CHAPTER 37

SSL 設定の指定

SSL

セキュリティ アプライアンス は、Secure Sockets Layer（SSL）プロトコルおよびその後継である Transport Layer Security（TLS）を使用して、ASDM セッションとクライアントレス ブラウザベース 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 ウィンドウでは、クライアントとサーバ、および暗号化アルゴリズムの SSL バージョンを設定できます。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。

フィールド

- [Server SSL Version]：サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコル バージョンを指定します。選択できるのは 1 つだけです。

Server SSL バージョンのオプションは、次のとおりです。

Any	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、SSL バージョン 3 または TLS バージョン 1 がネゴシエートされます。
Negotiate SSL V3	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、SSL バージョン 3 にネゴシエートされます。
Negotiate TLS V1	セキュリティ アプライアンスによって SSL バージョン 2 クライアントの hello が受け入れられ、TLS バージョン 1 にネゴシエートされます。
SSL V3 Only	セキュリティ アプライアンスによって SSL バージョン 3 クライアントの hello のみが受け入れられ、SSL バージョン 3 のみが使用されます。
TLS V1 Only	セキュリティ アプライアンスによって TLSv1 クライアントの hello のみが受け入れられ、TLS バージョン 1 のみが使用されます。

（注） クライアントレス SSL VPN のポート転送を使用するには、Any または Negotiate SSL V3 を選択する必要があります。問題は、ポート フォワーディング アプリケーションを起動すると、JAVA ではクライアントの Hello パケットで SSLv3 のみがネゴシエートされることです。

- [Client SSL Version]：サーバとして動作するときにセキュリティ アプライアンスが使用する SSL/TLS プロトコル バージョンを指定します。選択できるのは 1 つだけです。

Client SSL バージョンのオプションは、次のとおりです。

any	セキュリティ アプライアンスによって SSL バージョン 3 の hello が送信され、SSL バージョン 3 または TLS バージョン 1 がネゴシエートされます。
sslv3-only	セキュリティ アプライアンスによって SSL バージョン 3 の hello が送信され、SSL バージョン 3 のみが受け入れられます。
tlsv1-only	セキュリティ アプライアンスによって TLSv1 クライアントの hello が送信され、TLS バージョン 1 のみが受け入れられます。

- [Encryption]：SSL 暗号化アルゴリズムを設定できます。
  - [Available Algorithms]：セキュリティ アプライアンス がサポートし、SSL 接続で使用されていない暗号化アルゴリズムを一覧表示します。使用可能なアルゴリズムを使用するか、またはアクティブにするには、アルゴリズムを選択して [Add] をクリックします。
  - [Active Algorithms]：セキュリティ アプライアンスがサポートし、現在 SSL 接続で使用中の暗号化アルゴリズムを一覧表示します。使用を中止するか、アクティブなアルゴリズムを [Available] ステータスに変更するには、アルゴリズムを選択して [Remove] をクリックします。
  - [Add/Remove]：[Available] または [Active Algorithms] カラムの暗号化アルゴリズムのステータスを変更します。
  - [Move Up] および [Move Down]：アルゴリズムを選択し、これらのボタンをクリックして優先順位を変更します。セキュリティ アプライアンスは、アルゴリズムの使用を試みます。
- [Certificates]：フォールバック証明書を選択できます。設定済みのインターフェイスおよびそれらに関連付けられている設定済みの証明書が表示されます。
  - [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、セキュリティ アプライアンス はデフォルトの RSA キーペアと証明書を使用します。
  - [Interface] カラムおよび [ID Certificate] カラム：設定済みインターフェイス、および存在する場合にはそのインターフェイスの証明書を表示します。
  - [Edit]：選択したインターフェイスのトラストポイントを変更します。
- [Apply]：変更を適用します。
- [Reset]：変更内容を取り消し、SSL パラメータをリセットして、ウィンドウを開いたときに保存されていた値に戻します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Edit SSL Certificate

フィールド

- [Interface]：編集中のインターフェイスの名前を表示します。
- [Certificate]：名前付きインターフェイスに関連付ける登録済みの証明書を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SSL 証明書

このペインでは、デバイス管理セッションで SSL 認証のユーザ証明書を必要とするように指定できます。

フィールド

- [Interface]：編集中のインターフェイスの名前を表示します。
- [User Certificate Required]：名前付きインターフェイスに関連付ける登録済み証明書を選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—