ASA でのクライアントレス SSL VPN（WebVPN）の設定

内容

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス（ASA）5500 シリーズで社内ネットワーク リソースへのクライアントレス セキュア ソケット レイヤ（SSL）VPN アクセスを実現するための簡単な設定を紹介します。クライアントレス SSL バーチャル プライベート ネットワーク（WebVPN）を使用すると、制限付きではありますが、あらゆる場所から社内ネットワークへの効率的かつ安全なアクセスが可能になります。ユーザは、企業リソースへの安全なブラウザベース アクセスをいつでも利用できます。内部リソースにアクセスするためにクライアントを追加する必要はありません。アクセスは、SSL 接続を介した Hypertext Transfer Protocol を使用して提供されます。

クライアントレス SSL VPN を使用することで、Hypertext Transfer Protocol（HTTP）インターネット サイトにアクセスできるほとんどすべてのコンピュータから、広範な Web リソース、および Web 対応アプリケーションとレガシー アプリケーションの両方に安全かつ簡単にアクセスできます。これには、次のような特徴があります。

- 内部 Web サイト

- Microsoft SharePoint 2003、2007、および 2010
- Microsoft Outlook Web Access 2003、2007、および 2013
- Microsoft Outlook Web App 2010
- Domino Web Access（DWA）8.5 および 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp バージョン 5 から 6.5
- Citrix XenDesktop バージョン 5 から 5.6、および 7.5
- VMware View 4

サポートされるソフトウェアのリストについては、『サポートされている VPN プラットフォーム（Cisco ASA 5500 シリーズ）』を参照してください。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- SSL 対応ブラウザ
- バージョン 7.1 以上がインストールされた ASA
- ASA ドメイン名に対して発行された X.509 証明書
- クライアントから ASA へのパスで TCP ポート 443 番がブロックされていないこと

要件の詳細については、『サポートされている VPN プラットフォーム（Cisco ASA 5500 シリーズ）』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASA Version 9.4(1)
- Adaptive Security Device Manager（ASDM）バージョン 7.4(2)
- ASA 5515-X

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

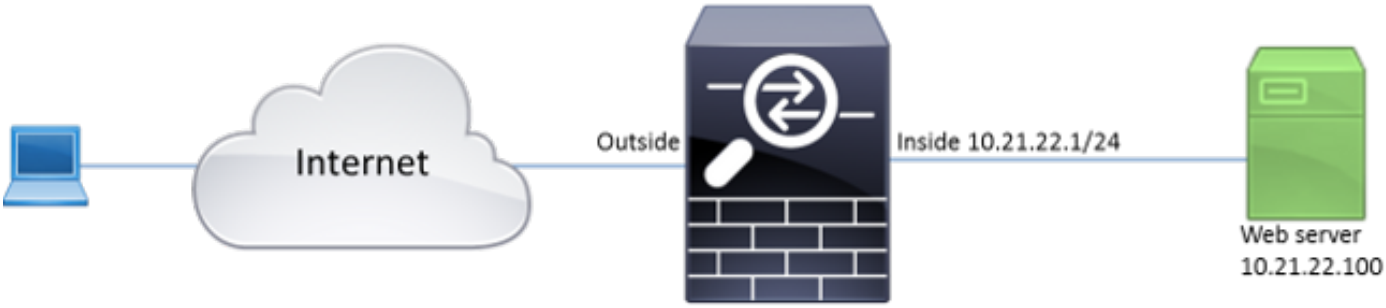
設定

この記事では、ASDM と CLI の両方の設定プロセスについて説明します。どちらのツールを使用しても WebVPN を設定できますが、一部の設定手順は ASDM でのみ実行できます。

> **注：このセク**ションで使用されるコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



背景説明

WebVPN は、クライアントとサーバの間で転送されるデータを保護するために SSL プロトコルを使用します。ブラウザが ASA への接続を開始すると、ASA は自身を認証するためにブラウザに証明書を提示します。クライアントと ASA の間の接続が安全であることを保証するために、クライアントですでに信頼されている認証局によって署名された証明書を ASA に提供する必要があります。この証明書を提供しないと、クライアントは ASA の信頼性を検証できません。その結果、接続が信頼できないことを示すアラートがブラウザで生成され、中間者攻撃が発生したり、ユーザ エクスペリエンスが低下したりする可能性があります。

> **注**：デフォルトでは、ASA の起動時に自己署名 X.509 証明書が生成されます。クライアント接続の確立には、デフォルトでこの証明書が使用されますが、この証明書の信頼性をブラウザで検証できないため、使用しないことを推奨します。また、この証明書はリブート時に毎回再生成されるので、リブートするたびに変更されます。

