ASA でのクライアントレス SSL VPN（WebVPN）の設定

目次

概要

この文書は（ASA） 5500 シリーズに内部ネットワーク リソースへの Clientless Secure Sockets Layer （SSL） VPN アクセスを許可するために簡単な設定を Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア提供したものです。 Clientless SSL バーチャル プライベート ネットワーク（WebVPN）はあらゆる位置からの社内ネットワークへの限られた、貴重品を、安全なアクセス可能にします。 ユーザは共有リソースへのセキュア ブラウザ・ベースのアクセスをいつでも実現できます。 追加クライアントは内部リソースへのアクセス権を得るため必要ではないです。 アクセスは SSL 接続上の a を使用して Hypertext Transfer Protocol（HTTP）提供されます。

Clientless SSL VPN はインターネット（HTTP）サイトに Hypertext Transfer Protocol（HTTP）達することができるほとんどあらゆるコンピュータからの Web リソースおよびウェブで可能およびレガシー アプリケーションの広い範囲へのセキュアおよび簡単なアクセスを提供します。 これには下記のものが含まれます。

- 内部 Webサイト

- Microsoft SharePoint 2003、2007 年、および 2010
- Microsoft Outlook Web アクセス 2003 年、2007 年、および 2013
- Microsoft Outlook Web アプリケーション 2010
- Domino Web アクセス（DWA）8.5 および 8.5.1
- Citrix Metaframe プレゼンテーション サーバ 4.x
- 6.5 への Citrix XenApp バージョン 5
- 5.6 への Citrix XenDesktop バージョン 5、および 7.5
- VMware ビュー 4

支援ソフトウェアのリストはサポートされた VPN プラットフォームで Cisco ASA 5500 シリーズ見つけることができます。

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 イネーブルになったブラウザ
- バージョン 7.1 以上がインストールされた ASA
- ASA ドメイン名に発行される 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

要件の詳細なリストはサポートされた VPN プラットフォームで Cisco ASA 5500 シリーズ見つけることができます。

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くものです。

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

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

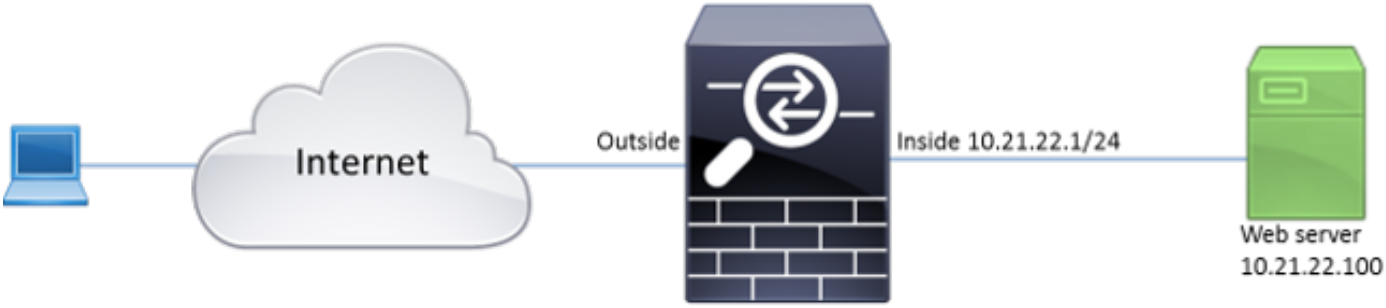
設定

この技術情報は ASDM および CLI 両方のためのコンフィギュレーションプロセスを説明します。WebVPN を設定するためにツールのどちらかに続くことを選択できますいくつかのコンフィギュレーションのステップは ASDM としか達成することができません。

> **注:** このセクションで使用されてい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、次のネットワーク構成を使用しています。



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き、ASA はブラウザにそれ自身を認証するために証明書を示します。 クライアントと ASA 間の接続がセキュアであることを確認するために、その認証局によってクライアント信頼既に署名している証明書を ASA に与える必要があります。 他では接続は信頼されないことブラウザが警告を発声するので、クライアントに man-in-the-middle攻撃および悪いユーザ エクスペリエンスの可能性という結果に終る ASA の信頼性を確認する方法がありません。

> **注:** デフォルトで、ASA は始動に自己署名 X.509 証明書を生成します。 この証明書はクライアント接続にデフォルトで役立つために使用されます。 信頼性がブラウザによって確認することができないのでこの証明書を使用することを推奨しません。 なお、この証明書は各リブートに再生します従って各リブートの後で変更します。

認証インストールはこの文書の範囲外にあります。

設定

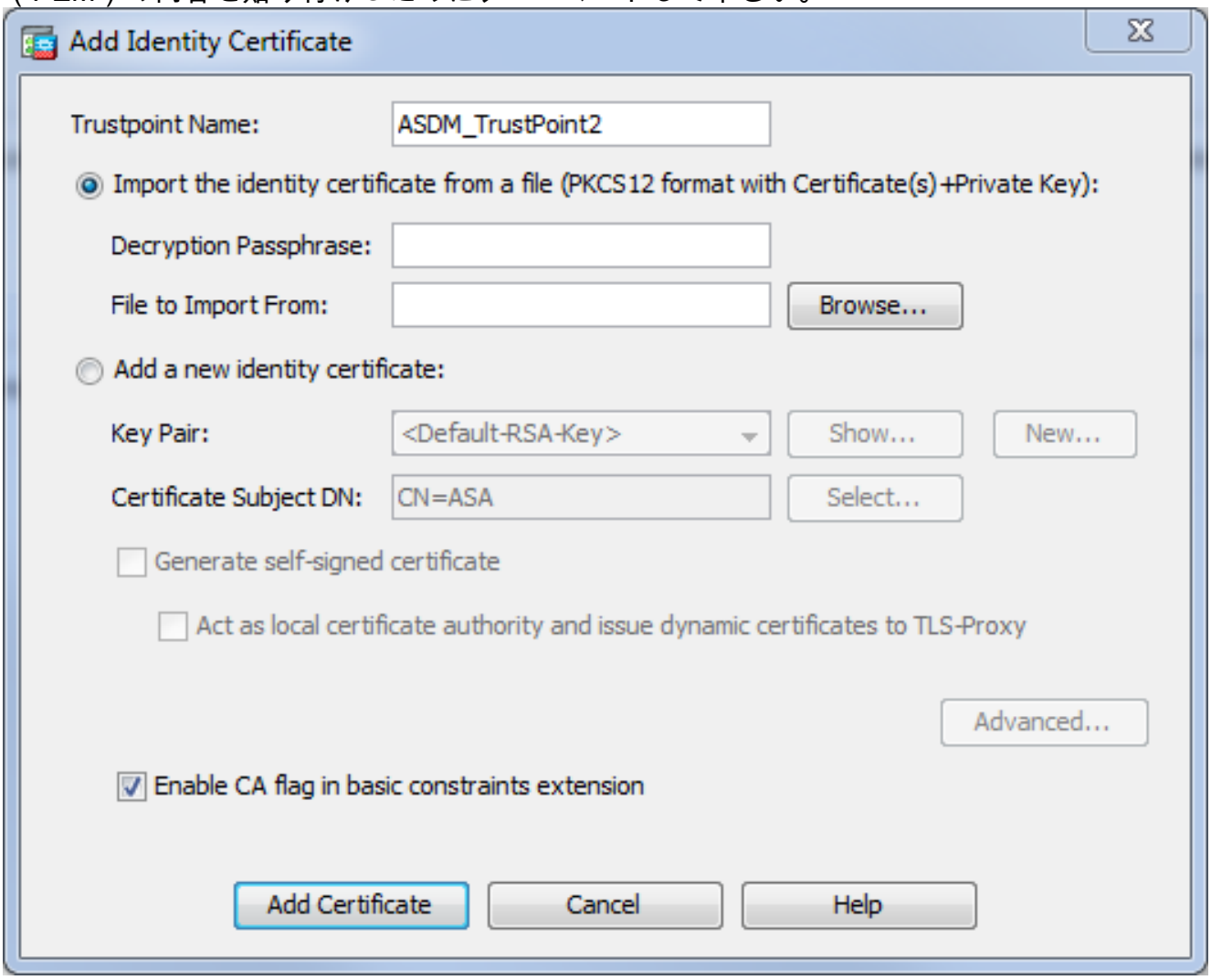
5 つの主要なステップで ASA の WebVPN を設定して下さい:

- ASA によって使用する証明書を設定して下さい。
- ASA インターフェイスで WebVPN を有効にします。
- WebVPN アクセスのためのサーバや Uniform Resource Locator （ URL ）のリストを作成して下さい。
- 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 でリリース 9.4 は、SSL 暗号を選択するのに使用されるアルゴリズム変更されたより以降をリリースします（ Cisco ASA シリーズについてはリリース ノートを、9.4(x)).If 参照して下さい楕円曲線可能なクライアントだけ使用される、そして証明書のために楕円カーブ プライベートキーを使用することは安全です。 自己署名ー時証明書さもなければカスタム暗号スイートは ASA 現在を持っていることを避けるために使用する必要があります。 **ssl 暗号 tlsv1.2 カスタム "AES256 SHA:AES128 SHA:DHE RSA AES256 SHA:DHE RSA**

AES128 SHA:DES CBC3 SHA:DES CBCSHA:RC4 SHA:RC4 MD5" コマンドで RSA ベースの暗号だけ使用するために ASA を設定できます。

1. **オプション 1** - pkcs12 ファイルが付いている証明書をインポートして下さい。**> ファイアウォール > 進めました > Certificate Management > ID証明 > Add を**『Configuration』 を選択して下さい。 pkcs12 ファイルとそれをインストールできますまたは Privacy Enhanced Mail（PEM）の内容を貼り付けるためにフォーマットして下さい。

