使用SDM配置瘦客户端SSL VPN(WebVPN)Cisco IOS

目录

简介 先决条件 要求 使用的组件 规则 配置 任务 网络图 配置瘦客户端 SSL VPN 配置 验证 检验配置 命令 故障排除 <u>用于排除故障的命令</u> 相关信息

<u>简介</u>

瘦客户端 SSL VPN 技术可用于允许使用静态端口的应用程序进行安全访问。例如,Telnet (23)、 SSH (22)、POP3 (110)、IMAP4 (143) 和 SMTP (25)。 瘦客户端可以由用户和/或策略驱动。可以 根据每个用户配置访问,也可以创建包含一个或多个用户的组策略。SSL VPN 技术可配置为三种主 要模式:无客户端 SSL VPN (WebVPN)、瘦客户端 SSL VPN(端口转发)和 SSL VPN 客户端 (SVC 全隧道模式)。

1. 无客户端 SSL VPN (WebVPN):

远程客户端只需一个启用了 SSL 的 Web 浏览器,便可访问公司局域网内启用了 http 或 https 的 Web 服务器。也可以使用通用 Internet 文件系统 (CIFS) 来访问浏览 Windows 文件。Outlook Web Access (OWA) 客户端是 http 访问的一个好例子。

请参阅<u>在 Cisco IOS 上使用 SDM 配置无客户端 SSL VPN (WebVPN) 的配置示例,以便了解有关</u> <u>无客户端 SSL VPN 的详细信息。</u>

2. 瘦客户端 SSL VPN(端口转发)

远程客户端必须下载一个基于 Java 的小程序,才能以安全方式访问使用静态端口号的 TCP 应用程序。不支持 UDP。示例包括对 POP3、SMTP、IMAP、SSH 和 Telnet 的访问。由于更改的是本地

计算机中的文件,因此用户需要具有本地管理权限。此 SSL VPN 方法不适用于使用动态端口分配 的应用程序,例如一些 FTP 应用程序。

3. SSL VPN 客户端(SVC 全隧道模式):

SSL VPN Client 将一个小客户端下载到远程工作站,从而允许对公司内部网络中的资源进行全面安全的访问。可将 SVC 永久下载到远程站,也可以在安全会话结束后将其删除。

请参阅<u>在 IOS 上使用 SDM 配置 SSL VPN 客户端 (SVC) 的配置示例,以便了解有关 SSL VPN 客</u> <u>户端的详细信息。</u>

本文档演示了在Cisco IOS®路由器上对瘦客户端SSL VPN进行的简^{单配}置。瘦客户端 SSL VPN 在 以下 Cisco IOS 路由器上运行:

- Cisco 870、1811、1841、2801、2811、2821 和 2851 系列路由器
- Cisco 3725、3745、3825、3845、7200 和 7301 系列路由器

<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:

Cisco IOS 路由器要求

- 以上列出的加载有 SDM 和 IOS 12.4(6)T 或更高版本的高级映像的任何路由器
- 加载有 SDM 的管理站Cisco 提供的新路由器附带有 SDM 的预安装副本。如果路由器未装有 SDM,可从<u>软件下载 - Cisco 安全设备管理器</u>获取该软件。您必须拥有一个已签署服务合同的 CCO 帐户。有关详细说明,请参阅使用安全设备管理器配置路由器。

客户端计算机要求

- •远程客户端应当具有本地管理特权;这不是必需的,但强烈建议进行此设置。
- 远程客户端必须安装有 Java Runtime Environment (JRE) 1.4 或更高版本。
- 远程客户端浏览器:Internet Explorer 6.0、Netscape 7.1、Mozilla 1.7、Safari 1.2.2 或 Firefox 1.0
- •已在远程客户端上启用 Cookie,并允许弹出窗口

<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 高级企业软件映像 12.4(9)T
- Cisco 3825 集成业务路由器
- Cisco Router and Security Device Manager (SDM) 2.3.1 版本

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。用于此配置 的 IP 地址来自 RFC 1918 地址空间。这些 IP 地址不能在 Internet 上合法使用。 有关文档约定的更多信息,请参考 Cisco 技术提示约定。

配置

<u>任务</u>

本部分包含在配置本文介绍的功能时所需要的信息。

网络图

本文档使用以下网络设置:



配置瘦客户端 SSL VPN

在 Cisco IOS 上使用安全设备管理器 (SDM) 界面中提供的向导配置瘦客户端 SSL VPN,或者在命 令行界面 (CLI) 中或在 SDM 应用程序中手动进行配置。本示例使用向导进行配置。

