クライアントレス SSL VPN ユーザ

パスワードの管理

必要に応じて、パスワードの期限切れが近づいたときにエンド ユーザに警告するように ASA を設定できます。

ASA は、RADIUS および LDAP プロトコルのパスワード管理をサポートしています。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。

IPsec リモート アクセスと SSL VPN トンネルグループのパスワード管理を設定できます。

パスワード管理を設定すると、ASA はリモート ユーザのログイン時に、現在のパスワードの期限切れが近づいていること、または期限が切れていることを通知します。それから ASA は、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

このコマンドは、この通知をサポートしている AAA サーバに対して有効です。

ASA のリリース 7.1 以降では、通常、LDAP による認証時または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント
- IPsec VPN クライアント
- クライアントレス SSL VPN

RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、ASA からは RADIUS サーバとのみ通信しているように見えます。

始める前に

- ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。
- 認証に LDAP ディレクトリ サーバを使用している場合、パスワード管理は Sun JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。
  - Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN が、サーバのデフォルトパスワードポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
  - Microsoft：Microsoft Active Directory でパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。
- MSCHAP をサポートする一部の RADIUS サーバは、現在 MSCHAPv2 をサポートしていません。このコマンドには MSCHAPv2 が必要なため、ベンダーに問い合わせてください。
- Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポートされません。
- LDAP でパスワードを変更するには、市販の LDAP サーバごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバに対してのみ、独自のパスワード管理ロジックを実装しています。
- RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] > [Add or Edit] > [Advanced] > [General] > [Password Management] に移動します。

ステップ 2 [Enable password management] オプションをクリックします。

クライアントレス SSL VPN でのシングル サインオンの使用

SAML 2.0 による SSO

SSO および SAML 2.0 について

ASA は SAML 2.0 をサポートしています。これにより、クライアントレス VPN のエンドユーザは、クレデンシャルを 1 回だけ入力して、クライアントレス VPN とプライベート ネットワーク外部のその他の SAAS アプリケーションと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、エンドユーザは一度サインインするだけで、クライアントレス VPN などのあらゆるサービスにアクセスできるようになります。

さらに、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、組み込みブラウザとの SAML 統合が拡張され、これが以前のリリースからのネイティブ（外部）ブラウザ統合に置き換わります。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。

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。クライアントレス VPN のエンドユーザは、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

エンドユーザがクライアントレス VPN を使用して ASA アクセスし、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. クライアントレス VPN のエンドユーザが 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 がエンドユーザのクレデンシャルを確認し、エンドユーザがログインします。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のクレデンシャルを確認します。エンドユーザ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）サーバを IdP NTP サーバ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 とユーザ間のすべてのトラフィックは変換されます。ユーザがログインすると、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、ユーザのユーザ名を特定し、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。
- SAML 2.0 SSO は、内部 SAML IdP と SP をサポートしておらず、プライベート ネットワーク外部の SAML IdP と SP のみをサポートしています。
- 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。
- DAP 評価で使用可能な SAML 認証属性は（AAA サーバから RADIUS 認証応答で送信される RADIUS 属性と同様に）サポートされていません。ASA は、DAP ポリシーで SAML 対応トンネルグループをサポートします。ただし、ユーザ名属性は SAML ID プロバイダーによってマスクされるため、SAML 認証の使用中はユーザ名属性を確認できません。
- 既存のクライアントレス VPN のタイムアウト設定は、まだ SAML セッションに適用されます。
- 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。
- AnyConnect で SAML を使用する場合は、次の追加ガイドラインに従ってください。
  - 信頼できないサーバ証明書は、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 で内部サーバにアクセスすることはできません。
  - SAML IdP NameID 属性は、ユーザのユーザ名を特定し、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。
  - VPN ロードバランシングまたは DNS ロードバランシングは使用できません。

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 （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 2 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。

ステップ 3 ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Single Sign On Servers] に移動します。

すでに設定されているすべての SAML 2.0 IdP が一覧表示されます。[Add] または [Delete] の次に説明されているように、[Edit] を使用してリストを編集できます。

ステップ 4 [Add] をクリックして、新しい IdP エントリを追加します。

ステップ 5 説明に従って、次のフィールドに入力します。

- [Sign In URL]：IdP にサインインするための URL。url value は 4 ～ 500 文字の範囲で指定します。
- [Sign Out URL]（オプション）：IdP からサインインするときのリダイレクト先 URL。url value は 4 ～ 500 文字の範囲で指定します。
- [Base URL]（オプション）：エンドユーザを 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。
- [Identity Provider Certificate]：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。すでに設定されているトラストポイントを選択します。

