ASA met WebVPN en Single aanmelding bij gebruik van ASDM en NTLMv1 Configuration Voorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configureren Een AAA-server voor Windows-domeinverificatie toevoegen Een zelfondertekend certificaat maken WebexVPN op de externe interface inschakelen Een URL-lijst configureren voor uw interne server(s) Een intern groepsbeleid configureren Een tunnelgroep configureren Automatische handtekeningen voor een server configureren **Definitieve ASA-configuratie** Verifiëren Een WebVPN-aanmelding testen **Monitorsessies** WebVPN-sessie verwijderen Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u de Cisco adaptieve security applicatie (ASA) kunt configureren om automatisch inlogaanmeldingsgegevens van WebVPN aan servers door te geven, evenals secundaire verificatie, waarvoor extra inlogvalidatie nodig is tegen Windows Active Directory met NT LAN Manager versie 1 (NTLMv1). Deze optie staat bekend als single-sign-on (SSO). Het geeft links die voor een specifieke WebVPN-groep zijn ingesteld de mogelijkheid om deze gebruikersauthenticatie-informatie door te geven, waardoor meerdere authenticatie-aanwijzingen worden geëlimineerd. Deze optie kan ook worden gebruikt op het niveau van de wereldwijde configuratie of gebruikersconfiguratie.

Voorwaarden

Vereisten

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

• Verzeker u ervan dat NTLMv1 en Windows toegang voor de beoogde VPN-gebruikers zijn geconfigureerd. Raadpleeg uw Microsoft documentatie voor meer informatie over Windows-toegangsrechten.

Gebruikte componenten

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

- Cisco ASA 7.1(1)
- Cisco Adaptieve Security Devices Manager (ASDM) 5.1(2)
- Microsoft Internet Information Services (IS)

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

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

In deze sectie, wordt u voorgesteld met de informatie om de ASA als een WebVPN server met SSO te vormen.

Opmerking: Gebruik het <u>Opname Gereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Een AAA-server voor Windows-domeinverificatie toevoegen

Voltooi deze stappen om de ASA te configureren om een domeincontroller te gebruiken voor verificatie.

 Selecteer Configuration > Properties > AAA Setup > AAA servers en klik op Add. Typ een naam voor de servergroep, zoals Windows_NT, en kies NT Domain als protocol.

🚰 Claco ASDM 5	i.1 for ASA - 177.16.177.57		
Fia Rules Bea	arch Options Tools Wizards	: Hsip	
Haven C	antiquentian Manlader	CO CO Q CO	
- 1MIC (G	Configuration • Procedies • A	AA Debu > AAA Derena	
,	全点平 町山山和日	「御御殿」(
Intertabes	Grantup Witeard	AVA Servers	
<u>ii</u> ,	Have Setup	Server Groupe	
Bd.	Set Die Attitude Mar	Server Group Protocol Accounting Node Reactivation Node Add	
NAT	-Second	Edit	
27	Brei ARF - ⊒Auto Upcate	Deele	
VIN	B-Dertificate		
8	田 静Device Administration		
CSD Manugar	⊡ ©*OHCF Services - ⊒DNS Clent	Bewers in Selected Group	
Q .	- #Fallover	ServerName or IP Address Interface Timeout 7000	
- P3 	- BHistory Metrics	Edi	
Nouting	- 福田TP/HTTPS 単載 F Audit	Decle	
æ	ii al Logging L → Priorite Outpue		
Global Objects	- BSSL	20.48.000×1	
2	- SUNRPC Server	Ter total Abb Surray Group	
Properties	-⊗Timeoute -⊗URL Siterios	Configure à éé senser amun The Accounting Minde site Jude la prive	
		Apply Reset applicable for RACIUS and TACACS+ protocols.	
		loreco INA(16) 🔂 🖧 Server Group: Windows_NT	
		Protocol MT Domain	
		Azactuntag Kode 🔿 Smulaneuva - 🛞 Single	
		Reactivation Mode:	
		Dead Time 10 minutes	
		May Called Atlantation	
		Nasi aleu wempe. 17	
		DK Cancel Help	

 Voeg een Windows server toe.Selecteer de nieuwe groep en klik op Toevoegen. Selecteer de interface waar de server zich bevindt en voer de IP-adres en domeincontrolenaam in. Zorg ervoor dat de domeincontrolenaam in alle hoofdletters is ingevoerd. Klik op OK wanneer u klaar bent.

