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。

セキュアクライアント VPN Client について

セキュアクライアント 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。

セキュアクライアント 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。

セキュアクライアント の要件

セキュア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 セキュアクライアント

- 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 セキュアクライアント、Cisco VPN フォン用 セキュアクライアント、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 セキュアクライアント 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 セキュアクライアント 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。

セキュアクライアント 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 セキュアクライアント 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 セキュアクライアント 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。

セキュアクライアント 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、セキュアクライアント 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 セキュアクライアント 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 コマンドでセキュア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。セキュアクライアント 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セキュア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 セキュアクライアント 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、セキュアクライアント 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セキュア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セキュアクライアント 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 セキュアクライアント 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セキュアクライアント 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 セキュアクライアント 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 セキュアクライアント 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。

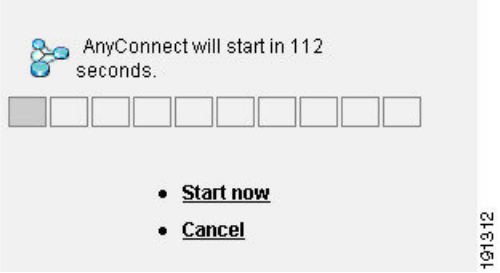
[**no**] **anyconnect ask** {**none** | **enable** [**default** {**webvpn** | } **timeout** *value*]}

- **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 timeout**value 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 timeout**value 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。

図 *1*: リモート ユーザーに表示される *SSL VPN* クライアントのダウンロードを求めるプロンプト



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
```

セキュアクライアント プロファイルダウンロードのイネーブル化

セキュアクライアント 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 セキュアクライアント 機能をイネーブルにします。ASA は セキュアクライアント 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、セキュアクライアント 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 用セキュアクライアント 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、セキュアクライアント 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。

セキュアクライアント 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） セキュアクライアント 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。

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

```
asa1(config-group-webvpn)# anyconnect profiles value sales type vpn
asa1(config-group-webvpn)#
```

セキュアクライアント 遅延アップグレードのイネーブル化

セキュアクライアント 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、セキュアクライアントは、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。セキュアクライアント 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	注記
DeferredUpdateAllowed	true false	false	true は遅延アップデートを有効にします。遅延アップデートが無効（false）の場合、次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	注記
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 セキュアクライアント 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。有効になっているモジュール（VPN を含む）がインストールされていないか、最小バージョンを満たしていない場合、接続は遅延アップデートの対象になりません。 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、遅延プロンプトが表示されます（または自動消去されます）。
DeferredUpdateDismissTimeout	0 ～ 300（秒）	none（ディセーブル）	遅延アップデート プロンプトが表示され、自動的に消去されるまでの秒数。この属性は、遅延アップデート プロンプトが表示される場合に限り適用されます（最小バージョン属性が最初に評価されます）。 この属性がない場合、自動消去機能が無効になり、ユーザが応答するまでダイアログが表示されます（必要な場合）。 この属性を 0 に設定すると、次に基づいて強制的に自動遅延またはアップグレードが実施されます。 • インストールされているバージョンおよび DeferredUpdateMinimumVersion の値。 • DeferredUpdateDismissResponse の値。
DeferredUpdateDismissResponse	defer update	update	DeferredUpdateDismissTimeout が発生した場合に実行するアクション。

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-custom***attr-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、セキュアクライアント 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 セキュアクライアント 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 セキュアクライアント 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 セキュア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、セキュアクライアント 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。例：

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

セキュアクライアント 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、セキュアクライアント 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、セキュアクライアント 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。セキュアクライアント ドメインの変換テーブルに対する変更は、ただちに セキュアクライアント 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、セキュアクライアント 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、セキュア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、セキュアクライアント 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セキュアクライアント 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。

```
hostname# import webvpn translation-table AnyConnect
language es-us tftp://209.165.200.225/client
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder

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、セキュア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 anyconnect language fr
ciscoasa#
```

高度な セキュアクライアント SSL 機能の設定

次の項では、セキュアクライアント 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 とセキュアクライアントが 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。
- **time***minutes* 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、セキュア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 セキュアクライアント 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 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 セキュアクライアント 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

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、セキュア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
```

