CHAPTER 38

SSL VPN クライアントの設定

SSL VPN Client（SVC）は、ネットワーク管理者がリモート コンピュータに IPSec VPN クライアントをインストールして設定しなくても、リモート ユーザが IPSec VPN クライアントの利点を活用できる VPN トンネリング テクノロジーです。SVC は、リモート コンピュータに既存の SSL 暗号化およびセキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

SVC セッションを確立するには、リモート ユーザがブラウザでセキュリティ アプライアンスの WebVPN インターフェイスの IP アドレスを入力し、ブラウザはそのインターフェイスに接続し、WebVPN ログイン画面を表示します。ユーザがログインと認証を完了し、ユーザが SVC を*必要としている*ことをセキュリティ アプライアンスが確認すると、セキュリティ アプライアンスは SVC をリモート コンピュータにダウンロードします。セキュリティ アプライアンスが、SVC を使用する*オプション*がユーザにあると確認した場合、セキュリティ アプライアンスは、SVC のインストールをスキップするリンクをユーザ画面に表示するとともに、SVC をリモート コンピュータにダウンロードします。

ダウンロードが完了すると、SVC はインストールと設定を実行します。接続が終了すると（設定に応じて）、SVC はリモート コンピュータに保持されるか、またはリモート コンピュータからアンインストールされます。

この項では、次のトピックについて取り上げます。

SVC のインストール

この項では、SVC をインストールするためのプラットフォーム要件と手順を示します。

プラットフォーム要件

SVC には、リモート コンピュータ上の Windows 2000 または Windows XP が必要です。

SVC ソフトウェアのインストール

SVC のインストール作業は、セキュリティ アプライアンスに SVC イメージをコピーし、イメージに順序を割り当てることから構成されます。SVC をインストールするには、次の手順を実行します。

ステップ 1　特権 EXEC モードで **copy** コマンドを使用して、または別の方法で SVC イメージをセキュリティ アプライアンスにコピーします。この例では、**copy tftp** コマンドを使用して、イメージを TFTP サーバからコピーします。

```
hostname# copy tftp flash
Address or name of remote host []? 209.165.200.226
Source filename []? sslclient-win-1.0.2.127.pkg
Destination filename []? sslclient-win-1.0.2.127.pkg
Accessing tftp://209.165.200.226/sslclient-win-1.0.2.127.pkg...!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file
disk0:/cdisk71...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
319662 bytes copied in 3.695 secs (86511 bytes/sec)
```

ステップ 2　webvpn モードで **svc image** コマンドを使用して、SVC イメージに順序を割り当てます。

svc image *filename order*

SVC イメージの番号付けにより、セキュリティ アプライアンスがそれらをリモート コンピュータにダウンロードする順序を設定できます。最も番号の小さい SVC イメージが最初にダウンロードされます。そのため、最も一般的なオペレーティング システムで使用されるイメージに、最も小さい値を割り当てる必要があります。

次の例では、**show webvpn svc** コマンドの出力により、windows.pkg イメージの順序番号が 1 であり、windows2.pkg イメージの順序番号が 2 であることが示されます。リモート コンピュータが SVC 接続の確立を試みるときに、windows.pkg イメージがまずダウンロードされます。このイメージがオペレーティング システムと一致しない場合、windows2.pkg イメージがダウンロードされます。

```
hostname(config)# webvpn
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows.pkg 1
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows2.pkg 2
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

その後、SVC のアーカイブ イメージが、最初のイメージとして windows2.pkg イメージがリモート PC にダウンロードされ、windows.pkg イメージが 2 番目にダウンロードされるように、**svc image** コマンドを使用して並べ替えられます。

```
hostname(config-webvpn)# no svc image
hostname(config-webvpn)# svc image windows2.pkg 1
hostname(config-webvpn)# svc image windows.pkg 2

Reentering the show webvpn svc command shows the new order of the images:
```

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows2.pkg 1
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows.pkg 2
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

SVC のイネーブル化

SVC のインストール後、次の手順を実行して、SVC をイネーブルにできます。

ステップ 1　webvpn モードで **enable** コマンドを使用して、インターフェイス上で WebVPN をイネーブルにします。

enable *interface*

次に例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

ステップ 2　webvpn モードで、**svc enable** セキュリティ アプライアンス コマンドを入力して、リモート コンピュータへの SVC イメージのダウンロードをイネーブルにします。

svc enable

次に例を示します。

```
hostname(config-webvpn)# svc enable
```

ステップ 3　アドレスの割り当て方式を設定します。DHCP や、ユーザが割り当てたアドレス指定を使用できます。また、webvpn モードで **ip local pool** コマンドを使用して、ローカル IP アドレス プールを作成することもできます。

ip local pool *poolname startaddr-endaddr* **mask** *mask*

次の例では、ローカル IP アドレス プール *vpn_users* を作成します。

