ASA에서 클라이언트리스 SSL VPN(WebVPN) 구성

목차

소개

이 문서에서는 클라이언트리스 SSL(Secure Sockets Layer) VPN이 내부 네트워크 리소스에 액세스할 수 있도록 Cisco ASA(Adaptive Security Appliance) 5500 Series에 대한 간단한 컨피그레이션을 제공합니다.클라이언트리스 SSL Virtual Private Network(WebVPN)를 사용하면 장소에 구애받지 않고 회사 네트워크에 제한적이지만 귀중하고 안전하게 액세스할 수 있습니다.사용자는 언제든지 기업 리소스에 대한 안전한 브라우저 기반 액세스를 얻을 수 있습니다.내부 리소스에 액세스하기 위해 추가 클라이언트가 필요하지 않습니다.SSL 연결을 통한 하이퍼텍스트 전송 프로토콜을 사용하여 액세스가 제공됩니다.

클라이언트리스 SSL VPN은 HTTP(Hypertext Transfer Protocol Internet) 사이트에 도달할 수 있는 거의 모든 컴퓨터에서 광범위한 웹 리소스와 웹 지원 및 레거시 애플리케이션에 안전하고 쉽게 액세스할 수 있도록 합니다.여기에는 다음이 포함됩니다.

- 내부 웹 사이트
- Microsoft SharePoint 2003, 2007 및 2010
- Microsoft Outlook Web Access 2003, 2007 및 2013

- Microsoft Outlook Web App 2010
- DWA(Domino Web Access) 8.5 및 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp 버전 5 ~ 6.5
- Citrix XenDesktop 버전 5~5.6 및 7.5
- VMware View 4

지원되는 소프트웨어 목록은 지원되는 VPN 플랫폼, Cisco ASA 5500 Series에서 확인할 수 있습니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- SSL 지원 브라우저
- 버전 7.1 이상의 ASA
- ASA 도메인 이름에 발급된 X.509 인증서
- TCP 포트 443. 클라이언트에서 ASA로의 경로를 따라 차단해서는 안 됩니다.

요구 사항의 전체 목록은 지원되는 VPN 플랫폼, Cisco ASA 5500 Series에서 확인할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 지워진(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

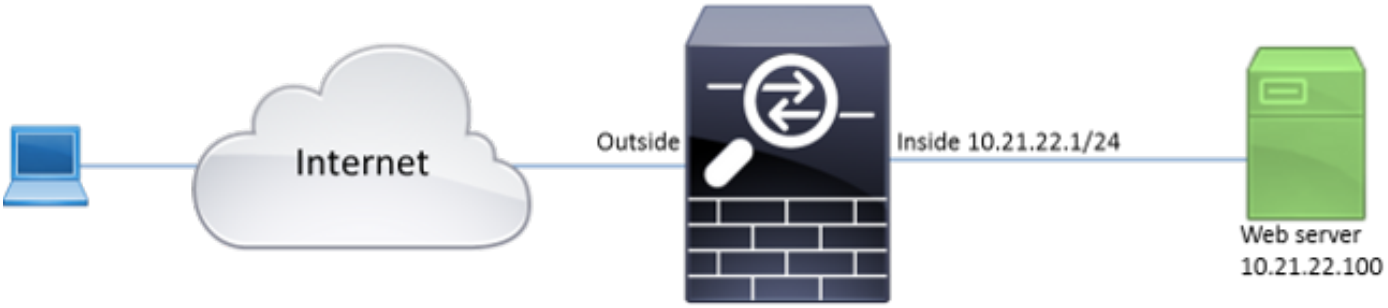
구성

이 문서에서는 ASDM과 CLI의 구성 프로세스에 대해 설명합니다.WebVPN을 구성하기 위해 두 툴 중 하나를 수행하도록 선택할 수 있지만 일부 컨피그레이션 단계는 ASDM에서만 수행할 수 있습니다.

> **참고:** 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 정보를 얻으십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



배경 정보

WebVPN은 클라이언트와 서버 간에 전송되는 데이터를 보호하기 위해 SSL 프로토콜을 사용합니다.브라우저가 ASA에 대한 연결을 시작하면 ASA는 브라우저에 자신을 인증하기 위한 인증서를 표시합니다.클라이언트와 ASA 간의 연결이 안전한지 확인하려면 클라이언트가 이미 신뢰하는 인증 기관에서 서명한 인증서를 ASA에 제공해야 합니다.그렇지 않으면 클라이언트가 ASA의 신뢰성을 검증할 수 없으므로, ASA가 중간자 공격(man-in-the-middle 공격) 및 사용자 환경이 저하될 수 있습니다. 이는 연결이 신뢰할 수 없다는 경고가 표시되기 때문입니다.

> **참고:**기본적으로 ASA는 시작 시 자체 서명 X.509 인증서를 생성합니다.이 인증서는 기본적으로 클라이언트 연결을 제공하는 데 사용됩니다.브라우저에서 이 인증서의 신뢰성을 확인할 수 없으므로 이 인증서를 사용하지 않는 것이 좋습니다.또한 이 인증서는 재부팅할 때마다 다시 생성되므로 재부팅할 때마다 변경됩니다.

인증서 설치가 이 문서의 범위를 벗어났습니다.

구성

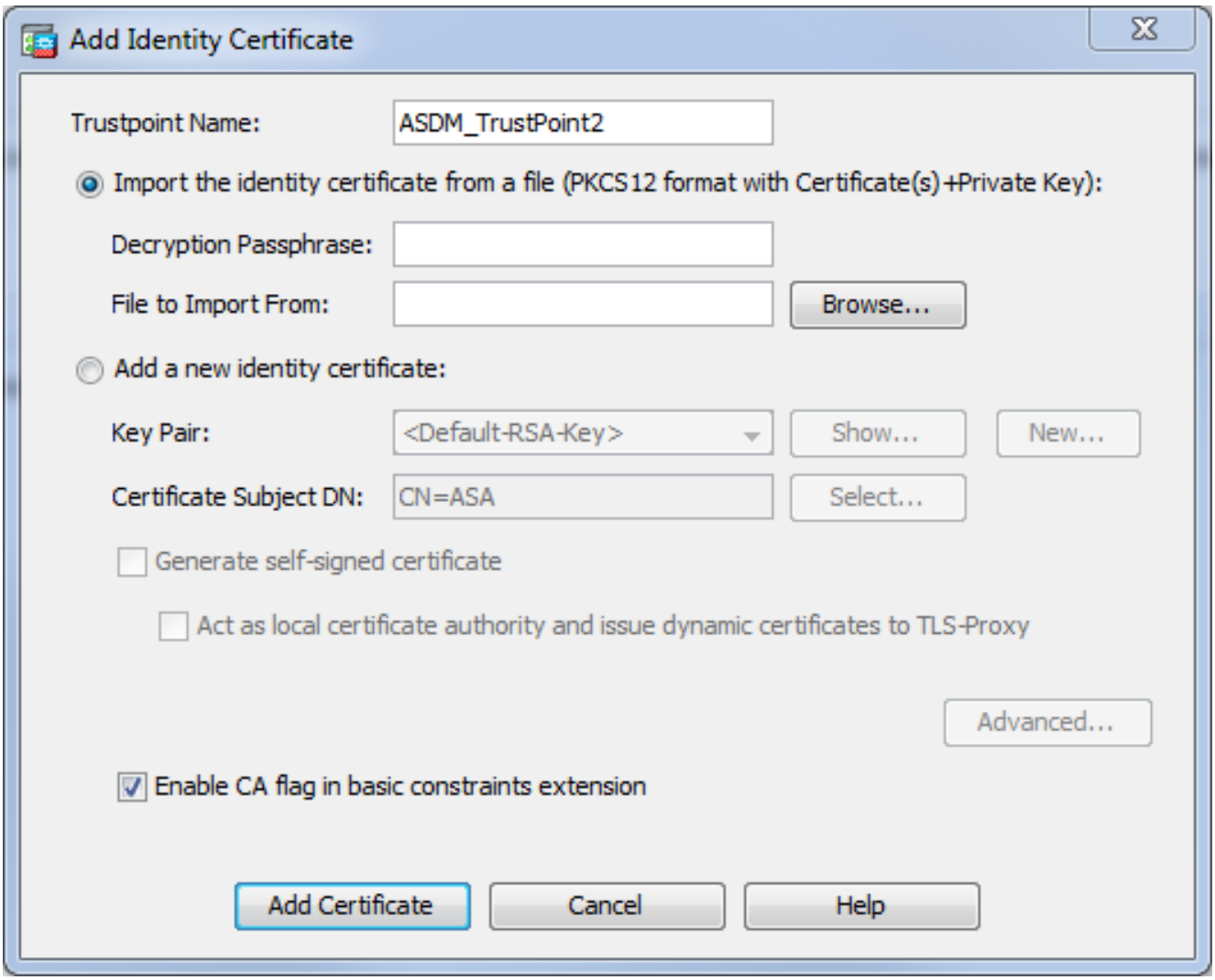
5가지 주요 단계로 ASA에서 WebVPN을 구성합니다.

