配置在ASA的无客户端SSL VPN (WebVPN)

目录

简介

本文为5500系列Cisco可适应的安全工具(ASA)提供一直接的配置为了允许无客户端对内部网络资源的安全套接字协议层(SSL) VPN访问。无客户端SSL虚拟专用网络(WebVPN)允许有限，但是贵重物品，对公司网络的安全访问从所有位置。用户能在任何时间完成对公司资源的安全基于浏览器的访问。另外的客户端不是需要的为了获得访问到内部资源。使用在SSL连接的一个超文本传输协议访问提供。

无客户端SSL VPN提供绑和容易进入到各种各样的Web资源和可激活网络和传统应用上从几乎能到达超文本传输协议互联网的任何计算机(HTTP)站点。包括：

- 内部网站
- Microsoft SharePoint 2003， 2007年和2010
- Microsoft Outlook Web访问2003年， 2007年和2013
- Microsoft Outlook Web App 2010
- Domino Web访问(DWA) 8.5和8.5.1
- Citrix Metaframe演示服务器4.x
- Citrix XenApp版本5到6.5

- Citrix XenDesktop版本5到5.6和7.5
- VMware图4

支持的软件列表可以在支持的VPN平台找到， 5500系列Cisco的ASA。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 已启用SSL浏览器
- 7.1 或更高版本的 ASA
- X.509证书发出对ASA域名
- TCP 端口 443，在从客户端到 ASA 的路径中不得阻止该端口

需求详尽列表可以在支持的VPN平台找到， 5500系列Cisco的ASA。

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)
- 可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。

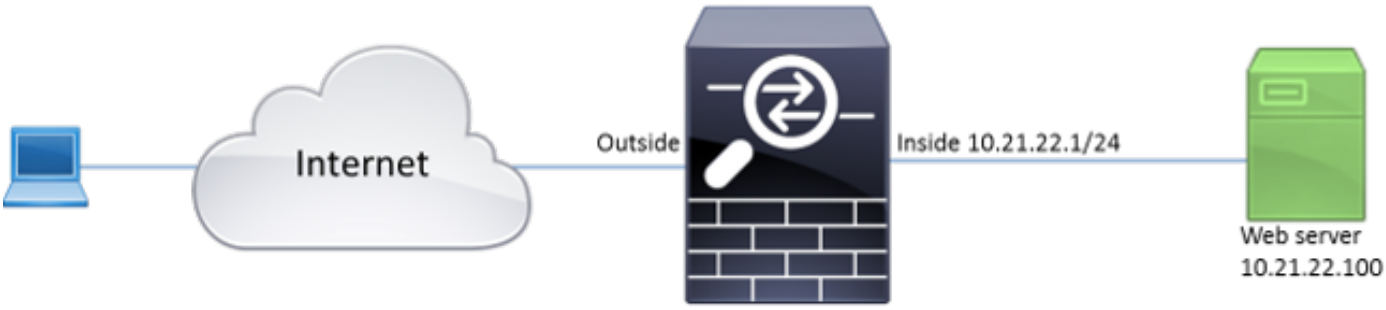
配置

此条款描述ASDM和CLI的配置过程。您能选择跟随工具之一为了配置WebVPN，但是某些配置步骤可能用ASDM只完成。

> **注意：** 使用命令查找工具（仅限注册用户）可详细了解本部分所使用的命令。

网络图

本文档使用以下网络设置：



背景信息

WebVPN使用SSL协议为了获取数据转接在客户端和服务器之间。当浏览器首次对ASA时的连接，ASA提交其证书验证到浏览器。为了保证客户端和ASA之间的连接安全，您需要提供ASA由签字认证机关客户端已经委托的证书。否则客户端不会有方法验证导致中间人攻击和恶劣的用户体验的可能性ASA的真实性，因为浏览器制造一警告连接没有委托。

> **注意**：默认情况下，ASA生成一自已签署的X.509证书在启动。默认情况下此证书用于为了服务客户端连接。因为其真实性不可能由浏览器，验证没有推荐使用此证书。此外，此证书被重新生成在每辆重新启动，因此在每辆重新启动以后更改。

