Cisco IOS XE 17.10.1a の新機能

この章は、次の項で構成されています。

ソフトウェアによる MACsec

概要

既存のすべての Cisco IOS XE ベースのルータ/スイッチは、特殊なトランシーバを使用して MACsec 暗号化/暗号解読を実行します。このソフトウェア MACsec は、QFP の CDAL インフラストラクチャを使用して暗号化操作を実行します。ハードウェアの選択と比較すると、設定/ステータス/データパスの実行方法が異なるため、機能にいくつかの制限が生じます。

リリース 17.10.1a は、L2 インターフェイスでのみ MACsec をサポートします。MACsec ポートをアクセスモードにする必要があります。暗号化は出力 SVI インターフェイスで行われるため、ポートに使用される VLAN は一意である必要があります。つまり、他のインターフェイスはその VLAN を使用できません。この制限は、QFP に MAC テーブル情報がないために生じています。

（注） MACsec はソフトウェアを介して実行されるため、パフォーマンスは L2 インターフェイスのラインレートではありません。

出力パケットの場合、SVI は、特定のインターフェイスに関する情報はなく、パケットが VLAN に送信される必要があることのみを認識しています。どのポートを使用するかを決定するのはスイッチチップです。MACsec タグのないパケットはすべて、通常どおり受信できます。発信 L2 パケットも、暗号化や変更なしで出力されます。

NE ライセンスと NA ライセンスの両方が GCM-AES-128 をサポートしています。この機能は、実行中の NPE イメージでは使用できません。

MACsec プロトコルは、IEEE802.1AE で定義されています。

機能の制約事項

- MACsec は、このリリースのコントローラモードではサポートされていません。
- MACsec インターフェイスには一意の VLAN ID が必要です。
- この初期リリースでは、gcm-aes-128 のみがサポートされています。
- 入力側では、明示的および非明示的な SCI の両方がサポートされています。IR1101 はエンドシステムではないため、明示的な SCI パケットのみを送信します。
- IR1101 は機密性オフセットをサポートしていません。
- この最初のリリースでは、「完全性のみ」がサポートされていません。
- gcm-aes-128 の場合、プレーンパケットと比較して、暗号化されたパケットには最大 32 バイトが追加されます。そのため、MTU セットアップは、正しく動作するために 32 を追加する必要があります。
- MACsec キーは MKA モジュールによって管理されます。そのデバイスでは、MKA が MACsec キーをネゴシエートするために静的キーが必要です。
- MIB のサポートはありません。

関連資料

詳細については、次を参照してください。

- MACsec and the MACsec Key Agreement (MKA) Protocol
- MACSEC and MKA Configuration Guide, Cisco IOS XE 17

MKA 設定の例

次の例を参照してください。

```
conf t
   aaa new-model
   mka policy p1
       key-server priority 1
       macsec-cipher-suite gcm-aes-128
       sak-rekey interval 3600
end
conf t
   key chain cak1 macsec
      key 414243
         cryptographic-algorithm aes-128-cmac
         key-string 0 12345678901234567890123456789012
         lifetime local 00:00:00 29 November 2021 infinite
end
conf t
   int fa 0/0/2
      switchport mode access
      switchport access vlan 77
      mtu 1532
```

```
      mka policy p1
      mka pre-shared-key key-chain cak1
      macsec network-link
      macsec replay-protection window-size 128
end
```

コマンドの表示

cpp_cp 内部情報を表示します。

```
show platform hardware cpp active feature soft-macsec server tx [dp] [item]
show platform hardware cpp active feature soft-macsec server rx [dp] [item]
show platform hardware cpp active feature soft-macsec server control [dp] [item]
```

その他の show コマンド：

```
show macsec summary
show macsec status int fa 0/0/2
show macsec statistics int fa 0/0/2A
```

統計のクリア

```
Clear macsec statis int fa 0/0/2
```

テストコマンド

デバッグ用に 10 MKA パケットを出力します。

```
test platform software smacsec mka-ingress
```

高セキュリティ（HSEC）ライセンス

HSEC（High Security）ライセンスは、ネットワークライセンス（NE/NA）に加えて設定できる機能ライセンスです。HSEC ライセンスは、強力なレベルの暗号化に対応した輸出規制を提供します。HSEC は、現在輸出入が禁止されている国を除くすべての国のお客様に利用可能です。これらの国は、米国商務省のリストに記載されています。HSEC ライセンスがない場合、SEC のパフォーマンスは各方向への IPsec スループットが合計 250 Mbps に制限されます。HSEC ライセンスによってこの制限を排除できます。

コマンドライン インターフェイス

IR1101 で HSEC を有効にする設定モード CLI は次のとおりです。

```
IR1101(config)# license feature hsec9
```

HSEC ライセンスにより、新しい帯域幅が利用可能になります。新しい帯域幅は **uncapped** と呼ばれ、設定モードから次の CLI で使用できます。

```
IR1101(config)# platform hardware throughput level ?
250M throughput in bps
uncapped throughput in bps
IR1101# platform hardware throughput level uncapped
```

