使用ASDM和NTLMv1的WebVPN和單一登入的 ASA配置示例

目錄

簡介 必要條件 需求 採用元件 慣例 設定 <u>為Windows域身份驗證新增AAA伺服器</u> 建立自簽名證書 在外部介面上啟用WebVPN 為內部伺服器配置URL清單 配置內部組策略 配置隧道組 配置伺服器的自動登入 最終ASA配置 驗證 測試WebVPN登入 監控作業階段 調試WebVPN會話 疑難排解 相關資訊

<u>簡介</u>

本文檔介紹如何配置思科自適應安全裝置(ASA),以自動將WebVPN使用者登入憑證以及輔助身份 驗證傳遞給需要針對運行NT LAN Manager版本1(NTLMv1)的Windows Active Directory進行額外登 入驗證的伺服器。此功能稱為單點登入(SSO)。 它為為特定WebVPN組配置的鏈路提供了傳遞此使 用者身份驗證資訊的功能,從而消除了多個身份驗證提示。此功能也可用於全域性或使用者配置級 別。

<u>必要條件</u>

<u>需求</u>

嘗試此組態之前,請確保符合以下要求:

• 確保配置了目標VPN使用者的NTLMv1和Windows許可權。有關Windows域訪問許可權的詳細

資訊,請參閱Microsoft文檔。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- Cisco ASA 7.1(1)
- •思科調適型安全裝置管理員(ASDM)5.1(2)
- Microsoft Internet資訊服務(IIS)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u>設定</u>

本節提供將ASA配置為具有SSO的WebVPN伺服器的資訊。

註:使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

<u>為Windows域身份驗證新增AAA伺服器</u>

完成以下步驟,將ASA配置為使用域控制器進行身份驗證。

 選擇Configuration > Properties > AAA Setup > AAA Servers,然後按一下Add。提供伺服器 組的名稱(例如Windows_NT),然後選擇NT Domain作為協定。

🔂 Cisco ASDM 5	.1 for ASA - 172.16.172.57		
Flia Rules Bea	orth Options Tools Wizards	s Halp	
- 🚯 🗌	🍇 😥		
Home C	onfiguration Monitoring	Back Forward Search Refresh Save Hap Anthroad Ital.	
_	Configuration • Properties • A	AA Seluo + AAA Senera	
N	◆ 急 革 ■ 値 氷 ■	と風影範に導出	
internapes C.L.	Startup Wizard	AVA Servers	
English Bolios	WA Servers	Server Groupe	
R4.	Sei DeB abilities Mor	Server Group Protocol Accounting Node Reactivation Mode Add	
NAT.	- Spoofing	Edit	
1941 1977	₩- 🗗 ARF	Deble	
2 6 3	B-Certificate		
a	🖶 🚅 Devke Access		
CSD Manu are	B BOEVice Administration	- Basers in Salarrad Organ	
tin .	- BDNS Clent	Server's Homeshorecop	
NS N	Fallover		
170	- 🔤 History Metrics		
Nouting	HTTP/HTTPS B-RAIF Audit	Dede	
(a)	🕒 🗃 Logging	Miron up	
Giobal Objects	- Priority Quaue	30, 500 (10+-0	
	- 49UNRPC Server	Tes:	
Properties	- MTCP Options	🔂 Add AAA Server Group	
	- ORL Filtering	Apple Report Configure AAA server group. The Accounting Mode sthebuts is only	
		applicable for RACIUS and TACACS+ protocols.	
		loreco INA(16) 🔛 🚓 Server Group: Windows_NT	
		Protocol MT Domain	
		Assessment and the Consultance on the Consultance on the Consultance of the Consultance o	
		raccinitalizada — Canadanacea — Canada	
		Feacivation Mode: 💿 Depletion 💿 Timed	
		Dead Time 10 minutes	
		Non-Failed Hypersolat	
		waar areo waemple. To	
		DK Cancel Help	

2. 新增Windows伺服器。選擇新建立的組,然後按一下Add。選擇伺服器所在的介面,並輸入 IP地址和域控制器名稱。請確保以所有大寫字母輸入域控制器名稱。完成後按一下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	Coperties A Coperties A p Witeand etup A Servers du Prompt MP Admission Kep poorting Jodate cate	AA Selay	A AA Servers arvers ver Groups mer Group SAL Sows_NT	Protocol LOCAL NT Elema	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	

此視窗顯示已完成的AAA配置

:



建立自簽名證書

完成以下步驟,將ASA配置為使用自簽名證書。

注意:在此範例中,自簽名的憑證用於簡化操作。有關其他證書註冊選項(例如向外部證書頒發機 構註冊),請參閱<u>配置證書</u>。

- 1. 選擇Configuration > Properties > Certificate > Trustpoint > Configuration,然後按一下Add。
- 2. 在顯示的視窗中,輸入信任點名稱(如Local-TP),並選中Generate a self-signed certificate on enrollment。其他選項可以保留其預設設定。完成後按一下OK。

🖾 Cisco ASDM 5	i.1 for ASA - 172.16.172.	52						3
File Rules Se	with Options Tools Witzs	indis Help						
Si Forre C	onfiguration Monitoring	Osek	Dorward Search	Q. Refresh	ing Save	? Help	Gisco Sesteus	
Interfaces Subarity Policy NAT	Contiguiation > Proceedies =	Continuels - T Continuels Continue Continue True	ruspoint - Configure E <table-cell> aton re a Certificate Author uspoint Name Devin</table-cell>	nty (CA) as a re Certificate	Instoant. Bubject CA Ce	rificale Subje	ct Add	
CSD Manager PS PS Routing Global Objects Properties	PayManage Certific: PayManage Certific: Payori Pa			Acc	Challenge Challenge	rolot Configu me: Local 1 a set is enabled, Settings Confault-F Confault-F Confault-F Confault-F Confault-F Confault-F Confault-F Confault-F Confault-F Confault-F Configuration Configu	Critical P efficience on empliments only Key Pair and Certificate Pair CRL Retineval Poincy CRL Re BACK Show Details Confirm Challenge Passwor Challenge Passwor Confirm Challenge Passwor Confirm	ameters can be specified freval Method Advanced New Key Patr rd. freval Method International transmitter rd. freval Advanced International transmitter rd. freval Advanced International transmitter rd. freval Advanced International transmitter
			j e	900	if Use C Use Enro Retry Retry	menuel ensett solumetic ens liment UEL: Period	ntent ul merit Itta A I minites D dise D to inclose u Cik Cantal	ntmited refdes) Certificate Parameters Help

此視窗顯示已完成的信任點配置

:



<u>在外部介面上啟用WebVPN</u>

完成以下步驟,允許網路外部的使用者使用WebVPN進行連線。

- 1. 選擇Configuration > VPN > WebVPN > WebVPN Access。
- 2. 選擇所需的介面,按一下Enable,然後在WebVPN登入頁面上選中Enable Tunnel Group下拉 選單。注意:如果對WebVPN和ASDM訪問使用相同的介面,則必須將ASDM訪問的預設埠從 埠80更改為新埠,例如8080。此操作在Configuration > Properties > Device Access > HTTPS/ASDM下完成。注意:當使用者導航到http://<ip_address>而不是 https://<ip_address>時,可以自動將使用者重定向到埠443。選擇Configuration > Properties > HTTP/HTTPS,選擇所需的介面,按一下Edit,然後選擇Redirect HTTP to HTTPS。

🖆 Cisco ASDM 5	5.1 for ASA - 172.16.171.51		
File Rules Se	arch Options Tools Wizards	Help	
G Home C	Configuration Monitoring	Sack Forward Search Refresh Save Help	Cisco Systems
	Configuration > VPN > WebVPN	> WebVPN Access	
	●金革 ■ 前 炎暭		
Interfaces	🔁 🝓 E-mail Proxy 📃 🛌	WebVPN Access	
Security Policy	General	Configure access parameters for WebYPN. (Note: The WebYPN feature	s in this software release are
31.	Group Policy	 currently provided as a free trial, and future major software releases will installation of a WebVPN feature license.) 	require the purchase and
No.	- Tunnel Group		
NA1	🚮 VPN System Opt	Interface WebVPN Enabled	Enable
<u> </u>	🕀 🕅 IKE	inside No	Disable
VPN	BIPSec	lucide les	Disable
A			
CSD Monager	E WebVPN		
1	-MAPOF		
IPS	- 🔏 CSD Setup	Port Number: 443	
474	Cache		
- Ag Routing	- The Encoding	Default Idle Timeout: 1800 seconds	
0	- Sport Forwarding	Max. Sessions Limit: 2	
State Chinese	- Proxies	Web/PN Memory Rize: 50 % of total physical memory	
Gibbal Objects	- MProxy Bypass	To or total physical memory	
5.	SSO Servers	Enable Tunnel Group Drop-down List on WebVPN Login Page	
Properties	- Servers and URL		
	Webyen Access	Apply Reset	
Configuration cha	anges saved successfully.	cisco 🛛 NA (15) 🔡 🙀	3/30/06 2:37:41 PM UTC