认证安装是超出本文的范围。

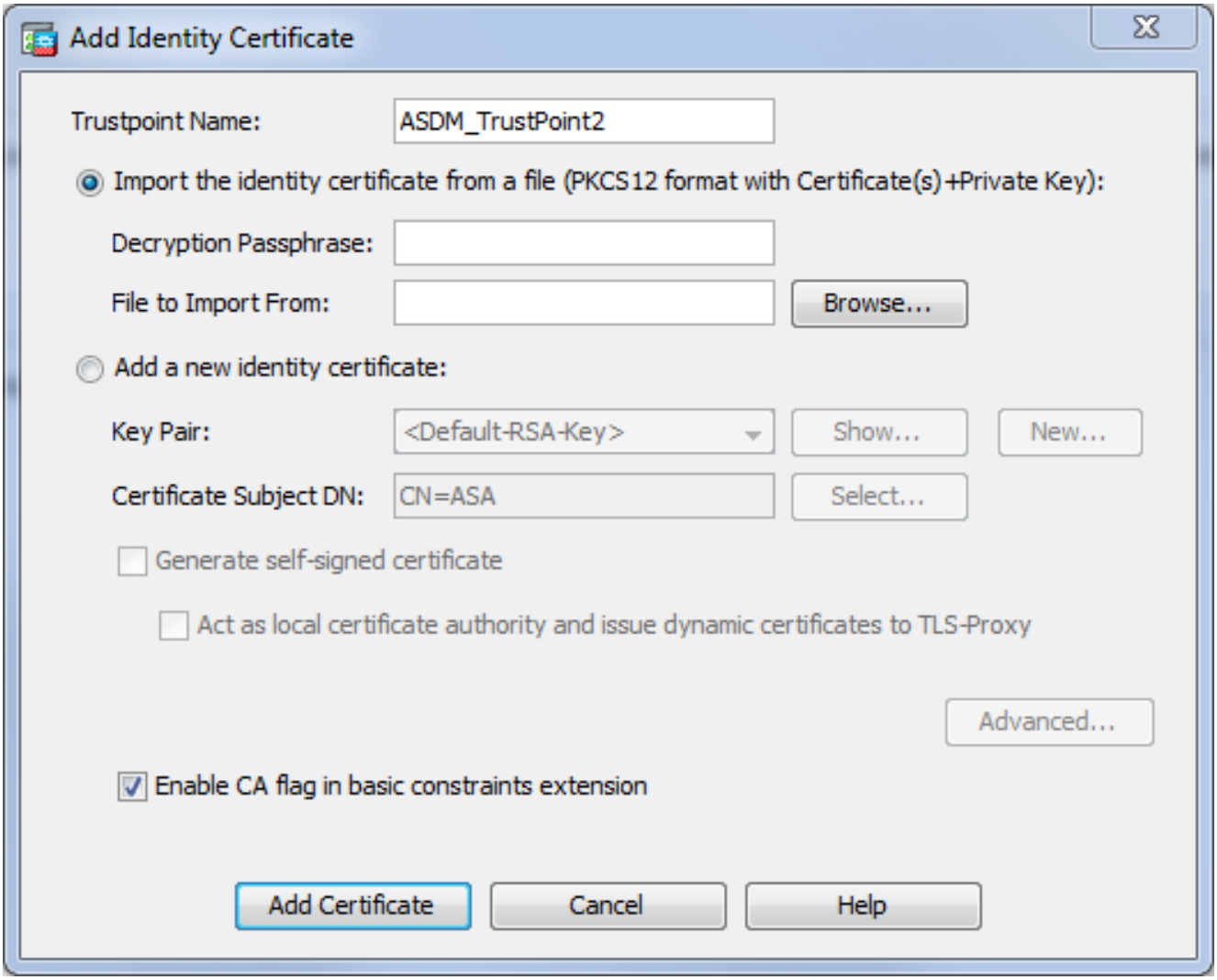
配置

配置在ASA的WebVPN与五个主要步骤：

- 配置将由ASA使用的证书。
- 在 ASA 接口上启用 WebVPN。
- 建立服务器和统一资源定位器(URL)列表WebVPN访问的。
- 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ASA中比版本9.4，用于的算法选择SSL密码器更改发布以后(请参阅版本注释关于思科ASA系列， 9.4(x)).If只有椭圆曲线有能力客户端将使用，然后使用椭圆曲线专用密钥证书是安全的。否则应该用于自定义密码器套件为了避免有ASA存在一自已签署的临时证书。您能配置ASA以**ssl密码器tlsv1.2自定义"AES256 SHA:AES128 SHA:DHE RSA AES256 SHA:DHE RSA AES128 SHA:DES CBC3 SHA:DES CBCSHA:RC4 SHA:RC4 MD5"**命令使用仅基于RSA的密码器。

1. **选项1** -导入证书用pkcs12文件。选择**Configuration>防火墙>Advanced > Certificate Management >身份证书>Add**。您能用pkcs12文件安装它或粘贴在增强加密邮件(PEM)格式的内容。

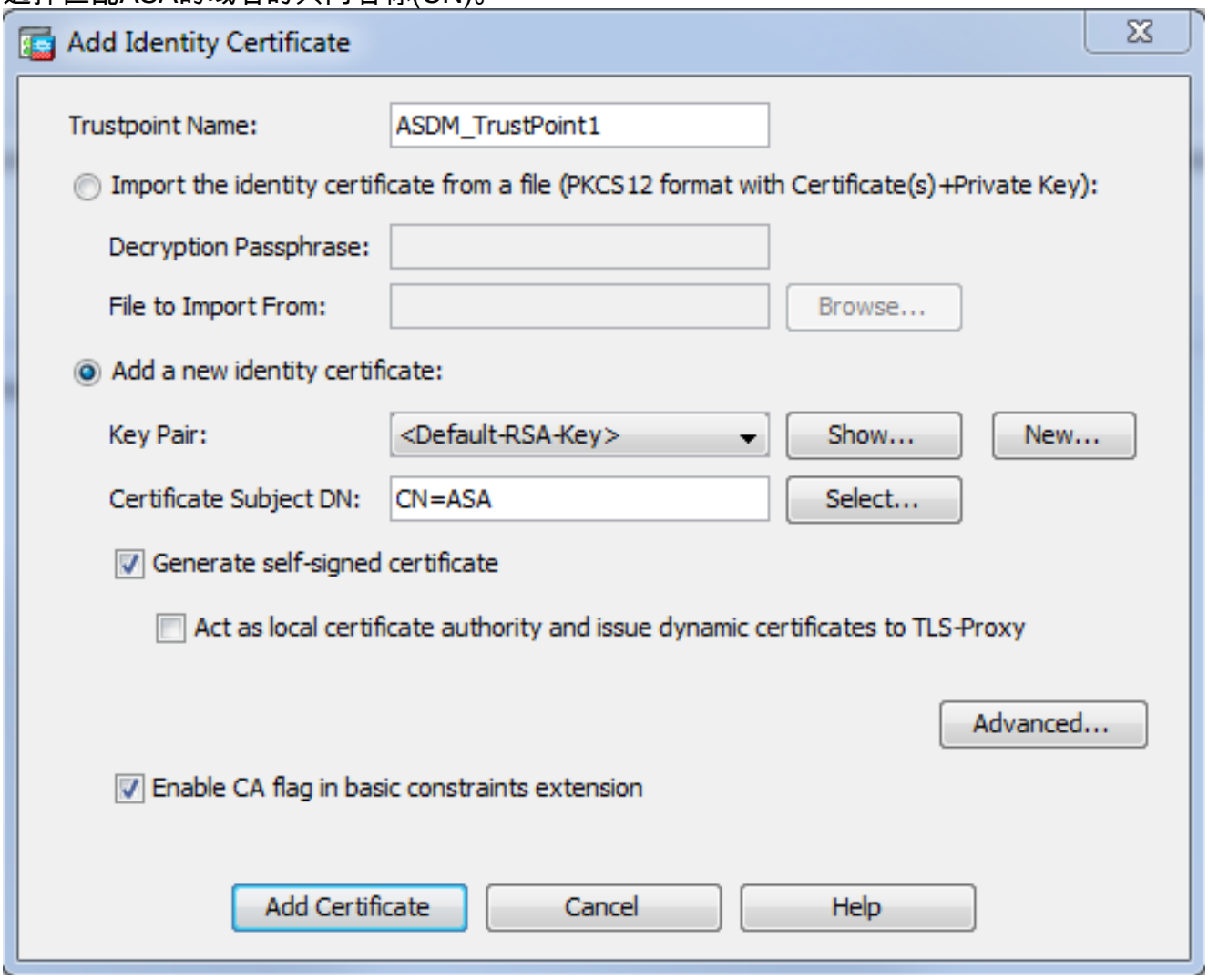


CLI :

