CloudSec 暗号化

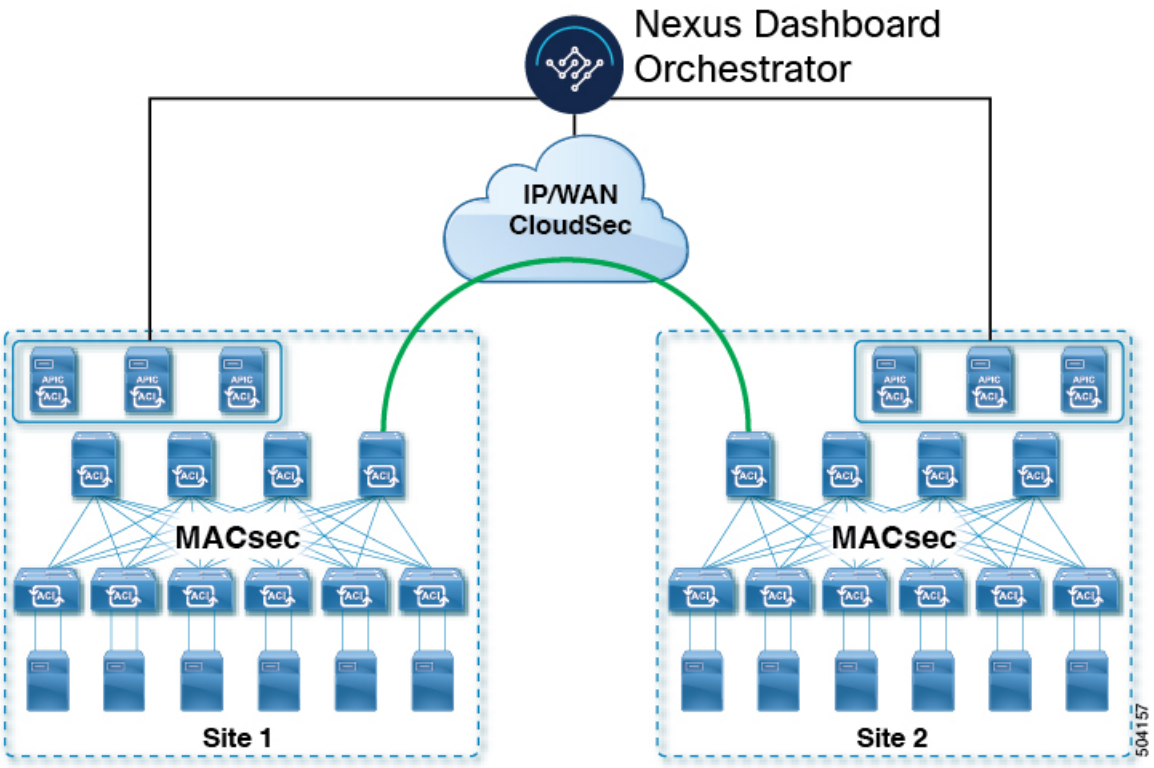
Cisco ACI CloudSec 暗号化

ほとんどの Cisco ACI 展開で、ディザスタリカバリとスケーリングに対処する Multi-Site アーキテクチャを採用しているため、ローカルサイト内で MACsec 暗号化を使用する現在のセキュリティ実装は、複数のサイトにわたるデータセキュリティと整合性を保証するには不十分になっています。それらのサイトは、安全でない外部 IP ネットワークによって接続されており、個別のファブリックを相互接続しているからです。Nexus Dashboard Orchestrator リリース 2.0(1) は、トラフィックのサイト間暗号化を提供するために設計された CloudSec 暗号化を導入しています。

Multi-Site トポロジはサイト間の接続を提供するために、3 つのトンネル エンドポイント (TEP) IP アドレス（Overlay Multicast TEP、Overlay Unicast TEP、および External TEP Pool）を使用します。これらの TEP アドレスは、 Nexus Dashboard Orchestrator の管理者により設定され、各サイトの Cisco APIC にプッシュ ダウンされ、その後スパイン スイッチで設定されます。これらの 3 つのアドレスは、トラフィックがリモートサイトに送信されるタイミングを決定するために使用されます。この場合、2 つのスパイン スイッチ間に暗号化された CloudSec トンネルが作成され、サイト間ネットワーク (ISN) を介して 2 つのサイト間の物理接続が提供されます。

次の図は、ローカルサイトトラフィックの MACsec とサイト間トラフィックの暗号化に CloudSec を組み合わせた全体的な暗号化アプローチを示しています。

図 *1 : CloudSec* 暗号化



要件と注意事項

CloudSec 暗号化を設定する場合は、次の注意事項が適用されます。

- CloudSec は、Nexus 9000 サイト間ネットワーク（ISN）インフラストラクチャを使用して検証されています。ISN インフラストラクチャがさまざまなデバイスで構成されている場合、またはデバイスが不明な場合（サービスプロバイダーから購入した回線の場合など）、ASR1K ルーターは、ACI スパイン（各サイトに展開された ASR1K デバイスの個別のペアを使用）、または Nexus 9000 ISN ネットワークに直接接続するファースト ホップ デバイスである必要があります。パディング フィックスアップが有効になっている ASR1K ルーターにより、CloudSec トラフィックはサイト間の任意の IP ネットワークを通過できます。

  ASR1K ルーターを構成するには：

  1. デバイスにログインします。
  2. UDP ポートを構成します。

（注） リリース 3.7(1) 以降を実行していて、IANA が割り当てたポート 8017 を使用するように CloudSec を構成する場合は、代わりに次のコマンドでそのポートを指定します。

```
ASR1K(config)# platform cloudsec padding-fixup dst-udp-port 9999
```

