使用 ASDM 和 NTLMv1 配置具有 WebVPN 和单 点登录的 ASA 示例

目录

简介 先决条件 要求 使用的组件 规则 配置 添加 AAA 服务器用于 Windows 域的身份验证 创建自签名证书 在外部接口上启用 WebVPN 配置内部服务器的 URL 列表 配置内部组策略 配置隧道组 配置服务器的自动登录 最终的 ASA 配置 验证 测试 WebVPN 登录 监视会话 调试 WebVPN 会话 故障排除 相关信息

<u>简介</u>

本文档介绍如何配置 Cisco 自适应安全设备 (ASA),从而自动将 WebVPN 用户登录凭证以及从属 身份验证传递到要求对照运行 NT LAN Manager 版本 1 (NTLMv1) 的 Windows Active Directory 进 行其他登录认证的服务器。此功能称为单一登录 (SSO)。通过此功能,为特定 WebVPN 组配置的 链路能够传递此用户的身份验证信息,从而消除多次身份验证提示。此功能还可用于全局或用户配 置级别。

<u>先决条件</u>

<u>要求</u>

尝试进行此配置之前,请确保满足以下要求:

• 确保配置了目标 VPN 用户的 NTLMv1 和 Windows 权限。有关 Windows 域访问权限的详细信

息,请参阅 Microsoft 文档。

<u>使用的组件</u>

本文档中的信息基于以下软件和硬件版本:

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

<u>规则</u>

有关文档规则的详细信息,请参阅 <u>Cisco 技术提示规则</u>。

配置

本部分提供有关将 ASA 配置为具有 SSO 功能的 WebVPN 服务器的信息。

注意: 使用<u>命令查找工具(仅限注册用户</u>)可获取有关本部分所使用命令的详细信息。

添加 AAA 服务器用于 Windows 域的身份验证

完成以下这些步骤,将 ASA 配置为使用域控制器进行身份验证。

1. 选择 Configuration > Properties > AAA Setup > AAA Servers,然后单击 Add。为服务器组提 供一个名称(如 Windows_NT),然后选择 NT Domain 作为协议。

🔂 Cisco ASDM 5	i.1 fne ASA - 172.16.172.52		
Fig Rules Bea	arch Options Tools Wizards	s Holp	
<u></u>	🖧 😥		
Hone (G	Continuation increasing	Soci Pervera Sector Percon Seve Perp Relineering.	
	金金茶 瞬间的复数		
Interfaces	Startup Wigard	AVA Servers	
<u>ii</u> ,	白 GAAA Setup	Sener Groupe	
Security Policy	Stath. Prompt	Server Group Protocol Accounting Node Reactivation Node Add	
24	¹ St DAP Athibuts Map -St And-Second	LOCAL LOCAL Edit	
NAT	₩- 🖬 ARF	Deele	
84 1	i - Auto Upcate ⊞-⊡ Certificate		
A	串 🔓 Device Access 時, 第日m ca Administration	8	
CSD Manu gar	Der Boler Cervices	Bevers in Selected Group	
1	- JEDNS Clent	Server Name or IP Address Interface Timeout Add	
PS PS	Fragment	Edi	
· <u>Ž</u>	- WHISTORY METRICS	Deide	
Routing	中心 IF Audit	Mirza uz	
- 🖓		Wilese street	
Global Objects	- #88L 	Tes:	
Drewarting	- TCP Options	😤 Add AAA Server Group	
Properties	는 잘 Timeoute 노출 URL Filtering	Configure AAA server group. The accounting Mode ath bute is only	
		Apply Hesst applicable for RACIUS and TACACS+ protocols.	
		lorero INA (16) 🖬 👼 📋 Server Group: Windows_NT	
		Protocol Victorian Y	
		Arctunting Mode. O Smultaneuva - Single	
		Featlyation Node:	
		Dead Time 10 minutes	
		Na: Faied Atempts: 3	
		DK Cancel Help	

2. 添加 Windows 服务器。选择新创建的组,然后单击 Add。选择服务器所在的接口,然后输入 IP 地址和域控制器名称。确保输入的域控制器名称全部为大写字母。完成后单击 OK。