上記のコマンドを実行した後、mem を書き込んでルータをリロードします。設定は、ルータが再起動すると有効になります。

ライセンスタイプ

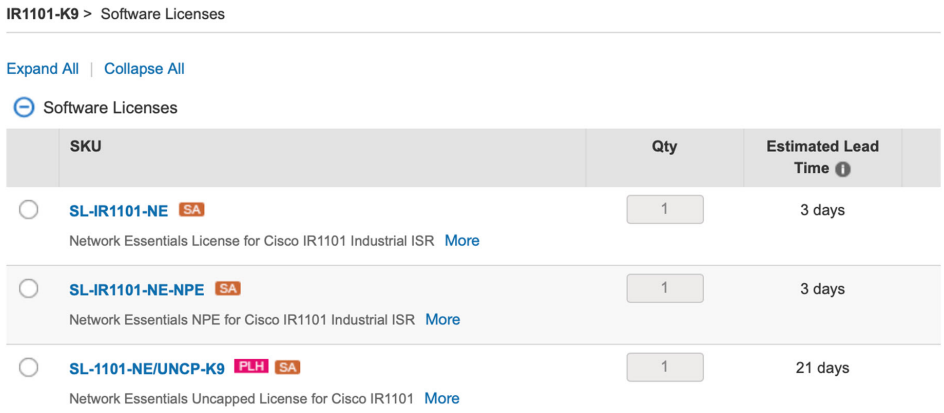
この新機能により、IR1101 は次の帯域幅/ライセンスタイプをサポートします。

- Network-essentials 250 Mbps
- Network-advantage 250 Mbps
- Network-essentials uncapped
- Network-advantage uncapped
- HSEC

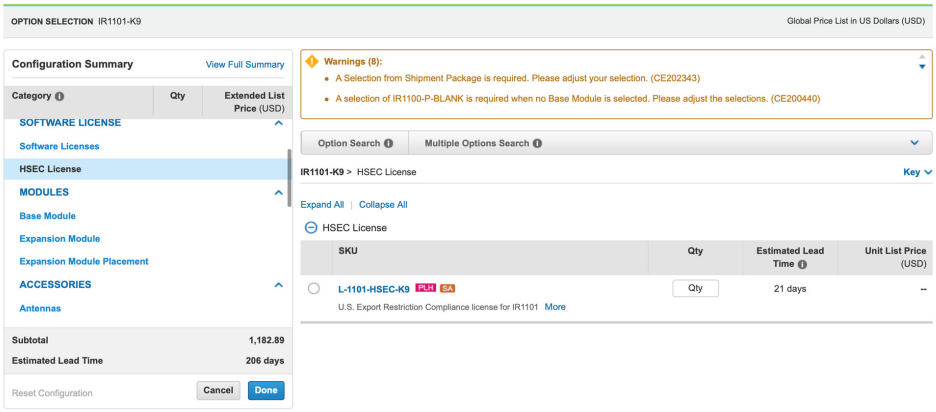
注文

以下は IR1101-K9 の例です。このライセンスは、IR1101-A-K9 でも利用できます。

次の例では、SL-1101-NE/UNCP-K9（Network Essentials Uncapped ライセンス）を選択します。



L-1101-HSEC-K9 ライセンスは、次に示すように、uncapped（上限なし）ライセンスを選択すると自動的に含まれます。



Cisco Software Central

このガイドでは、シスコスマートライセンスを注文、アクティブ化、および管理する方法について説明します。

https://software.cisco.com/software/csws/ws/platform/home?locale=en_US&locale=en_US&locale=en_US#

セキュアデータワイプ機能の有効化

セキュアデータワイプは、すべての IOS XE ベースのプラットフォーム上のストレージデバイスが NIST SP 800-88r1 準拠の安全に消去するコマンドを使用して適切に消去されるようにするためのシスコ全体のイニシアチブです。可能な限り常に、IoT プラットフォームは、対応する ENG の設計とこれまでのプラットフォームで利用可能な実装を活用します。

この機能は、次の IoT プラットフォームでサポートされます。

- IR1101
- IR1800
- IR8140
- ESR6300

セキュアデータワイプの有効化が実行されると、以下が消去されます。

- IR1101、IR1800、IR8140：NVRAM、rommon 変数、およびブートフラッシュ
- ESR6300：NVARM、rommon 変数、ブートフラッシュ

コマンドの実行後、ルータは工場出荷時のデフォルト設定（ボーレート 9600）で rommon プロンプトになります。TFTP ダウンロード（プラットフォームでサポートされている場合）または usbflash を介して IOS イメージで起動するまで、ブートフラッシュはフォーマットされません。

セキュアデータワイプの実行

この機能を有効にするには、次を実行します。

```
Router#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure?
[confirm]Y
```

重要 この操作には数時間かかる場合があります。電源を入れ直さないでください。

コマンドの実行後にログを確認し、IOS XE を起動するには、次の手順を実行します。

```
Router#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IR1800
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```

raw ソケットキープアライブ設定 CLI

非同期インターフェイスの raw ソケットキープアライブは、従来の IOS プラットフォームに存在していた機能の 1 つです。17.10.1a の一部として、この機能は IOS-XE ベースのプラットフォームに拡張されます。次の構文を持つ新しい CLI が raw ソケットの下に追加されます。

```
Router(config-line)#raw-socket tcp keepalive interval
```

CLI の変更

17.10.1a 以降の IOS-XE プラットフォームでは、CLI の修正があり、追加の CLI が raw ソケットの一部として追加されました。

修正は、**raw-socket idle timeout** コマンドに対するものです。以前の設定では分のみを使用していましたが、分と秒に基づいてタイムアウトを設定するオプションが追加されました。

```
Router(config-line)# raw-socket tcp idle-timeout [0-1440] [<0-59> | cr]
```

追加の CLI は、raw ソケット TCP クライアントをクリアするためのものです。コマンドの構文は **clear raw-socket line** *[1-145|tty|x/y/z]* です。例：

```
Router# clear raw-socket line 0/2/0
```

（注） clear raw-socket line を開始すると、**show raw-socket tcp sessions** コマンドから raw ソケットクライアントの raw ソケットセッションがクリアされます。接続は、TCP ハンドシェイク後に再確立されます。これは、TCP 接続インターフェイスで shut/no shut を実行することで達成できます。

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。