# 使用SDM的IOS上的SSL VPN客戶端(SVC)配置 示例

### 目錄

簡介 必要條件 需求 採用元件 網路圖表 預配置任務 慣例 背景資訊 配置IOS上的SVC 步驟1.在IOS路由器上安裝並啟用SVC軟體 步驟2.使用SDM嚮導配置WebVPN上下文和WebVPN網關 步驟3.為SVC使用者配置使用者資料庫 步驟4.配置向使用者公開的資源 結果 驗證 程式 指令 疑難排解 SSL連線問題

疑難排解指令

<u>相關資訊</u>

# <u>簡介</u>

SSL VPN客戶端(SVC)為與企業內部網路的安全通訊提供全通道。您可以按使用者配置訪問,也可以建立將一個或多個使用者放置到的不同WebVPN上下文。

以下IOS路由器平台支援SSL VPN或WebVPN技術:

• 870、1811、1841、2801、2811、2821、2851

• 3725、3745、3825、3845、7200和7301

您可以在以下模式下配置SSL VPN技術:

 無客戶端SSL VPN(WebVPN) — 提供需要啟用SSL的Web瀏覽器來訪問公司區域網(LAN)上的 HTTP或HTTPS Web伺服器的遠端客戶端。此外,無客戶端SSL VPN通過通用網際網路檔案 系統(CIFS)協定為Windows檔案瀏覽提供訪問許可權。Outlook Web Access(OWA)是HTTP訪 問的一個示例。請參閱使用SDM的Cisco IOS上的無客戶端SSL VPN(WebVPN)配置示例,瞭 解有關無客戶端SSL VPN的詳細資訊。

- · 瘦客戶端SSL VPN(埠轉發) 提供遠端客戶端,可下載基於Java的小程式,並允許使用靜 態埠號的傳輸控制協定(TCP)應用程式的安全訪問。存在點(POP3)、簡單郵件傳輸協定 (SMTP)、Internet郵件訪問協定(IMAP)、安全外殼(ssh)和Telnet都是安全訪問的示例。由於本 地電腦上的檔案發生更改,因此使用者必須具有本地管理許可權才能使用此方法。SSL VPN的 這種方法不適用於使用動態埠分配的應用程式,例如某些檔案傳輸協定(FTP)應用程式。請參閱 使用SDM的瘦客戶端SSL VPN(WebVPN)IOS配置示例,瞭解有關瘦客戶端SSL VPN的詳細資 訊。注意:不支援使用者資料包協定(UDP)。
- SSL VPN客戶端(SVC全通道模式) 將小型客戶端下載到遠端工作站,並允許對內部公司 網路上的資源進行完全安全訪問。您可以將SVC永久下載到遠端工作站,也可以在安全會話關 閉後刪除客戶端。

本文檔演示了用於SSL VPN客戶端的Cisco IOS路由器的配置。

### <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:

- Microsoft Windows 2000或XP
- •帶有SUN JRE 1.4或更高版本或ActiveX控制瀏覽器的Web瀏覽器
- 客戶端上的本地管理許可權
- <u>簡介</u>中列出的路由器之一,帶有高級安全映像(12.4(6)T或更高版本)
- 思科安全裝置管理員(SDM)版本2.3如果路由器上尚未載入Cisco SDM,您可以從<u>Software</u>
   <u>Download</u>(僅限註冊客戶)獲取軟體的免費副本。您必須擁有具有服務合約的CCO帳戶。有 關安裝和配置SDM的詳細資訊,請參閱<u>Cisco路由器和安全裝置管理器</u>。
- 路由器上的數位證書您可以使用永久的自簽名證書或外部證書頒發機構(CA)來滿足此要求。有 關永久性自簽名證書的詳細資訊,請參閱<u>永久性自簽名證書</u>。

#### <u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- •採用12.4(9)T的Cisco IOS路由器3825系列
- 安全裝置管理員(SDM)版本2.3.1

**注意:**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。

#### 網路圖表

本檔案會使用以下網路設定:



#### <u>預配置任務</u>

- 為SDM配置路由器。(可選)具有相應安全捆綁許可證的路由器已將SDM應用程式載入到快 閃記憶體中。請參閱<u>下載和安裝Cisco Router and Security Device Manager(SDM</u>),獲取並配 置軟體。
- 2. 將SVC副本下載到您的管理PC。您可以從<u>軟體下載</u>獲得SVC包檔案的副本:<u>Cisco SSL</u> VPN客戶端(僅限註冊客戶)。 您必須擁有具有服務合約的有效CCO帳戶。
- 3. 設定正確的日期、時間和時區,然後在路由器上配置數位證書。

#### <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>背景資訊</u>

SVC最初載入到WebVPN網關路由器上。每次客戶端連線時,SVC的副本都會動態下載到PC上。 若要更改此行為,請將路由器配置為使軟體永久保留在客戶端電腦上。

## 配置IOS上的SVC

本節提供設定本檔案中所述功能所需的步驟。此示例配置使用SDM嚮導在IOS路由器上啟用SVC操 作。

要在IOS路由器上配置SVC,請完成以下步驟:

- 1. 在IOS路由器上安裝並啟用SVC軟體
- 2. 使用SDM嚮導配置WebVPN上下文和WebVPN網關
- 3. 為SVC使用者配置使用者資料庫
- 4. <u>配置向使用者公開的資源</u>

### 步驟1.在IOS路由器上安裝並啟用SVC軟體

完成以下步驟,以便在IOS路由器上安裝和啟用SVC軟體:

1. 開啟SDM應用程式,按一下**Configure**,然後按一下**VPN**。

2.	展開WebVF	PN,然後選	擇Packag	es。				
	Sa Cisco Router a	nd Security Devic	e Manager (SDM	): 10.89.129	.170			
	File Edit View	Tools Help						
	🔥 Home	Configure	Monitor	@ Refresh	Gave Save	Q Search	? Help	Cisco Systems attlitumentItum
	Tasks	🚰 VPN						
	Interfaces and Connectors Frewall and RCL VPN Security Rudt Security Rudt WPN NRT NRT NRT Cusity of Service	VPN     Ste-to-S     Ste-t	ite VPN N Remote N Server Multipoint VPN PN Gateways	Cisco Wet You must in with this rou Install Status Cisco Sec You must in	bVPN Client Istall Cisco Iter. : Not Instal ure Desito Istall Cisco	Software	nt software for stall: wnload the ins t on the router <u>Hoad latest Cri</u> actify the curren	r clients to establish a full tunnel WebVPN session tallation bundle (pkg file) to your PC. If you already or on the PC, proceed to step 2. sco WebVPN client installation bundle. It location of the install bundle on your PC or on your t software: er on the router: filesh: gin installation. Install or WebVPN clients to use a Secure Desktop. tallation bundle (pkg file) to your PC. If you already or on the PC, proceed to step 2. t Cisco Secure Desktop (CSD) installation bundle. It location of the install bundle on your PC or on your
	NRC NRC				Lo De	cation of client	er on the router.	
	Additional Tasks					3. Chie	K install to be	gin installation. Install
	VPN	р <b>.</b>						17:30:14 UTC Thu Aug 03 2006 👩

3. 在Cisco WebVPN Client Software區域中,按一下**Browse**按鈕。系統將顯示Select SVC location對話方塊。



- 4. 按一下**My Computer**單選按鈕,然後按一下**Browse**以在管理PC上找到SVC包。
- 5. 按一下OK,然後按一下Install按鈕。



6. 按一下**Yes**,然後按一下**OK**。SVC包的成功安裝如下圖所示



#### 步驟2.使用SDM嚮導配置WebVPN上下文和WebVPN網關

完成以下步驟以配置WebVPN上下文和WebVPN網關:

- 1. 在路由器上安裝SVC後,按一下Configure,然後按一下VPN。
- 2. 按一下WebVPN,然後按一下Create WebVPN頁籤。



3. 選中Create a New WebVPN單選按鈕,然後按一下Launch the selected task。系統將顯示 WebVPN嚮導對話方塊。

WebVPN Wizard		×
WebVPN Wizard	Welcome to the Create WebVPN Wizard	
WebVPN Wizard	The New WebVPN wizard lets you to do the following: * Specify an IP address, name and digital certificate for the WebVPN. * Create users locally, and specify how these users should be authenticated. * Enable the router to download full-tunnel WebVPN client software to client PCs, for full-tunnel connectivity. * Specify the corporate intranet sites users are allowed to visit, and provide a link to their e-mail. * Customize the WebVPN portal page.	
	< Back Next Finish Cancel H	lelp