証明書のインストールについては、このドキュメントでは扱いません。

コンフィギュレーション

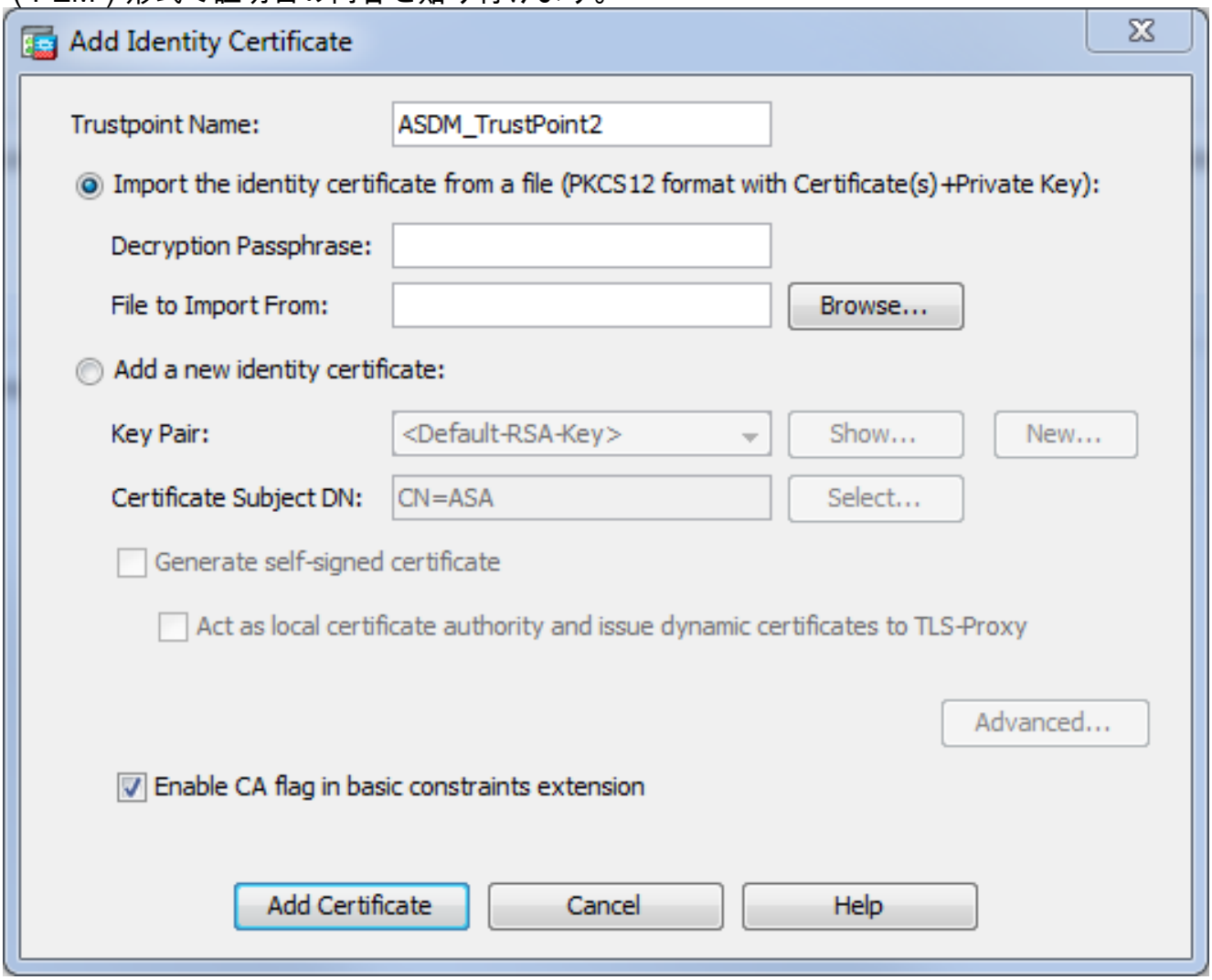
ASA で WebVPN を設定する際の主な手順は、次の 5 つです。

- ASA で使用する証明書を設定します。
- ASA インターフェイスで WebVPN を有効にします。
- WebVPN アクセスに使用するサーバや Uniform Resource Locator（URL）のリストを作成します。
- WebVPN ユーザ用のグループ ポリシーを作成します。
- トンネル グループに新しいグループ ポリシーを適用します。

> **注**：ASA リリース 9.4 以降では、SSL 暗号の選択に使用されるアルゴリズムが変更されています（『Cisco ASA シリーズ 9.4(x) リリース ノート』を参照）。楕円曲線対応クライアントのみを使用する場合は、証明書に楕円曲線の秘密キーを使用すると安全です。この方法を使用しない場合は、ASA による自己署名仮証明書の提示を避けるために、カスタム暗号スイートを使用する必要があります。**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" コマンドを使用すると、ASA が RSA ベースの暗号化のみを使用**

するように設定できます。

1. **オプション 1：pkcs12 ファイルで証明書をインポートする。**[Configuration] > [Firewall] > [Advanced] > [Certificate Management] > [Identity Certificates] > [Add] を選択します。pkcs12 ファイルを使用して証明書をインストールするか、プライバシー強化メール（PEM）形式で証明書の内容を貼り付けます。