3. 設定を確認します。

   次の出力で、前の手順で構成したポート（8017 または 9999）が表示されていることを確認します。

```
ASR1K# show platform software ip rp active cloudsec
  CloudSec Debug: disabled
  CloudSec UDP destination port: enabled
  1st UDP destination port: 9999
  2nd UDP destination port: 0
  3rd UDP destination port: 0

ASR1K# show platform software ip fp active cloudsec
  CloudSec Debug: disabled
  CloudSec UDP destination port: enabled
  1st UDP destination port: 9999
  2nd UDP destination port: 0
  3rd UDP destination port: 0
```

- CloudSec暗号化を無効にしようとしたときに1つ以上のスパインスイッチがダウンした場合、スイッチがアップするまで、これらのスイッチでディセーブルプロセスは完了しません。これにより、スイッチが再起動したときにパケットがドロップされることがあります。

  CloudSec暗号化を有効または無効にする前に、ファブリック内のすべてのスパインスイッチが稼働していること、または完全に停止していることを確認することを推奨します。

- Nexus Dashboard Orchestrator リリース 3.7(1) 以降では、IANA が割り当てたポートを使用するように CloudSec 暗号化を構成できます。

  デフォルトでは、CloudSec は独自の UDP ポートを使用します。Orchestrator リリース 3.7(1) 以降は、サイト間の CloudSec 暗号化に IANA が予約した公式ポート 8017 を使用するように構成できます。

（注） IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。

この設定を変更するには、すべてのサイトでCloudSecを無効にする必要があります。IANA 予約ポートを有効にしたいが、すでに 1 つ以上のサイトで CloudSec 暗号化を有効にしている場合は、すべてのサイトで CloudSec を無効にし、[IANA 予約 UDP ポート（IANA Reserve UDP Port）] オプションを有効にしてから、必要なサイトで CloudSec を再度有効にします。

- CloudSec 暗号化機能は、次の機能ではサポートされません。
  - 高精度時間プロトコル（PTP）
  - リモート リーフ ダイレクト
  - 仮想ポッド（vPod）
  - SDA
  - リモート リーフまたはマルチポッド構成
  - サイト間 L3Out（サイトが 5.2(4) より前の Cisco APIC リリースを実行している場合）。

    CloudSec は、リリース 5.2(4) 以降を実行している APIC サイトのサイト間 L3Out でサポートされています。

要件

CloudSec 暗号化機能では、次のものが必要です。

- Cisco ACI スパイン/リーフアーキテクチャと 1 台の Cisco APIC クラスタ（各サイト用）
- 各サイトを管理する Cisco Nexus Dashboard Orchestrator
- ファブリックのデバイス（リーフのみ）ごとに 1 つの **Advantage** または **Premier** ライセンス
- デバイスが固定スパインである場合には、暗号化のため、デバイスごとに 1 つの **ACI-SEC-XF** アドオン ライセンス
- デバイスがモジュール スパインである場合には、暗号化のため、デバイスごとに 1 つの **ACI-SEC-XM** アドオン ライセンス

次の表に、CloudSec 暗号化に対応したハードウェア プラットフォームとポート範囲を示します。

ハードウェア プラットフォーム	ポート範囲
N9K C9364C スパインスイッチ	ポート 49-64
N9K-C9332C スパインスイッチ	ポート 25-32
N9K-X9736C-FX ラインカード	ポート 29-36

CloudSec がサイトに対して有効になっているが、暗号化がポートでサポートされていない場合、サポートされていないインターフェイスのエラーメッセージで障害が発生します。

CloudSec 暗号化のパケット カプセル化は、DWDM-C SFP10G などの Cisco QSFP から SFP へのアダプタ (QSA) がサポートされている光ファイバで使用されている場合にサポートされます。サポートされている光ファイバの完全なリストは、https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html のリンクから入手できます。

IANA が割り当てたポートと Orchestrator のダウングレードの使用

次のセクションで説明されているように、IANA が割り当てたポートを使用するように CloudSec 暗号化を構成した場合、Orchestrator サービスをリリース 3.7(1) より前のリリースにダウングレードする場合、いくつかの手順を実行する必要があります。

Nexus Dashboard Orchestrator を IANA ポートがサポートされていないリリースにダウングレードする前に:

1. すべての管理対象サイトの CloudSec 暗号化を無効にします。
2. インフラ構成設定で IANA 予約済み UDP ポート オプションを無効にします。
3. 以前に有効にしたすべてのサイトで CloudSec 暗号化を再度有効にします。
4. 通常どおり、Orchestrator サービスをダウングレードします。

CloudSec 暗号化に関する用語

CloudSec 暗号化機能は、サイト間の初期キーとキー再生成の要件に対して、安全なアップストリーム対称キーの割り当てと配布方法を提供します。この章では、次の用語を使用します。

- アップストリーム デバイス – CloudSec 暗号化ヘッダーを追加し、ローカルで生成された対称暗号化キーを使用してリモート サイトへの送信時に VXLAN パケット ペイロードの暗号化を行うデバイス。
- ダウンストリーム デバイス – CloudSec 暗号化ヘッダーを解釈し、リモート サイトで生成された暗号化キーを使用して受信時に VXLAN パケットペイロードの復号化を行うデバイス。
- アップストリーム サイト – 暗号化された VXLAN パケットを発信するデータ センター ファブリック。
- ダウンストリーム サイト – 暗号化されたパケットを受信して復号するデータ センター ファブリック。
- TX キー – クリアな VXLAN パケット ペイロードを暗号化するために使用される暗号化キー。ACI では、1 つの TX キーがすべてのリモート サイトに対してアクティブであることができます。
- RX キー – 暗号化された VXLAN パケット ペイロードを復号するために使用される暗号化キー。ACI では、2 つの RX キーをリモート サイトごとにアクティブにできます。

