Configure Clientless SSL VPN (WebVPN) on the ASA

Document ID: 119417

Contributed by Jan Krupa, Cisco TAC Engineer.
Jan 05, 2016

Contents

Introduction

This document provides a straightforward configuration for the Cisco Adaptive Security Appliance (ASA) 5500 Series in order to allow Clientless Secure Sockets Layer (SSL) VPN access to internal network resources. Clientless SSL Virtual Private Network (WebVPN) allows for limited, but valuable, secure access to the corporate network from any location. Users can achieve secure browser-based access to corporate resources at any time. No additional client is needed in order to gain access to internal resources. The access is provided using a Hypertext Transfer Protocol over SSL connection.

Clientless SSL VPN provides secure and easy access to a broad range of web resources and both web-enabled and legacy applications from almost any computer that can reach Hypertext Transfer Protocol Internet (HTTP) sites. This includes:

- Internal websites
- Microsoft SharePoint 2003, 2007, and 2010
- Microsoft Outlook Web Access 2003, 2007, and 2013
- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 and 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp Version 5 to 6.5
- Citrix XenDesktop Version 5 to 5.6, and 7.5

- VMware View 4

A list of supported software can be found in Supported VPN Platforms, Cisco ASA 5500 Series.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- SSL-enabled browser
- ASA with Version 7.1 or higher
- X.509 certificate issued to the ASA domain name
- TCP port 443, which must not be blocked along the path from the client to the ASA

The full list of requirements can be found in Supported VPN Platforms, Cisco ASA 5500 Series.

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All the devices used in this document began with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

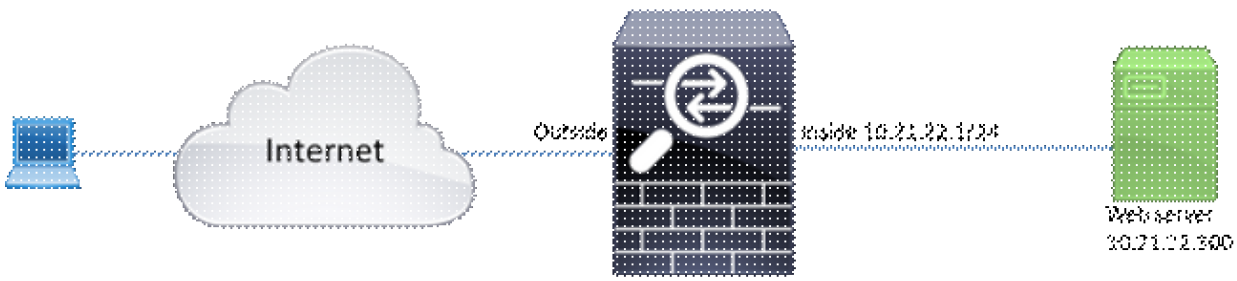
Configure

This article describes the configuration process for both the ASDM and the CLI. You can choose to follow either of the tools in order to configure the WebVPN, but some of the configuration steps can only be achieved with the ASDM.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information about the commands used in this section.

Network Diagram

This document uses this network setup:



Background Information

WebVPN uses the SSL protocol in order to secure the data transferred between the client and the server. When the browser initiates a connection to the ASA, the ASA presents its certificate to authenticate itself to the browser. In order to ensure that the connection between the client and the ASA is secure, you need to provide the ASA with the certificate that is signed by the Certificate Authority that the client already trusts. Otherwise the client will not have the means to verify authenticity of the ASA which results in the possibility of the man-in-the-middle attack and poor user experience, because the browser produces a warning that the connection is not trusted.

Note: By default, the ASA generates a self-signed X.509 certificate upon startup. This certificate is used in order to serve client connections by default. It is not recommended to use this certificate because its authenticity cannot be verified by the browser. Furthermore, this certificate is regenerated upon each reboot so it changes after each reboot.

Certificate installation is out of the scope of this document.

Configuration

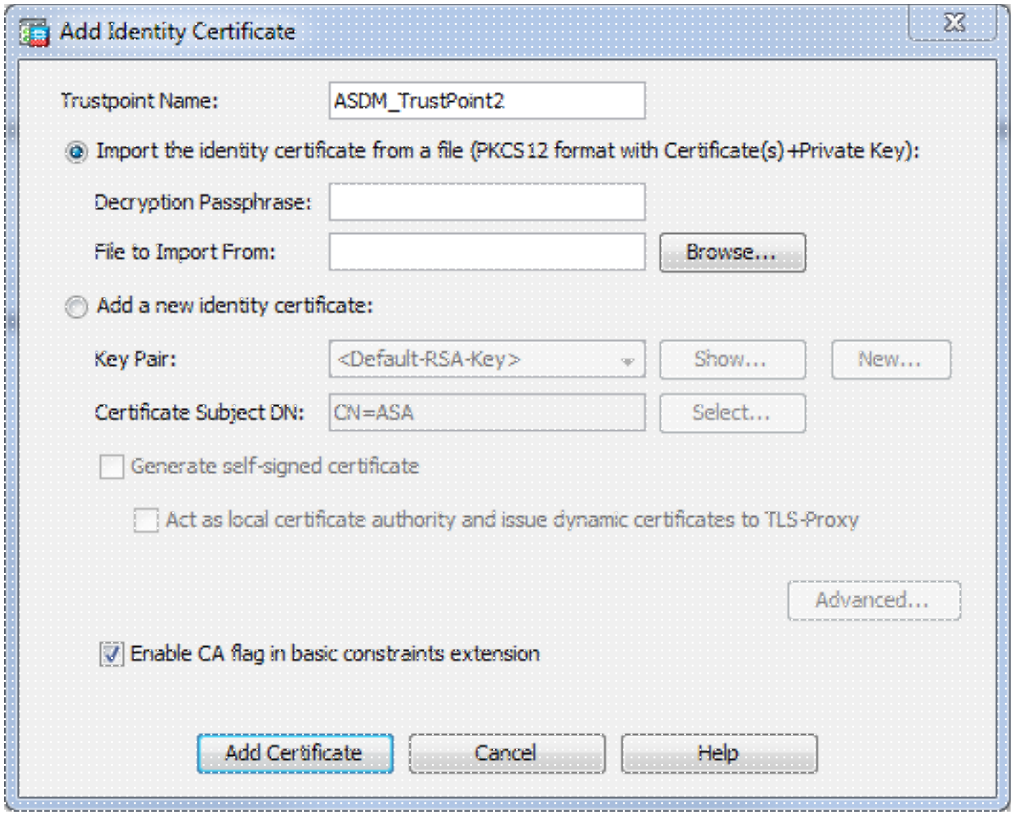
Configure the WebVPN on the ASA with five major steps:

- Configure the certificate that will be used by the ASA.
- Enable the WebVPN on an ASA interface.
- Create a list of servers and/or Uniform Resource Locator (URL) for WebVPN access.
- Create a group policy for WebVPN users.
- Apply the new group policy to a Tunnel Group.

Note: In ASA releases later than Release 9.4, the algorithm used to choose SSL ciphers has been changed (see Release Notes for the Cisco ASA Series, 9.4(x)).If only elliptic curve-capable clients will be used, then it is safe to use elliptic curve private key for the certificate. Otherwise the custom cipher suite should be used in order to avoid having the ASA present a self-signed temporary certificate. You can configure the ASA to use only RSA-based ciphers with the **ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-S** command.

1. **Option 1** - Import the certificate with the pkcs12 file.

   Choose **Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Add**. You can install it with the pkcs12 file or paste the contents in the Privacy Enhanced Mail (PEM) format.



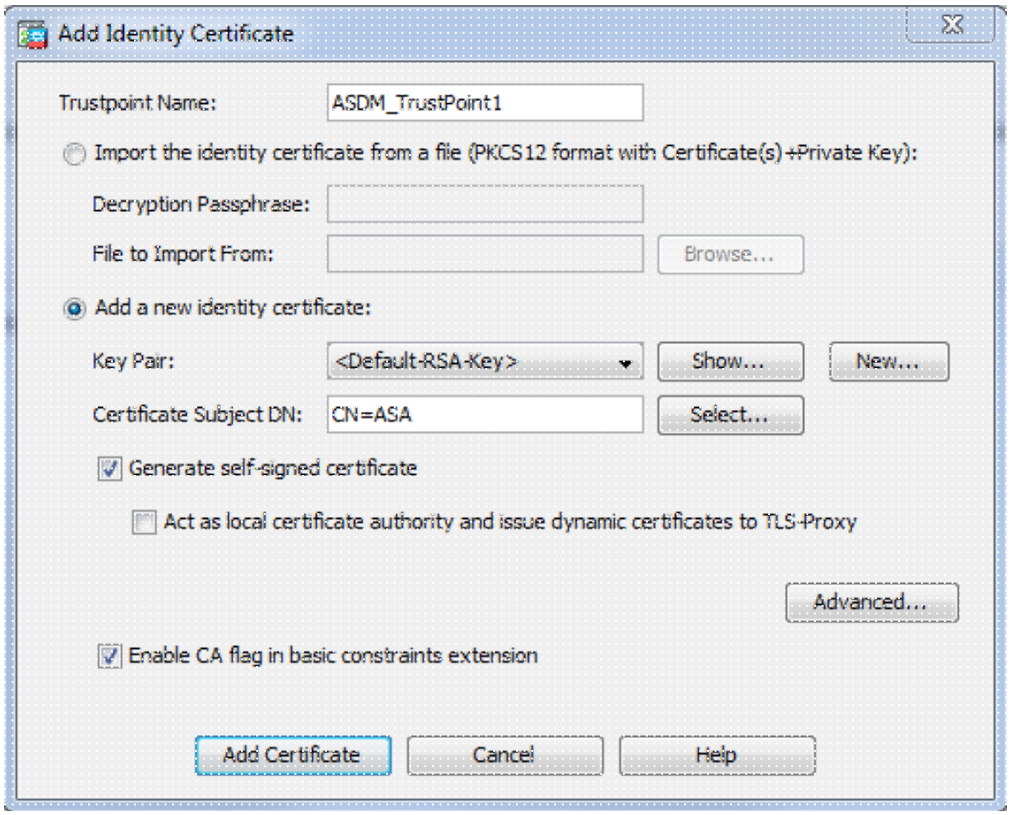
CLI:

```
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
```

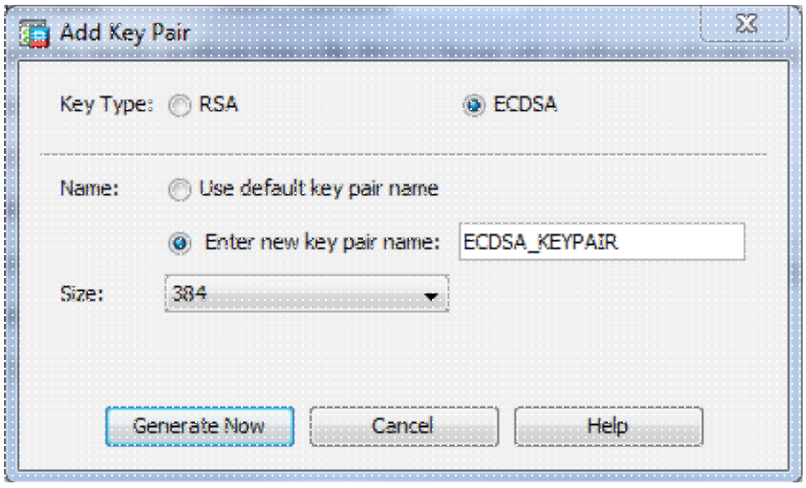
Option 2 - Create a self-signed certificate.

Choose **Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Add**.