<u>為內部伺服器配置URL清單</u>

完成以下步驟以建立包含要授予您的WebVPN使用者訪問許可權的伺服器的清單。

- 1. 選擇Configuration > VPN > WebVPN > Servers and URLs,然後按一下Add。
- 2. 輸入URL清單的名稱。此名稱對終端使用者不可見。按一下「Add」。
- 3. 輸入URL顯示名稱,使其顯示給使用者。輸入伺服器的URL資訊。這應該是通常訪問伺服器的 方式。



4. 按一下「OK」、「OK」,然後「Apply」。



<u>配置內部組策略</u>

完成以下步驟,為WebVPN使用者配置組策略。

- 1. 選擇Configuration > VPN > General > Group Policy,按一下Add,然後選擇Internal Group Policy。
- 2. 在General頁籤上,指定一個策略名稱,例如Internal-Group_POL_WEBVPN。然後取消選中 Tunneling Protocols旁邊的Inherit並選中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 corr	esponding 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: 🔽 Inherit	Primary: Secondary:
WINS Servers: 🔽 Inherit	Primary: Secondary:
DHCP Scope: 🔽 Inherit	
OK	Cancel Help

3. 在WebVPN頁籤上,選擇**Other**子頁籤。取消選中Servers and URL Lists旁邊的**Inherit**,然後 從下拉選單中選擇配置的URL清單。完成後按一下**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: Velocities Manage
SSO Server: Inherit New
HTTP Compression: VInherit O Enable O Disable
Keepalive Ignore
Specify upper limit of the HTTP/HTTPS traffic, per transaction to ignore. Transaction Size: Inherit KB
Deny Message
OK Cancel Help

配置隧道組

完成以下步驟,為WebVPN使用者配置隧道組。

1. 選擇Configuration > VPN > General > Tunnel Group,按一下Add,然後選擇WebVPN Access...



2. 輸入隧道組的名稱,例如WEB_VPN-GRP。在Basic頁籤上,選擇您建立的組策略,並驗證組 型別是否為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
OK Cancel Help

3. 轉到AAA頁籤。對於Authentication Server Group,選擇您配置的組以啟用域控制器的 NTLMv1身份驗證。**可選:**選中**Use LOCAL if Server Group Fails**,以在配置的AAA組發生故 障時啟用本地使用者資料庫的使用。這有助於您稍後進行故障排除。

🖆 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							
Dasic Cilent 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 None							
Authorization Server Group: LOCAL							
Users must exist in the authorization database to connect							
Accounting Server Group: None							
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							
Covernde account-disabled indication from AAA server Covernde account-disabled indication from AAA server							
Enable notification upon password expiration to allow user to change password							
OK Cancel Hein							

- 4. 轉到WebVPN頁籤,然後轉到Group Aliases and URLs子頁籤。
- 5. 在「組別名」下輸入別名,然後按一下Add。此別名顯示在登入時向WebVPN使用者顯示的下 拉選單中。

🖆 Edit Tunnel Group		×
Name: WEB_VPN-GRP	Type: webvpn	
General WebVPN		
Configure WebVPN access attribut	Aliases and URLS. Web Page	
Group Aliacon	Anases and onces wep Page	
Group Anases	Alias Status	
Alias:	Add >> Group-Selection enable	
Enable	<< Remove	
Enable		
-Group LIRI s		
	URL Status	
URL (http or https):	Add >>	
✓ Enable	<< Remove	
OK	< Cancel Help	

6. 按一下「OK」,然後「Apply」。

<u>配置伺服器的自動登入</u>

切換到命令列以啟用內部伺服器的SSO。

注意:此步驟無法在ASDM中完成,必須使用命令列完成。如需詳細資訊,請參閱<u>存取指令行介面</u> 。

使用auto-signon命令指定要授予使用者訪問許可權的網路資源,如伺服器。此處配置了單個伺服器 IP地址,但也可以指定網路範圍,如10.1.1.0 /24。如需詳細資訊,請參閱<u>auto-signon</u> 命令。 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

在此輸出範例中,**auto-signon**命令是針對WebVPN全域性設定的。此命令也可以在WebVPN組配置 模式或WebVPN使用者名稱配置模式下使用。在WebVPN組配置模式下使用此命令可將其限製為特 定組。同樣,在WebVPN使用者名稱配置模式下使用此命令會將其限製為單個使用者。如需詳細資 訊,請參閱<u>auto-signon</u> 命令。

<u>最終ASA配置</u>

本檔案會使用以下設定:

```
ASA版本7.1(1)
ASA# show running-config
: Saved
ASA Version 7.1(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
1
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
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 le311c30 la06092a 864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30 le170d30 36303333 30313334 3930345a 170d3136 30333237 31333439 30345a30 le311c30 la06092a 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 sip inspect xdmcp ! service-policy global_policy global !--- 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:c80ac5f6232df50fclecc915512c3cd6
: end
```