  2 つの RX キーをキーの再生成プロセス中に同時にアクティブにすることができます。ダウンストリームサイトは、新しいキーの展開が一定期間終了した後、古い RX キーと新しい RX キーを保持し、いずれかのキーを適切に復号することで、順序どおりでないパケット配信が可能になるようにします。
- 対象キー – 同じ暗号化キーを使用して、アップストリーム デバイスとダウンストリーム デバイスによるパケットストリームの暗号化 (TX キー) と復号 (RX キー) をそれぞれ行う場合。

- キーの再生成 – 古いキーの有効期限が切れた後、すべてのダウンストリーム サイトの古いキーを新しいキーに置き換えるためにアップストリームサイトによって開始されたプロセス。
- 安全なチャネル識別子 （SCI） – サイト間のセキュリティ関連付けを表す 64 ビット識別子。CloudSecヘッダーの暗号化されたパケットで送信され、パケットの復号化のためにダウンストリームデバイスの RX キーを取得するために使用されます。
- アソシエーション番号値 （AN） – 暗号化されたパケットのCloudSecヘッダーで送信される2ビットの数値(0, 1, 2, 3)。これは、復号化のために SCI とともにダウンストリームデバイスでキーを導出するために使用されます。これにより、ダウンストリームデバイスで複数のキーをアクティブにして、キーの再生成操作の後で、同じアップストリームデバイスからの異なるキーを使用したパケットの順序どおりでない到着を処理できます。

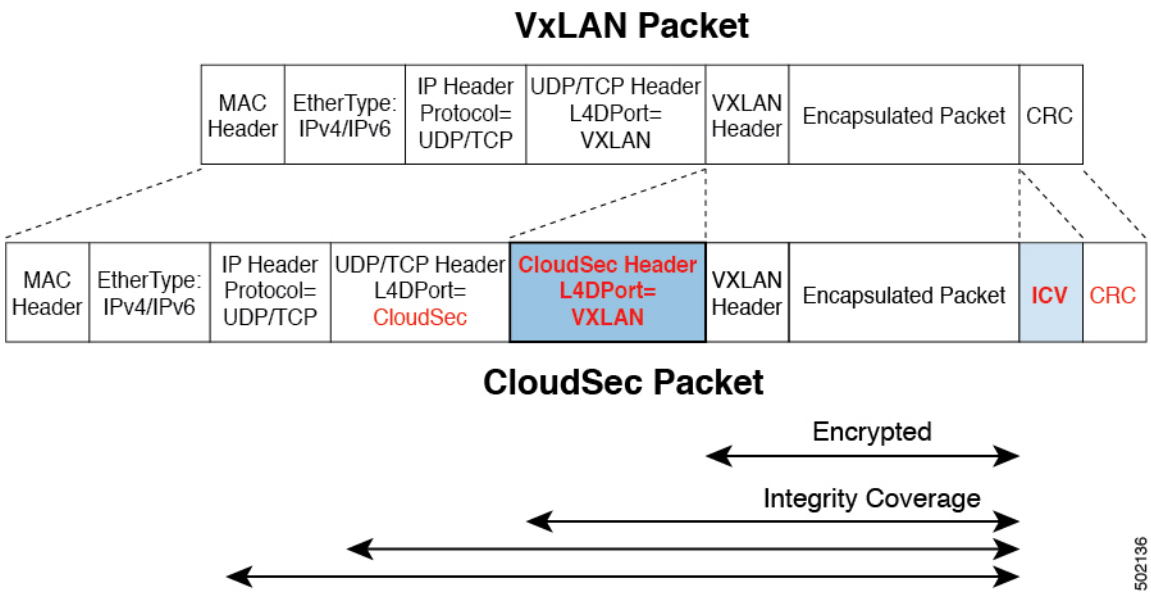
  ACI では、2 つのアクティブな RX キーには 2 つのアソシエーション番号値（0 または 1 1）のみが使用され、TX キーには常に 1 つのアソシエーション番号値（0 または 1）のみが使用されます。
- 事前共有キー （PSK） – CloudSec TX および RX キーを生成するためのランダム シードとして使用するには、Cisco APIC GUI で 1 つ以上のキーを設定する必要があります。複数の PSK が設定される場合、各キーの再生成プロセスはインデックスの順序で次の PSK を使用します。さらに高いインデックスの PSK がない場合、最下位のインデックスの PSK が使用されます。各 PSK は、64文字の長さの16進数ストリングでなければなりません。Cisco APIC は最大256の事前共有キーをサポートします。

CloudSec の暗号化と復号の処理

リリース2.0(1)以降では、データセキュリティと整合性の両方に対応する、完全に統合されたシンプルでコスト効率の高いソリューションを提供するために、Multi-Site は Multi-Site ファブリック間の送信元から宛先への完全なパケット暗号化を可能にする CloudSec 暗号化機能を提供します。

次の図は、CloudSec カプセル化の前後のパケット ダイアグラムと、その後の暗号化および復号化プロセスの説明を示しています。

図 *2 : CloudSec* パケット



パケット暗号化

次に、CloudSec が発信トラフィック パケットを処理する方法の概要を示します。

- パケットは、外部 IP ヘッダ宛先アドレス フィールドとレイヤ 4 宛先ポート情報を使用してフィルタ処理され、フィルタされたパケットは暗号化の対象としてマークされます。
- 暗号化に使用するオフセットは、パケットのフィールドに基づいて計算されます。たとえば、オフセットは、802.1q VLAN があるかどうか、またはパケットが IPv4 または IPv6 パケットであるかどうかによって異なります。

