

CHAPTER

シナリオ:SSL VPN クライアン トレス接続

この章では、適応型セキュリティアプライアンスを使用して、ソフトウェアク ライアントなしで(クライアントレス)リモートアクセス SSL VPN 接続を受け 入れる方法について説明します。クライアントレス SSL VPN では、Web ブラウ ザを使用して、インターネットを介したセキュアな接続(トンネル)を作成でき ます。このため、オフサイトのユーザにソフトウェア クライアントまたはハー ドウェア クライアントを使用せずに、セキュアなアクセスを提供できます。

この章には、次の項があります。

- クライアントレス SSL VPN について (P.6-2)
- ブラウザベースの SSL VPN アクセスを使用するネットワークの例 (P.6-4)
- クライアントレス SSL VPN シナリオの実装 (P.6-5)
- 次の手順 (P.6-20)

6

クライアントレス SSL VPN について

クライアントレス SSL VPN 接続を使用すると、インターネット上のほぼすべて のコンピュータから、豊富な Web リソースと Web 対応アプリケーションにセ キュアかつ簡単にアクセスできます。アクセスできるものは次のとおりです。

- 内部 Web サイト
- Web 対応アプリケーション
- NT/Active Directory および FTP ファイル共有
- POP3S、IMAP4S、SMTPS などの電子メール プロキシ
- MS Outlook Web Access
- MAPI
- アプリケーション アクセス(他の TCP ベースのアプリケーションにアクセ スするためのポート転送)とスマート トンネル

クライアントレス SSL VPN は、Secure Sockets Layer Protocol (SSL) とその後継 プロトコルである Transport Layer Security (TLSI) を使用して、中央サイトで設 定するサポート対象の特定内部リソースとリモート ユーザとの間でセキュアな 接続を提供します。適応型セキュリティ アプライアンスはプロキシで処理する 必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを 認証します。

ネットワーク管理者は、グループ単位でクライアントレス SSL VPN のユーザに リソースへのアクセス権限を付与します。

クライアントレス SSL VPN 接続のセキュリティに関する検討事項

適応型セキュリティアプライアンス上のクライアントレス SSL VPN 接続は、特に SSL 対応サーバとの対話方法および証明書の検証に関して、リモートアクセス IPsec 接続とは異なります。

クライアントレス SSL VPN 接続では、適応型セキュリティアプライアンスがエ ンドユーザの Web ブラウザとターゲット Web サーバとの間でプロキシとして機 能します。ユーザが SSL 対応 Web サーバに接続すると、適応型セキュリティア プライアンスはセキュアな接続を確立し、サーバの SSL 証明書を検証します。エ ンドユーザのブラウザは、提示される証明書を受け取ることはありません。した がって、エンドユーザのブラウザでは証明書の検査および検証はできません。 適応型セキュリティアプライアンス上の現在のクライアントレス SSL VPN の実 装では、有効期限が切れた証明書を提示したサイトとの通信は許可されません。 また、適応型セキュリティアプライアンスでは、信頼されている CA 証明書の 検証は行われません。そのため、ユーザは、SSL 対応 Web サーバと通信する前 に、SSL 対応 Web サーバが提供する証明書を解析することはできません。

SSL 証明書に関するリスクを最小限に抑えるには、次の方法があります。

- クライアントレス SSL VPN アクセスを必要とするすべてのユーザで構成されるグループポリシーを設定し、そのグループポリシーに対してのみクライアントレス SSL VPN アクセスをイネーブルにします。
- クライアントレス SSL VPN ユーザのインターネット アクセスを制限しま す。たとえば、ユーザがクライアントレス SSL VPN 接続を使用してアクセ スできるリソースを制限します。これを実行すると、インターネット上の一 般的なコンテンツへのユーザによるアクセスが制限されることがあります。 その場合は、クライアントレス SSL VPN ユーザがアクセスできる内部ネッ トワーク上の特定ターゲットへのリンクを設定できます。
- ユーザを教育します。SSL 対応サイトがプライベート ネットワーク内部にない場合、ユーザはクライアントレス SSL VPN 接続を介してそのサイトにアクセスすべきではありません。そのようなサイトにアクセスするには、別のブラウザ ウィンドウを開く必要があります。そのブラウザを使用して、提示された証明書を参照します。