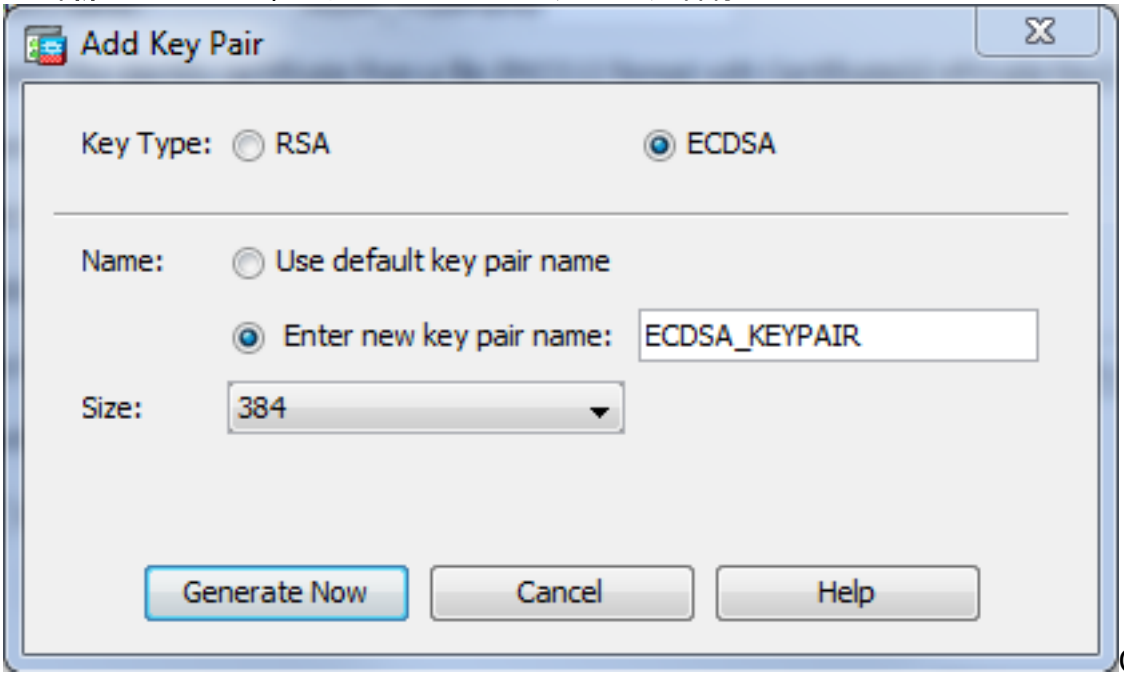
```
ASA(config)# crypto ca import TrustPoint-name pkcs12 "password"


Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCAggAgIIFuHFrV6enVflNv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh0O7No4Ycx75Y5sOhyuQGPhLJRdionbi1s1ioe4Dplx1b


--- output ommited ---


Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJUQIBAzCCCRcGCSqGSIb3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIb3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQI8F3N
+vkvjUgCAggAgIIFuHFrV6enVflNv3sBByB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh0O7No4Ycx75Y5sOhyuQGPhLJRdionbi1s1ioe4Dplx1b

quit
```

```
INFO: Import PKCS12 operation completed successfully
```

选项2 -创建自签名证书。选择**Configuration>防火墙>Advanced > Certificate Management >身份证书>Add**。单击 **Add a new identity certificate** 单选按钮。检查**生成自签名证书复选框**。选择匹配ASA的域名的共同名称(CN)。



单击**新**为了创建证书的密钥对。选择关键类型、名称和大小。

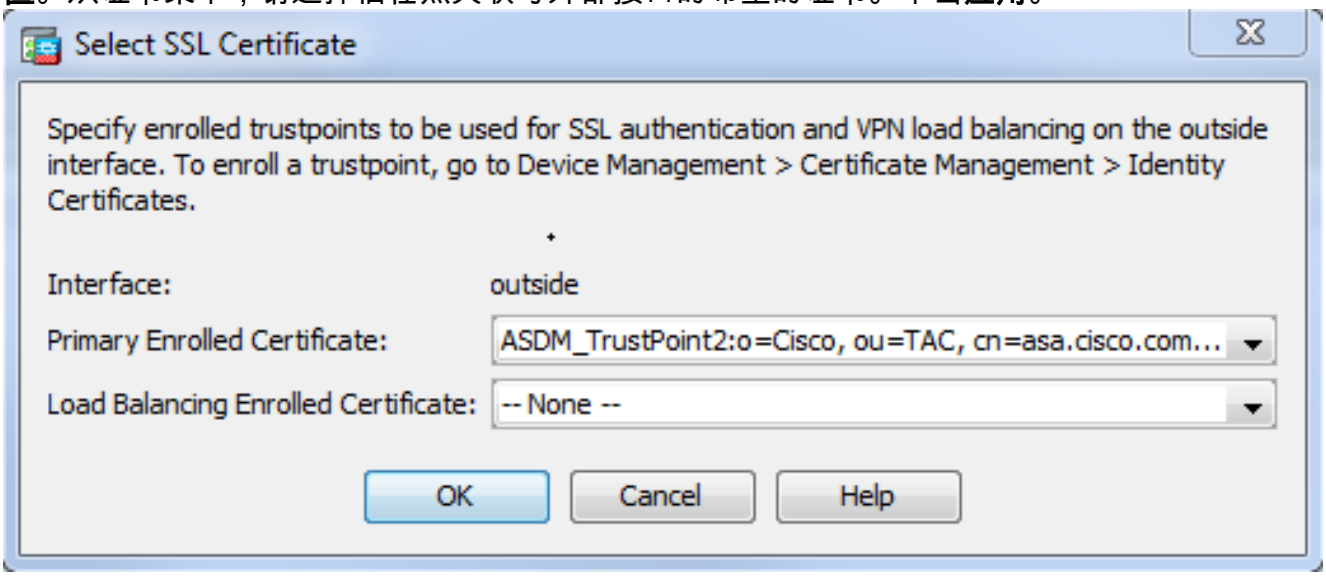


CLI ：

```
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
```

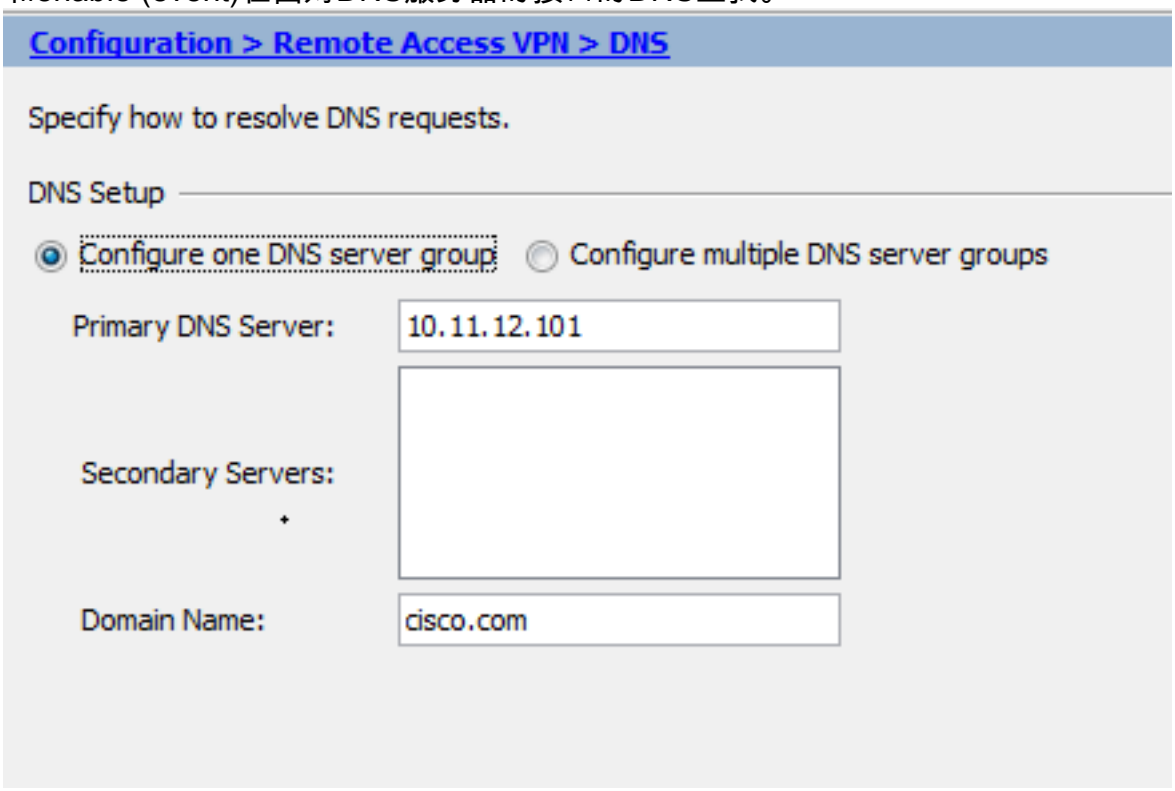
2. 选择将使用服务WebVPN连接的证书。选择**Configuration>远程访问VPN >Advanced > SSL设置**。从证书菜单，请选择信任点关联与外部接口的希望的证书。单击**应用**。