- [Service Provider Certificate]（オプション）：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）証明書含むトラストポイントを指定します。すでに設定されているトラストポイントを選択します。
- [Request Signature]：ドロップダウンを使用して、SAML IdP サーバに対して希望する署名方法を選択します。rsa-sha1、rsa-sha256、rsa-sha384、rsa-sha512 から選択できます。
- [Request Timeout]（オプション）：SAML 要求のタイムアウト。

  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。
- [Enable the Signature]：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。
- [Enable the Internal]：IdP が内部ネットワーク内かどうかを決定するには、有効または無効（デフォルト設定）にします。

  （注） 内部 IdP を使用してログインした後に SSO で内部サーバにアクセスすることはできません。
- Enable the Force Re-authentication：SAML 認証要求が発生するときにこの設定を有効にしていると、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なります。再認証の強制有効がデフォルト値です。

ステップ 6 [OK] をクリックします。
新しい IdP エンティティがこのページに一覧表示されます。

例

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 （8 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

特定のトンネル グループを SAML SP として設定するには、次の手順を実行します。

（注） AnyConnect 4.4 または 4.5 で SAML 認証を使用していて、ASA バージョン 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）（リリース日付：2018 年 4 月 18 日）を展開している場合、SAML のデフォルトの動作は、AnyConnect 4.4 および4.5 でサポートされていない組み込みブラウザになります。したがって、[Connection Profiles] 領域で [SAML External Browser] チェックボックスをオンにして、AnyConnect 4.4 および 4.5 クライアントが外部（ネイティブ）ブラウザを使用して、SAML で認証できるようにする必要があります。

[SAML External Browser] チェックボックスは、AnyConnect 4.6 以降にアップグレードするクライアントの移行のために使用されます。セキュリティ上の制限のため、AnyConnect ソフトウェアをアップグレードする際の一時的な移行の一環としてのみこのソリューションを使用してください。今後、このチェックボックス自体がサポートされなくなります。

手順

ステップ 1 ASDM で、[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Connection Profiles] > [Add/Edit] に移動します。

ステップ 2 このトンネル グループの認証方式として（[Authentication] **[Method]**）[Saml] を選択します。

ステップ 3 [SAML Identity Provider] セクションで、すでに設定されている [SAML Server] を選択するか、[Manage] をクリックして新規に作成します。
既存の SAML 設定を変更した場合、この操作によってトンネル グループの IdP が再度有効になります。

ステップ 4 [OK] をクリックします。
[Preview CLI Commands] ウィンドウが表示され、承認した変更に基づいて生成された CLI コマンドが示されます。[Send] をクリックすると ASA にコマンドを送信できます。

自動サインオンの使用

[Auto Sign-on] ウィンドウまたはタブでは、クライアントレス SSL VPN ユーザの自動サインオンを設定または編集できます。自動サインオンは、内部ネットワークに SSO 方式をまだ展開していない場合に使用できる簡素化された単一サインオン方式です。特定の内部サーバに対して自動サインオンを設定すると、ASA は、クライアントレス SSL VPN ユーザが ASA へのログオン時に入力したログインクレデンシャル（ユーザ名とパスワード）をそれら特定の内部サーバに渡します。特定範囲のサーバの特定の認証方式に応答するように、ASA を設定します。応答するように ASA に設定できる認証方式は、Basic（HTTP）方式、NTLM 方式、FTP および CIFS 方式を使用する認証、またはこれらの方式すべてを使用する認証から構成されます。

ユーザ名とパスワードのルックアップが ASA で失敗した場合は、空の文字列で置き換えられ、動作は自動サインオンが不可の場合の状態に戻されます。

自動サインオンは、特定の内部サーバに SSO を設定する直接的な方法です。この項では、自動サインオンを行うように SSO をセットアップする手順について説明します。

次のフィールドが表示されます。

- [IP Address]：次の [Mask] と組み合わせて、認証されるサーバの IP アドレスの範囲を [Add/Edit Auto Sign-on] ダイアログボックスで設定されたとおりに表示します。サーバは、サーバの URI またはサーバの IP アドレスとマスクで指定できます。
- [Mask]：前の [IP Address] と組み合わせて、[Add/Edit Auto Sign-on] ダイアログボックスで自動サインオンをサポートするように設定されたサーバの IP アドレスの範囲を表示します。
- [URI]：[Add/Edit Auto Sign-on] ダイアログボックスで設定されたサーバを識別する URI マスクを表示します。
- [Authentication Type]：[Add/Edit Auto Sign-on] ダイアログボックスで設定された認証のタイプ（Basic（HTTP）、NTLM、FTP と CIFS、またはこれらの方式すべて）を表示します。

