ASA を介した AnyConnect Web セキュリティの導入

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）で終端するクライアント ベースの VPN への AnyConnect Web セキュリティ モジュールの導入について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

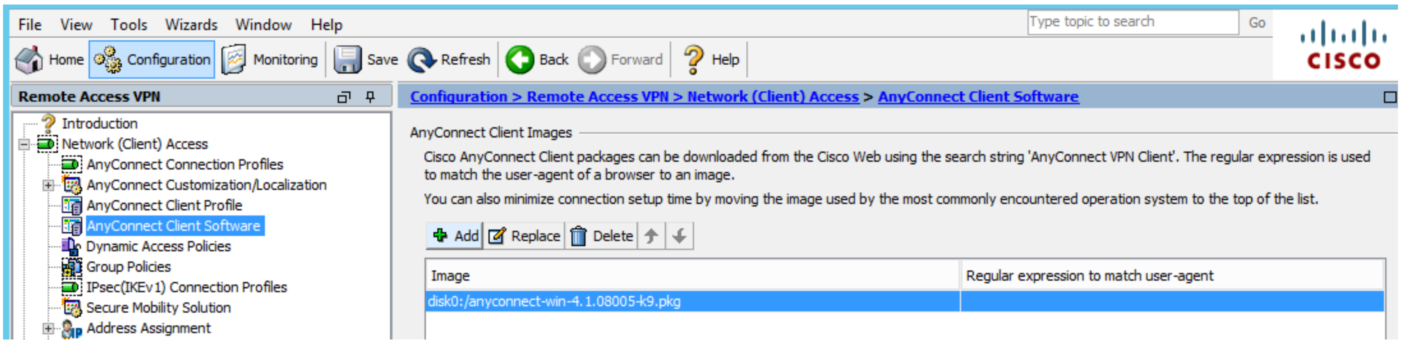
使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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、初期（デフォルト）設定の状態から起動しています。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。

背景説明

- ASA で AnyConnect（v4.1+ を推奨）イメージをアップロードします



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software

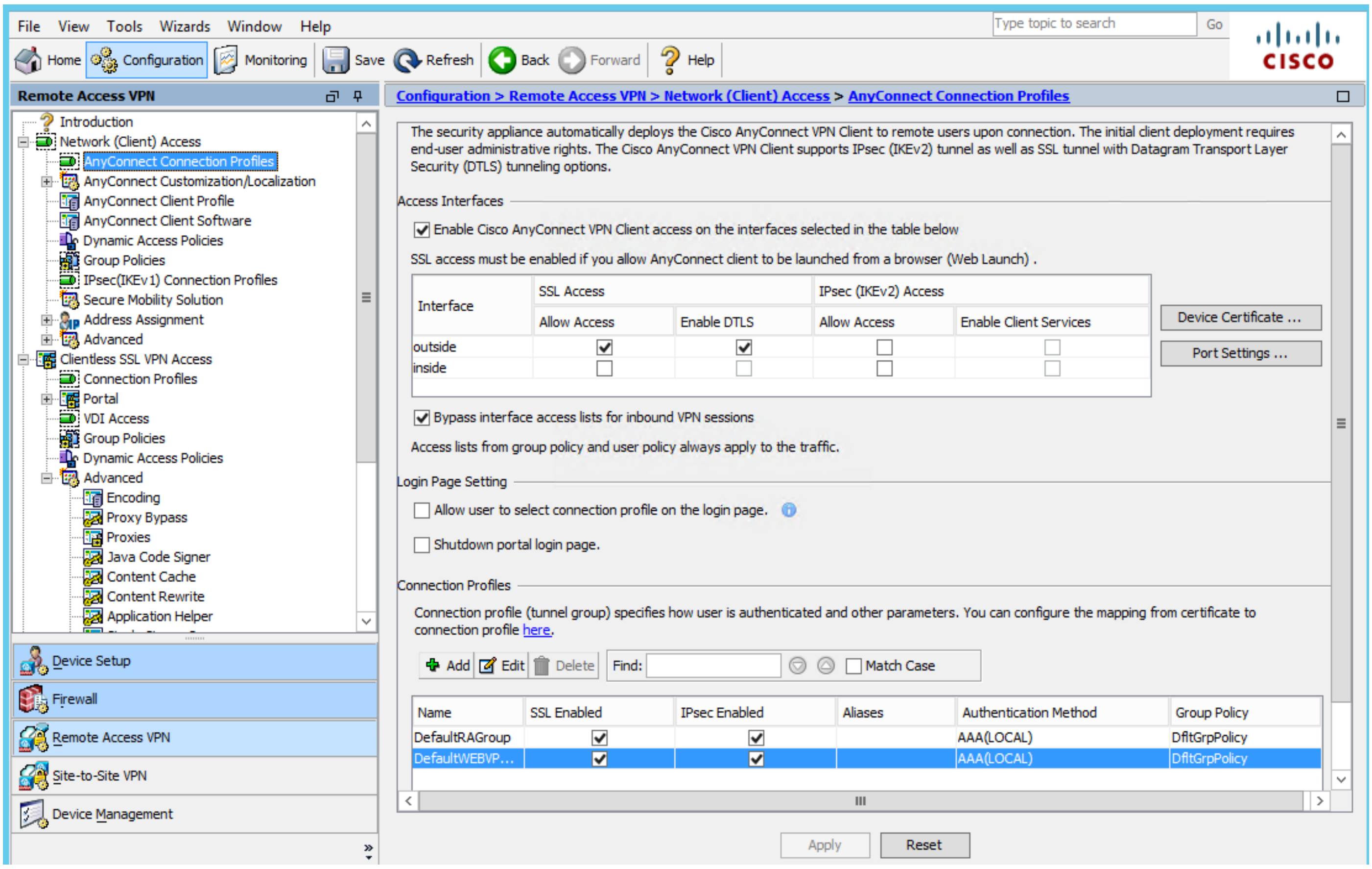
AnyConnect Client Images

Cisco AnyConnect Client packages can be downloaded from the Cisco Web using the search string 'AnyConnect VPN Client'. The regular expression is used to match the user-agent of a browser to an image.

You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Image	Regular expression to match user-agent
disk0:/anyconnect-win-4.1.08005-k9.pkg	

- 図に示すように、ASA で VPN プロファイルを有効にします



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☐	☐
inside	☐	☐	☐	☐

☑ Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

☐ Allow user to select connection profile on the login page.

☐ Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.