  オフセットは自動的に決定され、ユーザーには表示されません。
- 暗号キーはハードウェア テーブルでプログラムされ、パケット IP ヘッダーを使用してテーブルから検索されます。

パケットに暗号化のマークが付けられると、暗号キーがロードされ、暗号化を開始するパケットの先頭からのオフセットが判明すると、次の追加の手順が実行されます。

- UDP 宛先ポート番号は、UDP ヘッダーから CloudSec フィールドにコピーされ、パケットが暗号解読されるときにリカバリされます。
- UDP 宛先ポート番号は、CloudSec パケットであることを示すために上書きされます。

  3.7(1) より前のリリースでは、ポートは Cisco 独自のレイヤ 4 ポート番号 9999 で上書きされます。

  IANA が割り当てたポート 8017 を使用するように CloudSec を構成できるリリース 3.7(1) 以降では、使用される宛先ポート番号は、このオプションを有効にしているかどうかに応じて 9999 または 8017 のいずれかです。

- [UDP 長(UDP length)] フィールドは、追加されるバイト数を反映するように更新されます。
- CloudSec ヘッダーは、UDP ヘッダーの後に直接挿入されます。
- 整合性チェック値 (ICV) は、ペイロードと CRC の間のパケットの最後に挿入されます。
- ICV では、128 ビットの初期化ベクトルを構築する必要があります。CloudSec の場合、ICV のために送信元 MAC アドレスを使用すると、SCI ごとのプログラム可能な値に置き換えられます。
- CRC は、パケットのコンテンツの変更を反映するように更新されます。

パケットの暗号解読

CloudSec が受信パケットを処理する方法は、上記で説明した発信パケット アルゴリズムと対称的です。

- 受信したパケットが CloudSec パケットである場合は、暗号解読され、ICV が検証されます。

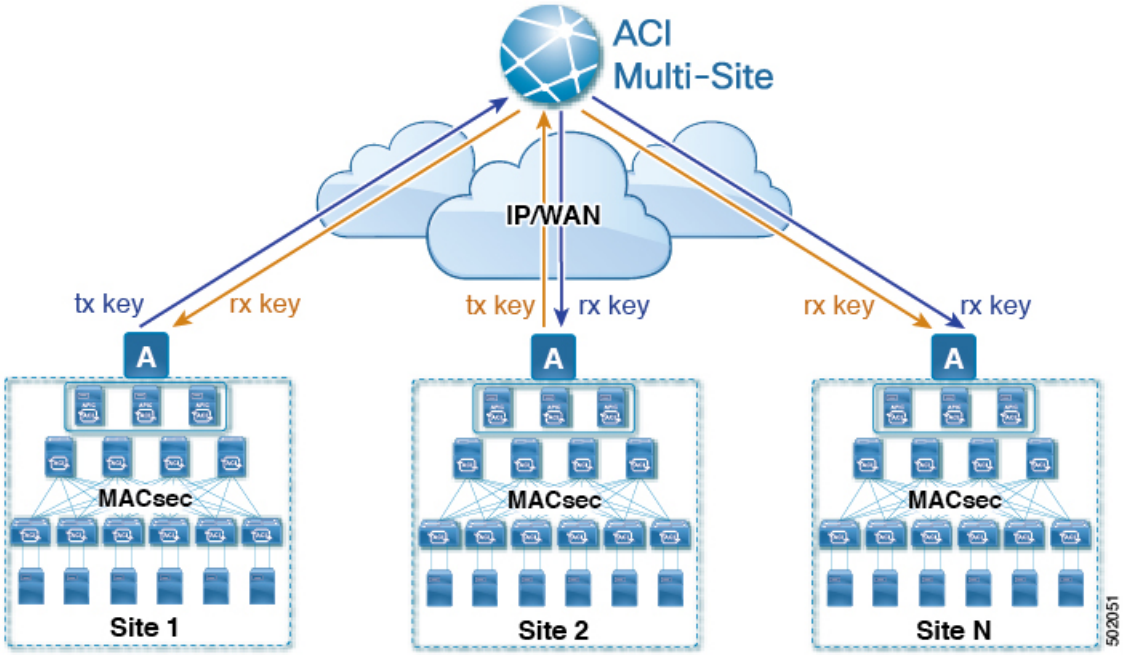
  ICV 検証に合格すると、追加フィールドが削除され、UDP 宛先ポート番号が CloudSec ヘッダーから UDP ヘッダーに移動され、CRC が更新され、パケットの暗号解読と CloudSec ヘッダーの削除後に宛先に転送されます。そうでない場合、パケットはドロップされます。

- 復号化キーは、受信した CloudSec パケットの外部 IP ヘッダーのソース アドレス フィールド、CloudSec ヘッダーの SCI、および AN 番号フィールドを使用してキー ストアから取得されます。
- パケットが CloudSec パケットでない場合、パケットはそのまま残ります。

CloudSec 暗号化キーの割り当てと配布

初期キー構成

図 *3 : CloudSec* キーの配布



次に、上記の図に示されている CloudSec 暗号キーの初期割り当ておよび配信プロセスの概要を示します。

- アップストリームサイトの Cisco APIC は、サイトから送信された VXLAN パケットのデータ暗号化に使用されるためのローカル対称キーを生成します。アップストリームサイトが暗号化に使用するのと同じキーが、ダウンストリームリモート受信サイトのパケットの復号に使用されます。

  各サイトはほかのサイトに送信するトラフィックのためのアップストリームサイトです。複数のサイトが存在する場合、各サイトは独自のサイトツーサイトキーを生成し、そのキーを暗号化に使用してからリモートサイトに送信します。