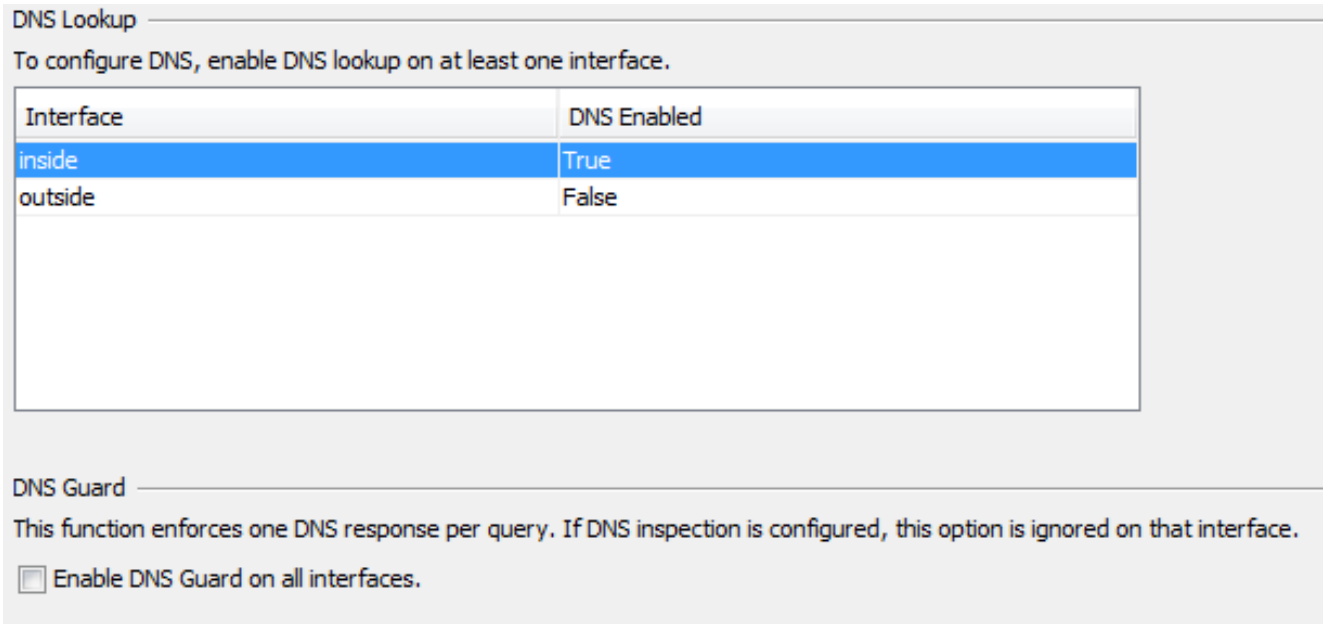


等同的CLI配置：

```
ASA(config)# ssl trust-point <trustpoint-name> outside
```

3. (可选) Enable (event)域名服务器(DNS)查找。WebVPN服务器作为客户端连接的一个代理。意味着ASA代表客户端创建对资源的连接。如果客户端需要对使用域名的资源的连接，则ASA需要执行DNS查找。选择**Configuration>远程访问VPN > DNS**。配置至少一个DNS服务器和enable (event)在面对DNS服务器的接口的DNS查找。

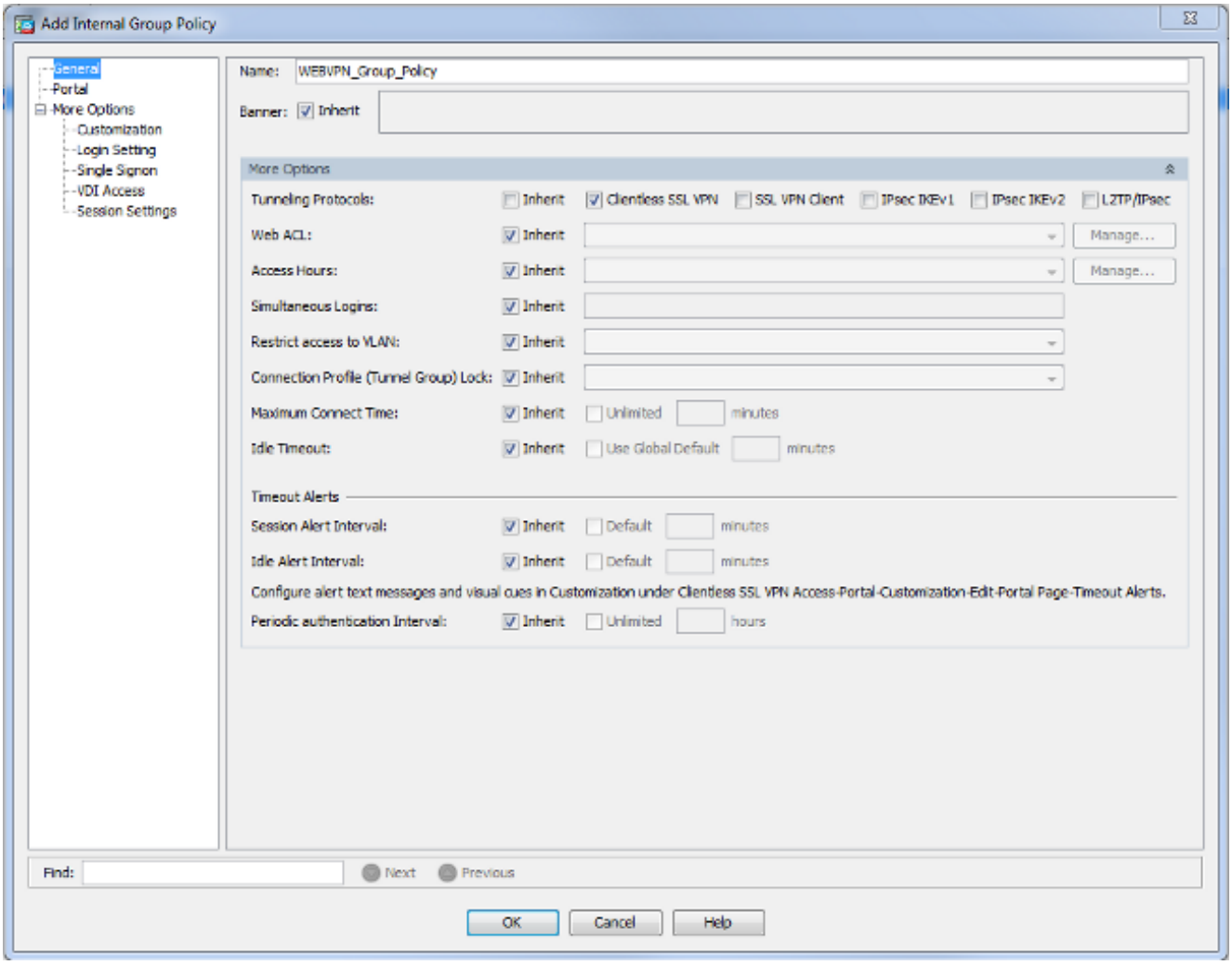




CLI ：

```
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)请创建WEBVPN连接的组策略。选择**Configuration>远程访问VPN >无客户端SSL VPN访问>组策略>Add内部组策略**。在一般选项下请更改Tunelling协议值对“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
```

