'RSA' (unselected) and 'ECDSA' (selected). Below that is a 'Name:' section with two radio buttons: 'Use default key pair name' (unselected) and 'Enter new key pair name:' (selected). The 'Enter new key pair name:' field contains 'ECDSA_KEYPAIR'. Below that is a 'Size:' dropdown menu showing '384'. At the bottom, there are three buttons: 'Generate Now', 'Cancel', and 'Help'. The 'Generate Now' button is highlighted in blue.

CLI :

```
ASA(config)# crypto key generate ecdsa label ECDSA_KEYPAIR noconfirm
```

```
ASA(config)# crypto ca trustpoint TrustPoint1
ASA(config-ca-trustpoint)# revocation-check none
ASA(config-ca-trustpoint)# id-usage ssl-ipsec
ASA(config-ca-trustpoint)# no fqdn
ASA(config-ca-trustpoint)# subject-name CN=ASA
ASA(config-ca-trustpoint)# enrollment self
ASA(config-ca-trustpoint)# keypair ECDSA_KEYPAIR
ASA(config-ca-trustpoint)# exit
ASA(config)# crypto ca enroll TrustPoint1 noconfirm
```

2. 选择将用于 WebVPN 连接的证书。依次选择配置 > 远程接入 VPN > 高级 > SSL 设置。在“证书”菜单中，为外部接口选择与所需证书关联的信任点。点击应用。



等效 CLI 配置：

```
ASA(config)# ssl trust-point
```

3. (可选) 启用域名服务器 (DNS) 查找。WebVPN 服务器充当客户端连接的代理。这意味着 ASA 会代表客户端创建与资源的连接。如果客户端需要连接到使用域名的资源，则 ASA 需要执行 DNS 查找。依次选择配置 > 远程接入 VPN > DNS。至少配置一台 DNS 服务器，并在面向 DNS 服务器的接口上启用 DNS 查找。

Configuration > Remote Access VPN > DNS

Specify how to resolve DNS requests.

DNS Setup

Configure one DNS server group Configure multiple DNS server groups

Primary DNS Server:

Secondary Servers:

+

Domain Name:

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
inside	True
outside	False

DNS Guard

This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.

Enable DNS Guard on all interfaces.

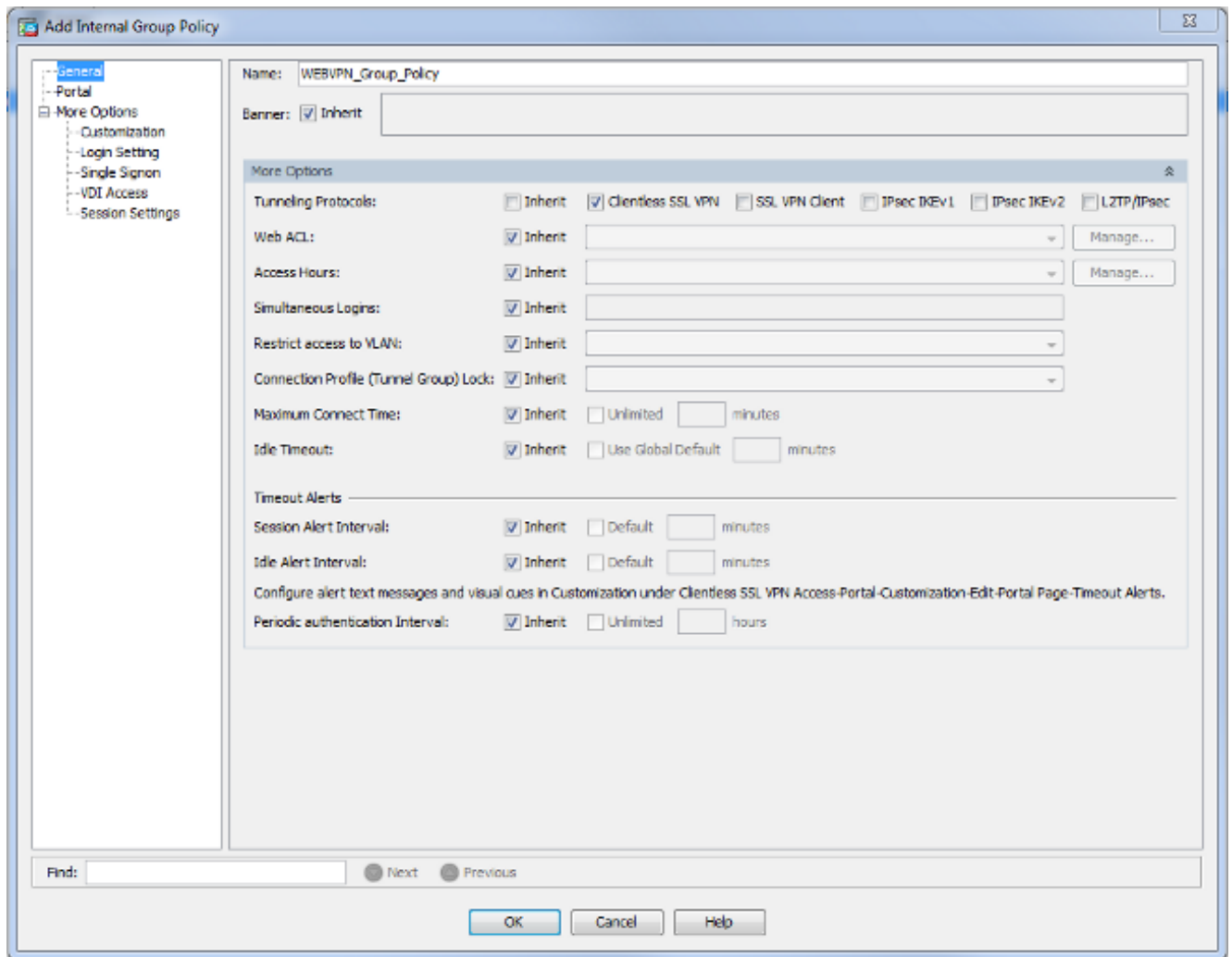
CLI :

```
ASA(config)# dns domain-lookup inside
```

```
ASA(config)# dns server-group DefaultDNS
```

```
ASA(config-dns-server-group)# name-server 10.11.12.101
```