- 生成された対称キーは、ダウンストリーム リモート サイトに配布するために、アップストリーム サイトの Cisco APIC によって Nexus Dashboard Orchestrator (NDO) にプッシュされます。

- NDO はメッセージ ブローカとして機能し、生成された対称キーをアップストリーム サイトの Cisco APIC から収集し、それをダウンストリーム リモート サイトの Cisco APIC に配布します。

  キーは、キー暗号化キー (KEK) を使用して暗号化され、TLS ベースのチャネルを介して配布されます。

- 各ダウンストリーム サイトの Cisco APIC は、受信したキーを、キーを生成したアップストリームサイトからのトラフィックを受信することを目的としたローカル スパイン スイッチの RX キーとして設定します。
- 各ダウンストリーム サイトの Cisco APIC は、ローカル スパイン スイッチから RX キーの展開ステータスを収集し、NDO にプッシュします。
- NDO は、すべてのダウンストリーム リモート サイトからアップストリーム サイトの Cisco APIC に戻って、主要な展開ステータスを中継します。
- アップストリームサイトはCisco APIC 、すべてのダウンストリーム リモート サイトから受信したキー展開ステータスが成功したかどうかを確認します。
  - ダウンストリームデバイスから受信した展開ステータスが成功した場合、アップストリーム サイトはスパイン スイッチの TX キーとしてローカル対称キーを展開し、ダウンストリーム サイトに送信される VXLAN パケットの暗号化を有効にします。
  - ダウンストリームデバイスから受け取った展開ステータスが失敗した場合、失敗した Cisco APIC サイトで障害が発生し、NDO で構成された「セキュア モード」設定に基づいて処理されます。「セキュアが必須 (must secure)」モードでは、パケットはドロップされ、「セキュアであるべき (should secure)」モードでは、パケットは宛先サイトに平文 (暗号化されていない) で送信されます。

（注） 現在のリリースでは、モードは常に「セキュアであるべき (should secure)」に設定されており、変更できません。

キー再生成プロセス

生成された各 TX / RX キーは、設定された時間が経過すると有効期限が切れます。デフォルトでは、キーの有効期限は 15 分に設定されています。TX/RX キーの初期セットが期限切れになると、キー再生成プロセスが行われます。

キーの再割り当てプロセスには、同じ一般的なキーの割り当てと配布フローが適用されます。キー再生成プロセスは「ブレーク前に作成 (make before break)」ルールに従います。つまり、新しい TX キーがアップストリーム サイトに展開される前に、ダウンストリーム サイトのすべての RX キーが展開されます。これを実現するために、アップストリーム サイトは、ローカル アップストリーム サイトのデバイスに新しい TX キーを構成する前に、ダウンストリーム サイトからの新しい RX キーの展開ステータスを待ちます。

ダウンストリーム サイトが新しい RX キーの展開で障害ステータスを報告した場合、キー再生成プロセスは終了し、古いキーはアクティブなままになります。ダウンストリームサイトは、新しいキーの展開が一定期間終了した後、古い RX キーと新しい RX キーを保持し、いずれかのキーを適切に復号することで、順序どおりでないパケット配信が可能になるようにします。

（注） スパイン スイッチのメンテナンス中のキー再生成プロセスに関しては、特別な注意が必要です。詳細については、スパイン スイッチ メンテナンス中のキー再生成プロセス （18 ページ）を参照してください。

キー再生成プロセスの失敗

ダウンストリーム サイトがキー再生成プロセスによって生成された新しい暗号化キーの展開に失敗した場合、新しいキーは破棄され、アップストリーム デバイスは以前の有効なキーを TX キーとして引き続き使用します。このアプローチにより、アップストリーム サイトは、ダウンストリーム サイトのセットごとに複数の TX キーを維持する必要がなくなります。ただし、このアプローチでは、いずれかのダウンストリーム サイトでキー再生成の展開エラーが発生し続ける場合、キー更新プロセスが遅延する可能性もあります。マルチサイト管理者は、キー再生成を成功させるために、キーの展開の失敗の問題を修正するための行動を取ることが期待されています。

Cisco APICキー管理のロール

Cisco APIC は、キー割り当て(初期キーとキー再配布の両方)、スパイン スイッチからのキー展開ステータス メッセージの収集、および他のサイトへの配布のための各キーのステータスに関する Nexus Dashboard Orchestrator への通知に責任をもちます。

キー管理における Nexus Dashboard Orchestrator の役割

Nexus Dashboard Orchestrator は、アップストリーム サイトから TX キー（初期キーと後続のキーの再生成の両方）を収集し、RX キーとして展開するためにすべてのダウンストリーム サイトに配布します。NDO はまた、ダウンストリーム サイトから RX キーの展開ステータス情報を収集し、成功した RX キー展開ステータスで TX キーを更新するために、アップストリーム サイトに通知します。

アップストリーム モデル

MPLS など、ダウンストリーム キー割り当てを使用する他のテクノロジーとは対照的に、CloudSec のアップストリーム モデルには次の利点があります。

- このモデルはシンプルで、運用とネットワークへの導入が容易です。
- モデルは、マルチサイトのユース ケースに適しています。
- 複数の宛先サイトに送信される複製パケットの各コピーに同じキーと CloudSec ヘッダーを使用できるため、マルチキャスト トラフィックに利点があります。ダウンストリーム モデルでは、各コピーは暗号化中にサイトごとに異なるセキュリティ キーを使用する必要があります。
- 障害が発生した場合のトラブルシューティングが容易になり、複製されたユニキャスト パケットとマルチキャスト パケットの両方に対して、送信元から宛先へのパケットのトレーサビリティが一貫して向上します。