☐ Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	☑	☑		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVP...	☑	☑		AAA(LOCAL)	DfltGrpPolicy

設定

ASA を通じた AnyConnect Web セキュリティの導入

設定に含まれる手順は次のとおりです。

- Anyconnect Web セキュリティ クライアント プロファイルを設定する
- Anyconnect VPN グループ ポリシーを編集する
- Web セキュリティのスプリット除外を設定し、Web セキュリティ クライアント モジュールのダウンロードを選択する
- Anyconnect VPN グループ ポリシーを編集し、Web セキュリティ クライアント プロファイルを選択する

手順 1：Anyconnect Web セキュリティ クライアント プロファイルを設定する

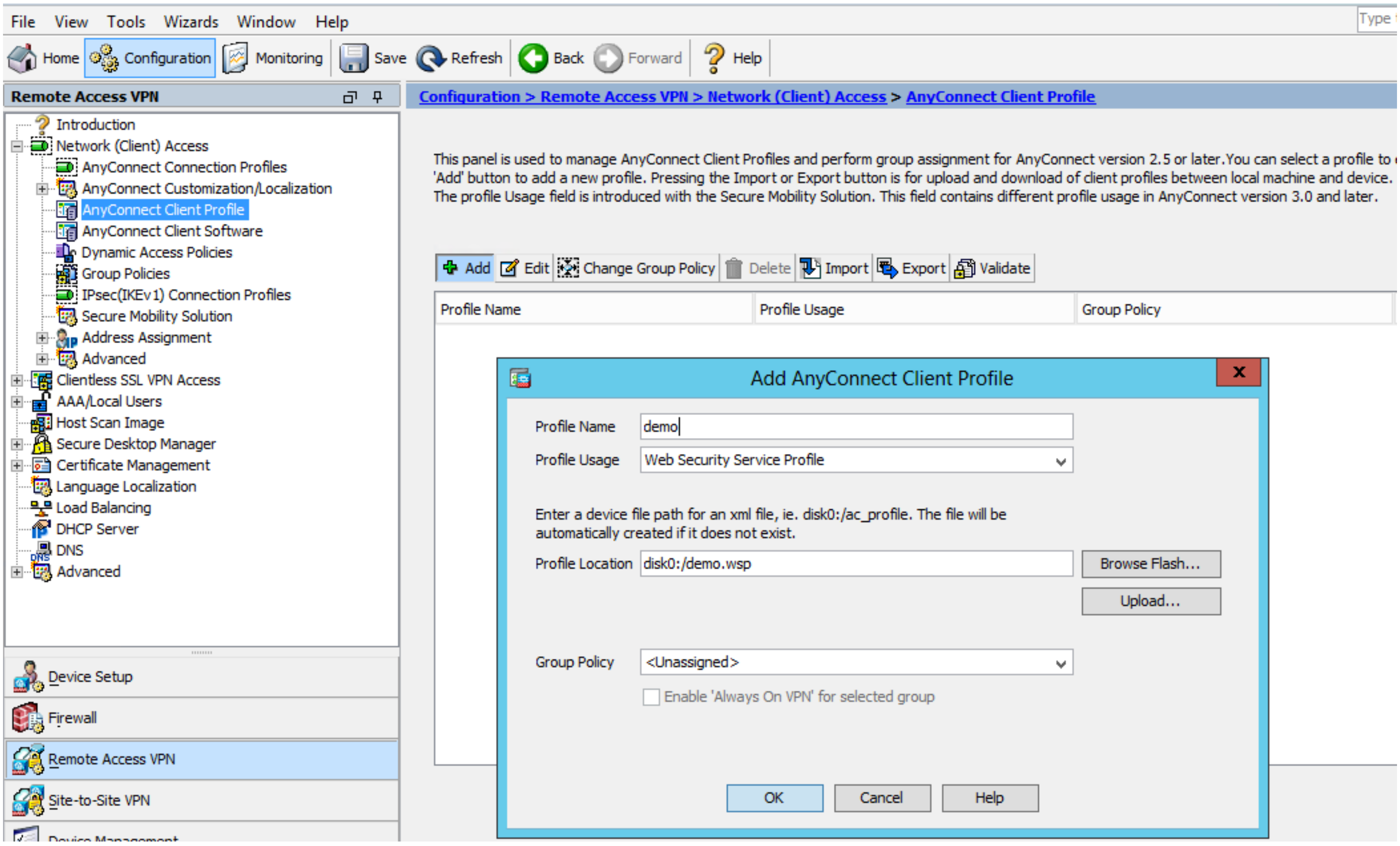
[Configuration] > [Remove Access VPN] > [Network (Client) Access] > [Anyconnect Client Profile]

を選択します。

[Add] をクリックし、[AnyConnect Web Security Client Profile] を選択します。

> 注：クライアント側の Profile Name はハードコードされているため、設定した名前に関係なく、ASA は常に **Websecurity_serviceprofile.wso をクライアントにプッシュします。**

> 注：これは、認証ライセンス キーのないデフォルト プロファイルです。


File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Add Edit Change Group Policy Delete Import Export Validate
Profile Name
Profile Usage
Group Policy
Add AnyConnect Client Profile
Browse Flash...
Upload...
OK Cancel Help

This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later.You can select a profile to 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device. The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.

Profile Name: demo

Profile Usage: Web Security Service Profile

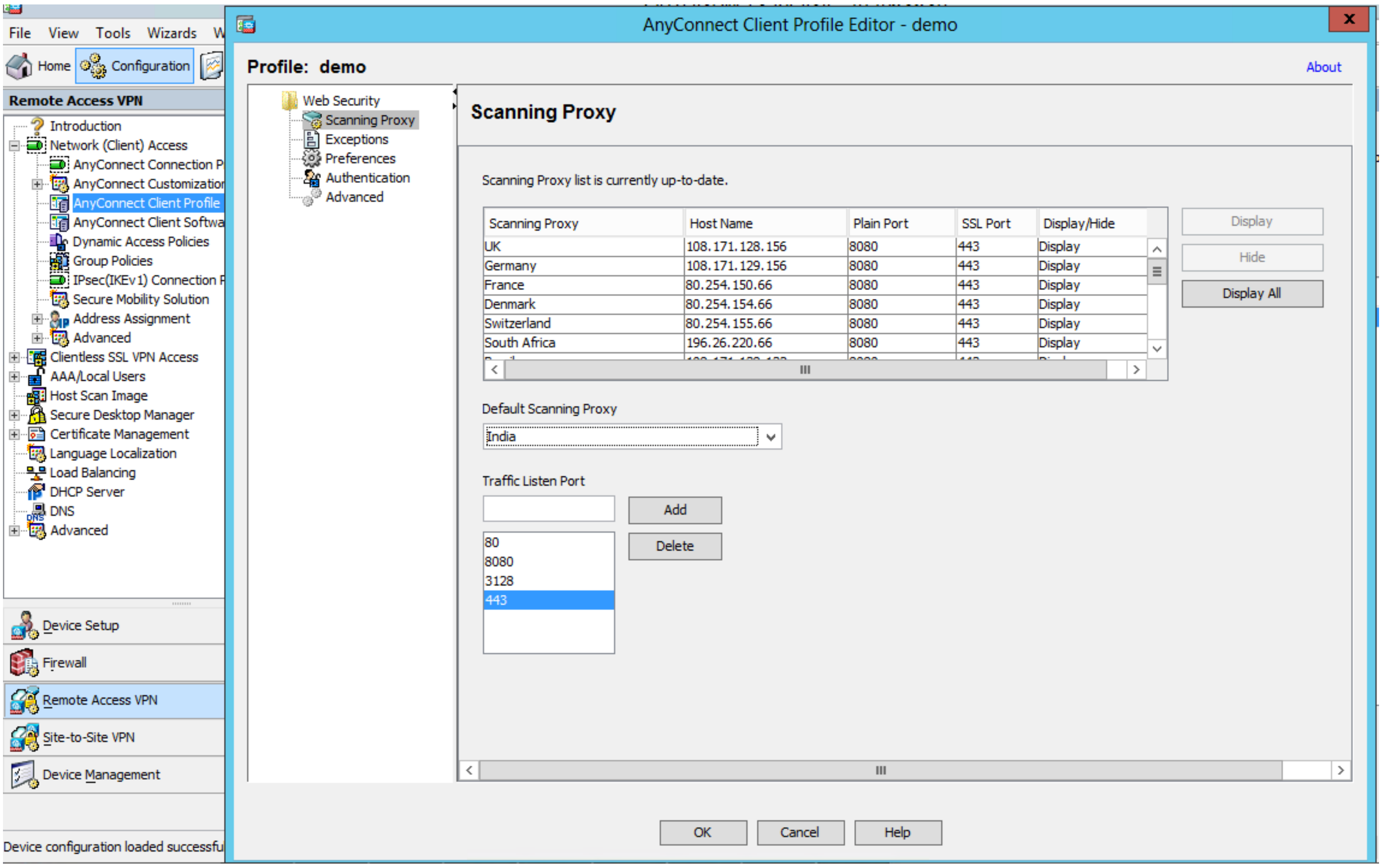
Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.