 选择 Configure(配置)选项卡。在导航窗格中,选择 VPN > WebVPN。单击 Create WebVPN 选项卡。单击 Create a new WebVPN 旁边的单选按钮。单击 Launch the selected task 按钮。



2. 此时将启动 WebVPN 向导。单击 Next。

WebVPN Wizard		
WebVPN Wizard	Welcome to the Create 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 Net Finish Cancel	Help

输入此 WebVPN 网关的 IP 地址和唯一名称。单击 Next。

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 Name: webvpn Enable secure SDM access through 192.168.0.37 Digital Certificate When users connect, this digital certificate will be sent to their web browser to authenticate the
	router. Certificate: ausnml-3825-01_Certificate
	Information URL to login to this WebVPN service: https://192.168.0.37/webvpn
	< Back Net Finish Cancel Help

3. 通过"User Authentication"屏幕可以对用户进行身份验证。此配置使用在路由器本地创建的帐 户。也可以使用验证、授权和记账 (AAA) 服务器。要添加用户,请单击 Add。在"Add an Account"屏幕上输入用户信息,然后单击 OK。在"User Authentication"屏幕上单击 Next。

WebVPN Wizard		×
WebVPN Wizard	User Authentication You can configure user accounts locally on this router. You can configure user accounts on AAA server so that the router can contact this server to authenticate users when they try to lo on. Specify how WebVPN should authenticate the users when they login.	a g
	Add an Account Enter the username and password Username: ausnml Password Password Password New Password: ***** Confirm New Password: ***** Encrypt password using MD5 hash algorithm Privilege Level: 1 OK Cancel	
	< Back Next > Finish Cancel Hel	р

通过"WebVPN Wizard"屏幕可以配置 Intranet 网站,但由于此应用程序访问使用端口转发,因此将省略此步骤。如果希望允许访问网站,请使用无客户端或完全客户端 SSL VPN 配置,这些配置不在本文档的论述范围内。

WebVPN Wizard			
WebVPN Wizard	Configure Intranet We You can configure grou can contain one or mor links that users can clic Add or select the group	absites ups of intranet websites here. Each group can be given re websites. Each of these groups will appear in the po ck to navigate to these sites. o of websites you want to display in the portal page.	a heading and ortal page as
ACCE	Action	URL List	Add
			Edit
			Delete
4			
		<back next=""> Finish C</back>	ancel Help

单击 Next。向导随即显示允许配置全隧道客户端的屏幕。这不适用于瘦客户端 SSL VPN(端 口转发)。取消选中 Enable Full Tunnel。单击 Next。

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:
	The full tunnel client software should be installed on your router, so that it can be downloaded by clients when they connect to WebVPN service on this router. Specify the location of the full tunnel software install bundle. Location: Download latest Full Tunnel client install bundle.
	Keep the Full Tunnel Client software installed on client's PC. Click Advanced Tunnel Options to configure split tunneling, split DNS, browser proxy settings, DNS and WINS servers.
	Advanced Tunnel Options < Back Nert> Finish Cancel Help

4. 自定义 WebVPN 门户页面的外观或接受默认外观。单击 Next。

WebVPN Wizard		
WebVPN Wizard	Customize WebVPN Portal Page You can customize the WebVPN portal page that is displayed to users. You can sele predefined theme for the portal page. A theme defines colors for texts and backgrour logo. You can create new themes, and customize colors, text and logo in Edit WebVP Theme: Open Highway Preview: Ocean Breeze Desert Sands Festival	cta Id and a 'N mode.
	CISCO SYSTEMS Web VPN Server	
	Websites	
	Internet	
	Enter Web address (URL): Go	
	< Back Next > Finish Cancel	Help

预览"Summary of the Configuration",然后单击 Finish > Save。

WebVPN Wizard	
WebVPN Wizard	Summary of the Configuration
	WebVPN Service Name : webvpn WebVPN Policy Name : policy_1 WebVPN Gateway Name : gateway_1 User Authentication Method List : Local Intranet websites: Disabled Full Tunnel Configuration SVC Status : No IP Address Pool : <none> Split Tunneling : Disabled Split DNS : Disabled Install Full Tunnel Client : Disabled</none>
	DNS is not enabled on your router. As some WebVPN services require DNS to work, it i recommended that you enable DNS.
	< Back Next > Finish Cancel Help

5. 此时,您已创建 WebVPN 网关,并且已将 WebVPN 上下文与组策略相连接。配置瘦客户端 端口,可在客户端连接到 WebVPN 时使用这些端口。选择 Configure。选择 VPN > WebVPN。选择 Create WebVPN。选择 Configure advanced features for an existing WebVPN 单选按钮,然后单击"Launch the selected task"。



