ローカル ポリシーでの FIPS の有効化

FIPS、NGE、および AnyConnect について

AnyConnect には、Cisco Common Cryptographic Module（C3M）が組み込まれています。この Cisco SSL の実装には、新世代の暗号化（NGE）アルゴリズムの一部として、連邦情報処理標準（FIPS）140-2 に準拠した暗号化モジュールや国家安全保障局（NSA）Suite B 暗号化が含まれます。

NGEには、増え続けるセキュリティおよびパフォーマンス要件のための新しい暗号化、認証、デジタル署名、キー交換アルゴリズムが導入されています。RFC 6279 では、Suite B 暗号化アルゴリズムが定義されています。これは、米国の FIPS 140-2 標準を満たします。

AnyConnect コンポーネントは、ヘッドエンド（ASA または IOS ルータ）の設定に基づいて FIPS 標準暗号化をネゴシエートして使用します。次の AnyConnect クライアント モジュールは FIPS をサポートしています。

- AnyConnect コア VPN：VPN クライアントの FIPS 準拠は、ユーザ コンピュータ上のローカル ポリシー ファイルの FIPS モード パラメータを使用して有効化されます。Suite B 暗号化は、TLS/DTLS および IKEv2/IPsec VPN 接続で使用可能です。詳細および手順については、「AnyConnect コア VPN クライアントのための FIPS の設定」を参照してください。

  AnyConnect ローカル ポリシー ファイル AnyConnectLocalPolicy.xml には、ローカル クライアントに適用される FIPS モードの他に追加のセキュリティ設定が含まれています。これは ASA によって展開されないため、手動でインストールするか、社内のソフトウェア展開システムを使用して展開する必要があります。このプロファイルの使用方法については、「AnyConnect ローカル ポリシーの設定」を参照してください。

- AnyConnect ネットワーク アクセス マネージャ：ネットワーク アクセス マネージャの FIPS 準拠は、AnyConnectLocalPolicy.xml ファイルの FIPS モード パラメータ、およびネットワーク アクセス マネージャ プロファイルの FIPS モード パラメータを使用して有効にします。ネットワーク アクセス マネージャのための FIPS は Windows でサポートされています。

詳細および手順については、「ネットワーク アクセス マネージャのための FIPS の設定」を参照してください。

AnyConnect の FIPS 機能

機能	コア VPN モジュール	ネットワーク アクセス マネージャ モジュール
対称暗号化や完全性のための AES-GCM サポート。	IKEv2 ペイロード暗号化と認証用の 128、192、256 ビットの各キー。 ESP パケット暗号化および認証。	ソフトウェア（Windows）で有線トラフィック暗号化を実現する 802.1AE（MACsec）用 128 ビット キー。
ハッシュ用 SHA-2 サポート、256/384/512 ビットの SHA。	IKEv2 ペイロード認証および ESP パケット認証。（Windows 7 以降および macOS 10.7 以降）。	TLS ベースの EAP 方式で SHA-2 を使用して証明書を使用できる機能。
キー交換向けの ECDH サポート。	グループ 19、20、および 21 の IKEv2 キー交換および IKEv2 PFS。	TLS ベースの EAP 方式で ECDH を使用できる機能（Windows）。
デジタル署名、非対称暗号化、および認証の ECDSA サポート、256、384、521 ビット楕円曲線。	IKEv2 ユーザ認証およびサーバ証明書の確認。	TLS ベースの EAP 方式で ECDSA を使用して証明書を使用できる機能。
その他のサポート。	IPsecV3 に必要なすべての暗号アルゴリズム（ヌル暗号化を除く）。 IKEv2 用の Diffie-Hellman Groups 14 および 24。 TLS/DTLS および IKEv2 用の 4096 ビット キーを使用する RSA 証明書。	該当なし

[1] Linux では、AnyConnect ファイル ストアのみが ECDSA でサポートされます。ファイル ストアに証明書を追加するには、「Mac および Linux での PEM 証明書ストアの作成」を参照してください。

[2] IPsecV3 は、ESN（Extended Sequence Numbers）がサポートされなければならないことも明記していますが、AnyConnect は ESN をサポートしません。