使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具(</u>僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

<u>測試WebVPN登入</u>

以使用者身份登入以測試您的組態。

1. 嘗試使用來自NT域的使用者資訊登入到ASA。在配置隧道組下選擇步驟5中配置的組別名。

WebVPN Service - Microsoft Internet Explorer	
Ele Edit View Figuraites Icols Help	a da an farair an tao an an 🕸
😋 Back 🔹 🐑 📓 🏠 🔎 Search 🤺 Favorites 🤣 😥 🍓 🔜 🦓	
Address 🕘 https://172.16.171.51/+webvpr+/index.html	🔽 🔂 Go 🛛 Unks 🎽
Cisco System: WebVPN Service Login Please enter your usemame and password. USERNAME: test PASSWORD: ••••••] CROUP: Comp.Selector	
Login Clear	
Done	🔒 🐞 Internet

2. 查詢為內部伺服器配置的鏈路。 按一下連結進行驗證。

WebVPN Service - Microsoft Internet	Explorer				
Elle Edit Yew Favorites Icols Help					1 I I I I I I I I I I I I I I I I I I I
🌀 Back = 🛞 - 🖹 🗟 🏠 🔎	🔎 Search 🤺 Favorites 🤞	🛛 🍰 🗟	8		
Address 👹 https://172.16.171.51/+webvpn+/	portal.html				🖌 🄁 Go 🛛 Links
Pop-up blocked. To see this pop-up or addition	al options dick here				د
Cisco Systems addimentalities - WebVPN Servi	ce				
		2	Click here to open th	ne Floating Toolbar	? / @X
WEB APPLICATIONS	Web Bookmarks				
Enter Web Address (URL)	Internal Server				
Go					
Web Bookmarks 😪					
javascript:top.doWebUH("https://10.1.1.200")				S 🔒 🕯	Internet

監控作業階段

選擇**Monitoring > VPN > VPN Statistics > Sessions**,然後查詢屬於本文檔中配置的組的 WebVPN會話。

E Cisco ASDM 5.1 for ASA - 172.16.171.51			
File Rules Search Options Tools Wizards Help			
Home Contiguration Monitoring Book	Search Refresh	Save Halp	Cisco Systems
Monitoring > VPN > VPN Statistics > See	sions		
Herrisces	ote LAN-to-LAN WebVPN SSLV	PN Client E-mail Proxy	Total
Acce	55 0 1		Cumulative
Cruster Loads			· · ·
IPS Compression Stat	By WebVPN 💽 All Ses	sions 💌	Filter
	Jsername Group Policy P Address Tunnel Group	Protocol Encryption	Login Ti Details Duration
Bressions test	Internal-GRP_POL_	WebVPN 15:	03:38 UTC Thu N Logout
L. SSO Statistics	0.89.116 WEB VPN-GRP	3DES 0h:	01m:18s Ping
To set	VPN sessions, right-click on the abov	ve table and select Table Sort (Order from popula menu
10000			,
Logou	it By: 🛛 All Sessions 💽 💌	Logout	Sessions
	<u>[</u>	Refresh	adated: 2/20/06 2:21:20 PM
Data Refreshed Successfully.	cisco N	NA (15)	B 3/30/06 3:05:21 PM UTC

調試WebVPN會話

此輸出是成功的WebVPN會話的調試示例。

附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊</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]
```

<u>疑難排解</u>

本節提供的資訊可用於對組態進行疑難排解。

- 如果WebVPN登入頁面上沒有Group下拉框,請確保您已完成<u>Enable WebVPN on the Outside</u> <u>Interface</u>下的步驟2,以及<u>Configure a Tunnel Group</u>下的步驟5。如果未完成這些步驟,並且缺 少下拉選單,則身份驗證將處於「預設組」之下,並且可能會失敗。
- 雖然您不能在ASDM或ASA上為使用者分配訪問許可權,但您可以限制在域控制器上具有 Microsoft Windows訪問許可權的使用者。為使用者身份驗證到的網頁新增必要的NT組許可權 。使用者使用組的許可權登入到WebVPN後,對指定頁面的訪問將相應地被授予或拒絕。 ASA僅代表域控制器充當代理身份驗證主機,此處的所有通訊都是NTLMv1。
- 無法為Sharepoint over WebVPN配置SSO,因為Sharepoint Server不支援基於表單的身份驗證。因此,此處不適用帶有post或post外掛過程的書籤。

相關資訊

- <u>Cisco ASA 5500系列調適型安全裝置</u>
- <u>技術支援與文件 Cisco Systems</u>