適応型セキュリティ アプライアンスは、クライアントレス SSL VPN 接続に対し て、次の機能をサポートしません。

- NAT(グローバルに一意の IP アドレスの必要性を低減する機能)
- PAT(複数のアウトバウンドセッションが単一の IP アドレスから発信されているように見せることを許可する機能)

ブラウザベースの SSL VPN アクセスを使用するネットワー クの例

図 6-1 に、Web ブラウザを使用してインターネット経由で SSL VPN 接続要求を 受け入れるように設定されている適応型セキュリティ アプライアンスを示しま す。



図 6-1 SSL VPN 接続のネットワーク レイアウト

191803

クライアントレス SSL VPN シナリオの実装

この項では、Web ブラウザからの SSL VPN 要求を受け入れるように適応型セキュリティ アプライアンスを設定する方法について説明します。設定内容の値の例は、図 6-1 に示したリモート アクセスのシナリオから使用しています。

次のトピックについて取り上げます。

- 必要な情報(P.6-5)
- ASDM の起動 (P.6-6)
- ブラウザベースの SSL VPN 接続用の ASA 5580 の設定(P.6-9)
- SSL VPN インターフェイスの指定 (P.6-10)
- ユーザ認証方式の指定(P.6-11)
- グループポリシーの指定(P.6-13)
- リモートユーザ用のブックマークリストの作成(P.6-14)
- 設定の確認(P.6-19)

必要な情報

リモート アクセス IPsec VPN 接続を受け入れるための適応型セキュリティ アプ ライアンスの設定を開始する前に、次の情報を用意してください。

- リモート ユーザが接続する適応型セキュリティ アプライアンスのインター フェイスの名前。リモート ユーザがこのインターフェイスに接続すると、 SSL VPN ポータル ページが表示されます。
- デジタル証明書。

ASA 5580 は、デフォルトで自己署名証明書を生成します。セキュリティを 強化し、かつブラウザの警告メッセージが表示されないようにするために、 システムを実稼働環境に設置する前に、公的に信頼されている SSL VPN 証 明書を購入することもできます。

- ローカル認証データベースを作成するときに使用するユーザのリスト(認証 に AAA サーバを使用している場合を除く)。
- AAA サーバ グループ名(認証に AAA サーバを使用している場合)。
- AAA サーバ上のグループポリシーに関する次の情報。
 ー サーバグループ名

- 使用する認証プロトコル (TACACS、SDI、NT、Kerberos、LDAP)
- AAA サーバの IP アドレス
- 認証に使用する適応型セキュリティ アプライアンスのインターフェイ
 ス
- AAA サーバで認証を行うための秘密鍵
- リモートユーザが接続を確立したときに、SSL VPN ポータルページに表示 する内部 Web サイトまたはページのリスト。これは、ユーザが初めて接続 を確立したときに表示されるページなので、リモートユーザが最も頻繁に 使用するターゲットを含める必要があります。

ASDM の起動

この項では、ASDM Launcher ソフトウェアを使用して ASDM を起動する方法に ついて説明します。ASDM Launcher ソフトウェアがインストールされていない 場合は、P.4-5 の「ASDM Launcher のインストール」を参照してください。

Web ブラウザまたは Java を使用して ASDM に直接アクセスする場合は、P.4-8の「Web ブラウザでの ASDM の起動」を参照してください。

ASDM Launcher ソフトウェアを使用して ASDM を起動するには、次の手順を実行します。

ステップ1 デスクトップから Cisco ASDM Launcher ソフトウェアを起動します。

ダイアログボックスが表示されます。

🖆 Cisco DM Launcher	v1.5(23)	
Cisco ASDM Launcher		cisco
Device IP Address / Name: Username:	2	×
Passworu:	OK Close	

- **ステップ2** 適応型セキュリティ アプライアンスの IP アドレスまたはホスト名を入力します。
- **ステップ3** Username フィールドと Password フィールドを空のままにします。



