

AnyConnect VPN Client 接続

この項では、AnyConnect VPN Client 接続を設定する方法について説明します。

- AnyConnect クライアントのライセンス要件 (3ページ)
- AnyConnect クライアント 接続の設定 (3ページ)
- AnyConnect クライアント 接続のモニタリング (24 ページ)
- AnyConnect VPN セッションのログオフ (26 ページ)
- AnyConnect クライアント 接続機能の履歴 (26 ページ)

AnyConnect クライアント VPN Client について

AnyConnectクライアントは、ASA へのセキュアな SSL および IKEv2 IPsec 接続をリモートユー ザーに提供します。事前にクライアントがインストールされていない場合、リモートユーザー は、SSL または IPsec/IKEv2 VPN 接続を受け入れるように設定されているインターフェイスの IP アドレスをブラウザに入力します。ASA が、http:// 要求を https:// にリダイレクトするよう に設定されていない限り、ユーザーは URL を https://<address>の形式で入力する必要がありま す。

URL が入力されると、ブラウザはそのインターフェイスに接続し、ログイン画面を表示しま す。ユーザーがログインと認証に成功し、そのユーザーがクライアントを要求しているとASA で識別されると、セキュリティアプライアンスは、リモート コンピュータのオペレーティン グシステムに合うクライアントをダウンロードします。ダウンロード後、クライアントは自分 自身でインストールと設定を行い、セキュアな SSL または IPsec/IKEv2 接続を確立します。接 続の終了時には、(設定に応じて)そのまま残るか、または自分自身をアンインストールしま す。

以前からインストールされているクライアントの場合は、ユーザーの認証時に、ASAによって クライアントのリビジョンが点検され、必要に応じてアップグレードされます。

クライアントが ASA と SSL VPN 接続をネゴシエートした場合は、Transport Layer Security (TLS)を使用して接続します。状況に応じて、Datagram Transport Layer Security (DTLS)が 使用されます。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避さ れ、パケット遅延の影響を受けやすいリアルタイムアプリケーションのパフォーマンスが向上 します。

AnyConnect クライアントは、ASA からダウンロードできます。または、システム管理者が手動でリモート PC にインストールできます。クライアントの手動インストールの詳細については、『Cisco AnyConnect Secure Mobility Configuration Guide』の適切なリリースを参照してください。

ASA は、ユーザーが確立している接続のグループ ポリシーまたはユーザー名属性に基づきク ライアントをダウンロードします。自動的にクライアントをダウンロードするように ASA を 設定するか、またはクライアントをダウンロードするかをリモートユーザーに確認するように 設定できます。後者の場合、ユーザーが応答しなかった場合は、タイムアウト時間が経過した 後にクライアントをダウンロードするか、ログインページを表示するように ASA を設定でき ます。

AnyConnect クライアント の要件

AnyConnect クライアントを実行しているエンドポイントコンピュータの要件については、 『Cisco AnyConnect Secure Mobility Release Notes』の適切なリリース』を参照してください。

に関する注意事項と制限事項 AnyConnect クライアント

- •ASA では、リモート HTTPS 証明書は確認されません。
- シングルまたはマルチコンテキストモードでサポートされます。AnyConnect Apex ライセンスは、マルチコンテキストモードのリモートアクセス VPN に必要です。ASA はAnyConnect Apex ライセンスを特異的に認識しませんが、プラットフォーム制限へのライセンス済み AnyConnect Premium、携帯電話用 AnyConnect クライアント、Cisco VPN フォン用 AnyConnect クライアント、および Advanced Endpoint Assessment など、Apex ライセンスのライセンス特性を適用します。共有ライセンス、AnyConnect Essentials、フェールオーバーライセンス集約、およびフレックス/時間ベースのライセンスはサポートされていません。
- RA VPN ヘッドエンドなどに対する curl などのコマンドの実行は直接サポートされていないため、望ましい結果が得られない可能性があります。たとえば、ヘッドエンドは HTTP HEAD リクエストに応答しません。
- Cisco 88xx シリーズなどのハードウェア VPN 電話機が AnyConnect クライアントを使用すると、DTLS がアップ状態で、Dead Peer Detection (DPD) が構成されていても、再接続が発生することがあります。
- クライアントが AnyConnect クライアントに接続すると、接続の前後でクライアントの IP アドレスが変わります。ASA は、この動作をサポートしています。

AnyConnect クライアントのライセンス要件

(注) この機能は、ペイロード暗号化機能のないモデルでは使用できません。

VPN ライセンスには、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。 モデルごとの最大値については、「Cisco ASA Series Feature Licenses」を参照してください。

クライアントレス SSL VPN セッションを開始後、ポータルから AnyConnect クライアント ク ライアントセッションを開始した場合は、合計で1つのセッションが使用されます。これに対 して、最初に AnyConnect クライアント を(スタンドアロンクライアントなどから)開始後、 クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されま す。

AnyConnect クライアント 接続の設定

ここでは、ASA が AnyConnect VPN クライアント接続を受け入れるように設定するための前提 条件、制限事項、および詳細なタスクについて説明します。

クライアントを Web 展開するための ASA の設定

この項では、AnyConnect クライアント を Web 展開するように ASA を設定する手順について 説明します。

始める前に

TFTP や別の方法を使用して、クライアント イメージ パッケージを ASA にコピーします。



(注) クライアントレス VPN 機能が ASA で無効になっている場合でも、Web ブラウザを使用して AnyConnect Web 展開(https://xxxx<ASA IP address>) にアクセスする際、ASA の VPN セッショ ンはクライアントレスとしてカウントされます。