🚰 Cisco ASDM 🕈	5.1 for ASA	172.16.172.5	2							
Fie Rulas Sa	and, Options	Tools Wizard	is Help							
Gi Hone C	Configuration	[2] Monitoring	C) Deck	O Forward	Q Search Re	🚱 🛄 stresti Save	? Help	Cisco Sr	allu	
Interfaces Security Policy NAT	Contiguistion 9 2 T - 3 ³ Startu D AAA 5 - 38400 - 58400 - 584000 - 58400 - 584000 - 58400 - 584000 - 584000 - 584000 - 584000 - 5840	Properties Vizand etup A Servers th. Prompt WP Admbute Map poofing	AM Setu Co III S Setu Co	An Eeners Anvers Mer Groups enver Groups CAL recove_NT	Protocol LOCAL NT Doma	Accounting Mod	e Reactivation N	rode Add		
	한 중 ARP - 실Auto U - 월 Certifi - 월 Certifi - 월 영 Device - 한 양 Device	lodate cate 2 Access 2 Administration 4 Services	-80	ware in Solector	1 Group			Delete		
Rouding Global Objects	L SONS (Selection of the selection of t	Client er y Motrics HTTPS HTTPS bit ng y Queue IPC Server	8	erver Name or I	P Address	Interface	Timeout	Add Folt Foltate Move up biove down		
Properties	드 MTCP C 이 Timeo - 쨤URL P	actions ints itering				Apply	Rese Server G	A Server roup:	Windows_NT	
					cisco	NA (15)	Server N Timeout: NT Doma Server Doma	Name: sme or IP Address: ain Parameters Port: n Controller: OK	inside 10.1.1 200 10 138 ESC-81-7600 Cancel	seconds

Dit venster toont de voltooide AAAconfiguratie:



Een zelfondertekend certificaat maken

Voltooi deze stappen om de ASA te configureren om een zelfondertekend certificaat te gebruiken.

Opmerking: In dit voorbeeld wordt een zelfgetekend certificaat gebruikt voor eenvoud. Raadpleeg voor andere opties voor het invoeren van certificaten, zoals inschrijven bij een externe certificeringsinstantie, de <u>configuratie</u> van <u>certificaten</u>.

- 1. Selecteer Configuratie > Eigenschappen > Certificaat > Trustpunt > Configuratie en klik op Toevoegen.
- In het venster dat verschijnt typt u een Trustpoint Name zoals Local-TP en controleer Generate een zelfgetekend certificaat over inschrijving. Andere opties kunnen met hun standaardinstellingen worden gelaten. Klik op OK wanneer u klaar bent.



Dit venster toont de voltooide configuratie van het schaalpunt:



WebexVPN op de externe interface inschakelen

Voltooi deze stappen om gebruikers buiten uw netwerk toe te staan om verbinding te maken met WebVPN.

- 1. Selecteer Configuratie > VPN > WebVPN > WebVPN Access.
- 2. Selecteer de gewenste interface, klik op Enable en controleer de vervolgkeuzelijst voor tunnelgroep inschakelen op de weblogpagina van VPN.Opmerking: Als dezelfde interface wordt gebruikt voor WebVPN- en ASDM-toegang, moet u de standaardpoort voor ASDM-toegang van poort 80 naar een nieuwe poort zoals 8080 wijzigen. Dit gebeurt onder Configuratie > Eigenschappen > Apparaattoegang > HTTPS/ASDM.Opmerking: U kunt een gebruiker automatisch doorsturen naar poort 443 als een gebruiker navigeert naar http://<ip_adres> in plaats van https://<ip_adres>. Selecteer Configuratie > Eigenschappen > HTTP/HTTPS, kies de gewenste interface, klik op Bewerken en selecteer HTTP opnieuw richten naar HTTPS.