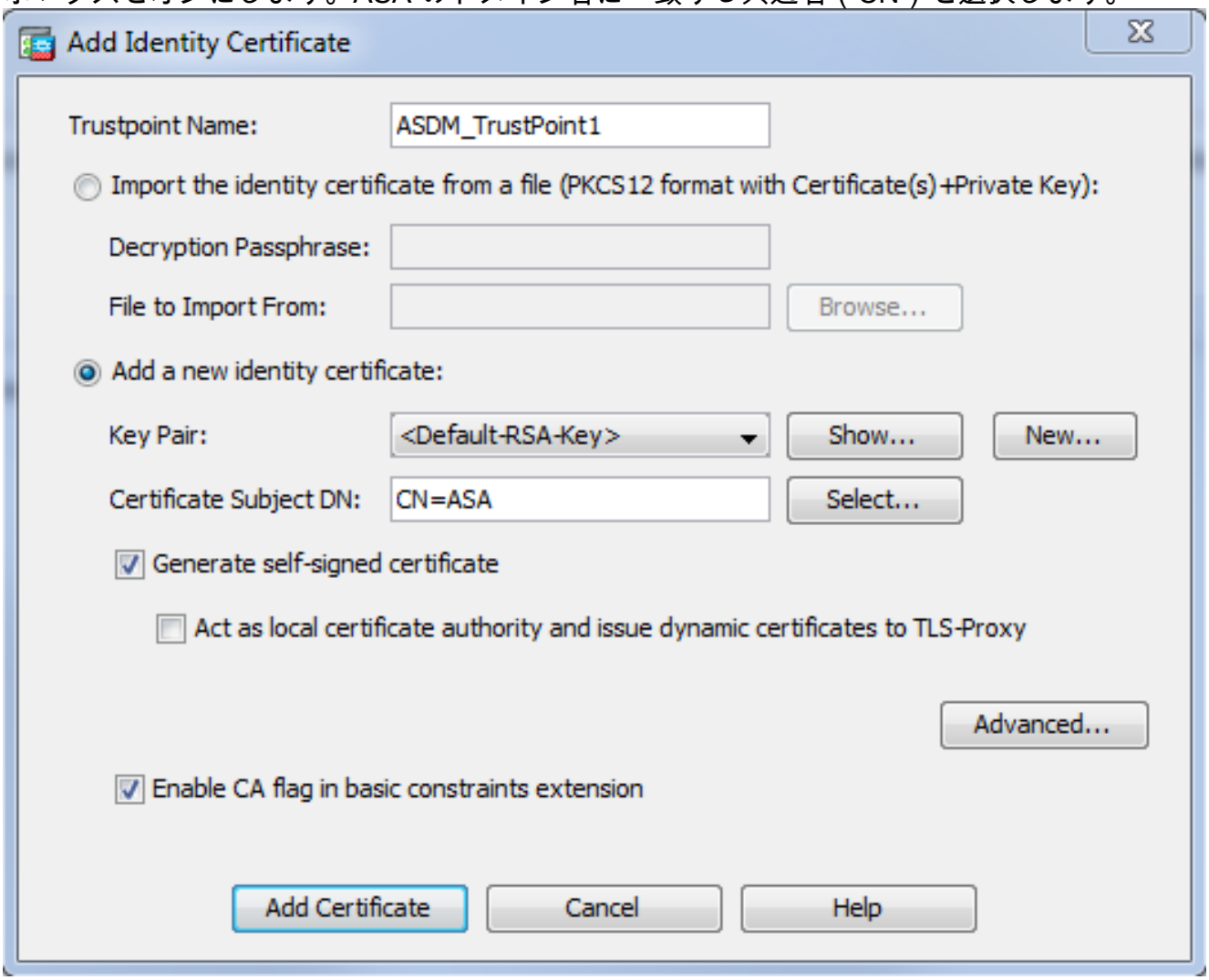


CLI：

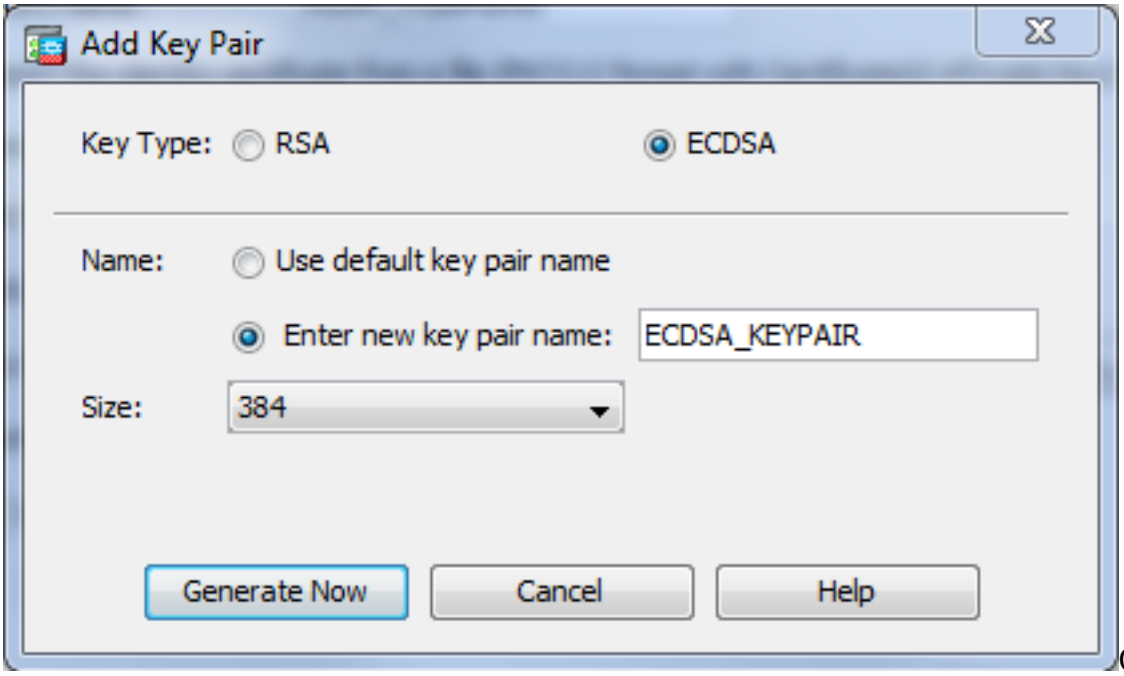
```
ASA(config)# crypto ca import TrustPoint-name pkcs12 "password"


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
```

オプション 2：自己署名証明書を作成する。[Configuration] > [Firewall] > [Advanced] > [Certificate Management] > [Identity Certificates] > [Add] を選択します。**Add a new identity certificate** オプション ボタンをクリックします。[Generate self-signed certificate] チェックボックスをオンにします。ASA のドメイン名に一致する共通名（CN）を選択します。



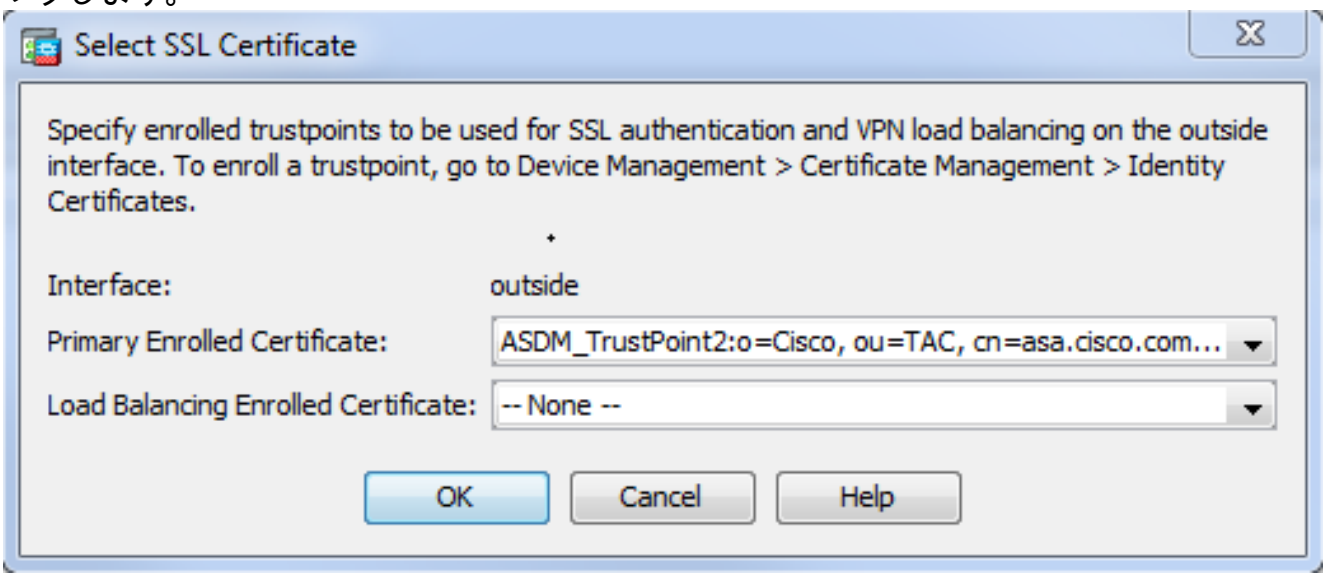
[New] をクリックして証明書のキー ペアを作成します。[Key Type]、[Name]、[Size] を選択します。



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. WebVPN 接続の確立に使用する証明書を選択します。[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings] を選択します。[Certificates] メニューから、外部インターフェイスに必要な証明書に関連付けられたトラストポイントを選択します。[apply] をクリックします。