Profile Location: disk0:/demo.wsp

Group Policy: <Unassigned>

□ Enable 'Always On VPN' for selected group

手順 2：新しく作成したプロファイルを編集し、認証ライセンス キーを追加し、設定をカスタマイズする。



AnyConnect Client Profile Editor - demo

Profile: demo

Scanning Proxy

Scanning Proxy list is currently up-to-date.

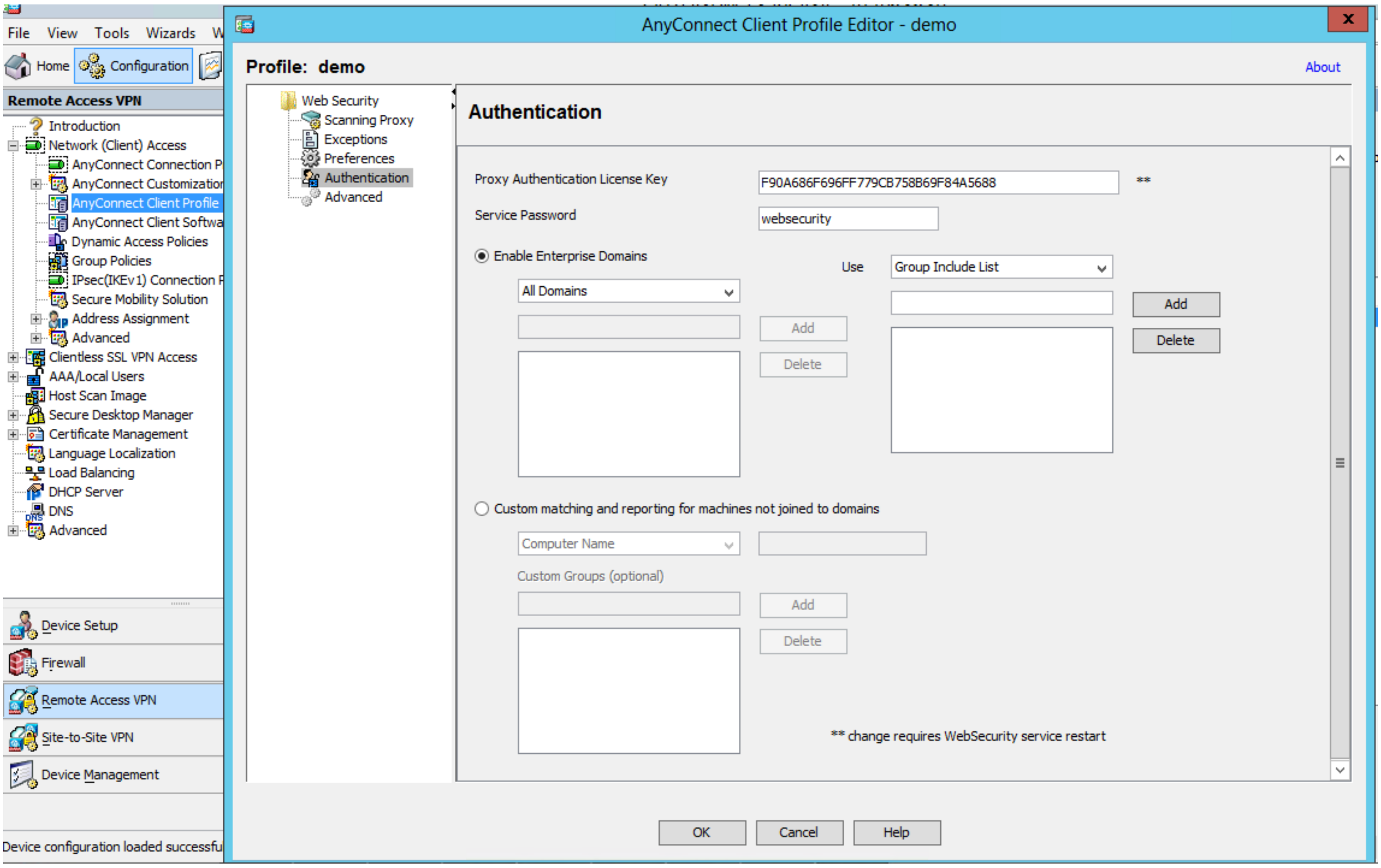
Scanning Proxy	Host Name	Plain Port	SSL Port	Display/Hide
UK	108.171.128.156	8080	443	Display
Germany	108.171.129.156	8080	443	Display
France	80.254.150.66	8080	443	Display
Denmark	80.254.154.66	8080	443	Display
Switzerland	80.254.155.66	8080	443	Display
South Africa	196.26.220.66	8080	443	Display

Default Scanning Proxy

India

Traffic Listen Port

80
8080
3128
443



AnyConnect Client Profile Editor - demo

Profile: demo

Authentication

Proxy Authentication License Key F90A686F696FF779CB758B69F84A5688 **

Service Password websecurity

● Enable Enterprise Domains

All Domains

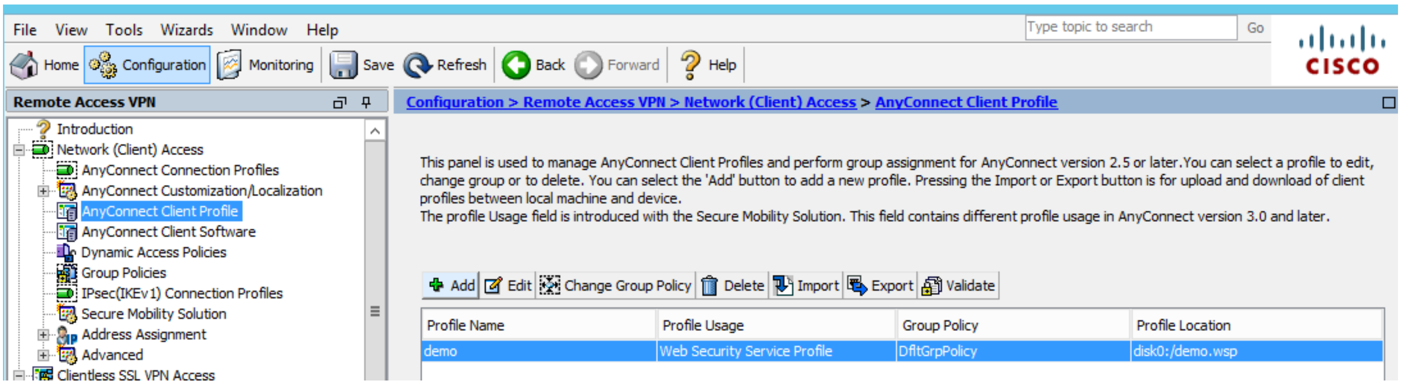
Use Group Include List

○ Custom matching and reporting for machines not joined to domains

Computer Name

Custom Groups (optional)

