ASA mit WebVPN und Single Sign-On mit ASDM und NTLMv1 Konfigurationsbeispiel

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Hinzufügen eines AAA-Servers für die Windows-Domänenauthentifizierung Erstellen eines selbstsignierten Zertifikats Aktivieren von WebVPN auf der externen Schnittstelle Konfigurieren einer URL-Liste für Ihre internen Server Konfigurieren einer Richtlinie für interne Gruppen Konfiguration einer Tunnelgruppe Konfigurieren der automatischen Anmeldung für einen Server Endqültige ASA-Konfiguration Überprüfen Testen einer WebVPN-Anmeldung Überwachungssitzungen Debuggen einer WebVPN-Sitzung Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie die Cisco Adaptive Security Appliance (ASA) so konfiguriert wird, dass sie WebVPN-Benutzeranmeldeinformationen sowie sekundäre Authentifizierung automatisch an Server übergibt, die eine zusätzliche Anmeldevalidierung für Windows Active Directory mit NT LAN Manager Version 1 (NTLMv1) erfordern. Diese Funktion wird als Single-Sign-on (SSO) bezeichnet. Links, die für eine bestimmte WebVPN-Gruppe konfiguriert sind, können diese Benutzerauthentifizierungsinformationen weitergeben, sodass mehrere Authentifizierungsanforderungen wegfallen. Diese Funktion kann auch auf globaler Ebene oder auf Benutzerkonfigurationsebene verwendet werden.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

• Stellen Sie sicher, dass NTLMv1- und Windows-Berechtigungen für die Ziel-VPN-Benutzer konfiguriert sind. Weitere Informationen zu Windows-Domänenzugriffsrechten finden Sie in der Microsoft-Dokumentation.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA 7.1(1)
- Cisco Adaptive Security Device Manager (ASDM) 5.1(2)
- Microsoft Internetinformationsdienste (IIS)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt werden die Informationen zum Konfigurieren der ASA als WebVPN-Server mit SSO angezeigt.

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Hinzufügen eines AAA-Servers für die Windows-Domänenauthentifizierung

Führen Sie diese Schritte aus, um die ASA so zu konfigurieren, dass sie einen Domänen-Controller für die Authentifizierung verwendet.

 Wählen Sie Konfiguration > Eigenschaften > AAA-Setup > AAA-Server aus, und klicken Sie auf Hinzufügen. Geben Sie einen Namen für die Servergruppe an, z. B. Windows_NT, und wählen Sie NT Domain als Protokoll aus.

Giaco ASDM :	5.1 for ASA - 172.16.172.57		
Fie Rules Be	arch Options Tools Wizards	a Halp	
6	🍫 [2]	000 9 00 9	CISCO SYSTEMS
Home	Configuration Monitoring	Back Forward Search Refresh Save Help	- allowellow
Interfaces Interfaces Security Policy NAT SSD Manugar ISS National SSD Manugar ISS Mading ISS	Consigned for Proceedies - As Consigned for Proceedies - As Consigned for the set Consigned for the set Consig	A Satur > AAA Gervers A Satur > AAA Gervers A Satur > AAA Gervers Server Groups Server Group Protocol Accounting Node React-value CC44 LOCA4 Satur > Name or IP Address Interface Timeout	en Mode Add Edit Orrele X Add Edit Dekte Mixwaz
Global Objects	- SSL - SSL		
3	TCF Options		🖬 Add AAA Server Group
Properties	-장Timeouts - ው입URL Filtering	Apply Reset	Configure AAA server group. The Accounting Mode attribute is only applicable for RACIUE and TACAGE+ protocole.
		orsoc (NA(16) 🕼 🍰 📋	Server Group: Windows_NT
			Primol Primol
			Accounting Koda, O Smoltaneous @ Single
			React vation Mode: Depiction Timed
			Dead Time. 10 minutes
			Nac Failed Altempts: 3
			DK Cancel Help

2. Hinzufügen eines Windows-ServersWählen Sie die neu erstellte Gruppe aus, und klicken Sie auf Hinzufügen. Wählen Sie die Schnittstelle aus, in der sich der Server befindet, und geben Sie die IP-Adresse und den Domänen-Controller-Namen ein. Stellen Sie sicher, dass der Domänen-Controller-Name in allen Großbuchstaben eingegeben wird. Klicken Sie abschließend auf

OK.