Cisco ASDM	5.1 for ASA - 172.16.171.51		
File Rules Se	arch Options Tools Wizards	Help	
in the second se	Configuration Monitoring	Sack Forward Search Refresh Save Help	STENS Allana
	Configuration > VPN > WebVPN	> WebVPN Access	
Ξ,	●金革 ■ 前 炎暭	8. 免 筋 ()	
Interfaces	(마 Material Proxy 📃	WebVPN Access	
<u>6</u>	General		
Security Policy	- B Client Update	Configure access parameters for WebVPN. (Note: The WebVPN features in this software release are currently provided as a free trial, and future major software releases will require the purchase and	6
24	Group Policy	installation of a WebVPN feature license.)	
NAT	- 💭 Tunnel Group		
13	- SIVPN System Opt	Interface WebVPN Enabled Enable	
<u>88</u>	E Address Manager	outside Yes Disable	
VPN	🕀 🥵 IPSec		- 1
<u> </u>			
CSD Manager			
۵.	-JAPCF		
IPS	- BCSD Setup	Port Number: 443	
4≩⊳	- Cache	Defaultiple Times de 1900	
Routing	- The Encoding	Default ldie Timeout: Tabu seconds	
(A)	- Sport Forwarding	Max. Sessions Limit: 2	
Clabel Objects	- Proxies	WebVPN Nemory Size: 50 % of Intel Integral memory	
Gibbal Objects	- 39 Proxy Bypass		
3	SSO Servers	Enable Tunnel Group Drop-down List on WebYPN Login Page	
Properties	Servers and URL		
	WebvPN Access	Apply Reset	
	<		
Configuration cha	anges saved successfully.	cisco 🛛 NA (15) 🛛 🛃 🖬 🔹 3/30/06 2:37:41 PM	UTC

Een URL-lijst configureren voor uw interne server(s)

Voltooi deze stappen om een lijst te maken die de servers bevat waarvoor u uw WebVPNgebruikers toegang wilt geven.

- 1. Selecteer Configuratie > VPN > WebVPN > servers en URL's en klik op Add.
- 2. Voer een naam in voor de URL-lijst. Deze naam is niet zichtbaar voor eindgebruikers. Klik op **Toevoegen**.
- 3. Voer de URL Display Name in zoals deze aan gebruikers moet worden weergegeven. Voer de URL-informatie van de server in. Dit zou moeten zijn hoe u normaal toegang tot de server heeft.



4. Klik op OK, OK, en Toepassen.



Een intern groepsbeleid configureren

Voltooi deze stappen om een groepsbeleid voor uw gebruikers van WebVPN te configureren.

- 1. Selecteer Configuratie > VPN > Algemeen > Groepsbeleid, klik op Toevoegen en selecteer Intern groepsbeleid.
- Specificeer op het tabblad General een beleidsnaam, zoals Interne-Group_POL_WEBVPN. Schakel de inloop vervolgens naast de tunneling-protocollen uit en controleer WebVPN.

🖆 Add Internal Group Policy 🛛 🛛 🔀					
Name: mal-GRP_POL_WEBVPN					
General IPSec Client Configuration Cl	ient Firewall Hardware Client WebVPN				
Check an Inherit checkbox to let the corre	esponding setting take its value from the default group policy.				
Tunneling Protocols: 📃 Inherit	IPSec VebVPN				
Filter: 🔽 Inherit	Manage				
Connection Settings					
Access Hours: 🗹 Inherit	Vew				
Simultaneous Logins: 🔽 Inherit					
Maximum Connect Time: 🗹 Inherit	Unlimited minutes				
Idle Timeout: 🗹 Inherit	Unlimited minutes				
Servers					
DNS Servers: 🔽 Inherit	Primary: Secondary:				
WINS Servers: 🔽 Inherit	Primary: Secondary:				
DHCP Scope: 🔽 Inherit					
OK	Cancel Help				

3. Selecteer in het tabblad WebVPN het tabblad **Overige** subtabblad. Schakel de **opdracht** naast servers en URL-lijsten uit en selecteer de URL-lijst die u hebt ingesteld in de vervolgkeuzelijst. Klik op **OK** wanneer u klaar bent.