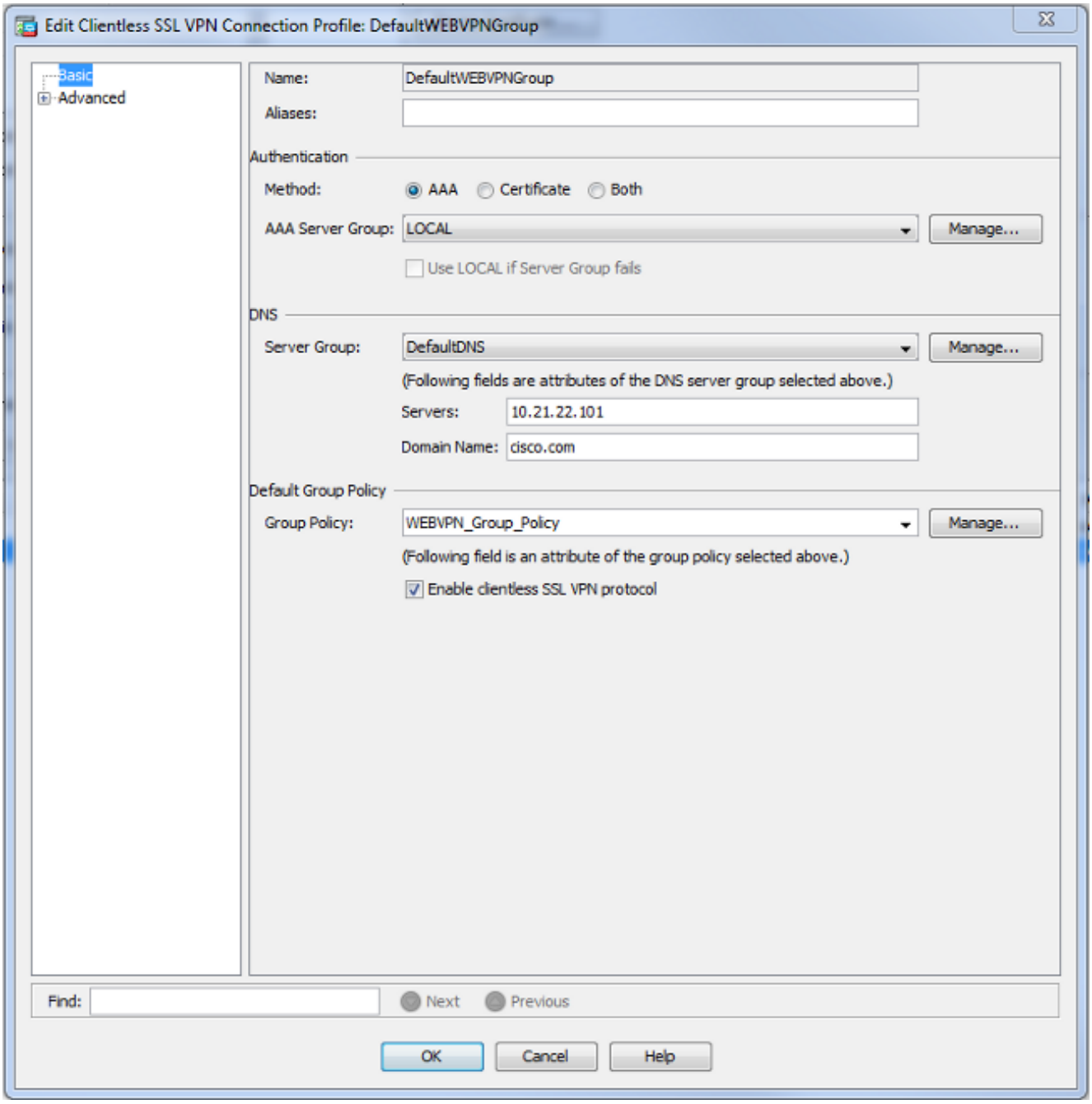
5. 配置连接配置文件。在ASDM，请选择**Configuration>远程访问VPN >无客户端SSL VPN访问>连接配置文件**。
   对于连接配置文件和组策略的概述，请咨询思科ASA系列VPN CLI配置指南， 9.4 -连接配置文件，组策略和用户。默认情况下， WebVPN连接使用DefaultWebVPNGroup配置文件。您能创建另外的配置文件。**注意**：有多种方式分配用户对其他配置文件。

   -用户能手工选择连接配置文件从下拉列表或与特定URL。请参阅ASA 8.x ：允许用户选择组在WebVPN洛金通过组别名和Group-url方法。

   -，当您使用一个LDAP服务器时，您能分配根据属性的用户配置文件接收从LDAP服务器，看到ASA使用LDAP属性地图配置示例。

   -，当您使用客户端的基于认证的验证时，您能映射用户到根据字段的配置文件包含在证书，看到思科ASA系列VPN CLI配置指南， 9.4 -请配置匹配为IKEv1的证书组。

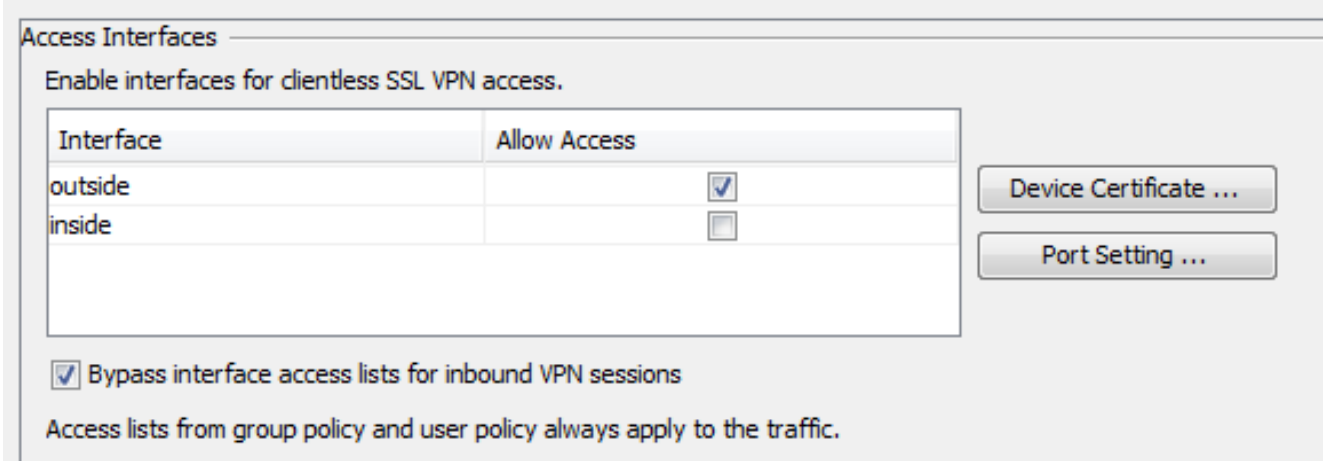
   -为了用户手册分配到组策略，请参阅思科ASA系列VPN CLI配置指南， 9.4 -配置个人用户的属性编辑DefaultWebVPNGroup配置文件并且根据默认组策略选择WEBVPN_Group_Policy。