- ASA에서 사용할 인증서를 구성합니다.
- ASA 인터페이스에서 WebVPN을 활성화합니다.
- WebVPN 액세스를 위한 서버 및/또는 URL(Uniform Resource Locator) 목록을 생성합니다.
- WebVPN 사용자에 대한 그룹 정책을 만듭니다.
- 터널 그룹에 새 그룹 정책을 적용합니다.

> **참고:**릴리스 9.4 이후 ASA 릴리스에서는 SSL 암호를 선택하는 데 사용된 알고리즘이 변경되었습니다(Cisco ASA Series 9.4(x)의 릴리스 정보 참조).EC(Elliptic Curve Capable) 클라이언트만 사용할 경우 인증서에 EC(Elliptic Curve) 개인 키를 사용하는 것이 안전합니다.그렇지 않으면 ASA에서 자체 서명된 임시 인증서를 제공하지 않도록 사용자 지정 암호 그룹을 사용해야 합니다.**ssl 암호 tlsv1.2 사용자 지정 "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:RSA1RSA-SHA1:2와 함께 RSA 기반 암호만** 사용하도록 ASA ASA를 구성할 수 있습니다. -CBC-SHA:RC4-SHA:RC4-MD5" 명령

1. **옵션 1** - pkcs12 파일이 있는 인증서를 가져옵니다.Configuration **> Firewall > Advanced > Certificate Management > Identity Certificates > Add를 선택합니다**.pkcs12 파일로 설치하거나 PEM(Privacy Enhanced Mail) 형식으로 내용을 붙여넣을 수 있습니다

.



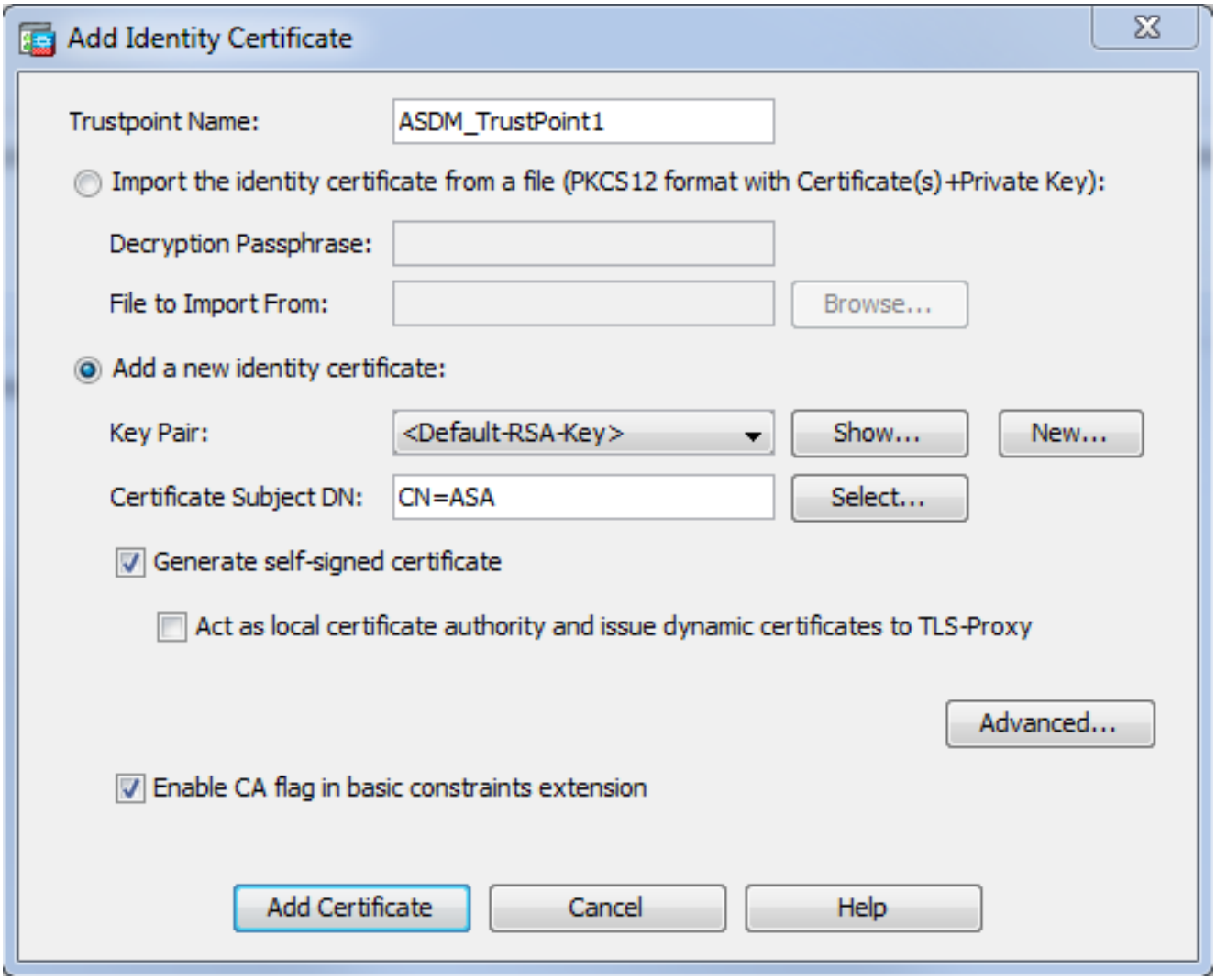
CLI:

```
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
```