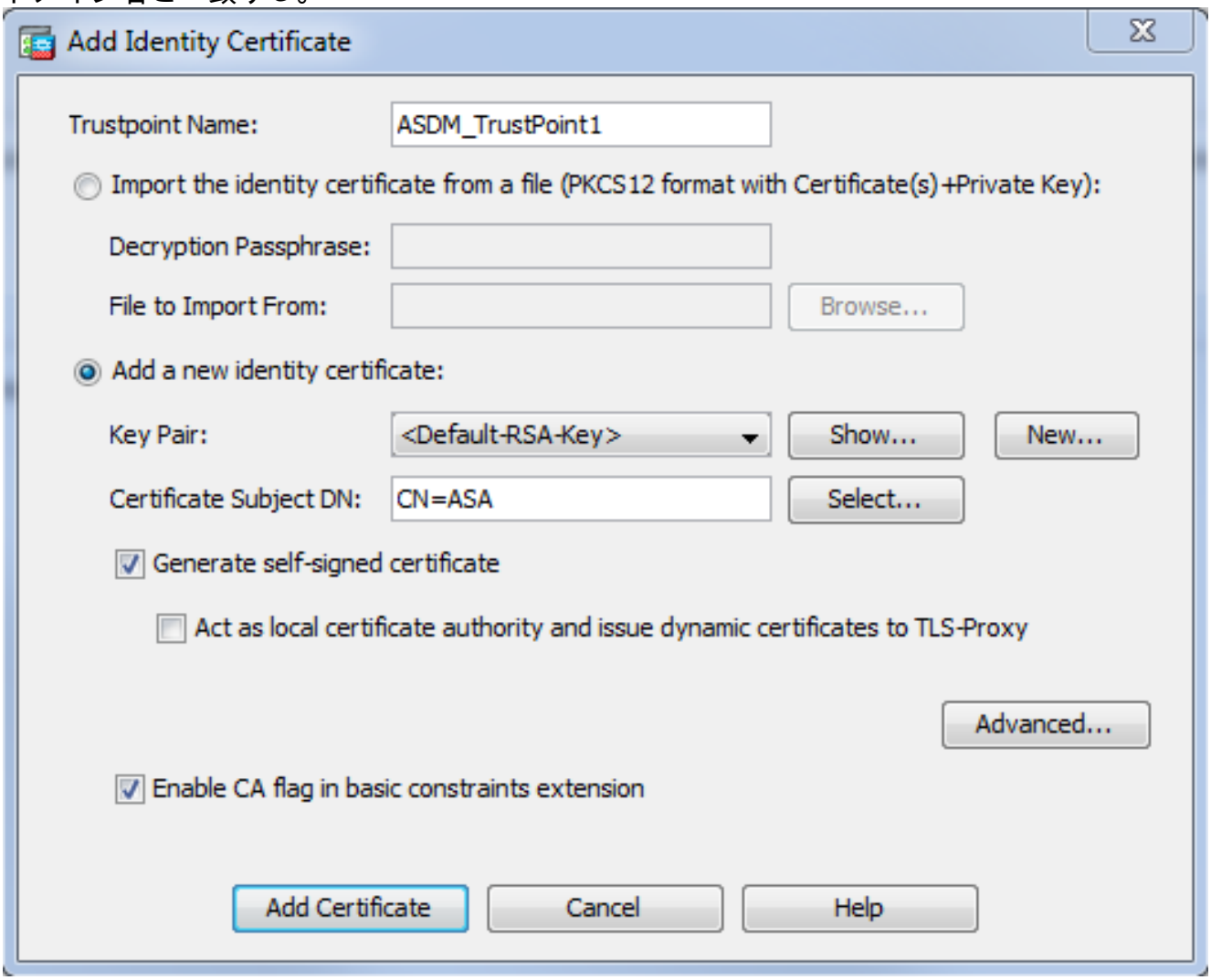


CLI：

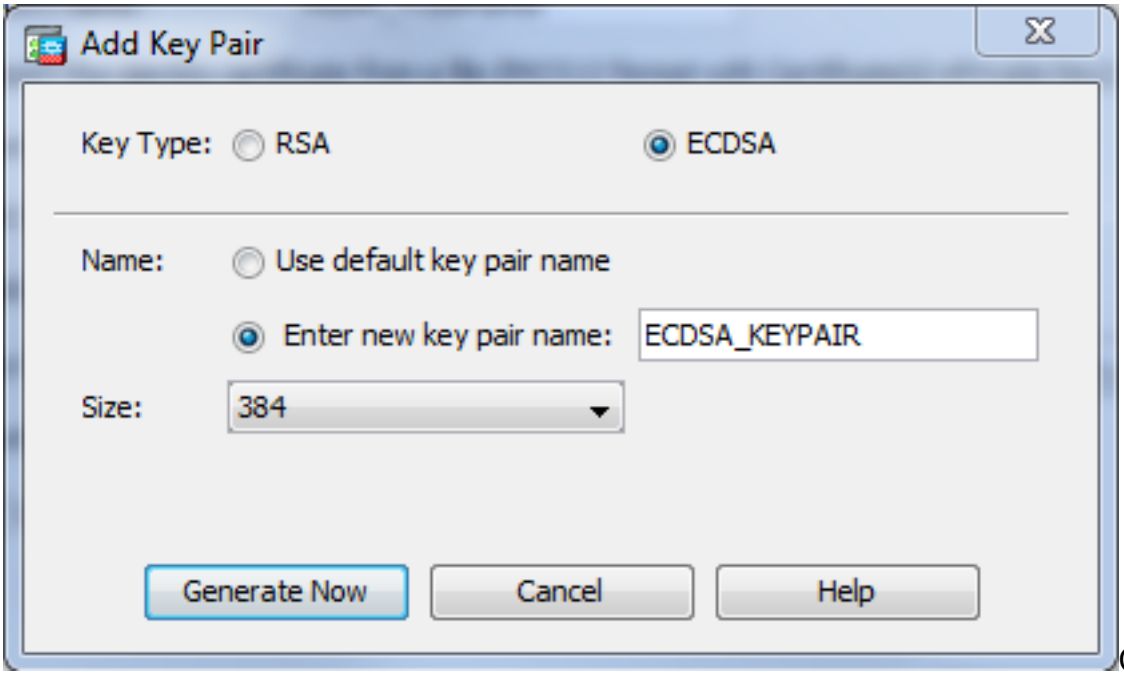
```
ASA(config)# crypto ca import TrustPoint-name pkcs12 "password"



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して下さい。**> ファイアウォール > 進めました > Certificate Management > ID証明 > Add を**『Configuration』 を選択 して下さい。**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**チェックして下さい。 Common Name （ CN ）を選択して下さい ASA のドメイン名と一致する。



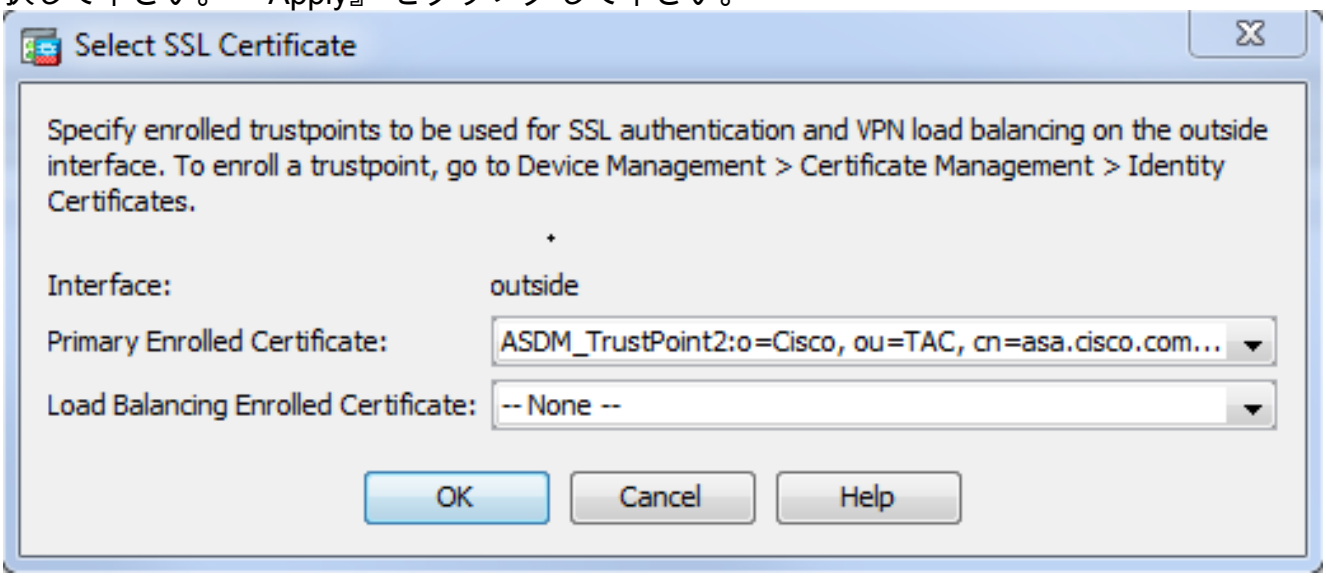
証明書のための keypair を作成するために『New』 をクリック して下さい。 キーの種類、名前およびサイズを選択して下さい。



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 接続に役立つのに使用する証明書を選択して下さい。**> リモートアクセス VPN > 進みました > SSL 設定**『Configuration』 を選択 して下さい。 証明書メニューから、outside インターフェイスのための望ましい証明書と関連付けられるトラストポイントを選択して下さい。 『Apply』 をクリック して下さい。