4. (可选) 为 WebVPN 连接创建组策略。依次选择配置 > 远程接入 VPN > 无客户端 SSL VPN 访问 > 组策略 > 添加内部组策略。在“常规选项”下，将“隧道协议”值更改为“无客户端 SSL VPN”。



CLI :

```
ASA(config)# group-policy WEBVPN_Group_Policy internal
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# vpn-tunnel-protocol ssl-clientless
```

5. 配置连接配置文件。在 ASDM 中，依次选择配置 > 远程接入 VPN > 无客户端 SSL VPN 访问 > 连接配置文件。

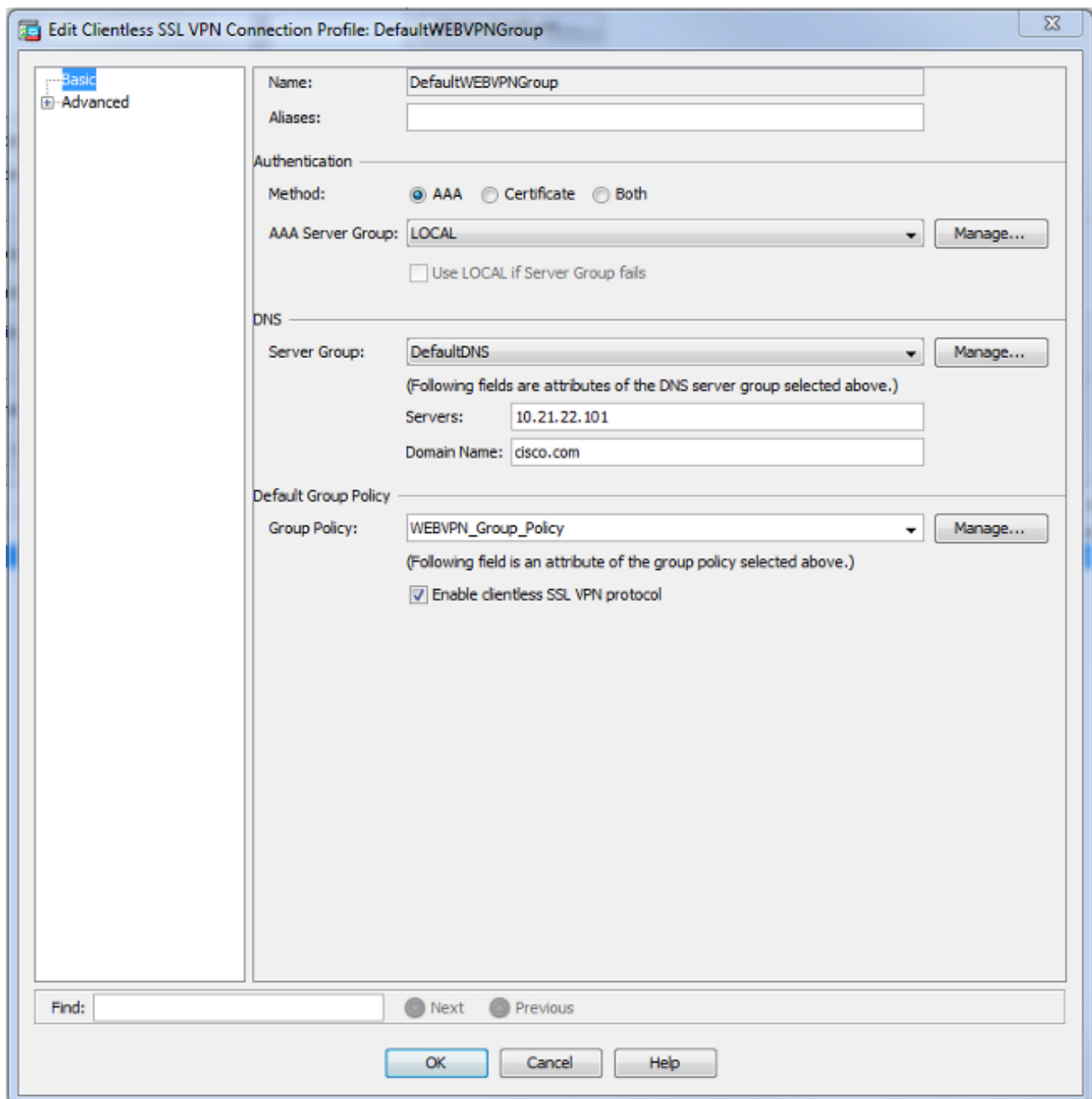
有关连接配置文件和组策略的概述，请参阅[思科 ASA 系列 VPN CLI 配置指南，版本 9.4 - 连接配置文件、组策略和用户](#)。默认情况下，WebVPN 连接使用 DefaultWEBVPNGroup 配置文件。您可以创建其他配置文件。**注意：**将用户分配到其他配置文件的方式有多种。

- 用户可以从下拉列表中手动选择连接配置文件，也可以使用特定 URL。请参阅 [ASA 8.x : 允许用户通过组别名和组 URL 方法在登录 WebVPN 时选择组](#)。

- 使用 LDAP 服务器时，可以根据从 LDAP 服务器接收的属性分配用户配置文件，请参阅 [ASA 使用 LDAP 属性映射配置示例](#)。

- 使用客户端的基于证书的身份验证时，可以根据证书中包含的字段将用户映射到配置文件，请参阅[思科 ASA 系列 VPN CLI 配置指南，版本 9.4 - 配置 IKEv1 的证书组匹配](#)。

- 要手动将用户分配到组策略，请参阅[思科 ASA 系列 VPN CLI 配置指南，版本 9.4 - 配置单个用户的属性](#)编辑 DefaultWEBVPNGroup 配置文件，并在“默认组策略”下选择 WEBVPN_Group_Policy。