** change requires WebSecurity service restart


File View Tools Wizards Window Help
Type topic to search Go
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Add Edit Change Group Policy Delete Import Export Validate

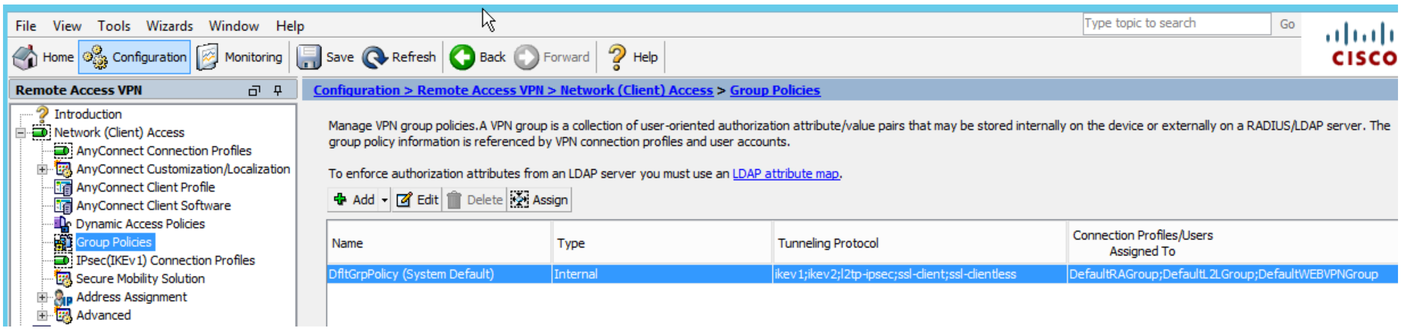
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile

This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later.You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.

Profile Name	Profile Usage	Group Policy	Profile Location
demo	Web Security Service Profile	DfltGrpPolicy	disk0:/demo.wsp

手順 3：Web セキュリティのスプリット除外を設定し、Web セキュリティ クライアント モジュールのダウンロードを選択する

図に示すように、Anyconnect VPN グループ ポリシーを編集します。


File View Tools Wizards Window Help
Type topic to search Go
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Add Edit Delete Assign

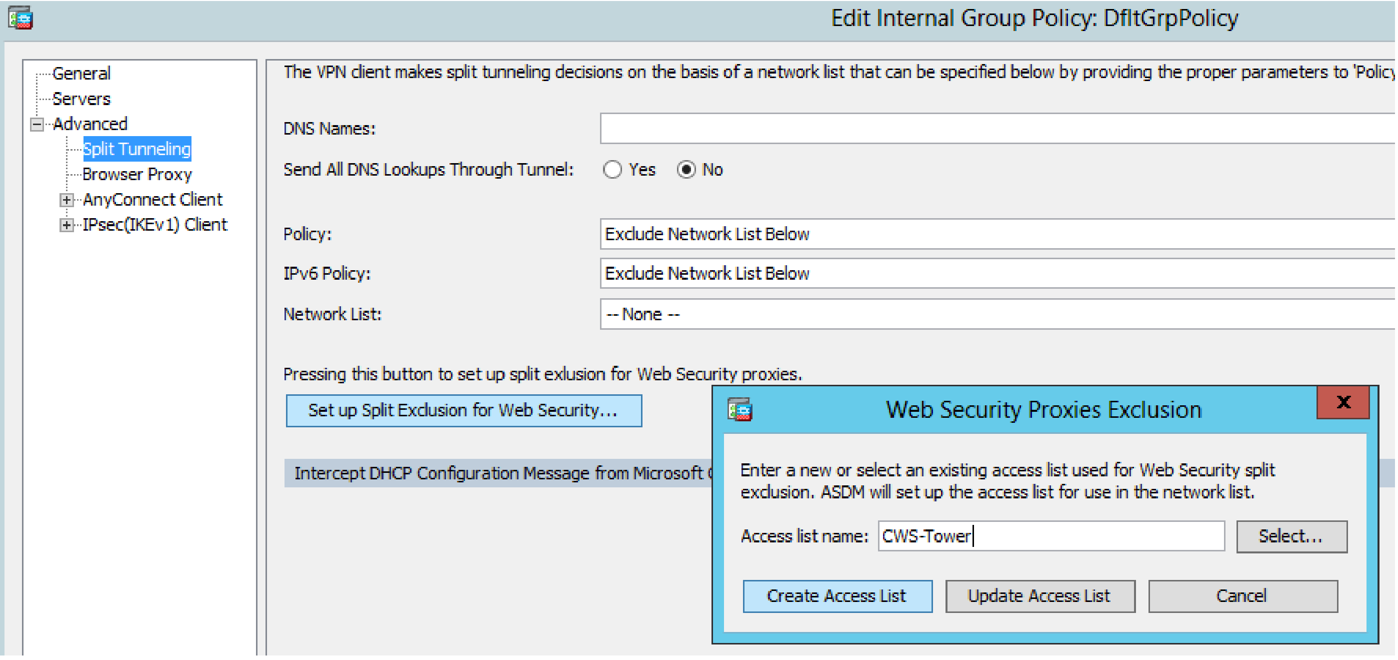
Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec;ssl-client;ssl-clientless	DefaultRAGroup;DefaultL2LGroup;DefaultWEBVPNGroup

図に示すように、Web セキュリティのスプリット除外を設定します。



Edit Internal Group Policy: DfltGrpPolicy

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy

DNS Names:

Send All DNS Lookups Through Tunnel: ○ Yes ● No

Policy: Exclude Network List Below

IPv6 Policy: Exclude Network List Below

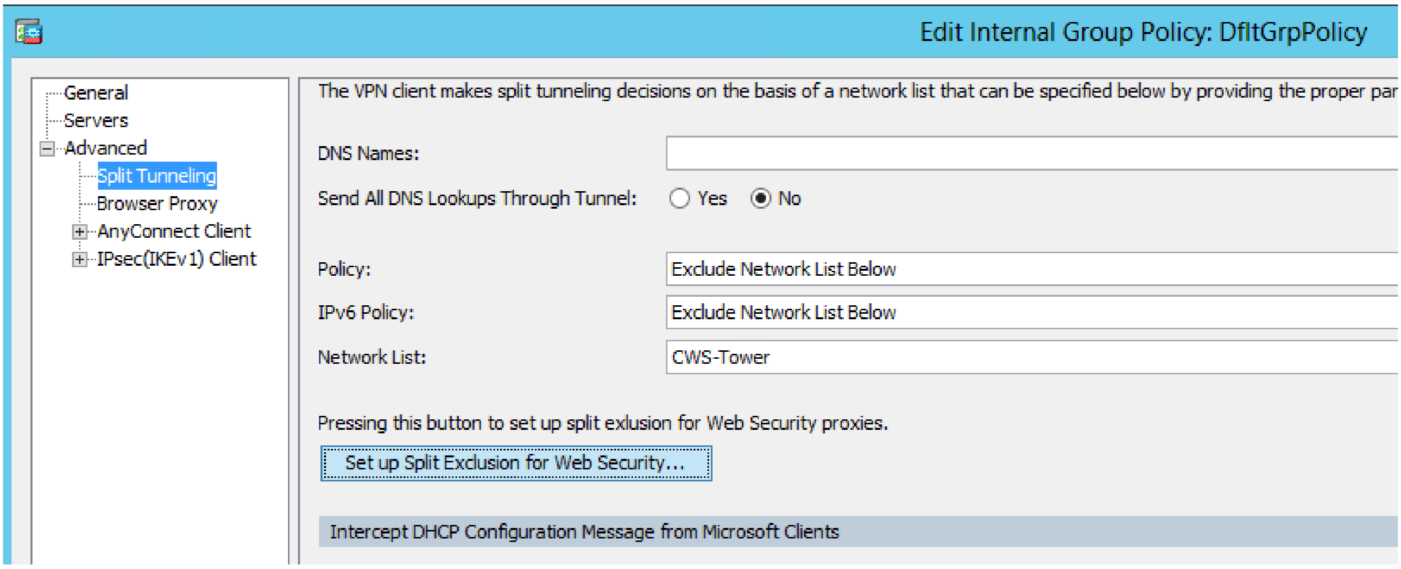
Network List: -- None --

Pressing this button to set up split exlusion for Web Security proxies.

Web Security Proxies Exclusion

Enter a new or select an existing access list used for Web Security split exclusion. ASDM will set up the access list for use in the network list.

Access list name: CWS-Tower


Edit Internal Group Policy: DfltGrpPolicy
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec(IKEv1) Client
Set up Split Exclusion for Web Security...
Intercept DHCP Configuration Message from Microsoft Clients

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper par

DNS Names:

Send All DNS Lookups Through Tunnel: ○ Yes ● No

Policy: Exclude Network List Below

IPv6 Policy: Exclude Network List Below

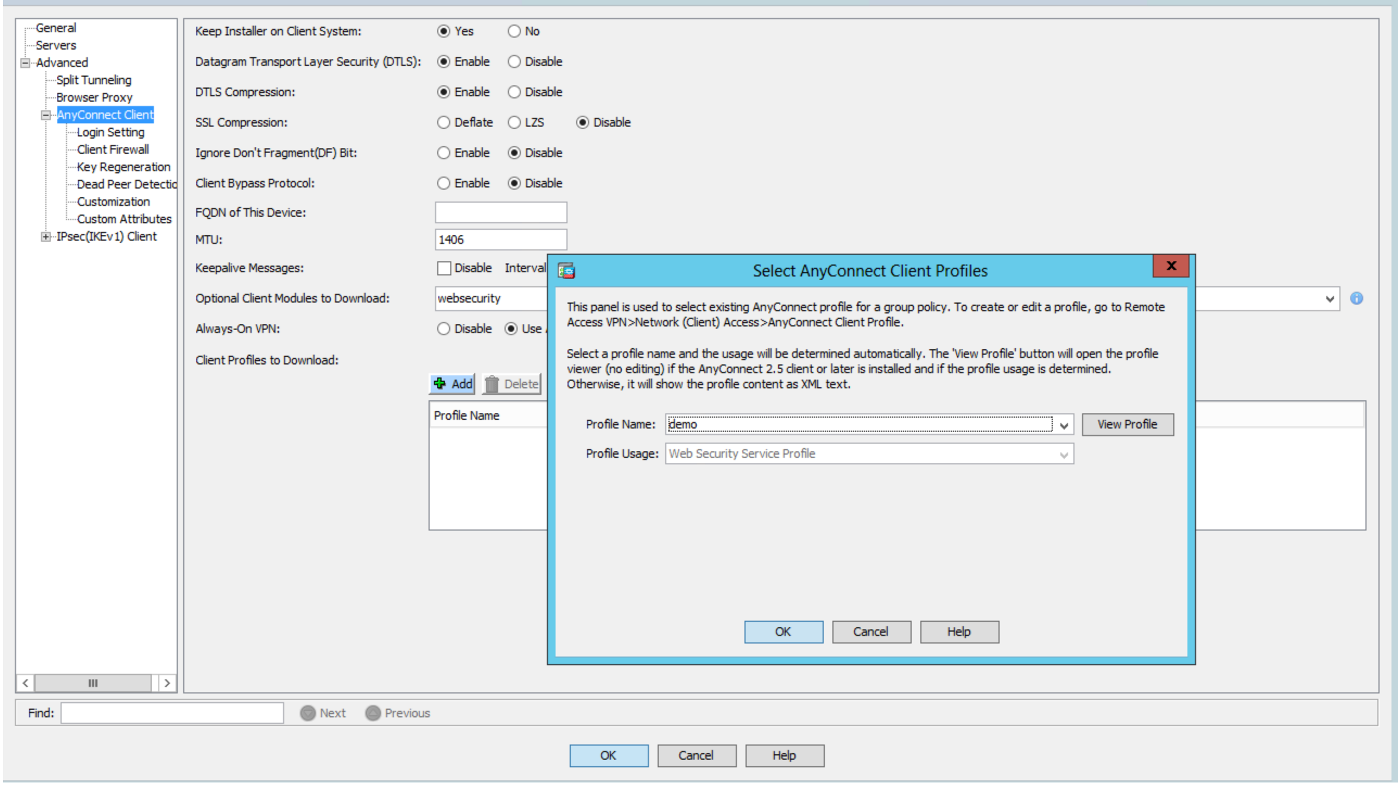
Network List: CWS-Tower

Pressing this button to set up split exlusion for Web Security proxies.

図に示すように、Web セキュリティ クライアント モジュールのダウンロードを選択します。

手順 4：Web セキュリティ クライアント プロファイルをダウンロードする

[Anyconnect VPN group policy] > [Client Profiles to Download] > [Add] を編集し、（手順 1 で）作成したプロファイルを選択します



Keep Installer on Client System: ● Yes ○ No

Datagram Transport Layer Security (DTLS): ● Enable ○ Disable

DTLS Compression: ● Enable ○ Disable

SSL Compression: ○ Deflate ○ LZS ● Disable

Ignore Don't Fragment(DF) Bit: ○ Enable ● Disable

Client Bypass Protocol: ○ Enable ● Disable

FQDN of This Device:

MTU: 1406

Keepalive Messages: □ Disable Interval

Optional Client Modules to Download: websecurity

Always-On VPN: ○ Disable ● Use

Client Profiles to Download:

Profile Name

Select AnyConnect Client Profiles

This panel is used to select existing AnyConnect profile for a group policy. To create or edit a profile, go to Remote Access VPN>Network (Client) Access>AnyConnect Client Profile.

