

Clientloze SSL VPN (WebVPN) configureren op de ASA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Achtergrondinformatie](#)

[Configuratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Procedures voor probleemoplossing](#)

[Opdrachten gebruikt voor probleemoplossing](#)

[Vaak voorkomende problemen](#)

[Gebruiker kan niet inloggen](#)

[Kan niet meer dan drie WebVPN-gebruikers aan de ASA verbinden](#)

[Clients voor WebeVPN kunnen geen favorieten maken en worden afgevoerd](#)

[Citrix Connection via WebVPN](#)

[Vermijd de noodzaak van een tweede verificatie voor de gebruikers](#)

[Gerelateerde informatie](#)

Inleiding

Dit document biedt een eenvoudige configuratie voor de Cisco adaptieve security applicatie (ASA) 5500 Series om clientloze Secure Socket Layer (SSL) VPN-toegang tot interne netwerkbronnen mogelijk te maken. Clientless SSL Virtual Private Network (WebVPN) maakt beperkte, maar waardevolle, beveiligde toegang tot het bedrijfsnetwerk vanuit elke locatie mogelijk. Gebruikers kunnen op elk moment een veilige toegang tot bedrijfsmiddelen bereiken die op een browser is gebaseerd. Er is geen extra cliënt nodig om toegang te krijgen tot interne middelen. De toegang wordt verleend met behulp van een Hypertext Transfer Protocol over SSL-verbinding.

Clientloze SSL VPN biedt veilige en gemakkelijke toegang tot een breed scala aan web resources en zowel web-enabled- als legacy-toepassingen van vrijwel elke computer die Hypertext Transfer Protocol Internet (HTTP)-sites kan bereiken. Dit omvat:

- Interne websites
- Microsoft SharePoint 2003, 2007 en 2010
- Microsoft Outlook Web Access 2003, 2007 en 2013

- Microsoft Outlook-app 2010
- Domino Web Access (DWA) 8.5 en 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp versie 5 tot 6.5
- Citrix XenDesktop versie 5 tot 5.6 en 7.5
- VMware View 4

Een lijst met ondersteunde software kan gevonden worden in [Ondersteunde VPN-platforms, Cisco ASA 5500 Series](#).

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- SSL-enabled-browser
- ASA met versie 7.1 of hoger
- X.509-certificaat afgegeven aan de ASA-domeinnaam
- TCP-poort 443, die niet geblokkeerd mag worden langs het pad van de client naar de ASA

De volledige lijst met vereisten kan worden gevonden in [Ondersteunde VPN-platforms, Cisco ASA 5500 Series](#).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA versie 9.4(1)
- Adaptieve Security Devices Manager (ASDM) versie 7.4(2)
- ASA 5515-X

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, begonnen met een gewiste (standaard) configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

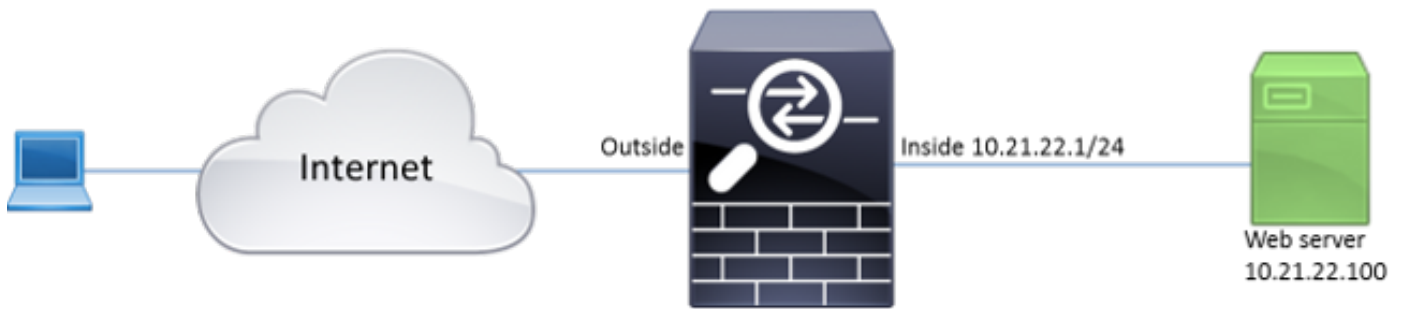
Configureren

Dit artikel beschrijft het configuratieproces voor zowel de ASDM als de CLI. U kunt ervoor kiezen een van de gereedschappen te volgen om WebVPN te configureren, maar sommige configuratiestappen kunnen alleen met ASDM worden uitgevoerd.

Opmerking: Gebruik het [Opdrachtupgereedschap](#) (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Achtergrondinformatie

Webex VPN gebruikt het SSL-protocol om de gegevens te beveiligen die tussen de client en de server zijn overgebracht. Wanneer de browser een verbinding met de ASA initieert, stelt de ASA zijn certificaat voor om zichzelf aan de browser te certificeren. Om ervoor te zorgen dat de verbinding tussen de klant en de ASA veilig is, moet u de ASA het certificaat geven dat door de certificaatautoriteit wordt ondertekend dat de klant reeds vertrouwt. Anders zal de klant niet over de middelen beschikken om de authenticiteit van de ASA te controleren, wat resulteert in de mogelijkheid van de man-in-het-midden aanval en de slechte gebruikerservaring, omdat de browser een waarschuwing geeft dat de verbinding niet vertrouwd is.

