SDMによるシンクライアントSSL VPN(WebVPN)Cisco IOSの設定

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 表記法 設定 タスク ネットワーク図 シンクライアント SSL VPN の設定 コンフィギュレーション 確認 設定の確認 コマンド トラブルシュート トラブルシューティングに使用するコマンド 関連情報

概要

シンクライアント SSL VPN テクノロジーを使用して、スタティック ポートを使用するアプリケ ーションにセキュアなアクセスが可能です。セキュアなアクセスの例としては、Telnet (23)、 SSH (22)、POP3 (110)、IMAP4 (143)、および SMTP (25) があります。 シンクライア ントは、ユーザ主導、ポリシー主導、またはその両方の場合があります。アクセス権はユーザ単 位で設定でき、また 1 人以上のユーザを含むグループ ポリシーを作成できます。SSL VPN テク ノロジーは 3 種類の主要なモードで設定できます。、すなわち、クライアントレス SSL VPN (WebVPN)、シンクライアント SSL VPN (ポート フォワーディング)、および SSL VPN クライアント (SVC フル トンネル モード)です。

1.クライアントレスSSL VPN(WebVPN):

リモート クライアント側で必要になるのは、企業 LAN 上にある http 対応または https 対応 Web サーバにアクセスするための SSL 対応 Web ブラウザだけです。このアクセスは、Common Internet File System (CIFS)による Windows ファイルのブラウズに利用可能です。http アクセ スの例としては、Outlook Web Access (OWA) クライアントが挙げられます。

クライアントレス SSL VPN についての詳細は、『<u>』を参照してください。</u>

2. シンクライアント SSL VPN (ポート フォワーディング)

リモート クライアントにサイズの小さい Java ベースのアプレットをダウンロードすることで、 静的ポート番号を使用する TCP アプリケーションの安全なアクセスを実現します。UDP はサポ ートされていません。このアクセス方法の例としては、POP3、SMTP、IMAP、SSH、および Telnet が挙げられます。ローカル マシン上のファイルに変更が加えられるため、ユーザにローカ ル管理者権限が必要になります。この SSL VPN 方式は、一部の FTP アプリケーションなど、動 的ポート割り当てを使用するアプリケーションでは使用できません。

3. SSL VPN Client (SVCフルトンネルモード):

SSL VPN クライアントがリモート ワークステーションにスモール クライアントをダウンロード することで、社内ネットワーク上のリソースへの安全な完全アクセスを実現します。SVC はリモ ート ステーションにダウンロードしたままにしておくことも、安全なセッションの終了後に削除 することも可能です。

SSL VPN Client の詳細は、『<u>SDM を使用した IOS での SSL VPN Client(SVC)の設定例</u>』を参 照してください。

このドキュメントでは、Cisco IOS® ルータでのシンクライアント SSL VPN の簡単な設定を示し ます。シンクライアント SSL VPN は次の Cisco IOS ルータで動作します。

- Cisco 870、1811、1841、2801、2811、2821、および 2851 シリーズ ルータ
- Cisco 3725、3745、3825、3845、7200、および 7301 シリーズ ルータ

<u>前提条件</u>

<u>要件</u>

この設定を行う前に、次の要件が満たされていることを確認します。

Cisco IOS ルータの要件

- リストされたルータのいずれかで、SDM および IOS バージョン 12.4(6)T 以降の拡張イメージがロードされていること
- SDM をロードした管理ステーションシスコでは SDM のコピーをプリインストールした新し いルータを出荷しています。ご使用のルータに SDM がインストールされていない場合は、 [Software Download-Cisco Security Device Manager] でソフトウェアを入手できます。サー ビス契約を結んでいる Cisco.com アカウントが必要です。詳細手順は、『Security Device Manager でのルータの設定』を参照してください。

クライアント コンピュータの要件

- リモート クライアントには、ローカルの管理者権限があること。これは必須事項ではありま せんが、重要な推奨事項です。
- リモート クライアントには、Java Runtime Environment(JRE)バージョン 1.4 以降が必要です。
- ・リモート クライアント ブラウザ: Internet Explorer 6.0、Netscape 7.1、Mozilla 1.7、Safari 1.2.2、Firefox 1.0 のいずれか
- リモート クライアントでクッキーがイネーブルにされており、ポップアップが許可されていること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Advanced Enterprise ソフトウェア イメージ 12.4(9)T
- Cisco 3825 サービス統合型ルータ
- Cisco Router and Security Device Manager (SDM) バージョン 2.3.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在 的な影響について確実に理解しておく必要があります。この設定に使用されている IP アドレスは RFC 1918 アドレス スペースからのものです。これらはインターネット上で正式なものではあり ません。