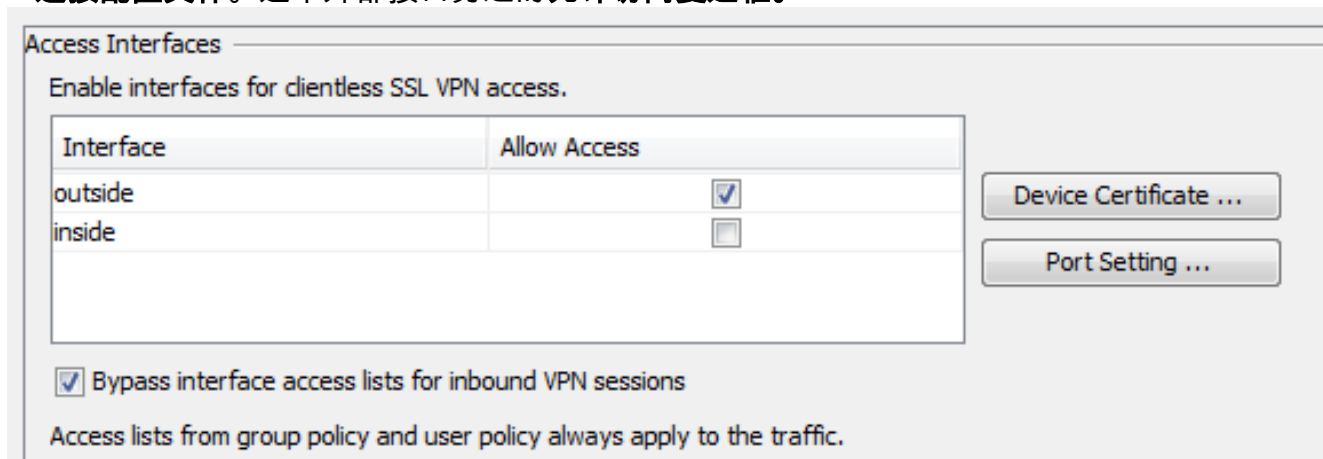


CLI :

```
ASA(config)# tunnel-group DefaultWEBVPNGroup general-attributes
```

```
ASA(config-tunnel-general)# default-group-policy WEBVPN_Group_Policy
```

6. 要在外部接口上启用 WebVPN，请依次选择配置 > 远程接入 VPN > 无客户端 SSL VPN 访问 > 连接配置文件。选中外部接口旁边的允许访问复选框。



CLI :

```
ASA(config)# webvpn
```

```
ASA(config-webvpn)# enable outside
```

7. (可选) 为内容创建书签。通过书签，用户可以轻松浏览内部资源，而无需记住 URL。要创建书签，请依次选择 **配置 > 远程接入 VPN > 无客户端 SSL VPN 访问 > 门户 > 书签 > 添加**。