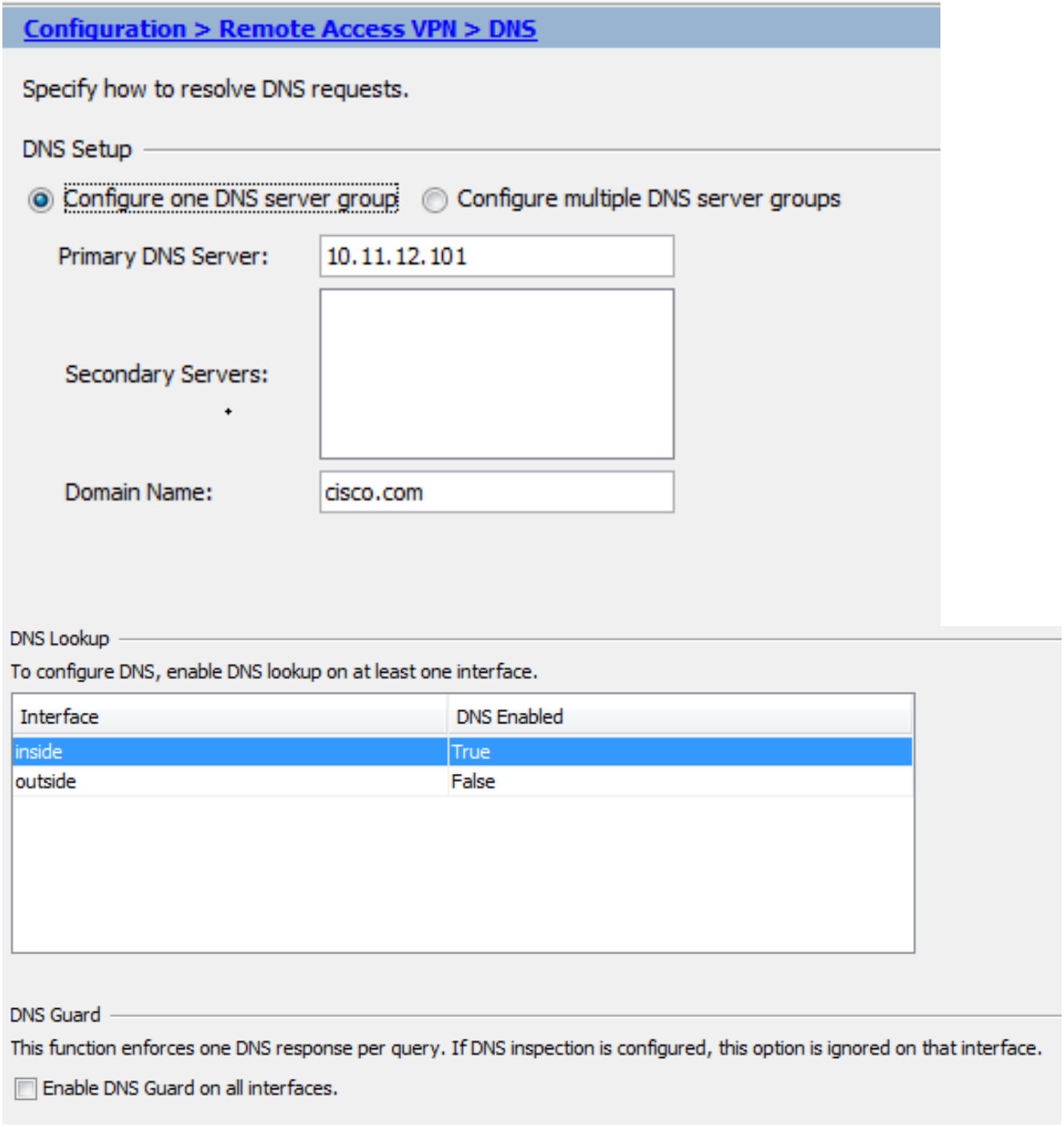


同等の CLI 設定：

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

3. （任意）ドメイン ネーム サーバ（DNS）ルックアップを有効にします。WebVPN サーバは

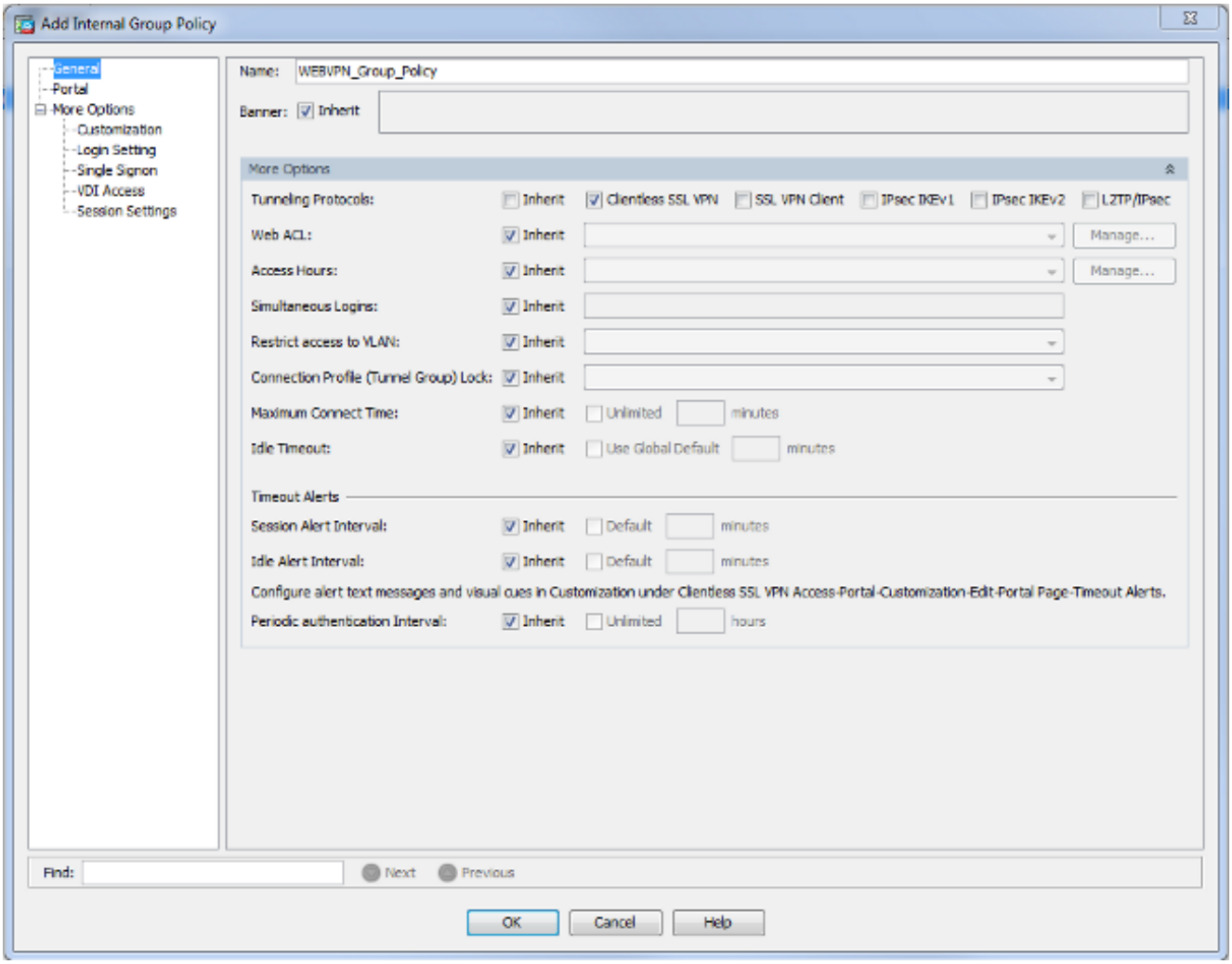
クライアント接続のプロキシとして動作します。つまり、ASA がクライアントに代わってリソースへの接続を作成することになります。クライアントでドメイン名を使用するリソースへの接続が必要になった場合は、ASA が DNS ルックアップを実行する必要があります。[Configuration] > [Remote Access VPN] > [DNS] を選択します。少なくとも 1 つの DNS サーバを設定し、DNS サーバに接続されているインターフェイスで DNS ルックアップを有効にします。



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. （任意）WEBVPN 接続のグループ ポリシーを作成します。[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Add Internal Group Policy] を選択します。[General] オプションで、[Tunelling Protocols] の値を [Clientless SSL VPN] に変更します。