"Welcome"屏幕提供向导功能要点。单击 Next。

WebVPN Wizard		X
WebVPN Wizard	Welcome to the Advanced WebVPN Wizard	
	The Advanced WebVPN wizard lets you configure advanced features for an existing WebVPN. You can use this wizard to do the following:	
.DA	* Configure links in the portal page to intranet websites and web-enabled applications such as Microsoft Office Outlook e-mail.	
	* Configure the router to operate in thin client mode. This mode supports port forwarding, which enables users to run client applications on their PCs and securely connect to corporate servers.	
A BY	* Enable the router to download full-tunnel WebVPN client software on users PCs, giving them full-tunnel connectivity.	
	* Enable the router to download Cisco Secure Desktop software on users PCs.	
	* Configure the router to use the Common Internet File System (CIFS).	
	* Enable clientless Citrix by configuring the router with the URLs for Citrix servers.	
	< Back Ner Finish Cancel He	elp

从下拉菜单选择 WebVPN 上下文和用户组。单击 Next。

WebVPN Wizard			\mathbf{X}
WebVPN Wizard	Select the WebVP Select the WebVPN additional advance First select the Web WebVPN: User Group:	PN user group N and the user group within that WebVPN for whom you want to con- ted features. ebVPN where the user group is defined and then select the user gro webvpn policy_1 T	figure Iup.
	Default Group:	policy_1	
		< Back Nert> Finish Cancel	Help

选择 Thin Client (Port Forwarding),**然后单击**"Next"。

WebVPN Wizard



×

输入希望通过端口转发使用的资源。服务端口必须是静态端口,但也可以接受向导分配的客户端 PC 上的默认端口。单击 Next。

WebVPN	Wizard	Thin Client (Port Thin client enabl servers in corpor public PC that co Specify the serve access to.	t Forwardii ed WebVP rate netwo nnects to a ers and por	ng) N users to run client app rk, For example clients c an e-mail (IMAP, SMTP) : t numbers of application	olications on their PCs an ould run an email client a server on the corporate r is you want WebVPN use	nd connect to application on a ietwork. ers to have
	12	Server	Port	Port on Client PC	Description	Add
-	100	172.22.1.50	25	3000	Email	
	-0. L.	172.22.1.30	23	3001	Router1	Edit
Carlos In	6	172.22.1.10	22	3003	Router2 SSH	Datata
	Add Port For	warding Server				Delete
	Server IP Add	ress: 172.2	22.1.20			
19	service is liste Port on Client	ening: 110 tPC: 3002	<u> </u>	_earn more.	IP address of	your SMTP
	Description:	Pop3	Email			
			Cancel	Help		
				< Ba	ck Next > Finish	Cancel Help

预览配置摘要,然后单击 Finish > OK > Save。



<u>配置</u>

SDM 配置的结果。

ausnml-3825-01
Building configuration
Current configuration : 4343 bytes
! Last configuration change at 15:55:38 UTC Thu Jul 27
2006 by ausnml
! NVRAM config last updated at 21:30:03 UTC Wed Jul 26
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
enable secret 5 \$1\$KbIu\$508qKYAVpWvyv9rYbrJLi/

```
aaa new-model
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
resource policy
ip cef
ip domain name cisco.com
voice-card 0
no dspfarm
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 !---- cut for
brevity quit ! username ausnml privilege 15 password 7
15071F5A5D292421 username fallback privilege 15 password
7 08345818501A0A12 username austin privilege 15 secret 5
$1$3xFv$W0YUsKDx1adDc.cVQF2Ei0 username sales_user1
privilege 5 secret 5 $1$2/SX$ep4fsCpodeyKaRji2mJkX/
username admin0321 privilege 15 secret 5
$1$FxzG$cQUJeUpBWgZ.scSzOt8Ro1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! 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 exec-timeout 40 0 privilege
level 15 password 7 071A351A170A1600 transport input
telnet ssh line vty 5 15 exec-timeout 40 0 password 7
001107505D580403 transport input telnet ssh ! scheduler
allocate 20000 1000 !--- the WebVPN Gateway webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint ausnml-3825-
01_Certificate inservice !--- the WebVPN Context webvpn
context webvpn title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all !---
resources available to the thin-client port-forward
"portforward_list_1" local-port 3002 remote-server
"172.22.1.20" remote-port 110 description "Pop3 Email"
local-port 3001 remote-server "172.22.1.30" remote-port
23 description "Router1" local-port 3000 remote-server
"172.22.1.50" remote-port 25 description "Email" local-
port 3003 remote-server "172.22.1.10" remote-port 22
description "Router2 SSH" !--- the group policy policy
group policy_1 port-forward "portforward_list_1"
default-group-policy policy_1 aaa authentication list
sdm_vpn_xauth_ml_2 gateway gateway_1 domain webvpn max-
users 2 inservice ! end
```