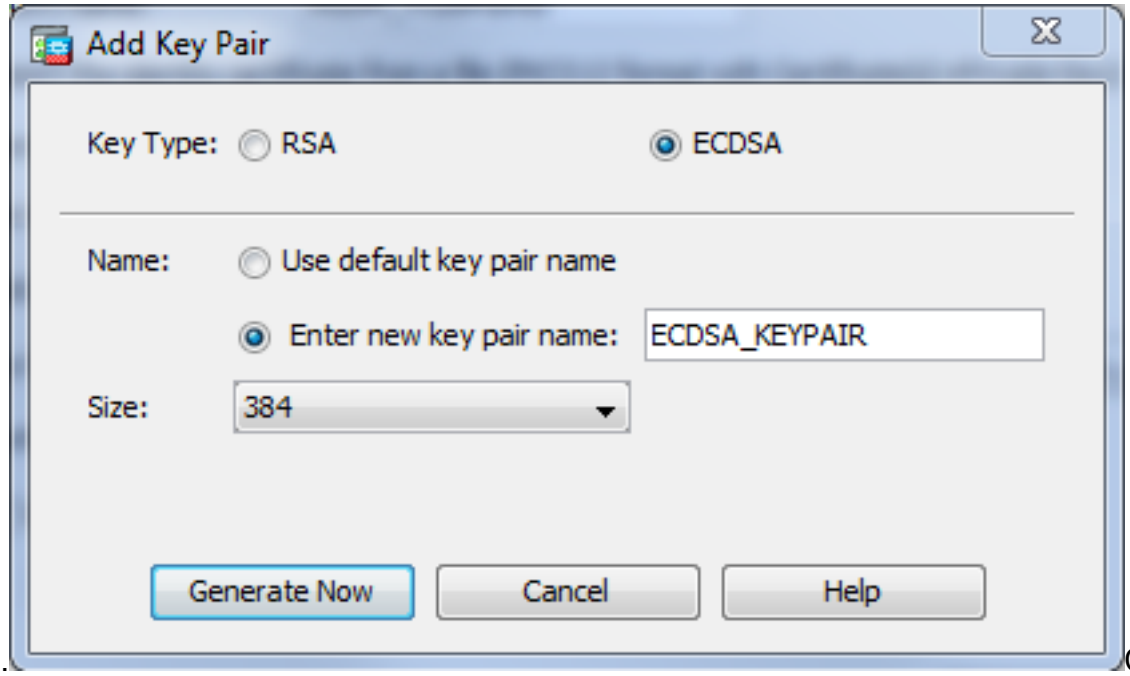
```
INFO: Import PKCS12 operation completed successfully
```

옵션 2 - 자체 서명 인증서를 생성합니다.Configuration **> Firewall > Advanced > Certificate Management > Identity Certificates > Add를 선택합니다**.Add a **new identity certificate** 라디오 버튼**을** 클릭합니다.Generate **self-signed certificate 확인란을 선택합니다**.ASA의 도메인 이름과 일치하는 CN(Common Name)을 선택합니다

.