始める前に

- 認証が不要なサーバ、または ASA とは異なるクレデンシャルを使用するサーバでは、自動サインオンをイネーブルにしないでください。自動サインオンがイネーブルの場合、ASA は、ユーザ ストレージにあるクレデンシャルに関係なく、ユーザが ASA へのログオン時に入力したログイン クレデンシャルを渡します。
- 一定範囲のサーバに対して 1 つの方式（HTTP Basic など）が設定されているときに、その中の 1 台のサーバが異なる方式（NTLM など）で認証を試みた場合、ASA はユーザのログイン クレデンシャルをそのサーバに渡しません。

手順

ステップ 1 クリックして自動サインオン命令を追加または編集します。自動サインオン命令は、自動サインオン機能を使用する内部サーバの範囲と、特定の認証方式を定義します。

ステップ 2 [Auto Sign-on] テーブルで選択した自動サインオン命令を削除する場合にクリックします。

ステップ 3 [IP Block] をクリックして、IP アドレスとマスクを使用して内部サーバの範囲を指定します。

- [IP Address]：自動サインオンを設定する範囲の最初のサーバの IP アドレスを入力します。
- [Mask]：[subnet mask] メニューで、自動サインオンをサポートするサーバのサーバ アドレス範囲を定義するサブネット マスクを選択します。

ステップ 4 [URI] をクリックして、URI によって自動サインオンをサポートするサーバを指定し、このボタンの横にあるフィールドに URI を入力します。

ステップ 5 サーバに割り当てられる認証方式を決定します。指定された範囲のサーバに対して、Basic HTTP 認証要求、NTLM 認証要求、FTP および CIFS 認証要求、またはこれら方式のいずれかを使用している要求に応答するように、ASA を設定できます。

- [Basic]：サーバが Basic（HTTP）認証をサポートする場合は、このボタンをクリックします。
- [NTLM]：サーバが NTLMv1 認証をサポートする場合は、このボタンをクリックします。
- [FTP/CIFS]：サーバが FTP と CIFS の認証をサポートする場合は、このボタンをクリックします。
- [Basic, NTLM, and FTP/CIFS]：サーバが上のすべての方式をサポートする場合は、このボタンをクリックします。

ユーザ名とパスワードの要件

ネットワークによっては、リモートセッション中にユーザが、コンピュータ、インターネットサービス プロバイダー、クライアントレス SSL VPN、メール サーバ、ファイル サーバ、企業アプリケーションの一部またはすべてにログインする必要が生じることがあります。ユーザはさまざまなコンテキストで認証を行うために、固有のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。次の表に、クライアントレス SSL VPN ユーザが理解しておく必要のあるユーザ名とパスワードのタイプを示します。

ログイン ユーザ名/ パスワードのタイプ		入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
Internet Service Provider：インターネット サービス プロバイダー	インターネットへのアクセス	インターネット サービス プロバイダーへの接続
クライアントレス SSL VPN	リモート ネットワークへのアクセス	クライアントレス SSL VPN の起動
File Server	リモート ファイル サーバへのアクセス	クライアントレス SSL VPN ファイル ブラウジング機能を使用して、リモート ファイル サーバにアクセスするとき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	クライアントレス SSL VPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバ	クライアントレス SSL VPN 経由によるリモート メール サーバへのアクセス	電子メール メッセージの送受信

セキュリティ ヒントの通知

ユーザはいつでもツールバーの[Logout]アイコンをクリックして、クライアントレスSSL VPNセッションを閉じることができます（ブラウザ ウィンドウを閉じてもセッションは閉じません）。

クライアントレス SSL VPN は、企業ネットワーク上のリモート PC やワークステーションと ASA との間のデータ転送のセキュリティを保証するものです。クライアントレス SSL VPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザに通知してください。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるリソース）にアクセスする場合、企業の ASA から目的の Web サーバまでの通信は暗号化されていないため、プライベートではありません。

クライアントレスSSLVPNの機能を使用するためのリモート システムの設定

この項では、クライアントレス SSL VPN を使用するようにリモート システムを設定する方法について説明します。

ユーザ アカウントを別々に設定でき、各ユーザは異なるクライアントレス SSL VPN の機能を使用できます。

クライアントレス SSL VPN について

次のようなサポートされている接続を使用して、インターネットに接続できます。

- 家庭の DSL、ケーブル、ダイヤルアップ。

- 公共のキオスク。
- ホテルのホットスポット。
- 空港の無線ノード。
- インターネット カフェ。

（注） クライアントレス SSL VPN がサポートしている Web ブラウザのリストについては、『サポート対象の VPN プラットフォーム、Cisco ASA 5500 シリーズ』を参照してください。