Opmerking: Standaard genereert de ASA een zichzelf getekend X.509-certificaat bij opstarten. Dit certificaat wordt gebruikt om standaardinstelling clientverbindingen te maken. Het wordt niet aanbevolen dit certificaat te gebruiken omdat de authenticiteit ervan niet kan worden geverifieerd door de browser. Bovendien wordt dit certificaat na elke herstart opnieuw gegenereerd, zodat het na elke herstart verandert.

De installatie van het certificaat is niet binnen het bereik van dit document.

Configuratie

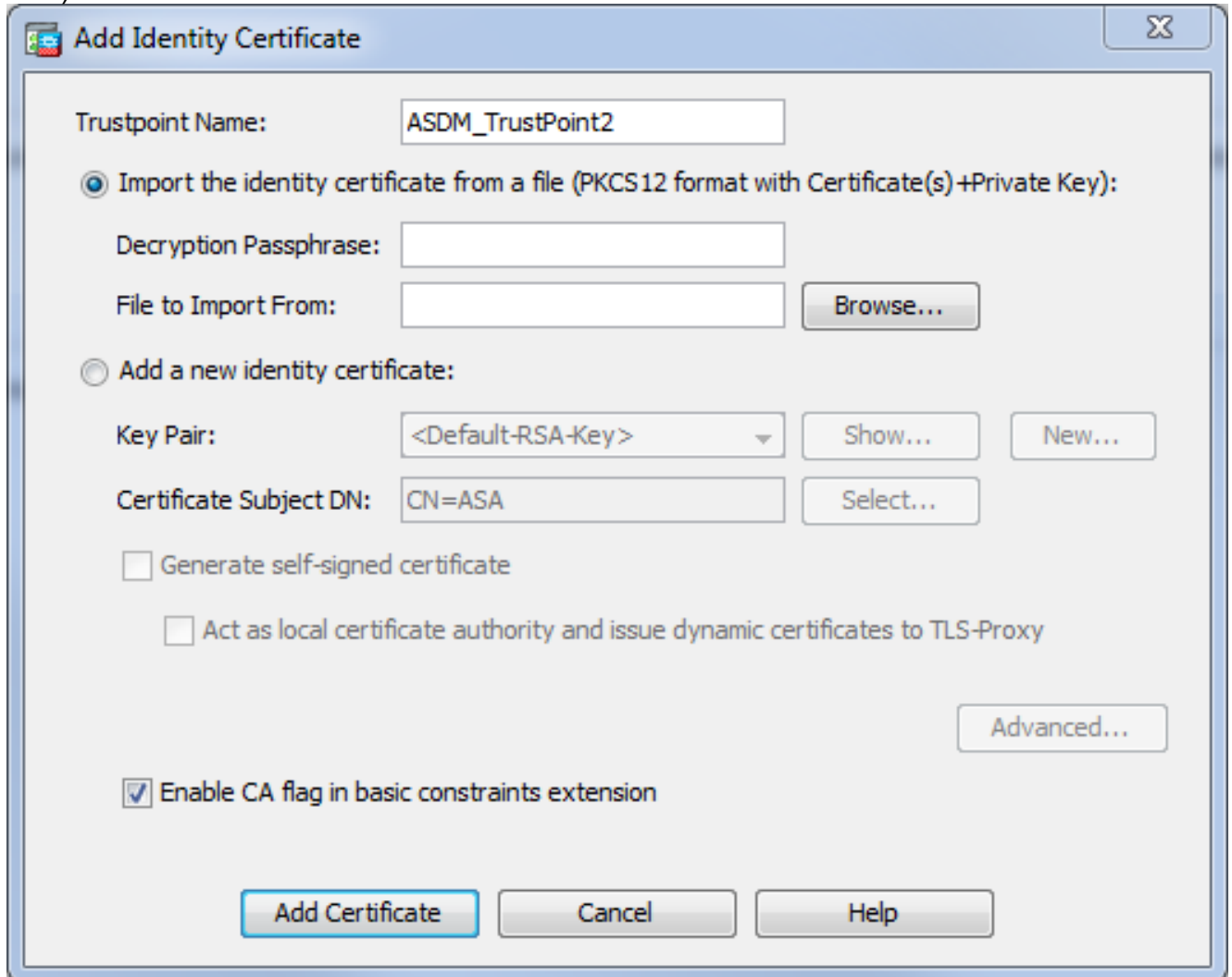
Configureer WebexVPN in de ASA met de volgende vijf belangrijke stappen:

- Configureer het certificaat dat door de ASA zal worden gebruikt.
- Schakel WebVPN in op een ASA-interface.
- Maak een lijst met servers en/of Unified Resource Locator (URL) voor WebVPN-toegang.
- Maak een groepsbeleid voor WebVPN-gebruikers.
- Pas het nieuwe groepsbeleid op een Tunnelgroep toe.