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
```

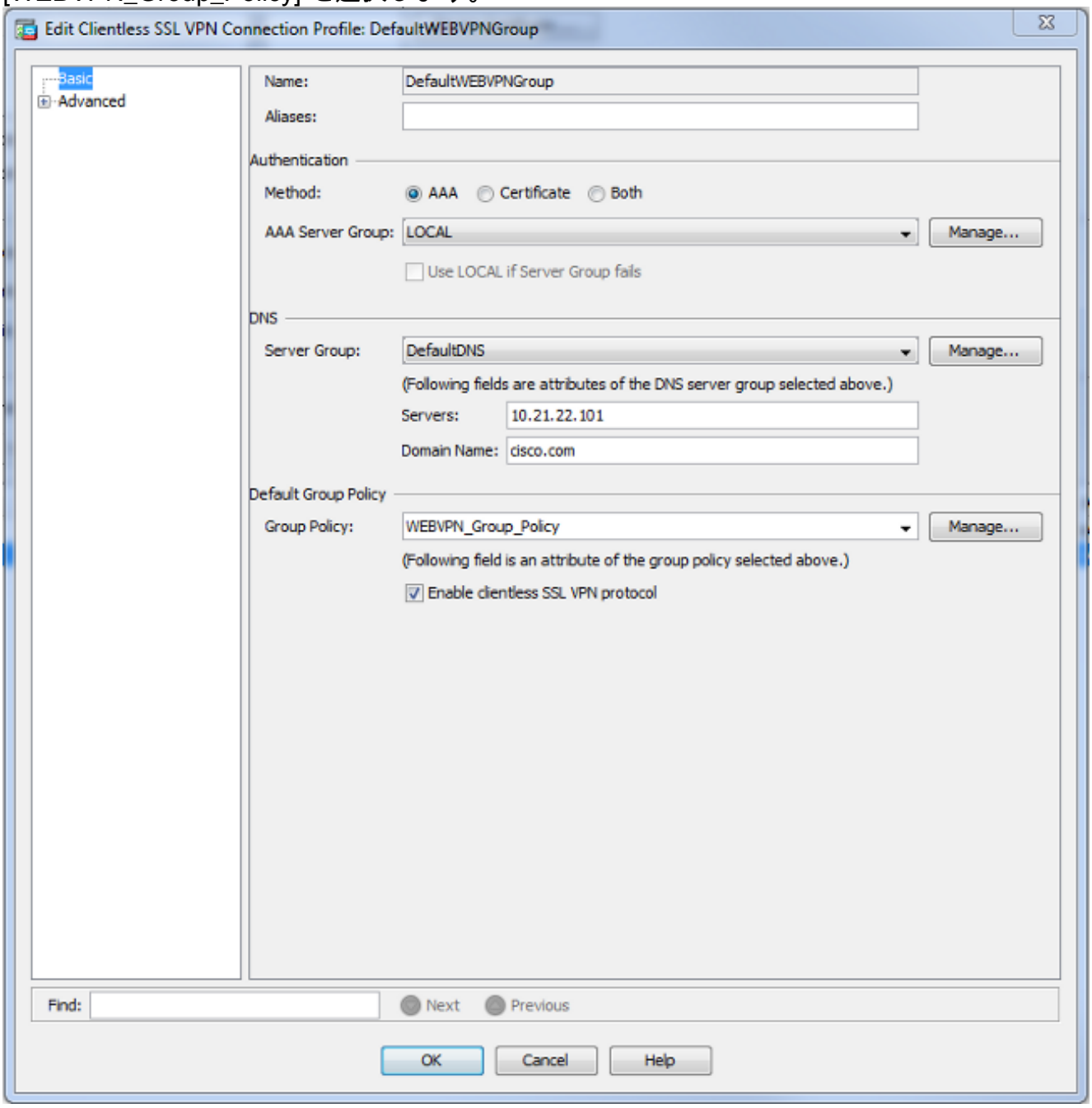
5. 接続プロファイルを設定します。ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] を選択します。
接続プロファイルとグループ ポリシーの概要については、『Cisco ASA シリーズ VPN 9.4 CLI コンフィギュレーション ガイド』の「接続プロファイル、グループ ポリシー、およびユーザ」を参照してください。デフォルトでは、WebVPN 接続には DefaultWEBVPNGroup プロファイルが使用されます。追加のプロファイルを作成できます。**注**：ユーザを他のプロファイルに割り当てるには、さまざまな方法があります。

- ユーザはドロップダウン リストまたは特定の URL を使用して、手動で接続プロファイルを選択できます。『ASA 8.x：WebVPN ログイン時のグループ エイリアスおよびグループ URL メソッドを使用したグループの選択をユーザに許可する』を参照してください。

- LDAP サーバを使用する場合は、LDAP サーバから受信した属性に基づいてユーザ プロファイルを割り当てることができます。『ASA で使用する LDAP 属性マップの設定例』を参照してください。