注) デフォルトでは、Cisco ASDM Launcher に Username と Password は設定さ れていません。

- **ステップ4** OK をクリックします。
- **ステップ5** 証明書の受け入れを求めるセキュリティ警告が表示された場合は、Yes をクリックします。

ASA 5580 は最新ソフトウェアが存在するかどうかを調べ、存在する場合は自動 的にダウンロードします。

ASDM のメイン ウィンドウが表示されます。

■ クライアントレス SSL VPN シナリオの実装

sco ASDM	6.1 for /	ISA - 172	.23.59.10	01									7)
Yiew <u>T</u> oo	ls Wizard	s <u>W</u> indov	v <u>H</u> elp						Look For:		6		
lome 🥰	Configurati	on 🔯 M	onitoring [🚽 Save 💽 Re	efresh	🔇 Back 🜔 Fo	orward 🧖 Help					CISC	0
lome		-					1 - 1						F
Dev	rice Dashbo	ard 😭 F	Firewall Dashl	oard									
Device Ir	nformatio	n					Interface Statu	5					
General	License						Interface	IP Ad	dress/Mask	Line	Link	Kbps	
							inside	172.23	.59.101/27	O up	🗿 up	16	
Host Na	ame:	ciscoas	a				redund	11.20.3	30.40/8	😐 down	😑 down	0	
Environ	nment Statu	s: 4	н ок	Total Flash: 1	ngle 024 MB		Select an interfac	e to view inp	out and output K	bps			
VPN Tunn	nels						Traffic Status						
IKE: O	IPse	c: 0	Clientless	5SL VPN: 0	SSL V	PN Client: 0	Connections Per	Second Usa	ige				
System F	Resources	Status											
Total Mem	iory Usage	Total CPU	Usage Cor	e Usage									
Memory	Memory	Jsage (MB)											
	4000							14:20	14:21	14:22	14:22	14:24	
	3500						UDP: 0	TCP: 0	Total: 0	17.22	14.25	14.24	
	3000						'redund' Interfac	e Traffic Lic	ana (Khoc)				
	2500						1.	o marine oo.	ago (napo)			1	
1048MB	2000												
	1500												
	1000						0	23:56	23:57	23:58	23:59	0:00	
atest ASD.)M Syslog	Message	s									084	1
Seve D	Date	Time	Syslog ID	Source IP	Sour	ce Destination IP	Destine Description						1
5 De	ec 31 2007	14:24:16	402128				CRYPTO: An att	empt to alloc	tate a large mem	nory block failed, s	size: 100, limit: (). 🔨	•
5 De	ec 31 2007	14:24:16	402128				CRYPTO: An att	empt to alloc	ate a large mem	nory block failed, s	size: 100, limit: (D	-
1,5 De	ec 31 2007	14:24:16	402128				CRYPTO: An att	empt to alloc	tate a large mem	nory block failed, s	size: 100, limit: (J. 🗸	
					(III)							>	

ブラウザベースの SSL VPN 接続用の ASA 5580 の設定

ブラウザベースの SSL VPN の設定プロセスを開始するには、次の手順を実行します。

ステップ1 ASDM のメイン ウィンドウで、Wizards ドロップダウン メニューから SSL VPN Wizard を選択します。SSL VPN Wizard Step 1 画面が表示されます。



ステップ2 SSL VPN Wizard の Step 1 で、次の手順を実行します。

- a. Clientless SSL VPN Access チェックボックスをオンにします。
- **b.** Next をクリックして続行します。

SSL VPN インターフェイスの指定

SSL VPN Wizard の Step 2 で、次の手順を実行します。

ステップ1 リモートユーザが接続する接続名を指定します。

🔂 SSL VPN Wizard	×
SSL VPN Wizard	SSL VPN Interface (Step 2 of 6)
· · · · · · · · · · · · · · · · · · ·	Provide a connection name and the interface that SSL VPN users connect to.
	Connection Name: Clientless-VPN
	The interface users access for SSL VPN connections.
	SSL VPN Interface:
	Name: outside Digital Certificate IP Address: 10.86.194.170 / 255.255.254.0 When users connect, the security appliance senddecurity Level:0 ser
	Certificate:
rest.	Connection Group Settings
1	Connection Group Alias/URL
	Display Group Alias list at the login page
1511	Information URL to access SSL VPN Service: https://10.86.194.170:445 URL to access ASDM: https://10.86.194.170/admin