セキュアクライアント 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 **anyconnect 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**]**anyconnect image** 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、**anyconnect image** 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）
セキュアクライアントに 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
```

SAML 2.0

ASA は SAML 2.0 をサポートしているので、VPN のエンドユーザーは、クレデンシャルを 1 回入力するだけで、プライベートネットワーク外の他の SAAS アプリケーションを切り替えることができるようになります。

たとえば、企業の顧客の場合は、SAML アイデンティティ プロバイダー(IdP）として PingIdentity をイネーブルにして、SAML 2.0 SSO 対応の Rally、Salesforce、Oracle OEM、Microsoft ADFS、onelogin、または Dropbox のアカウントを持ちます。サービスプロバイダー（SP）として 2.0 SAML SSO をサポートするように ASA を設定すると、エンドユーザーは、一度サインインするだけであらゆるサービスにアクセスできるようになります。

AnyConnect 4.4 クライアントが SAML 2.0 を使用して SAAS ベースのアプリケーションにアクセスできるように、AnyConnect SAML サポートが追加されました。AnyConnect 4.6 では、以前のリリースのネイティブ（外部）ブラウザ統合が、組み込みブラウザとの SAML 統合の拡張バージョンに置き換えられました。組み込みブラウザを搭載した新しい拡張バージョンを使用

するには、AnyConnect 4.6（またはそれ以降）および ASA 9.7.1.24（またはそれ以降）、9.8.2.28（またはそれ以降）、または 9.9.2.1（またはそれ以降）へのアップグレードが必要です。

ASA リリース 9.17.1/ASDM リリース 7.17.1 では、AnyConnect 4.10.04065（またはそれ以降）を使用した AnyConnect VPN SAML 外部ブラウザのサポートが導入されました。AnyConnect VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、Web 認証の実行時にセキュアクライアントがセキュアクライアント組み込みブラウザではなくローカルブラウザを使用する設定を選択できます。この機能により、セキュアクライアントは WebAuthN および他の SAML ベースの Web 認証オプション（シングルサインオン、生体認証、または組み込みブラウザでは利用できないその他の拡張方法など）をサポートします。SAML 外部ブラウザを使用するには、「SAML 認証用のデフォルト OS ブラウザの設定 （32 ページ）」で説明する設定を実行する必要があります。

トンネル グループやデフォルト トンネル グループなどの認証方式として SAML が設定されている場合、ASA は SP に対応します。VPN のユーザーは、イネーブルになっている ASA または SAML IdP にアクセスして、シングルサインオンを開始します。以下では、これらの各シナリオについて説明します。

SAML SP によって開始される SSO

ユーザーが ASA にアクセスしてログインを開始した場合、サインオン動作は次のように進行します。

1. VPN のユーザーが SAML 対応のトンネルグループにアクセスするか、またはグループを選択すると、そのユーザーは認証のために SAML IdP にリダイレクトされます。グループ URL に直接アクセスしない限り、ユーザーは入力を要求されます。直接アクセスした場合、リダイレクトは行われません。

   ASA は、ブラウザによって SAML IdP にリダイレクトされる SAML 認証要求を生成します。

2. IdP がエンドユーザーのクレデンシャルを確認し、エンドユーザーがログインします。入力されたクレデンシャルは IdP の認証設定に合致していなければなりません。

3. IdP の応答がブラウザに返信され、ASA のサインイン URL に送信されます。ASA は応答を確認し、ログインを完了させます。

SAML IdP によって開始される SSL

エンドユーザーが IdP にアクセスしてログインを開始した場合、サインオン動作は次のように進行します。

1. エンドユーザーが IdP にアクセスします。IdP は、独自の認証設定に従ってエンドユーザーのクレデンシャルを確認します。エンドユーザーはクレデンシャルを入力し、IdP にログインします。

2. 一般的には、エンドユーザーは、IdP で設定された SAML 対応サービスのリストを取得します。エンドユーザーが ASA を選択します。

3. SAML の応答がブラウザに返信され、ASA のサインイン URL に送信されます。ASA は応答を確認し、ログインを完了させます。

信頼の輪

ASA と SAML アイデンティティ プロバイダーとの信頼関係は、設定されている証明書（ASA トラストポイント）によって確立されます。

エンドユーザーと SAML アイデンティティ プロバイダーとの信頼関係は、IdP に設定されている認証によって確立されます。

SAML のタイムアウト

SAML アサーションには、次のような NotBefore と NotOnOrAfter があります：<saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

ASA で設定されている SAML のタイムアウトと NotBefore の合計が NotOnOrAfter よりも早い場合は、そのタイムアウトが NotOnOrAfter よりも優先されます。NotBefore + タイムアウトが NotOnOrAfter よりも遅い場合は、NotOnOrAfter が有効になります。

タイムアウト後にアサーションによって再利用されないように、タイムアウトにはごく短い時間を設定してください。SAML 機能を使用するためには、ASA の Network Time Protocol（NTP）サーバーを IdP NTP サーバーと同期する必要があります。

プライベート ネットワークでのサポート