Opmerking: In ASA releases later dan release 9.4 is het algoritme dat wordt gebruikt om SSL-ciften te kiezen gewijzigd (zie [Releaseopmerkingen voor de Cisco ASA-serie, 9.4\(x\)](#)). Als alleen elliptische bocht-enabled klanten worden gebruikt, is het veilig om elliptische bocht-privé-toets voor het certificaat te gebruiken. Anders moet de aangepaste cementsuite worden gebruikt om te voorkomen dat de ASA een zelf-ondertekend tijdelijk certificaat overlegt. U kunt de ASA configureren om alleen op RSA gebaseerde cifers te gebruiken met

het SSL-algoritme tlsv1.2 aangepast "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-SHA A:DES-CBC-SHA:RC4-SHA:RC4-MD5" opdracht

1. **Optie 1** - Importeer het certificaat met de PC12-bestand. Kies **Configuratie > Firewall > Geavanceerd > certificaatbeheer > identiteitsbewijzen > Toevoegen**. U kunt het programma installeren met het PDF12-bestand of de inhoud ervan plakken in het PEM-formaat (Privacy Enhanced Mail).



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  
+vkvjUgCAggAgIIFuHFrV6enVf1Nv3sBBYB/yZswHELY5KpeALbXhfrFDpLNncAB  
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x30zo0JJxSAafmTWqDOEOS/  
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbilslie4Dplx1b
```

--- output ommited ---

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
MIIJUQIBAzCCRCGCSqGSIB3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIB3DQEH  
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIB3DQEMAQYwDgQI8F3N  
+vkvjUgCAggAgIIFuHFrV6enVflNv3sBBYB/yZswhELY5KpeALbXhfrFDpLNncAB  
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/  
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5sOhyuQGPhLJRdionbilslie4Dplx1b
```

quit

INFO: Import PKCS12 operation completed successfully

Optie 2 - Maak een zelfondertekend certificaat. Kies **Configuratie > Firewall > Geavanceerd > certificaatbeheer > identiteitsbewijzen > Toevoegen**. Klik op de knop **Een nieuw identiteitsbewijs** toevoegen. Controleer het **vakje** voor **eigen certificaat genereren**. Kies een gezamenlijke naam (CN) die aan domeinnaam van de ASA overeenkomt.

Add Identity Certificate

Trustpoint Name:

Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

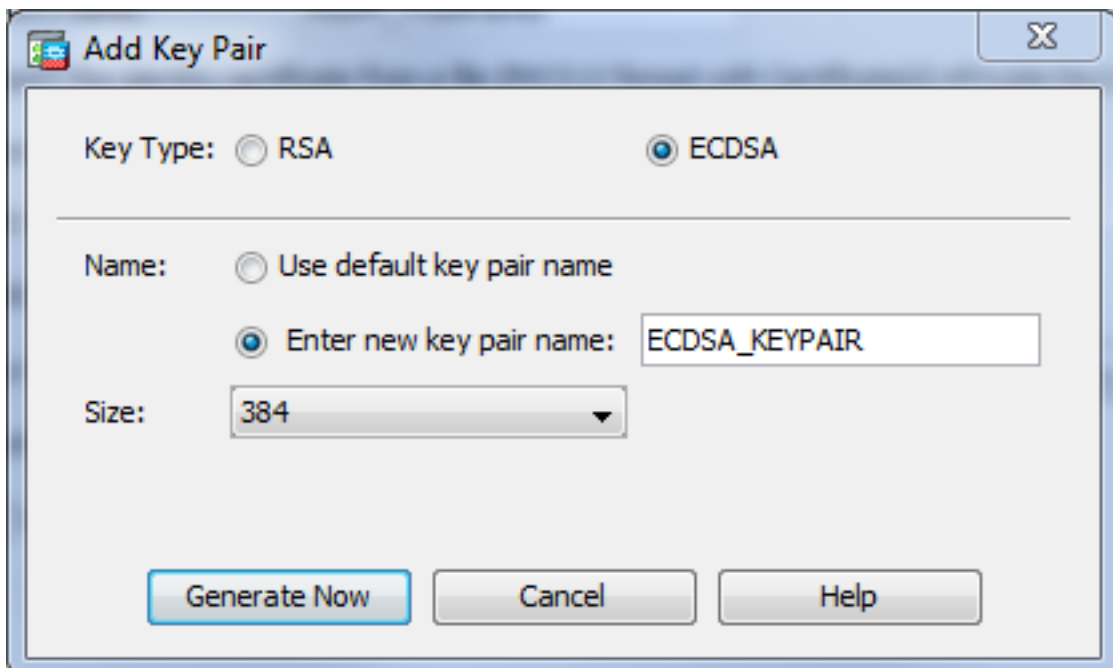
Certificate Subject DN:

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Enable CA flag in basic constraints extension

Klik op **Nieuw** om de toetsencombinatie voor het certificaat te maken. Kies het sleuteltype, de naam en de