- ステップ2 SSL VPN Interface ドロップダウン リストから、リモート ユーザが接続するイン ターフェイスを選択します。ユーザがこのインターフェイスへの接続を確立する と、SSL VPN ポータルページが表示されます。
- **ステップ3** Certificate ドロップダウン リストから、ASA 5580 を認証するために ASA 5580 が リモート ユーザに送信する証明書を選択します。



ASA 5580 は、デフォルトで自己署名証明書を生成します。セキュリティを強化 し、かつブラウザの警告メッセージが表示されないようにするために、システ ムを実稼働環境に設置する前に、公的に信頼されている SSL VPN 証明書を購入 することもできます。

ユーザ認証方式の指定

ユーザは、ローカル認証データベース、または外部認証、認可、アカウンティン グ(AAA)サーバ(RADIUS、TACACS+、SDI、NT、Kerberos、および LDAP) で認証できます。

SSL VPN Wizard の Step 3 で、次の手順を実行します。

- **ステップ1** AAA サーバまたはサーバ グループを認証に使用している場合、次の手順を実行 します。
 - a. Authenticate using a AAA server group オプション ボタンをクリックします。

薩 SSL VPN Wizard		X
SSL VPN Wizard	User Authentication (Step 3 of 6)	
	The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login. Authenticate using a AAA server group AAA Server Group Name: AAA Server Group Name: New AAA Server Group Name: New AAA Server Group Name: New New.	
	<u>≤Back</u> <u>N</u> ext > ⊟nish <u>C</u> ancel <u>H</u> elp	

b. AAA Server Group Name ドロップダウン リストから事前設定済みのサーバ グループを選択するか、New をクリックして新しい AAA サーバ グループを 追加します。

新しい AAA サーバ グループを作成するには、New をクリックします。New Authentication Server Group ダイアログボックスが表示されます。

このダイアログボックスで、次の内容を指定します。

- サーバグループ名
- 使用する認証プロトコル (TACACS、SDI、NT、Kerberos、LDAP)
- AAA サーバの IP アドレス
- 適応型セキュリティアプライアンスのインターフェイス
- AAA サーバと通信するときに使用する秘密鍵

OK をクリックします。

Cisco ASA 5580 スタート ガイド

ステップ2 ローカル ユーザ データベースでユーザを認証する場合は、ここで新しいユーザ アカウントを作成できます。ASDM 設定インターフェイスを使用して後でユー ザを追加することもできます。

> 新しいユーザを追加するには、ユーザ名とパスワードを入力し、Add をクリック します。

ステップ3 新しいユーザの追加が終了したら、Nextをクリックして続行します。

グループ ポリシーの指定

SSL VPN Wizard の Step 4 で、次の手順を実行してグループ ポリシーを指定します。

ステップ1 Create new group policy オプション ボタンをクリックし、グループ名を指定します。

または

Modify existing group policy オプション ボタンをクリックし、ドロップダウン リ ストからグループを選択します。

🔂 SSL VPN Wizard	2	:
SSL VPN Wizard	Group Policy (Step 4 of 6)	
SSL VPN WIZHD	A group policy is a collection of user-oriented attribute/value pairs. Unless assigned to a specific group policy, all users are members of the default group policy (DfltGrpPolicy). Therefore, configuring the default group policy lets users inherit attributes that you have not configured at the individual group policy or username level.	
	<u>≤ Back</u> <u>N</u> ext > ⊟nish <u>C</u> ancel <u>H</u> elp	

ステップ2 Next をクリックします。

リモート ユーザ用のブックマーク リストの作成

ユーザが簡単にアクセスできるように URL のリストを指定して、ポータルページ(ブラウザベースのクライアントが適応型セキュリティ アプライアンスへの VPN 接続を確立したときに表示される特別な Webページ)を作成できます。