SAML 2.0 ベースのサービス プロバイダー IdP は、プライベート ネットワークでサポートされます。SAML IdP がプライベート クラウドに展開されると、ASA およびその他の SAML 対応サービスはピアの位置になり、すべてプライベート ネットワーク内になります。ASA をユーザーとサービス間のゲートウェイとして、IdP の認証は制限された匿名の webvpn セッションで処理され、IdP とユーザー間のすべてのトラフィックは変換されます。ユーザーがログインすると、ASA は対応する属性のセッションを修正し、IdP セッションを保存します。その後は、クレデンシャルを再度入力することなくプライベート ネットワークのサービス プロバイダーを使用できます。

SAML IdP *NameID* 属性は、ユーザーのユーザー名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。

（注） プライベート ネットワークとパブリック ネットワーク間で認証情報を交換することはできません。内部および外部の両方のサービス プロバイダーに同じ IdP を使用する場合、個別に認証する必要があります。内部専用の IdP を外部サービスで使用することはできません。外部専用の IdP は、プライベート ネットワーク内のサービス プロバイダーでは使用できません。

SAML 2.0 に関する注意事項と制約事項

- ASA は、SAML 認証用に次のシグニチャをサポートしています。

  - RSA および HMAC を使用する SHA1
  - RSA および HMAC を使用する SHA2

- ASA は、すべての SAML IdP でサポートされる SAML 2.0 Redirect-POST バインディングをサポートしています。
- ASA は SAML SP としてのみ機能します。ゲートウェイ モードやピア モードでアイデンティティ プロバイダーとして動作することはできません。
- この SP SAML SSO 機能は相互排他認証方式です。この方式は、AAA や証明書と併用できません。
- ユーザー名/パスワード認証、証明書認証、および KCD に基づく機能はサポートされません。たとえば、ユーザー名/パスワードの事前フィルタリング機能、フォーム ベースの自動サインオン、マクロ置換ベースの自動サインオン、KCD SSO などです。
- ASA は、AnyConnect SAML 認証を使用した VPN ロードバランシングをサポートするようになりました。
- SAML 認証に Safari を使用している場合は、Safari アップデート 14.1.2 以降がインストールされていることを確認してください。
- 認証アサーションが適切に処理され、タイムアウトが適切に機能するように、ASA の管理者は、ASA と SAML IdP とのクロック同期を確保する必要があります。
- ASA の管理者は、次の点を考慮して、ASA と IdP の両方で有効な署名証明書を保持する責任があります。
  - ASA に IdP を設定する際には、IdP の署名証明書が必須です。
  - ASA は、IdP から受け取った署名証明書に対して失効チェックを行いません。
- SAML アサーションには、NotBefore と NotOnOrAfter 条件があります。ASA SAML に設定されている**タイムアウト**と、これらの条件との相関関係は次のとおりです。
  - NotBefore とタイムアウトの合計が NotOnOrAfter よりも早い場合は、タイムアウトが NotOnOrAfter に優先します。
  - NotBefore + タイムアウトが NotOnOrAfter よりも遅い場合は、NotOnOrAfter が有効になります。
  - NotBefore 属性が存在しない場合、ASA はログイン要求を拒否します。NotOnOrAfter 属性が存在せず、SAML タイムアウトが設定されていない場合、ASA はログイン要求を拒否します。
- 二要素認証（プッシュ、コード、パスワード）のチャレンジ/応答中に FQDN が変更されるため、ASA がクライアントとのプロキシを強制的に認証する、内部 SAML を使用した展開では ASA は Duo と連携しません。
- 信頼できないサーバー証明書は、組み込みブラウザでは許可されません。

- 組み込みブラウザSAML統合は、CLIモードまたはSBLモードではサポートされません。
- Web ブラウザに確立された SAML 認証は AnyConnect と共有されず、その逆も同じです。
- 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、AnyConnect では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのにAnyConnectがどのプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。
- SAML 機能を使用するためには、ASA の Network Time Protocol（NTP）サーバを IdP NTP サーバと同期する必要があります。
- ASDM の VPN ウィザードは現在、SAML 設定をサポートしていません。
- 内部IdPを使用してログインした後にSSOで内部サーバーにアクセスすることはできません。
- SAML IdP NameID 属性は、ユーザーのユーザー名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。
- マルチコンテキストモードで SAML はサポートされません。
- SAML アサーションで受信した複数の属性はサポートされていません。
- Chromebookは、外部ブラウザ認証を備えたSecure Client SAMLをサポートしていません。
- IdP が、SAML 応答に、 対応する SAML 要求で受信したのと同じ Relay state パラメータを含めていることを確認します。

SAML 2.0 アイデンティティ プロバイダー（IdP）の設定

始める前に

SAML（IdP）プロバイダーのサインイン URL とサインアウト URL を取得します。URL はプロバイダーの Web サイトから取得できます。また、プロバイダーがメタデータ ファイルで情報を提供していることもあります。

手順

ステップ 1 webvpn コンフィギュレーション モードで SAML アイデンティティ プロバイダーを作成し、webvpn で saml-idp サブモードを開始します。

[**no**] **saml idp** *idp-entityID*

idp-entityID：SAML IdP の entityID には 4 ～ 128 文字を指定します。

SAML IdP を削除するには、このコマンドの **no** 形式を使用します。

ステップ 2　IdP URL を設定します。