- 証明書ベースのクライアント認証を使用する場合は、証明書に含まれるフィールドに基づいてユーザをプロファイルにマッピングできます。『Cisco ASA シリーズ VPN 9.4 CLI コンフィギュレーション ガイド』の「IKEv1 の証明書グループ照合の設定」を参照してください。

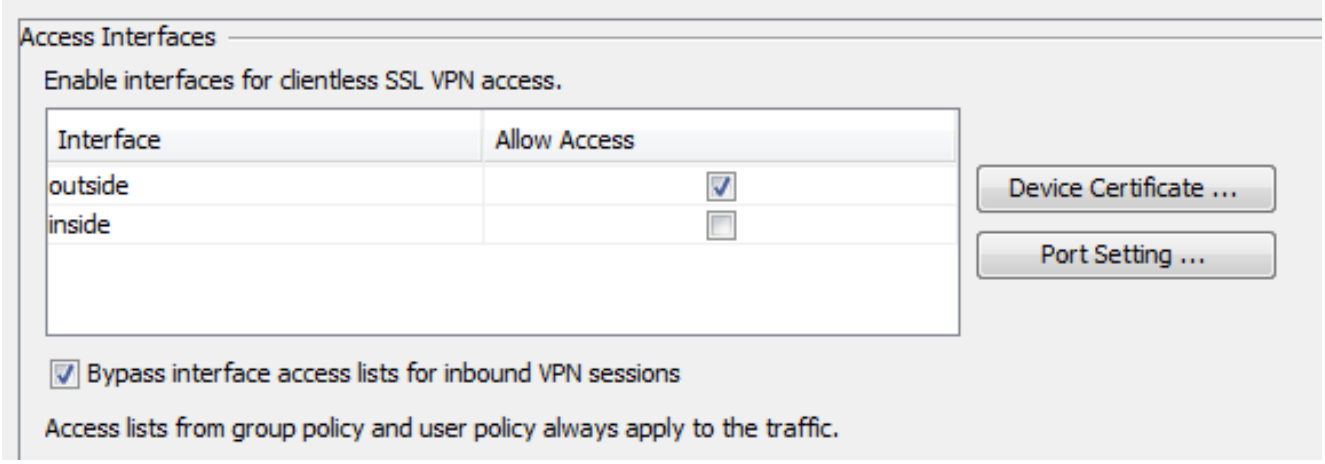
- グループ ポリシーにユーザを手動で割り当てるには、『Cisco ASA シリーズ VPN 9.4 CLI コンフィギュレーション ガイド』の「個々のユーザの属性の設定」を参照してください
DefaultWEBVPNGroup プロファイルを編集して、[Default Group Policy] で [WEBVPN_Group_Policy] を選択します。



CLI：

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

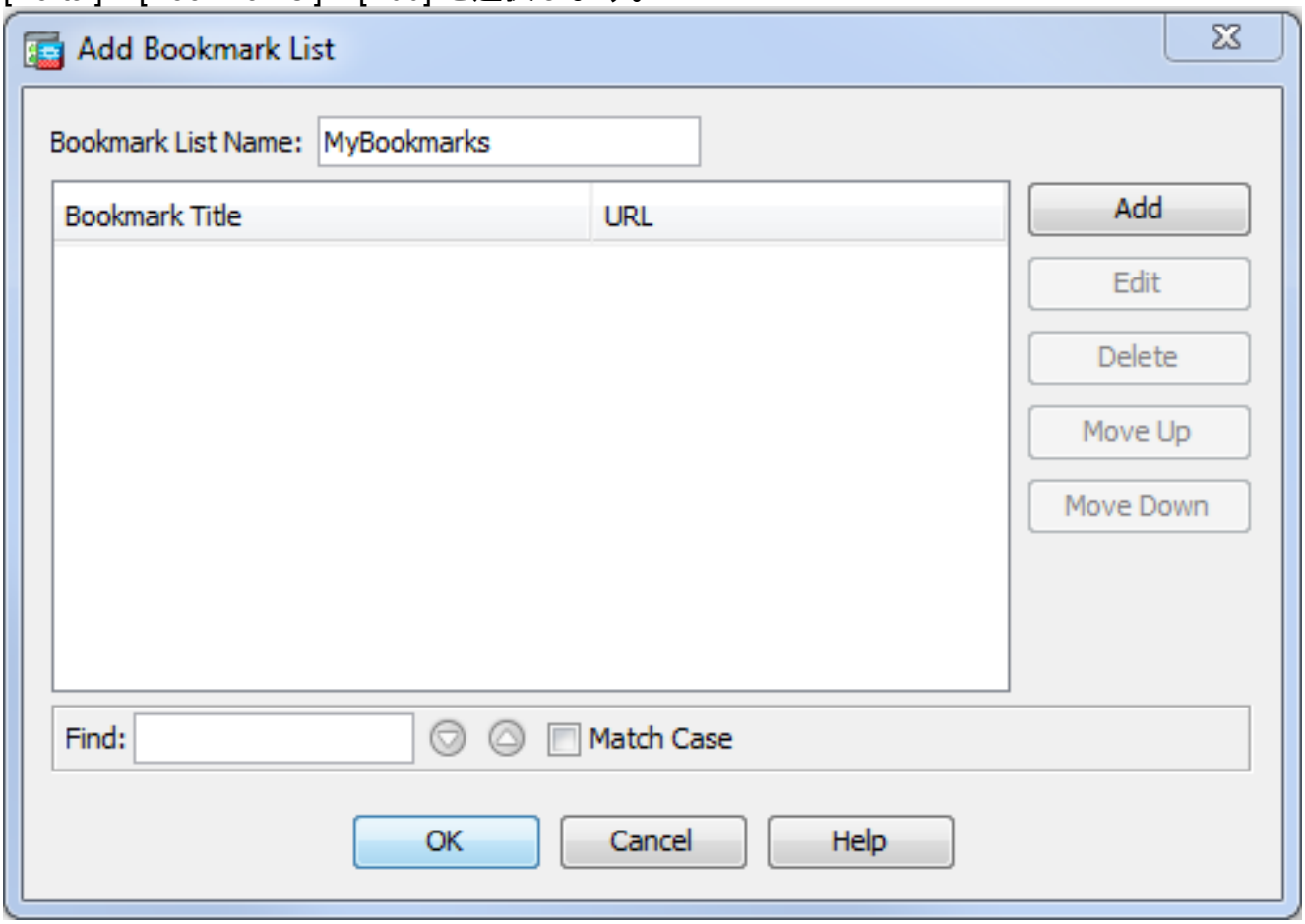
6. 外部インターフェイスで WebVPN を有効にするには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] を選択します。外部インターフェイスの横の [Allow Access] **チェックボックスをオンにします。**



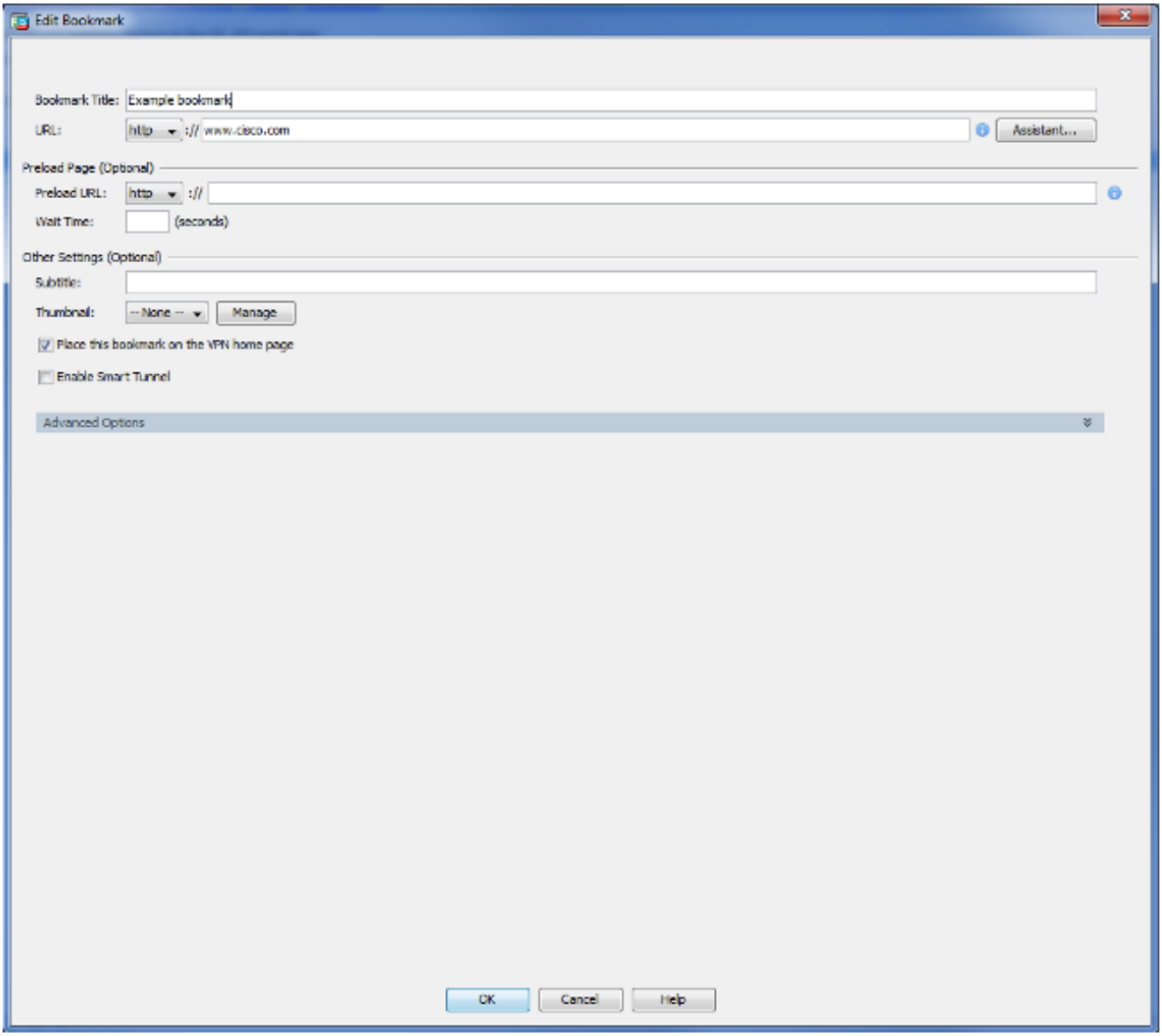
CLI：

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