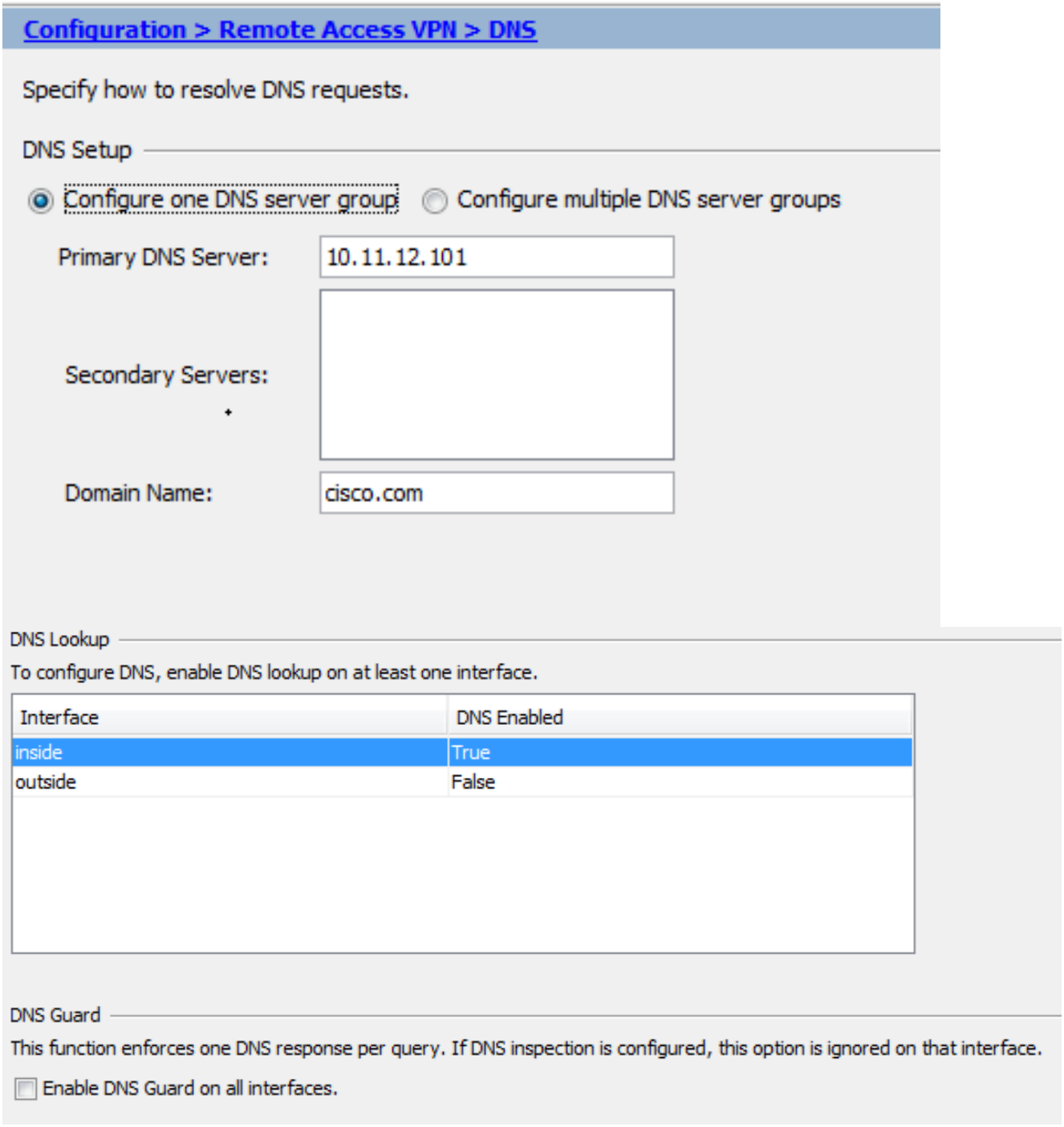


同等の CLI 設定:

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

3. （オプションの）イネーブル Domain Name Server （DNS）ルックアップ。WebVPN サーバはクライアント接続のためのプロキシとして機能します。 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を意味します。 クライアントがドメイン名を使用するリソースへの接続を必要とすれば、ASA は DNS lookup を行う必要があります。**> リモートアクセス VPN > DNS** 『Configuration』 を選択 して下さい。少なくとも 1 つの DNSサーバ

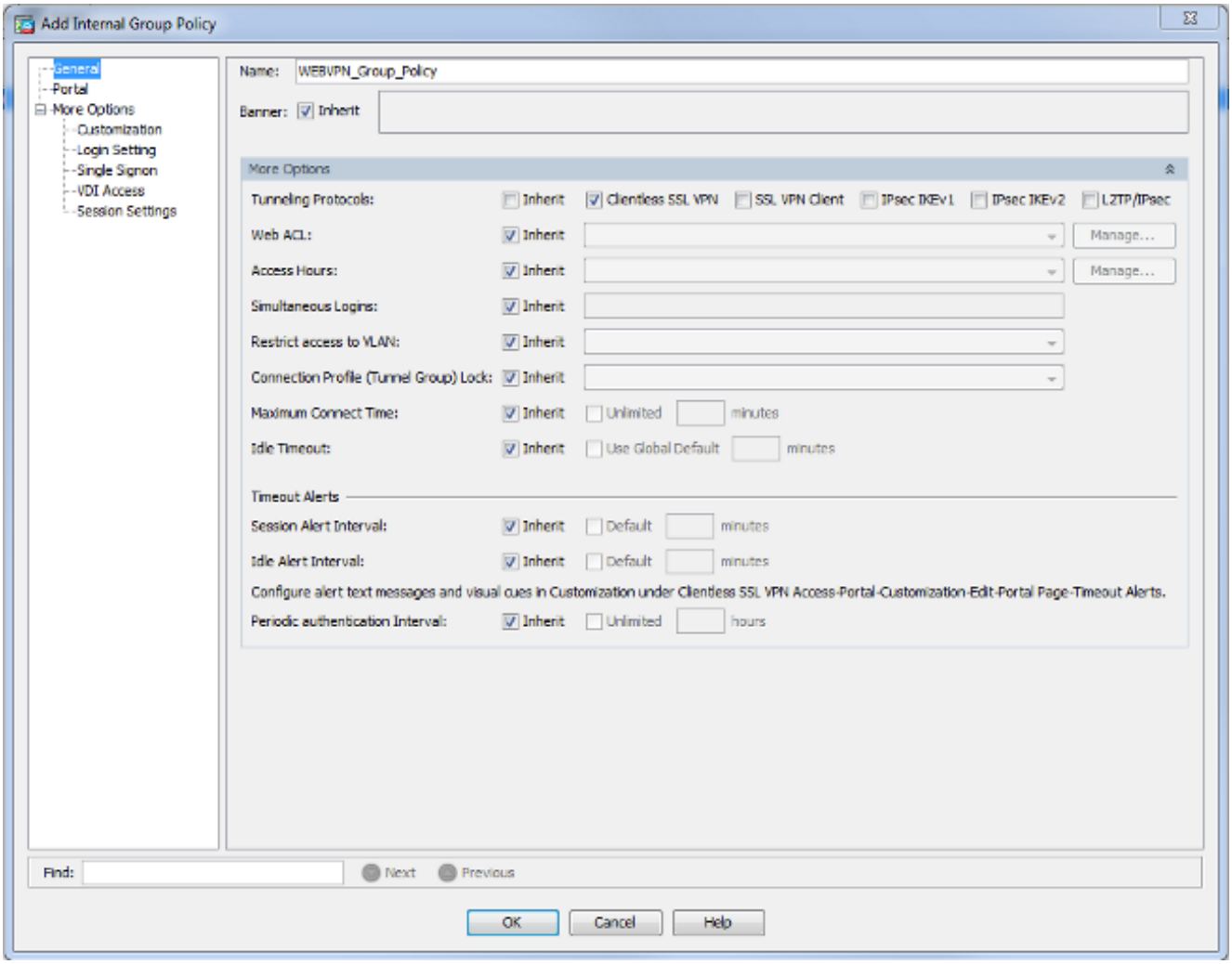
を設定し、DNSサーバに直面するインターフェイスの DNS ルックアップを有効に して下さい。



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. （オプション）WEBVPN 接続のためのグループ ポリシーを作成して下さい。**> リモートアクセス VPN > Clientless SSL VPN アクセス > グループ ポリシー > Add 内部グループ ポリシー**『Configuration』 を選択 して下さい。一般のオプションの下で Protocols 値「Clientless SSL VPN」に Tunelling を変更して下さい。