🖆 Add Internal Group Policy
Name: mal-GRP_POL_WEBVPN
General IPSec Client Configuration Client Firewall Hardware Client WebVPN
Configure WebVPN attributes using the following tabs .
Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.
Functions Content Filtering Homepage Port Forwarding Other SSL VPN Client
Servers and URL Lists: Inherit webserver Vebserver
Web-Type ACL ID: Veb-Type ACL ID: Veb-Ty
SSO Server: Inherit New
HTTP Compression: 🗹 Inherit 🔷 Enable 🔷 Disable
Keepalive Ignore
Specify upper limit of the HTTP/HTTPS traffic, per transaction to ignore.
Transaction Size: Inherit KB
Deny Message
✓ Inherit
OK Cancel Help

Een tunnelgroep configureren

Voltooi deze stappen om een Tunnelgroep voor uw WebVPN-gebruikers te configureren.

 Selecteer Configuration > VPN > General > Tunnel Group, klik op Add en selecteer WebeVPN Access...



2. Voer een naam in voor de Tunnelgroep, zoals WEB_VPN-GRP. Selecteer in het tabblad Basic het groepsbeleid dat u hebt gemaakt en controleer of het groepstype **webvpn** is.

📧 Edit Tunnel Group 🛛 🔀
Name: WEB_VPN-GRP Type: webvpn
General WebVPN
Configure general access attributes from the following sub-tabs.
Basic AAA Client Address Assignment Advanced
Group Policy: Internal-GRP_POL Internal-GRP_POL_WEBV DiftGrpPolicy Strip the realm from username before passing it on to the AAA server Strip the group from username before passing it on to the AAA server
OK Cancel Help

3. Ga naar het tabblad AAA.Voor de Groep van de Verificatieserver, kies de groep die u hebt ingesteld om NTLMv1-verificatie met uw domeincontroller mogelijk te maken.Optioneel: Controleer LOKAAL als de servergroep er niet in slaagt het gebruik van de LOKALE gebruikersdatabase in te schakelen voor het geval de geconfigureerde AAA-groep niet werkt. Dit kan u helpen bij het oplossen van problemen op een later tijdstip.

Name: WEB_VPN-GRP Type: webvpn General WebVPN Configure general access attributes from the following sub-tabs. Racis AAA Client Address Assignment Advanced					
General WebVPN Configure general access attributes from the following sub-tabs.					
Configure general access attributes from the following sub-tabs.					
Pacia AAA Client Address Assignment Advanced					
Dasit om Client Audiess Assignment Auvanceu					
To set authentication server aroun per interface, go to the Advanced tab					
Authentication Server Group:					
Use LOCAL if Server Gra None					
Authorization Server Group:					
Users must exist in the authorization database to connect					
Accounting Server Group: None 💙					
Authorization Settings					
 Use the entire DN as the username 					
 Specify individual DN fields as the username 					
Primary DN Field: CN (Common Name)					
Secondary DN Field: OU (Organization Unit)					
-Password Management					
Override account-disabled indication from AAA server					
Enable notification upon password expiration to allow user to change password					
Enable notification prior to expiration Notify days prior to expiration					
OK Cancel Help					

- 4. Ga naar het tabblad WebVPN en ga vervolgens naar het subtabblad Group Aliases en URLs.
- Voer een alias in onder Group Aliases en klik op Add. Deze alias verschijnt in de vervolgkeuzelijst die bij inloggen aan WebVPN-gebruikers wordt gepresenteerd.