🔂 Cisco ASDM !	5.1 for ASA	172.16.172.5									
Fie Rulas Se	and, Options	Tools Wizard	is Help								
in the second se	Sonfiguration	[2] Monitoring	Co Dack	Ecrward	Q Search Re	C 🔛	?		Cisco Srs	тель: (h	
interfaces Escurity Policy	Contiguration 용 쇼 푸 다양Startu 탄 음AAA 5 다 월 Au	Properties P Vitzard etup A Convers th. Prompt WP Attribute Map	AMA SI	AVA Bervers A Kall (2) Arvers er Groups mer Group Mu	Protocol	Accounting	lloole Read	Ination Mode	Add		
NAT VPN	ト 職 Anti-B 使 』 ARP 上 温 Auto U 単 配 Certifi 段 』 Device 段 愛 Device	poofing Jodate cate e Access e Administration		NGWS_NT	NT Doma	n		Depistion	Delete		
CSD Honoger	E PDHCF	^a Bervices Client Gr Hent y Metrics Hentrys Gr	Ser	ers in Selecter ner Name or If	Group Address	Interface	Tin	recut (Add Edit Dalate		
Gideal Objects	Priorit Priorita Priorita	ng y Queue IPC Server Options auto					-		Nime up kiewe dawa Test		
		ibering				Apply	Rese	Add AAA Serve Berver Group:	r	Windows_NT	
					¢isco	NA (15)	1 2 61	nlerface Name : Server Name or I Timeout: NT Domain Para Server Port Domain Contro	P Address: meters pter:	inside 10.1.1.200 10 139 ESC-&I-7600	seconds

In diesem Fenster wird die abgeschlossene AAA-Konfiguration angezeigt:



Erstellen eines selbstsignierten Zertifikats

Führen Sie diese Schritte aus, um die ASA für die Verwendung eines selbstsignierten Zertifikats zu konfigurieren.

Hinweis: In diesem Beispiel wird ein selbstsigniertes Zertifikat zur Vereinfachung verwendet. Weitere Registrierungsoptionen für Zertifikate, z. B. die Registrierung bei einer externen Zertifizierungsstelle, finden Sie unter <u>Konfigurieren von Zertifikaten</u>.

- 1. Wählen Sie Konfiguration > Eigenschaften > Zertifikat > Trustpoint > Konfiguration aus, und klicken Sie auf Hinzufügen.
- Geben Sie im sich öffnenden Fenster einen Trustpoint-Namen wie Local-TP ein, und aktivieren Sie bei der Registrierung die Option Generate a self-signed certificate (Eigenes Zertifikat generieren). Andere Optionen können mit ihren Standardeinstellungen belassen werden. Klicken Sie abschließend auf OK.



In diesem Fenster wird die abgeschlossene Trustpoint-Konfiguration angezeigt:



Aktivieren von WebVPN auf der externen Schnittstelle

Gehen Sie wie folgt vor, um Benutzern außerhalb Ihres Netzwerks die Verbindung über WebVPN zu ermöglichen.

- 1. Wählen Sie Konfiguration > VPN > WebVPN > WebVPN Access aus.
- 2. Wählen Sie die gewünschte Schnittstelle aus, klicken Sie auf Aktivieren, und aktivieren Sie auf der WebVPN-Anmeldeseite die Option Dropdown-Liste Tunnelgruppe aktivieren.Hinweis: Wenn dieselbe Schnittstelle für den WebVPN- und ASDM-Zugriff verwendet wird, müssen Sie den Standard-Port für den ASDM-Zugriff von Port 80 auf einen neuen Port wie 8080 ändern. Dies erfolgt unter Konfiguration > Eigenschaften > Gerätezugriff > HTTPS/ASDM.Hinweis: Sie können einen Benutzer automatisch an Port 443 umleiten, wenn ein Benutzer zu http://<ip_address> statt zu https://<ip_address> navigiert. Wählen Sie Konfiguration > Eigenschaften > Gerätezugriff > aus, klicken Sie auf Bearbeiten, und wählen Sie HTTP zu HTTPS umleiten aus.