AnyConnect FIPS の要件

- Suite B 暗号化は、TLS/DTLS および IKEv2/IPsec VPN 接続で使用可能です。
- FIPS または Suite B のサポートは、セキュア ゲートウェイで必要です。シスコは、ASA バージョン 9.0 以降では Suite B 機能、ASA バージョン 8.4.1 以降では FIPS 機能を提供します。
- ECDSA 証明書の要件は次のとおりです。
  - カーブ強度以上のダイジェスト強度がなければなりません。たとえば、EC-384 キーは SHA2-384 以上を使用しなければなりません。
  - Windows 7 以降、macOS 10.7 以降、Red Hat Enterprise Linux 6.x または 6.4（64 ビット）、Ubuntu 12.4 および 12.10（64 ビット）でサポートされています。ECDSA スマート カードは、Windows 7（およびそれ以降のバージョン）でのみサポートされています。

AnyConnect FIPS の制限事項

SHA-2 を使用して署名された証明書を検証する際、EAP 方式は、TLS ベースの EAP を除き SHA-2 をサポートしません。

AnyConnect FIPS のガイドライン

- AnyConnect クライアントの [統計情報（Statistics）] パネル（[トランスポート情報（Transport Information）] ヘッダーの下）には、使用中の暗号名が表示されます。
- AES-GCM は、計算集約型のアルゴリズムであるため、これらのアルゴリズムを使用するときは、全体的なデータ レートが低くなる可能性があります。新しい Intel プロセッサの一部は、特に AES-GCM の性能を向上させるために採用された特別な命令を含むものもあります。AnyConnect は、それが実行されるプロセッサ上でそれらの新しい命令がサポートされているかどうかを自動的に検出します。サポートされている場合は、AnyConnect は新しい命令を使用し、特別な命令を持たないプロセッサと比較して VPN データ レートを大幅に向上させます。新しい命令をサポートするプロセッサのリストについては、http://ark.intel.com/Search/FeatureFilter?productType=processors&AESTech=true を参照してください。詳細については、http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/ を参照してください。
- 暗号化と整合性の検証の両方が 1 回の操作で実行される複合モードの暗号化アルゴリズムは、ハードウェア クリプト アクセラレーションを使用する SMP ASA ゲートウェイ（5585 および 5515-X など）でのみサポートされます。AES-GCM は、シスコがサポートする複合モードの暗号化アルゴリズムです。

（注） IKEv2 ポリシーは、通常モードまたは複合モードの暗号化アルゴリズムのうちの 1 つを含めることができますが、両方は不可能です。複合モードのアルゴリズムが IKEv2 ポリシーで設定されると、通常モードのアルゴリズムすべてが無効になるので、唯一有効な整合性アルゴリズムは NULL です。

IKEv2 IPsec プロポーザルは別のモデルを使用し、同じプロポーザル内で標準モードと複合モードの両方の暗号化アルゴリズムを指定できます。この使用方法では、両方に整合性アルゴリズムを設定する必要があります。その結果、非 NULL 整合性アルゴリズムが AES-GCM 暗号化で設定されます。

- ASA が SSL および IPsec 用の異なるサーバ証明書で設定されている場合は、信頼できる証明書を使用してください。異なる IPsec および SSL 証明書を持つ Suite B（ECDSA）の信用されていない証明書を使用する場合、ポスチャ評価、WebLaunch、またはダウンローダの障害が発生する可能性があります。

AnyConnect FIPS のレジストリ変更によるエンドポイントに関する問題の回避

コア AnyConnect クライアントの FIPS を有効にすると、エンドポイントで Windows レジストリの設定が変更されます。エンドポイントの他のコンポーネントでは、AnyConnect が FIPS を有効にしたこと、および暗号化の使用を開始したことを検出できます。たとえば、Remote Desktop Protocol（RDP）では、サーバで FIPS 準拠の暗号化を使用している必要があるため、Microsoft Terminal Services クライアントの RDP は機能しません。

これらの問題を回避するために、パラメータ
[Use FIPS compliant algorithms for encryption, hashing, and signing] を Disabled に変更することにより、[Windows Local System Cryptography] 設定で FIPS 暗号化を一時的に無効にできます。エンドポイントデバイスをリブートすると、この設定が変更されて有効に戻ることに注意してください。

次の表に、認識の必要がある、AnyConnect によって実行される Windows レジストリ変更を示します。

レジストリ キー	変更内容
HKLM\System\CurrentControlSet\ Control\Lsa	FIPSAlgorithmPolicy が 0 から 1 に変更されます。
HKCU\Software\Microsoft\Windows\ CurrentVersion\Internet Settings	元の設定にビット単位で 0x080 の「or」を実行することにより、[SecureProtocols] 設定が TLSV1 に変更されます。