Click the **Add a new identity certificate** radio button. Check the **Generate self-signed certificate check box**. Choose a Common Name (CN) that matches domain name of the ASA.



Click **New** in order to create the keypair for the certificate. Choose the Key Type, Name, and Size.



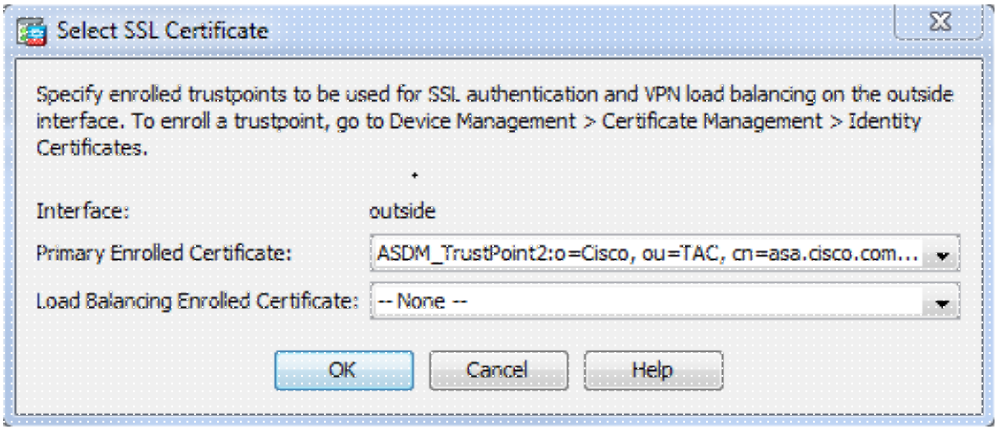
CLI:

```
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. Choose the certificate that will be used to serve WebVPN connections.

   Choose **Configuration > Remote Access VPN > Advanced > SSL Settings**. From the Certificates menu, choose the trustpoint associated with the desired certificate for the outside interface. Click **apply**.