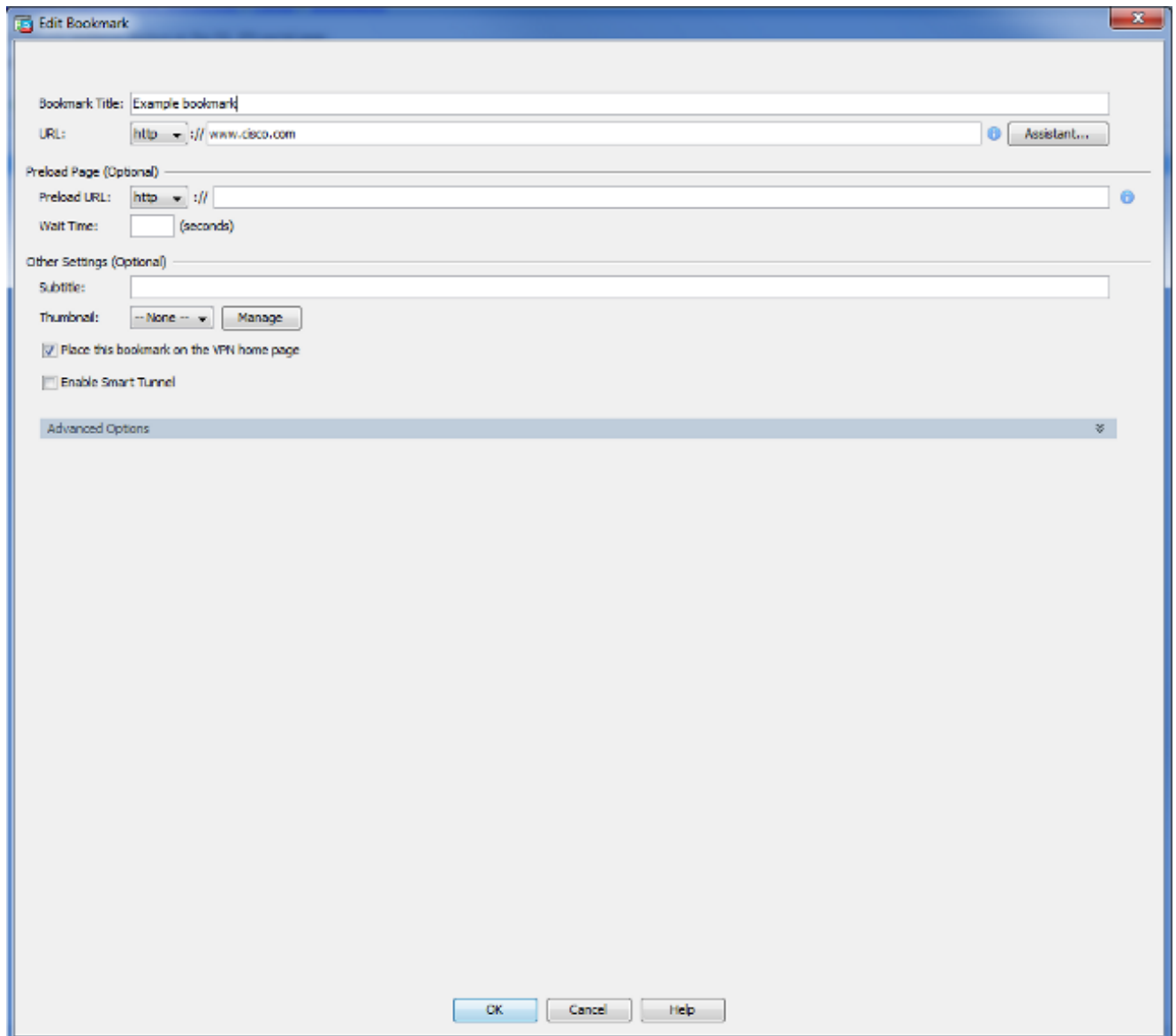
Add Bookmark List

Bookmark List Name:

Bookmark Title	URL
----------------	-----

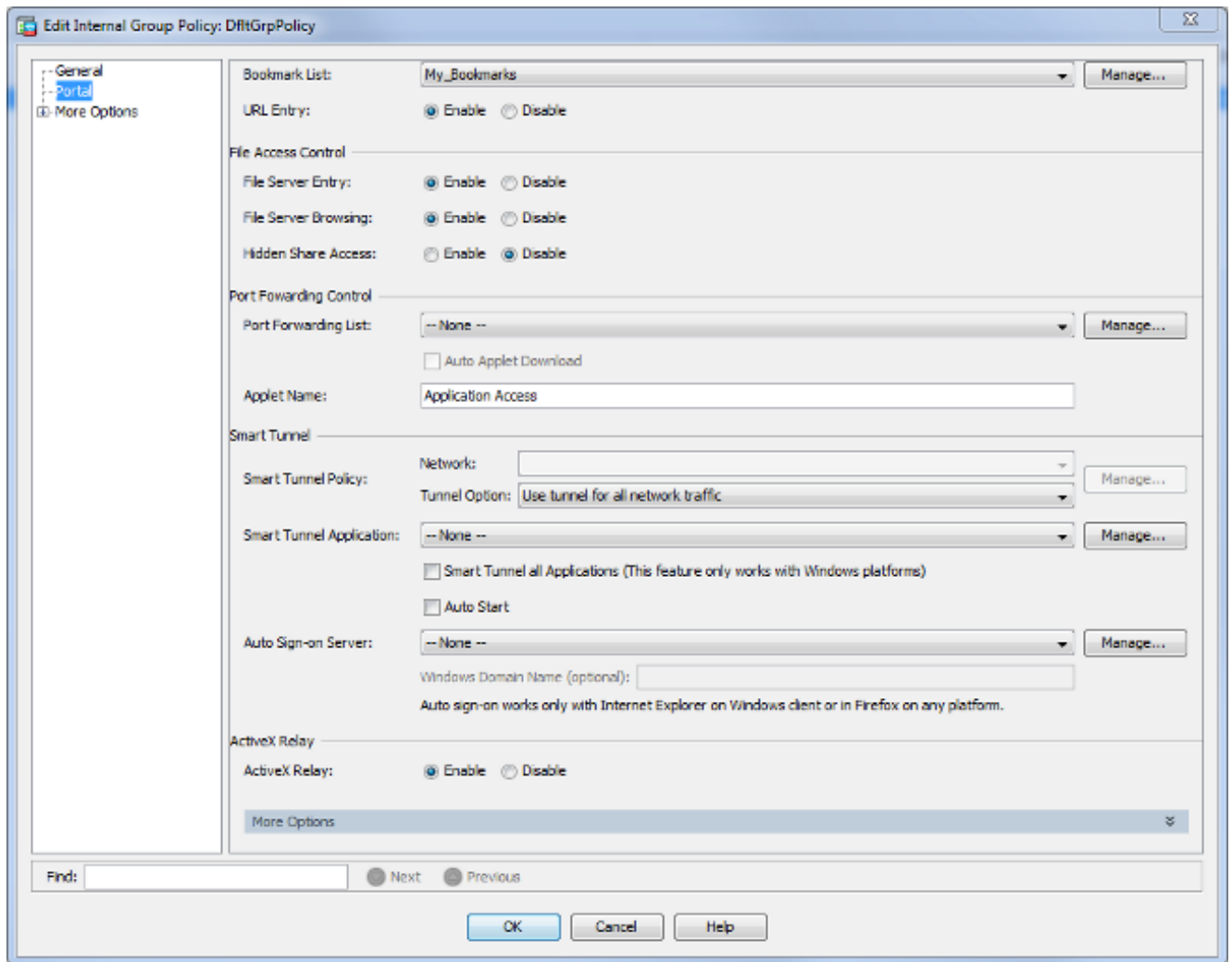
Find: Match Case

选择添加以添加特定书签。



CLI : 无法通过 CLI 创建书签，因为它们是以 XML 文件的形式创建的。

8. (可选) 将书签分配到特定组策略。依次选择**配置 > 远程接入 VPN > 无客户端 SSL VPN 访问 > 组策略 > 编辑 > 门户 > 书签列表**。