🔂 Cisco ASDM 5.1 for ASA - 172.16.171.51					
File Rules Se	arch Options Tools Wizards	Help			
ổ Home	Configuration Montering	O O Q Q Q Q Cisco Systems Back Forward Search Refresh Save Help International formation			
	Configuration > VPN > WebVPN	> WebVPN Access			
Ξ,	●金革 ■ 前 る暭				
Interfaces	한 월E-mail Proxy 🔺	WebVPN Access			
<u>6</u> ,	General				
Security Policy	- Default Tunnel G	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			
24	Group Policy	installation of a WebVPN feature license.)			
NAT	- Tunnel Group				
13	HIVE System Opt	Interface WebVPN Enabled Enable			
<u>88</u>	E SpiP Address Manager	outside Yes Disable			
VPN	⊕ IBIPSec				
<u>6</u>	- Store Balancing				
CSD Manager	- ACLs				
<u>i</u>	JAPCE				
IPS	- ACSD Setup	Port Number: 443			
4 ≩¢		Defaultide Timeeud			
++⊚ Routing	- TEncoding	Seconds			
<u>e</u>	Port Forwarding	Max. Sessions Limit: 2			
Global Objects	- Proxies	WebVPN Memory Size: 50 % of total physical memory			
	-33SL VPN Client				
20	SSO Servers	Enable Tunnel Group Drop-down List on WebYPN Login Page			
Properties	- Servers and URL				
	Webpage Custor -	Apply Reset			
Configuration cha	anges saved successfully.	cisco 🛛 NA (15) 🛛 😹 🔂 🔹 3/30/06 2:37:41 PM UTC			

Konfigurieren einer URL-Liste für Ihre internen Server

Gehen Sie wie folgt vor, um eine Liste zu erstellen, die die Server enthält, für die Sie Ihren WebVPN-Benutzern Zugriff gewähren möchten.

- 1. Wählen Sie Konfiguration > VPN > WebVPN > Server und URLs aus, und klicken Sie auf Hinzufügen.
- 2. Geben Sie einen Namen für die URL-Liste ein. Dieser Name ist für Endbenutzer nicht sichtbar. Klicken Sie auf **Hinzufügen**.
- Geben Sie den Namen der URL-Anzeige ein, wie er Benutzern angezeigt werden soll. Geben Sie die URL-Informationen des Servers ein. So greifen Sie normalerweise auf den Server

zu.

Cisco ASDM 5.1 for A File Rules Search Op	A 172.16.172.52 ans Taols Wizards Help	
G Home Configure	an Montoning Back Forward Search Refre	sh Save Help
Interfaces Interfaces Security Policy NAT Image: Security Policy Image: Security Policy <	Image: State of the server	access over WebVPN.
CSD Manager	Content Rewrite Content Rewrite Encoding Pot Forwarding Proxies Proxy Bypass SSL VPN Client SSD VPN Client SSO VPN Client SSO VPN Access Webpage Customi	ver and URL List
	URL Display Name: Internal Server URL: https V 10.1.1.20 OK Cancel	Cl Help

4. Klicken Sie auf **OK**, **OK** und dann auf **Übernehmen**.



Konfigurieren einer Richtlinie für interne Gruppen

Gehen Sie wie folgt vor, um eine Gruppenrichtlinie für Ihre WebVPN-Benutzer zu konfigurieren.

- 1. Wählen Sie Konfiguration > VPN > Allgemein > Gruppenrichtlinie aus, klicken Sie auf Hinzufügen, und wählen Sie Interne Gruppenrichtlinie aus.
- Geben Sie auf der Registerkarte Allgemein einen Richtliniennamen an, z. B. Internal-Group_POL_WEBVPN. Deaktivieren Sie dann Inherit neben Tunneling-Protokolle, und aktivieren Sie WebVPN.