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て下さい。ASDM で、**> リモートアクセス VPN > Clientless SSL VPN アクセス > 接続プロファイル** 『Configuration』 を選択 して下さい。
接続プロファイルおよびグループ ポリシーの概要に関しては、Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイド、9.4 -接続プロファイル、グループ ポリシーおよびユーザに相談して下さい。デフォルトで、WebVPN 接続使用 DefaultWEBVPNGroup プロファイル。 追加プロファイルを作成できます。**注:** 他のプロファイルにユーザを割り当てるさまざまな方法があります。

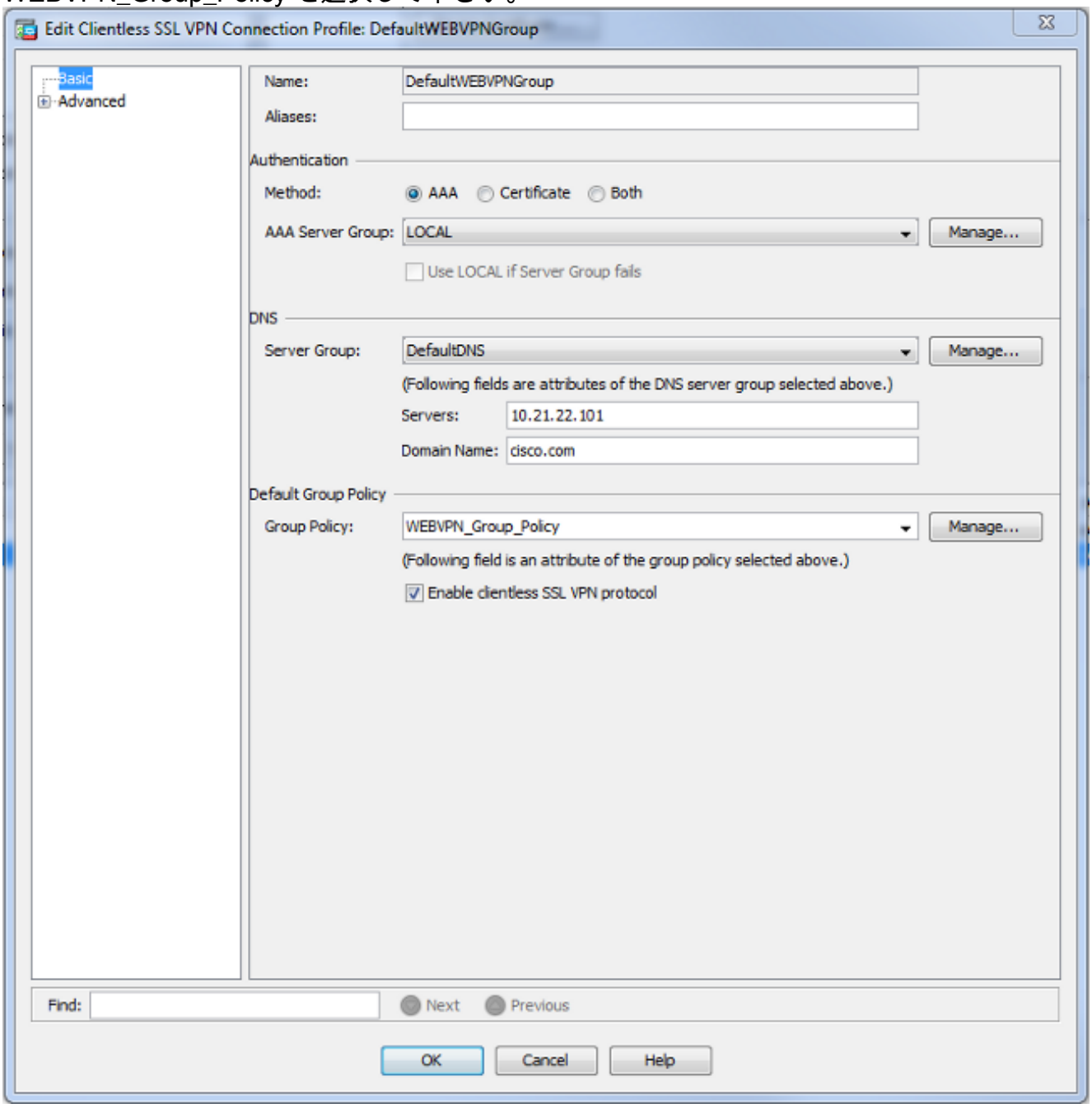
-ユーザはドロップダウン リストからまたは仕様 URL と手動で接続プロファイルを選択できます。 ASA 8.x を参照して下さい: ユーザをグループ エイリアスおよびグループ URL 方式によって WebVPN ログオンでグループを選択することを許可して下さい。

- LDAPサーバを使用する時、見ます LDAP 属性マップ設定例の ASA 使用を LDAPサーバから届く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。