手順

ステップ1 フラッシュ上のファイルを AnyConnect クライアント パッケージファイルとして指定します。 ASA は、リモート PC にダウンロードするために、キャッシュ メモリのファイルを展開しま す。複数のクライアントがある場合は、order 引数を使用して、クライアント イメージに順序 を割り当てます。 ASAは、リモートPCのオペレーティングシステムと一致するまで、指定されている順序で各 クライアントの一部をダウンロードします。そのため、最も一般的に使用されているオペレー ティングシステム用のイメージには、最も低い数値を割り当てます。

anyconnect image filename order

例:

```
hostname(config-webvpn)# anyconnect image
anyconnect-win-2.3.0254-k9.pkg 1
hostname(config-webvpn)# anyconnect image
anyconnect-macosx-i386-2.3.0254-k9.pkg 2
hostname(config-webvpn)# anyconnect image
anyconnect-linux-2.3.0254-k9.pkg 3
```

(注)

anyconnect image コマンドで AnyConnect クライアント イメージを設定した後に anyconnect enable コマンドを発行する必要があります。AnyConnect クライアント をイネーブルにしない 場合、AnyConnect の動作は不完全になり、show webvpn anyconnect コマンドは SSL VPN クラ イアントがイネーブルにされていないと見なし、インストールされた AnyConnect クライアン ト パッケージのリストは表示されません。

ステップ2 クライアントレス接続または AnyConnect クライアント SSL 接続のインターフェイスの SSL を イネーブルにします。

enable interface

例:

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

ステップ3 このコマンドを発行しないと、AnyConnect クライアント は想定したとおりに機能せず、show webvpn anyconnect コマンドは、インストールされた AnyConnect クライアント パッケージの リストを表示する代わりに、「SSL VPN is not enabled」というメッセージを返します。

AnyConnect のイネーブル

ステップ4 (任意) アドレス プールを作成します。DHCP やユーザーによる割り当てのアドレスの指定 など、別のアドレス割り当ての方法を使用することもできます。

ip local pool poolname startaddr-endaddr mask mask

例:

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

ステップ5 アドレス プールをトンネル グループに割り当てます。

address-pool poolname

例:

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

ステップ6 デフォルトのグループ ポリシーをトンネル グループに割り当てます。

default-group-policy name

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

ステップ7 クライアントレスポータルおよび AnyConnect クライアント GUI のログインページでのトンネ ルグループリストの表示をイネーブルにします。エイリアスのリストは、group-alias name enable コマンドによって定義されます。

group-alias name enable

例:

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

ステップ8 グループまたはユーザーの許可された VPN トンネリングプロトコルとして AnyConnect クライ アント を指定します。

tunnel-group-list enable

例:

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

ステップ9 グループまたはユーザーの許可された VPN トンネリング プロトコルとして SSL を指定しま す。その他のプロトコルを追加して指定することもできます。詳細については、コマンドリ ファレンスの vpn-tunnel-protocol コマンドを参照してください。

vpn-tunnel-protocol

例:

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

次のタスク

グループ ポリシーに対するユーザーの割り当ての詳細については、第6章「接続プロファイル、グループ ポリシー、およびユーザーの設定」を参照してください。

永続的なクライアント インストールのイネーブル化

永続的なクライアントインストールをイネーブルにすると、クライアントの自動アンインス トール機能がディセーブルになります。クライアントは、後続の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 ユーザーの接続時間が短縮されます。 特定のグループまたはユーザーに対する永続的なクライアント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 webvpn モードまたはユーザー名 webvpn モードで anyconnect keep-installer コマンドを使用します。

デフォルトでは、クライアントの永続的なインストールはイネーブルになっています。セッションの終了時に、クライアントはリモート コンピュータ上に残ります。次の例では、セッションの終了時点でリモート コンピュータのクライアントを削除するように既存のグループ 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)# anyconnect keep-installer installed none

DTLS の設定

Datagram Transport Layer Security(DTLS)を使用すると、SSL VPN 接続を確立している AnyConnect クライアントで、2 つのトンネル(SSL トンネルと DTLS トンネル)を同時に使 用できます。DTLS を使用すると、SSL 接続で発生する遅延および帯域幅の問題が回避され、 パケット遅延の影響を受けやすいリアルタイムアプリケーションのパフォーマンスが向上しま す。

始める前に

このヘッドエンドで DTLS を設定し、使用する DTLS のバージョンを確認するには、SSL の詳 細設定 を参照してください。

DTLS を TLS 接続にフォール バックさせるには、デッドピア検知(DPD) をイネーブルにす る必要があります。DPD をイネーブルにしない場合、DTLS 接続で問題が発生すると、TLS に フォール バックする代わりに接続は終了します。DPD の詳細については、デッドピア検出の 設定(19ページ)を参照してください。

手順

ステップ1 AnyConnect クライアント VPN 接続に対して DTLS オプションを指定します。

a) webvpn モードのインターフェイスで SSL と DTLS を有効にします。

デフォルトでは、DTLS がイネーブルになるのは、インターフェイスで SSL VPN アクセス をイネーブルにした場合です。

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

webvpn コンフィギュレーション モードで、enable *interface* tls-only コマンドを使用し、すべての AnyConnect クライアント ユーザーに対して DTLS をディセーブルにします。