```
hostname(config-webvpn)# ip local pool vpn_users 209.165.200.225-209.165.200.254
mask 255.255.255.224
```

ステップ 4　トンネル グループに IP アドレスを割り当てます。これを実行する 1 つの方法は、一般属性モードで **address-pool** コマンドを使用してローカル IP アドレスを設定することです。

address-pool *poolname*

これを実行するためには、まず **tunnel-group** *name* **general-attributes** コマンドを入力して、一般属性モードを開始します。次に、**address-pool** コマンドを使用して、ローカル IP アドレス プールを指定します。

次の例では、既存のトンネル グループ *telecommuters* が、ステップ 3 で作成したアドレス プール *vpn_users* を使用するように設定しています。

```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```

ステップ 5　トンネル グループ一般属性モードで **default-group-policy** コマンドを使用して、トンネル グループにデフォルトのグループ ポリシーを割り当てます。

default-group-policy *name*

次の例では、グループ ポリシー *sales* をトンネル グループ *telecommuters* に割り当てます。

```
hostname(config-tunnel-general)# default-group-policy sales
```

ステップ 6　トンネル グループ属性モードで **group-alias** コマンドを使用して、WebVPN ログイン ページのグループ リストに表示されるグループ エイリアスを作成し、イネーブルにします。

group-alias *name* **enable**

まず、グローバル コンフィギュレーション モードに戻り、次に **tunnel-group** *name* **webvpn-attributes** コマンドを入力してトンネル グループ属性モードを開始します。

次の例では、トンネル グループ *telecommuters* の webvpn 属性コンフィギュレーション モードを開始して、グループ エイリアス *sales_department* を作成します。

```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```

ステップ 7　webvpn モードで、WebVPN ログインページのトンネル グループ リストの表示をイネーブルにします。

tunnel-group-list enable

まず、グローバル コンフィギュレーション モードに戻り、次に webvpn モードを開始します。

次の例では、webvpn モードを開始してから、トンネル グループ リストをイネーブルにします。

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

ステップ 8　グループ ポリシー モードまたはユーザ名モードで **vpn-tunnel-protocol webvpn** コマンドを使用して、WebVPN を、グループまたはユーザに対して許可された VPN トンネリング プロトコルとして指定します。

vpn-tunnel-protocol webvpn

SSL を指定するには、まず、グローバル コンフィギュレーション モードに戻り、**group-policy** *name* **attributes** コマンドを入力してグループ ポリシー モードに入るか、**username** *name* **attributes** コマンドを入力してユーザ名モードに入ります。次に、**webvpn** コマンドを入力して webvpn モードに入り、グループまたはユーザに対する WebVPN 設定を変更します。

次の例では、グループ ポリシー *sales* に対して許可されたトンネリング プロトコルとして WebVPN を指定します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# vpn-tunnel-protocol webvpn
```

ステップ 9　グループ ポリシー webvpn モードまたはユーザ名 webvpn モードで **svc** コマンドを使用して、特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。

svc {**none** | **enable** | **required**}

次の例では、既存のグループ ポリシー *sales* に対して SVC を *required* に設定します。

```
hostname(config-group-webvpn)# svc required
```

ユーザをグループ ポリシーに割り当てる方法の詳細については、第 30 章「トンネル グループ、グループ ポリシーおよびユーザの設定」を参照してください。

SVC の永続的インストールのイネーブル化

SVC の永続的インストールをイネーブルにすると、SVC の自動アンインストール機能がディセーブルになります。SVC は、後続の SVC 接続のためにリモート コンピュータにインストールされたままなので、リモート ユーザの SVC 接続時間が短縮されます。

特定のグループまたはユーザに対する SVC の永続的インストールをイネーブルにするには、グループ ポリシーまたはユーザ名 webvpn モードで **svc keep-installer** コマンドを使用します。

svc keep-installer {**installed** | **none**}

no svc keep-installer {**installed** | **none**}

それぞれの説明は次のとおりです。

installed は、リモート コンピュータへの SVC の永続的インストールを指定します。

none は、アクティブな SVC 接続が終了した後、リモート コンピュータから SVC が削除されるように指定します。

デフォルトでは、SVC の永続的インストールはディセーブルになっています。リモート コンピュータ上の SVC は、すべての SVC セッションの終了時にアンインストールされます。