url [**sign-in** | **sign-out**] *value*

value：IdP にサインインするための URL、または IdP からサインアウトするときにリダイレクトされる URL です。**sign-in** URL は必須ですが、**sign-out** URL はオプションです。url の値には 4 ～ 500 文字を指定します。

ステップ 3　（任意）クライアントレス VPN のベース URL を設定します。

base-url *URL*

この URL は、エンドユーザーを ASA にリダイレクトするために、サードパーティ製 IdP に提供されます。

base-url が設定されている場合、その URL は **show saml metadata** の AssertionConsumerService と SingleLogoutService 属性のベース URL として使用されます。

base-url が設定されていない場合、URL は ASA のホスト名とドメイン名から決定されます。たとえば、ホスト名が `ssl-vpn`、ドメイン名が `cisco.com` の場合は、`https://ssl-vpn.cisco.com` が使用されます。

base-url もホスト名/ドメイン名も設定されていない場合は、**show saml metadata** を入力するとエラーが発生します。

ステップ 4　IdP と SP（ASA）間のトラストポイントを設定します。

trustpoint idp *trustpoint-name1* [*trustpoint-name2*]

trustpoint sp *trustpoint-name1*

idp：ASA が SAML アサーションを検証するための IdP 証明書を含むトラストポイントを指定します。

デバイスの SAML IdP に 2 つのトラストポイントを構成できるようになりました。この機能を使用すると、サービスを失わずに、新しいアイデンティティ プロバイダー（IdP）証明書に問題なく移行できます。同じ証明書ですべての ASA と IdP を同時に更新するためにメンテナンスウィンドウを開く必要はありません。新しい IdP 証明書が IdP で有効になると、デバイスは新しい証明書を自動的に検出します。元のトラストポイントは、移行後に安全に削除できます。

sp ：IdP が ASA（SP）の署名や暗号化 SAML アサーションを検証するための ASA（SP）証明書を含むトラストポイントを指定します。

trustpoint-name：設定されているトラストポイントを指定します。

ステップ 5　（任意）ローカルベース URL を設定します。

local base-url *URL*

DNS ロードバランシングクラスタでは、SAML 認証を ASA で設定するときに、設定が適用されるデバイスに一意に解決されるベース URL を指定できます。

ステップ 6　（任意）SAML タイムアウトを設定します。

timeout assertion *timeout-in-seconds*

指定した場合、NotBefore と timeout-in-seconds の合計が NotOnOrAfter よりも早い場合は、この設定が NotOnOrAfter に優先します。

指定しない場合は、セッションの NotBefore と NotOnOrAfter が有効期間の確認に使用されます。

（注）
既存の SAML IdP が設定済みのトンネル グループの場合、webvpn での saml idp CLI に対するすべての変更は、SAML がその特定のトンネル グループに再度有効にされたときにのみトンネル グループに適用されます。タイムアウトを設定すると、更新されたタイムアウトはトンネル グループの webvpn 属性の saml アイデンティティ プロバイダー CLI 再発行後にのみ有効になります。

ステップ 7 （任意） SAML 要求の署名をイネーブルまたはディセーブル（デフォルト設定）にします。

signature <value>

（注）
SSO 2.5.1 へのアップグレードに伴い、デフォルトの署名方法は SHA1 から SHA256 に変更します。*value* に rsa-sha1、rsa-sha256、rsa-sha384、または rsa-sha512 を入力すると、希望する署名方法のオプションを設定できます。

ステップ 8 （オプション）IdP が内部ネットワークであることを特定するフラグを設定するには、**internal** コマンドを使用します。ASA はゲートウェイ モードで機能するようになります。

ステップ 9 **show webvpn saml idp** を使用してコンフィギュレーションを表示します。

ステップ 10 SAML 認証要求が発生したときに、以前のセキュリティ コンテキストに依存するのではなくアイデンティティ プロバイダーが直接認証するようにするには、**force re-authentication** を使用します。この設定はデフォルトなので、ディセーブルにする場合は **no force re-authentication** を使用します。

例

次の例では、salesforce_idp という名前の IdP を設定し、事前設定されたトラストポイントを使用します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#saml idp salesforce_idp

ciscoasa(config-webvpn-saml-idp)#url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)#url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect

ciscoasa(config-webvpn-saml-idp)#trustpoint idp salesforce_trustpoint
salesforce_trustpoint2
ciscoasa(config-webvpn-saml-idp)#trustpoint sp asa_trustpoint

ciscoasa(config)#show webvpn saml idp
saml idp salesforce_idp
url sign-in https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
url sign-out https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
```

```
trustpoint idp salesforce_trustpoint salesforce_trustpoint2
trustpoint  sp asa_trustpoint
```