   Equivalent CLI configuration:

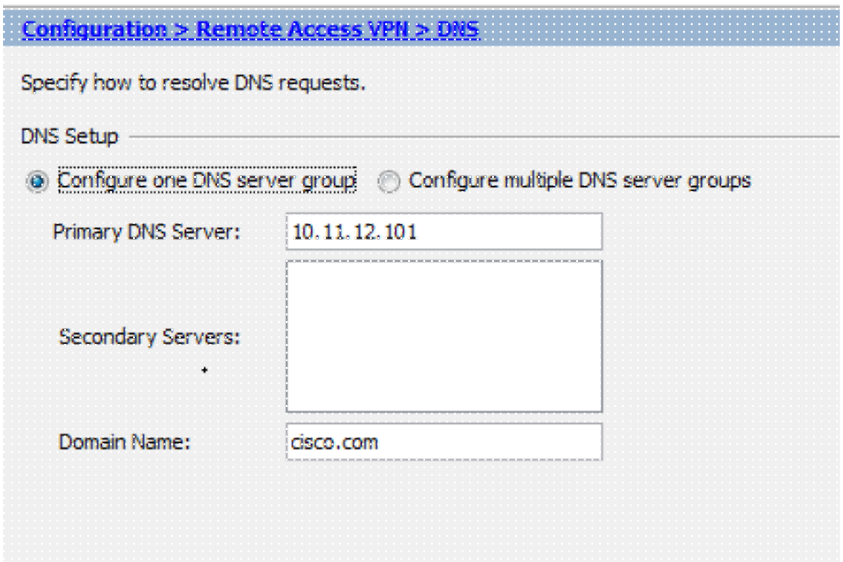
```
ASA(config)# ssl trust-point <trustpoint-name> outside
```

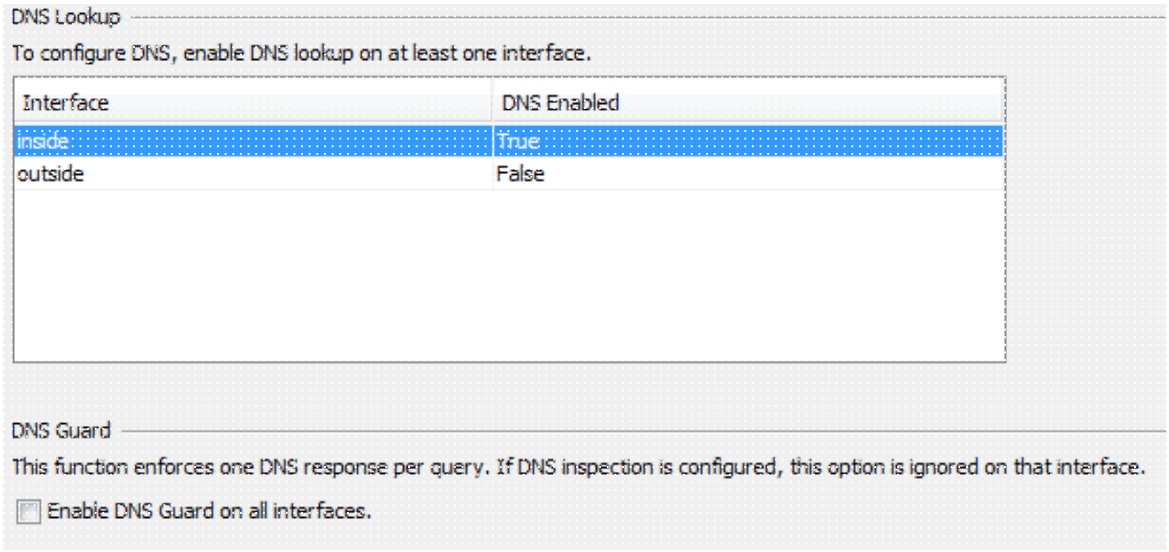
3. (Optional) Enable Domain Name Server (DNS) lookups.

   WebVPN server acts as a proxy for client connections. It means that the ASA creates connections to the resources on behalf of the client. If the clients require connections to the resources that use domain names, then the ASA needs to perform the DNS lookup.

   Choose **Configuration > Remote Access VPN > DNS**.

   Configure at least one DNS server and enable DNS lookups on the interface that faces the DNS server.





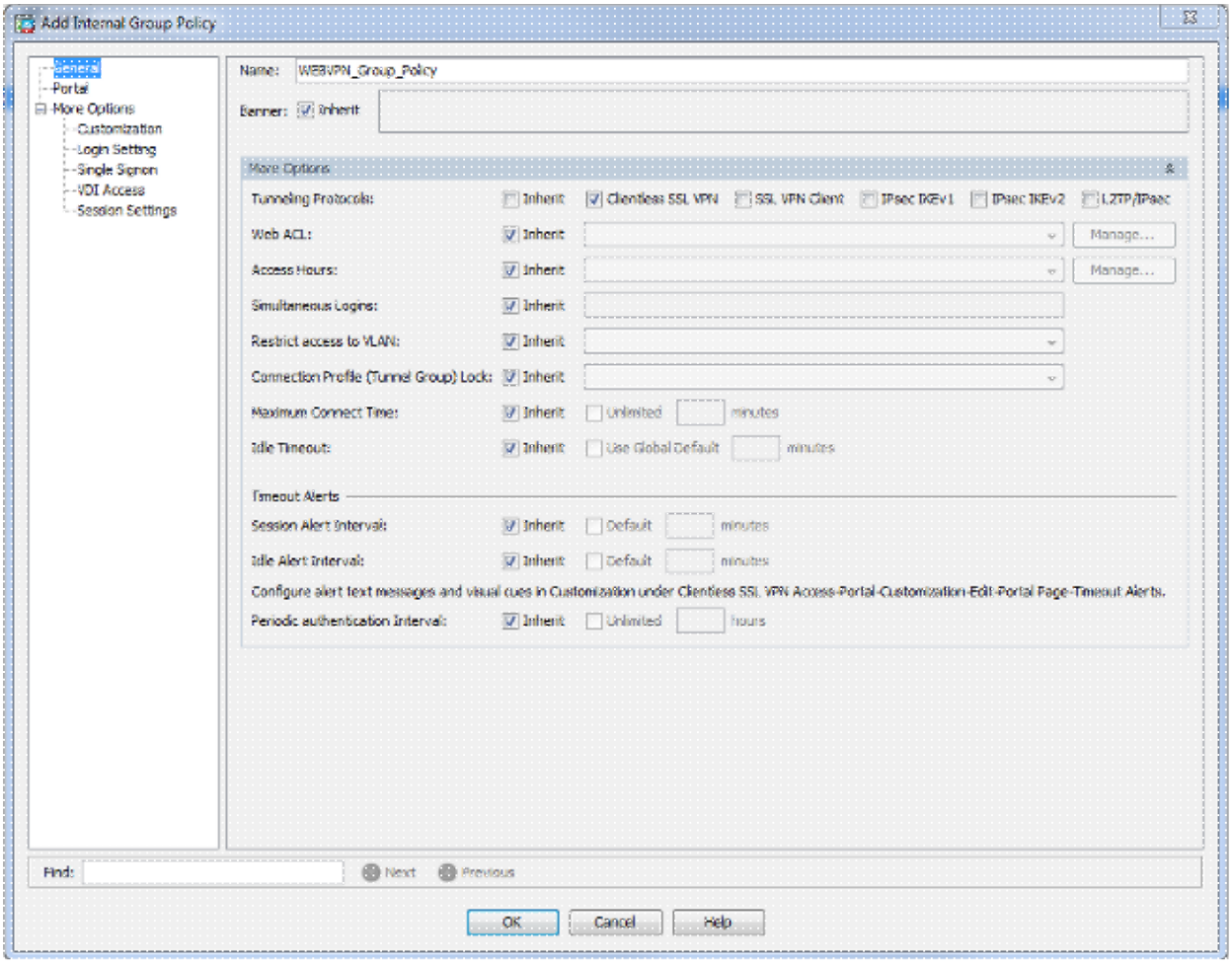
CLI:

```
ASA(config)# dns domain-lookup inside
ASA(config)# dns server-group DefaultDNS
ASA(config-dns-server-group)# name-server 10.11.12.101
```

4. (Optional) Create Group Policy for WEBVPN connections.

   Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add Internal Group Policy**.

   Under General Options change the Tunelling Protocols value to "Clientless 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. Configure the Connection Profile.

   In ASDM, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

   For an overview of the Connection profiles and the Group policies, consult Cisco ASA Series VPN CLI Configuration Guide, 9.4 - Connection Profiles, Group Policies, and Users.

   By default, the WebVPN connections use DefaultWEBVPNGroup profile. You can create additional profiles.

   Note: There are various ways to assign users to other profiles.

   - Users can manually select the connection profile from the drop-down list or with a specific URL. See ASA 8.x: Allow Users to Select a Group at WebVPN Login via Group-Alias and Group-URL Method.

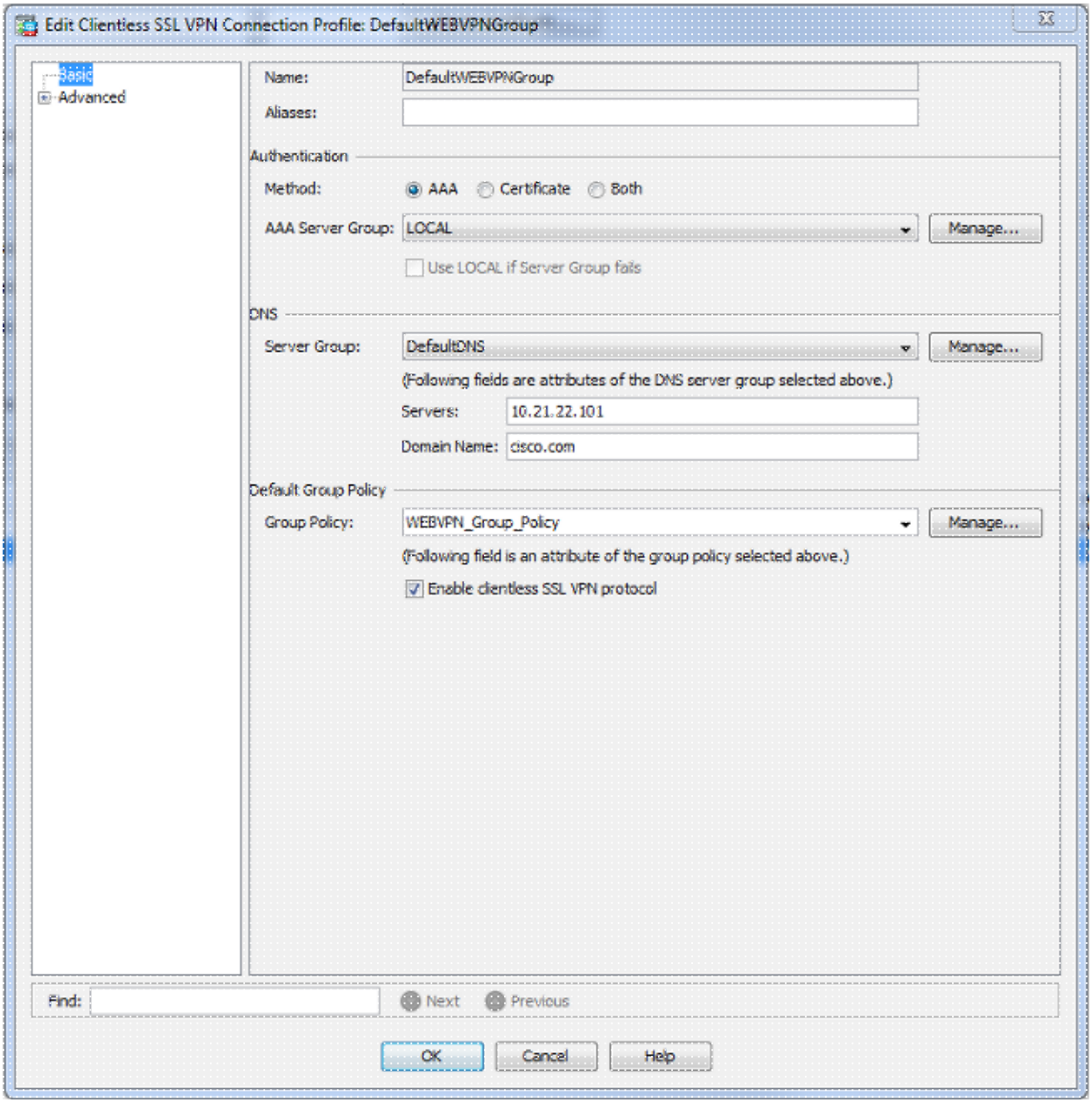
   - When you use an LDAP server, you can assign the user profile based on the attributes received from the LDAP server, see ASA Use of LDAP Attribute Maps Configuration Example.

   - When you use certificate-based authentication of the clients, you can map the user to the profiles

based on the fields contained in the certificate, see Cisco ASA Series VPN CLI Configuration Guide, 9.4 - Configure Certificate Group Matching for IKEv1.

- In order to assign the users manually to the Group policy, see Cisco ASA Series VPN CLI Configuration Guide, 9.4 - Configuring Attributes for Individual Users

Edit the DefaultWEBVPNGroup profile and choose the WEBVPN_Group_Policy under Default Group Policy.

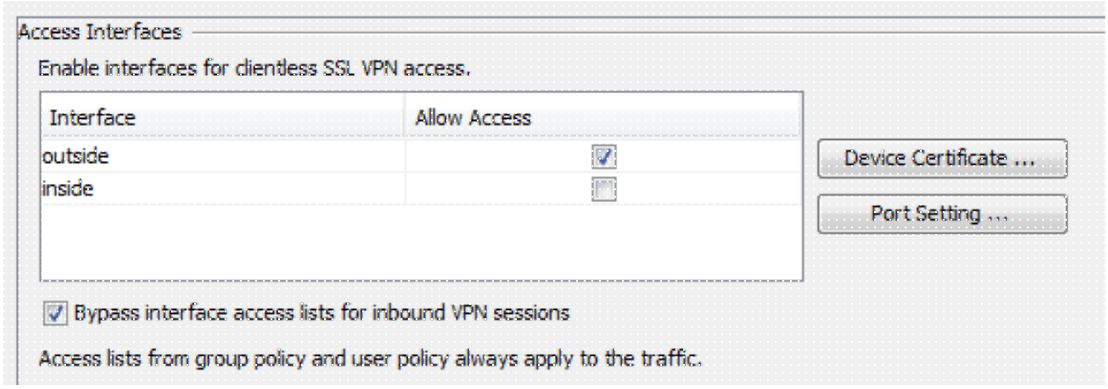


CLI:

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

6. In order to enable the WebVPN on the outside interface, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