Select a profile name and the usage will be determined automatically. The 'View Profile' button will open the profile viewer (no editing) if the AnyConnect 2.5 client or later is installed and if the profile usage is determined. Otherwise, it will show the profile content as XML text.

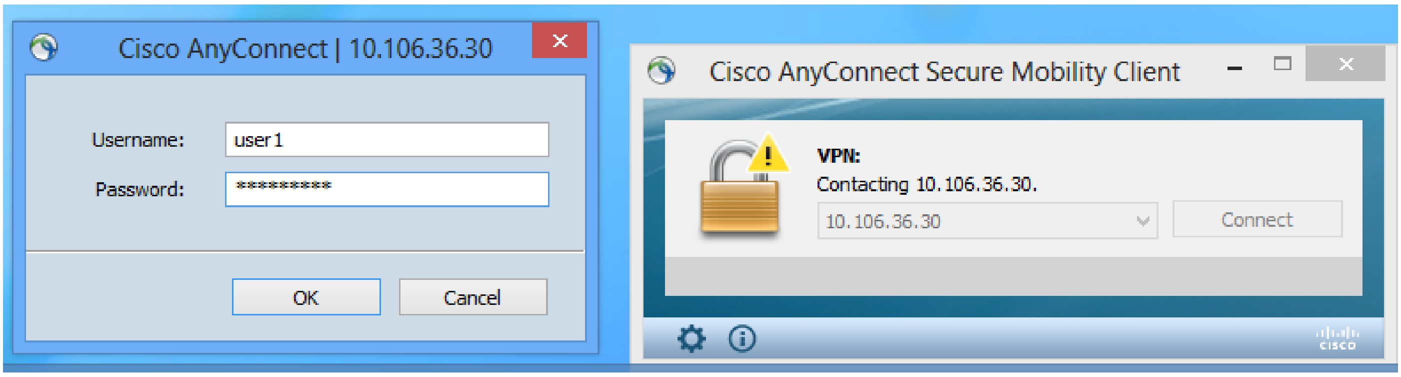
Profile Name: demo

Profile Usage: Web Security Service Profile

[OK] をクリックし、変更を適用します。

確認

Anyconnect VPN に接続すると、図に示すように、ASA は VPN 経由で、Anyconnect Web セキュリティ モジュールをプッシュします。

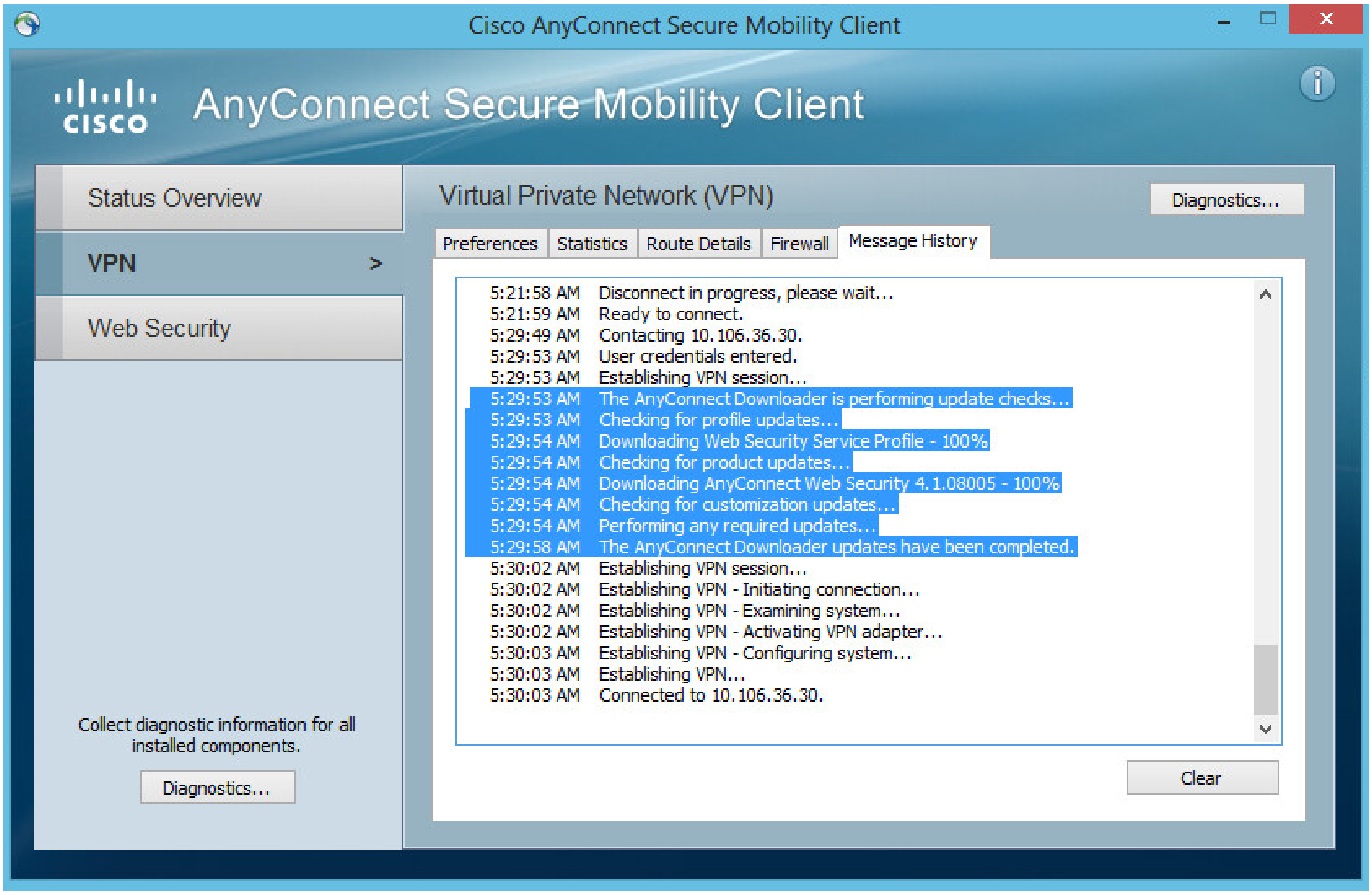


Cisco AnyConnect | 10.106.36.30

Username: user1

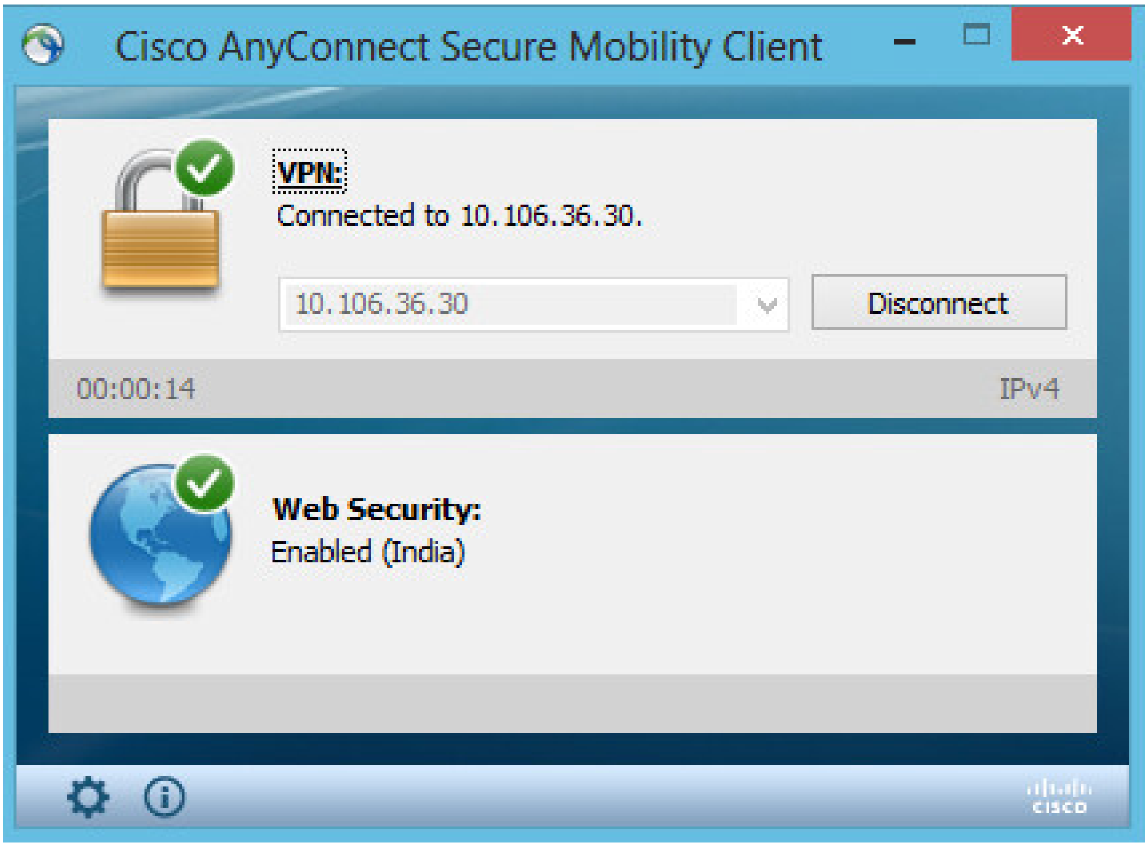
Password: **********

VPN:
Contacting 10.106.36.30.



```
5:21:58 AM   Disconnect in progress, please wait...
5:21:59 AM   Ready to connect.
5:29:49 AM   Contacting 10.106.36.30.
5:29:53 AM   User credentials entered.
5:29:53 AM   Establishing VPN session...
5:29:53 AM   The AnyConnect Downloader is performing update checks...
5:29:53 AM   Checking for profile updates...
5:29:54 AM   Downloading Web Security Service Profile - 100%
5:29:54 AM   Checking for product updates...
5:29:54 AM   Downloading AnyConnect Web Security 4.1.08005 - 100%