4. 按「**Next**」(下一步)。

WebVPN Wizard	
WebVPN Wizard	IP Address and Name This is the IP address users will enter to access the WebVPN portal page. If multiple WebVPN services are configured in this router, the unique name is used to distinguish the service. IP Address: 192.168.0.37
	▲ Information URL to login to this WebVPN service: https://192.168.0.37/sales
	< Back Nert> Finish Cancel Help

- 5. 輸入新WebVPN網關的IP地址,並為此WebVPN上下文輸入唯一名稱。您可以為同一IP地址 (WebVPN網關)建立不同的WebVPN上下文,但每個名稱都必須唯一。此範例使用以下IP位 址: https://192.168.0.37/sales
- 6. 按一下「Next」,然後繼續<u>步驟3</u>。

#### 步驟3.為SVC使用者配置使用者資料庫

對於身份驗證,您可以使用AAA伺服器、本地使用者或同時使用。此配置示例使用本地建立的使用 者進行身份驗證。

完成以下步驟,以便為SVC使用者配置使用者資料庫:

1. 完成<u>步驟2</u>後,按一下WebVPN Wizard User Authentication對話方塊中的**Locally on this router**單選按鈕。

WebVPN Wizard	
WebVPN Wizard	User Authentication  You can configure user accounts locally on this router. You can configure user accounts on a AAA server so that the router can contact this server to authenticate users when they try to log on. Specify how WebVPN should authenticate the users when they login.    External AAA server    Locally on this router:
	< Back Next > Finish Cancel Help

此對話方塊允許您向本地資料庫新增使用者。

2. 按一下「Add」,然後輸入使用者資訊。

Add an Account					
Enter the username and password					
Username:	ausnml				
Password					
Password	<none></none>				
New Password:	******				
Confirm New Password:	******				
Encrypt password using MD5 has	Encrypt password using MD5 hash algorithm				
Privilege Level: 15 💌					
OK Cancel	Help				

3. 按一下「OK」,然後根據需要新增使用者。

4. 新增必要的使用者後,按一下Next,然後繼續步驟4。

#### 步驟4.配置向使用者公開的資源

通過「配置Intranet網站WebVPN嚮導」對話方塊,您可以選擇要向SVC客戶端公開的Intranet資源 。

完成以下步驟,配置向使用者顯示的資源:

1. 完成<u>步驟3</u>後,按一下Configure Intranet Websites對話方塊中的Add按鈕。

WebVPN Wizard						
WebVPN Wizard	Configure Intranet Websites You can configure groups of intranet websites here. Each group can be given a heading and can contain one or more websites. Each of these groups will appear in the portal page as links that users can click to navigate to these sites. Add or select the group of websites you want to display in the portal page.					
	Action	URL List	Add			
		< Back Next >	Finish Cancel Help			

2. 輸入URL清單名稱,然後輸入標題。

Add URL List	t	
URL List Na Heading:	me: WebServers	(This will appear on Portal page)
Label SalesSite	URL Link http://172.22.1.10	Outlook Web Acces Add
	OK Cance	el Help

- 3. 按一下Add,然後選擇Website以新增您要向此客戶端公開的網站。
- 4. 輸入URL和連結資訊,然後按一下**OK**。
- 5. 要新增對OWA Exchange伺服器的訪問許可權,請按一下Add並選擇E-mail。

Add URL Lis	t						
URL List Name:		WebServers					
Heading:	Heading:		Intranet Web			(This will appear	r on Portal page
List of URLs	:						
Label	UR	L Link			0	utlook Web Acces	Add $ abla$
SalesSite	SalesSite http:		//172.22.1.10				Website
							E-mail
							201010-0
•					_	•	
		OK	1	Cancel	1	Help	
				ouncer			
選中Outlook W	eb Ac	cess覈耳	又方塊	,輸入UF	RL模		然後按一下 <b>確定</b>

Add URL Label:				
URL Label:	OWAServer			
URL Link:	http://172.22.1.20			
🔽 Outlook W	(Example: http://myintranet.mycompany.com/payroll) /eb Access			
	OK Cancel Help			