DTLS をディセーブルにすると、SSL VPN 接続は SSL VPN トンネルだけに接続します。

hostname(config)# webvpn
hostname(config-webvpn)# enable outside tls-only

b) port および dtls port コマンドを使用して SSL および DTLS のポートを設定します。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
hostname(config-webvpn)# port 555
hostname(config-webvpn)# dtls port 556
```

- ステップ2 特定のグループ ポリシーに対して DTLS オプションを指定します。
 - a) グループ ポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コン フィギュレーションモードで、anyconnect ssl dtls コマンドを使用して特定のグループまた はユーザーに対して DTLS をイネーブルにします。

hostname(config)# group-policy sales attributes hostname(config-group-policy)# webvpn hostname(config-group-webvpn)# anyconnect ssl dtls enable

b) 必要に応じて、anyconnect dtls compression コマンドを使用して DTLS 圧縮をイネーブルに します。

hostname(config-group-webvpn)# anyconnect dtls compression lzs

リモート ユーザーに対するプロンプト

手順

ASA で、リモート SSL VPN クライアント ユーザーがクライアントをダウンロードするための プロンプトをイネーブルにするには、グループポリシー webvpn コンフィギュレーションモー ドまたはユーザー名 webvpn コンフィギュレーション モードで anyconnect ask コマンドを使用 します。

[no] anyconnect ask {none | enable [default {webvpn | } timeout value]}

- anyconnect enable を指定すると、クライアントをダウンロードするか、クライアントレスポータルページに移動するかを尋ねるプロンプトをリモートユーザーに表示し、ユーザーの応答を無期限に待機します。
- anyconnect ask enable default を指定すると、すぐにクライアントがダウンロードされます。
- anyconnect ask enable default webvpn を指定すると、すぐにポータル ページに移動します。
- anyconnect ask enable default timeoutvalue を指定すると、クライアントをダウンロードするか、またはクライアントレスポータルページに移動するかを尋ねるプロンプトをリモートユーザーに表示し、デフォルトアクション(クライアントのダウンロード)を実行する前に、valueの間待機します。

 anyconnect ask enable default clientless timeoutvalue を指定すると、クライアントをダウン ロードするか、またはクライアントレスポータルページに移動するかを尋ねるプロンプ トをリモートユーザーに表示し、デフォルトアクション(クライアントレスポータル ページの表示)を実行する前に、valueの間待機します。

次の図に、**default anyconnect timeout** *value* または **default webvpn timeout** *value* が設定された 場合にリモート ユーザーに表示されるプロンプトを示します。

8° s	econd	S.	wiii 3	lantin	1112		
		• 5	tartr	<u>10W</u>			
		• <u>C</u>	ance	1			

例

次の例では、ASA でクライアントをダウンロードするか、またはクライアントレス ポータルページに移動するかをユーザーに尋ねるプロンプトを表示して、クライアン トをダウンロードする前に応答を 10 秒待機するように設定しています。

hostname(config-group-webvpn)# anyconnect ask enable default anyconnect timeout
10

AnyConnect クライアント プロファイルダウンロードのイネーブル化

AnyConnect クライアント プロファイル (コア クライアントとその VPN 機能のコンフィギュ レーション設定、およびオプションのクライアントモジュールのコンフィギュレーション設定 を含む XML ファイル) で AnyConnect クライアント 機能をイネーブルにします。ASA は AnyConnect クライアント のインストールおよび更新中にプロファイルを展開します。ユーザ がプロファイルの管理や修正を行うことはできません。

クライアントにダウンロードされるファイルのフォーマットは、<profile_name>.xml です。

プロファイルは、AnyConnect クライアント プロファイル エディタを使用して設定できます。 このエディタは、ASDM または ISE から起動できる便利な GUI ベースの構成ツールです。 Windows 用 AnyConnect クライアント ソフトウェアパッケージにはエディタが含まれていま す。このエディタは、クライアントパッケージを選択したヘッドエンドデバイスにロードし、 AnyConnect クライアント イメージとして指定するとアクティブになります。

ASDM または ISE に統合されたプロファイル エディタの代わりに、Windows 用プロファイル エディタのスタンドアロンバージョンも使用できます。クライアントを事前展開する場合は、 ソフトウェア管理システムを使用してコンピュータに展開する、VPNサービス用のプロファイルおよびその他のモジュールを、スタンドアロンのプロファイルエディタを使用して作成できます。

AnyConnect クライアントおよびプロファイルエディタの詳細については、『Cisco AnyConnect Secure Mobility Configuration Guide』の適切なリリースを参照してください。

(注) AnyConnect クライアントプロトコルのデフォルトは SSL です。IPsec IKEv2 をイネーブルにするには、ASA で IKEv2 設定を設定し、また、クライアントプロファイルのプライマリプロトコルとして IKEv2 を設定する必要があります。IKEv2enabled プロファイルは、エンドポイントコンピュータに展開する必要があります。それ以外の場合、クライアントは SSL を使用して接続を試行します。

手順

- **ステップ1** ASDM/ISEのプロファイルエディタまたはスタンドアロンプロファイルエディタを使用して、 プロファイルを作成します。
- **ステップ2** tftp または別の方式を使用して、ASA のフラッシュ メモリにプロファイル ファイルをロード します。
- ステップ3 webvpn コンフィギュレーションモードで anyconnect profiles コマンドを使用して、キャッシュ メモリにロードするクライアント プロファイルとしてこのファイルを識別します。

例:

次に、プロファイルとしてファイル sales_hosts.xml と engineering_hosts.xml を指定する例を示します。

asal(config-webvpn)# anyconnect profiles sales disk0:/sales_hosts.xml asal(config-webvpn)# anyconnect profiles engineering disk0:/engineering_hosts.xml

これで、プロファイルをグループポリシーに利用できます。

dir cache:stc/profiles コマンドを使用して、キャッシュメモリにロードされたプロファイルを 表示します。

hostname(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0 ---- 774 11:54:41 Nov 22 2006 engineering.xml 0 ---- 774 11:54:29 Nov 22 2006 sales.xml 2428928 bytes total (18219008 bytes free) hostname(config-webvpn)# ステップ4 グループ ポリシー webvpn コンフィギュレーション モードを開始し、anyconnect profiles コマ ンドを使用して、グループ ポリシーのクライアント プロファイルを指定します。

例:

使用可能なプロファイルを表示するには、client profiles value コマンドに続けて、疑問符(?) を入力します。次に例を示します。

asa1(config-group-webvpn)# anyconnect profiles value ?