5:29:54 AM   Checking for customization updates...
5:29:54 AM   Performing any required updates...
5:29:58 AM   The AnyConnect Downloader updates have been completed.
5:30:02 AM   Establishing VPN session...
5:30:02 AM   Establishing VPN - Initiating connection...
5:30:02 AM   Establishing VPN - Examining system...
5:30:02 AM   Establishing VPN - Activating VPN adapter...
5:30:03 AM   Establishing VPN - Configuring system...
5:30:03 AM   Establishing VPN...
5:30:03 AM   Connected to 10.106.36.30.
```

Collect diagnostic information for all installed components.



すでにログインしている場合、この機能が有効になるよう、ログオフして、ログインすることを推奨します。

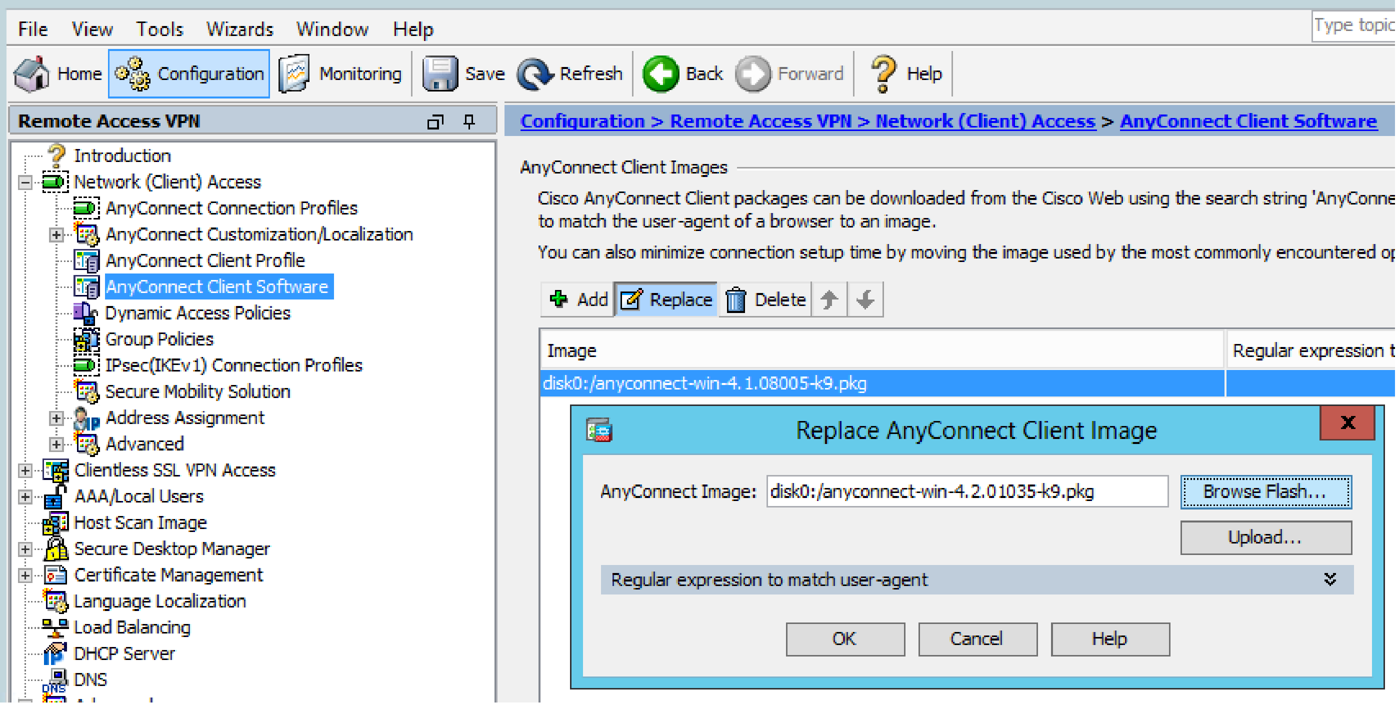
Anyconnect バージョンのアップグレード/ダウングレード

バージョンがアップグレードされた場合、導入機能は変更ありません。ただしダウングレードすることはできません。したがって、4.1.x の現在の例では、バージョン 4.2 にアップグレードできます

含まれる手順は次のとおりです。

手順 1：最新の Anyconnect パッケージ 4.2 をフラッシュにアップロードし、4.1 を最新のファイルで置き換える。

[Anyconnect Client Software] > [Replace] で最新のイメージ ファイルを選択します。



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software

AnyConnect Client Images

Cisco AnyConnect Client packages can be downloaded from the Cisco Web using the search string 'AnyConne
to match the user-agent of a browser to an image.