🚰 Cisco ASDM 5	5.1 for ASA	172.16.172.52	2									
Fie Rulas Sea	arck Options	Tools Wizard	s Help									
G Home C	Sonfiguration	() Monitoring	Co Deck	Corvers	Q Search R	🚱 🛄 stresh Save	?		Cisco Srs	rens Ih		
interfaces Becurity Policy NAT	Contiguration P 2 P P 3 Startu P 4 AAA S P 4 AAAA S P 4 AAAA S P 4 AAAA S P 4 AAAA S P 4 AA	Coperties A Coperties A p Witeand etup A Servers du Prompt MP Admission Kep poorting Jodate cate	AAA Setup AAAA S Setup Cool Cool Cool Cool Cool	A AA Servers arvers ver Groups mer Group SAL Sows_NT	Protocol LOCAL NT Doma	Accounting to	ode Rea	chrolion Mode Depiction	Add Edit Defete			
CSD Honoger	E al Denter E al	e Access a Administration Berutices Client er rent y Matrices HTTPS HTTP	Ser	vers in Selecter	d Group P Address	Interface	Tr	reaut	Add Folt Delete Move up Itotice down Test			
Proposass		itering				Apply	Rese	Add AAA Serve Server Group:	r	Windows_N	т	
					6500	NA (15)	10 (A	Interface Name : Server Name or I Timeout: NT Domain Para Server Port Domain Contra	P Address: meters pler:	inside 10.1.1 200 10 138 ESC-&I-78 Cancel	seconds	

此窗口显示完整的 AAA 配置

:



创建自签名证书

完成以下这些步骤,将 ASA 配置为使用自签名证书。

注意:为简单起见,在本例中使用自签名证书。有关其他证书注册选项(如注册到外部证书颁发机 构),请参阅<u>配置证书</u>。

- 1. 选择 Configuration > Properties > Certificate > Trustpoint > Configuration,然后单击 Add.
- 2. 在出现的窗口中输入 Trustpoint Name(如 Local-TP),并选中 Generate a self-signed certificate on enrollment。其他选项可保留其默认设置。完成后单击 OK。



此窗口显示完整的信任点配置

:



在外部接口上启用 WebVPN

完成以下这些步骤,以允许网络外部的用户使用 WebVPN 进行连接。

- 1. 选择 Configuration > VPN > WebVPN > WebVPN Access。
- 2. 选择所需的接口,单击 Enable,然后选中 Enable Tunnel Group Drop-down List on WebVPN Login Page。注意:如果使用同一个接口访问 WebVPN 和 ASDM,则必须将用于访问 ASDM 的默认端口从端口 80 更改为 8080 等新端口。此操作在 Configuration > Properties > Device Access > HTTPS/ASDM 下完成。注意: 在用户导航到 http://<IP 地址> 而非 https://<IP 地址> 的情况下,可以自动将用户重定向到端口 443。选择 Configuration > Properties > HTTP/HTTPS,选择所需的接口,单击 Edit,然后选择 Redirect HTTP to HTTPS。

🕼 Cisco ASDM	5.1 for ASA - 172.16.171.51		🛛
File Rules Se	earch Options Tools Wizards	Help	
ổ Home	Configuration Monitoring	Cack Forward Search Refresh Save Help	STSTENS
	Configuration > VPN > WebVPN	I > WebVPN Access	
	● 金 革 [■] 俞 義 电	a @ 魚 篇 傘	
Interfaces	🕀 🙀 E-mail Proxy 🔺 🔒	-WebVPN Access	
<u>6</u>	🛱 🚰 General		
Security Policy	- 🚽 Client Update	Configure access parameters for WebVPN. (Note: The WebVPN features in this software releas	se are
a.	Provide Paralle Tunnel G	 currently provided as a free trial, and future major software releases will require the purchase ar installation of a WebVPN feature license.) 	nd
68	- Tunnel Group	notalisation of a vyoern national of monitory	
NAT	🚮 VPN System Opt	Interface WebVPN Enabled Enab	ole .
<u> </u>	⊕ % IKE	inside No	
VPN	田· SpiP Address Managei	outside Yes Disat	alt
A	Here Balancing		
CSD Managar	E WebVPN		
	-ACLs		
Q ,	- APCF		
IPS	- CSD Setup	Port Number: 443	
4 <u>7</u> 2	- Content Rewrite	Default Idle Timeout: 1800 seconds	
Routing	Encoding		
<u>, (a</u>)	Port Forwarding	Max. Sessions Limit: 2	
Global Objects	- Provies	WebVPN Memory Size: 50 % of total physical memory	
	-33SSL VPN Client		
3	SSO Servers	Enable Tunnel Group Drop-down List on WebYPN Login Page	
Properties	- Bervers and URL		
	WebVPN Access	Apply Reset	
Configuration cha	anges saved successfully.	cisco NA (15) 🛛 😹 🔂 🔒 3/30/06 2:37:41	1 PM UTC

配置内部服务器的 URL 列表

完成以下这些步骤,创建包含要授予其 WebVPN 用户访问权限的服务器的列表。

- 1. 选择 Configuration > VPN > WebVPN > Servers and URLs, 然后单击 Add。
- 2. 输入 URL 列表的名称。此名称对最终用户不可见。单击 Add。
- 3. 输入 URL Display Name,要向用户显示该名称。输入服务器的 URL 信息。一般应该用此方 式访问服务器。