CloudSec 暗号化のための Cisco APIC の設定

CloudSec 暗号と復号キーを生成するために、Cisco APIC で使用する 1 個以上の事前共有キー（PSK）を構成する必要があります。PSK は再キー プロセス中のランダム シードとして使用されます。複数の PSK が設定される場合、各再キープロセスはインデックスの順序で次の PSK を使用します。さらに高いインデックスの PSK がない場合、最下位のインデックスの PSK が使用されます。

暗号キーの生成に対するシードとして PSK が使用されるため、複数の PSK の設定では生成された暗号キーの長時間にわたる脆弱性を下げることにより、追加のセキュリティを提供します。

（注） Cisco APIC で事前共有キーが構成されていない場合、CloudSec はそのサイトに対して有効にはなりません。その場合、マルチサイトで CloudSec 設定をオンにすると、障害が生じます。

いつでも新しい PSK で前に追加した PSK を更新したい場合、新しいキーを追加するときと同様の手順を繰り返すだけですが、インデックスは既存のものを指定してください。

1 つ以上の事前共有キーを次の 3 通りの方法のいずれかを使用して設定できます。

- GUI を使用した CloudSec 暗号化の Cisco APIC の設定 （12 ページ） で説明されている Cisco APIC GUI の使用
- NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定 （13 ページ） で説明されている Cisco APIC NX-OS スタイルの CLI の使用
- REST API を使用した CloudSec 暗号化の Cisco APIC の設定 （14 ページ）で説明されている Cisco APIC REST API の使用

GUI を使用した CloudSec 暗号化の Cisco APIC の設定

このセクションは、Cisco APIC GUI を使用して 1 つ以上の事前共有キー (PSK) を設定する方法について説明します。

ステップ 1 APIC にログインします。

ステップ 2 **[テナント]** > **[インフラ]** > **[ポリシー]** > **[CloudSec 暗号化]**に移動します。

ステップ 3 **SA キーの有効期限**を指定します。

このオプションは、各キーが有効な時間(分)を指定します。それぞれの生成された TX/RX キーは、再キープロセスをトリガした後指定の時間で期限切れになります。期限の時間は、5～1440 分の範囲で入力できます。

ステップ 4 **[事前共有キー]**テーブルの + アイコンをクリックします。

ステップ 5 追加する事前共有キーの**インデックス**を指定し、その後、**事前共有**キー自体を指定します。

[インデックス (Index)] フィールドは、事前共有キーを使用する順序を指定します。最後 (最高位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大256個の事前共有キーをサポートするので、PSKインデックスチは1～256でなければなりません。

各**事前共有キー**は、64 文字の 16 進数文字列である必要があります。

NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定

このセクションでは、 Cisco APIC NX OS Style CLI を使用して1つ以上の事前共有キー (PSK) を設定する方法について説明します。

ステップ 1 Cisco APIC NX-OS style CLI にログインします。

ステップ 2 コンフィギュレーション モードを入力します。

例：

```
apic1# configure
apic1 (config)#
```

ステップ 3 デフォルト CloudSec プロファイルのコンフィグレーション モードを入力します。

例：

```
apic1(config)# template cloudsec default
apic1(config-cloudsec)#
```

ステップ 4 事前共有キー (PSK) の有効期限を指定します。

このオプションは、各キーが有効な時間 (分) を指定します。それぞれの生成された TX/RX キーは、再キープロセスをトリガした後指定の時間で期限切れになります。期限の時間は、5～1440 分の範囲で入力できます。

例：

```
apic1(config-cloudsec)# sakexpirytime <duration>
```

ステップ 5 1 つまたは複数の事前共有キーを指定します。

次のコマンドでは、設定している PSK のインデックスと PSK 文字列自体を指定します。

例：

```
apic1(config-cloudsec)# pskindex <psk-index>
apic1(config-cloudsec)# pskstring <psk-string>
```

<*psk-index*> パラメータは、事前共有キーが使用される順序を指定します。最後 (最上位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大 256 個の事前共有キーをサポートするので、PSK インデックスチは 1 ～ 256 でなければなりません。

<*psk-string*>パラメータは、実際の PSK を指定します。これは、64 文字の 16 進数文字列である必要があります。

ステップ 6 (オプション) 現在の PSK 設定を表示します。

現在設定されている PSK の数とその期間を表示するには、次のコマンドを使用します。

例：

```
apic1(config-cloudsec)# show cloudsec summary
```

REST API を使用した CloudSec 暗号化の Cisco APIC の設定

このセクションは、Cisco APIC REST API を使用して 1 つ以上の事前共有キー (PSK) を設定する方法について説明します。

PSK 有効期限、インデックス、文字列を設定します。

次の XML POST で、次を置換します。

- 各 PSK の期限をもつ **sakExpiryTime** の値。

  この **sakExpiryTime** パラメータは各キーが有効な時間 (分) を指定します。それぞれの生成された TX/RX キーは、再キー プロセスをトリガした後指定の時間で期限切れになります。期限の時間は、5 ～1440 分の範囲で入力できます。

- 設定している PSK のインデックスをもつ **インデックス** の値。

  インデックス パラメータは、事前共有キーが使用される順序を指定します。最後 (最高位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大 256 個の事前共有キーをサポートするので、PSK インデックスチは 1 ～ 256 でなければなりません。