-クライアントの認証ベース認証を使用する時、証明書に含まれているフィールドに基づいてプロファイルに見ます Cisco ASA シリーズ VPN CLI コンフィギュレーション ガイドを、9.4 ユーザをマップできます- IKEv1 のために一致する証明書グループを設定して下さい。

-ユーザをグループ ポリシーに手動で割り当てるために、Cisco ASA シリーズ VPN CLI コン

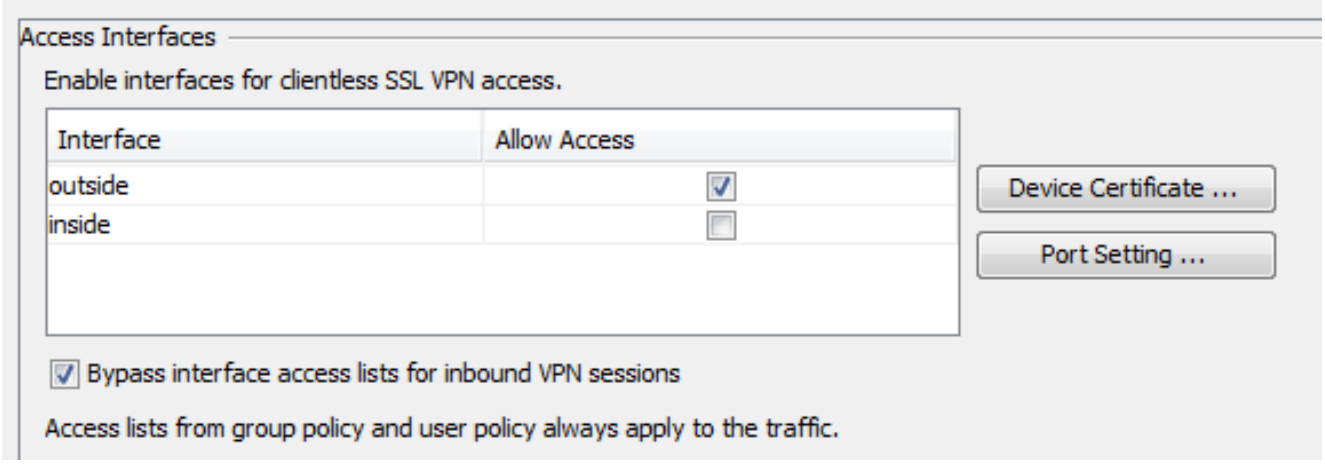
フィギュレーション ガイドを、9.4 -個々のユーザ向けの属性を設定すること参照して下さいDefaultWEBVPNGroup プロファイルを編集し、デフォルト グループ ポリシーの下でWEBVPN_Group_Policy を選択して下さい。



CLI：

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

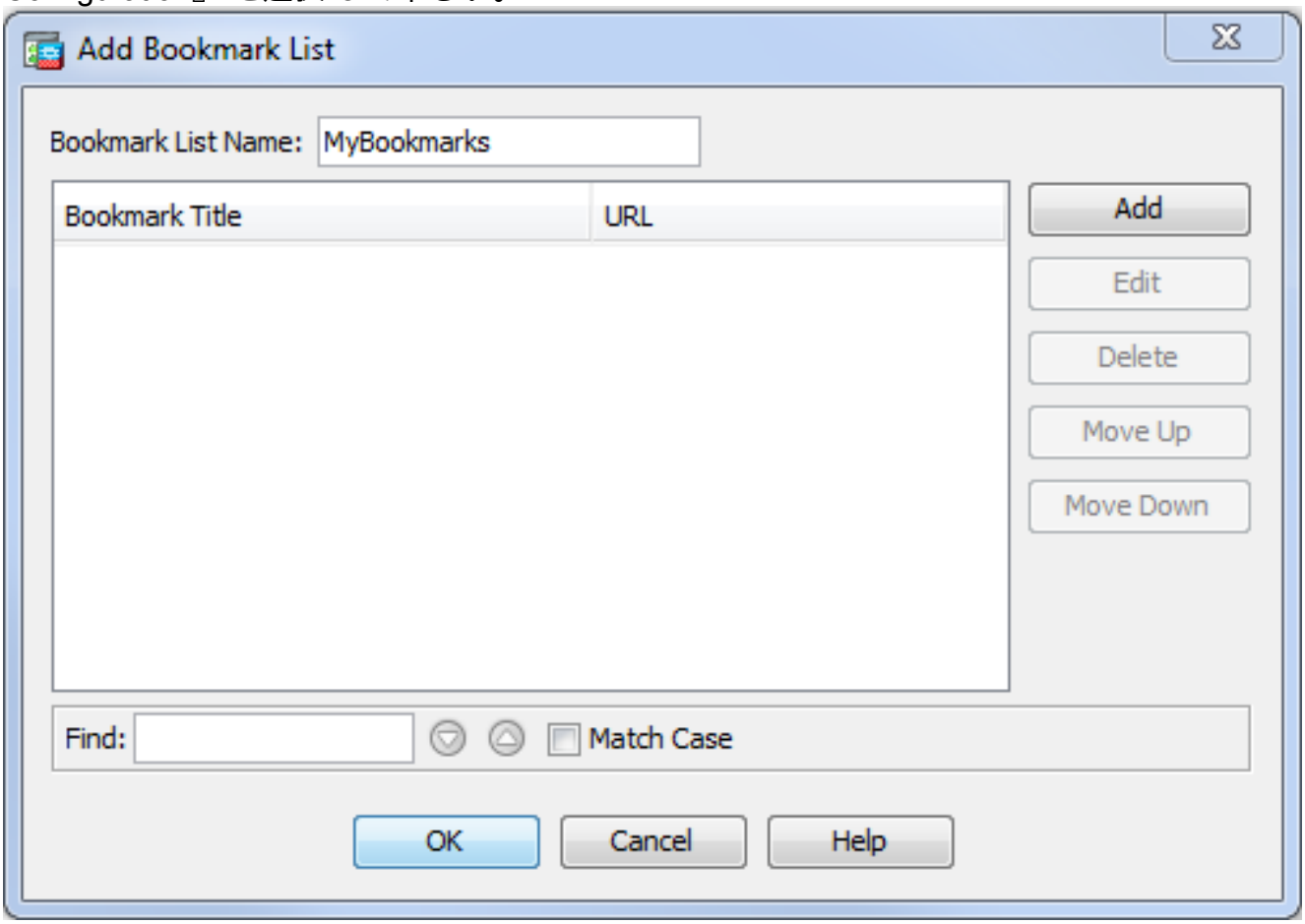
6. outside インターフェイスの WebVPN を有効に するために、**> リモートアクセス VPN > Clientless SSL VPN アクセス > 接続プロファイル** 『Configuration』 を選択 して下さい。outside インターフェイスの隣で **Allow Access チェックボックスを**チェックして下さい。



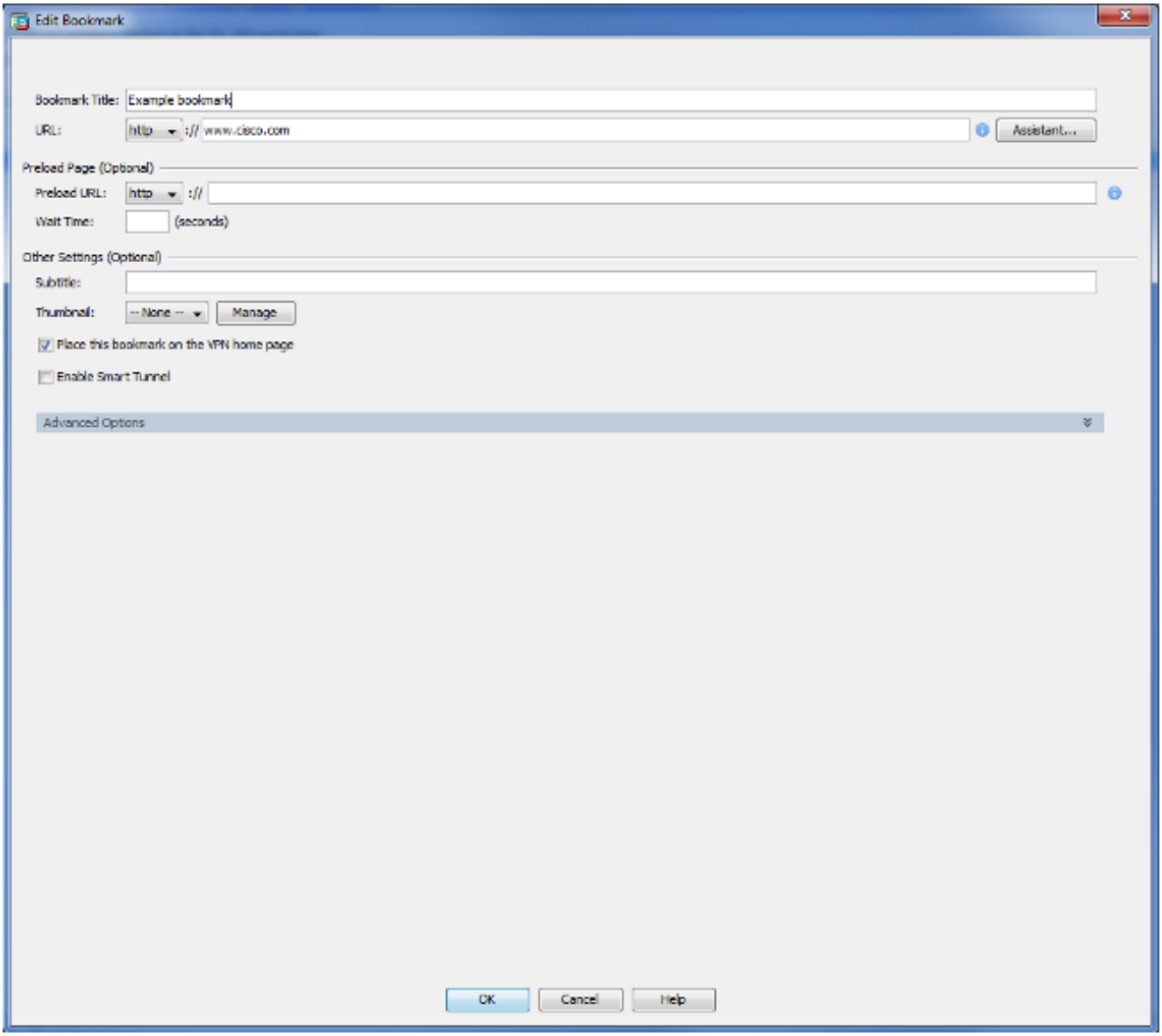