4. 单击 **OK**,然后单击 Apply。



<u>配置内部组策略</u>

完成以下这些步骤,为 WebVPN 用户配置组策略。

- 1. 选择 **Configuration > VPN > General > Group Policy**,单击 Add,然后选择 Internal Group Policy。
- 2. 在 General 选项卡上,指定一个策略名称,如 Internal-Group_POL_WEBVPN。然后,取消选 中 Tunneling Protocols 旁的 **Inherit**,再选中 WebVPN。

🖆 Add Internal Group Policy	/	
Name: mal-GRP_POL	WEBVPN	
General IPSec Client Con	figuration CI	ient Firewall Hardware Client WebVPN
Check an Inherit checkbox	to let the corr	esponding setting take its value from the default group policy.
Tunneling Protocols:	📃 Inherit	IPSec VebVPN
Filter:	🗹 Inherit	Manage
Connection Settings		
Access Hours:	🕑 innerit	New
Simultaneous Logins:	🗹 Inherit	
Maximum Connect Time	: 🗹 Inherit	Unlimited minutes
Idle Timeout:	🗹 Inherit	Unlimited minutes
Servers		
DNS Servers:	🗹 Inherit	Primany: Secondary:
WINS Servers:	🗹 Inherit	Primary: Secondary:
DHCP Scope:	🗹 Inherit	
	0K	Cancel Help

3. 在 WebVPN 选项卡上,选择 **Other** 子选项卡。取消选中 Servers and URL Lists 旁的 **Inherit**,然后从下拉列表中选择所配置的 URL 列表。完成后单击 **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: Veb-Type ACL ID: Manage
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
Deny Message
OK Cancel Help

配置隧道组

完成以下这些步骤,为 WebVPN 用户配置隧道组。

1. 选择 Configuration > VPN > General > Tunnel Group,单击 Add,然后选择 WebVPN Access...。



2. 输入隧道组的名称,如 WEB_VPN-GRP。在 Basic 选项卡上,选择所创建的组策略,并且确 认组类型为 **webvpn**。

📧 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
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

3. 转到 AAA 选项卡。对于 Authentication Server Group,选择您所配置的组,以便对您的域控 制器启用 NTLMv1 身份验证。**可选:**选中 **Use LOCAL if Server Group Fails**,以便在所配置 的 AAA 组失败时使用 LOCAL 用户数据库。这可以帮助您以后排除故障。

🖆 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
To set authentication server group per interface, go to the Advanced tab.
Authentication Server Group: Windows_NT
Use LOCAL if Server Gra
Authorization Server Group: LOCAL
Accounting Server Group None
Autorization settings
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. 转到 WebVPN 选项卡,再转到 Group Aliases and URLs 子选项卡。
- 5. 在 Group Aliases 下输入别名,然后单击 Add。登录时,此别名显示在向 Webvpn 用户提供的 下拉列表中。

	Type: webvpn	
Group Aliases	Add >> Ad	Status enable
Group URLs URL (http or https): ✓ Enable	Add >>	Status
OK	Cancel Help	

6. 单击 OK, 然后单击 Apply。

配置服务器的自动登录

切换到命令行,以便为内部服务器启用 SSO。

注意: 在 ASDM 中无法完成此步骤,而是必须使用命令行实现此步骤。有关详细信息,请参阅<u>访</u> <u>问命令行界面</u>。

请使用 auto-signon 命令指定要让用户可访问的网络资源(如服务器)。此处仅配置一个服务器 IP 地址,但还可以指定网络范围(如 10.1.1.0 /24)。有关详细信息,请参阅 <u>auto-signon</u> 命令。

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

在本示例输出中,从全局范围对 WebVPN 配置了 auto-signon 命令。还可以在 WebVPN 组配置模

式或 WebVPN 用户名配置模式下使用此命令。在 WebVPN 组配置模式下使用此命令会将其适用范 围限制在某个特定的组内。同样,在 WebVPN 用户名配置模式下使用此命令会将其适用范围限制 在某个用户内。有关详细信息,请参阅 <u>auto-signon</u> 命令。

<u>最终的 ASA 配置</u>

本文档使用以下配置:

ASA 7.1(1) 版

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 securitylevel 0 ip address 172.16.171.51 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside securitylevel 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-domaincontroller 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 la06092a 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 sip inspect xdmcp ! service-policy global_policy global !--- WebVPN Configuration webvpn enable outside url-list webserver "Internal Server" https://10.1.1.200 1 tunnelgroup-list enable auto-signon allow ip 10.1.1.200 255.255.255.255 auth-type ntlm Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6 : end

