

SDM を使用した IOS での SSL VPN Client (SVC) の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[設定前の作業](#)

[表記法](#)

[背景説明](#)

[IOS での SVC の設定](#)

[ステップ 1. IOS ルータでの SVC ソフトウェアのインストールと有効化](#)

[ステップ 2. SDM ウィザードによる WebVPN コンテキストと WebVPN ゲートウェイの設定](#)

[ステップ 3. SVC ユーザのユーザ データベースの設定](#)

[ステップ 4. ユーザに提示するリソースの設定](#)

[結果](#)

[確認](#)

[手順](#)

[コマンド](#)

[トラブルシューティング](#)

[SSL の接続の問題](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

SSL VPN Client (SVC) は、フルトンネルによるセキュアな通信を企業の社内ネットワークに提供します。ユーザごとのアクセスを設定することも、異なる WebVPN コンテキストを作成して、それらに 1 人以上のユーザを配置することもできます。

SSL VPN、または WebVPN テクノロジーは、次の IOS ルータ プラットフォームでサポートされています。

- 870、1811、1841、2801、2811、2821、2851
- 3725、3745、3825、3845、7200、および 7301

SSL VPN テクノロジーは、次のモードで設定できます。

- **クライアントレス SSL VPN (WebVPN)** : 企業のローカル エリア ネットワーク (LAN) 上の HTTP サーバまたは HTTPS Web サーバへアクセスする際に SSL 対応の Web ブラウザが

必要となるリモート クライアントです。また、クライアントレス SSL VPN は、Common Internet File System (CIFS) プロトコルによる Windows ファイル ブラウジングへのアクセスも提供します。Outlook Web Access (OWA) は、HTTP アクセスの一例です。クライアントレス SSL VPN についての詳細は、『[SDM を使用した Cisco IOS でのクライアントレス SSL VPN \(WebVPN \) の設定例](#)』を参照してください。

- **シンクライアント SSL VPN (ポート転送)** : 小規模な Java ベースのアプリレットをダウンロードし、スタティックなポート番号を使用する Transmission Control Protocol (TCP; 伝送制御プロトコル) アプリケーションのセキュアなアクセスを可能にするリモート クライアントです。Point of Presence (POP3)、Simple Mail Transfer Protocol (SMTP)、Internet Message Access Protocol (IMAP)、Secure Shell (ssh; セキュア シェル)、および Telnet は、セキュアなアクセスの例です。ローカル マシン上のファイルが変更されるため、この方法を使用するには、ユーザにローカル管理者特権が必要です。SSL VPN のこの方法は、一部の File Transfer Protocol (FTP; ファイル転送プロトコル) アプリケーションなど、ダイナミックな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。シンクライアント SSL VPN についての詳細は、『[SDM によるシンクライアント SSL VPN \(WebVPN \) の IOS 設定例](#)』を参照してください。注: User Datagram Protocol (UDP; ユーザ データグラム プロトコル) はサポートされていません。
- **SSL VPN クライアント (SVC フルトンネル モード)** : リモート ワークステーションに小規模なクライアントをダウンロードし、社内ネットワークのリソースへの完全なセキュア アクセスを可能にします。SVC をリモート ワークステーションへ永続的にダウンロードすることも、セキュアなセッションが閉じられた後にクライアントを削除することもできます。

このドキュメントでは、SSL VPN クライアントによって使用される Cisco IOS ルータの設定を紹介します。

前提条件

要件

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。

- Microsoft Windows 2000 または XP
- SUN JRE 1.4 以降を搭載した Web ブラウザまたは ActiveX コントロール対応ブラウザ
- クライアント上のローカルな管理者権限
- 拡張セキュリティ イメージ (12.4(6)T またはそれ以降) の[概要](#)でリストに記載されるルータの 1 つ
- Cisco Security Device Manager (SDM) バージョン 2.3Cisco SDM がルータにロードされていない場合は、このソフトウェアの無償コピーを [\[Software Download\] ページ](#) ([登録ユーザ専用](#)) からダウンロードできます。サービス契約を結んでいる Cisco.com アカウントが必要です。SDM のインストールと設定についての詳細、『[Cisco ルータとセキュリティ デバイスマネージャ](#)』を参照してください。
- ルータでのデジタル証明書この要件を満たすには、永続的な自己署名証明書を使用することも、外部の Certificate Authority (CA; 認証局) を使用することもできます。永続的な自己署名証明書の詳細については、『[永続的な自己署名証明書](#)』を参照してください。

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くものです。

- Cisco IOS ルータ 3825 シリーズ 12.4(9)T
- Security Device Manager (SDM) バージョン 2.3.1

注: 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たものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

設定前の作業

1. ルータの SDM 設定を行います。 (オプション) ライセンスに適切なセキュリティがバンドルされているルータには、SDM アプリケーションがすでにフラッシュにロードされています。 [ソフトウェアの取得と設定については、『Cisco Router and Security Device Manager \(SDM \) のダウンロードおよびインストール』](#) を参照してください。
2. SVC のコピーを管理 PC にダウンロードします。 [ソフトウェアダウンロード](#) からの SVC パッケージ ファイルのコピーを入手できます: [Cisco SSL VPN Client \(登録ユーザのみ \)](#)。サービス契約を結んでいる、有効な Cisco.com アカウントが必要です。
3. ルータに正しい日付、時刻、および時間帯を設定し、次にデジタル証明書を設定します。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