次の Web ページには、Onelogin の URL の取得方法について例が示されています。

https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen

次の Web ページには、メタデータを使用して Onelogin から URL を検索する方法について、例が示されています。

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

次のタスク

SAML 2.0 サービス プロバイダー（SP）としての ASA の設定 （31 ページ） の説明に従って、SAML 認証を接続プロファイルに適用します。

SAML 2.0 サービス プロバイダー（SP）としての ASA の設定

始める前に

事前に IdP を設定しておく必要があります。SAML 2.0 アイデンティティ プロバイダー（IdP）の設定 （28 ページ）を参照してください。

手順

ステップ 1 tunnel-group webvpn サブモードで、saml identify-provider コマンドを使用して IdP を割り当てます。

saml identity-provider *idp-entityID*

idp-entityID：設定されている既存の IdP のいずれかを指定します。

SAML SP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 2 SAML 認証を有効化します。

authentication saml

ステップ 3 （オプション）トンネル グループの SAML IdP トラストポイントを構成します。

saml idp-trustpoint *trustpoint-name* [*trustpoint-name2*]

Azure IdP など、IdP で複数のアプリケーションがある場合も同じ SAML エンティティ ID を共有しますが、アプリケーションごとに独自の証明書を使用します。上記のコマンドを特定のアプリケーションに関連付けて使用して、メインの webvpn saml 構成を上書きできます。