🖆 Edit Tunnel Group	X
Name: WEB_VPN-GRP Type: webvpn	
General WebVPN	
Configure WebVPN access attributes from the following sub-tabs.	
Basic NetBIOS Servers Oroup Anases and ORLs Web Page	٦
Alias Status	
Alias: Add >> Group-Selection enable	
<< Remove	
✓ Enable	
Group URLs	
URL (http or https): Add >>	
<< Remove	
✓ Enable	
OK Cancel Help	

6. Klik op OK en vervolgens op Toepassen.

Automatische handtekeningen voor een server configureren

Schakelt over naar de opdrachtregel zodat de BF beschikbaar is voor uw interne server(s).

Opmerking: deze stap kan niet in de ASDM-indeling worden voltooid en moet met de opdrachtregel worden voltooid. Raadpleeg <u>De opdrachtregel-interface gebruiken</u> voor meer informatie.

Gebruik de opdracht **automatisch** verzenden om de netwerkbron op te geven, zoals een server, waartoe u de gebruikers toegang wilt geven. Er wordt hier één IP-adres voor de server ingesteld, maar er kan ook een netwerkbereik worden opgegeven zoals **10.1.1.0/24**. Raadpleeg de opdracht <u>automatisch tekenen</u> voor meer informatie.

```
ASA>enable
ASA#configure terminal
ASA(config)#webvpn
ASA(config-webpvn)#auto-signon allow ip 10.1.1.200 255.255.255.255 auth-type ntlm
ASA(config-webvpn)#quit
ASA(config)#exit
ASA#write memory
```

In deze voorbeelduitvoer wordt de **auto-signaalopdracht** mondiaal ingesteld voor WebVPN. Deze opdracht kan ook worden gebruikt in de configuratiemodus van de WebVPN-groep of in de modus voor de gebruikersnaam van Webex. Het gebruik van deze opdracht in de WebVPN groepsconfiguratie modus beperkt het tot een bepaalde groep. Vergelijkbaar beperkt het gebruik van deze opdracht in de gebruikersnaam voor de configuratie van WebVPN deze tot een individuele gebruiker. Raadpleeg de opdracht <u>automatisch tekenen</u> voor meer informatie.

Definitieve ASA-configuratie

Dit document gebruikt deze configuratie:

```
ASA versie 7.1(1)
ASA# show running-config
: Saved
ASA Version 7.1(1)
terminal width 200
hostname ASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.171.51 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
1
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
1
interface Management0/0
shutdown
no nameif
no security-level
no ip address
```

passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-group DefaultDNS domain-name cisco.com pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image disk0:/asdm512.bin no asdm history enable arp timeout 14400 route outside 0.0.0.0 0.0.0.0 172.16.171.1 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute !--- AAA server configuration aaa-server Windows_NT protocol nt aaa-server Windows_NT host 10.1.1.200 ntauth-domain-controller ESC-SJ-7800 !--- Internal group policy configuration group-policy Internal-GRP_POL_WEBVPN internal group-policy Internal-GRP_POL_WEBVPN attributes vpn-tunnel-protocol webvpn webvpn url-list value webserver username cisco password Q/odgwmtmVIw4Dcm encrypted privilege 15 aaa authentication http console LOCAL aaa authentication ssh console LOCAL aaa authentication enable console LOCAL http server enable 8181 http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart !--- Trustpoint/certificate configuration crypto ca trustpoint Local-TP enrollment self crl configure crypto ca certificate chain Local-TP certificate 31 308201b0 30820119 a0030201 02020131 300d0609 2a864886 f70d0101 04050030 1e311c30 1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 1e170d30 36303333 30313334 3930345a 170d3136 30333237 31333439 30345a30 1e311c30 1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 819f300d 06092a86 4886f70d 01010105 0003818d 00308189 02818100 e47a29cd 56becf8d 99d6d919 47892f5a 1b8fc5c0 c7d01ea6 58f3bec4 a60b2025 03748d5b 1226b434 561e5507 5b45f30e 9d65a03f 30add0b5 81f6801a 766c9404 9cabcbde 44b221f9 b6d6dc18 496fe5bb 4983927f adabfb17 68b4d22c cddfa6c3 d8802efc ec3af7c7 749f0aa2 3ea2c7e3 776d6d1d 6ce5f748 e4cda3b7 4f007d4f 02030100 01300d06 092a8648 86f70d01 01040500 03818100 c6f87c61 534bb544 59746bdb 4e01680f 06a88a15 e3ed8929 19c6c522 05ec273d 3e37f540 f433fb38 7f75928e 1b1b6300 940b8dff 69eac16b af551d7f 286bc79c e6944e21 49bf15f3 c4ec82d8 8811b6de 775b0c57 e60a2700 fd6acc16 a77abee6 34cb0cad 81dfaf5a f544258d cc74fe2d 4c298076 294f843a edda3a0a 6e7f5b3c quit !--- Tunnel group configuration tunnel-group WEB_VPN-GRP type webvpn tunnel-group WEB_VPN-GRP general-attributes authentication-server-group Windows_NT default-grouppolicy Internal-GRP_POL_WEBVPN tunnel-group WEB_VPN-GRP webvpn-attributes group-alias Group-Selection enable telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspectiontraffic ! ! policy-map global_policy class inspection_default inspect dns maximum-length 512

inspect ftp inspect h323 h225 inspect h323 ras inspect			
netbios inspect rsh inspect rtsp inspect skinny inspect			
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect			
<pre>sip inspect xdmcp ! service-policy global_policy global</pre>			
! WebVPN Configuration webvpn enable outside url-list			
webserver "Internal Server" https://10.1.1.200 1 tunnel-			
group-list enable auto-signon allow ip 10.1.1.200			
255.255.255.255 auth-type ntlm			
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6			
: end			

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Een WebVPN-aanmelding testen

Meld u aan als gebruiker om de configuratie te testen.

1. Probeer met gebruikersinformatie uit uw NT-domein in te loggen op de ASA. Selecteer de groepsalias die in stap 5 is geconfigureerd onder <u>Configuratie van een</u>

Tunnelgroep.	
WebVPN Service - Microsoft Internet Explorer	
Ele Edit View Figurates Icols Help	a da kana da kana a 🖉 🖉
😋 Back 🔹 🐑 💌 😰 🏠 🔎 Search 🤸 Favorites 🤣 😒 - 🌺 🔜 🦓	
Address 🕘 https://172.16.171.51/+webvpr+/index.html	💙 ラ Go Unks 🎽
CISCO STATENS 	
Login	
Please enter your usemame and password.	
USERNAME: test	
PASSWORD:	
GROUP: Group-Selection	
Login Clear	
	2
a Done	🔒 🤨 Internet

2. Zoek de link(s) die is (zijn) ingesteld op de interne server(s). Klik op de link om het te controleren.

🗃 WebVPN Service - Microsoft Internet Explorer 📃 🗖 🔀					
Elle Edit Yew Favorites Iools Help		N			
🔾 Back = 🛞 - 💌 🖻 🏠 🏑	🔎 Search 🤺 Favorites 🚱 🔗 - 🌺 🥽 🖏				
Address 🕘 https://172.16.171.51/+webvpn+/	+/portal.html 🔽 🄁 Go	Links *			
S Pop-up blocked. To see this pop-up or addition	ional options dick here	×			
Cisco Systems antificant line - WebVPN Servi	vice	_			
	Click here to open the Floating Toolbar				
WEB APPLICATIONS	Web Bookmarks				
Enter Web Address (URL)	Internal Server				
Go					
Web Bookmarks 🛛 👻					
iavascript:top.doWebUrl("https://10.1.1.200")	7) 🔂 😫 🕲 Internet				

Monitorsessies

Selecteer **Monitoring > VPN > VPN Statistieken > Sessies** en kijk naar een WebVPN-sessie die behoort tot de groep die in dit document is ingesteld.