CLI：

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

7. （オプション）内容のためのブックマークを作成して下さい。ブックマーク割り当ては容易に URL を覚えないで内部リソースを参照するユーザ。ブックマークを作成するために、**> リモートアクセス VPN > Clientless SSL VPN アクセス > ポータル > ブックマーク > Add** 『Configuration』 を選択 して下さい。

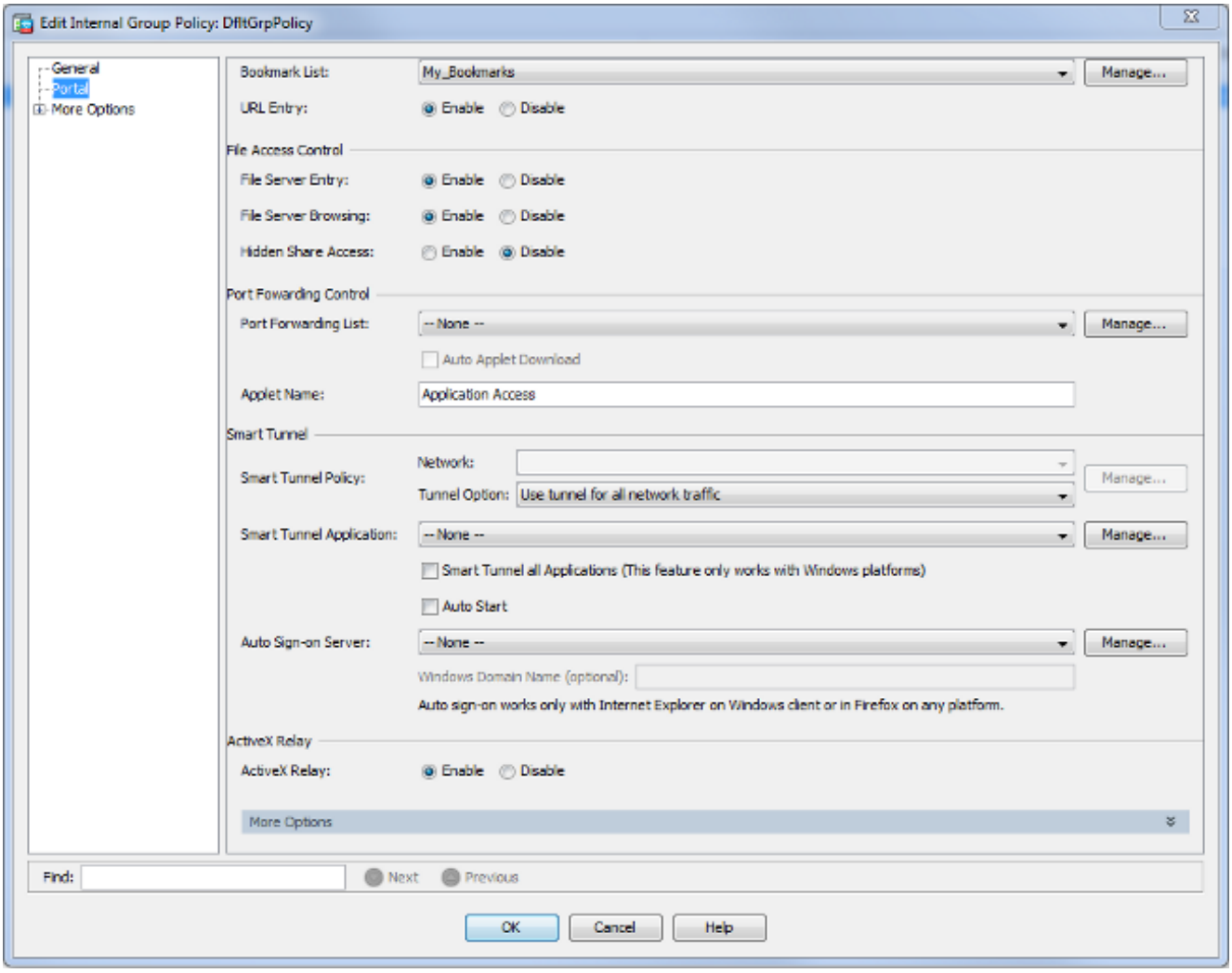


特定のブックマークを追加するために『Add』 を選択 して下さい。



CLI：XML ファイルとして作成されるので CLI によってブックマークを作成することは不可能です。

8. （オプション）特定のグループ ポリシーにブックマークを割り当てて下さい。**> リモートアクセス VPN > Clientless SSL VPN アクセス > グループ ポリシー > Edit > ポータル > ブックマーク リスト**『Configuration』 を選択 して下さい。

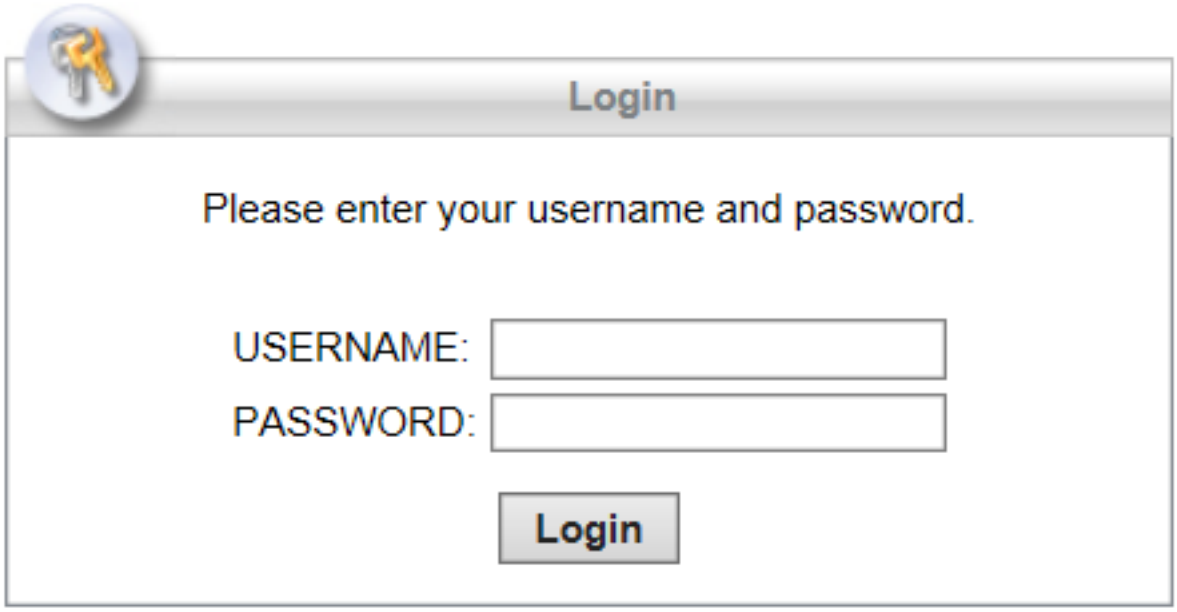


CLI：

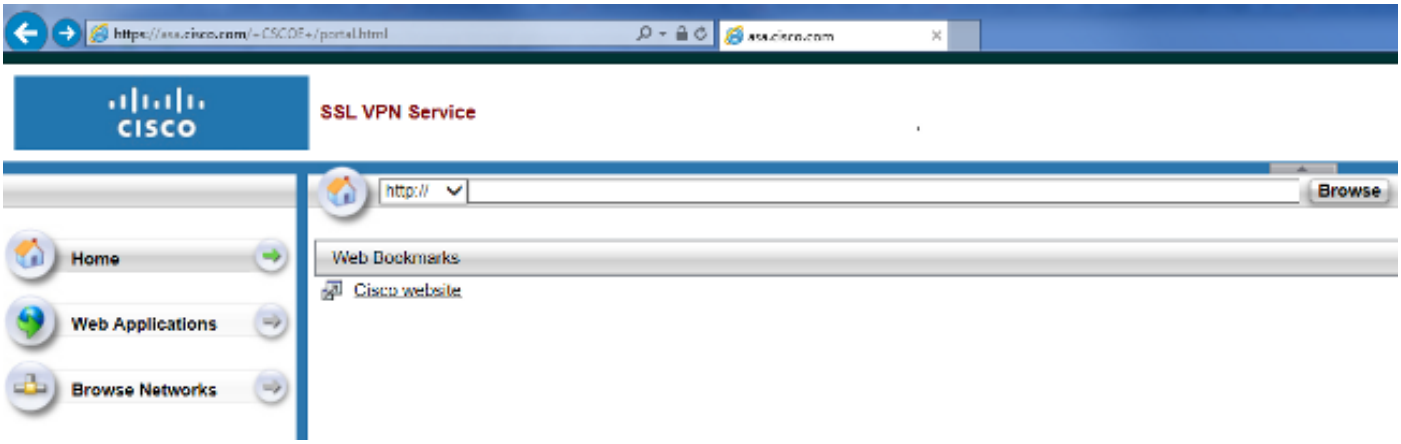
```
ASA(config)# group-policy DfltGrpPolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