인증서**에** 대한 키 쌍을 생성하려면 New를 클릭합니다.키 유형, 이름 및 크기를 선택합니다

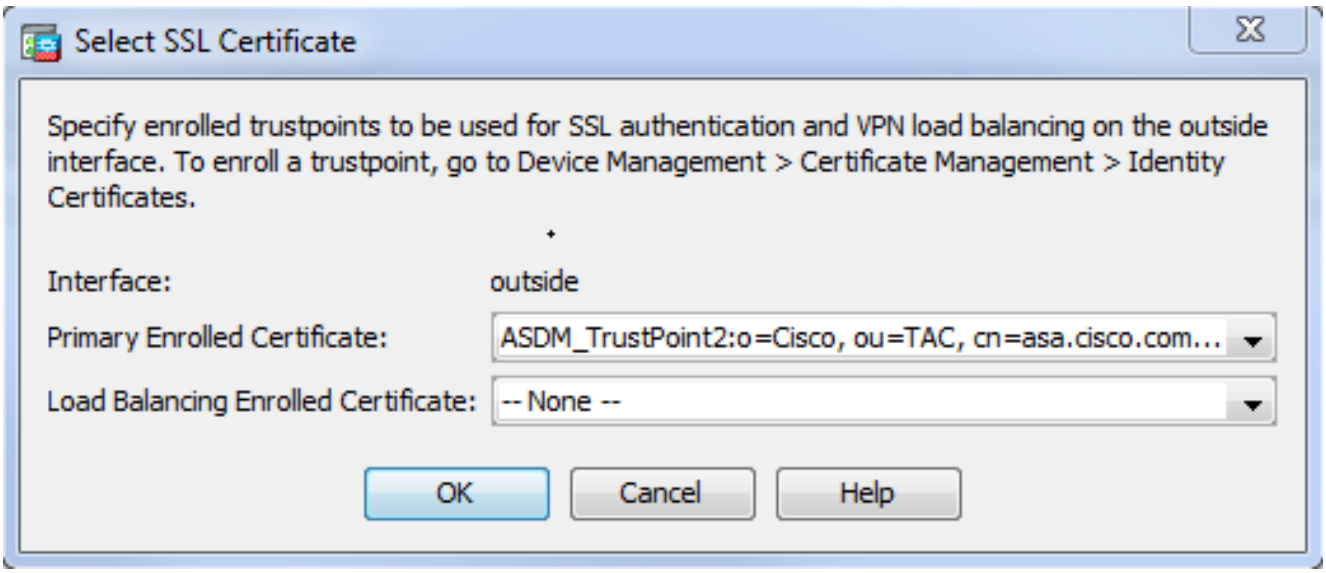


.CLI:

```
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 연결을 제공하는 데 사용할 인증서를 선택합니다.Configuration **> Remote Access VPN > Advanced > SSL Settings를 선택합니다**.Certificates(인증서) 메뉴에서 외부 인터페이스에 대해 원하는 인증서와 연결된 신뢰 지점을 선택합니다.**적용**을 **클릭합니다**

.

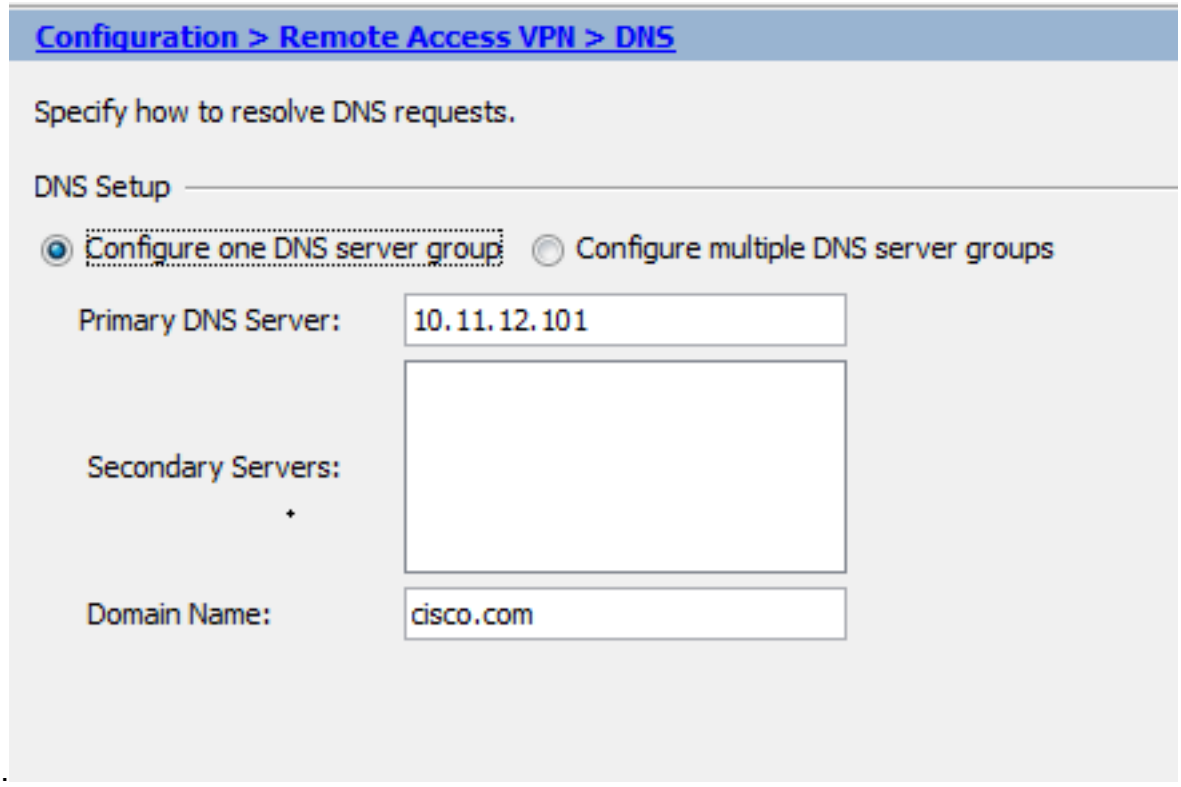


동일한 CLI 구성:

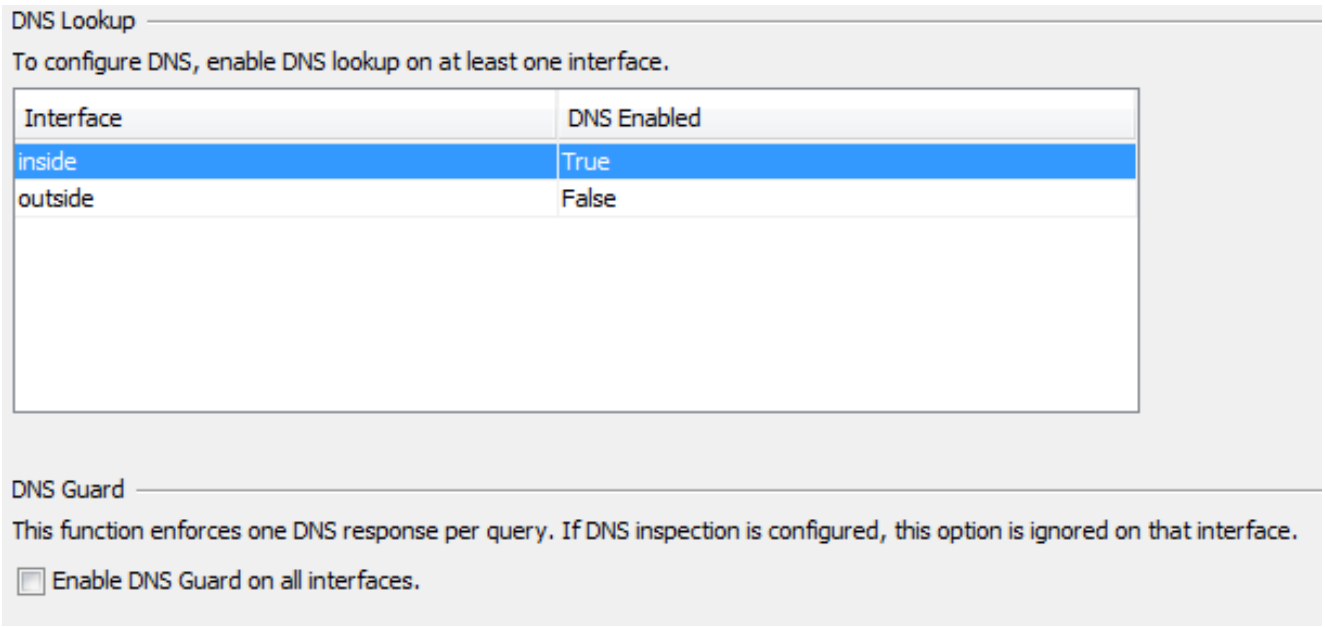
```
ASA(config)# ssl trust-point
```

3. (선택 사항) DNS(Domain Name Server) 조회를 활성화합니다.WebVPN 서버는 클라이언트

연결을 위한 프록시 역할을 합니다.이는 ASA가 클라이언트를 대신하여 리소스에 대한 연결을 생성함을 의미합니다.클라이언트가 도메인 이름을 사용하는 리소스에 연결해야 하는 경우 ASA는 DNS 조회를 수행해야 합니다.Configuration(**컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > DNS를 선택합니다**.하나 이상의 DNS 서버를 구성하고 DNS 서버를 접하는 인터페이스에서 DNS 조회를 활성화합니다



.

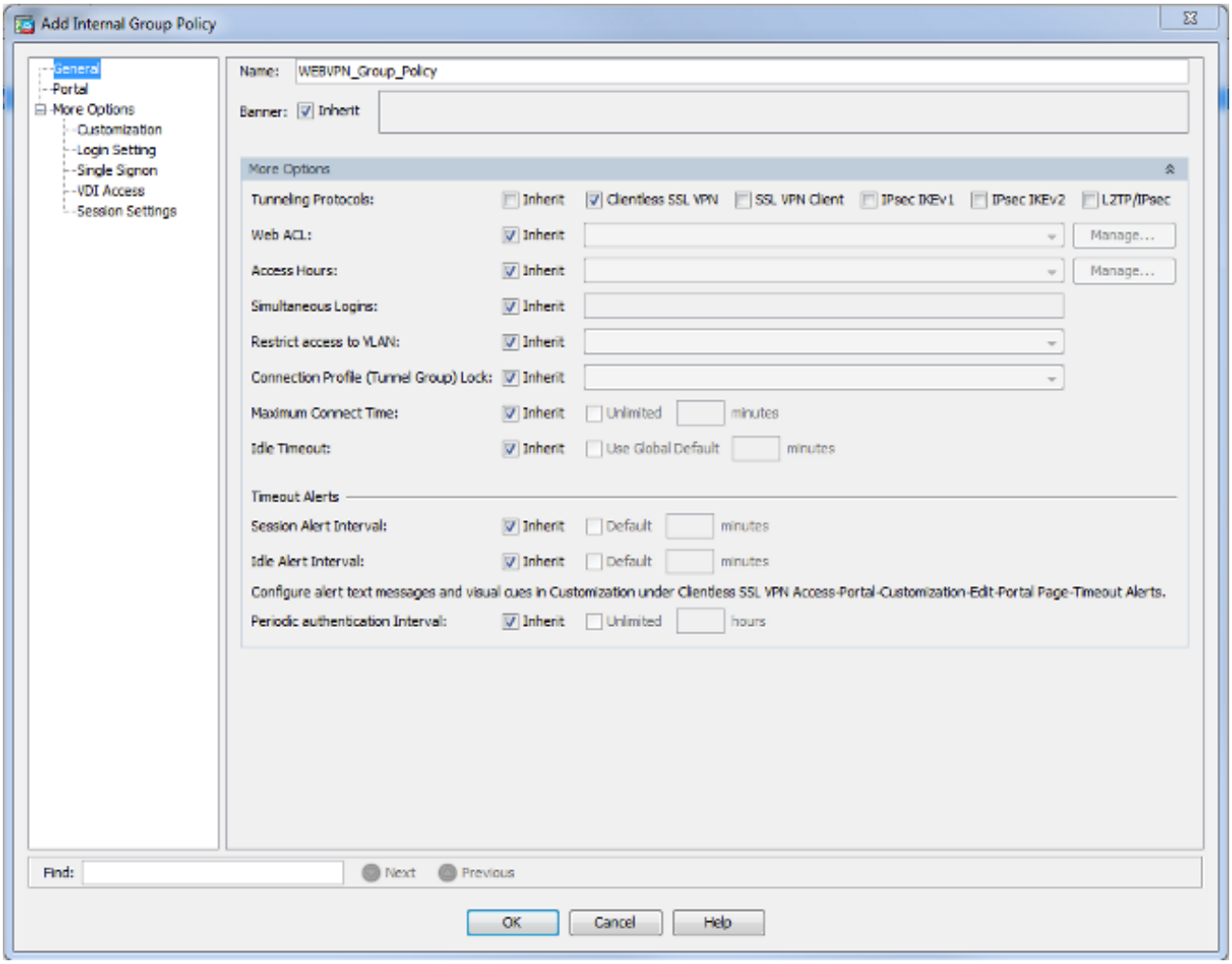


