Configurer Cisco IOS VPN SSL client léger (WebVPN) avec SDM

Contenu

Introduction Conditions préalables **Conditions requises Components Used Conventions** Configuration Tâche Diagramme du réseau Configuration du VPN SSL client léger Configuration Vérification Vérifier votre configuration Commandes Dépannage Commandes utilisées pour dépanner Informations connexes

Introduction

La technologie VPN SSL client léger peut être utilisée pour permettre un accès sécurisé aux applications qui utilisent des ports statiques. Exemples : Telnet (23), SSH (22), POP3 (110), IMAP4 (143) et SMTP (25). Le client léger peut être piloté par l'utilisateur, piloté par des politiques, ou les deux. L'accès peut être configuré utilisateur par utilisateur, ou des stratégies de groupe qui incluent un ou plusieurs utilisateurs peuvent être créées. La technologie VPN SSL peut être configurée en trois modes principaux : VPN SSL sans client (WebVPN), VPN SSL client léger (transfert de port) et client VPN SSL (mode tunnel SVC-Full).

1. VPN SSL sans client (WebVPN) :

Un client distant a seulement besoin d'un navigateur Web compatible SSL pour accéder à des serveurs Web HTTP ou HTTPS sur le LAN de l'entreprise. L'accès est également disponible pour parcourir des fichiers Windows avec le système de fichiers Common Internet File System (CIFS). Un bon exemple d'accès HTTP est le client Outlook Web Access (OWA).

Référez-vous à <u>Exemple de configuration de VPN SSL sans client (WebVPN) sur Cisco IOS</u> <u>utilisant SDM</u> afin d'en savoir plus sur le VPN SSL sans client.

2. VPN SSL client léger (transfert de port)

Un client distant doit télécharger un petit applet Javas pour l'accès sécurisé des applications TCP qui utilisent des numéros de port statiques. UDP n'est pas pris en charge. Les exemples incluent l'accès à POP3, SMTP, IMAP, SSH et Telnet. L'utilisateur doit disposer de privilèges d'administration locaux parce que des modifications sont apportées à des fichiers sur l'ordinateur local. Cette méthode de VPN SSL ne fonctionne pas avec les applications qui utilisent des affectations de ports dynamiques, par exemple, plusieurs applications FTP.

3. Client VPN SSL (mode de tunnel SVC-Full) :

Le client VPN SSL télécharge un petit client sur le poste de travail distant et permet un accès total et sécurisé aux ressources sur le réseau d'entreprise interne. Le SVC peut être téléchargé de manière permanente sur le poste de travail distant, ou il peut être supprimé après la fin de la session sécurisée.

Référez-vous à <u>Exemple de configuration du client VPN SSL (SVC) sur IOS à l'aide de SDM</u> afin d'en savoir plus sur le client VPN SSL.

Ce document présente une configuration simple pour le VPN SSL client léger sur un routeur Cisco IOS[®]. Le VPN SSL client léger s'exécute sur les routeurs Cisco IOS suivants :

- Routeurs de la gamme Cisco 870, 1811, 1841, 2801, 2811, 2821 et 2851
- Routeurs de la gamme Cisco 3725, 3745, 3825, 3845, 7200 et 7301

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

Configuration requise pour le routeur Cisco IOS

- Tous les routeurs répertoriés chargés avec SDM et une image avancée d'IOS version 12.4(6)T ou ultérieure
- Station de gestion chargée avec SDMCisco fournit de nouveaux routeurs avec une copie préinstallée de SDM. Si SDM n'est pas installé sur votre routeur, vous pouvez obtenir le logiciel sur <u>Software Download-Cisco Security Device Manager</u>. Vous devez posséder un compte CCO avec un contrat de service. Référez-vous à <u>Configurer votre routeur avec</u> <u>Security Device Manager</u> pour des instructions détaillées.