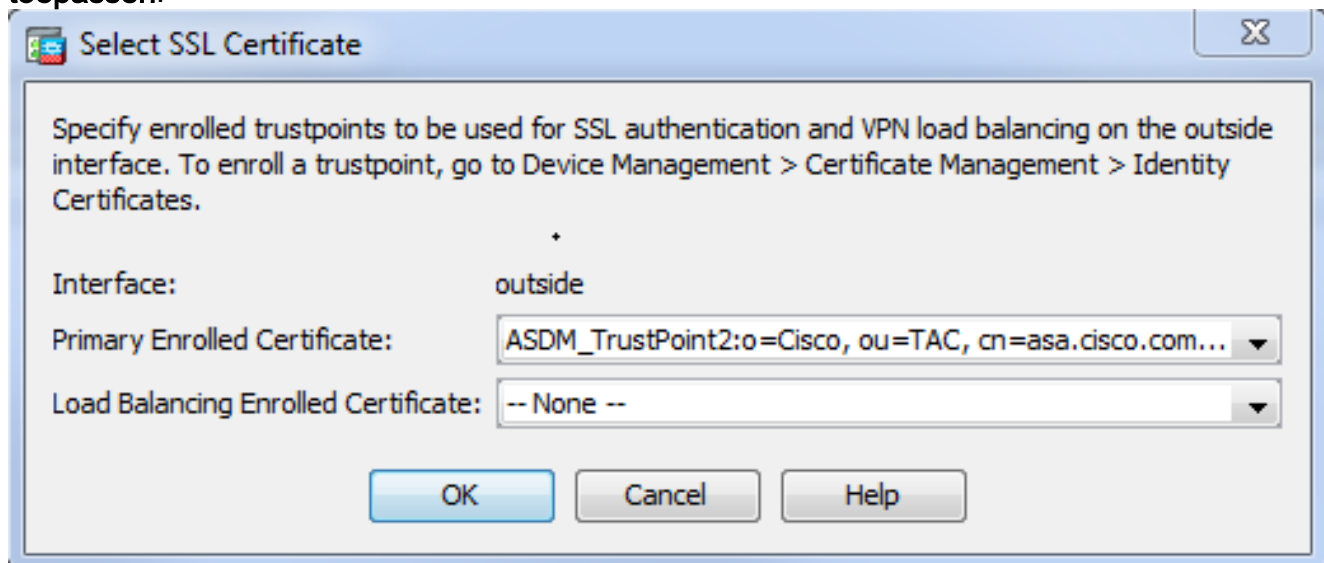
grootte.

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. Kies het certificaat dat wordt gebruikt om WebVPN-verbindingen te dienen. Kies **Configuration > Remote Access VPN > Advanced > SSL-instellingen**. Kies in het menu Certificaten het vertrouwen dat aan het gewenste certificaat voor de externe interface is gekoppeld. Klik op **toepassen**.



Equivalente CLI-configuratie:

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

3. (Optioneel) Schakel DNS-raadpleging (Domain Name Server) in. WebVPN server werkt als een proxy voor clientverbindingen. Het betekent dat de ASA verbindingen met de middelen creëert voor de cliënt. Als de klanten verbindingen met de middelen nodig hebben die domeinnamen gebruiken, dan moet de ASA de DNS raadpleging uitvoeren. Kies **Configuration > Remote Access VPN > DNS**. Configuratie van minstens één DNS server en laat DNS raadpleging op de interface toe die met de DNS server te maken

Configuration > Remote Access VPN > DNS

Specify how to resolve DNS requests.

DNS Setup

Configure one DNS server group Configure multiple DNS server groups

Primary DNS Server:

Secondary Servers:

Domain Name:

heeft.

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
inside	True
outside	False

DNS Guard

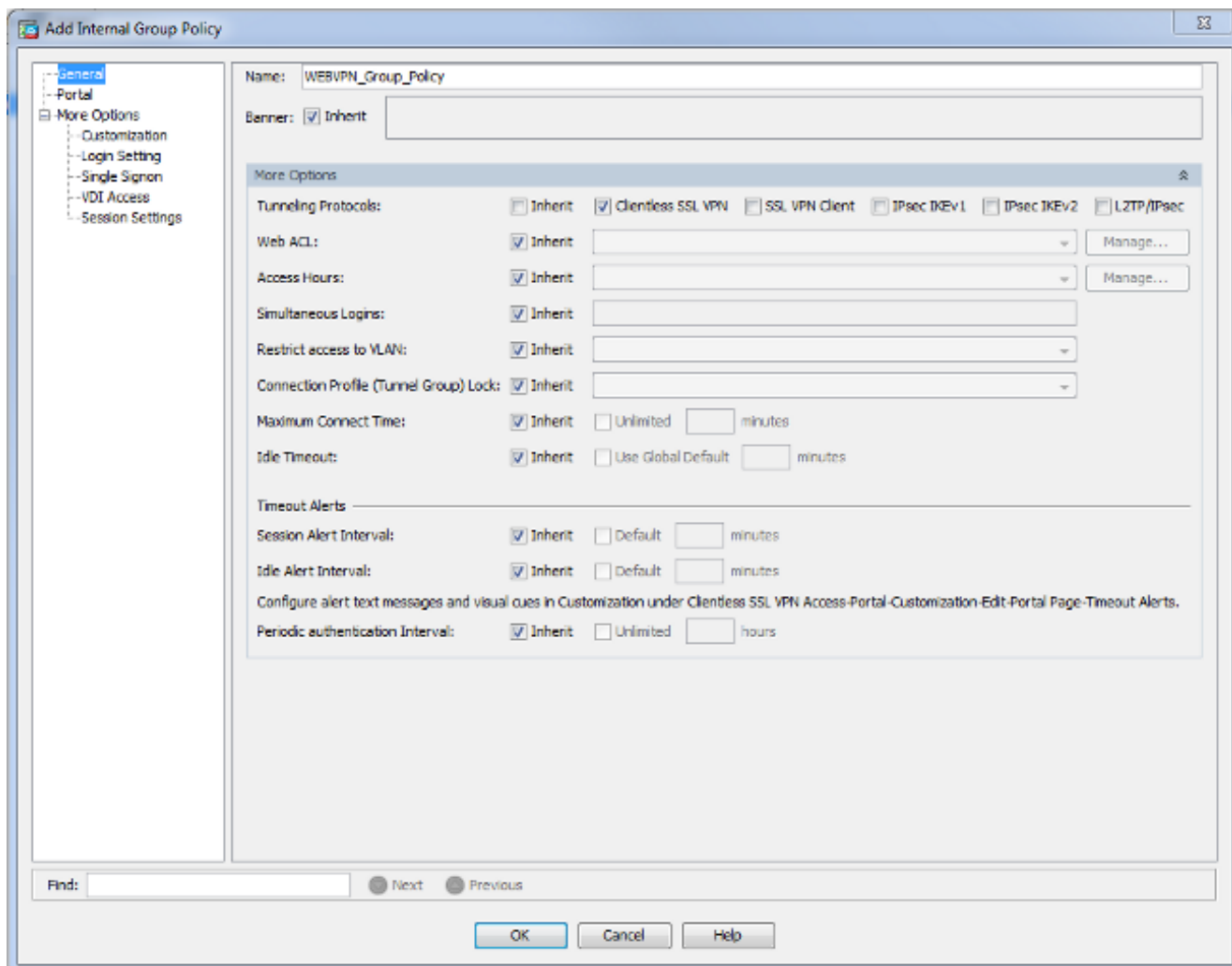
This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.