检验配置

使用本部分可确认配置能否正常运行。

1. 使用客户端计算机访问位于 https://gateway_ip_address 的 WebVPN 网关。如果创建唯一的 WebVPN 上下文,请切记包括 WebVPN 域名。例如,如果创建了称为"sales"的域,请输入 https://gateway_ip_address/sales。

🕙 WebVPN Service - Microsoft Internet Explorer 📃 🗖 🔀
File Edit View Favorites Tools Help
😋 Back • 🐑 - 🖹 🗟 🏠 🔎 Search 🧙 Favorites 🊱 😒 - 嫨 🗹 • 🗔 🏭 🐢
Address 🕘 https://192.168.0.37/webvpn.html
Google - 📉 💽 Search 🔹 🏈 🖓 🔁 Popups okay 👋 Check 🔹 🔍 AutoLink 🗠 »
Cisco Statena WebVPN Service
Login
Please enter your username and password
Username: ausnmi
Password: ••••••
Login Clear
🔄 Done 🔲 🔒 🜒 Internet

2. 登录并接受 WebVPN 网关提供的证书。单击 Start Application Access。

WebVPN Service - Microsoft Internet Explorer		
File Edit View Favorites Tools Help		<u>Ay</u>
🎯 Back 🝷 🕥 - 💌 🗟 🏠 🔎 Search 🖕	Favorites 🚱 🔗 嫨 👿 🔹	<mark></mark> 🗶 🥥 🚳
Address 🕘 https://192.168.0.37/index.html		🖌 🄁 Go 🛛 Links 🍟
Google - ⊂ G Search - ⊘	🄝 🛃 Popups okay 😽 Check 🔹	AutoLink - »
CISCO SYSTEMS WebVPN Service		
If the Floating Toolbar does not open, click here to open it. Start Application Access		
2 ¹		
Websites		
Enter Web Address (URL)	https://192.168 Image: Start Application Access Start Application Access Enter Web Address (URL) Go	Go
interps://192.168.0.37/tcp/index.html		Dinternet

3. 此时将显示"Application Access"屏幕。可使用本地端口号和本地环回 IP 地址访问应用程序。 例如,要远程登录到路由器 1,请输入 telnet 127.0.0.1 3001。Java 小程序将此信息发送到 WebVPN 网关,然后,该网关尝试以安全方式将消息发送到会话两端。成功连接可导致 Bytes Out 和"Bytes In"列增大。 🐔 https://192.168.0.37 - Application Access - Microsoft Internet Ex... 💶 🗔 🔀 Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications. If you shut down your computer without closing this window, you might later have problems running the applications listed below. Click here for details. Bytes Out Bytes In Local Remote Sockets Name Pop3 Email 127.0.0.1:3002 172.22.1.20:110 0 0 0 ol 0 0 Router 1 127.0.0.1:3001 172.22.1.30:23 Email 127.0.0.1:3000 172.22.1.50:25 0 0 0 Router2 SSH 127.0.0.1:3003 172.22.1.10:22 0 0 0 Click to activate and use this control **Reset byte counts** e Internet

命令

有若干 show 命令与 WebVPN 关联。可以在命令行界面 (CLI) 上执行这些命令以显示统计信息和其 他信息。要详细查看 show 命令的用法,请参阅<u>验证 WebVPN 配置</u>。

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

<u>故障排除</u>

使用本部分可排除配置故障。

客户端计算机必须加载有 SUN Java 1.4 版或更高版本。可从 Java 软件下载获取此软件的副本

<u>用于排除故障的命令</u>

注意:在使用debug命令之前,请参阅Importent Information。

- show webvpn -有许多与WebVPN相关的show命令。可在 CLI 中执行这些命令,以便显示统计 信息和其他信息。要详细查看 show 命令的用法,请参阅<u>验证 WebVPN 配置。</u>
- **debug webvpn** -使用debug命令**可**能对路由器造成负面影响。要更详细地查看 **debug 命令的用** 法,请参阅<u>使用 WebVPN Debug 命令。</u>



- <u>Cisco IOS SSLVPN</u>
- SSL VPN WebVPN
- Cisco IOS WebVPN 问与答
- <u>技术支持和文档 Cisco Systems</u>