🖆 Cisco ASDM 5	.1 for ASA - 172.16.171.51	
File Rules Sea	arch Options Tools Wizards	s Help
G Home C	Sconfiguration Monitoring	Back Forward Search Refresh Save Help Cisco States
Hiterfaces	Monitoring > VPN > VPN Status VPN Connection Grapt PSec Tunnels WebVPN/SVC VPN Statistics Cluster Loads Chypto Statistics Compression Stat Compression Statistic Compression Statistics Protocol Statistics Sessions Sessions Statistics Statistics	Sessions Remote LAN-to-LAN WebVPN SSL VPN Client E-mail Proxy Total Cumulative 0 0 1 0 0 1 3 Filter By: WebVPN - All Sessions Filter Filter Username Group Policy Protocol Login Ti Details IP Address Tunnel Group Encryption Duration Logout test Internal-GRP_POLWebVPN 15:03:36 UTC Thut Logout 171 99.89.116 VYEB_VPN-GRP3DES 0h 01m 18s Ping To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu. Logout Sessions Logout By: - All Sessions Logout Sessions Refresh Last Updated: 3/30/06 2:31:30 PM
Data Refreshed S	uccessfully.	CISCO MA (15) 🔛 📷 🚱 🔄 3/30/06/3/05/21 PM UTC

WebVPN-sessie verwijderen

Deze uitvoer is een voorbeeld van het debug van een succesvolle WebVPN-sessie.

Opmerking: Raadpleeg <u>Belangrijke informatie over debug Commands</u> voordat u **debug**opdrachten gebruikt.

```
ASA#debug webvpn 255
INFO: debug webvpn enabled at level 255
ASA#
ASA# webvpn_portal.c:ewaFormServe_webvpn_login[1570]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286]
WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782]
!--- Begin AAA WebVPN: calling AAA with ewsContext (78986968) and nh (78960800)! WebVPN: started
user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422]
WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095]
WebVPN: user: (test) authenticated.
!--- End AAA webvpn_auth.c:http_webvpn_auth_accept[2093]
webvpn_session.c:http_webvpn_create_session[159] webvpn_session.c:http_webvpn_find_session[136]
```

WebVPN session created!

```
webvpn_session.c:http_webvpn_find_session[136]
webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202]
traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421]
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
!--- Output supressed webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn auth.c:webvpn auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

- Als het vervolgkeuzevenster Group niet aanwezig is op de inlogpagina van WebVPN, zorg er dan voor dat u stap 2 hebt voltooid onder <u>WebeVPN inschakelen op de buiteninterface</u> en stap 5 onder <u>Een tunnelgroep configureren</u>. Als deze stappen niet zijn voltooid en de uitrollijst ontbreekt, valt de authenticatie onder de Standaardgroep en zal deze waarschijnlijk mislukken.
- Alhoewel u geen toegangsrechten aan de gebruiker in ASDM of op de ASA kunt toewijzen, kunt u gebruikers met Microsoft Windows toegangsrechten op uw domeincontroller beperken. Voeg de benodigde NT groepsrechten toe voor de webpagina waaraan de gebruiker echt verklaart. Zodra de gebruiker zich in Webex met de rechten van de groep inlogt, wordt de toegang tot de opgegeven pagina's dienovereenkomstig verleend of ontkend. De ASA treedt alleen op als proxy-authenticatie host namens de domeincontroller en alle communicatie hier is NTLMv1.
- U kunt SSO voor Sharepoint via WebVPN niet configureren omdat de Sharepoint Server geen op formulieren gebaseerde verificatie ondersteunt. Als gevolg daarvan zijn de bladwijzers met de post of de post-plug-procedure hier niet van toepassing.

Gerelateerde informatie

- <u>Cisco ASA 5500 Series adaptieve security applicaties</u>
- Technische ondersteuning en documentatie Cisco Systems