Enable DNS Guard on all interfaces.

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. (Optioneel) Maak groepsbeleid voor WEBVPN-verbindingen. Kies **Configuration > Remote Access VPN > Clientloze SSL VPN-toegang > Groepsbeleid > Intern groepsbeleid toevoegen**. Wijzig onder General Opties de waarde van de Tunelling Protocols in "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. Configuratie van het verbindingsprofiel. Kies in ASDM de optie **Configuration > Remote Access VPN > Clientloze SSL VPN Access > Connection-profielen**.

Voor een overzicht van de verbindingsprofielen en het groepsbeleid, raadpleeg [Cisco ASA Series VPN CLI Configuration Guide, 9.4 - Connection Profiles, Group Policy en Gebruikers](#). Standaard gebruiken de WebVPN-verbindingen het profiel DefaultWEBVPN. U kunt extra profielen maken. Opmerking: Er zijn verschillende manieren om gebruikers aan andere profielen toe te wijzen.

- Gebruikers kunnen het verbindingsprofiel handmatig selecteren in de vervolgkeuzelijst of met een specifieke URL. Zie [ASA 8.x: Sta gebruikers toe om een Groep bij Login WebVPN te selecteren via Groep-alias en Groep-URL Methode](#).

- Wanneer u een LDAP-server gebruikt, kunt u het gebruikersprofiel toewijzen op basis van de eigenschappen die van de LDAP-server worden ontvangen, zie [ASA Use of LDAP Attribution Maps Configuration Voorbeeld](#).

- Wanneer u op certificaat gebaseerde verificatie van de clients gebruikt, kunt u de gebruiker in kaart brengen naar de profielen op basis van de velden in het certificaat, zie [Cisco ASA Series VPN CLI Configuration Guide 9.4 - certificaatgroep configureren voor IKEv1](#).

- Zie [Cisco ASA Series VPN CLI Configuration Guide, 9.4 - Eigenschappen voor individuele gebruikers configureren](#) om de gebruikers handmatig aan het groepsbeleid toe te wijzen. Bewerk het profiel DefaultWEBVT groepsprofiel en kies WEBVPN_Group_Policy onder Standaardgroepsbeleid.

The screenshot shows the configuration window for a Clientless SSL VPN Connection Profile named 'DefaultWEBVPNGroup'. The window is split into 'Basic' and 'Advanced' sections. The 'Advanced' section is currently selected and contains the following settings:

- Name:** DefaultWEBVPNGroup
- Aliases:** (empty field)
- Authentication:**
 - Method: AAA Certificate Both
 - AAA Server Group: LOCAL (with a 'Manage...' button)
 - Use LOCAL if Server Group fails
- DNS:**
 - Server Group: DefaultDNS (with a 'Manage...' button)
 - (Following fields are attributes of the DNS server group selected above.)
 - Servers: 10.21.22.101
 - Domain Name: disco.com
- Default Group Policy:**
 - Group Policy: WEBVPN_Group_Policy (with a 'Manage...' button)
 - (Following field is an attribute of the group policy selected above.)
 - Enable clientless SSL VPN protocol

At the bottom of the window, there is a 'Find:' search box, 'Next' and 'Previous' navigation buttons, and 'OK', 'Cancel', and 'Help' action buttons.

CLI:

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

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

6. Kies **Configuration > Remote Access VPN-toegang > Clientloze SSL VPN Access > Connection-profielen** om WebVPN op de externe interface in te schakelen. Controleer het selectieteken **Toegang toestaan** naast de externe interface.

Access Interfaces

Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

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

Device Certificate ...

Port Setting ...

CLI:

```
ASA(config)# webvpn
```

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

7. (Optioneel) Maak bladwijzers voor inhoud. Bladwijzers staan de gebruiker toe om eenvoudig de interne bronnen te bladeren zonder de URL's te onthouden. Kies **Configuration > Remote Access VPN > Clientloze SSL VPN Access > Portal > Bookmarks > Add** om een favoriet te maken.