例

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

トンネル グループの IdP トラストポイントを構成します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group partner-saml type remote-access
ciscoasa(config)# tunnel-group partner-saml webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://sts.windows.net/123-3456-7890/
ciscoasa(config-tunnel-webvpn)# saml idp-trustpoint azure-partner-idp-tp
```

SAML 認証用のデフォルト OS ブラウザの設定

AnyConnectが、プラットフォームのネイティブブラウザ（オペレーティングシステムのデフォルトブラウザ）またはAnyConnectに組み込まれているブラウザを使用してSSO認証プロセスを処理するかどうかを指定します。

AnyConnect外部ブラウザパッケージ（*external-sso-4.10.04065-webdeploy-k9.pkg* など）をダウンロードして、ASAにアップロードする必要があります。次に、SAML認証用のSAMLログイン方法（AnyConnectの組み込みブラウザまたはオペレーティングシステムのデフォルトブラウザ）を選択できます。このバンドルは、認証目的でVPNクライアントがデフォルトのOS Webブラウザを起動できるようにするスクリプトです。このバンドルは、オペレーティングシステム、ブラウザ、およびVPNクライアントのバージョンに依存してはいません。この機能が有効になっていれば、VPNクライアントのバージョンと外部ブラウザのパッケージのバージョン ファイルが一致している必要はありません。

オペレーティングシステムのデフォルトブラウザを選択すると、VPN認証と他の企業ログインの間のシングルサインオン（SSO）が有効になります。VPNクライアントの組み込みブラウザでは実行できないWeb認証方式（生体認証など）をサポートしたい場合も、このオプションを選択します。オペレーティングシステムのブラウザを選択する前に、ブラウザで実行できるパッケージをアップロードしてWeb認証を有効にする必要があります。

手順

ステップ 1 オペレーティングシステムのデフォルトブラウザを使用してAnyConnect SAML認証を有効にするには、webvpnサブモードでanyconnect external-browser-pkgコマンドを使用します。

anyconnect external-browser-pkg *path*

SAML 認証用のオペレーティングシステムのデフォルトブラウザを無効にするには、このコマンドの **no** 形式を使用します。

ステップ 2 オペレーティングシステムのデフォルトブラウザを使用して AnyConnect SAML 認証を有効にするには、tunnel-group webvpn サブモードで external-browser コマンドを使用します。

external-browser enable *idp-entityID*

SAML 認証用のオペレーティングシステムのデフォルトブラウザを無効にするには、このコマンドの **no** 形式を使用します。

例

この例では、AnyConnect 外部ブラウザパッケージのパスを選択し、SAML 認証用に外部ブラウザ（オペレーティングシステムのデフォルトブラウザ）を有効にします。

```
asa(config-webvpn)# anyconnect external-browser-pkg flashshow :
asa(config)# tunnel-group SAML webvpn-attributes
asa(config-tunnel-webvpn)# external-browser enable
asa(config-tunnel-webvpn)#
```

証明書と SAML 認証の設定

SAML ベースの接続プロファイル用の証明書と SAML 認証を設定して、特定のファイル/レジストリキーのプロファイルを作成せずに、お客様が所有するアセットを検証できます。SAML ベースの認証は、承認済みのアセットおよび/またはユーザーに関連付けることができます。認証には、SAML による単一の証明書または複数の証明書を使用できます。

セキュアクライアントが接続を開始すると、ASA または FTD は、SAML 認証が実行される前に、エンドポイントからの 1 つ以上の証明書を要求して認証します。

SAML 認証が完了すると、SAML と証明書のユーザー名に対して以下を実行できます。

SAML 認証が完了すると、承認フェーズに進む前に SAML と証明書のユーザー名を比較できます。

始める前に

証明書と SAML 認証を設定する前に、必要な SAML 設定を構成してください。

- SAML（IdP）プロバイダーのサインイン URL とサインアウト URL を取得します。URL はプロバイダーの Web サイトから取得できます。また、プロバイダーがメタデータ ファイルで情報を提供していることもあります。
- SAML ID プロバイダーとトラストポイントの設定を構成します。証明書と SAML 認証の設定 （33 ページ）を参照してください

手順

ステップ 1 証明書と SAML 認証を設定するには、次のコマンドを入力して tunnel-group webvpn-attributes モードを開始します。プロンプトが変化して、モードが変更されたことがわかります。

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

ステップ 2 使用する認証方法を指定するには、次のコマンドを入力します。

```
hostname(config-tunnel-webvpn)#authentication authentication_method
```

たとえば、次のコマンドは SAML と証明書認証の両方を許可します。