7. 新增所需的資源後,按一下**OK**,然後按一下**Next**。出現WebVPN嚮導全通道對話方塊。

WebVPN Wizard	x x x x x x x x x x x x x x x x x x x
WebVPN Wizard	Enable Full Tunnel     Enabling full tunnel downloads the WebVPN full tunnel client software to the client.     IP Address Pool     Create a new or select an existing address pool from which clients will be given an IP address     when they connect.     IP Address Pool:
	Full Tunnel Client Software is already installed in your router. Keep the Full Tunnel Client software installed on client's PC. Advanced Options Click Advanced Tunnel Options to configure split tunneling, split DNS, browser proxy settings, DNS and WINS servers.
	Advanced Tunnel Options
	< Back Next > Finish Cancel Help

- 8. 確認Enable Full Tunnel覈取方塊已勾選。
- 9. 建立此WebVPN上下文的客戶端可以使用的IP地址池。地址池必須對應您的Intranet上可用和可路由的地址。
- 10. 按一下IP Address Pool欄位**旁邊的省略號**(...),然後選擇Create a new IP Pool。



11. 在Add IP Local Pool對話方塊中,輸入池的名稱,然後按一下Add。

WebVPN Wizard		×
WebVPN Wizard	Enable Full Tunnel Enabling full tunnel downloads the WebVPN full tunnel client software to	the client.
A 8	Add IP Local Pool 🛛 🔀	
	Pool Name: Intranet	given an IP address
	Add IP address range	
	Pool Name: Intranet	
	Start IP address: 172.22.1.75	
	End IP address: 172.22.1.95	owser proxy
		Tunnel Options
	OK Cancel Help	
	OK Cancel Help	
	< Back Next > Finish	Cancel Help

- 12. 在新增IP地址範圍對話方塊中,輸入SVC客戶端的地址池範圍,然後按一下確定。註:IP地 址池應位於直接連線到路由器的介面範圍內。如果要使用不同的池範圍,可以建立一個與新 池關聯的環回地址以滿足此要求。
- 13. 按<u>一下「**OK**」(確定)。</u>

WebVPN Wizard	
WebVPN Wizard	Enable Full Tunnel Enabling full tunnel downloads the WebVPN full tunnel client software to the client.
	IP Address Pool         Create a new or select an existing address pool from which clients will be given an IP address when they connect.         IP Address Pool:       Intranet         IP Address Pool:
	Click Advanced Tunnel Options to configure split tunneling, split DNS, browser proxy settings, DNS and WINS servers.
	< Back Next > Finish Cancel Help

- 14. 如果您希望遠端客戶端永久儲存SVC副本,請按一下Keep the Full Tunnel Client Software installed on client's PC覈取方塊。清除此選項可要求客戶端在每次客戶端連線時下載SVC軟 體。
- 15. 配置高級隧道選項,例如拆分隧道、拆分DNS、瀏覽器代理設定以及DNS和WNS伺服器。思 科建議您至少配置DNS和WINS伺服器。要配置高級隧道選項,請完成以下步驟:按一下 Advanced Tunnel Options按鈕。

Advanced Tunnel Options			×
Split Tunneling Browser P	roxy Settings DNS and W	INS Servers	
DNS Servers		WINS Servers	
Primary DNS Server:	172.22.1.100	Primary WINS Server:	172.22.1.101
Secondary DNS Server:		Secondary WINS Server:	
Default Domain:			
	OK C	ancel Help	

按一下**DNS和WINS伺服器**頁籤,並輸入DNS和WINS伺服器的主IP地址。要配置拆分隧道和 瀏覽器代理設定,請按一下**拆分隧道**或**瀏覽器代理設定**頁籤。

Split Tunneling	Browser Proxy Settings DNS	and WINS Servers
Split Tunneli	ng	<sup>LC</sup> Split DNS
Select Include shown in the lis	or Exclude to configure the Netw st.	orks Use the corporate DNS server to resolve the domain names for the following domains. Other domains the client ISP DNS server will be used.
C Include Traf	ic <u>Learn Mo</u>	<u>e</u>
C Exclude Tra	ffic	
Destination Ne	tworks:	
IP Address	Mask Add.	
	Edit	
	Dele	
E Evolutie Loo	of I Ahie	Use semicolons (;) to separate entries.
	ALC: MAR	