CLI:

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

4. (선택 사항) WEBVPN 연결을 위한 그룹 정책을 생성합니다.Configuration(**구성) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Group Policies(그룹 정책) > Add Internal Group Policy(내부 그룹 정책 추가)를 선택합니다**.General Options(일반 옵션)에서 Tuneling Protocols(터널링 프로토콜) 값을 "Clientless SSL VPN"으로 변경합니다

.



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. 연결 프로파일을 구성합니다.ASDM에서 Configuration(구성) **> Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Connection Profiles(연결 프로파일)를** 선택합니다.
연결 프로파일 및 그룹 정책에 대한 개요는 Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.4 - 연결 프로파일, 그룹 정책 및 사용자를 참조하십시오.기본적으로 WebVPN 연결은 DefaultWEBVPNGroup 프로필을 사용합니다.추가 프로파일을 생성할 수 있습니다.**참고:**다른 프로파일에 사용자를 할당하는 방법은 다양합니다.

- 사용자는 드롭다운 목록 또는 특정 URL에서 연결 프로파일을 수동으로 선택할 수 있습니다.ASA 8.x 참조사용자가 그룹 별칭 및 그룹-URL 방법을 통해 WebVPN 로그인 시 그룹을 선택할 수 있습니다.

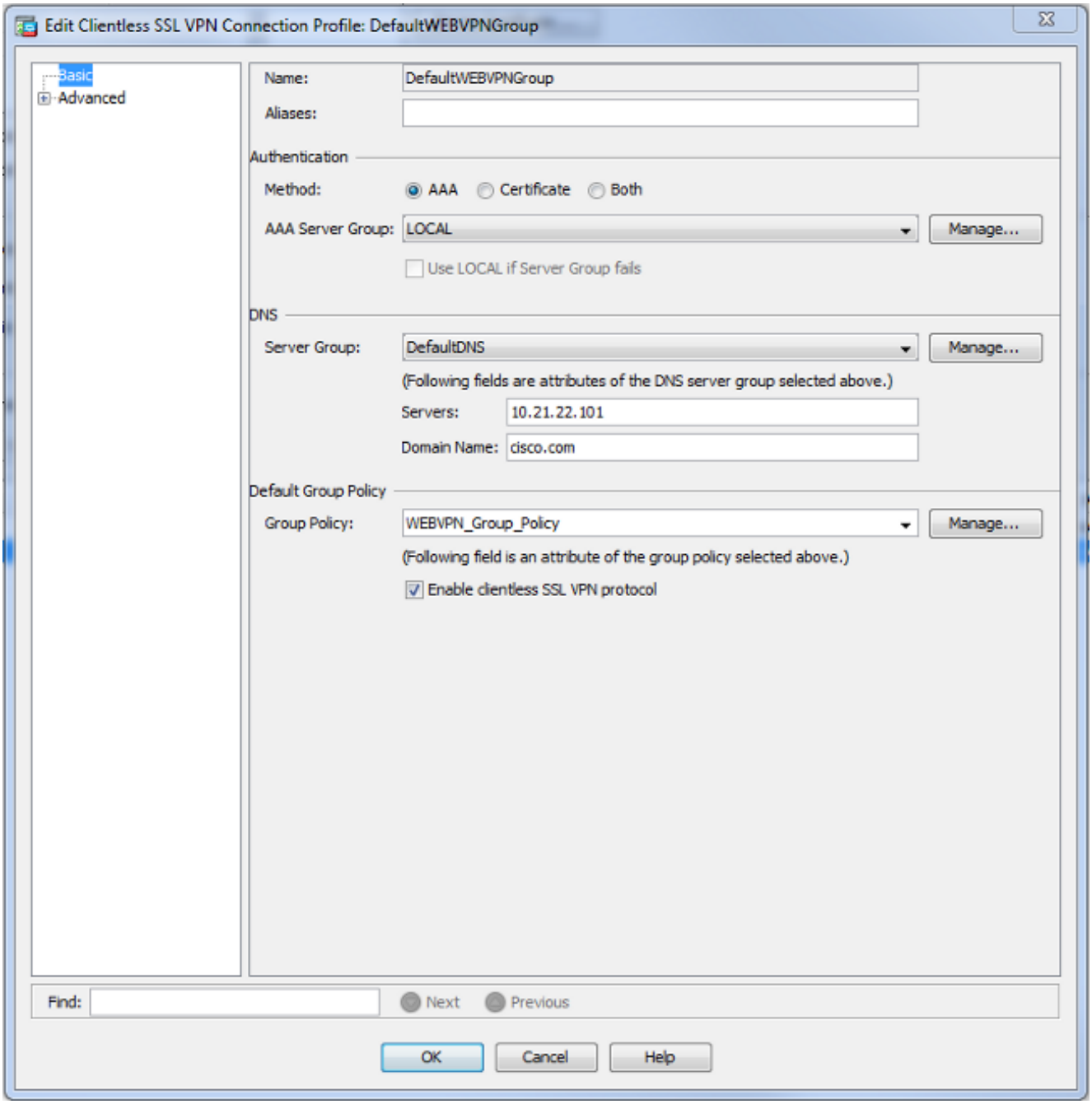
- LDAP 서버를 사용하는 경우 LDAP 서버에서 받은 특성을 기반으로 사용자 프로필을 할당할 수 있습니다. ASA Use of LDAP Attribute Maps Configuration Example을 참조하십시오.

- 클라이언트의 인증서 기반 인증을 사용하는 경우 인증서에 포함된 필드를 기반으로 사용자를 프로파일에 매핑할 수 있습니다. Cisco ASA Series VPN CLI 컨피그레이션 가이드, 9.4 - IKEv1에 대한 인증서 그룹 일치 구성 을 참조하십시오.

- 사용자를 그룹 정책에 수동으로 할당하려면 Cisco ASA Series VPN CLI 컨피그레이션 가이

드, 9.4 - 개별 사용자에 대한 특성 구성을 참조하십시오.DefaultWEBVPNGroup 프로필을 편집하고 Default Group Policy(기본 그룹 정책) 아래에서 WEBVPN_Group_Policy를 선택합니다

.

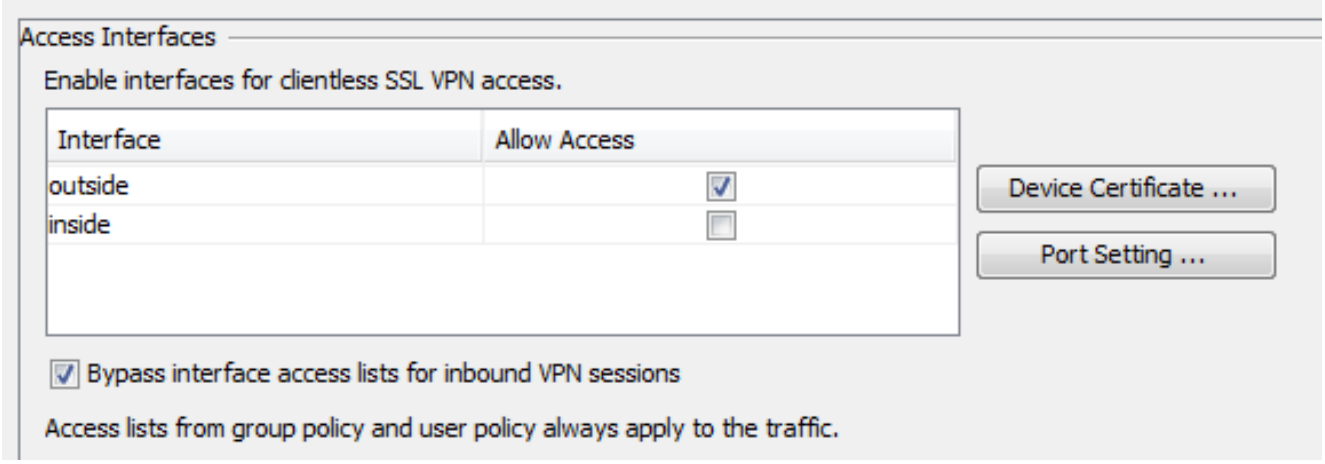


CLI:

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

6. 외부 인터페이스에서 WebVPN을 활성화하려면 Configuration(구성) **> Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Connection Profiles(연결 프로파일)**를 선택합니다.외부 인터페이스 옆에 있는 **Allow Access**(액세스 허용) 확인란을 선택합니다

.