クライアントレス SSL VPN の前提条件

- ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
- クライアントレス SSL VPN の URL が必要です。URL は、https://*address* 形式の https アドレスでなければなりません。*address* は、SSL VPN がイネーブルになっている ASA（またはロード バランシング クラスタ）のインターフェイスの IP アドレスまたは DNS ホスト名です。たとえば、https://cisco.example.com などです。
- クライアントレス SSL VPN のユーザ名とパスワードが必要です。

（注） クライアントレス SSL VPN ではローカル印刷がサポートされていますが、VPN 経由による企業ネットワーク上のプリンタへの印刷はサポートされていません。

クライアントレス SSL VPN フローティング ツールバーの使用

フローティング ツールバーを使用すると、クライアントレス SSL VPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。

フローティング ツールバーは、現在のクライアントレス SSL VPN セッションを表します。[**Close**] ボタンをクリックすると、クライアントレス SSL VPN セッションの終了を求めるメッセージが ASA によって表示されます。

ヒント テキスト フィールドにテキストを貼り付けるには、Ctrl+V を使用します（クライアントレス SSL VPN セッション中は、表示されるツールバー上での右クリックはオフになっています）。

（注） ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。

Web のブラウズ

クライアントレス SSL VPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。セキュリティ ヒントの通知 （12 ページ）を参照してください。

クライアントレス SSL VPN での Web ブラウジングのルックアンドフィールは、ユーザが使い慣れたものと異なる場合があります。次に例を示します。

- クライアントレス SSL VPN のタイトル バーが各 Web ページの上部に表示される。
- Web サイトへのアクセス方法：
  - クライアントレス SSL VPN ホーム ページ上の [Enter Web Address] フィールドに URL を入力する
  - クライアントレス SSL VPN ホーム ページ上にある設定済みの Web サイト リンクをクリックする
  - 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする
  - 保護されている Web サイトのユーザ名とパスワードが必要です。

特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN ホーム ページ上にリンクとして表示されるものに限られる

また、特定のアカウントの設定によっては、次のようになる場合もあります。

- 一部の Web サイトがブロックされている
- 使用可能な Web サイトが、クライアントレス SSL VPN ホーム ページ上にリンクとして表示されるものに限られる

ネットワークのブラウズ（ファイル管理）

ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。

（注） コピー処理の進行中は、**Copy File to Server** コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。

重要なポイントは次のとおりです。

- 共有リモート アクセス用にファイル アクセス権を設定する必要があります。
- 保護されているファイル サーバのサーバ名とパスワードが必要です。
- フォルダとファイルが存在するドメイン、ワークグループ、およびサーバの名前が必要です。

（注） クライアントレス SSL VPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。

Remote File Explorer の使用

ユーザは、Remote File Explorer を使用して、Web ブラウザから企業ネットワークをブラウズできます。ユーザが Cisco SSL VPN ポータル ページの [Remote File System] アイコンをクリックすると、ユーザのシステムでアプレットが起動し、ツリーおよびフォルダ ビューにリモート ファイル システムが表示されます。

（注） この機能を使用するには、ユーザのマシンに Oracle Java ランタイム環境（JRE）がインストールされ、Web ブラウザで Java がイネーブルになっている必要があります。リモート ファイルの起動には、JRE 8u131 b11、7u141 b11、6u151 b10 以降が必要です。

ユーザはブラウザで次を実行できます。

- リモート ファイル システムのブラウズ。
- ファイルの名前の変更。
- リモートファイルシステム内、およびリモートとローカルのファイルシステム間でのファイルの移動またはコピー。
- ファイルのバルク アップロードおよびダウンロードの実行。

  ファイルをダウンロードするには、ブラウザでファイルをクリックして、[Operations] > [Download] を選択し、[Save] ダイアログで場所と名前を指定してファイルを保存します。

  ファイルをアップロードするには、宛先フォルダをクリックして、[Operations] > [Upload] を選択し、[Open] ダイアログでファイルの場所と名前を指定します。

  この機能には次の制限があります。

- ユーザは、アクセスを許可されていないサブフォルダを表示できません。
- ユーザがアクセスを許可されていないファイルは、ブラウザに表示されても移動またはコピーできません。
- ネストされたフォルダの最大の深さは 32 です。
- ツリー ビューでは、ドラッグ アンド ドロップのコピーがサポートされていません。
- Remote File Explorer の複数のインスタンスの間でファイルを移動するときは、すべてのインスタンスが同じサーバを探索する必要があります（ルート共有）。
- Remote File Explorer は、1 つのフォルダに最大 1500 のファイルおよびフォルダを表示できます。フォルダがこの制限を超えた場合、フォルダは表示されません。