次の例では、リモート コンピュータに SVC がインストールされた状態を保持するために、既存のグループ ポリシー *sales* を設定します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc keep-installer installed
```

キーの再生成のイネーブル化

セキュリティ アプライアンスと SVC がキーの再生成を行うときは、暗号キーと初期ベクトルを再ネゴシエーションして、接続のセキュリティを高めます。

特定のグループまたはユーザの SVC セッションで、SVC によるキーの再生成の実行をイネーブルにするには、グループ ポリシー モードおよびユーザ名 webvpn モードで **svc rekey** コマンドを使用します。

svc rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time** *minutes*}

no svc rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time** *minutes*}

それぞれの説明は次のとおりです。

method new-tunnel は、SVC キーの再生成中に SVC が新規トンネルを確立するように指定します。

method none は、SVC キーの再生成をディセーブルにします。

method ssl は、SVC キーの再生成中に SSL の再ネゴシエーションを実行するように指定します。

time *minutes* は、セッションの開始からキーの再生成が発生するまでの時間（分）を指定します。1 ～ 10080（1 週間）の範囲です。

次の例では、セッション開始の 30 分後に実施されるキーの再生成中に、既存のグループ ポリシー *sales* に対する SSL との再ネゴシエーションを実施するように SVC を設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc rekey method ssl
hostname(config-group-policy)# svc rekey time 30
```

Dead Peer Detection のイネーブル化と調整

Dead Peer Detection（DPD）により、ピアの応答がなく接続が失敗している場合には、確実にセキュリティ アプライアンス（ゲートウェイ）または SVC 側で瞬時に検出できます。

セキュリティ アプライアンスまたは SVC で特定のグループまたはユーザについて DPD をイネーブルにし、セキュリティ アプライアンスまたは SVC が DPD を実行する頻度を設定するには、グループ ポリシーまたはユーザ名 webvpn モードで **svc dpd-interval** コマンドを使用します。

svc dpd-interval {[**gateway** {*seconds* | **none***}]* | [**client** {*seconds* | **none***}]*}

no svc dpd-interval {[**gateway** {*seconds* | **none***}]* | [**client** {*seconds* | **none***}]*}

それぞれの説明は次のとおりです。

gateway seconds は、セキュリティ アプライアンス（ゲートウェイ）による DPD の実行をイネーブルにし、セキュリティ アプライアンス（ゲートウェイ）が DPD を実行する頻度を 30 ～ 3600 秒の範囲内で指定します。

gateway none は、セキュリティ アプライアンスによる DPD をディセーブルにします。

client *seconds* は、SVC（クライアント）による DPD の実行をイネーブルにし、SVC が DPD を実行する頻度を 30 ～ 3600 秒の範囲内で指定します。

client none は、SVC によって実行される DPD をディセーブルにします。

svc dpd-interval コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

次の例では、セキュリティ アプライアンスによる DPD の実行頻度が 3000 秒に設定され、SVC による既存のグループ ポリシー *sales* に対する DPD の実行頻度が 1000 秒に設定されています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# svc dpd-interval gateway 3000
hostname(config-group-policy)# svc dpd-interval client 1000
```

キープアライブのイネーブル化

キープアライブ メッセージの頻度を調整することで、接続がアイドルでいられる時間がデバイスによって制限されている場合でも、プロキシ、ファイアウォール、または NAT デバイス経由の SVC 接続をオープンのまま確実に維持します。頻度を調整することで、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケットベースのアプリケーションをアクティブに実行していない場合でも、SVC が切断して再接続をしないようにできます。

キープアライブ メッセージの頻度を設定するには、グループ ポリシーまたはユーザ名 webvpn モードで、次のように **svc keepalive** コマンドを使用します。

svc keepalive {none | *seconds***}**

no svc keepalive {none | *seconds***}**

それぞれの説明は次のとおりです。

none は、SVC のキープアライブ メッセージをディセーブルにします。

seconds は、SVC によるキープアライブ メッセージの送信をイネーブルにし、メッセージの頻度を 15 ～ 600 秒の範囲で指定します。

デフォルトでは、キープアライブ メッセージはディセーブルになっています。

コンフィギュレーションからこのコマンドを削除して、値が継承されるようにするには、コマンドの **no** 形式を使用します。

次の例では、既存のグループ ポリシー *sales* に対して、SVC がキープアライブ メッセージを 300 秒（5 分）の頻度で送信できるようにセキュリティ アプライアンスを設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc keepalive 300
```

SVC 圧縮の使用

SVC 圧縮を行うと、転送されるパケットのサイズが減少するため、セキュリティ アプライアンスと SVC 間の通信パフォーマンスが向上します。デフォルトでは、セキュリティ アプライアンスでは、グローバル レベルと特定のグループまたはユーザの両方において、すべての SVC 接続に対する圧縮がイネーブルになっています。