```
config-group-webvpn mode commands/options:
Available configured profile packages: engineering sales
```

次の例では、クライアントプロファイルタイプが vpn のプロファイル sales を使用するように グループ ポリシーを設定します。

asal(config-group-webvpn) # anyconnect profiles value sales type vpn
asal(config-group-webvpn) #

AnyConnect クライアント 遅延アップグレードのイネーブル化

AnyConnect クライアント ユーザーは、遅延アップグレードを使用して、クライアントアップ グレードのダウンロードを遅らせることができます。クライアントアップデートが使用できる 場合、AnyConnect クライアントは、更新するか、またはアップグレードを延期するかを尋ね るダイアログを開きます。AnyConnect クライアント プロファイル設定で [自動更新 (AutoUpdate)]が [有効(Enabled)]に設定されていない限り、このアップグレードダイアロ グは表示されません。

遅延アップグレードをイネーブルにするには、カスタム属性タイプと名前付きの値を ASA に 追加して、グループ ポリシーでこれらの属性を参照および設定します。

次のカスタム属性は遅延アップグレードをサポートします。

表1:遅延アップグレードのカスタム属性

カスタム属性タイプ	有効な値	デフォルト値	注意
DeferredUpdateAllowed	true false	false	[true]を指定すると、延期アップデートが有効 になります。延期アップデートが無効(false) の場合、下記の設定は無視されます。

カスタム属性タイプ	有効な値	デフォルト値	注意
DeferredUpdateMinimumVersion	x.y.z	0.0.0	アップデートを遅延できるようにインストー ルする必要がある AnyConnect クライアントの 最小バージョン。
			最小バージョンのチェックは、ヘッドエンド で有効になっているすべてのモジュールに適 用されます。VPNを含む有効な任意のモジュー ルがインストールされていない、または最小 要件を満たしていない場合、接続して延期アッ プデートすることはできません。
			この属性が指定されていない場合、エンドポ イントにインストールされているバージョン に関係なく、延期プロンプトが表示されるか (自動的に却下されます)。
DeferredUpdateDismissTimeout	0~300(秒)	none (ディセー ブル)	延期アップグレードプロンプトが表示され、 自動的に却下されるまでの秒数。この属性は、 延期アップデートプロンプトを表示する場合 のみ適用されます(最小バージョンの属性が 最初に評価されます)。
			この属性が見つからない場合、自動却下機能 が無効になり、ユーザーが応答するまで(必 要に応じて)ダイアログが表示されます。
			この属性をゼロに設定すると、次に基づいて 強制的に自動延期またはアップグレードが実 施されます。
			 インストール済みバージョンと
			DeferredUpdateMinimumVersionの値 • DeferredUpdateDismissResponseの値
DeferredUpdateDismissResponse	defer update	update	DeferredUpdateDismissTimeout 発生時に実施するアクション。

手順

ステップ1 webvpn コンフィギュレーションモードで anyconnnect-custom-attr コマンドを使用してカスタ ム属性タイプを作成します。

[no] anyconnect-custom-attr *attr-type* [description *description*]

例:

次に、カスタム属性タイプ DeferredUpdateAllowed および DeferredUpdateDismissTimeout を追加 する例を示します。

hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
description Indicates if the deferred update feature is enabled or not
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateDismissTimeout

ステップ2 グローバル コンフィギュレーション モードで anyconnect-custom-data コマンドを使用してカ スタム属性の名前付きの値を追加します。長い値を持つ属性の場合は、重複するエントリを指 定でき、連結が可能です。ただし、設定エントリが重複している場合、[Defer Update] ダイア ログは表示されず、ユーザーはアップグレードを保留できません。代わりに、アップグレード が自動的に行われます。

[no] anyconnect-custom-data attr-type attr-name attr-value

例:

次に、カスタム属性タイプ DeferredUpdateDismissTimeout の名前付きの値と、 DeferredUpdateAllowed をイネーブルにするための名前付きの値を追加する例を示します。

```
hostname(config)# anyconnect-custom-data DeferredUpdateDismissTimeout
def-timeout 150
hostname(config)# anyconnect-custom-data DeferredUpdateAllowed
def-allowed true
```

- **ステップ3** anyconnect-custom コマンドを使用して、カスタム属性の名前付きの値をグループ ポリシーに 追加するか、グループ ポリシーから削除します。
 - anyconnect-customattr-type value attr-name
 - anyconnect-custom attr-type none
 - no anyconnect-custom attr-type

例:

次に、sales という名前のグループ ポリシーで延期アップデートを有効にしてタイムアウトを 150 秒に設定する例を示します。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# anyconnect-custom DeferredUpdateAllowed
value def-allowed
hostname(config-group-policy)# anyconnect-custom DeferredUpdateDismissTimeout
value def-timeout
```

DSCPの保存の有効化

Windows または OS X プラットフォームでは、DTLS 接続の場合にのみ別のカスタム属性を設 定することで DiffServ コード ポイント (DSCP) を制御できます。DSCP の保存を有効にする と、デバイスは遅延の影響を受けやすいトラフィックを優先することができます。ルータで は、これが設定されているかどうかが反映され、アウトバウンド接続品質の向上のために優先 トラフィックがマークされます。

手順

ステップ1 webvpn コンフィギュレーション モードで anyconnect-custom-attr コマンドを使用してカスタ ム属性タイプを作成します。

[no] anyconnect-custom-attr DSCPPreservationAllowed description Set to control Differentiated Services Code Point (DSCP) on Windows or OS X platforms for DTLS connections only.

ステップ2 グローバル コンフィギュレーション モードで anyconnect-custom-data コマンドを使用してカ スタム属性の名前付きの値を追加します。

[no] anyconnect-custom-data DSCPPreservationAllowed true

(注)

デフォルトでは、AnyConnectクライアントはDSCPの保存を実行します(true)。無効にする には、ヘッドエンドでカスタム属性を false に設定し、接続を再実行します。

追加 AnyConnect クライアント 機能のイネーブル化

ダウンロード時間を最小限に抑えるために、クライアントは必要なコアモジュールのダウン ロード(ASAまたはISEから)だけを要求します。追加機能がAnyConnectクライアントで使 用可能になったら、それらの機能を使用できるようにするためにリモートクライアントを更新 する必要があります。

新しい機能をイネーブルにするには、グループ ポリシー webvpn またはユーザー名 webvpn コ ンフィギュレーション モードで anyconnect modules コマンドを使用して、新しいモジュール 名を指定する必要があります。