CLI ：

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

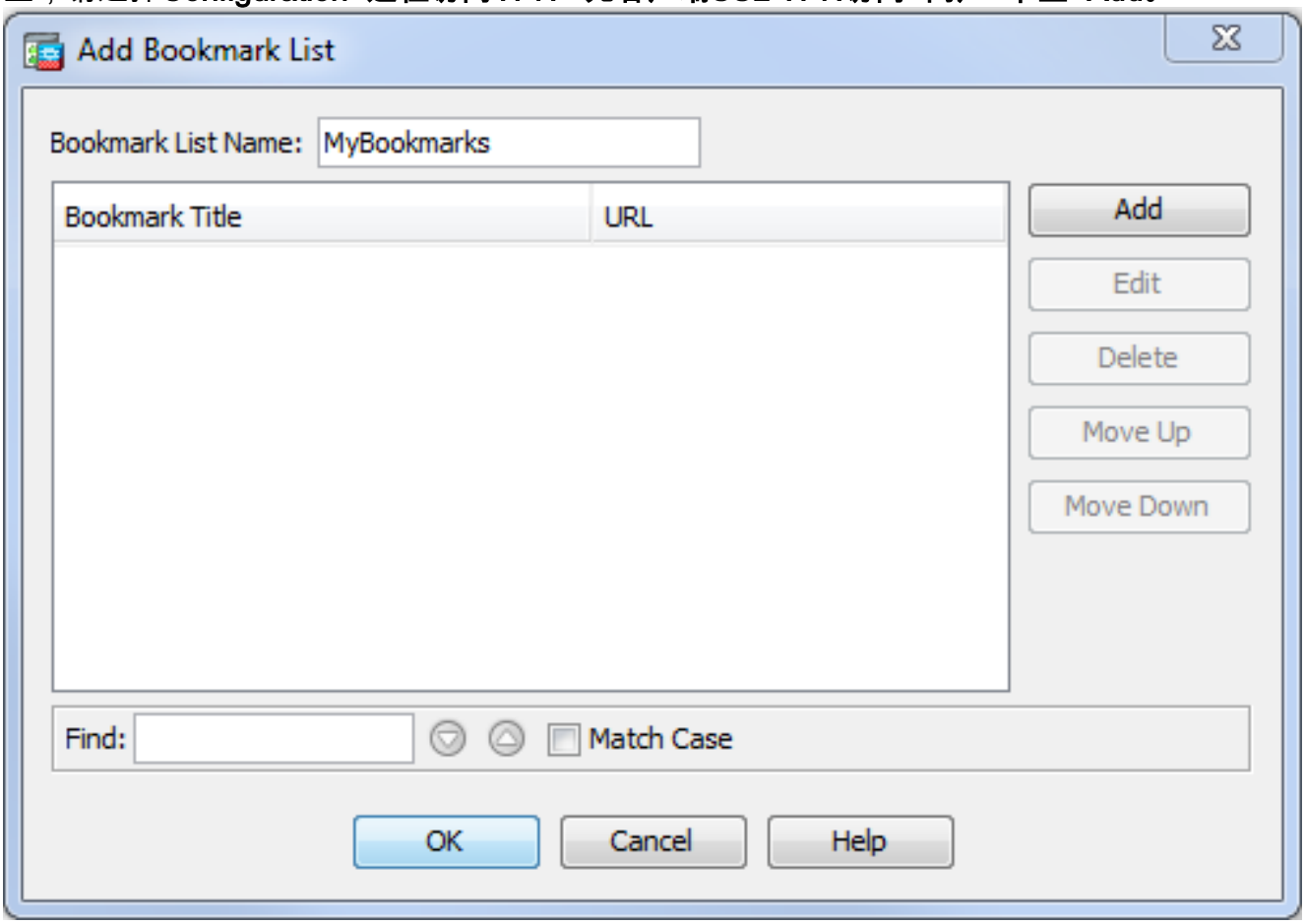
6. 为了启用在外部接口的WebVPN，请选择**Configuration>远程访问VPN >无客户端SSL VPN访问>连接配置文件**。在外部接口旁边检查**允许**复选框。