<u>表記法</u>

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

<u>設定</u>

<u>タスク</u>

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しま す。

<u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



<u>シンクライアント SSL VPN の設定</u>

Security Device Manager (SDM) インターフェイスで提供されるウィザードを使用して、Cisco

IOS でシンクライアント SSL VPN を設定するか、コマンドライン インターフェイス(CLI)で 設定するか、または SDM アプリケーションで手動で設定します。この例では、ウィザードを使 用します。

1. [Configure] タブを選択します。ナビゲーション ペインで [VPN] > [WebVPN] を選択します。 。[Create WebVPN] タブをクリックします。[Create a new WebVPN] の横のラジオ ボタン をクリックします。[Launch the selected task]ボタンをクリックします



2. WebVPN ウィザードが起動します。[next] をクリックします。

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 Ner> Finish Cancel	Help

この WebVPN ゲートウェイの IP アドレスと一意な名前を入力します。[next] をクリックし ます。

WebVPN Wizard	\sim
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 proviser to authenticate the
	Certificate: ausnml-3825-01_Certificate
	Information URL to login to this WebVPN service: https://192.168.0.37/webvpn
	< Back Net Finish Cancel Help

 [User Authentication] 画面でユーザの認証を実行できます。この設定では、ルータでローカ ルに作成されたアカウントを使用します。Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウンティング)サーバを使用することもできます。ユ ーザを追加するには、[Add] をクリックします。[Add an Account] 画面でユーザ情報を入力 し、[OK] をクリックします。[User Authentication] 画面で [Next] をクリックします。

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

WebVPN ウィザード画面でイントラネット Web サイトを設定できますが、このアプリケー ション アクセスにはポート フォワーディングが使用されているため、この手順は省略され ます。Web サイトへのアクセスを許可する場合は、クライアントレス SSL VPN 設定または フル クライアント SSL VPN 設定を使用します。これについての説明はこのドキュメントの 範囲外です。

WebVPN Wizard			
WebVPN Wizard	Configure Intranet We You can configure grou can contain one or mor links that users can clin Add or select the group	ebsites 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 rtal page as
	Action	URL List	Add Edit Delete
		< Back Next > Finish C	ancel Help

[next] をクリックします。ウィザードでフル トンネル クライアントを設定できる画面が表示されます。これは、シンクライアント SSL VPN(ポート フォワーディング)には適用されません。[Enable Full Tunnel] のチェックマークを外します。[next] をクリックします。

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: ▼ Instali 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. ✓ 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. WebVPN ポータル ページの外観をカスタマイズするか、デフォルトの外観を承認します。 [next] をクリックします。

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 ogo. You can create new themes, and customize colors, text and logo in Edit WebVPN mode Theme: Open Highway Preview: Ocean Breeze Desert Sands Festival	
	CISCO SYSTEMS Web VPN Server	
	Websites	
	Internet	
	Enter Web address (URL): Go	
1 - Marine Marine		
	< Back Next > Finish Cancel Help	

設定の概要をプレビューし、[Finish] > [Save] をクリックします。

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 is recommended that you enable DNS.
	< Back Next > Finish Cancel Help

WebVPN ゲートウェイとグループ ポリシーにリンクした WebVPN コンテキストが作成されました。クライアントが WebVPN に接続すると使用可能になるシンクライアント ポートを設定します。[Configure]を選択します。[VPN] > [WebVPN] を選択します。[Create WebVPN] を選択します。[Configure advanced features for an existing WebVPN] ラジオ ボタンを選択し、[Launch the selected task] をクリックします。



初期画面には、ウィザードの機能の概要が説明されています。[next] をクリックします。

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:	
	* 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 H	lelp

ドロップダウン メニューから WebVPN コンテキストとユーザ グループを選択します。 [next] をクリックします。

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

[Thin Client (Port Forwarding)] を選択して、[Next] をクリックします。

WebVPN Wizard



ポート フォワーディングで使用できるようにするリソースを入力します。サービス ポート はスタティック ポートにする必要がありますが、クライアント PC でウィザードによって割 り当てられたデフォルトのポートを受け入れることができます。[next] をクリックします。