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

3. Wählen Sie auf der Registerkarte WebVPN die Unterregisterkarte **Andere** aus. Deaktivieren Sie **Vererben** neben Servern und URL-Listen, und wählen Sie in der Dropdown-Liste die von Ihnen konfigurierte URL-Liste aus. Klicken Sie abschließend auf **OK**.

🖆 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 🔽 🔽 New	
Web-Type ACL ID: 🔽 Inherit 🐱 Manage	
SSO Server: Inherit New	
HTTP Compression: V Inherit O Enable O Disable	
Keepalive Ignore	
Specify upper limit of the HTTP/HTTPS traffic, per transaction to ignore.	
Transaction Size: 🔽 Inherit 🛛 🛛 🕅	
- Deny Message	
✓ Inherit	
OK Cancel Help	

Konfiguration einer Tunnelgruppe

Führen Sie diese Schritte aus, um eine Tunnel-Gruppe für Ihre WebVPN-Benutzer zu konfigurieren.

 Wählen Sie Configuration > VPN > General > Tunnel Group, klicken Sie auf Add, und wählen Sie WebVPN Access.. aus.



 Geben Sie einen Namen f
ür die Tunnelgruppe ein, z. B. WEB_VPN-GRP. W
ählen Sie auf der Registerkarte Basic (Grundlegend) die erstellte Gruppenrichtlinie aus, und
überpr
üfen Sie, ob die Gruppe Type webvpn ist.

📧 Edit Tunnel Group 🛛 🔀
Name: WEB_VPN-GRP Type: webvpn
General WebVPN
Configure general eccess officientes from the following out take
Basic AAA Client Address Assignment Advanced
AAA Client Address Assignment Advanced
Group Policy: Internal-GRP_POL 💌
Internal-GRP_POL_WEBV DftGrpPolicy
strip the realm from usemame before passing it on to the AAA server
Strip the group from username before passing it on to the AAA server
OK Cancel Hein

3. Öffnen Sie die Registerkarte AAA.Wählen Sie für Authentication Server Group (Authentifizierungsserver-Gruppe) die Gruppe aus, die Sie konfiguriert haben, um die NTLMv1-Authentifizierung mit Ihrem Domänen-Controller zu aktivieren.Optional: Aktivieren Sie die Option LOCAL verwenden, wenn die Servergruppe die Verwendung der LOKALEN Benutzerdatenbank bei Ausfall der konfigurierten AAA-Gruppe nicht aktiviert. So können Sie die Fehlerbehebung zu einem späteren Zeitpunkt durchführen.

🖆 Edit Tunnel Group 🔀						
Name: WEB_VPN-GRP Type: webvpn						
General WebVPN						
Configure general access attributes from the following sub-tabs.						
Pacia AAA Client Address Assignment Advanced						
Dasit om Client Audress Assignment Auvanceu						
To set authentication server group per interface, go to the Advanced tab.						
Authentication Server Group: Windows_NT						
Use LOCAL if Server Gro-None						
Authorization Server Group: Local						
Users must exist in the authorization database to connect						
Accounting Server Group: None						
Authorization Settings						
O Use the entire DN as the username						
Specify individual DN fields as the username Brimen: DN Field: ON (Common Name)						
Primary DN Field. CN (Common Name)						
Secondary DN Field: 00 (Organization Onit)						
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. Wechseln Sie zur Registerkarte WebVPN und dann zur Unterregisterkarte **GruppenAliase** und URLs.
- 5. Geben Sie unter GruppenAliase einen Alias ein, und klicken Sie auf **Hinzufügen**. Dieser Alias wird in der Dropdown-Liste angezeigt, die WebVPN-Benutzern bei der Anmeldung angezeigt wird.

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

6. Klicken Sie auf OK und dann auf Übernehmen.

Konfigurieren der automatischen Anmeldung für einen Server

Wechseln Sie zur Befehlszeile, um SSO für Ihre internen Server zu aktivieren.