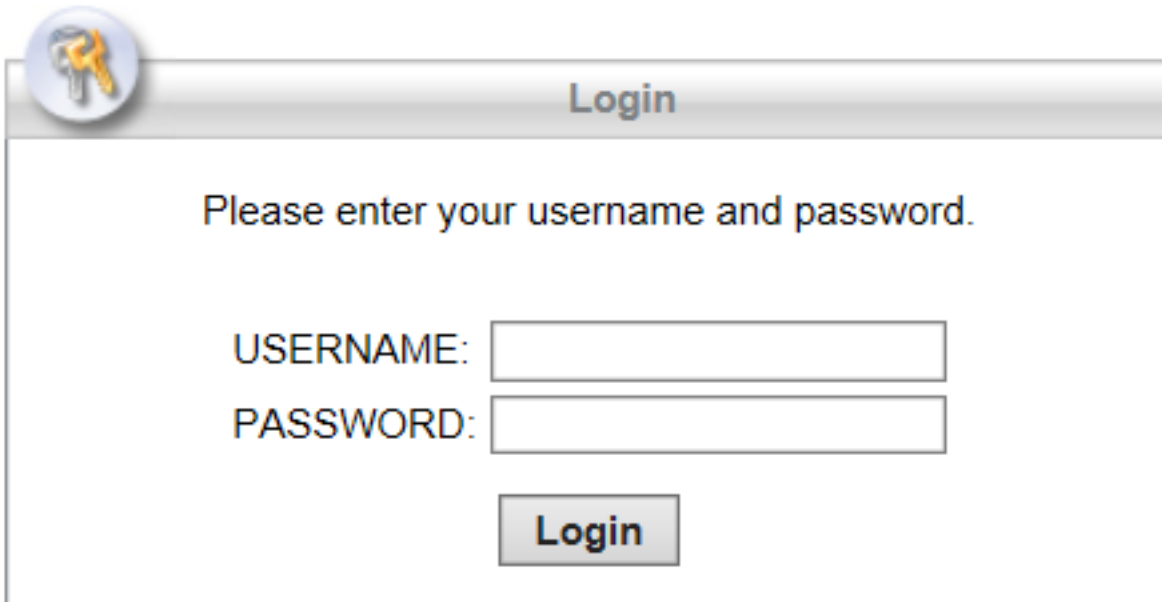


CLI :

```
ASA(config)# group-policy DfltGrpPolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

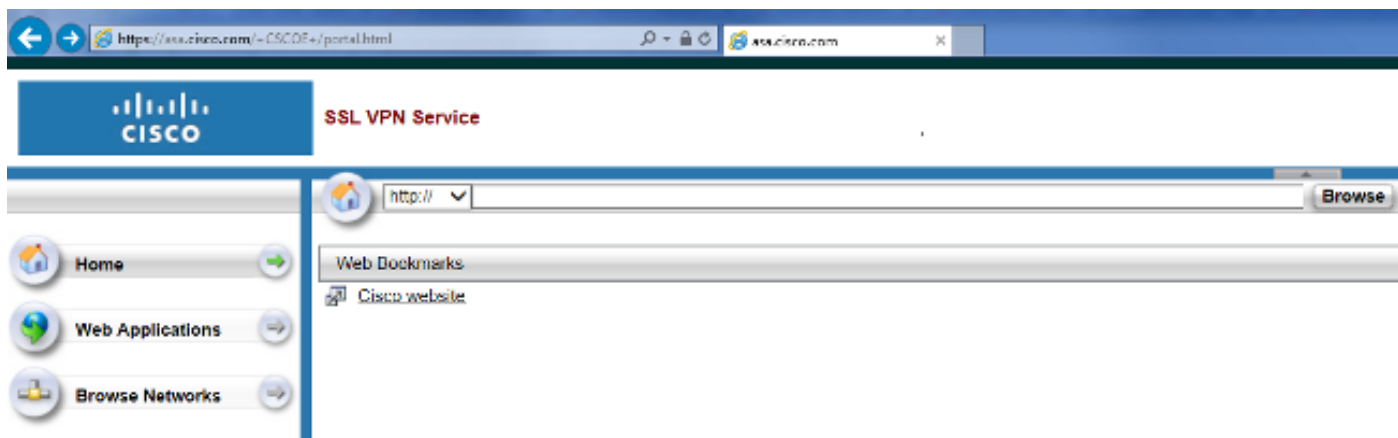
验证

配置 WebVPN 后，使用浏览器中的地址 <https://<ASA 的 FQDN>>。



The image shows a login window titled "Login" with a key icon in the top-left corner. The text "Please enter your username and password." is centered. Below this, there are two input fields: "USERNAME:" followed by a text box, and "PASSWORD:" followed by a text box. At the bottom center is a "Login" button.

登录后，您应该能够看到用于导航到网站和书签的地址栏。



故障排除

用于排除故障的步骤

请按照以下说明排除配置故障。

在 ASDM 中，选择 **Monitoring > Logging > Real-time Log Viewer > View**。当客户端连接到 ASA 时，请注意 TLS 会话是否已建立、组策略是否已选择以及用户身份验证是否成功。

```

Device completed SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLSv1.2 session
SSL client outside:10.229.20.77/61307 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLS session
SSL client outside:10.229.20.77/61306 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLS session
Built inbound TCP connection 107 for outside:10.229.20.77/61307 (10.229.20.77/61307) to identity:10.48.66.179/443 (10.48.66.179/443)
Built inbound TCP connection 106 for outside:10.229.20.77/61306 (10.229.20.77/61306) to identity:10.48.66.179/443 (10.48.66.179/443)