Configuration requise pour les ordinateurs clients

- Les clients distants doivent disposer de privilèges d'administration locaux ; il n'est pas nécessaire, mais il est fortement suggéré.
- Les clients distants doivent disposer de Java Runtime Environment (JRE) version 1.4 ou ultérieure.
- Navigateurs clients distants : Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 ou Firefox 1.0
- Cookies activés et fenêtres publicitaires intempestives autorisées sur les clients distants

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Image logicielle Cisco Advanced Enterprise 12.4(9)T
- Routeur à services intégrés Cisco 3825
- Cisco Router and Security Device Manager (SDM) version 2.3.1

The information in this document was created from the devices in a specific lab environment. Tous les périphériques utilisés dans ce document ont commencé par une configuration effacée (par défaut). If your network is live, make sure that you understand the potential impact of any command. Les adresses IP utilisées pour cette configuration proviennent de l'espace d'adressage RFC 1918. Ils ne sont pas légaux sur Internet.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Configuration

Tâche

Cette section contient les informations requises pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration du VPN SSL client léger

Utilisez l'Assistant fourni dans l'interface SDM (Security Device Manager) pour configurer le VPN SSL client léger sur Cisco IOS, ou configurez-le soit à l'interface de ligne de commande (CLI), soit manuellement dans l'application SDM. Cet exemple utilise l'Assistant.

 Sélectionnez l'onglet Configurer.Dans le volet de navigation, sélectionnez VPN > WebVPN.Cliquez sur l'onglet Create WebVPN.Activez la case d'option en regard de Create a new WebVPN.Cliquez sur le bouton Lancer la tâche



 L'Assistant WebVPN démarre. Cliquez sur Next (Suivant).

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 nert=""> Finish Cancel</back>	Help

Entrez l'adresse IP et un nom unique pour cette passerelle WebVPN. Cliquez sur **Next** (Suivant).

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					
	Digital Certificate When users connect, this digital certificate will be sent to their web browser to authenticate the router. Certificate: ausnml-3825-01. Certificate					
<u>A</u>	URL to login to this WebVPN service: https://192.168.0.37/webvpn					
	< Back Netz> Finish Cancel Help					

3. L'écran User Authentication (Authentification utilisateur) permet de fournir l'authentification des utilisateurs. Cette configuration utilise un compte créé localement sur le routeur. Vous pouvez également utiliser un serveur AAA (Authentication, Authorization, and Accounting).Pour ajouter un utilisateur, cliquez sur Ajouter.Entrez les informations utilisateur dans l'écran Ajouter un compte, puis cliquez sur OK.Cliquez sur Suivant dans l'écran Authentification utilisateur.

	34
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. Add an Account Enter the username and password Username: ausnml
	Password Password Add Password New Password: ***** Confirm New Password: ***** Edit
	Privilege Level: OK Cancel Help < Back Next > Finish Cancel Help

L'écran WebVPN Wizard permet de configurer des sites Web intranet, mais cette étape est omise car Port-Forwarding est utilisé pour cet accès d'application. Si vous souhaitez autoriser l'accès à des sites Web, utilisez les configurations VPN SSL sans client ou client complet, qui ne sont pas dans le champ d'application de ce document.

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	bsites ps of intranet websites e websites. Each of the k to navigate to these s of websites you want to	here. Each group c se groups will appo ites. o display in the port	an be given a h sar in the portai al page.	eading and page as
	Action		URL List		Add
					Edit
					Delete
			< Back Next >	Finish Cano	el Help

Cliquez sur **Next** (Suivant). L'Assistant affiche un écran qui permet de configurer le client Full Tunnel. Cela ne s'applique pas au VPN SSL client léger (transfert de port).Désélectionnez **Activer le tunnel complet**. Cliquez sur **Next** (Suivant).