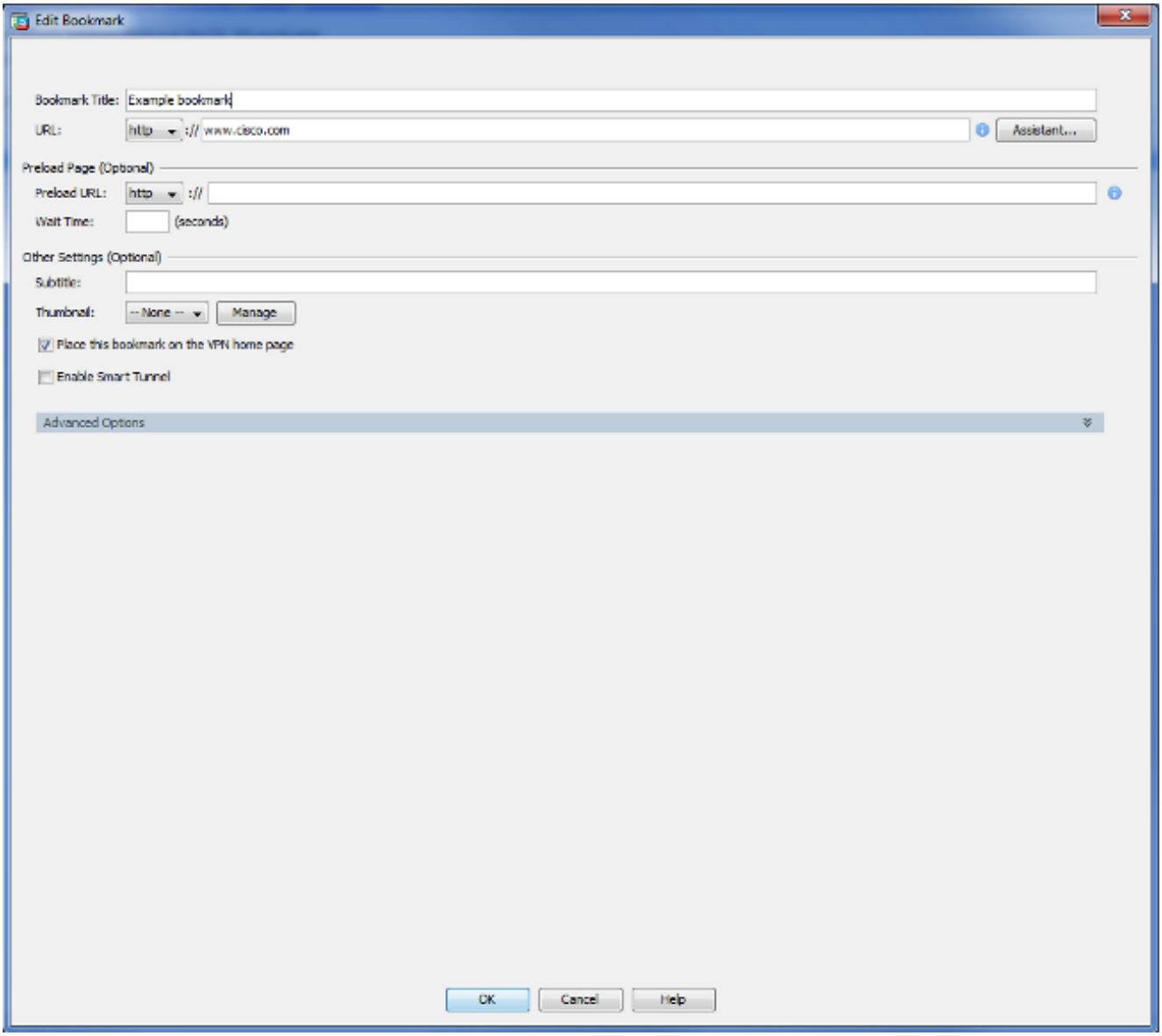
CLI ：

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

7. (可选)请创建内容的书签。书签允许用户容易地浏览内部资源，而不必记住URL。为了创建书签，请选择**Configuration>远程访问VPN >无客户端SSL VPN访问>门户>书签>Add**。

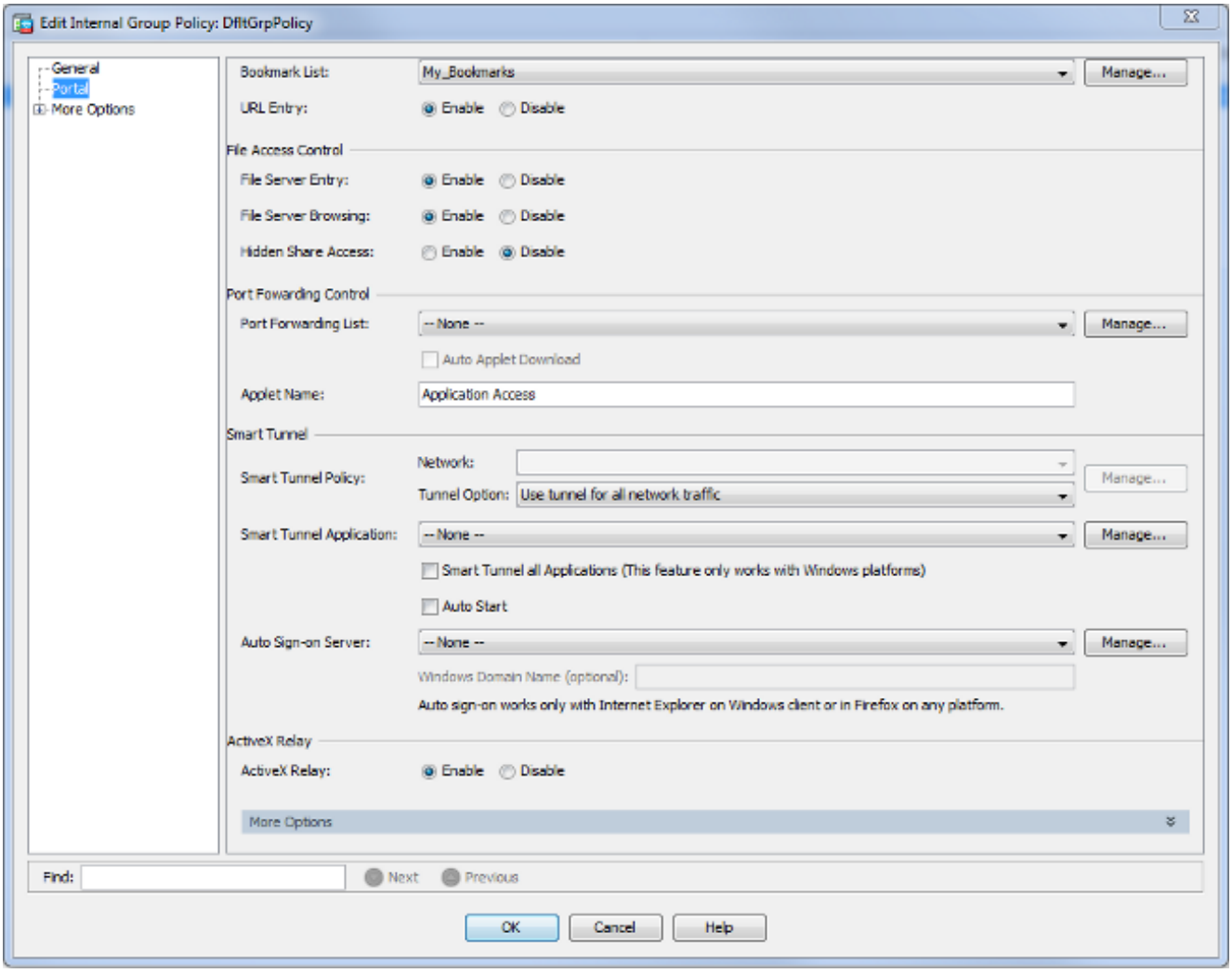


选择**添加**为了添加一张特定书签。



CLI ：因为他们创建作为XML文件，通过CLI创建书签是不可能的。

8. (可选)请分配书签到一项特定组策略。选择**Configuration>远程访问VPN >无客户端SSL VPN访问>组策略> Edit >门户>书签列表**。