Hinweis: Dieser Schritt kann im ASDM nicht ausgeführt werden und muss über die Befehlszeile ausgeführt werden. Weitere Informationen finden Sie unter <u>Zugreifen auf die</u> <u>Befehlszeilenschnittstelle</u>.

Verwenden Sie den Befehl **für die automatische Anmeldung**, um die Netzwerkressource (z. B. einen Server) anzugeben, auf die Ihre Benutzer zugreifen möchten. Hier wird eine einzelne Server-IP-Adresse konfiguriert, aber ein Netzwerkbereich wie **10.1.1.0** /24 kann ebenfalls angegeben werden. Weitere Informationen finden Sie im <u>Befehl für die automatische Anmeldung</u>.

```
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 dieser Beispielausgabe wird der Befehl **zur automatischen Anmeldung** global für WebVPN konfiguriert. Dieser Befehl kann auch im WebVPN-Gruppenkonfigurationsmodus oder im WebVPN-Konfigurationsmodus für Benutzernamen verwendet werden. Die Verwendung dieses Befehls im WebVPN-Gruppenkonfigurationsmodus beschränkt ihn auf eine bestimmte Gruppe. Die Verwendung dieses Befehls im Konfigurationsmodus für WebVPN-Benutzernamen beschränkt diesen auf einen einzelnen Benutzer. Weitere Informationen finden Sie im <u>Befehl für die</u> automatische Anmeldung.

Endgültige ASA-Konfiguration

In diesem Dokument wird diese Konfiguration verwendet:

ASA Version 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
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
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 nt-
auth-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 le311c30 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-group-
policy 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-inspection-
```

traffic ! ! 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				

<u>Überprüfen</u>

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Testen einer WebVPN-Anmeldung

Melden Sie sich als Benutzer an, um Ihre Konfiguration zu testen.

 Versuchen Sie, sich mit Benutzerinformationen von Ihrer NT-Domäne bei der ASA anzumelden. Wählen Sie den in Schritt 5 konfigurierten Gruppen-Alias unter <u>Tunnelgruppe</u> <u>konfigurieren</u> aus

Web/PN Service - Microsoft Internet Explorer Image: Big of the provides into the provides into the provides into the provide of t		
Ele Edi Yev Favories Took teb C Ecci C Total C Ecci C Ecc	WebVPN Service - Microsoft Internet Explorer	
Control	Ele Edit View Favorites Icols Help	
Address in the function of the	🚱 Back 🔹 🛞 🔛 📓 🏠 🔎 Search 🤺 Favorites 🚱 🍓 🔜 🖄	
WebVPN Service Login Please enter your usemame and password. USERNAME: test PassWORD: orosp-Selection Login Login	Addross 🕘 https://172.16.171.51/+webvpr+/index.html	🗸 🛃 🚱 Unks 🎽
Login Please enter your usemame and password. USERNAME: test PASSWORD: •••••• GROUP: Group-Selection Login Clear	CISCO STSTERS 	
Please enter your usemame and password. USERNAME: test PASSWORD:	Login	
USERNAME: test PASSWORD: •••••i GROUP: Group-Selection V Login Clear	Please enter your usemame and password.	
PASSWORD: e GROUP: Group-Selection Clear	USERNAME: test	
GROUP: Group-Selection	PASSWORD:	
Login Clear	GROUP: Group-Selection	
Done	Login Clear	
Done		
Done		
Done		
Dome		
The Internet		
Dome		
🖉 Done		
🖉 Done 🚔 🕲 Internet 🗤		
🖉 Done 🚔 🎱 Internet		
	a Done	🔒 😨 Internet

2. Suchen Sie nach den Verbindungen, die für die internen Server konfiguriert sind. Klicken Sie

auf den Link, um dies zu überprüfen.