レジストリ キー	変更内容
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet	元の設定にビット単位で 0x080 の「or」を実行することにより、[SecureProtocols] 設定が TLSV1 に変更されます。 これにより、1 つのグループ ポリシーに対する TLSv1 が設定されます。

AnyConnect コア VPN クライアントのための FIPS の設定

AnyConnect コア VPN のための FIPS の有効化

手順

ステップ 1 AnyConnect プロファイル エディタで、VPN ローカル ポリシー プロファイルを開くか、作成します。

ステップ 2 [FIPS モード（FIPS Mode）] を選択します。

ステップ 3 VPN ローカル ポリシー プロファイルを保存します。

FIPS が有効であることを示す名前をプロファイルに付けることをお勧めします。

Windows インストール時の FIPS の有効化

Windows インストールでは、Cisco MST ファイルを標準 MSI インストール ファイルに適用して、AnyConnect ローカル ポリシーで FIPS を有効にできます。この MST のダウンロード元の詳細については、FIPS 用に受け取ったライセンシング情報を参照してください。インストール時に、FIPS が有効にされた AnyConnect ローカル ポリシー ファイルが生成されます。このユーティリティを実行した後、ユーザのシステムを更新します。

（注） この MST は FIPS だけを有効にします。その他のパラメータは変更しません。Windows インストール中に他のローカル ポリシーの設定を変更するには、「MST ファイルでのローカル ポリシー パラメータの有効化」を参照してください。

ネットワーク アクセス マネージャのための FIPS の設定

ネットワーク アクセス マネージャは、FIPS ネットワークと非 FIPS ネットワークの両方に同時に接続したり、FIPS ネットワークだけに接続したりするように設定できます。

手順

ステップ 1 ネットワーク アクセス マネージャのための FIPS の有効化。

FIPS を有効にすると、ネットワーク アクセス マネージャは FIPS ネットワークと非 FIPS ネットワークの両方に接続できます。

ステップ 2 必要に応じて、ネットワーク アクセス マネージャに対する FIPS モードの適用。

FIPS モードを適用すると、ネットワーク アクセス マネージャの接続が FIPS ネットワークだけに制限されます。

ネットワーク アクセス マネージャのための FIPS の有効化

手順

ステップ 1 AnyConnect ローカル ポリシーで FIPS モードを有効にします。

a) AnyConnect プロファイル エディタで、VPN ローカル ポリシー プロファイルを開くか、作成します。
b) [FIPS モード（FIPS Mode）] を選択します。
c) VPN ローカル ポリシー プロファイルを保存します。

FIPS が有効であることを示す名前をプロファイルに付けることをお勧めします。

ステップ 2 AnyConnect ネットワーク アクセス マネージャ クライアント プロファイルで FIPS モードを有効にします。

a) AnyConnect プロファイル エディタで、ネットワーク アクセス マネージャ プロファイルを開くか、作成します。
b) [クライアント ポリシー（Client Policy）] 設定ウィンドウを選択します。
c) [管理ステータス（Administrative Status）] セクションで、[FIPS モード（FIPS Mode）] に [有効（Enable）] を選択します。
d) ネットワーク アクセス マネージャ プロファイルを保存します。

FIPS が有効であることを示す名前をプロファイルに付けることをお勧めします。

ネットワーク アクセス マネージャに対する FIPS モードの適用

ネットワーク アクセス マネージャ プロファイルで、許可する関連付け、暗号化モード、認証方式を制限することにより、企業の従業員に対して FIPS 準拠のネットワークのみへの接続を強制します。

まず、ネットワーク アクセス マネージャのための FIPS の有効化を行い、FIPS モードを適用します。

手順

ステップ 1 AnyConnect プロファイル エディタでネットワーク アクセス マネージャ プロファイルを開きます。

ステップ 2 ネットワーク アクセス マネージャの FIPS 準拠では、WPA2 パーソナル（WPA2-PSK）、WPA2 エンタープライズ（802.1X）などの FIPS 認定の AES 暗号化モードをサポートしています。

ステップ 3 ネットワーク アクセス マネージャの FIPS サポートには、EAP 方式 EAP-TLS、EAP-TTLS、PEAP、EAP-FAST、および LEAP が含まれています。

ステップ 4 ネットワーク アクセス マネージャ プロファイルを保存します。

FIPS 接続だけが可能であることを示す名前をプロファイルに付けることをお勧めします。