[no]anyconnect modules {none | value string}

複数のストリングを指定する場合は、カンマで区切ります。

Start Before Logon のイネーブル化

Start Before Logon (SBL) を使用すると、Windows PC にインストールされている AnyConnect クライアントに対するログインスクリプト、パスワードキャッシング、ドライブマッピングな どが使用できるようになります。SBL では、AnyConnect クライアントの Graphical Identification and Authentication (GINA) をイネーブルにするモジュールをダウンロードするように ASA を イネーブルにする必要があります。次の手順は、SBL をイネーブルにする方法を示していま す。

手順

ステップ1 グループ ポリシー webvpn またはユーザー名 webvpn コンフィギュレーション モードで anyconnect modules *vpngina* コマンドを使用して、特定のグループまたはユーザーへの VPN 接 続のための GINA モジュールを ASA でダウンロードする機能を有効にします。

例:

次の例では、ユーザーはグループ ポリシー telecommuters でグループ ポリシー属性モードを開始し、そのグループポリシーで webvpn コンフィギュレーションモードを開始し、ストリング vpngina を指定します。

hostname(config)# group-policy telecommuters attributes hostname(config-group-policy)# webvpn hostame(config-group-webvpn)#anyconnect modules value vpngina

ステップ2 クライアントプロファイルファイル (AnyConnectProfile.tmpl)のコピーを取得します。

ステップ3 プロファイル ファイルを編集して SBL がイネーブルであることを指定します。次の例では、 Windows 用のプロファイル ファイル (AnyConnectProfile.tmpl)の関係部分を示しています。

```
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>false</UseStartBeforeLogon>
</ClientInitialization>
```

<UseStartBeforeLogon>タグによって、クライアントがSBLを使用するかどうかが決まります。
 SBLをオンにするには、*falseを true* で置き換えます。次の例は、SBL がオンになっているタグを示しています。

```
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

ステップ4 AnyConnectProfile.tmpl に対する変更を保存し、webvpn コンフィギュレーションモードで profile コマンドを使用して、ASA のグループまたはユーザーに対するプロファイル ファイルをアップデートします。次に例を示します。

asa1(config-webvpn)#anyconnect profiles sales disk0:/sales_hosts.xml

AnyConnect クライアント ユーザーメッセージの言語の変換

ASA には、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザーに表示されるポータルと画面、および Cisco AnyConnect VPN Client ユーザーに表示されるインターフェイスの言語変換機能があります。

この項では、これらのユーザーメッセージを変換するために ASA を設定する方法について説明します。

言語変換について

リモートユーザーに可視である機能エリアとそれらのメッセージは、変換ドメイン内にまとめ られています。すべての Cisco AnyConnect VPN Client のユーザーインターフェイスに表示され るメッセージは、AnyConnect クライアント ドメイン内にあります。

ASAのソフトウェアイメージパッケージには、AnyConnectクライアントドメインの変換テー ブルテンプレートが含まれています。このテンプレートはエクスポートでき、入力する URL にテンプレートの XML ファイルが作成されます。このファイルのメッセージフィールドは空 です。メッセージを編集して、テンプレートをインポートし、フラッシュメモリに置かれる新 しい変換テーブル オブジェクトを作成できます。

既存の変換テーブルをエクスポートすることもできます。作成した XML ファイルに事前に編 集したメッセージが表示されます。この XML ファイルを同じ言語名で再インポートすると、 変換テーブルオブジェクトの新しいバージョンが作成され、以前のメッセージが上書きされま す。AnyConnect クライアント ドメインの変換テーブルに対する変更は、ただちに AnyConnect クライアント クライアントユーザーに表示されます。

変換テーブルの作成

次の手順では、AnyConnect クライアント ドメインの変換テーブルを作成する方法について説 明します。

手順

ステップ1 特権 EXEC モードで **export webvpn translation-table** コマンドを使用して、コンピュータに変換テーブル テンプレートをエクスポートします。

次の例では、show import webvpn translation-table コマンドによって、使用可能な変換テーブ ルテンプレートとテーブルを表示しています。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
```

PortForwarder url-list webvpn Citrix-plugin RPC-plugin Telnet-SSH-plugin VNC-plugin

Translation Tables:

次に、AnyConnect クライアント 変換ドメイン用の変換テーブルをエクスポートします。作成 された XML ファイルのファイル名は *client* という名前が付けられ、空のメッセージフィール ドが含まれています。 hostname# export webvpn translation-table AnyConnect template tftp://209.165.200.225/client

次の例では、テンプレートからインポートした *zh* という名前の変換テーブルをエクスポート します。*zh* は Microsoft Internet Explorer における中国語の省略形です。

hostname# export webvpn translation-table customization
language zh tftp://209.165.200.225/chinese_client

ステップ2 変換テーブルのXMLファイルを編集します。次の例は、AnyConnectクライアントテンプレートの一部を示しています。この出力の最後には、ConnectedメッセージのメッセージIDフィールド(msgid)とメッセージ文字列フィールド(msgstr)が含まれています。このメッセージは、クライアントが VPN 接続を確立するときに AnyConnect クライアント GUI に表示されます。完全なテンプレートには、多くのメッセージフィールドのペアが含まれています。

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"
#: C:\cygwin\home\<user>\cvc\main\Api\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\check\AgentIfc.cpp:22
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp~:20
```

```
#: C:\cygwin\home\<user>\cvc\main\Api\save\older\AgentIfc.cpp:22
msgid "Connected"
msgstr ""
```

msgid には、デフォルト変換が含まれています。msgid に続く msgstr が変換を提供します。変換を作成するには、msgstr 文字列の引用符の間に変換対象のテキストを入力します。たとえば、メッセージ「Connected」をスペイン語で変換するには、引用符の間にスペイン語のテキストを挿入します。

