IPsec 拡張シーケンス番号

拡張シーケンス番号（ESN）は、IPsec 標準シーケンス番号に追加され、高速 IPsec 実装を支援するために使用されます。IPsec パケットには 32 ビットのシーケンス番号があり、IKE キー付き IPsec セキュリティ アソシエーション（SA）では、シーケンス番号のロールオーバー後のキー再生成が必須です。ESN は、シーケンス番号を 64 ビットに拡張することにより、この高い IPsec SA キー再生成レートの低下を試みます。これにより、必須のキー再生成までの時間が長くなります。

IPsec 拡張シーケンス番号の前提条件

- ESN は、セキュアな接続の確立に関与する両方の IPsec ピアでサポートされている必要があります。いずれかのピアが ESN をサポートしていない場合、この機能は機能しません。
- ESN を使用する場合は、アンチリプレイ設定が必要です。詳細については、「IPsec アンチリプレイウィンドウの拡張と無効化」を参照してください。

IPsec 拡張シーケンス番号に関する制約事項

- ESN は、Cisco Catalyst 8500 シリーズ エッジ プラットフォームと Cisco ASR 1000 シリーズ ESP 100-X および ESP 200-X でのみサポートされています。
- ESN 機能は、DES または 3DES アルゴリズムではサポートされません。

IPsec 拡張シーケンス番号に関する情報

IPsec 拡張シーケンス番号

拡張シーケンス番号（ESN）は、IPsec 標準シーケンス番号に追加され、高速 IPsec 実装を支援するために使用されます。ESN は、標準のシーケンス番号よりも大きなシーケンス番号スペースを使用します。これにより、顧客は、キーを再生成せずに大量のデータを高速で送信できます。

IPsec パケットには 32 ビットのシーケンス番号があり、IKE キー付き IPsec セキュリティ アソシエーション（SA）では、シーケンス番号のロールオーバー後のキー再生成が必須です。ESN は、シーケンス番号を 64 ビットに拡張することにより、この高い IPsec SA キー再生成レートの低下を試みます。これにより、必須のキー再生成までの時間が長くなり、シーケンス番号のロールオーバーが防止されます。その結果、システムリソースの使用率が低下し、高速 IPsec 接続や、長い IPsec SA ライフタイムを必要とする IPsec 実装での、頻繁なキー再生成が防止されます。

IPsec 拡張シーケンス番号の設定方法

IPsec 拡張シーケンス番号の設定

IPsec 拡張シーケンス番号のサポートを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*]
4. **esn**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] 例： `Router (config)# crypto ipsec transform-set foo esp-aes esp-sha-hmac`	IPsec 用のトランスフォームセットを設定します。 • transform 引数に使用できるエントリを定義する複合ルールがあります。これらルールについては、**crypto ipsec transform-set** コマンドのコマンド解説で説明します。また、「トランスフォームセットの概要」の表に、許可されるトランスフォームの組み合わせのリストを示します。
ステップ 4	**esn** 例： `Router(cfg-crypto-trans)#[no] esn [optional]`	（オプション）IPsec ESN を有効にします。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS セキュリティ コマンド リファレンス』

IPsec ESN サポートに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : IPsec* 拡張シーケンス番号に関する機能情報

機能名	リリース	機能情報
IPsec 拡張シーケンス番号（ESN）	Cisco IOS XE Gibraltar 16.11.1 リリース	この機能は、次のプラットフォームに導入されました。 • Cisco Catalyst 8500 シリーズエッジプラットフォーム • Cisco ASR 1000 シリーズ ESP 100-X および ESP 200-X

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。