WebVPN Service - Microsoft Internet Explorer						
Elle Edit Yew Fgyorites Iools Help						- 🥂
🌀 Back • 💿 - 💌 🖻 🏠 🔎	🔿 Search 🤺 Favorites 🤞	🛛 🖉 · 🍇 🖻	- 25			
Address 🕘 https://172.16.171.51/+webvpn+/p	portal.html				💌 🄁 Go	Links *
Pop-up blocked. To see this pop-up or addition	al options dick here					×
Cisco Systems without the WebVPN Service	ce					
			<u>Click here to open</u>	<u>the Floating Toolbar</u>	? / @/	\leq
WEB APPLICATIONS	Web Bookmarks					
Enter Web Address (URL)	Internal Server					
Go						
Web Bookmarks 💌						
						-
iavascript:top.doWebUrl("https://10.1.1.200")				S 🔒 🌢	Internet	

Überwachungssitzungen

Wählen Sie **Monitoring > VPN > VPN Statistics > Sessions** aus, und suchen Sie eine WebVPN-Sitzung, die zu der in diesem Dokument konfigurierten Gruppe gehört.

🖆 Cisco ASDM 5.1 for ASA - 172.16.171.51							
File Rules Search Options Tools Wiz	ards Help						
Home Configuration Monitoring	Back Forward Search Refresh Save Help Cisco States						
Image: Second statistics Image: Se	Sessions PI Remote Access LAN-to-LAN WebVPN SSL VPN Client E-mail Proxy Total Cumulative 0 0 1 0 0 1 3 at fit Filter By WebVPN - All Sessions Filter Username Group Policy Protocol Login Ti Details IP Address Tunnel Group Encryption Duration Logout 171.99.88.116 WEB VPN-QRP 3DES 0h.01m.18s Ping To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu. Logout By: - All Sessions I.ogout Sessions Refresh Last Updated: 3/30/06 2.31:30 PM East Updated: 3/30/06 2.31:30 PM East Updated: 3/30/06 2.31:30 PM						
Data Refreshed Successfully.	cisco NA (15) 🛛 😹 🐼 🐼 🔒 3/30/06 3:05:21 PM UTC						

Debuggen einer WebVPN-Sitzung

Diese Ausgabe ist ein Beispiel für das Debuggen einer erfolgreichen WebVPN-Sitzung.

Hinweis: Beachten Sie <u>vor der</u> Verwendung von **Debug-**Befehlen die <u>Informationen</u> zu <u>Debug-</u><u>Befehlen</u>.

```
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]
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Wenn das Dropdown-Feld "Gruppe" nicht auf der WebVPN-Anmeldeseite vorhanden ist, stellen Sie sicher, dass Sie Schritt 2 unter <u>WebVPN aktivieren</u> und Schritt 5 unter <u>Tunnelgruppe konfigurieren</u> abgeschlossen haben. Wenn diese Schritte nicht abgeschlossen sind und das Dropdown-Menü fehlt, fällt die Authentifizierung unter die Standardgruppe und schlägt wahrscheinlich fehl.
- Obwohl Sie Benutzern in ASDM oder auf der ASA keine Zugriffsrechte zuweisen können, können Sie Benutzer mit Microsoft Windows-Zugriffsrechten auf Ihrem Domänen-Controller einschränken. Fügen Sie die erforderlichen NT-Gruppenberechtigungen für die Webseite hinzu, bei der sich der Benutzer authentifiziert. Wenn sich der Benutzer mit den Berechtigungen der Gruppe bei WebVPN angemeldet hat, wird der Zugriff auf die angegebenen Seiten entsprechend gewährt oder verweigert. Die ASA fungiert nur als Proxy-Authentifizierungs-Host für den Domänen-Controller, und alle Kommunikation hier ist NTLMv1.
- Sie können SSO für SharePoint nicht über WebVPN konfigurieren, da der SharePoint-Server keine formularbasierte Authentifizierung unterstützt. Daher sind die Lesezeichen mit Post oder das Post-Plugin-Verfahren hier nicht anwendbar.

Zugehörige Informationen

- <u>Cisco Adaptive Security Appliances der Serie ASA 5500</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>