背景説明

SVC は、最初に WebVPN ゲートウェイ ルータにロードされます。クライアントが接続するたびに、SVC のコピーがダイナミックに PC にダウンロードされます。この動作を変更するには、ソフトウェアが永続的にクライアント コンピュータに残るようにルータを設定します。

IOS での SVC の設定

このセクションでは、このドキュメントに記載されている機能を設定するために必要な手順を示します。次の設定例では、IOS ルータで SVC の動作を有効にするのに、SDM ウィザードを使用しています。

IOS ルータの SVC を設定するためにこれらのステップを完了して下さい:

1. [IOS ルータに SVC ソフトウェアをインストールし、有効にする](#)
2. [SDM ウィザードを使用して、WebVPN コンテキストと WebVPN ゲートウェイを設定する](#)
3. [SVC ユーザのユーザ データベースを設定する](#)
4. [ユーザに提示するリソースを設定する](#)

ステップ 1. IOS ルータでの SVC ソフトウェアのインストールと有効化

IOSルータで SVC ソフトウェアをインストールし、有効にするためにこれらのステップを完了して下さい:

1. SDM アプリケーションを開いて [Configure] をクリックし、次に [VPN] をクリックします。
2. **WebVPN** を展開し、**Packages** を選択します。
3. Cisco WebVPN Client Software のエリアで、**Browse** ボタンをクリックします。Select SVC location ダイアログ ボックスが表示されます。
4. [My Computer] オプション ボタンをクリックし、次に [Browse] をクリックして、管理 PC にある SVC パッケージを探します。
5. [OK] をクリックし、次に [Install] ボタンをクリックします。
6. [Yes] をクリックし、次に [OK] をクリックします。SVC パッケージが正しくインストールされると、次のイメージが表示されます。

[ステップ 2. SDM ウィザードによる WebVPN コンテキストと WebVPN ゲートウェイの設定](#)

WebVPN WebVPN コンテキストおよびゲートウェイを設定するためにこれらのステップを完了して下さい:

1. SVC をルータにインストールした後、[Configure] をクリックし、次に [VPN] をクリックします。
2. [WebVPN] をクリックし、[Create WebVPN] タブをクリックします。
3. Create a New WebVPN オプション ボタンをチェックし、次に Launch the selected task をクリックします。WebVPN Wizard ダイアログ ボックスが表示されます。
4. [Next] をクリックします。
5. 新しい WebVPN ゲートウェイの IP アドレスを入力し、この WebVPN コンテキストの一意の名前を入力します。同じ IP アドレス (WebVPN ゲートウェイ) に異なった WebVPN コンテキストを作成できますが、それぞれの名前は一意にする必要があります。この例では、次の IP アドレスを使用します。 *https://192.168.0.37/sales*
6. [Next] をクリックし、[ステップ 3](#) へ移ります。

[ステップ 3. SVC ユーザのユーザデータベースの設定](#)

認証には、AAA サーバ、ローカル ユーザ、またはその両方を使用できます。この設定例では、ローカルに作成されたユーザを認証に使用しています。

SVC ユーザ向けのユーザデータベースを設定するためにこれらのステップを完了して下さい:

1. [手順 2](#) が完了したら、WebVPN Wizard User Authentication ダイアログ ボックスにある [Locally on this router] オプション ボタンをクリックします。このダイアログ ボックスで、ユーザをローカル データベースに追加できます。
2. [Add] をクリックして、ユーザ情報を入力します。
3. [OK] をクリックして、必要に応じてさらにユーザを追加します。
4. 必要なユーザを追加したら、[Next] をクリックし、[ステップ 4](#) へ移ります。

[ステップ 4. ユーザに提示するリソースの設定](#)

Configure Intranet Websites WebVPN Wizard ダイアログ ボックスでは、SVC クライアントに提

示するイントラネット リソースを選択できます。

リソースをユーザに露出するために設定するためにこれらのステップを完了して下さい:

1. [ステップ 3](#) が完了したら、[Configure Intranet] Websites ダイアログ ボックスにある [Add] ボタンをクリックします。
2. URL リスト名を入力し、ヘッディングを入力します。
3. [Add] をクリックし、[Website] を選択して、このクライアントに提示する Web サイトを追加します。
4. URL とリンク情報を入力し、[OK] をクリックします。
5. OWA エクスチェンジ サーバ へのアクセスを追加するため、[Add] をクリックし、[E-mail] を選択します。
6. [Outlook Web Access] チェック ボックスにチェックマークを入れ、URL ラベルとリンク情報を入力して、[OK] をクリックします。
7. 必要なリソースを追加したら、OK をクリックし、Next をクリックします。WebVPN Wizard full tunnel ダイアログ ボックスが表示されます。
8. [Enable Full Tunnel] チェック ボックスにチェックマークが入っていることを確認します。
9. この WebVPN コンテキストのクライアントが使用できる IP アドレスのプールを作成します。アドレスのプールは、イントラネット上で使用可能でルーティング可能なアドレスと対応している必要があります。
10. [IP Address Pool] フィールドの横の省略記号 ([...]) をクリックし、[Create a new IP Pool] を選択します。
11. Add IP Local Pool ダイアログボックスで、プールの名前を入力し、[Add] をクリックします。
12. Add IP address range ダイアログボックスで、SVC クライアントのアドレス プールの範囲を入力し、OK をクリックします。注: IP アドレス プールは、直接ルータに接続しているインターフェイスの範囲内である必要があります。異なるプール範囲を使用する場合は、必要条件を満たすために、新しいプールに関連するループバック アドレスを作成できます。
13. [OK] をクリックします。
14. リモート クライアントで SVC のコピーを永続的に保存する場合は、[Keep the Full Tunnel Client Software installed on client's PC] チェック ボックスをクリックします。クライアントが接続するたびにクライアントが SVC ソフトウェアをダウンロードするように要求するようにこのオプションをクリアして下さい。
15. スプリット トンネリング、スプリット DNS、ブラウザのプロキシ設定、DNS サーバと WNS サーバなどの拡張トンネル オプションを設定します。Cisco では、最小限、DNS サーバと WINS サーバを設定することを推奨しています。拡張トンネル オプションを設定するには、次の手順を実行します。[Advanced Tunnel Options] ボタンをクリックします。[DNS and WINS Servers] タブをクリックし、DNS サーバと WINS サーバのプライマリ IP アドレスを入力します。スプリット トンネリングとブラウザのプロキシ設定を設定するには、[Split Tunneling] または [Browser Proxy Settings] タブをクリックします。
16. 必要なオプションを設定したら、[Next] をクリックします。
17. WebVPN Portal Page をカスタマイズするか、またはデフォルト値を選択します。Customize WebVPN Portal Page では、お客様への WebVPN Portal Page の表示方法をカスタマイズできます。
18. WebVPN Portal Page を設定したら、[Next] をクリックし、[Finish] をクリックしてから、[OK] をクリックします。WebVPN Wizard は、ルータへコマンドを発行します。
19. [OK] をクリックして、設定を保存します。注: エラー メッセージが表示された場合は、

WebVPN ライセンスに誤りがある可能性があります。次のイメージに、エラー メッセージの例を示します。ライセンスの問題を解決するには、次の手順を実行します。

[Configure] をクリックし、次に [VPN] をクリックします。[WebVPN] を展開し、[Edit WebVPN] タブをクリックします。新規作成したコンテキストを選択して、[Edit] ボタンをクリックします。[Maximum Number of users] フィールドで、ライセンスの正確なユーザー数を入力します。[OK] をクリックし、さらに [OK] をクリックします。コマンドがコンフィギュレーション ファイルに書き込まれます。[Save] をクリックし、[Yes] をクリックして変更を確定します。

結果

ASDM は次のコマンドライン設定を作成します。

```
ausnml-3825-01
ausnml-3825-01#show run
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
!
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
$l$r4CW$SeP6ZwQEAAU68W9kbR16U. username ausnml privilege
15 password 7 044E1F505622434B username sales privilege
15 secret 5 $l$/Lc1$K.Zt41zF1jSdKZrPgNK1A. username
newcisco privilege 15 secret 5
$l$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
```

確認

ここでは、設定が正常に動作していることを確認します。

手順

設定をテストするには、SSL 対応のクライアント Web ブラウザに <http://192.168.0.37/sales> と入力します。

コマンド

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 コマンドの詳細は、『[WebVPN 設定の確認](#)』を参照してください。

注: [Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の show コマンドがサポートさ

れています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

[トラブルシューティング](#)

ここでは、設定に関するトラブルシューティングについて説明します。

[SSL の接続の問題](#)

問題： SSL VPN クライアントがルータに接続できない。

解決策： IP アドレスプール内の IP アドレスが足りない場合、この問題が引き起こされる可能性があります。この問題を解決するには、ルータの IP アドレスのプールで、IP アドレスの数を増やしてください。

[トラブルシューティングのためのコマンド](#)

いくつかの **clear** コマンドは、WebVPN に関連しています。これらのコマンドの詳細については、「[WebVPN の Clear コマンドの使用](#)」を参照してください。

いくつかの **debug** コマンドは、WebVPN に関連しています。これらのコマンドの詳細については、「[WebVPN の Debug コマンドの使用](#)」を参照してください。

注: **debug** コマンドを使用すると、Cisco デバイスに悪影響が及ぶ可能性があります。 **debug** コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

[関連情報](#)

- [Cisco IOS SSLVPN](#)
- [SSL VPN - WebVPN](#)
- [SDM を使用した Cisco IOS でのクライアントレス SSL VPN \(WebVPN \) の設定例](#)
- [SDM によるシンクライアント SSL VPN \(WebVPN \) の IOS 設定例](#)
- [WebVPN および DMVPN コンバージェンス導入ガイド](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)