ポート転送の使用

ポート フォワーディングを使用するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用してクライアント アプリケーションを設定する必要があります。

- アプリケーションを使用した後、ユーザは [**Close**] アイコンをクリックして必ず [Application Access] ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体がオフに切り替わる可能性があります。

始める前に

- macOS では、この機能をサポートしているのは Safari 11 以前のブラウザだけです。
- クライアント アプリケーションがインストールされている必要があります。
- ブラウザでクッキーをイネーブルにする必要があります。
- DNS 名を使用してサーバを指定する場合、ホスト ファイルの変更に必要になるため、PC に対する管理者アクセス権が必要です。
- Oracle Java Runtime Environment（JRE）をインストールしておく必要があります。

  JREがインストールされていない場合は、ポップアップ ウィンドウが表示され、ユーザに対して使用可能なサイトが示されます。まれに、Java例外エラーで、ポート フォワーディング アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。

  1. ブラウザのキャッシュをクリアして、ブラウザを閉じます。
  2. Java アイコンがコンピュータのタスク バーに表示されていないことを確認します。
  3. Java のインスタンスをすべて閉じます。
  4. クライアントレス SSL VPN セッションを確立し、ポート フォワーディング Java アプレットを起動します。

- ブラウザで javascript をイネーブルにする必要があります。デフォルトでは有効に設定されています。
- 必要に応じて、クライアント アプリケーションを設定する必要があります。

（注） Microsoft Outlook クライアントの場合、この設定手順は不要です。Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。Windows アプリケーションの設定が必要かどうかを確認するには、[Remote Server] フィールドの値をチェックします。[Remote Server] フィールドにサーバ ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。[Remote Server] フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。

手順

ステップ 1 クライアントレス SSL VPN セッションを開始して、[Home] ページの [Application Access] リンクをクリックします。[Application Access] ウィンドウが表示されます。

ステップ 2 [Name] カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を [Local] カラムで確認します。

ステップ 3 この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。

（注） クライアントレス SSL VPN セッション上で実行しているアプリケーションで URL（電子メール メッセージ内のものなど）をクリックしても、サイトがそのセッションで開くわけではありません。サイトをセッション上で開くには、その URL を [Enter Clientless SSL VPN (URL) Address] フィールドに貼り付けます。

ポート転送を介した電子メールの使用

電子メールを使用するには、クライアントレス SSL VPN のホームページから Application Access を起動します。これにより、メール クライアントが使用できるようになります。

（注） IMAP クライアントの使用中にメール サーバとの接続が中断したり、新しく接続を確立できない場合は、IMAP アプリケーションを終了してクライアントレス SSL VPN を再起動します。

アプリケーション アクセスおよびその他のメール クライアントの要件を満たしている必要があります。

Web アクセスを介した電子メールの使用

次の電子メール アプリケーションがサポートされています。

- Microsoft Outlook Web App to Exchange Server 2010

  OWA には、Internet Explorer 11（以降）、または最新の Firefox が必要です。

- Exchange Server 2013 への Microsoft Outlook Web アクセス。

  最適な結果を得るために、Internet Explorer11（以降）または最新の Firefox で OWA を使用してください。

- Louts iNotes

（注） Web ベースの電子メール製品がインストールされており、その他の Web ベースの電子メール アプリケーションも動作する必要がありますが、検証されていません。

電子メール プロキシを介した電子メールの使用

メール アプリケーションの使用方法と例については、「クライアントレス SSL VPN を介した電子メールの使用」を参照してください。

はじめる前に

SSL 対応メール アプリケーションがインストールされている必要があります。

ASA SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express では TLS はサポートされません。

メール アプリケーションが正しく設定されている必要があります。

その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。

スマート トンネルの使用

スマート トンネルの使用に管理権限は必要ありません。

（注） ポート フォワーダの場合と異なり、Java は自動的にダウンロードされません。

- スマート トンネルを使用する場合、Windows では ActiveX または JRE、Mac OS X では Java Web Start が必要です。
- ブラウザでクッキーをイネーブルにする必要があります。

- ブラウザで javascript をイネーブルにする必要があります。
- Mac OS X では、フロントサイド プロキシはサポートされていません。
- サポートされているオペレーティング システムとブラウザだけを使用してください。
- TCP ソケットベースのアプリケーションだけがサポートされています。