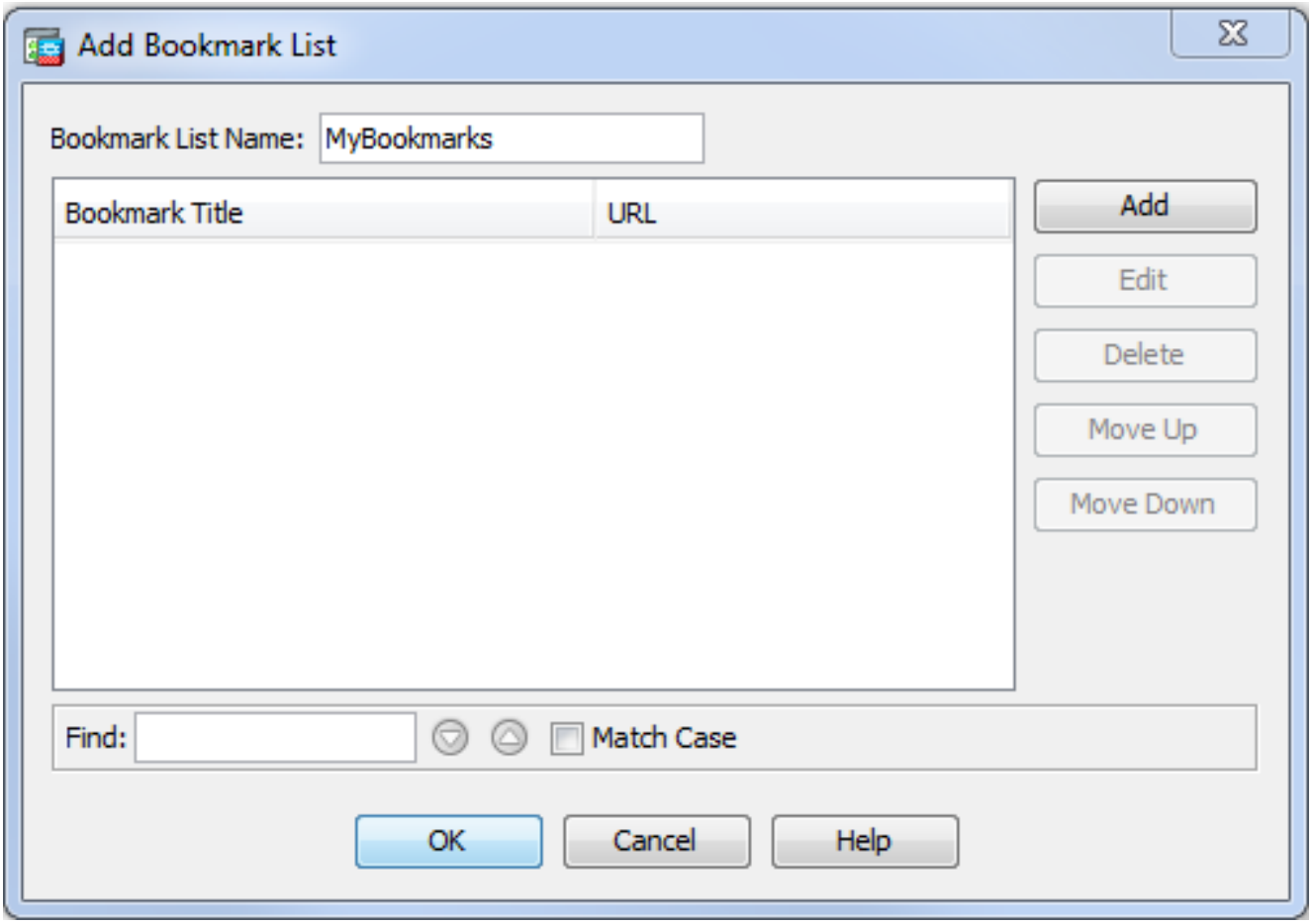


CLI:

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

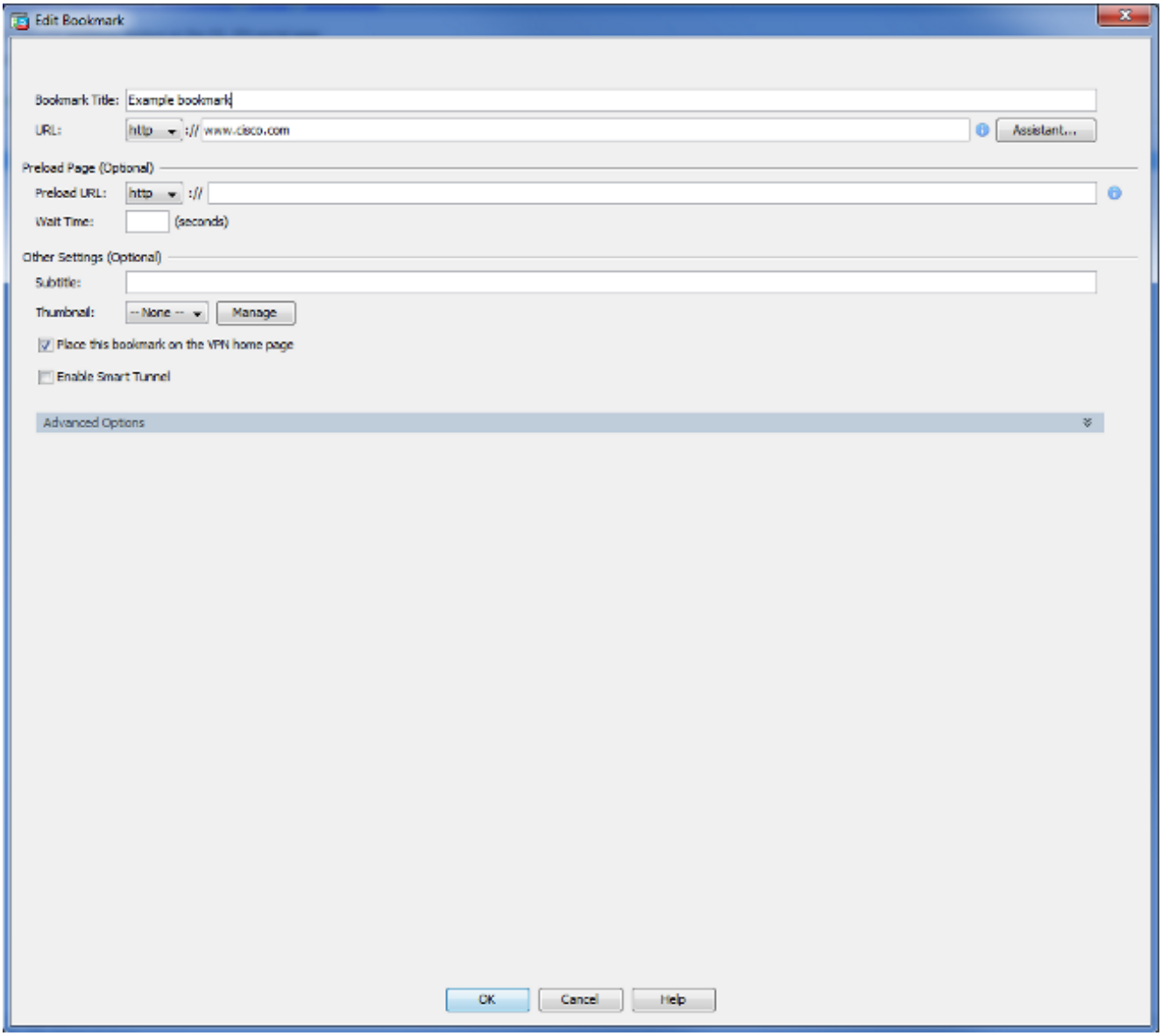
7. (선택 사항) 콘텐츠에 대한 책갈피를 만듭니다.북마크를 사용하면 URL을 기억하지 않고도 내부 리소스를 쉽게 탐색할 수 있습니다.북마크를 생성하려면 Configuration(구성) **> Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Portal(포털) > Bookmarks(책갈피) > Add(추가)를** 선택합니다

.



특정 책갈피를 추가하려면 Add(추가)를 선택합니다

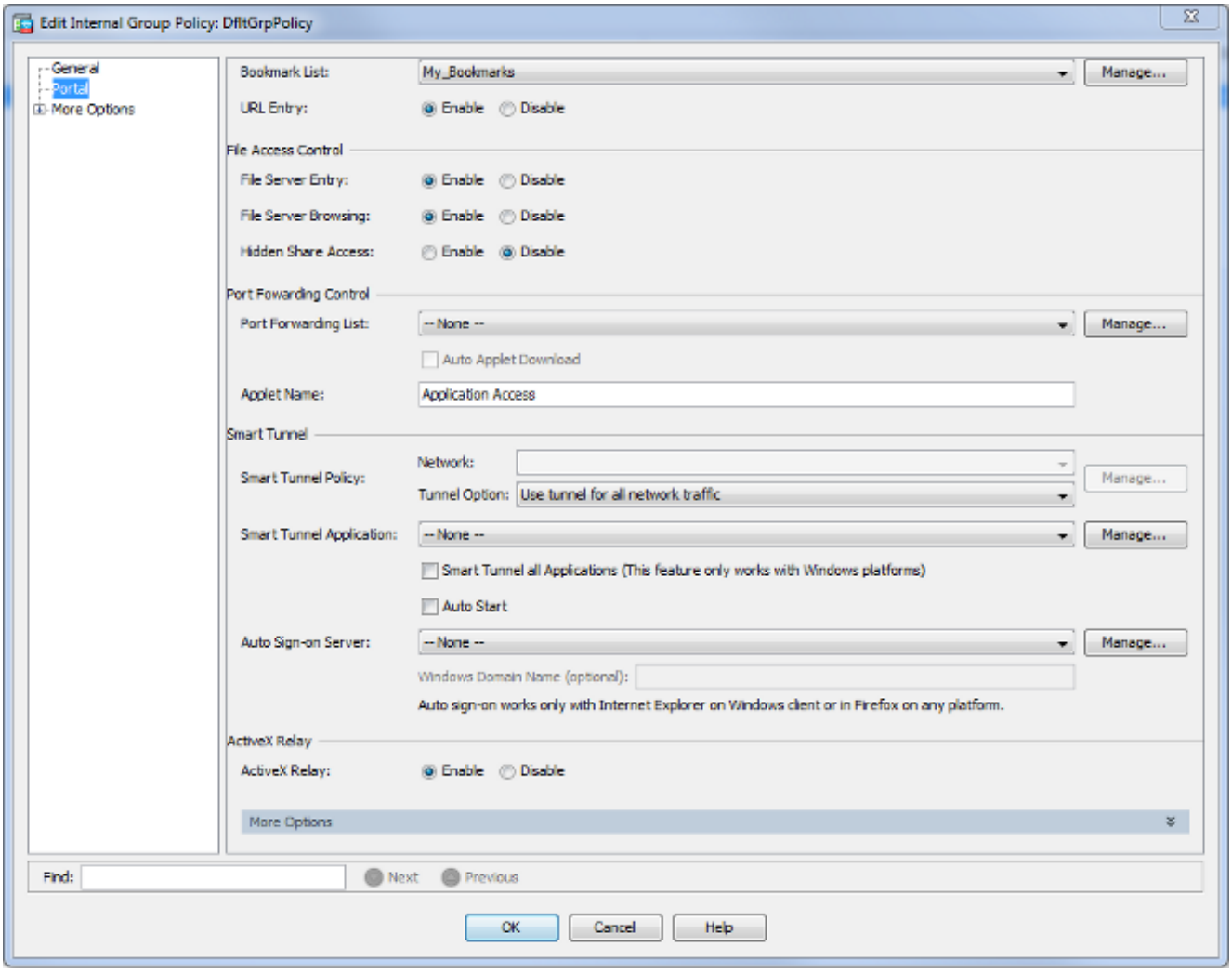
.



CLI:CLI를 통해 북마크를 생성하는 것은 XML 파일로 생성되므로 불가능합니다.

8. (선택 사항) 특정 그룹 정책에 책갈피를 할당합니다.Configuration(**구성**) > **Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Group Policies(그룹 정책) > Edit(편집) > Portal(포털) > Bookmark List(책갈피 목록)를 선택합니다**

.

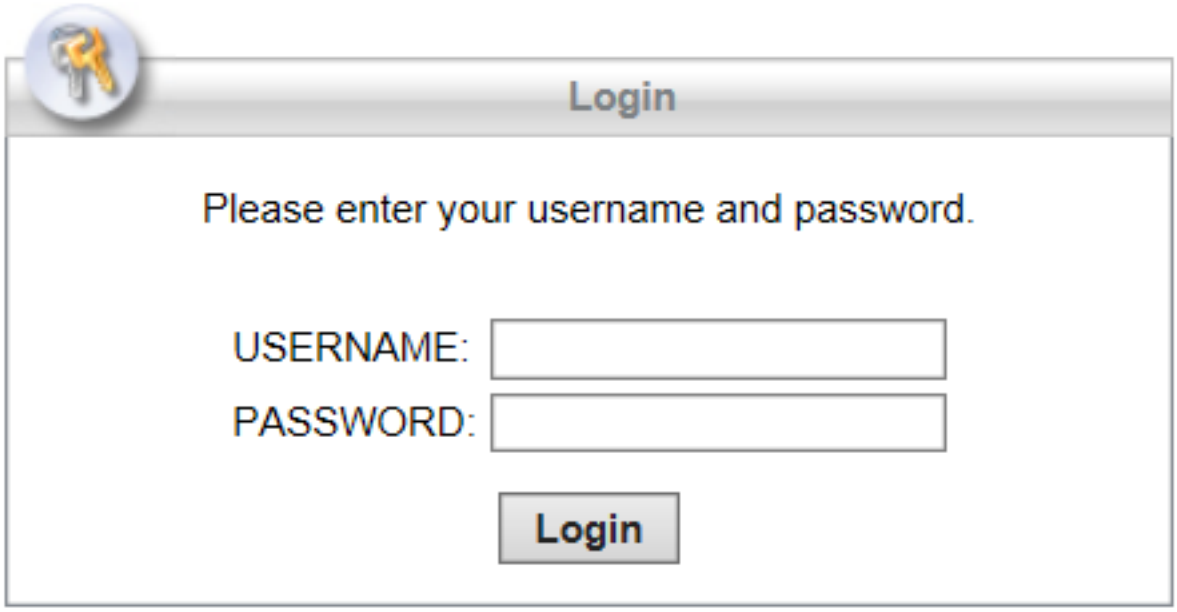


CLI:

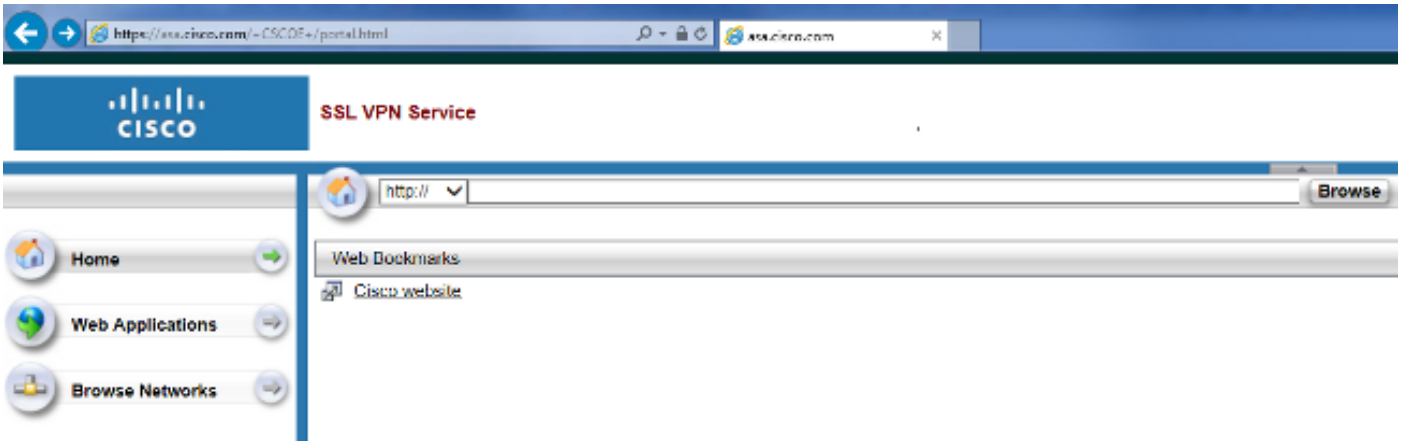
```
ASA(config)# group-policy DfltGrpPolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