```
msgid "Connected"
msgstr "Conectado"
```

ファイルは必ず保存してください。

ステップ3 特権 EXEC モードで import webvpn translation-table コマンドを使用して、変換テーブルをイ ンポートします。ブラウザと互換性がある言語の省略形を付けて新しい変換テーブルの名前を 指定します。

次の例では、米国スペイン語用の Microsoft Internet Explorer で使用される省略形である *es-us* で XML ファイルがインポートされます。

customization keepout url-list webvpn Citrix-plugin RPC-plugin Telnet-SSH-plugin VNC-plugin

Translation Tables: es-us AnyConnect

変換テーブルの削除

変換テーブルが必要なくなった場合は、削除できます。

手順

ステップ1 既存の変換テーブルを一覧表示します。

次の例では、show import webvpn translation-table コマンドによって、使用可能な変換テーブ ルテンプレートとテーブルを表示しています。フランス語(fr)、日本語(ja)、ロシア語 (ru)のさまざまなテーブルが用意されています。

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
 banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  fr
                       PortForwarder
  fr
                       AnyConnect
  fr
                       customization
  fr
                       webvpn
```

ja	PortForwarder
ja	AnyConnect
ja	customization
ja	webvpn
ru	PortForwarder
ru	customization
ru	webvpn

ステップ2 不要な変換テーブルを削除します。

revert webvpn translation-table translationdomain language language

translationdomain は上記に示す変換テーブルの右側に記載されているドメインで、*language* は 2 文字の言語名です。

各テーブルを個別に削除する必要があります。1つのコマンドを使用して、特定の言語のテー ブルをすべて削除することはできません。

たとえば、AnyConnect クライアントのフランス語の変換テーブルを削除するには、次のコマンドを使用します。

ciscoasa# revert webvpn translation-table any connect language fr ciscoasa#

高度な AnyConnect クライアント SSL 機能の設定

次の項では、AnyConnect クライアント SSL VPN 接続を調整する高度な機能について説明します。

キー再生成の有効化

ASA と AnyConnect クライアント が SSL VPN 接続でキー再生成を行うときは、暗号キーと初 期化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ーの SSL VPN 接続で、クライアントによるキー再生成の実行を 有効にするには、グループポリシー webvpn モードまたはユーザー名 webvpn モードで anyconnect ssl rekey コマンドを使用します。

[no]anyconnect ssl rekey {method {new-tunnel | none | ssl} | time minutes}

- method new-tunnel キーの再生成中にクライアントによって新しいトンネルが確立される ことを指定します。
- method ssl キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
- method none キーの再生成を無効にします。
- timeminutes は、セッションの開始からまたは前回のキー再生成から、キーの再生成が行われるまでの時間を1から10080(1週間)の分数で指定します。

(注) キーの再生成方法を ssl または new-tunnel に設定すると、キー再生成時に SSL 再ネゴシエー ションが行われず、クライアントがキー再生成時に新規トンネルを確立することが指定されま す。anyconnect ssl rekey コマンドの履歴については、コマンドリファレンスを参照してください。

次の例では、セッション開始の 30 分後に実施されるキー再生成中に、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クライアントを設定してい ます。

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

デッドピア検出の設定

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、ASA (ゲートウェイ) またはクライアント側で瞬時に検出できます。デッドピア検出 (DPD) を有 効にし、AnyConnect クライアント または ASA ゲートウェイが DPD を実行する頻度を設定す るには、以下の手順を実行します。

始める前に

- この機能は、ASAゲートウェイとAnyConnectクライアントSSL VPN クライアント間の接続のみに適用されます。DPDは、埋め込みが許可されない標準実装に基づくため、IPsecとは併用できません。
- DTLSをイネーブルにすると、Dead Peer Detection (DPD) もイネーブルになります。DPD により、失敗したDTLS接続のTLSへのフォールバックがイネーブルになります。それ以 外の場合、接続は終了します。
- ASA で DPD が有効になっているとき、Optimal MTU (OMTU) 機能を使用すると、クラ イアントが DTLS パケットを正常に渡すことができる最大のエンドポイント MTU を見つ けることができます。最大 MTU までパディングされた DPD パケットを送信することに よって、OMTU を実装します。ペイロードの正しいエコーをヘッドエンドから受信する と、MTUサイズが受け入れられます。受け入れられなかった場合、MTU は小さくされ、 プロトコルで許可されている最小 MTU に到達するまで、繰り返しプローブが送信されま す。

手順

ステップ1 目的のグループ ポリシーに移動します。 グループ ポリシーまたはユーザー名 webvpn モードを開始します。

```
hostname(config)# group-policy group-policy-name attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

または

```
hostname# username attributes
hostname(config-username)# webvpn
hostname (config-username-webvpn #
```

ステップ2 ゲートウェイ側の検出を設定します。

[no] anyconnect dpd-interval {[gateway {seconds | none}] コマンドを使用します。

gateway は、ASA のことです。DPD を有効にし、ASA がクライアントからのパケットを待機 する時間を 30 秒(デフォルト)から 3600 秒(1 時間)の範囲で指定します。値 300 が推奨さ れます。その間隔内にパケットが受信されない場合、ASA は同じ間隔で DPD テストを 3 回試 行します。ASA はクライアントからの応答がない場合、TLS/DTLS トンネルを切断します。

(注)

noneを指定すると、ASA が実行する DPD テストはディセーブルになります。このコマンドを 構成から削除するには、**no anyconnect dpd-interval**を使用します。

noneを指定すると、ASA が実行する DPD テストはディセーブルになります。このコマンドを 設定から削除するには、 **no anyconnect dpd-interval** を使用します。

ステップ3 クライアント側の検出を設定します。

[no] anyconnect dpd-interval {[client {seconds | none}]] コマンドを使用します。

client は AnyConnect クライアントのことです。DPD を有効にし、クライアントが DPD テスト を実行する頻度を 30 秒 (デフォルト)から 3600 秒 (1 時間)の範囲で指定します。30 秒が推 奨されます。

client none を指定すると、クライアントにより実行される DPD はディセーブルになります。 このコマンドを設定から削除するには、no anyconnect dpd-interval を使用します。

例

次の例では、ASA による DPD の実行頻度が 30 秒に設定され、クライアント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 10 秒に設定されています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 30
hostname(config-group-webvpn)# anyconnect dpd-interval client 10
```