Check the **Allow Access** checkbox next to the outside interface.



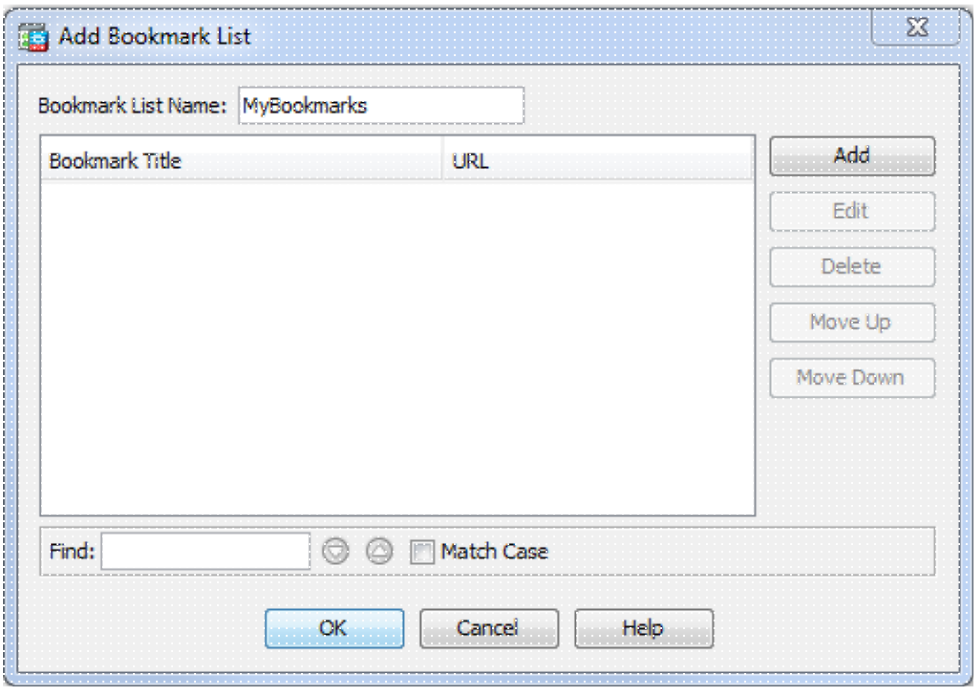
CLI:

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

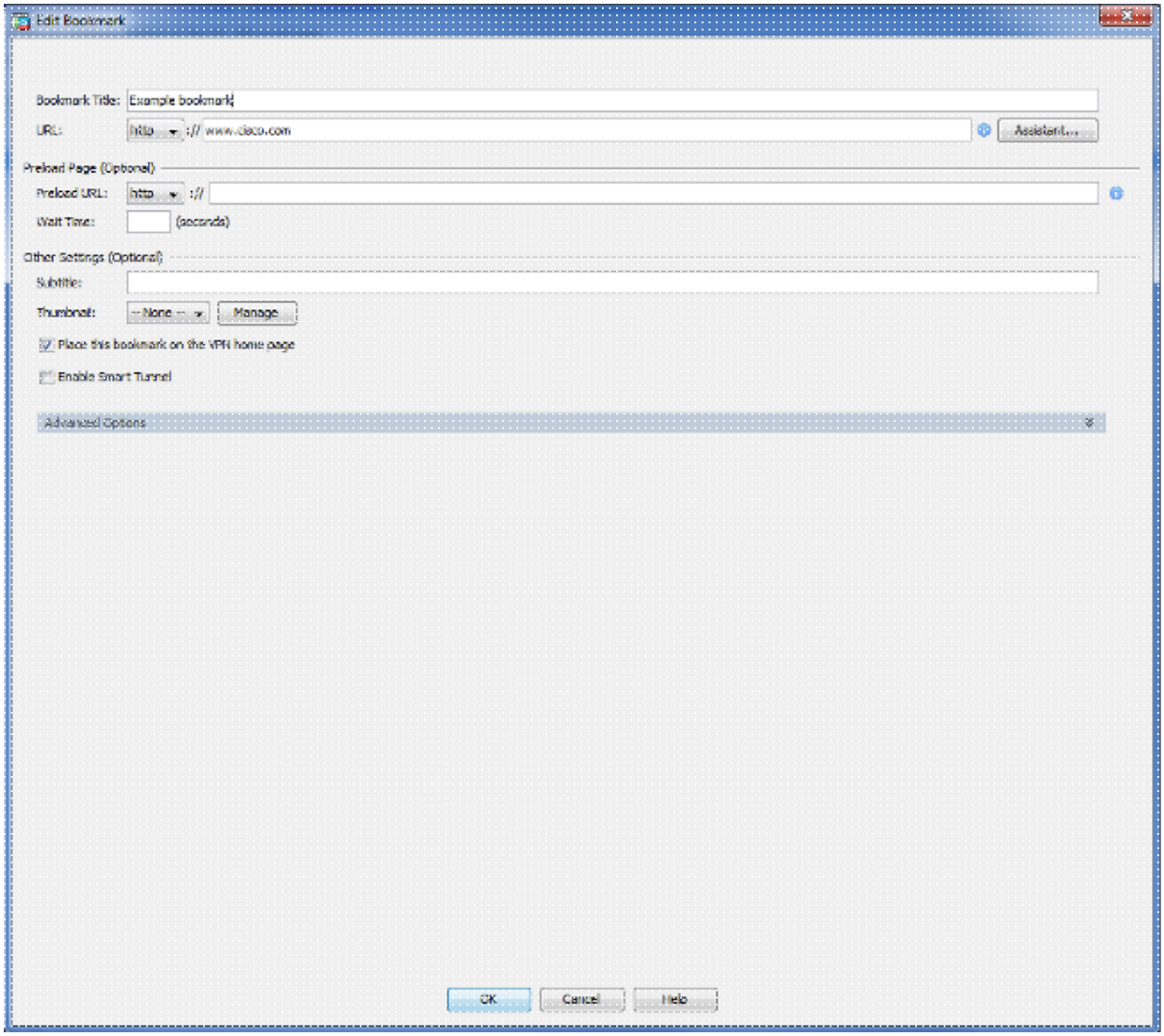
7. (Optional) Create bookmarks for content.

   Bookmarks allow the user to easily browse the internal resources without having to remember the URLs.

   In order to create a bookmark, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Add**.



   Choose **Add** in order to add a specific bookmark.

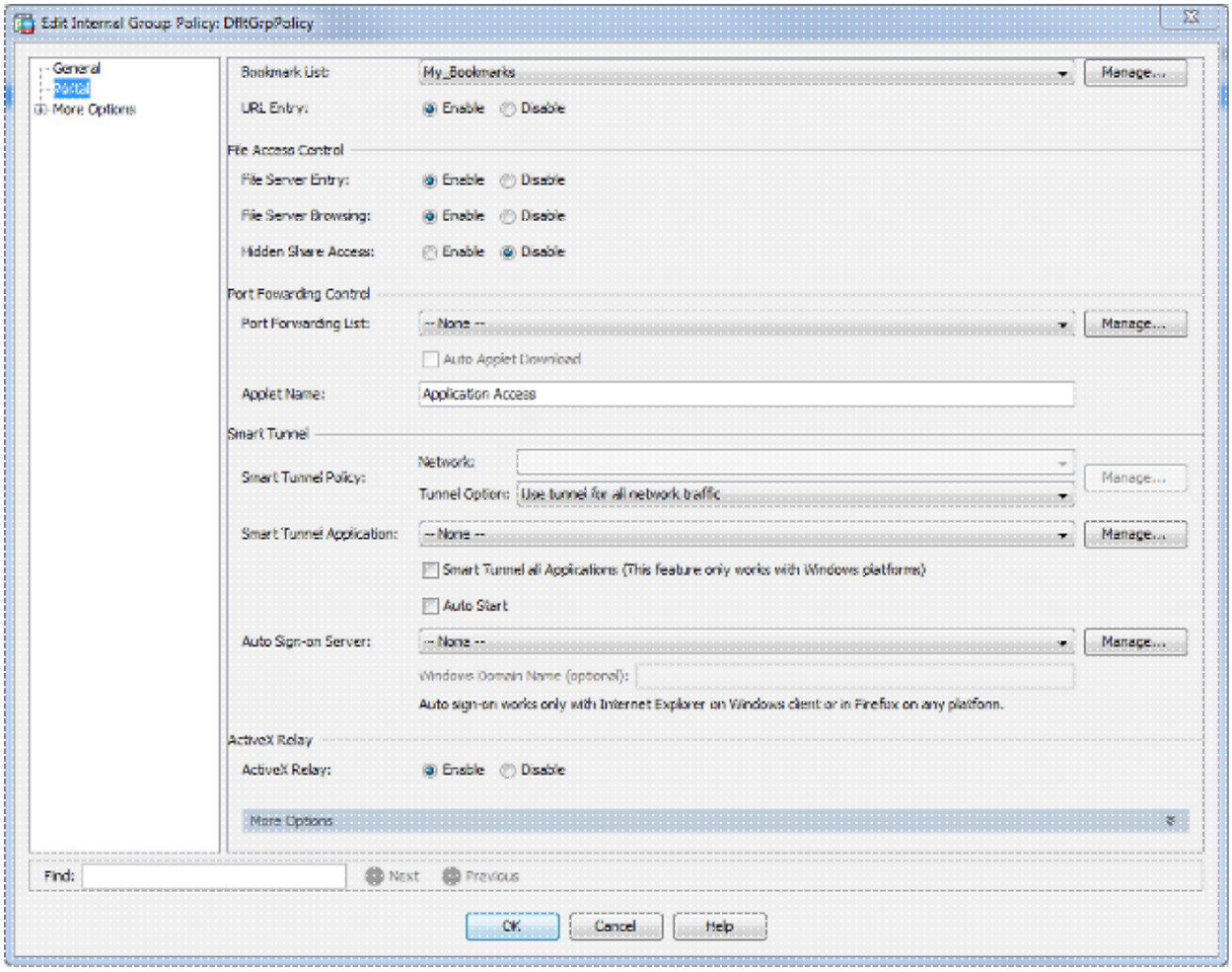


CLI:

It is impossible to create bookmarks via the CLI because they are created as XML files.

8. (Optional) Assign bookmarks to a specific group policy.

   Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Portal > Bookmark List**.

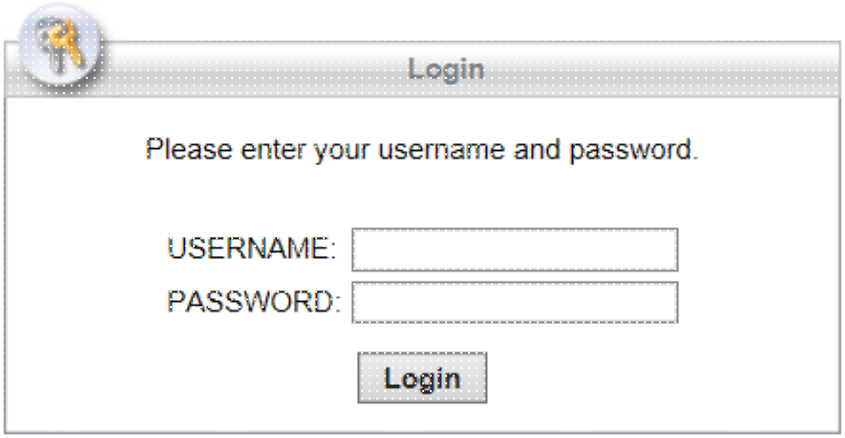


CLI:

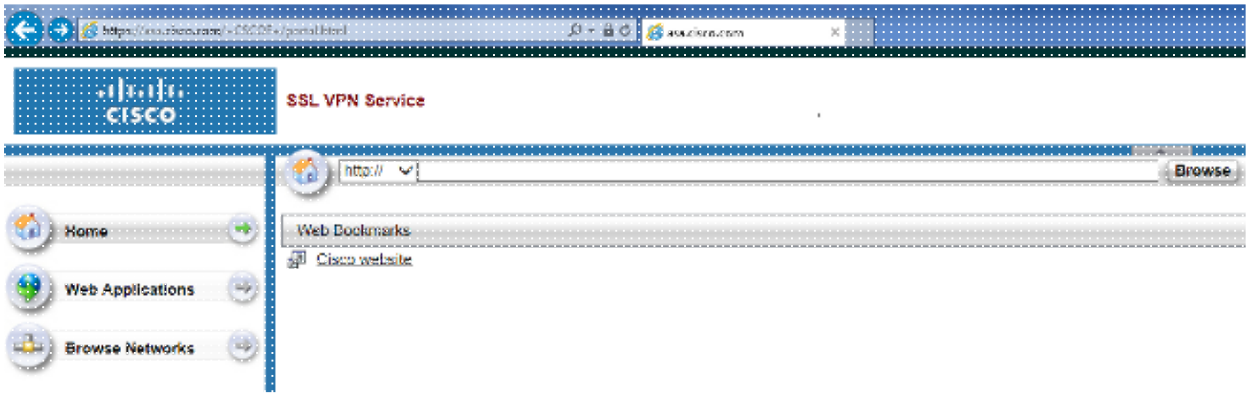
```
ASA(config)# group-policy DfltGrpPolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