Add Bookmark List

Bookmark List Name:

Bookmark Title	URL
----------------	-----

Add

Edit

Delete

Move Up

Move Down

Find: Match Case

OK Cancel Help

Kies **Toevoegen** om een specifieke favoriet toe te voegen.

Bookmark Title: Example bookmark

URL: http :// www.cisco.com AssistantL...

Preload Page (Optional)

Preload URL: http ://

Wait Time: (seconds)

Other Settings (Optional)

Subtitle:

Thumbnail: -- None -- Manage

Place this bookmark on the VPN home page

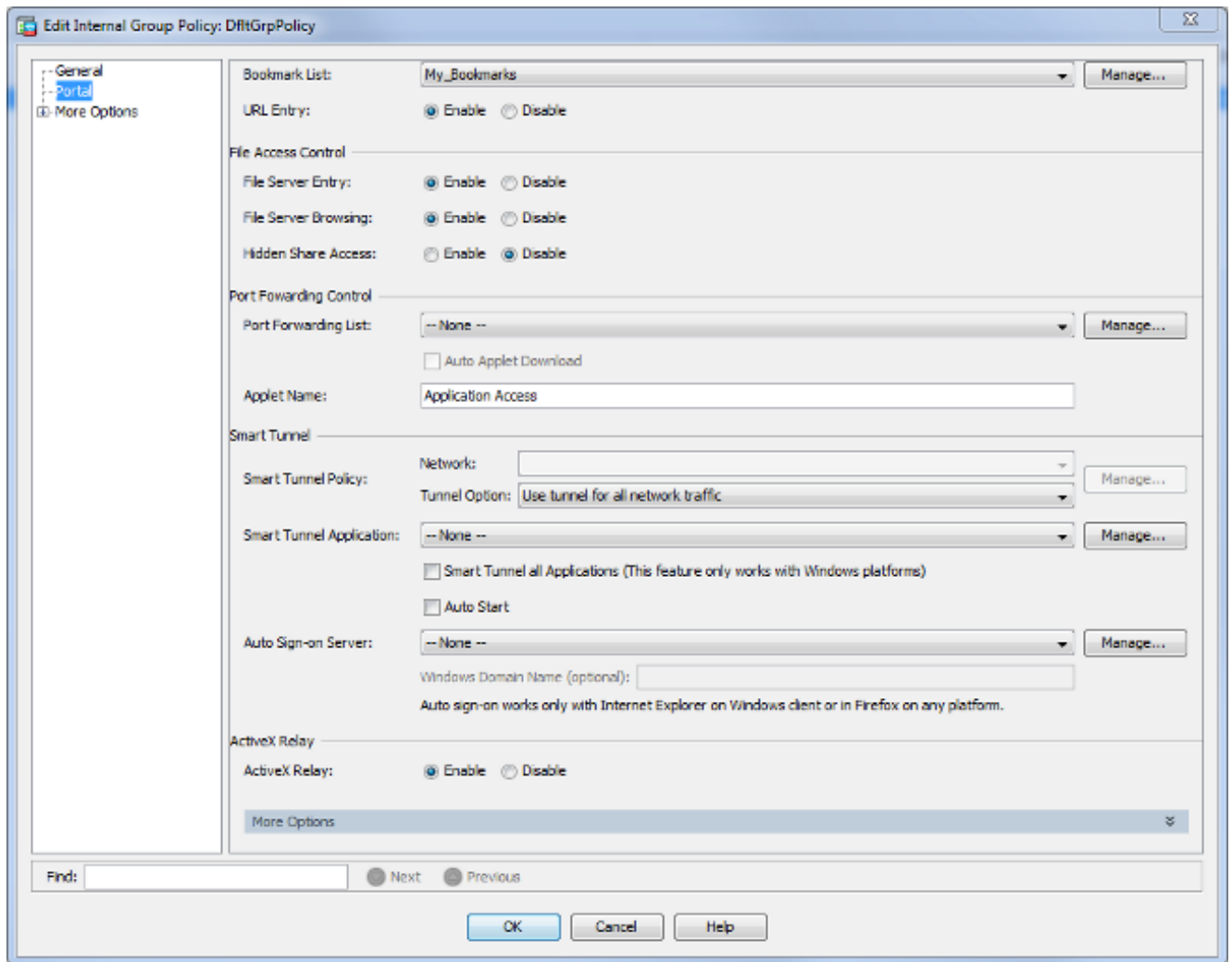
Enable Smart Tunnel

Advanced Options

OK Cancel Help

CLI: Het is onmogelijk om favorieten te maken via CLI omdat ze als XML bestanden worden gemaakt.

8. (Optioneel) Benoeming van bladwijzers aan een specifiek groepsbeleid. Kies **Configuration > Remote Access VPN > Clientloze SSL VPN-toegang > Groepsbeleid > Bewerken > Portal > Bookmark-lijst**.