You can also minimize connection setup time by moving the image used by the most commonly encountered op

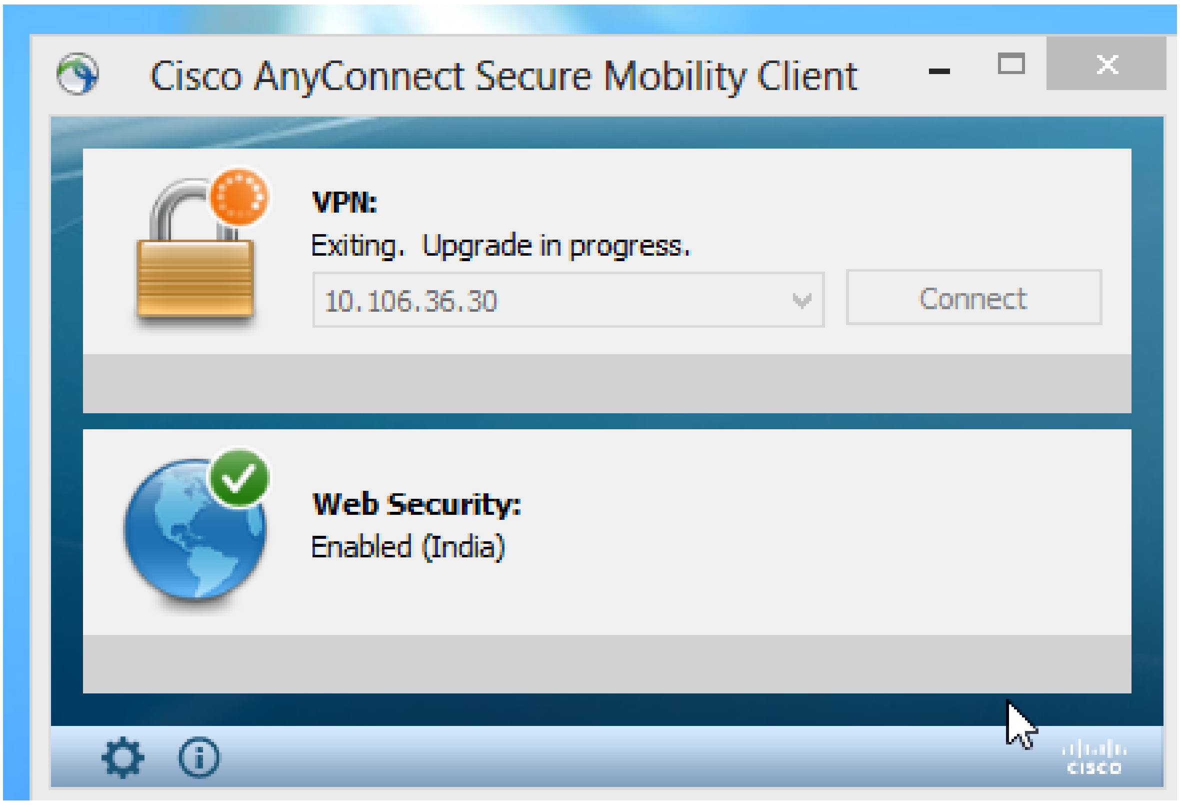
Image	Regular expression t
disk0:/anyconnect-win-4.1.08005-k9.pkg	

Replace AnyConnect Client Image

AnyConnect Image: disk0:/anyconnect-win-4.2.01035-k9.pkg

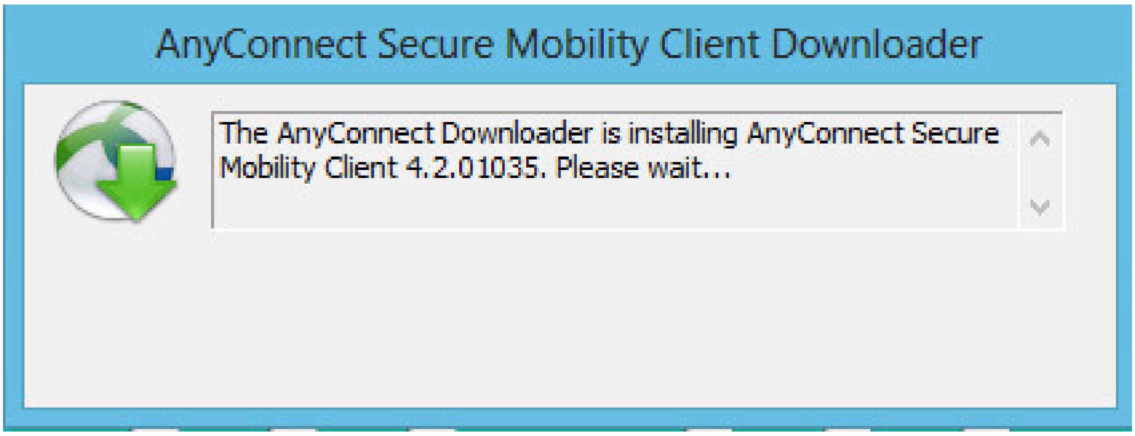
Regular expression to match user-agent

ステップ２： Anyconnect VPN に再接続した際、Web セキュリティ プロファイルは変更されず、ASA が VPN 経由で最新の Anyconnect モジュールをプッシュする。



VPN:
Exiting. Upgrade in progress.
10.106.36.30

Web Security:
Enabled (India)



The AnyConnect Downloader is installing AnyConnect Secure Mobility Client 4.2.01035. Please wait...

注：ダウングレードはサポートされません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

DART を使用したトラブルシューティング情報の収集：

DART は AnyConnect Diagnostics and Reporting Tool の略で、AnyConnect のインストールと接続に関する問題のトラブルシューティングに役立つデータの収集に使用できます。DART は、Windows 7、Windows Vista、Windows XP、Mac バージョン 10.5 と 10.6、および Linux Redhat をサポートします。DART ウィザードは、AnyConnect を実行するコンピュータ上で実行されます。これによってログ、ステータス、および診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用でき、管理者権限は不要です。

DART は、AnyConnect ソフトウェアのコンポーネントに依存せずに機能しますが、AnyConnect から起動可能で、AnyConnect ログ ファイル（存在する場合）の収集を行います。現在のところ、DART はスタンドアロン インストールを実行できます。または、管理者は AnyConnect ダイナミック ダウンロード インフラストラクチャの一部として、このアプリケーションをクライアント PC にプッシュできます。インストールしたら、[Start] ボタンを通して、Cisco フォルダからウィザードを起動できます。