SVC 圧縮は、グローバル コンフィギュレーション モードで **compression svc** コマンドを使用してグローバルに設定できます。グループ ポリシーおよびユーザ名 webvpn モードで **svc compression** コマンドを使用して、特定のグループまたはユーザに対してこれを設定することもできます。グローバル設定によって、グループ ポリシーおよびユーザ名の設定が上書きされます。

グローバルな SVC 圧縮の変更

グローバルな SVC 圧縮の設定を変更するには、グローバル コンフィギュレーション モードで **compression svc** コマンドを使用します。

compression svc

no compression svc

このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

次の例では、すべての SVC 接続の圧縮は、グローバルにディセーブルになっています。

```
hostname(config)# no compression svc
```

グループおよびユーザに対する SVC 圧縮の変更

特定のグループまたはユーザに対する圧縮を変更するには、グループ ポリシーおよびユーザ名 webvpn モードで **svc compression** コマンドを使用します。

svc compression {**deflate** | **none**}

no svc compression {**deflate** | **none**}

デフォルトでは、グループおよびユーザに対する SVC 圧縮は *deflate*（イネーブル）に設定されています。

コンフィギュレーションから **svc compression** コマンドを削除し、グローバル設定から値が継承されるようにするには、このコマンドの **no** 形式を使用します。

次の例では、グループ ポリシー sales に対して SVC 圧縮はディセーブルです。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc compression none
```

（注）　グローバル コンフィギュレーション モードで設定した **compression svc** コマンドによって、グループ ポリシー モードおよびユーザ名 webvpn モードで設定した **svc compression** コマンドは上書きされます。

SVC セッションの表示

特権 EXEC モードで **show vpn-sessiondb** コマンドを使用すると、アクティブな SVC セッションについての情報を表示できます。

show vpn-sessiondb svc

show vpn-sessiondb svc コマンドの出力例を次に示します。

```
hostname# show vpn-sessiondb svc

Session Type: SSL VPN Client

Username     : lee
Index        : 1                      IP Addr      : 161.44.128.249
Protocol     : SSL VPN Client         Encryption   : 3DES
Hashing      : SHA1                   Auth Mode    : userPassword
TCP Dst Port : 443                    TCP Src Port : 54230
Bytes Tx     : 20178                  Bytes Rx     : 8662
Pkts Tx      : 27                     Pkts Rx      : 19
Client Ver   : Cisco STC 1.1.0.117
Client Type  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Q312461)
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Apr 20 2005
Duration     : 0h:00m:04s
Filter Name  :
```

SVC セッションのログオフ

すべての SVC セッションをログオフするには、グローバル コンフィギュレーション モードで **vpn-sessiondb logoff svc** コマンドを使用します。

vpn-sessiondb logoff svc

次に、すべての SVC セッションをログオフする例を示します。

```
hostname# vpn-sessiondb logoff svc
INFO: Number of sessions of type "svc" logged off : 1
```

個々の SVC セッションは、**name オプションまたは index オプション**を使用してログオフできます。

vpn-session-db logoff name *name*

vpn-session-db logoff index *index*

ユーザ名とインデックス番号（SVC イメージの順序で設定される）は、両方とも **show vpn-sessiondb svc** コマンドの出力で確認できます。次の例は、ユーザ名 *lee* とインデックス番号 *1* を示しています。

```
hostname# show vpn-sessiondb svc

Session Type: SSL VPN Client

Username     : lee
Index        : 1                      IP Addr      : 161.44.128.249
```

```
Protocol     : SSL VPN Client         Encryption   : 3DES
Hashing      : SHA1                   Auth Mode    : userPassword
TCP Dst Port : 443                    TCP Src Port : 54230
Bytes Tx     : 20178                  Bytes Rx     : 8662
Pkts Tx      : 27                     Pkts Rx      : 19
Client Ver   : Cisco STC 1.1.0.117
Client Type  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Q312461)
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Apr 20 2005
Duration     : 0h:00m:04s
Filter Name  :
```

次の例では、**vpn-session-db logoff コマンド**の **name** オプションを使用してセッションを終了します。

```
hostname# vpn-session-db logoff name lee
INFO: Number of sessions with name "lee" logged off : 1
```

SVC のアップデート

セキュリティ アプライアンスの SVC イメージは、次の手順を使用していつでもアップデートできます。

ステップ 1　特権 EXEC モードで **copy** コマンドを使用して、または別の方法で新しい SVC イメージをセキュリティ アプライアンスにコピーします。

ステップ 2　新しい SVC イメージ ファイルの名前が、すでにロードされているファイルと同じ場合は、設定内の **svc image** コマンドを再入力します。新しいファイル名が異なっている場合は、**no svc image** コマンドを使用して古いファイルをアンインストールします。次に、**svc image** コマンドを使用して、SVC イメージに順序を割り当て、セキュリティ アプライアンスが新しい SVC イメージをロードするようにします。