- 16. 配置必要的選項後,按一下**下一步**。
- 17. 自定義WebVPN門戶頁面或選擇預設值。Customize WebVPN Portal Page允許您自定義 WebVPN Portal Page對客戶的顯示方式。

WebVPN Wizard	
WebVPN Wizard	Customize WebVPN Portal Page You can customize the WebVPN portal page that is displayed to users. You can select a predefined theme for the portal page. A theme defines colors for texts and background and a logo. You can create new themes, and customize colors, text and logo in Edit WebVPN mode. Theme: Open Highway
	CISCO SYSTEMS Web VPN Server
	Websites Internet Enter Web address (URL): Go
	< Back Net Finish Cancel Help

- 18. 配置WebVPN Portal Page後,按一下**Next**,按一下**Finish**,然後按一下**OK**。WebVPN嚮導 向路由器提交瀏覽命令。
- 19. 按一下「**OK**」以儲存組態。**注意:**如果收到錯誤消息,則WebVPN許可證可能不正確。下圖 顯示一條錯誤訊息範例 :

WebVPN Wizard						×
WebVPN Wizard	Summary of the Configu	ration				
	WebVPN Service Name WebVPN Policy Name WebVPN Gateway Name User Authentication Meth Intranet websites:	. sales : policy_1 e : gateway_1 nod List : Local Enabled				<
	URL List Name	:WebServers : OWAServer - http : SalesSite - http: o	o://172.22.1.30/e //172.22.1.10	exchange		
	SVC Status IP Address Poo Split Tunneling Split DNS Primary DNS Se Primary WINS S Install Full Tunn	'Yes I Intranet Disabled Disabled erver: 172.22. erver: 172.22. el Client Disable	1.100 1.101 ed			*
	DNS is not enabl recommended th	ed on your router. A at you enable DNS.	s some WebVP	N services req	uire DNS to v	≥ vork, it is
			< Back Next	Finish	Cancel	Help

要更正許可證問題,請完成以下步驟:按一下Configure,然後按一下VPN。展開 WebVPN,然後按一下Edit WebVPN頁籤。



突出顯示新建立的上下文,然後按一下Edit按鈕。

Edit WebVPN Context -sales			×
WebVPN Context     Group Policies     HTML Display Settings     NetBIOS Name Server Lis     Port Forward Lists     URL Lists     Cisco Secure Desktop	Name: Associated Gateway: Domain: Authentication List: Authentication Domain: I Enable Context Maximum Number of users: VRF Name: Default Group Policy:	sales   gateway_1   sales   sdm_vpn_xauth_ml_4   2 <none>   policy_1</none>	7
	OK Cancel	Help	

在最大使用者數欄位中,輸入許可證的正確使用者數。按一下「OK」,然後按一下「OK」。命令會寫入組態檔。按一下Save,然後按一下Yes接受更改。

### <u>結果</u>

ASDM建立以下命令列配置:

ausnml-3825-01
ausnml-3825-01# <b>show run</b>
Building configuration
Current configuration : 4393 bytes !
! Last configuration change at 22:24:06 UTC Thu Aug 3
2006 by ausnml
! NVRAM config last updated at 22:28:54 UTC Thu Aug 3
2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
boot-start-marker

```
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
no logging buffered
1
aaa new-model
!
!--- Added by SDM for local aaa authentication. aaa
authentication login sdm_vpn_xauth_ml_1 local aaa
authentication login sdm_vpn_xauth_ml_2 local aaa
authentication login sdm_vpn_xauth_ml_3 local aaa
authentication login sdm_vpn_xauth_ml_4 local ! aaa
session-id common ! resource policy ! ip cef ! ip domain
name cisco.com ! voice-card 0 no dspfarm !--- Digital
certificate information. crypto pki trustpoint TP-self-
signed-577183110 enrollment selfsigned subject-name
cn=IOS-Self-Signed-Certificate-577183110 revocation-
check none rsakeypair TP-self-signed-577183110 ! crypto
pki certificate chain TP-self-signed-577183110
certificate self-signed 01 3082024E 308201B7 A0030201
02020101 300D0609 2A864886 F70D0101 04050030 30312E30
2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274 69666963 6174652D 35373731 38333131 30301E17
0D303630 37323731 37343434 365A170D 32303031 30313030
30303030 5A303031 2E302C06 03550403 1325494F 532D5365
6C662D53 69676E65 642D4365 72746966 69636174 652D3537
37313833 31313030 819F300D 06092A86 4886F70D 01010105
0003818D 00308189 02818100 F43F6DD9 32A264FE 4C5B0829
698265DC 6EC65B17 21661972 D363BC4C 977C3810 !--- Output
suppressed. quit username wishaw privilege 15 secret 5
$1$r4CW$SeP6ZwQEAAU68W9kbR16U. username ausnml privilege
15 password 7 044E1F505622434B username sales privilege
15 secret 5 $1$/Lc1$K.Zt41zF1jSdKZrPgNK1A. username
newcisco privilege 15 secret 5
$1$Axlm$7k5PWspXKxUpoSReHo7IQ1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
ip virtual-reassembly duplex auto speed auto media-type
rj45 no keepalive ! interface GigabitEthernet0/1 ip
address 172.22.1.151 255.255.255.0 duplex auto speed
auto media-type rj45 !--- Clients receive an address
from this pool. ip local pool Intranet 172.22.1.75
172.22.1.95 ip route 0.0.0.0 0.0.0.0 172.22.1.1 ! ip
http server ip http authentication local ip http secure-
server ip http timeout-policy idle 600 life 86400
requests 100 ! control-plane ! line con 0 stopbits 1
line aux 0 stopbits 1 line vty 0 4 ! scheduler allocate
20000 1000 !--- Identify the gateway and port. webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint TP-self-signed-577183110
inservice !--- SVC package file. webvpn install svc
flash:/webvpn/svc.pkg ! !--- WebVPN context. webvpn
context sales title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all ! !---
Resources available to this context. url-list
"WebServers" heading "Intranet Web" url-text "SalesSite"
url-value "http://172.22.1.10" url-text "OWAServer" url-
value "http://172.22.1.20/exchange" ! nbns-list NBNS-
Servers nbns-server 172.22.1.15 master !--- Group policy
for the context. policy group policy_1 url-list
"WebServers" functions svc-enabled svc address-pool
"Intranet" svc default-domain "cisco.com" svc keep-
client-installed svc dns-server primary 172.22.1.100 svc
wins-server primary 172.22.1.101 default-group-policy
policy_1 aaa authentication list sdm_vpn_xauth_ml_4
```

```
gateway gateway_1 domain sales max-users 2 inservice ! !
end
```

# 驗證

使用本節內容,確認您的組態是否正常運作。

#### 程式

要測試配置,請在啟用SSL的客戶端Web瀏覽器中輸入http://192.168.0.37/sales。

### <u>指令</u>

有幾個**show**命令與WebVPN關聯。您可以在命令列介面(CLI)上執行這些命令,以顯示統計資訊和 其他資訊。有關**show**命令的詳細資訊,請參閱<u>驗證WebVPN配置</u>。

**註**: <u>Output Interpreter Tool(僅限註</u>冊客戶)(OIT)支援某些show命令。使用OIT檢視show命令輸出的 分析。

### <u>疑難排解</u>

使用本節內容,對組態進行疑難排解。

#### SSL連線問題

問題:SSL VPN客戶端無法連線路由器。

**解決方案:**IP地址池中的IP地址不足可能會導致此問題。增加路由器上IP地址池中的IP地址數量 ,以解決此問題。

#### <u>疑難排解指令</u>

有幾個**clear**命令與WebVPN關聯。有關這些命令的詳細資訊,請參閱<u>使用WebVPN Clear命令</u>。

有幾個debug命令與WebVPN關聯。有關這些命令的詳細資訊,請參閱使用WebVPN Debug命令。

**注意:**使用debug指令可能會對思科裝置造成負面影響。使用debug指令之前,請先參閱<u>有關</u> <u>Debug指令的重要資訊</u>。

## 相關資訊

- <u>Cisco IOS SSLVPN</u>
- <u>SSL VPN WebVPN</u>
- 使用SDM的Cisco IOS上的無客戶端SSL VPN(WebVPN)配置示例
- 使用SDM的瘦客戶端SSL VPN(WebVPN)IOS配置示例
- WebVPN和DMVPN融合部署指南
- 技術支援與文件 Cisco Systems