7. （任意）コンテンツのブックマークを作成します。ブックマークを使用すれば、ユーザは簡単に内部リソースを参照できます。URL を覚えておく必要はありません。ブックマークを作成するには、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Portal] > [Bookmarks] > [Add] を選択します。

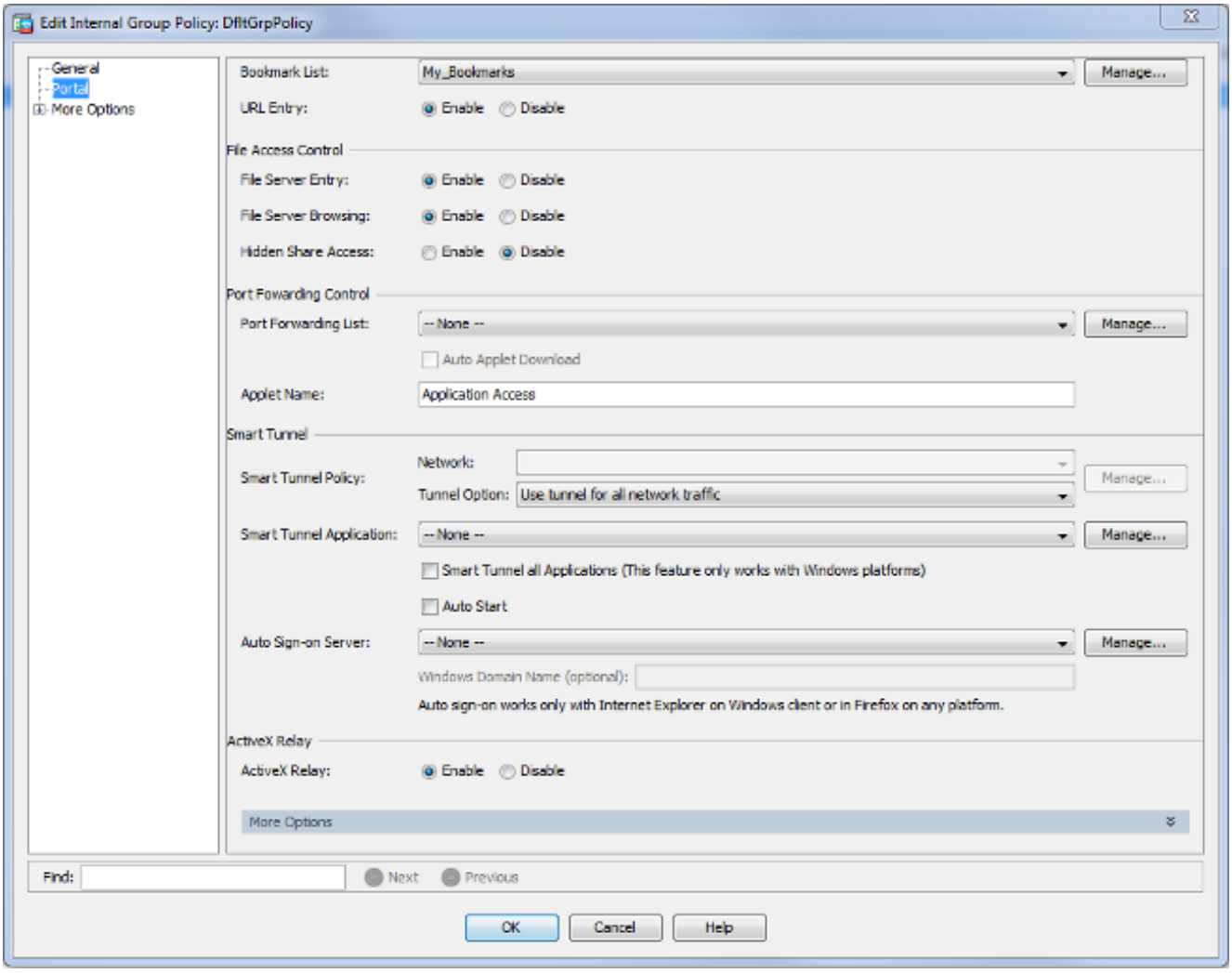


[Add] を選択して特定のブックマークを追加します。



CLI：ブックマークは XML ファイルとして作成されるため、CLI を使用してブックマークを作成することはできません。

8. （任意）特定のグループ ポリシーにブックマークを割り当てます。[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Group Policies] > [Edit] > [Portal] > [Bookmark List] を選択します。

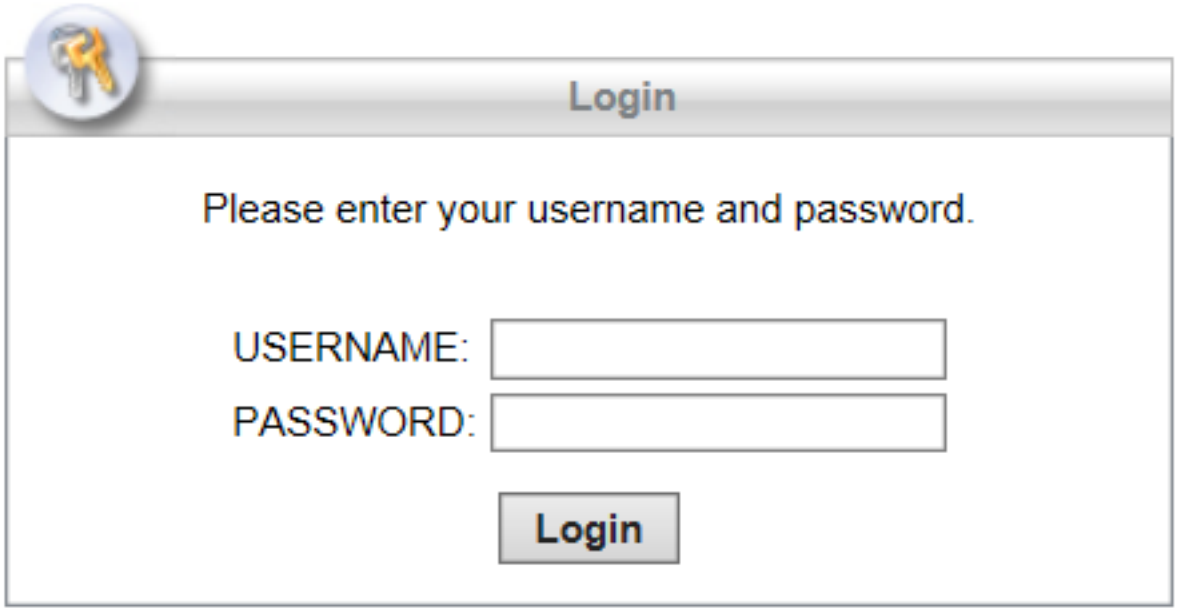


CLI：

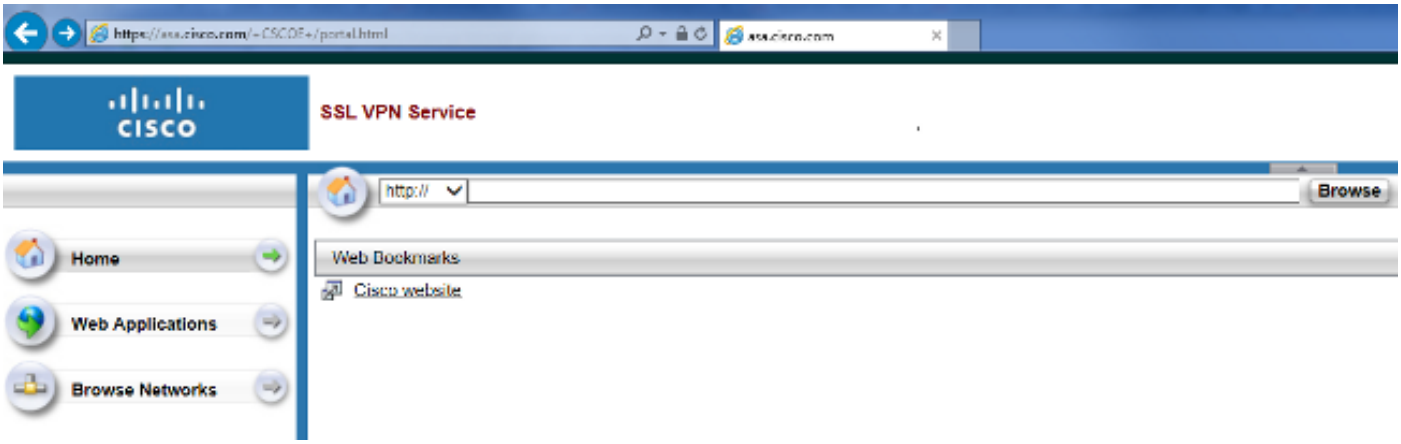
```
ASA(config)# group-policy DfltGrpPolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