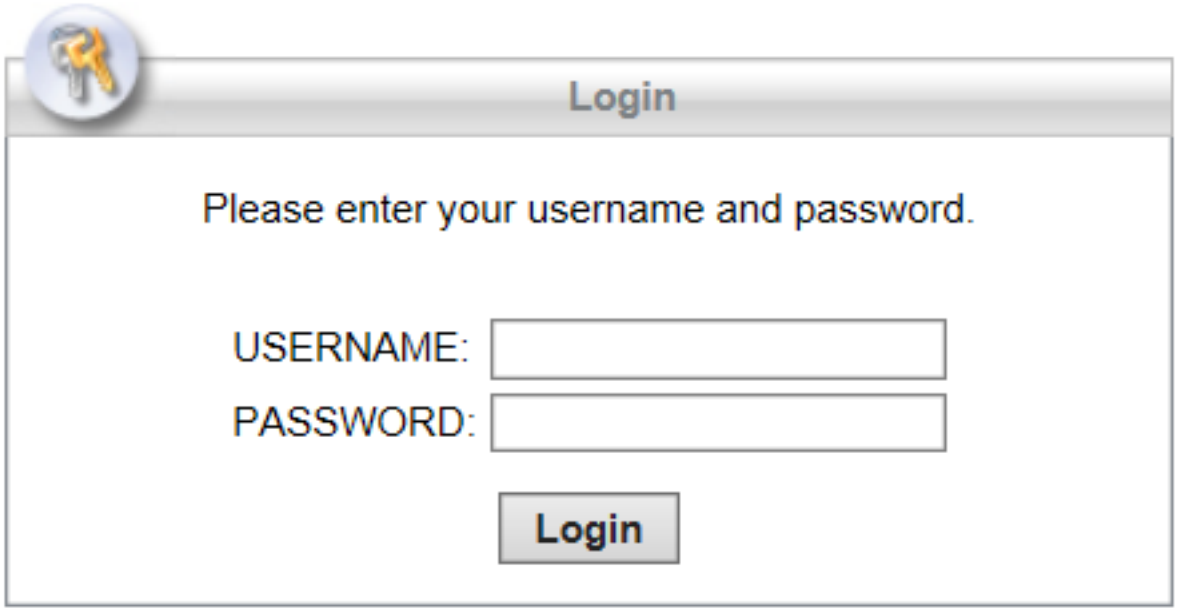


CLI ：

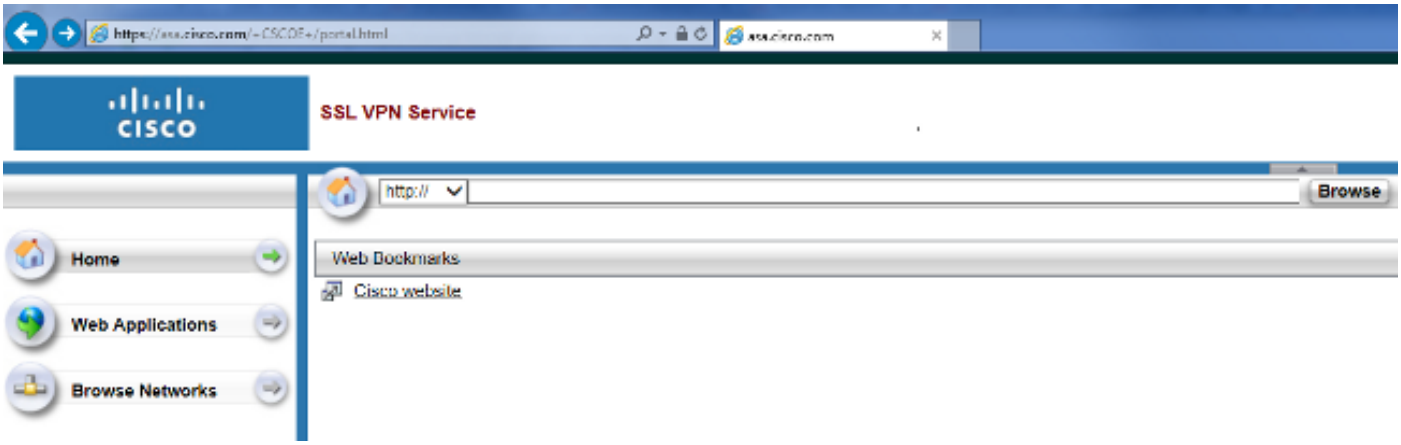
```
ASA(config)# group-policy DfltGrpPolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

验证

一旦WebVPN配置，请使用*ASA>的*地址https:// <FQDN在浏览器。



在登陆以后您应该能发现用于的地址栏导航到网站和书签。



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。

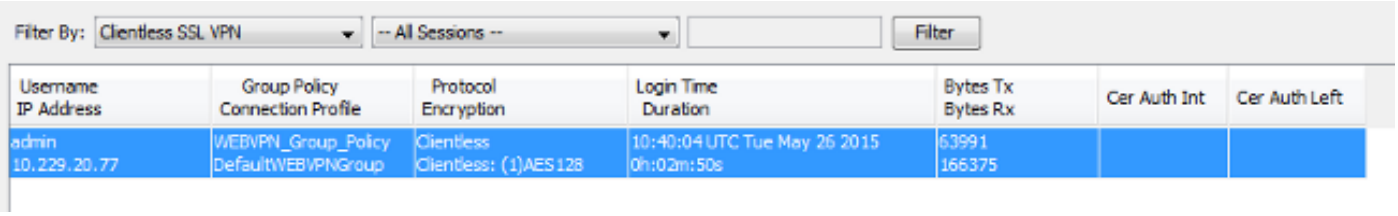
在 ASDM 中，选择 **Monitoring** > Logging > Real-time Log Viewer > View。当客户端连接对ASA时，请注释TLS会话的组策略的建立，用户的选择和成功认证。

```
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，请选择**Monitoring> VPN > VPN统计信息>塞申斯>过滤器：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。



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。

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

- **显示WebVPN** -有许多**显示**与WebVPN的associated命令。为了看到使用详细**显示**命令，请参阅Cisco安全设备的命令参考部分。
- **调试WebVPN** -使用调试指令能负面影响ASA。为了较详细地看到使用调试指令，请参阅Cisco安全设备的命令参考部分。

常见问题

用户不能登录

问题

消息“无客户端(浏览器) SSL VPN访问没有允许”。在浏览器出现在一个不成功登录尝试以后。AnyConnect优质许可证在ASA没有安装或不是在使用中的如显示由“优质AnyConnect许可证在ASA没有启用”。

解决方案

启用优质AnyConnect许可证用这些命令：

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

问题

消息“登录失败”在浏览器出现在一个不成功登录尝试以后。AnyConnect许可证限制超过了。

解决方案

寻找在日志的此消息：

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

并且，请验证您的许可证限制：

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

问题

消息“AnyConnect在VPN服务器在浏览器没有启用”出现在一个不成功登录尝试以后。无客户端VPN协议在组政策没有启用。

解决方案

寻找在日志的此消息：

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

确保无客户端VPN协议为希望的组政策启用：

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

无法联络超过三个WebVPN用户到ASA

问题

仅三个WebVPN客户端能连接到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。请使用此图示为了配置同时登录所需的数量。在本例中，所需的值是20。

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

WebVPN客户端不能点击书签和变灰

问题

如果这些书签配置为了用户能签到到无客户端VPN，但是在“Web应用程序下的”家庭屏幕他们出现如变灰，如何能启用这些HTTP链路，以便用户能点击他们和进入特定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。

Citrix连接通过WebVPN

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.**”为在WebVPN的Citrix发生。

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。

如何避免需要对于用户的秒钟验证

问题

当您访问在无客户端WebVPN门户时的CIFS链路，提示对于凭证，在您点击书签后。轻量级目录访问协议(LDAP)用于为了验证资源，并且用户已经输入LDAP凭证登录对VPN会话。

解决方案

您能在这种情况下使用自动登录功能。根据使用和在其WebVPN属性下的特定组政策，请配置此：

```
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
```

那里CIFS服务器和*=restofX.X.X.X=IP共享文件/文件夹的有问题的。

配置示例片断显示此处：

```
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
```

关于此的更多信息，请参阅配置与基本的HTTP的SSO或NTLM验证。

相关信息

- ASA ：使用ASDM的Smart Tunnel配置示例
- 技术支持和文档 - Cisco Systems