Verify

Once the WebVPN has been configured, use the address https://<*FQDN of the ASA*> in the browser.



After logging in you should be able to see the address bar used to navigate to websites and the bookmarks.



Troubleshoot

Procedures Used to Troubleshoot

Follow these instructions in order to troubleshoot your configuration.

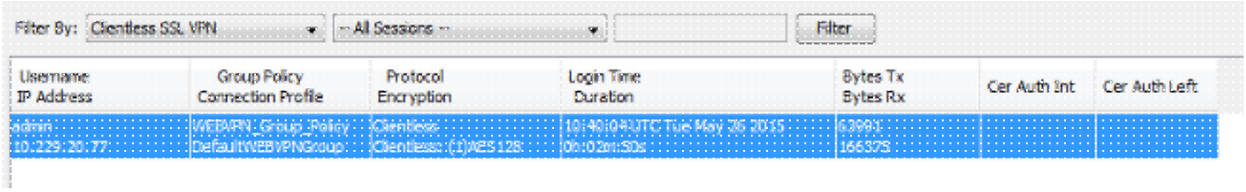
In ASDM, choose **Monitoring > Logging > Real-time Log Viewer > View**. When a client connects to the ASA, note the establishment of TLS session, selection of group policy, and successful authentication of the user.

```
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
```

In ASDM, choose **Monitoring > VPN > VPN Statistics > Sessions > Filter by: Clientless SSL VPN.** Look for the new WebVPN session. Be sure to choose the WebVPN filter and click **Filter**. If a problem occurs, temporarily bypass the ASA device to ensure that clients can access the desired network resources. Review the configuration steps listed in this document.



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 : 0a151601000030005564d84
Security Grp : none
```

Commands Used to Troubleshoot

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **show webvpn** - There are many **show** commands associated with WebVPN. In order to see the use of **show** commands in detail, see the command reference section of the Cisco Security Appliance.
- **debug webvpn -** The use of **debug** commands can adversely impact the ASA. In order to see the use of **debug** commands in more detail, see the command reference section of the Cisco Security Appliance.

Common Problems

User Cannot Log In

Problem

The message "Clientless (browser) SSL VPN access is not allowed." appears in the browser after an unsuccessful login attempt. The AnyConnect Premium license is not installed on the ASA or it is not in use as shown by "Premium AnyConnect license is not enabled on the ASA."

Solution

Enable the Premium AnyConnect license with these commands:

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

Problem

The message "Login failed" appears in the browser after an unsuccessful login attempt. The AnyConnect license limit has been exceeded.

Solution

Look for this message in the logs:

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

Also, verify your license limit:

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

Problem

The message "AnyConnect is not enabled on the VPN server" appears in the browser after an unsuccessful login attempt. Clientless VPN protocol is not enabled in the group-policy.

Solution

Look for this message in the logs:

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

Make sure that Clientless VPN protocol is enabled for the desired group-policy:

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

Unable to Connect More Than Three WebVPN Users to the ASA

Problem

Only three WebVPN clients can connect to the ASA. The connection for the fourth client fails.

Solution

In most cases, this issue is related to a simultaneous login setting within the group policy. Use this illustration in order to configure the desired number of simultaneous logins. In this example, the desired value is 20.

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

WebVPN Clients Cannot Hit Bookmarks and is Grayed Out

Problem

If these bookmarks were configured for users to sign in to the clientless VPN, but on the home screen under "Web Applications" they show up as grayed out, how can I enable these HTTP links so that the users are able to click them and go into the particular URL?

Solution

You should first make sure that the ASA can resolve the websites through DNS. Try to ping the websites by name. If the ASA cannot resolve the name, the link is grayed out. If the DNS servers are internal to your network, configure the DNS domain-lookup private interface.

Citrix Connection Through WebVPN

Problem

The error message "**the ica client received a corrupt ica file.**" occurs for Citrix over WebVPN.

Solution

If you use the *secure gateway* mode for Citrix connection through WebVPN, the ICA file can corrupt. Because the ASA is not compatible with this mode of operation, create a new ICA file in the Direct Mode (non-secure mode).

How to Avoid the Need for a Second Authentication for the Users

Problem

When you access CIFS links on the clientless WebVPN portal, you are prompted for credentials after you click the bookmark. Lightweight Directory Access Protocol (LDAP) is used in order to authenticate both the resources and the users already have entered LDAP credentials to log in to the VPN session.

Solution

You can use the auto-signon feature in this case. Under the specific group-policy being used and under its WebVPN attributes, configure this:

```
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
```

where `X.X.X.X=IP` of the CIFS server and `*=rest of the path` to reach the share file/folder in question.

An example configuration snippet is shown here:

```
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
```

For more information about this, see Configuring SSO with HTTP Basic or NTLM Authentication.

Related Information

- **ASA: Smart Tunnel using ASDM Configuration Example**
- **Technical Support & Documentation - Cisco Systems**

Updated: Jan 05, 2016 Document ID: 119417