CHAPTER 8

SSL 設定

SSL 設定

[Configuration] > [Device Management] > [Advanced] > [SSL Settings]

[Configuration] > [Remote Access VPN] > [Advanced] > [SSL Settings]

ASA は、Secure Sockets Layer（SSL）プロトコルおよび Transport Layer Security（TLS）を使用して、ASDM、クライアントレス SSL VPN、VPN、およびブラウザベースのセッションのセキュアなメッセージ伝送を実現します。[SSL Settings] ペインでは、クライアントとサーバの SSL バージョンおよび暗号化アルゴリズムを設定できます。また、以前に設定したトラストポイントを特定のインターフェイスに適用したり、関連付けられたトラストポイントのないインターフェイスのフォールバック トラストポイントを設定したりすることもできます。

(注) リリース 9.3（2）では、SSLv3 は廃止されています。現在のデフォルトは [any] ではなく [tlsv1] です。[any] キーワードは廃止されました。[any]、[sslv3] または [sslv3-only] を選択した場合、設定は受け入れられますが警告が表示されます。[OK] をクリックして作業を続行します。ASA の次のメジャー リリースでは、これらのキーワードは ASA から削除されます。

フィールド

- [Server SSL Version] : サーバとして動作するときに ASA が使用する最小の SSL/TLS プロトコル バージョンをドロップダウン リストから指定します。

Any	SSLv2 クライアントの hello を受け入れ、共通の最新バージョンをネゴシエートします。
SSL V3	SSLv2 クライアントの hello を受け入れ、SSLv3（以降）をネゴシエートします。
TLS V1	SSLv2 クライアントの hello を受け入れ、TLSv1（以降）をネゴシエートします。
TLSV1.1	SSLv2 クライアントの hello を受け入れ、TLSv1.1（以降）をネゴシエートします。
TLSV1.2	SSLv2 クライアントの hello を受け入れ、TLSv1.2（以降）をネゴシエートします。

- [Client SSL Version] : クライアントとして動作するときに ASA が使用する最小の SSL/TLS プロトコル バージョンをドロップダウン リストから指定します。

Any	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。
SSL V3	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。
TLS V1	TLSv1 クライアントの hello を送信し、TLSv1（以降）をネゴシエートします。
TLSV1.1	TLSv1.1 クライアントの hello を送信し、TLSv1.1（以降）をネゴシエートします。
TLSV1.2	TLSv1.2 クライアントの hello を送信し、TLSv1.2（以降）をネゴシエートします。

- [Diffie-Hellmann group to be used with SSL]：ドロップダウン リストからグループを選択します。使用可能なオプションは、[Group1]（768 ビット絶対値）、[Group2]（1024 ビット絶対値）、[Group5]（1536 ビット絶対値）、[Group14]（2048 ビット絶対値、224 ビット素数位数）、および [Group24]（2048 ビット絶対値、256 ビット素数位数）です。デフォルト値は [Group2] です。
- SSL 暗号化アルゴリズムを指定します。[Configure Cipher Algorithms/Custom String] ダイアログボックスを使用してテーブル エントリを定義または変更するには、[Edit] をクリックします。SSL 暗号のセキュリティ レベルを選択し、[OK] をクリックします。
  - [Cipher Version]：ASA でサポートされ、SSL 接続に使用される暗号バージョンを一覧表示します。
  - [Cipher Security Level]：ASA でサポートされ、SSL 接続に使用される暗号セキュリティ レベルを一覧表示します。次のいずれかのオプションを選択します。

    [All]：NULL-SHA を含むすべての暗号。

    [Low]：NULL-SHA を除くすべての暗号。

    [Medium]：NULL-SHA、DES-CBC-SHA、RC4-SHA、および RC4-MD5 を除くすべての暗号（これがデフォルトです）。

    [Fips]：NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除く FIPS 準拠のすべての暗号。

    [High]：SHA-2 を使用する AES-256 暗号だけが含まれ、TLS バージョン 1.2 にのみ適用されます。

    [Custom]：[Cipher algorithms/custom string] ボックスで指定する 1 つ以上の暗号。このオプションでは、OpenSSL 暗号定義文字列を使用して暗号スイートを詳細に管理できます。
  - [Cipher Algorithms/Custom String]：ASA でサポートされ、SSL 接続に使用される暗号アルゴリズムを一覧表示します。OpenSSL を使用した暗号の詳細については、https://www.openssl.org/docs/apps/ciphers.html を参照してください。

    ASA では、サポートされる暗号の優先順位が次のように指定されています。

    TLSv1.2 だけでサポートされる暗号

DHE-RSA-AES256-SHA256
AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256
DHE-RSA-AES256-SHA
AES256-SHA
DHE-RSA-AES128-SHA
AES128-SHA
DES-CBC3-SHA

TLSv1.1 または TLSv1.2 でサポートされない暗号

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

- [Server Name Indication (SNI)]：ドメイン名とそのドメインに関連付けるトラストポイントを指定します。[Add/Edit Server Name Indication (SNI)] ダイアログボックスを使用して各インターフェイスのドメインおよびトラストポイントを定義または変更するには、[Add] または [Edit] をクリックします。
  - [Specify domain]：ドメイン名を入力します。
  - [Select trustpoint to associate with domain]：ドロップダウン リストからトラストポイントを選択します。
- [Certificates]：各インターフェイスの SSL 認証に使用する証明書を割り当てます。[Select SSL Certificate] ダイアログボックスを使用して各インターフェイスのトラストポイントを定義または変更するには、[Edit] をクリックします。
  - [Primary Enrolled Certificate]：このインターフェイスの証明書に使用するトラストポイントを選択します。
  - [Load Balancing Enrolled Certificate]：VPN ロード バランシングが設定されている場合、証明書で使用するトラストポイントを選択します。
- [Fallback Certificate]：証明書が関連付けられていないインターフェイスで使用する証明書を選択します。[None] を選択すると、ASA はデフォルトの RSA キー ペアと証明書を使用します。
- [Forced Certification Authentication Timeout]：証明書認証がタイムアウトするまでの分数を設定します。
- [Apply]：変更内容を保存します。
- [Reset]：変更内容を取り消し、SSL パラメータを以前に定義した値にリセットします。