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 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: Browse Download latest Full Tunnel client install bundle.
	Click Advanced Tunnel Options to configure split tunneling, split DNS, browser proxy settings, DNS and WINS servers.
	< Back Nert> Finish Cancel Help

 Personnalisez l'apparence de la page du portail WebVPN ou acceptez l'apparence par défaut.Cliquez sur Next (Suivant).

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 at logo. You can create new themes, and customize colors, text and logo in Edit WebVPN m Theme: Open Highway Open Highway Ocean Breeze Desert Sands Festival Cisco Systems Web VPN Server I the Floating Toolbar does not open, click here to open if Websites	nd a hode.
	Internet Enter Web address (URL): Go	
	< Back Next > Finish Cancel H	lelp

Affichez un aperçu du récapitulatif de la configuration et cliquez sur **Terminer > Enregistrer**.

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>	
1		>
H	DNS is not enabled on your router. As some WebVPN services require DNS to recommended that you enable DNS.	work, it is
	< Back Next > Finia Cancel	Help

5. Vous avez créé une passerelle WebVPN et un contexte WebVPN avec une stratégie de groupe liée. Configurez les ports client léger, qui sont rendus disponibles lorsque les clients se connectent au WebVPN.Choisissez Configurer.Choisissez VPN > WebVPN.Choisissez Create WebVPN.Sélectionnez la case d'option Configurer les fonctionnalités avancées pour un WebVPN existant et cliquez sur Lancer la tâche sélectionnée.



L'écran Welcome (Bienvenue) présente les fonctionnalités de l'Assistant. Cliquez sur **Next** (Suivant).

WebVPN Wizard	
WebVPN Wizard	Welcome to the Advanced WebVPN Wizard
a la	The Advanced WebVPN wizard lets you configure advanced features for an existing WebVPN. You can use this wizard to do the following:
.De	* 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.
	* 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 Next Finish Cancel Help

Sélectionnez le contexte WebVPN et le groupe d'utilisateurs dans les menus déroulants. Cliquez sur **Next** (Suivant).

WebVPN Wizard		
WebVPN Wizard	Select the WebVPN Select the WebVPN additional advance First select the Web WebVPN:	N user group I and the user group within that WebVPN for whom you want to configure d features. bVPN where the user group is defined and then select the user group. webvpn
	User Group: Default Group:	policy_1
		< Back Nett> Finish Cancel Help

Choisissez Client léger (Transfert de port) et cliquez sur Suivant.

WebVPN Wizard



Saisissez les ressources que vous souhaitez rendre disponibles via Port Forwarding. Le port de service doit être un port statique, mais vous pouvez accepter le port par défaut sur le PC client attribué par l'Assistant. Cliquez sur **Next** (Suivant).

Webvpn Wi	zard					
WebVPN	Wizard	Thin Client (Po Thin client ena servers in corp public PC that Specify the ser access to.	ort Forwardin bled WebVP orate networ connects to a vers and por	ng) N users to run client ap; rk, For example clients c an e-mail (IMAP, SMTP) : t numbers of applicatior	olications on their PCs a ould run an email client server on the corporate 1s you want WebVPN us	and connect to application on a network. sers to have
THAN .	111	Server	Port	Port on Client PC	Description	Add
		172.22.1.50	25	3000	Email	
12UN	AL LA	172.22.1.30	23	3001	Router1	Edit
17 Ale	പ്	172.22.1.10	22	3003	Router2 SSH	Dalata
	Add Port For	warding Serve	r			Delete
	Server IP Add	ress: 172	22.1.20			
	Server port on service is liste	which ening: 110				
1º	Port on Client	PC: 300	12 <u>I</u>	_earn more.	IP address o	fyour SMTP
<u> </u>	Description:	Pop	3 Email			
	2	ок	Cancel	Help		
				< Ba	ck Next > Finish	Cancel Help

Affichez un aperçu de votre configuration et cliquez sur **Terminer > OK > Enregistrer**.



Configuration

Résultats de la configuration SDM.