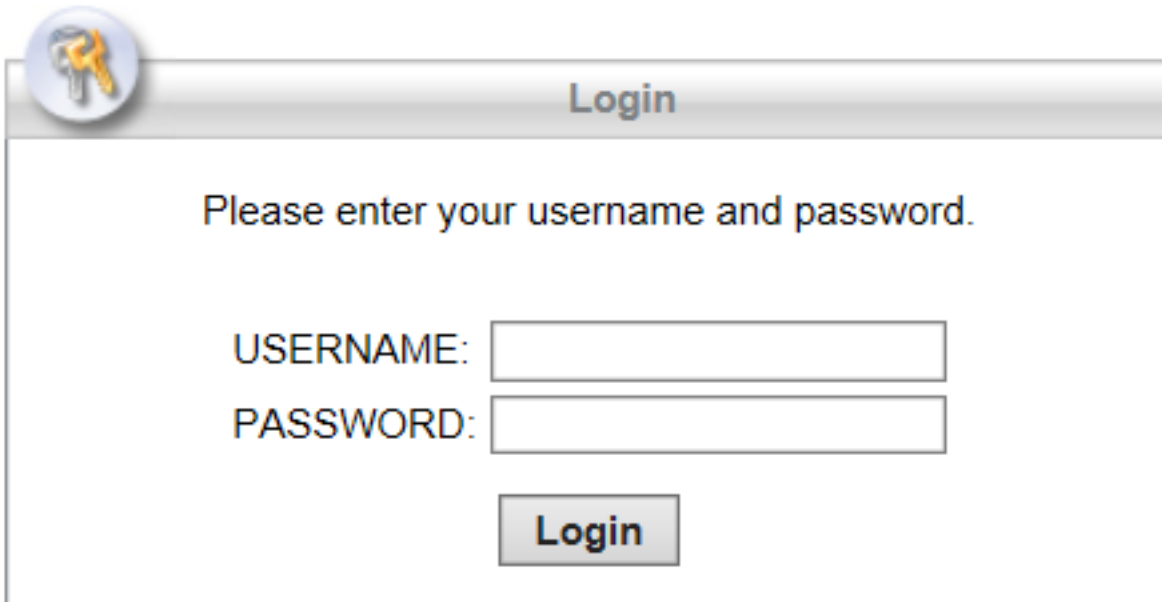


CLI:

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

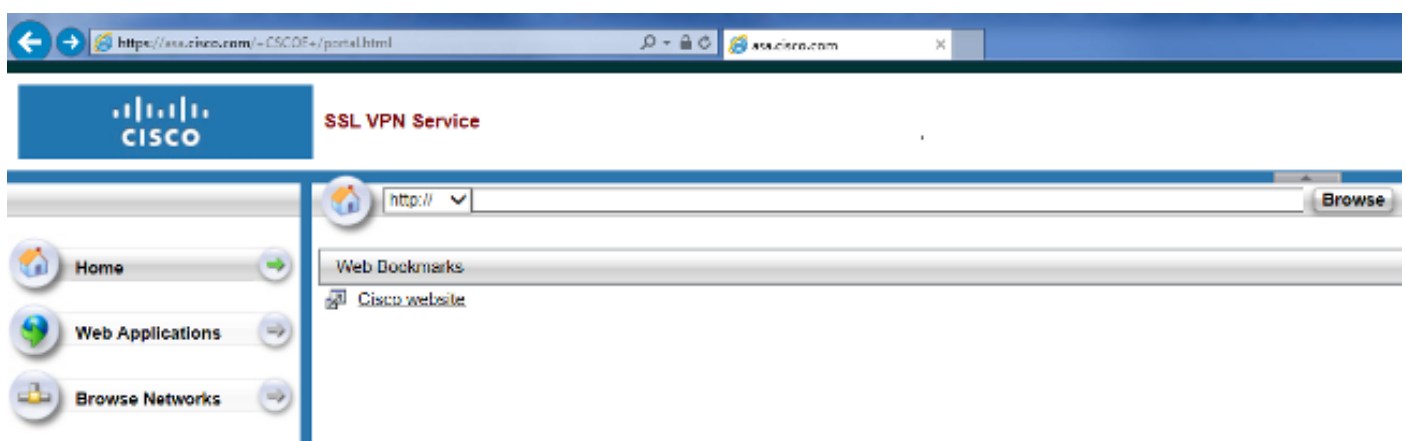
Verifiëren

Zodra WebVPN is geconfigureerd gebruikt u het adres `https://<FQDN van de ASA>` in de browser.



A login dialog box with a title bar containing a key icon and the word "Login". The main area contains the text "Please enter your username and password." followed by two input fields labeled "USERNAME:" and "PASSWORD:". Below the fields is a "Login" button.

Nadat u hebt gelogd, kunt u de adresbalk zien die wordt gebruikt om naar websites en de bladwijzers te navigeren.



Problemen oplossen

Procedures voor probleemoplossing

Volg deze instructies om uw configuratie problemen op te lossen.

Kies in ASDM de optie **Monitoring > Vastlegging > Realtime logvenster > View**. Wanneer een cliënt zich verbindt met de ASA, noteer de instelling van de TLS sessie, selectie van groepsbeleid en succesvolle authenticatie van de gebruiker.

```

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

```

Kies in ASDM Monitoring > VPN > VPN Statistieken > Sessies > Filter door: Clientloze SSL VPN. Zoek de nieuwe WebVPN sessie. Kies het WebVPN-filter en klik op Filter. Als er een probleem optreedt, passeert u tijdelijk het ASA-apparaat om ervoor te zorgen dat klanten toegang hebben tot de gewenste netwerkbronnen. Bekijk de configuratiestappen in dit document.