- 設定している PSK のインデックスをもつ **pskString** の値。

  pskString パラメータは実際の PSK を指定します。これは 16 進文字列で長さ 64 文字でなければなりません。

例：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">

    <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "false" status=""
 >
        <cloudsecPreSharedKey index="1"
pskString="1234567812345678123456781234567812345678123456781234567812345678" status=""/>
    </cloudsecIfPol>
</fvTenant>
```

Cisco Nexus Dashboard Orchestrator 内の CloudSec 暗号の有効化

CloudSec 暗号化は、サイトごとに個別に有効または無効にすることができます。ただし、2 つのサイト間の通信は、この機能が両方のサイトで有効になっている場合にのみ暗号化されます。

始める前に

2 つ以上のサイト間で CloudSec 暗号化を有効にする前に、次のタスクを完了しておく必要があります。

- 『*Cisco APIC* のインストール、アップグレード、ダウングレード ガイド』で説明されているように、複数のサイトに Cisco APIC クラスタをインストールして設定します。
- 『*Cisco Nexus Dashboard Orchestrator* インストレーションおよびアップグレード ガイド』の説明に従って、Cisco Nexus Dashboard Orchestrator をインストールし、構成します。
- 『*Cisco ACI* マルチサイト構成ガイド』の説明に従って、各 Cisco APIC サイトを Cisco Nexus Dashboard Orchestrator に追加します。

ステップ 1 Cisco Nexus Dashboard Orchestrator にログインします。

ステップ 2 左のナビゲーション メニューから、**[構成（Config）] > [サイト間接続（Site To Site Connectivity）]**を選択します。

ステップ 3 メイン ウィンドウの右上にある **[構成（Configure）]** ボタンをクリックします。

ステップ 4 （オプション）[一般設定（General Settings）] ページの [コントロール プレーンの構成（Control Plane Configuration）] タブで、[IANA 予約済み UDP ポート（IANA Reserved UDP Port）] オプションを有効にします。

デフォルトでは、CloudSec は独自の UDP ポートを使用します。このオプションを使用すると、サイト間の CloudSec 暗号化に公式の IANA 予約ポート 8017 を使用するように CloudSec を構成できます。

（注） IANA 予約ポートは、リリース 5.2(4) 以降を実行している Cisco APIC サイトでサポートされています。

この設定を変更するには、すべてのサイトで CloudSec を無効にする必要があります。IANA 予約ポートを有効にしたいが、すでに 1 つ以上のサイトで CloudSec 暗号化を有効にしている場合は、すべてのサイトで CloudSec を無効にし、**[IANA 予約 UDP ポート（IANA Reserve UDP Port）]** オプションを有効にしてから、必要なサイトで CloudSec を再度有効にします。

ステップ 5 左のサイドバーから、CloudSec 構成を変更するサイトを選択します。

ステップ 6 右のサイドバーで、**[Cloudsec 暗号化（Cloudsec encryption）]** 設定を切り替えて、サイトの CloudSec 暗号化機能を有効または無効にします。

スイッチでの CloudSec 構成の確認

次のコマンドを使用すると、Nexus Dashboard Orchestrator から CloudSec 暗号化を有効にした後、スパイン スイッチに展開された現在の CloudSec 構成を確認できます。

ステップ 1 スパイン スイッチにログインします。

ステップ 2 `show cloudsec sa interface all` コマンドを実行して、CloudSec 構成を表示します。

次の出力で、各インターフェイスについて次のことを確認します。

- [動作ステータス（Operational Status）] の値は UP を示します。
- [制御（Control）] 値は、CloudSec 暗号化に現在使用されている UDP ポートを示すため、すべての CloudSec 対応サイトのすべてのインターフェイスで同じです。

  次の例は、デフォルトのシスコ独自の UDP ポート（deprecatedUdpPort）を示しています。IANA が割り当てたポート 8017 を使用するように CloudSec を構成すると、**[制御（Control）]** フィールドには代わりに ianaUdpPort が表示されます。

```
spine1# show cloudsec sa interface all
================================================================================
Interface: Eth1/49.49(0x1a030031) Physical Interface: Eth1/49(0x1a030000)
    Operational Status: UP Retry: Off Control: deprecatedUdpPort
--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.204.0/24 Type: ext-routable-tep-pool Operational Status: UP
    Pod-Id: 1
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 0 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.520-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs
--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.202.1/32 Type: msite-unicast-tep Operational Status: UP
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 2 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.563-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs
    RX Key: ******************************** Assoc Num: 1 Sci: 0x20001
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
       Hardware Index: 3 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.442-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs
    RX Key: ******************************** Assoc Num: 0 Sci: 0x20001
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
       Hardware Index: 2 Operational Status: UP Control: NONE
       Last Updated: PST 2022-01-11 23:26:37.453-08:00 Retry: Off
       Uptime: 11 hours 30 mins 45 secs

--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.201.1/32 Type: msite-multicast-tep Operational Status: UP
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
       Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
```

```
        Hardware Index: 1 Operational Status: UP Control: NONE
        Last Updated: PST 2022-01-11 23:26:37.549-08:00 Retry: Off
        Uptime: 11 hours 30 mins 45 secs
    RX Key: ******************************** Assoc Num: 1 Sci: 0x20001
        Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
        Hardware Index: 1 Operational Status: UP Control: NONE
        Last Updated: PST 2022-01-11 23:26:36.501-08:00 Retry: Off
        Uptime: 11 hours 30 mins 46 secs
    RX Key: ******************************** Assoc Num: 0 Sci: 0x20001
        Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
        Hardware Index: 0 Operational Status: UP Control: NONE
        Last Updated: PST 2022-01-11 23:26:37.495-08:00 Retry: Off
        Uptime: 11 hours 30 mins 45 secs

