



第 14 章

クライアントレス SSL VPN の概要

2014 年 4 月 14 日

クライアントレス SSL VPN の概要

クライアントレス SSL VPN を使用すると、エンド ユーザは SSL 対応 Web ブラウザを使用して、任意の場所から社内ネットワークのリソースに安全にアクセスできます。ユーザは、まず、クライアントレス SSL VPN ゲートウェイで認証し、事前設定されたネットワーク リソースにアクセスできるようにします。



(注) クライアントレス SSL VPN がイネーブルになっている場合、セキュリティ コンテキスト (ファイアウォール マルチモードとも呼ばれる) と Active/Active ステートフル フェールオーバーはサポートされません。

クライアントレス SSL VPN は、ソフトウェアまたはハードウェア クライアントを必要とせずに、Web ブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを作成します。HTTP 経由でインターネットに接続できるほとんどのデバイスから、幅広い Web リソースと、Web 対応およびレガシー アプリケーションに安全かつ簡単にアクセスできます。次の内容で構成されています。

- 内部 Web サイト
- Web 対応アプリケーション
- NT/Active Directory ファイル共有
- POP3S、IMAP4S および SMTPS などのプロキシに、電子メールを送信します。
- Microsoft Outlook Web Access Exchange Server 2000、2003、および 2007
- Microsoft Web App to Exchange Server 2010 (8.4(2) 以降において)
- Application Access (他の TCP ベースのアプリケーションにアクセスするためのスマート トンネルまたはポート転送)

クライアントレス SSL VPN は Secure Sockets Layer (SSL) プロトコルおよびその後継の Transport Layer Security (SSL/TLS1) を使用して、リモート ユーザと、内部サイトで設定した特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。ASA はプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ネットワーク管理者は、クライアントレス SSL VPN セッションのユーザに対してグループ単位でリソースへのアクセスを提供します。ユーザは、内部ネットワーク上のリソースに直接アクセスすることはできません。

前提条件

ASA Release 9.0 でサポートされているプラットフォームおよびブラウザについては、『[Supported VPN Platforms, Cisco ASA Series](#)』を参照してください。

注意事項と制約事項

- ActiveX ページでは、ActiveX リレーをイネーブルにするか、関連するグループ ポリシーに **activex-relay** を入力しておく必要があります。あるいは、スマート トンネル リストをポリシーに割り当て、エンドポイント上のブラウザ プロキシ例外リストにプロキシが指定されている場合、ユーザはそのリストに「shutdown.webvpn.relay.」 エントリを追加する必要があります。
- ASA では、Windows 7、Vista、Internet Explorer 8 ~ 10、Mac OS X、および Linux から Windows 共有 (CIFS) Web フォルダへのクライアントレス アクセスはサポートされていません。
- DoD Common Access Card および SmartCard を含む証明書認証は、Safari キーチェーンだけで動作します。
- ASA は、クライアントレス SSL VPN 接続では DSA または RSA 証明書をサポートしていません。
- 一部のドメインベースのセキュリティ製品には、ASA から送信された要求を超える要件があります。
- コンフィギュレーション制御の検査およびモジュラ ポリシー フレームワークのインスペクション機能はサポートされません。
- グループ ポリシーの **vpn-filter** コマンドは、クライアント ベースのアクセス用であり、サポートされません。グループ ポリシーのクライアントレス SSL VPN モードのフィルタは、クライアントレス ベースのアクセス用です。
- NAT および PAT はクライアントに適用可能ではありません。
- ASA は、**police** や **priority-queue** などの QoS レート制限コマンドの使用をサポートしません。
- ASA は、接続制限値の使用、スタティックまたはモジュラ ポリシー フレームワークの **set connection** コマンドを使用した確認をサポートしません。
- クライアントレス SSL VPN のコンポーネントの一部には、Java ランタイム環境 (JRE) が必要です。Mac OS X v10.7 以降では Java はデフォルトではインストールされていません。Mac OS X で Java をインストールする方法については、http://java.com/en/download/faq/java_mac.xml を参照してください。

クライアントレス ポータル用に設定された複数のグループ ポリシーがある場合は、ログイン ページのドロップダウンに表示されます。リストにある最初のグループ ポリシーで証明書が必要な場合は、ユーザはマッチング証明書が必要です。グループ ポリシーの一部が証明書を使用しない場合、非証明書ポリシーを最初に表示するには、リストを設定します。また、「0-Select-a-group」の名前でダミー グループ ポリシーを作成することもできます。



ヒント

グループポリシーの名前をアルファベット順に付けることで、最初に表示されるポリシーを制御できます。また、ポリシーの先頭に数字を付けることもできます。たとえば、1-AAA、2-Certificate とします。