SSL VPN Wizard の Step 5 で、次の手順を実行して、VPN ポータル ページに表示 する URL を指定します。

ステップ1 既存のブックマーク リストを指定するには、ドロップダウン リストからブック マーク リスト名を選択します。

🖆 SSL VPN Wizard	X	
SSL VPN Wizard	WebVPN - Bookmark list (Step 5 of 7)	
	Configure a list of group intranet websites that appears in the portal page as links that users can navigate to. Bookmark List: None Manage	
	Sack Wext > Einish Cancel Help	

新しいリストを追加するか、既存のリストを編集するには、Manage をクリック します。

Configure GUI Customization Objects ダイアログボックスが表示されます。

🖆 Configure GUI Customization Objects	×
Configure bookmark lists that the security appliance displays on the SSL VPN portal page.	
💠 Add 🧭 Edit 🗊 Delete 💠 Import 🗹 Export	
Bookmarks	
Template	
OK Cancel Help	842
	1910

ステップ2新しいブックマークリストを作成するには、Add をクリックします。

既存のブックマーク リストを編集するには、リストを選択し、Edit をクリック します。

Add Bookmark List ダイアログボックスが表示されます。

Gookmark List	arks	X
Name	URL	Edit Delete Move Up Move Down
ОК	Cancel Help	6 PG

- **ステップ3** Bookmark List Name フィールドで、作成するブックマーク リストの名前を指定 します。この名前は、VPN ポータル ページのタイトルとして使用されます。
- ステップ4 Add をクリックして新しい URL をブックマーク リストに追加します。

Add Bookmark Entry ダイアログボックスが表示されます。

🔂 Add Bookmarl	k Entry	×
Bookmark Title: URL Value:	SalesReport http •// companysales.companyl.com	
Advanced Op	otions 🛛 😵	
	OK Cancel Help	191844

ステップ5 Bookmark Title フィールドで、リストのタイトルを指定します。

ステップ6 URL Value ドロップダウン リストから、指定する URL のタイプを選択します。 たとえば、http、https、ftp などを選択します。

次に、ページの完全な URL を指定します。

- **ステップ7** OK をクリックして Add Bookmark List ダイアログボックスに戻ります。
- **ステップ8** ブックマーク リストの追加が終了したら、**OK** をクリックして Configure GUI Customization Objects ダイアログボックスに戻ります。
- ステップ9 ブックマーク リストの追加および編集が終了したら、OK をクリックして SSL VPN Wizard の Step 5 に戻ります。
- **ステップ10** Bookmark List ドロップダウン リストから、この VPN グループのブックマーク リストの名前を選択します。
- ステップ11 Next をクリックして続行します。

設定の確認

SSL VPN Wizard の Step 6 で、設定内容が正しいことを確認します。表示される 設定は、次のようになります。



設定が正しいことを確認したら、Finish をクリックして、変更を適応型セキュリ ティアプライアンスに適用します。

設定の変更をスタートアップ設定に保存して、デバイスを次回に起動したときに この変更が適用されるようにする場合は、File メニューの Save をクリックしま す。あるいは、ASDM の終了時に、設定の変更を保存するかどうかの確認を求 めるメッセージが表示されます。

設定の変更を保存しないと、次回にデバイスを起動したときに、以前の設定が有 効になります。

Cisco ASA 5580 スタート ガイド

次の手順

クライアントレス SSL VPN 環境に適応型セキュリティ アプライアンスを配置す るだけの場合は、これで初期設定は終了です。このほかに、次の手順について、 実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機	Cisco Security Appliance Command Line
能と高度な機能の設定	Configuration Guide
日常のオペレーションの学習	Cisco Security Appliance Command Reference
	Cisco Security Appliance Logging Configuration and System Log Messages

適応型セキュリティアプライアンスは、複数のアプリケーション用に設定でき ます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
AnyConnect VPN の設定	第5章「シナリオ: Cisco AnyConnect VPN ク
	ライアント用の接続の設定」
サイトツーサイト VPN の設定	第7章「シナリオ:サイトツーサイト VPN の
	設定」
リモートアクセス VPN の設定	第8章「シナリオ: IPsec リモート アクセス
	VPN の設定」