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
1
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname ausnml-3825-01
1
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
1
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
```

Vérification

Vérifier votre configuration

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

 Utilisez un ordinateur client pour accéder à la passerelle WebVPN à l'adresse https://gateway_ip_address. N'oubliez pas d'inclure le nom de domaine WebVPN si vous créez des contextes WebVPN uniques. Par exemple, si vous avez créé un domaine appelé ventes, saisissez

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 - 🖌 C Search - 🏈 🐲 🗗 Popups okay 👋 Check - 🖄 AutoLink - »
Cisco Systems WebVPN Service
Login Please enter your username and password Username: ausnml Password: •••••• Login Clear
Done

 Connectez-vous et acceptez le certificat offert par la passerelle WebVPN. Cliquez sur Start Application Access.

WebVPN Service - Microsoft Internet Explorer		
File Edit View Favorites Tools Help		A
🎯 Back 🔹 🕥 - 💌 🗟 🏠 🔎 Search 🦻	Favorites 🚱 🔗 🌺 👿 -	, 🎎 🥥 🦓
Address 🕘 https://192.168.0.37/index.html		
Google - G Search - C	🔊 🛷 🛃 Popups okay 👋 Check 🔹 🔍	AutoLink 🔹 🍽
CISCO SYSTEMS WebVPN Service	[286×
If the Floating Toolbar does not open, click here to open it. Start Application Access		
Websites		
Enter Web Address (URL)	https://192.168 Image: Start Application Access Enter Web Address (URL) Go	G0

3. Un écran Application Access s'affiche. Vous pouvez accéder à une application avec le numéro de port local et votre adresse IP de bouclage local. Par exemple, pour établir une connexion Telnet avec le routeur 1, entrez telnet 127.0.0.1 3001. La petite applet Java envoie ces informations à la passerelle WebVPN, qui relie ensuite les deux extrémités de la session de manière sécurisée. Les connexions réussies peuvent entraîner l'augmentation des colonnes Bytes Out et Bytes In.

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 Local Remote Bytes In Sockets Name Pop3 Email 127.0.0.1:3002 172.22.1.20:110 0 0 0 ol 127.0.0.1:3001 172.22.1.30:23 0 0 Router 1 0 0 Email 127.0.0.1:3000 172.22.1.50:25 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

Commandes

Plusieurs **commandes show sont associées à WebVPN.** Vous pouvez exécuter ces commandes dans l'interface de ligne de commande (CLI) afin d'afficher les statistiques et autres informations. Pour voir l'utilisation des commandes **show** en détail, référez-vous à <u>Vérification de la</u> <u>configuration WebVPN</u>.

L'<u>Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines</u> <u>commandes show.</u> Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Dépannage

Utilisez cette section pour dépanner votre configuration.

Les ordinateurs clients doivent être chargés avec SUN Java Version 1.4 ou ultérieure. Obtenir une copie de ce logiciel à partir du <u>téléchargement de logiciels Java</u>

Commandes utilisées pour dépanner

Remarque : reportez-vous à <u>Informations importantes sur les commandes de débogage</u> avant d'utiliser les commandes **de débogage**.

• show webvpn ?---Il existe de nombreuses commandes show associées à WebVPN. Elles

peuvent être effectuées à l'interface de ligne de commande pour afficher des statistiques et d'autres informations. Afin de voir l'utilisation des commandes **show** en détail, référez-vous à <u>Vérification de la configuration WebVPN</u>.

• debug webvpn ?—L'utilisation des commandes debug peut avoir un impact négatif sur le routeur. Afin de voir l'utilisation des commandes de débogage plus en détail, référez-vous à <u>Utilisation des commandes de débogage WebVPN.</u>

Informations connexes

- <u>Cisco IOS SSLVPN</u>
- VPN SSL WebVPN
- Questions et réponses sur Cisco IOS WebVPN
- Support et documentation techniques Cisco Systems