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

60)

設定の概要をプレビューして、[Finish] > [OK] > [Save] をクリックします。



<u>コンフィギュレーション</u>

SDM の設定の結果

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				
1				
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
```



設定の確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. クライアント コンピュータを使用して、WebVPN ゲートウェイ

(https://gateway_ip_address)にアクセスします。一意の WebVPN コンテキストを作成す る場合、WebVPN ドメイン名を含めることを忘れないでください。たとえば、「sales」と いう名前のドメインを作成した場合は、https://gateway_ip_address/sales と入力します。

WebVPN Service - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
🌀 Back 🔹 🐑 - 💽 😰 🏠 🔎 Search 🦖 Favorites 🤣 🍰 - چ 😥 🔹 🛄 🐢	**
Address 🕘 https://192.168.0.37/webvpn.html	s »
Google - 💽 Search - 🧭 🥩 🔁 Popups okay 👋 Check - 🔍 AutoLink - ×	•
	~
WebVPN Service	
Login	
Please enter your username and password	
Login Clear	
	~
all Done 🔄 😫 Thternet	

2. ログインして、WebVPN ゲートウェイで提供される証明書を受け入れます。[Start Application Access] をクリックします。

E WebVPN Service - Microsoft Internet Explorer					
File Edit View Favorites Tools Help					27
🎯 Back 🝷 🐑 🔺 📓 🏠 🔎 Search 🚽	Favorites 🚱	Ø• 👙	w -	🔵 🛍 🤇	P 🚳
Address 🕘 https://192.168.0.37/index.html				👻 🔁 G	o Links ³⁰
Google - 💽 Search - 🏈 😻 🔁 Popups okay 👋 Check - 🔍 AutoLink - »					
CISCO SYSTEMS WebVPN Service				?80	
If the Floating Toolbar does not open, click here to open it. Start Application Access					
Websites					
Enter Web Address (URL)	Enter Web	2.168 🖃 ication Acc Address (U	Cess JRL) Go	Go	X
Attps://192.168.0.37/tcp/index.html		nternet		Internet	

3. [Application Access] 画面が表示されます。ローカル ポート番号とローカル ループバック IP アドレスでアプリケーションにアクセスできます。たとえば、ルータ 1 に Telnet 接続する には、telnet 127.0.0.1 3001 と入力します。小さな Java アプレットがこの情報を WebVPN ゲートウェイに送信し、続いてこのゲートウェイでセッションの両端が安全に接続されます 。接続に成功すると、[Bytes Out] および [Bytes In] 列の数字が増える場合があります。 🐔 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 172.22.1.30:23 0 0 Router 1 127.0.0.1:3001 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

<u>コマンド</u>

いくつかの show コマンドは WebVPN に関連しています。これらのコマンドをコマンドライン インターフェイス(CLI)で実行して、統計情報や他の情報を表示できます。show コマンドの使 用方法についての詳細は、『<u>WebVPN 設定の確認</u>』を参照してください。

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

<u>トラブルシュート</u>

このセクションは、設定のトラブルシューティングを行う際に参照してください。

クライアント コンピュータには SUN Java バージョン 1.4 以降がロードされている必要がありま す。Java ソフトウェアのダウンロード ページからこのソフトウェアのコピーを入手してくださ <u>い。</u>

<u>トラブルシューティングに使用するコマンド</u>

注:debugコマンドを使用す<u>る前に、『デバッグコマンド</u>の重要な情報』を参**照してく**ださい。

• show webvpn ?: WebVPN に関連するさまざまな show コマンドが用意されています。CLI で実行すると、統計情報やその他の情報が表示されます。show コマンドの使用方法について

の詳細は、『WebVPN 設定の確認』を参照してください。

 debug webvpn?: debug コマンドの使用は ASA に悪影響を及ぼす場合があります。debug コマンドの使用方法についての詳細は、『<u>WebVPN Debug コマンドの使用』を参照してくだ</u> <u>さい。</u>

関連情報

- <u>Cisco IOS SSLVPN</u>
- SSL VPN WebVPN
- <u>Cisco IOS WebVPN Q&A</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>