確認

WebVPN が設定されたら、ブラウザで *ASA>* のアドレス https:// <FQDN を使用して下さい。



ログオンの後で Webサイトおよびブックマークにナビゲート するのに使用されるアドレスバーを見られますはずです。



トラブルシューティング

トラブルシューティングの手順

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。

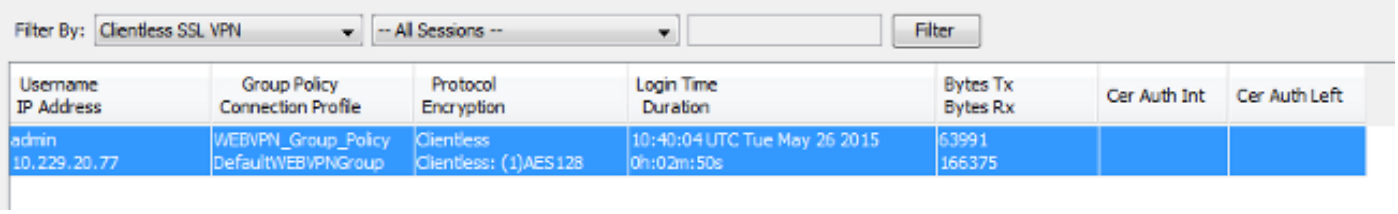
ASDM で **Monitoring > Logging > Real-time Log Viewer > View** の順に選択します。 クライアントが ASA に接続するとき、TLS セッションの確立、グループ ポリシーの選択、およびユーザの認証の成功に注意して下さい。

```
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 では、**> フィルタ下記によって** Monitoring > VPN > VPN Statistics > Sessions の順に選択して下さい: **Clientless SSL VPN。** 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

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

> **注:** debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **示して下さい webvpn** - WebVPN と関連付けられる多くの **show コマンドが**あります。 **show コマンド**の使用を詳しく見るために、Ciscoセキュリティ機器のコマンドレファレンス セクションを参照して下さい。
- **デバッグ webvpn - debug コマンド**の使用は ASA に逆効果をもたらすことができます。 **debug コマンド**の使用をより詳しく見るために、Ciscoセキュリティ機器のコマンドレファレンス セクションを参照して下さい。

一般的な問題

ユーザはログインできません

問題

メッセージ「Clientless（ブラウザ）SSL VPN アクセス許可されません」。は 不成功なログイン試行の後でブラウザに現われます。 AnyConnect 優れたライセンスは ASA でインストールされていませんか、または「AnyConnect 優れたライセンスによって示されていて ASA で」。イネーブルになられていないように使用中ではないです

解決策

これらのコマンドで AnyConnect 優れたライセンスを有効に して下さい:

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

問題

不成功なログイン試行の後でブラウザにメッセージ「失敗される」がログオン現れます。 AnyConnect ライセンス制限は超過しました。

解決策

ログのこのメッセージを探して下さい:

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

また、ライセンス制限を確認して下さい:

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

問題

不成功なログイン試行の後でブラウザに VPN サーバでメッセージ「AnyConnect」が現れますイネーブルになっていません。 Clientless VPN プロトコルはグループ ポリシーでイネーブルになっていません。

解決策

ログのこのメッセージを探して下さい:

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

Clientless VPN プロトコルが望ましいグループ ポリシーのためにイネーブルになっていることを確かめて下さい:

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

ASA に WebVPN 3 人以上のユーザを接続することが不可能

問題

WebVPN 3 人のクライアントだけ ASA に接続できます。 4 人目のクライアントの接続に失敗します。

解決策

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。 同時ログオンの望ましい 番号を設定するためにこの実例を使用して下さい。 この例では、希望値は 20 です。

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

WebVPN クライアントはブックマークを見つけることができないし、選択不可能になります

問題

これらのブックマークがユーザ向けに clientless VPN に署名するために設定されたが「Webアプリケーション」の下の Home 画面で選択不可能にされるように出て来る場合、ユーザがそれらをクリックし、特定の URL に入れるようにどのようにこれらの HTTP リンクをイネーブルにすることができますか。

解決策

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 による 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 WebVPN 上の Citrix のために発生します。

解決策

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。

ユーザに対する 2 番目の認証を不要にする方法

問題

WebVPN clientless ポータルの CIFS リンクにアクセスするとき、ブックマークをクリックした後信任状のためにプロンプト表示されます。 Lightweight Directory Access Protocol（LDAP）はリソースを認証するために使用され、ユーザは VPN セッションにログインに既に LDAP 信任状を入力してしまいました。

解決策

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
```

X.X.X.X は、CIFS サーバの IP です。また、? は、目的の共有ファイルまたはフォルダへのパスの残りの部分です。

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 基本か NTLM 認証で SSO を設定することを参照して下さい。

関連情報

- ASA: ASDM 設定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