キープアライブの有効化

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SSL VPN接続をオープンのまま維持します。また、頻度を調整すると、リモートユーザー が Microsoft Outlook または Microsoft Internet Explorer などのソケット ベース 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、クライアントは切断および再接続されません。

キープアライブはデフォルトでイネーブルになっています。キープアライブをディセーブルに すると、フェールオーバーの際に、SSL VPN クライアント セッションはスタンバイ デバイス に引き継がれません。

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 webvpn またはユーザー 名 webvpn コンフィギュレーション モードから keepalive コマンドを使用します。設定からコ マンドを削除して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。

[no] anyconnect ssl keepalive {none | seconds}

- none は、クライアントのキープアライブ メッセージを無効にします。
- secondsは、クライアント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。

次の例では、既存のグループポリシー *sales* に対して、クライアントがキープアライ ブメッセージを 300 秒(5分)の頻度で送信できるように ASA を設定しています。

hostname(config)# group-policy sales attributes hostname(config-group-policy)# webvpn hostname(config-group-webvpn)# anyconnect ssl keepalive 300

圧縮の使用

圧縮により、低帯域幅の接続に転送されるパケットのサイズが減少し、ASAとクライアント間の通信パフォーマンスが向上します。デフォルトでは、ASAでは、グローバルレベルと特定のグループまたはユーザーの両方において、すべてのSSL VPN 接続に対する圧縮がイネーブルになっています。



(注) ブロードバンド接続の圧縮を実装する場合は、圧縮が損失が少ない接続に依存していることを 慎重に考慮する必要があります。これが、ブロードバンド接続ではデフォルトで圧縮がイネー ブルになっていない主な理由です。

圧縮は、グローバルコンフィギュレーションモードで compression コマンドを使用してグロー バルにオンにする必要があります。そうすることで、グループ ポリシーおよびユーザー名 webvpn モードで anyconnect ssl compression コマンドを使用して、特定のグループまたはユー ザーに圧縮を設定することができます。

圧縮のグローバルな変更

グローバルな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 anyconnect ssl compression コマンドを使用します。設定からコマンドを削除するには、コマン ドの no 形式を使用します。

次の例では、すべての SSL VPN 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

グループおよびユーザーに対する圧縮の変更

特定のグループまたはユーザー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 ザー名 webvpn モードで anyconnect ssl compression コマンドを使用します。

[no] anyconnect ssl compression {deflate | none}

デフォルトでは、グループおよびユーザーに対する SSL 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 anyconnect ssl 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。

次に、グローバルポリシー salesの圧縮をディセーブルにする例を示します。

hostname(config)# group-policy sales attributes hostname(config-group-policy)# webvpn hostname(config-group-webvpn)# no anyconnect ssl compression none

MTU サイズの調整

クライアントによって確立された SSL VPN 接続の MTU サイズ(576~1406 バイト)は、グ ループポリシー webvpn またはユーザー名 webvpn コンフィギュレーションモードで anyconnect mtu コマンドを使用して調整できます。

[no] anyconnect mtu size

このコマンドは、AnyConnect クライアントのみに影響します。レガシー Cisco SSL VPN クラ イアント (SVC) は、さまざまな MTU サイズに調整できません。また、SSL で確立されたク ライアント接続と DTLS による SSL で確立された接続は、このコマンドの影響を受けます。

デフォルトのグループ ポリシーでのこのコマンドのデフォルトは、no anyconnect mtu です。 MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS の オーバーヘッドを差し引いて、自動的に調整されます。

たとえば、ISE Posture AnyConnect モジュールの実行時に、「MTU configuration sent from the secure gateway is too small」というメッセージが表示されることがあります。anyconnect ssl df-bit-ignore disable と一緒に anyconnect mtu 1200 を入力すると、これらのシステム スキャン エラーを回避できます。

例

次の例では、グループ ポリシー telecommuters の MTU サイズを 1200 バイトに設定します。

hostname(config)# group-policy telecommuters attributes hostname(config-group-policy)# webvpn hostname(config-group-webvpn)# anyconnect mtu 1200

AnyConnect クライアント イメージの更新

ASA のクライアントイメージは、次の手順を使用していつでもアップデートできます。

手順

- **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クライアントイメージを ASA にコピーします。
- ステップ2 新しいクライアント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anyconnectimage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]anyconnectimage 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、anyconnectimageコマンドを使用して、イメージに順序を割り当て、ASAが新しいイメージをロードするようにします。

IPv6 VPN アクセスのイネーブル化

IPv6 アクセスを設定する場合は、コマンドラインインターフェイスを使用します。ASA のリ リース 9.0(x) では、外部インターフェイスへの IPv6 VPN 接続(SSL および IKEv2/IPsec プロ トコルを使用)のサポートが追加されています。

IPv6アクセスをイネーブルにするには、SSL VPN 接続のイネーブル化の一部として ipv6 enable コマンドを使用します。次は、外部インターフェイスで IPv6 をイネーブルにする IPv6 接続の 例です。

hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable

IPV6 SSL VPN をイネーブルにするには、次の一般的なアクションを実行します。

- 1. 外部インターフェイスで IPv6 をイネーブルにする。
- 2. 内部インターフェイスで IPv6 および IPv6 アドレスをイネーブルにする。
- 3. クライアント割り当て IP アドレス用に IPv6 アドレス ローカル プールを設定する。
- 4. IPv6 トンネルのデフォルトゲートウェイを設定する。

手順

ステップ1 インターフェイスを設定します。

interface GigabitEthernet0/0
nameif outside
security-level 0

```
ip address 192.168.0.1 255.255.255.0
ipv6 enable ; Needed for IPv6.
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.0.1 255.255.0.0
ipv6 address 2001:DB8::1/32 ; Needed for IPv6.
ipv6 enable ; Needed for IPv6.
```

```
ステップ2 「ipv6 local pool」(IPv6 アドレスの割り当てに使用)を設定します。
```

ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100 ; Use your IPv6 prefix here

(注) AnyConnect クライアント に IPv4 アドレスと IPv6 アドレスの一方または両方を割り当てるように ASA を設定できます。そのように設定するには、ASA 上で内部アドレスプールを作成するか、ASA 上のローカルユーザーに専用アドレスを割り当てます。

ステップ3 ipv6 アドレス プールをトンネルグループ ポリシー(またはグループ ポリシー)に追加します。

tunnel-group YourTunGrp1 general-attributes ipv6-address-pool ipv6pool

(注) ここでは「address-pool」コマンドを使用して IPv4 アドレスプールも設定する必要があります。

ステップ4 IPv6 トンネルのデフォルト ゲートウェイを設定します。

ipv6 route inside ::/0 X:X:X:X:X tunneled

AnyConnect クライアント 接続のモニタリング

アクティブなセッションに関する情報を表示するには、show vpn-sessiondb コマンドを使用し ます。

コマンド	目的
show vpn-sessiondb	アクティブなセッションに関する情報を表示します。
vpn-sessiondb logoff	VPN セッションをログオフします。
show vpn-sessiondb anyconnect	VPNセッションの要約を拡張して、OSPFv3セッション ます。
show vpn-sessiondb ratio encryption	Suite-B のアルゴリズム(AES-GCM-128、AES-GCM-192 AES-GCM-256、AES-GMAC-128 など)用のトンネル数: ンテージを表示します。

(注) AnyConnect 親トンネル

AnyConnect 親トンネルには IP アドレスが割り当てられません。

これは、ネットワーク接続の問題またはハイバネーションが原因で再接続が必要な場合に必要 なセッショントークンをセットアップするために、ネゴシエーション中に作成されるメイン セッションです。接続メカニズムに基づいて、Cisco適応型セキュリティアプライアンス(ASA) は、セッションをクライアントレス(ポータル経由のWeblaunch)または親(スタンドアロン AnyConnect)として一覧表示します。

AnyConnect 親は、クライアントがアクティブに接続されていない場合のセッションを表しま す。事実上、これは特定のクライアントからの接続にマッピングされる ASA のデータベース エントリであるという点で、Cookie と同様に機能します。クライアントがスリープ/ハイバネー ション状態になると、トンネル(IPsec/インターネット キー エクスチェンジ(IKE)/Transport Layer Security(TLS)/Datagram Transport Layer Security(DTLS)プロトコル)が切断されます が、親は、アイドルタイマーまたは最大接続時間が有効になるまで機能し続けます。これによ り、ユーザーは再認証しないで再接続できます。

例

Inactivityフィールドに、AnyConnectクライアントセッションが接続を失ってからの経 過時間が表示されています。セッションがアクティブな状態の場合、このフィールド には 00:00m:00s が表示されます。

hostname# show vpn-sessiondb

Session Type: SSL VPN Client Username : lee : 1 TP Addr : 209.165.200.232 Index : SSL VPN Client Encryption : 3DES Protocol : userPassword Hashing : SHA1 Auth Mode TCP Dst Port : 443 TCP Src Port : 54230 : 20178 Bytes Tx Bytes Rx : 8662 Pkts Tx : 27 Pkts Rx : 19 Client Ver : Cisco STC 1.1.0.117 Client Type : Internet Explorer : DfltGrpPolicy Group Login Time : 14:32:03 UTC Wed Mar 20 2007 Duration : 0h:00m:04s : 0h:00m:04s Inactivitv Filter Name : hostname# vpn-sessiondb logoff INFO: Number of sessions of type "" logged off : 1

hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1

AnyConnect VPN セッションのログオフ

すべての VPN 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 コマンドを使用します。

次に、すべての VPN セッションをログオフする例を示します。

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

name 引数または index 引数のいずれかを使用して、個々のセッションをログオフできます。

vpn-sessiondb logoff name name vpn-sessiondb logoff index index

ライセンス容量に達して新しいユーザーがログインできなくることがないように、非アクティ ブの状態が最長時間続いたセッションはアイドル状態になります(自動的にログオフされま す)。後でセッションが再開されると、非アクティブリストから削除されます。

ユーザー名とインデックス番号(クライアントイメージの順序で設定される)は、両方とも show vpn-sessiondb anyconnect コマンドの出力で確認できます。次の例は、ユーザー名 *lee* と インデックス番号 *l* を示しています。

hostname# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username	:	lee	Index		: 1
Assigned IP	:	192.168.246.1	Public IP		: 10.139.1.2
Protocol	:	AnyConnect-Parent S	SL-Tunnel DTLS-	Tur	nnel
License	:	AnyConnect Premium			
Encryption	:	RC4 AES128	Hashing		SHA1
Bytes Tx	:	11079	Bytes Rx		4942
Group Policy	:	EngPolicy	Tunnel Group	: I	EngGroup
Login Time	:	15:25:13 EST Fri Ja	n 28 2011		
Duration	:	0h:00m:15s			
Inactivity	:	0h:00m:00s			
NAC Result	:	Unknown			
VLAN Mapping	:	N/A	VLAN		none

次の例は、**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て います。

hostname# vpn-sessiondb logoff name lee Do you want to logoff the VPN session(s)? [confirm] INFO: Number of sessions with name "lee" logged off : 1

hostname#

AnyConnect クライアント 接続機能の履歴

次の表に、この機能のリリース履歴を示します。

表 2: AnyConnect クライアント 接続機能の履歴

機能名	リリース	機能情報
AnyConnect クライアント接続	7.2(1)	authentication eap-proxy、authentication ms-chap-v1、authent ms-chap-v2、authentication pap、l2tp tunnel hello、および vp l2tp-ipsec コマンドが導入または変更されました。
IPsec IKEv2	8.4(1)	AnyConnect クライアントおよびLAN-to-LANのIPsec IKEv トする IKEv2 が追加されました。

I

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては 、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている 場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容につい ては米国サイトのドキュメントを参照ください。