다음을 확인합니다.

WebVPN이 구성되면 브라우저에서 https://<*ASA의 FQDN*> 주소를 사용합니다.



로그인한 후에는 웹 사이트 및 책갈피를 탐색하는 데 사용되는 주소 표시줄을 볼 수 있어야 합니다.



문제 해결

문제 해결에 사용되는 절차

컨피그레이션 문제를 해결하려면 다음 지침을 따르십시오.

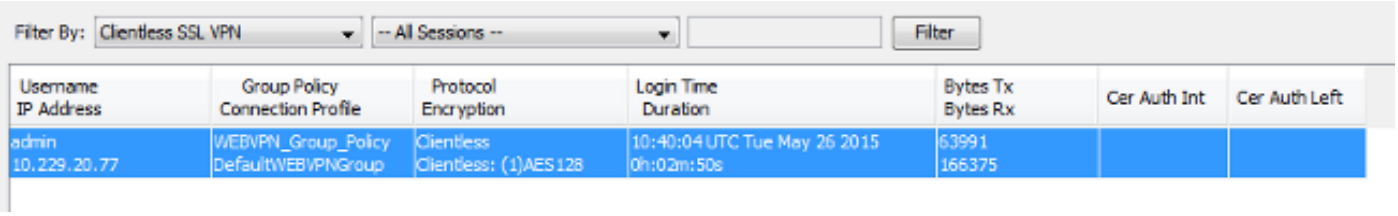
ASDM에서 **Monitoring > Logging > Real-time Log Viewer > View**를 선택합니다.클라이언트가 ASA에 연결되면 TLS 세션 설정, 그룹 정책 선택, 사용자의 성공적인 인증에 유의하십시오.

```
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
```

ASDM에서 **Monitoring > VPN > VPN Statistics > Sessions > Filter by:(필터링 기준:클라이언트리스 SSL VPN.**새 WebVPN 세션을 찾습니다.WebVPN 필터를 선택하고 Filter(필터)를 **클릭합니다**.문제가 발생하면 클라이언트가 원하는 네트워크 리소스에 액세스할 수 있도록 ASA 디바이스를 일시적으로 우회합니다.이 문서에 나열된 구성 단계를 검토합니다.



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
```

문제 해결에 사용되는 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여

show 명령 출력의 분석을 봅니다.

참고:debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **show webvpn** - WebVPN과 관련된 **show** 명령이 많습니다.**show** 명령의 사용을 자세히 보려면 Cisco Security Appliance의 명령 참조 섹션을 참조하십시오.
- **debug webvpn -** debug 명령을 사용하면 ASA에 부정적인 영향을 미칠 수 있습니다 .debug 명령의 사용을 자세히 보려면 Cisco Security Appliance의 명령 참조 섹션을 참조하십시오.

일반적인 문제

사용자가 로그인할 수 없음

문제

"클라이언트리스(브라우저) SSL VPN 액세스는 허용되지 않습니다." 메시지 가 로그인 실패 후 브라우저에 나타납니다.AnyConnect Premium 라이센스는 ASA에 설치되지 않았거나 "Premium AnyConnect 라이센스가 ASA에서 활성화되지 않음"과 같이 사용되지 않습니다.

솔루션

다음 명령을 사용하여 Premium AnyConnect 라이센스를 활성화합니다.

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

문제

로그인 실패 후 브라우저에 "Login failed(로그인 실패)" 메시지가 나타납니다.AnyConnect 라이센스 제한을 초과했습니다.

솔루션

로그에서 다음 메시지를 찾습니다.

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

또한 라이센스 제한을 확인합니다.

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

문제

로그인 실패 후 브라우저에 "AnyConnect is not enabled on the VPN server(VPN 서버에서 AnyConnect가 활성화되지 않음)" 메시지가 나타납니다.클라이언트리스 VPN 프로토콜은 그룹 정책에서 활성화되지 않습니다.

솔루션

로그에서 다음 메시지를 찾습니다.

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

클라이언트리스 VPN 프로토콜이 원하는 그룹 정책에 대해 활성화되었는지 확인합니다.

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

3명 이상의 WebVPN 사용자를 ASA에 연결할 수 없음

문제

3개의 WebVPN 클라이언트만 ASA에 연결할 수 있습니다.네 번째 클라이언트에 대한 연결이 실패합니다.

솔루션

대부분의 경우 이 문제는 그룹 정책 내의 동시 로그인 설정과 관련이 있습니다.원하는 동시 로그인 수를 구성하려면 이 그림을 사용합니다.이 예에서 원하는 값은 20입니다.

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

WebVPN 클라이언트가 책갈피를 누를 수 없으며 회색으로 표시됩니다.

문제

사용자가 클라이언트리스 VPN에 로그인하도록 북마크를 구성했지만 홈 화면에서 "Web Applications(웹 애플리케이션)"가 회색으로 표시되는 경우, 사용자가 해당 북마크를 클릭하여 특정 URL로 이동할 수 있도록 이러한 HTTP 링크를 어떻게 활성화합니까?

솔루션

먼저 ASA가 DNS를 통해 웹 사이트를 확인할 수 있는지 확인해야 합니다.이름으로 웹 사이트에 ping을 시도합니다.ASA에서 이름을 확인할 수 없는 경우 링크가 회색으로 표시됩니다.DNS 서버가 네트워크의 내부에 있는 경우 DNS 도메인 조회 개인 인터페이스를 구성합니다.

WebVPN을 통한 Citrix 연결

문제

오류 메시지 "ica **클라이언트가 손상된 ica 파일을 받았습니다.**" WebVPN을 통해 Citrix에 대해 발생합니다.

솔루션

WebVPN을 통해 Citrix 연결에 *보안 게이트웨이* 모드를 사용하는 경우 ICA 파일이 손상될 수 있습니다.ASA는 이 작업 모드와 호환되지 않으므로 직접 모드(비보안 모드)에서 새 ICA 파일을 생성합니다.

사용자를 위한 두 번째 인증이 필요하지 않게 하는 방법

문제

클라이언트리스 WebVPN 포털에서 CIFS 링크에 액세스하면 책갈피를 클릭한 후 자격 증명을 입력하라는 메시지가 표시됩니다.LDAP(Lightweight Directory Access Protocol)는 리소스 및 사용자가 VPN 세션에 로그인하기 위해 이미 LDAP 자격 증명을 입력한 사용자를 모두 인증하는 데 사용됩니다.

솔루션

이 경우 자동 사인온 기능을 사용할 수 있습니다.사용 중인 특정 그룹 정책 및 WebVPN 특성 아래에서 다음을 구성합니다.

```
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
```

여기서 `X.X.X.X=CIFS` 서버의 `IP` 및 `*=` 문제의 공유 파일/폴더에 도달할 수 있습니다.

다음은 컨피그레이션 조각의 예입니다.

```
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
```

이에 대한 자세한 내용은 HTTP 기본 또는 NTLM 인증을 사용하여 SSO 구성을 참조하십시오.

관련 정보

- ASA:ASDM 컨피그레이션을 사용하는 스마트 터널 예
- 기술 지원 및 문서 – Cisco Systems