```
hostname(config-tunnel-webvpn)#authentication saml certificate
```

次のコマンドは、証明書と SAML 認証を許可します。

```
hostname(config-tunnel-webvpn)#authentication certificate saml
```

次のコマンドは、複数の証明書と SAML 認証の両方を許可します。

```
hostname(config-tunnel-webvpn)#authentication multiple-certificate saml
```

ステップ 3 接続プロファイルを追加または編集してから、[基本（Basic）]接続プロファイル属性設定を選択します。

ステップ 4 証明書と SAML 認証の認証方法を指定するには、ドロップダウンから SAML と証明書、または複数の証明書と SAML を選択します。

例

次の例では、sales_group 接続プロファイルに複数の証明書と SAML 認証を設定しています。

```
ciscoasa(config)# tunnel-group sales_group webvpn
ciscoasa(config-tunnel-webvpn)#authentication multiple-certificate saml
```

SAML 2.0 と Onelogin の例

以下の例を実行する際は、Onelogin の情報とネーミングの代わりにサードパーティ製の SAML 2.0 IdP を使用してください。

1. IdP と ASA（SP）間での時刻の同期を設定します。

```
ciscoasa(config)# ntp server 209.244.0.4
```

2. サードパーティ製 IdP で指定されている手順に従って、IdP から IdP の SAML メタデータを取得します。

3. トラストポイントに IdP の署名証明書をインポートします。

```
ciscoasa(config)# crypto ca trustpoint onelogin
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# no ca-check
ciscoasa(config-ca-trustpoint)# crypto ca authenticate onelogin
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
quit
INFO: Certificate has the following attributes:
Fingerprint:     85de3781 07388f5b d92d9d14 1e22a549
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

4. トラストポイントに SP（ASA）署名 PKCS12 をインポートします

```
ciscoasa(config)# crypto ca import asa_saml_sp pkcs12 password
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
quit
INFO: Import PKCS12 operation completed successfully
```

5. SAML IdP を追加します。

```
ciscoasa(config-webvpn)# saml idp https://app.onelogin.com/saml/metadata/462950
```

6. saml-idp サブモードで属性を設定します。

   IdP サインイン URL とサインアウト URL を設定します。

```
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://ross.onelogin.com/trust/saml2/http-post/sso/462950
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://ross.onelogin.com/trust/saml2/http-redirect/slo/462950
```

   IdP トラストポイントと SP トラストポイントを設定します

```
ciscoasa(config-webvpn-saml-idp)# trustpoint idp onelogin
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_saml_sp
```

   クライアントレス VPN ベース URL、SAML 要求の署名、および SAML アサーション タイムアウトを設定します。

```
ciscoasa(config-webvpn-saml-idp)# base-url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

7. トンネル グループの IdP を設定し、SAML 認証をイネーブルにします。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

8. ASA の SAML SP メタデータを表示します。

ASA の SAML SP メタデータは、`https://172.23.34.222/saml/sp/metadata/cloud_idp_onelogin` から取得できます。この URL の `cloud_idp_onelogin` は、トンネル グループ名です。

9. サードパーティ製 IdP で指定されている手順に従って、その IdP で SAML SP を設定します。

SAML 2.0 のトラブルシューティング

SAML 2.0 の動作をデバッグするには、**debug webvpn saml***value* を使用します。*value* に応じて次の SAML メッセージが表示されます。

- 8：エラー
- 16：警告およびエラー
- 128 または 255：デバッグ、警告、およびエラー

セキュアクライアント 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セッション情ます。
show vpn-sessiondb ratio encryption	Suite-B のアルゴリズム（AES-GCM-128、AES-GCM-192AES-GCM-256、AES-GMAC-128 など）用のトンネル数お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、セキュアクライアント 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
Index        : 1                        IP Addr      : 209.165.200.232
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  : Internet Explorer
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Mar 20 2007
Duration     : 0h:00m:04s
Inactivity    : 0h:00m:04s
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 *1* 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 SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 11079                  Bytes Rx     : 4942
Group Policy : EngPolicy            Tunnel Group : EngGroup
Login Time   : 15:25:13 EST Fri Jan 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#
```

セキュアクライアント 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:* セキュアクライアント 接続機能の履歴

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

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。