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> Authentication: successful, Session Type: WebVPN.
Device selects trust-point ASA-self-signed for client outside:10.229.20.77/53047 to 10.48.66.179/443
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> WebVPN session started.
DAP: User admin, Addr 10.229.20.77, Connection Clientless: The following DAP records were selected for this connection: DfltAccessPolicy
AAA transaction status ACCEPT : user = admin
AAA retrieved default group policy (WEBVPN_Group_Policy) for user = admin
AAA user authentication Successful : local database : user = admin
Device completed SSL handshake with client outside:10.229.20.77/61304 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61303 to 10.48.66.179/443 for TLSv1.2 session

```

CLI :

```

ASA(config)# logging buffered debugging
ASA(config)# show logging

```

在 ASDM 中，依次选择**监控 > VPN > VPN 统计信息 > 会话 > 筛选条件：无客户端 SSL VPN**。查找新的 WebVPN 会话。请务必选择 WebVPN 过滤器，然后单击 **Filter**。如果出现问题，请暂时绕过 ASA 设备，以确保客户端可以访问所需的网络资源。请查看本文列出的配置步骤。

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Cer Auth Int	Cer Auth Left
admin 10.229.20.77	WEBVPN_Group_Policy DefaultWEBVPNGroup	Clientless Clientless: (1)AES128	10:40:04 UTC Tue May 26 2015 0h:02m:50s	63991 166375		

CLI :