================================================================================
Interface: Eth1/50.50(0x1a031032) Physical Interface: Eth1/50(0x1a031000)
    Operational Status: UP Retry: Off Control: deprecatedUdpPort
--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.204.0/24 Type: ext-routable-tep-pool Operational Status: UP
    Pod-Id: 1
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
        Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
        Hardware Index: 1 Operational Status: UP Control: NONE
        Last Updated: PST 2022-01-11 23:26:37.577-08:00 Retry: Off
        Uptime: 11 hours 30 mins 45 secs
--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.201.1/32 Type: msite-multicast-tep Operational Status: UP
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
        Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
        Hardware Index: 0 Operational Status: UP Control: NONE
        Last Updated: PST 2022-01-11 23:26:37.537-08:00 Retry: Off
        Uptime: 11 hours 30 mins 45 secs
    RX Key: ******************************** Assoc Num: 1 Sci: 0x20001
        Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
        Hardware Index: 1 Operational Status: UP Control: NONE
        Last Updated: PST 2022-01-11 23:26:36.463-08:00 Retry: Off
        Uptime: 11 hours 30 mins 46 secs
    RX Key: ******************************** Assoc Num: 0 Sci: 0x20001
        Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
        Hardware Index: 0 Operational Status: UP Control: NONE
        Last Updated: PST 2022-01-11 23:26:37.416-08:00 Retry: Off
        Uptime: 11 hours 30 mins 45 secs

--------------------------------------------------------------------------------
Site-Id: 2 Peer: 200.200.202.1/32 Type: msite-unicast-tep Operational Status: UP
--------------------------------------------------------------------------------
    TX Key: ******************************** Assoc Num: 1 Sci: 0x10002
        Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
        Hardware Index: 2 Operational Status: UP Control: NONE
        Last Updated: PST 2022-01-11 23:26:37.593-08:00 Retry: Off
        Uptime: 11 hours 30 mins 45 secs
    RX Key: ******************************** Assoc Num: 0 Sci: 0x20001
        Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6827 Oper Rekey Num: 6827
        Hardware Index: 2 Operational Status: UP Control: NONE
        Last Updated: PST 2022-01-11 23:26:37.481-08:00 Retry: Off
        Uptime: 11 hours 30 mins 45 secs
    RX Key: ******************************** Assoc Num: 1 Sci: 0x20001
        Cipher Suite: gcm-aes-xpn-256 Rekey Num: 6826 Oper Rekey Num: 6826
        Hardware Index: 3 Operational Status: UP Control: NONE
```

```
Last Updated: PST 2022-01-11 23:26:37.507-08:00 Retry: Off
Uptime: 11 hours 30 mins 45 secs
```

スパインスイッチメンテナンス中のキー再生成プロセス

次に、この機能が有効になっているスパイン スイッチの一般的なメンテナンス シナリオでの CloudSec キー再生成プロセスの概要を示します。

- **通常の解放**: CloudSec 対応スパイン スイッチがデコミッションされると、 CloudSec キー再生成プロセスが自動的に停止します。解放されたノードが再起動されるか、解放されたノードIDが次から削除されるまで、キー再生成プロセスは再度開始されません:Cisco APIC
- **スパイン スイッチのソフトウェア アップグレード**: スパイン スイッチがソフトウェアのアップグレードによりリロードされると、CloudSec キー再生成プロセスは自動的に停止します。キー再生成プロセスは、スパイン スイッチのリロードが完了すると、再開されます。
- **メンテナンス (GIR モード)** : CloudSec キー再生成プロセスは、NX-OS Style CLI を使用してキーの再生成プロセスを無効にして再度有効にする （18 ページ）に記載されている手順を使用して、手動で停止する必要があります。キー再生成は、ノードがトラフィックを転送する準備が再度整った後にのみ、有効にできます。
- **Cisco APICからの解放と削除** : CloudSec キー再生成プロセスは、NX-OS Style CLI を使用してキーの再生成プロセスを無効にして再度有効にする （18 ページ） に記載されている手順を使用して、手動で停止する必要があります。キー再生成は、Cisco APICからノードが削除された後にのみ有効にできます。

NX-OS Style CLI を使用してキーの再生成プロセスを無効にして再度有効にする

キーの再生成プロセスを手動で停止し再開することが可能です。特定の状況でキーの再生成プロセスを手動で管理することが必要な場合があります。たとえば、でコミッションとメンテナンスの切り替えなどです。このセクションは、 Cisco APIC NX-OS Style CLI を使用して設定を切り替える方法を説明します。

ステップ 1 Cisco APIC NX-OS style CLI にログインします。

ステップ 2 コンフィギュレーション モードを入力します。

例：

```
apic1# configure
apic1(config)#
```

ステップ 3 デフォルト CloudSec プロファイルのコンフィグレーション モードを入力します。

例：

```
apic1(config)# template cloudsec default
apic1(config-cloudsec)#
```

ステップ 4 キーの再生成プロセスを停止するか、再開します。

キーの再生成を停止するには:

例：

```
apic1(config-cloudsec)# stoprekey yes
```

キーの再生成プロセスを再開するには:

例：

```
apic1(config-cloudsec)# stoprekey no
```

REST API を使用したキー再生成プロセスの無効化と再有効化

キーの再生成プロセスを手動で停止し再開することが可能です。特定の状況でキーの再生成プロセスを手動で管理することが必要な場合があります。たとえば、でコミッションとメンテナンスの切り替えなどです。このセクションでは、Cisco APICREST API を使用して設定を切り替える方法について説明します。

ステップ 1 キー再生成プロセスは、次のXML メッセージを使用して無効にすることができます。

例：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">

    <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "true" status=""
 />
</fvTenant>
```

ステップ 2 キー再生成プロセスは、次のXML メッセージを使用して有効にすることができます。

例：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">

    <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "false" status=""
 />
</fvTenant>
```

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。