<u>验证</u>

使用本部分可确认配置能否正常运行。

<u>命令输出解释程序(仅限注册用户</u>)(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输 出的分析。

<u>测试 WebVPN 登录</u>

以用户身份登录,测试您的配置。

1. 尝试从您的 NT 域登录到包含用户信息的 ASA。选择<u>配置隧道组</u>下第 5 步中配置的组别名。

🗿 WebVPN Service - Microsoft Internet Explorer	
Ele Edit View Figurantes Icols Help	R
🌀 Back 🔹 🐑 💌 😰 🏠 🔎 Search 🧙 Favorites 🤣 😥 - 🌺 🔜 🦓	
Address 💩 https://172.16.171.51/+webvpr+/index.html	nks 🎇
CISCO SYSTEMS WebVPN Service	
Login	
Please enter your usemame and password.	
USERNAME: test	
PASSWORD:	
GROUP: Group-Selection	
Login Clear	
🙆 Done 🕒 😫 🐲 Internet	

2. 查找经过配置指向内部服务器的链接。单击该链接进行验证。

WebVPN Service - Microsoft Internet	t Explorer					
Elle Edit Yew Favorites Iools Help				i jakara	Street a	- 🥂
🌀 Back 🔹 🕥 - 💌 🖻 🏠 🎾	🔎 Search 🤺 Favorites 🔗	🖉 - 🍓 🖂	8			
Address 🕘 https://172.16.171.51/+webvpn+/	portal.html				👻 🄁 Go	Links *
S Pop-up blocked. To see this pop-up or addition	nal options dick here					×
Cisco Systems authorial line- WebVPN Servi	ce					Î
			Click here to ope	n the Floating To	obar ? 🖌 🖾	\mathbf{X}
WEB APPLICATIONS	Web Bookmarks					
Enter Web Address (URL)	Internal Server					
Veb Bookmarks						3
iavascript:top.doWebUdChttps://10.1.1.2000				8	🔒 🧔 Internet	×

监视会话

选择 Monitoring > VPN > VPN Statistics > Sessions,并查找属于本文档中配置的组的 WebVPN 会

ドト	
坧	c

Cisco ASDM 5	i.1 for ASA - 172.16.171.51							
File Rules Ser	arch Options Tools Wizards	Help						0
Home (Configuration Monitoring	G Back Fo	rward Se	arch Re	Normal Save	? Help		LISCO STSTENS
Home PriterTacces VPN IPS Routing Properties Logging	Configuration Monitoring	Book Fo Sessions Remote Access 0 Filter By: User IP Ad test 171.69.89 • To sort VPN Locout By	rward Se IS LAN-to-LAN WebVPN name dress 116 I sessions, riv	WebVPN 1 Group Pe Tunnel G Memal-ORP VEB VPN-G	All Sessions Dicy F roup E POL WebVP RP 3DES	Help E-mail Proxy 0 Protocol Encryption N	Total 1 1 1 1 1 5:03:38 UTO 0 1:01m:18s	Total Cumulative 3 Filter cogin Ti Details uration Thu ti Dotails Ping
					Refres	<u>h </u>	st Lindated: 31	30/06 2:31:30 PM
Data Refreshed S	Buccessfully.			cisco	NA (15)		(a) Optimized, sv (b) 12 (3/30)	006 3:05:21 PM UTC

调试 WebVPN 会话

以下输出是对某个成功的 WebVPN 会话的调试示例。

注意: 使用 debug 命令之前,请参阅<u>有关 Debug 命令的重要信息</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_session.c:webvpn_update_idle_time[924] WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:http_webvpn_find_session[136]

<u>故障排除</u>

本部分提供的信息可用于对配置进行故障排除。

- 如果 WebVPN 登录页上不存在 Group 下拉框,请确保完成了<u>在外部接口上启用 WebVPN</u>下的 第 2 步和<u>配置隧道组</u>下的第 5 步。如果未完成这些步骤,并且缺少该下拉框,则身份验证将在 默认组下进行,并有可能失败。
- 尽管不能在 ASDM 中或 ASA 上向用户分配访问权限,但可以在域控制器上用 Microsoft Windows 访问权限限制用户。添加进入用户要对其进行身份验证的网页的必要 NT 组权限。用 户以组权限登录到 WebVPN 后,即相应地授予或拒绝对指定页面的访问权限。ASA 仅代表域 控制器作为代理身份验证主机,并且此处的所有通信都是 NTLMv1。
- •因为Sharepoint服务器不支持表基于验证,您不能配置Sharepoint的SSO在WebVPN。结果 ,有发表物或发表物插件步骤的书签不可适用的在这里。

相关信息

- <u>Cisco ASA 5500 系列自适应安全设备</u>
- <u>技术支持和文档 Cisco Systems</u>