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Cer Auth Int	Cer Auth Left
admin 10.229.20.77	WEBVPN_Group_Policy DefaultWEBVPNGroup	Clientless Clientless: (1)AES128	10:40:04 UTC Tue May 26 2015 0h:02m:50s	63991 166375		

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

```

Opdrachten gebruikt voor probleemoplossing

Het [Uitvoer Tolk \(uitsluitend geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten.

Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg [Important Information on Debug Commands \(Belangrijke informatie over opdrachten met debug\) voordat u opdrachten met debug opgeeft.](#)

- **toon website** - Er zijn veel **show** opdrachten verbonden met WebVPN. Zie het [gedeelte](#) met de [opdrachtreferentie](#) van de Cisco security applicatie voor meer informatie over het gebruik van opdrachten in detail van de **show**.
- **debug webVPN** - Het gebruik van **debug**-opdrachten kan een negatieve invloed hebben op de ASA. Zie het [gedeelte](#) met de [opdracht](#) van de Cisco security applicatie om in detail het gebruik van debug-opdrachten te zien.

Vaak voorkomende problemen

Gebruiker kan niet inloggen

Probleem

Het bericht "Clientless (browser) SSL VPN toegang is niet toegestaan." verschijnt in de browser na een onsuccesvolle inlogpoging. De AnyConnect Premium-licentie is niet op de ASA geïnstalleerd of is niet in gebruik zoals wordt aangegeven door "Premium AnyConnect-licentie is niet op de ASA ingeschakeld."

Oplossing

Schakel de Premium AnyConnect-licentie in met deze opdrachten:

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

Probleem

Het bericht "Aanmelden mislukt" verschijnt in de browser na een onsuccesvolle inlogpoging. De AnyConnect-licentielimiet is overschreden.

Oplossing

Bekijk dit bericht in de weblogs:

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

Controleer ook uw licentielimiet:

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

Probleem

Het bericht "AnyConnect is niet ingeschakeld op de VPN-server" verschijnt in de browser na een

onsuccesvolle inlogpoging. Het clientloze VPN-protocol is niet ingeschakeld in het groepsbeleid.

Oplossing

Bekijk dit bericht in de weblogs:

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

Zorg ervoor dat het clientloze VPN-protocol is ingeschakeld voor het gewenste groepsbeleid:

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

Kan niet meer dan drie WebVPN-gebruikers aan de ASA verbinden

Probleem

Slechts drie WebVPN cliënten kunnen met de ASA verbinden. De verbinding voor de vierde client mislukt.

Oplossing

In de meeste gevallen houdt dit probleem verband met een instelling voor gelijktijdige inloggen binnen het groepsbeleid. Gebruik deze illustratie om het gewenste aantal gelijktijdige inloggen te configureren. In dit voorbeeld is de gewenste waarde 20.

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

Clients voor WebeVPN kunnen geen favorieten maken en worden afgevoerd

Probleem

Als deze bladwijzers zodanig zijn geconfigureerd dat gebruikers zich aan de clientloze VPN konden aanmelden, maar op het thuis scherm onder "Web Toepassingen" verschijnen ze in grijs waarden, hoe kan ik deze HTTP-links dan inschakelen zodat de gebruikers op ze kunnen klikken en in de specifieke URL kunnen gaan?

Oplossing

U dient er eerst voor te zorgen dat de ASA de websites via DNS kan oplossen. Probeer de websites onder de naam te pingelen. Als de ASA de naam niet kan oplossen, wordt de link grijs weergegeven. Als de DNS-servers intern op uw netwerk zijn, moet u de DNS-domeinlookup-privé-interface configureren.

Citrix Connection via WebVPN

Probleem

De foutmelding "de ICS-client heeft een beschadigd beeldbestand ontvangen." vindt plaats voor Citrix via WebVPN.

Oplossing

Als u de *beveiligde* gateway-modus gebruikt voor een Citrixverbinding via WebVPN, kan het ICA-bestand beschadigd raken. Omdat de ASA niet compatibel is met deze modus van de bediening, kunt u een nieuw ICA-bestand maken in de Direct Mode (niet-beveiligde modus).

Vermijd de noodzaak van een tweede verificatie voor de gebruikers

Probleem

Wanneer u CIFS-links opzoekt in het clientloze WebVPN-portaal, wordt u gevraagd om aanmeldingsgegevens nadat u op de favoriet klikt. Lichtgewicht Directory Access Protocol (LDAP) wordt gebruikt om zowel de bronnen als de gebruikers die al LDAP aanmeldingsgegevens hebben ingevoerd, voor de VPN-sessie echt te maken.

Oplossing

U kunt in dit geval de optie Automatisch signaleren gebruiken. Onder het specifieke groep-beleid dat en onder zijn eigenschappen WebVPN wordt gebruikt, moet u dit configureren:

```
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

```

waarin X.X.X=IP van de CIFS-server en *=rest van het pad om het betrokken bestand/de betreffende map te bereiken, wordt gebruikt.

Hier wordt een voorbeeld van de configuratie getoond:

```
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

```

Zie [SSO configureren met HTTP Basic of NTLM Verificatie](#) voor meer informatie [hierover](#).

Gerelateerde informatie

- [ASA: Smart Tunnel met ASDM-configuratievoorbeeld](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)