確認

WebVPN の設定が完了したら、ブラウザで https://<FQDN of the ASA> アドレスを使用します。



ログインすると、Web サイトおよびブックマークへの移動に使用するアドレス バーが表示されます。



トラブルシュート

トラブルシューティングに使用する手順

設定のトラブルシューティングをするには、次の手順を実行します。

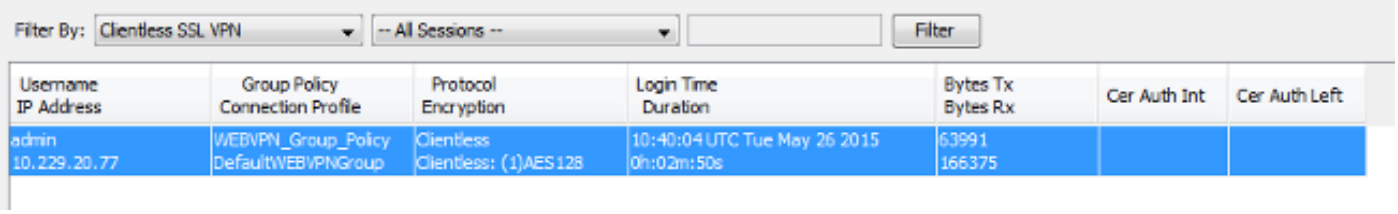
ASDM で、[Monitoring] > [Logging] > [Real-time Log Viewer] > [View] の順に選択します。クライアントと ASA の接続では、TLS セッションの確立、グループ ポリシーの選択、ユーザの認証成功に注意してください。

```
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
```

ASDM で、[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] > [Filter by:**Clientless SSL VPN] を選択します。**新しい WebVPN セッションを探します。WebVPN フィルタを選択して、[Filter] をクリックします。問題が発生する場合は、一時的に ASA デバイスをバイパスさせ、指定したネットワーク リソースにクライアントがアクセスできるかどうかを確認します。また、このドキュメントの設定手順を再確認してください。



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
```

トラブルシューティングに使用するコマンド

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：debug コマンドを使用する前に、「デバッグ コマンドの重要な情報」を参照してください。

- **show webvpn：WebVPN に関連付けられている show コマンドは多数存在します。show コマンドの使用方法を確認するには、Cisco セキュリティ アプライアンスの「コマンド リファレンス」を参照してください。**
- **debug webvpn：debug コマンドの使用は、ASA に悪影響を及ぼす可能性があります。debug コマンドの使用方法を確認するには、Cisco セキュリティ アプライアンスの「コマンド リファレンス」を参照してください。**

一般的な問題

ユーザがログインできない

問題

ログイン試行が失敗し、「Clientless (browser) SSL VPN access is not allowed」というメッセージが ブラウザに表示されます。ASA に AnyConnect Premium ライセンスがインストールされていないか、または「Premium AnyConnect license is not enabled on the ASA」と表示される場合はこのライセンスが使用されていません

解決方法

次のコマンドを使用して、Premium AnyConnect ライセンスを有効にします。

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

問題

ログイン試行が失敗し、「Login failed」メッセージがブラウザに表示されます。AnyConnect のライセンス制限を超えています。

解決方法

ログで次のメッセージを探します。

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

さらに、ライセンス制限を確認します。

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

問題

ログイン試行が失敗し、「AnyConnect is not enabled on the VPN server」というメッセージがブラウザに表示されます。クライアントレス VPN プロトコルがグループ ポリシーで有効になっていません。

解決方法

ログで次のメッセージを探します。

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

目的のグループ ポリシーに対して、クライアントレス VPN プロトコルが有効になっていることを確認します。

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

最大 3 人の WebVPN ユーザしか ASA に接続できない

問題

ASA に接続できる WebVPN クライアントが 3 つのみで、4 つ目のクライアントは接続できません。

解決方法

ほとんどの場合、この問題はグループ ポリシー内の同時ログイン設定に関係しています。同時ログインの必要数を設定するには、次の例を使用します。この例では、必要な値は 20 です。

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

WebVPN クライアントでブックマークがグレー表示されてクリックできない

問題

クライアントレス VPN にログインするユーザ用に設定されたブックマークが、ホーム画面の [Web Applications] でグレー表示される場合、これらの HTTP リンクを有効にして、ユーザがクリックすることで特定の URL にアクセスできるようにするにはどうすればよいでしょうか。

解決方法

最初に、ASA が DNS を介して Web サイトを解決できていることを確認します。Web サイトの名前を使用して ping を発行してみてください。ASA が名前を解決できない場合、そのリンクはグレー表示されます。DNS サーバがネットワークの内部にある場合は、DNS ドメイン ルックアップ プライベート インターフェイスを設定します。

WebVPN を介した Citrix 接続

問題

WEBVPN を介した Citrix への接続で "the ica client received a corrupt ica file." というエラー メッセージが が表示されます。

解決方法

WebVPN を介した Citrix への接続に *セキュア ゲートウェイ モードを使用すると、ICA ファイルが破損する場合があります。*ASA はこの動作モードと互換性がないので、ダイレクト モード (非セキュア モード) で新しい ICA ファイルを作成してください。

ユーザの 2 度目の認証を不要にする方法

問題

クライアントレス WebVPN ポータルで CIFS リンクにアクセスした場合、ブックマークをクリックするとクレデンシャルの入力を求められます。Lightweight Directory Access Protocol (LDAP) は、リソースと、すでに LDAP クレデンシャルを入力して VPN セッションにログイン済みのユーザの両方の認証に使用されます。

解決方法

この場合は、自動サインオン機能を使用できます。特定のグループ ポリシーが使用されている状況下で、そのポリシーの WebVPN 属性を次のように設定します。

```
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
```

ここで`CIFSX.X.X.X=IP`と、対象の共有ファイル/フォルダに到達するための残りのパスを示します。

設定例のスニペットを次に示します。

```
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
```

これに関する詳細については、『HTTP 基本認証または NTLM 認証による SSO の設定』を参照してください。

関連情報

- ASA：ASDM を使用したスマート トンネルの設定例
- テクニカル サポートとドキュメント – Cisco Systems