```

ASA(config)# show vpn-sessiondb webvpn

```

```

Session Type: WebVPN

Username : admin Index : 3
Public IP : 10.229.20.77
Protocol : Clientless
License : AnyConnect Premium
Encryption : Clientless: (1)AES128 Hashing : Clientless: (1)SHA256
Bytes Tx : 72214 Bytes Rx : 270241
Group Policy : WEBVPN_Group_Policy Tunnel Group : DefaultWEBVPNGroup
Login Time : 10:40:04 UTC Tue May 26 2015
Duration : 0h:05m:21s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a1516010000300055644d84
Security Grp : none

```

用于排除故障的命令

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

注意：使用 `debug` 命令之前，请参阅有关 Debug 命令的重要信息。

- `show webvpn` - 有许多与 WebVPN 关联的 `show` 命令。要详细了解 `show` 命令的用法，请参阅思科安全设备的[命令参考部分](#)。
- `debug webvpn` - 使用 `debug` 命令可能会对 ASA 产生不利影响。要详细了解 `debug` 命令的用法，请参阅思科安全设备的[命令参考部分](#)。

常见问题

用户无法登录

问题

尝试登录失败后，浏览器中显示“Clientless (browser) SSL VPN access is not allowed.”（不允许无客户端（浏览器）SSL VPN 访问。）消息。如果显示“Premium AnyConnect license is not enabled on the ASA.”（ASA 上未启用高级 AnyConnect 许可证）消息，则表明 AnyConnect 高级版许可证未安装在 ASA 上或未使用。

解决方案

使用以下命令启用高级 AnyConnect 许可证：

```
ASA(config)# webvpn
ASA(config-webvpn)# no anyconnect-essentials
```

问题

尝试登录失败后，浏览器中显示“Login failed”（登录失败）消息。已超出 AnyConnect 许可证限制。

解决方案

在日志中查找此消息：

```
%ASA-4-716023: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>
Session could not be established: session limit of 2 reached.
```

此外，请验证您的许可证限制：

```
ASA(config)# show version | include Premium
AnyConnect Premium Peers : 2 perpetual
```

问题

尝试登录失败后，浏览器中显示“AnyConnect is not enabled on the VPN server”（VPN 服务器上未启用 AnyConnect）消息。组策略中未启用无客户端 VPN 协议。

解决方案

在日志中查找此消息：

```
%ASA-6-716002: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>  
WebVPN session terminated: Client type not supported.
```

确保为所需组策略启用无客户端 VPN 协议：

```
ASA(config)# show run all group-policy | include vpn-tunnel-protocol  
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-clientless
```

无法将三个以上的 WebVPN 用户连接到 ASA

问题

只能将三个 WebVPN 客户端连接到 ASA。连接第四个客户端时将失败。

解决方案

在许多情况下，此问题与组策略中的一个同时登录设置有关。可以使用以下命令配置所需的同时登录数。在本例中，所需值为 20。

```
ASA(config)# group-policy Cisco attributes  
ASA(config-group-policy)# vpn-simultaneous-logins 20
```

WebVPN 客户端无法点击书签且显示为灰色

问题

如果配置了这些书签以让用户登录到无客户端 VPN，但在“Web 应用”下的主屏幕上这些书签显示为灰色，那么如何启用这些 HTTP 链接，以使用户能够点击它们并进入特定 URL？

解决方案

首先应确保 ASA 能通过 DNS 解析网站。尝试按名称 ping 这些网站。如果 ASA 无法解析该名称，链接将变灰。如果 DNS 服务器在网络内部，请配置 DNS 域查找专用接口。

通过 WebVPN 进行 Citrix 连接

问题

通过 WEBVPN 进行 Citrix 连接时出现错误消息“the ica client received a corrupt ica file.” 在通过 WebVPN 进行 Citrix 连接时显示。

解决方案

如果将安全网关 模式用于通过 WebVPN 进行的 Citrix 连接，ICA 文件可能损坏。由于 ASA 与此操作模式不兼容，请在直接模式（非安全模式）下新建一个 ICA 文件。

如何避免需要对用户进行第二次身份验证

问题

当您访问无客户端 WebVPN 门户上的 CIFS 链接时，点击书签后系统会提示您输入凭证。轻型目录访问协议 (LDAP) 用于验证资源和用户已输入 LDAP 凭证以登录到 VPN 会话。

解决方案

在这种情况下，您可以使用自动登录功能。在正在使用的特定组策略及其 WebVPN 属性下，配置以下内容：

```
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri cifs://X.X.X.X/* auth-type all
```

其中X.X.X.X=CIFS服务器IP*=到达相关共享文件/文件夹的路径的其余部分。

下面显示了配置片段示例：

```
ASA(config)# group-policy ExamplePolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri
https://*.example.com/* auth-type all
```

有关详细信息，请参阅[配置使用 HTTP 基本身份验证或 NTLM 身份验证的 SSO](#)。

相关信息

- [ASA : 使用ASDM的Smart Tunnel配置示例](#)
- [技术支持和文档 - Cisco Systems](#)