SIP シグナリング暗号化

SIP シグナリング暗号化は、すべての SIP メッセージを発信側から着信側のドメインに送信するセキュアな暗号化転送を提供します。これにより、要求は着信側に安全に送信されます。SBC は、SIP シグナリング暗号化に対して次のサポートを提供します。

- セキュリティ保護された SIP コールは SBC を通過できます。
- SIP 隣接は、セキュリティ保護されていないとして設定することも、非暗号化関連メカニズム（単一の信頼できる物理層リンク、または信頼できるネットワークとのインターフェイスなど）によってセキュリティ保護されているとして設定することも、暗号化によってセキュリティ保護されているとして設定することもできます。
- 暗号化がサポートされていないときにリモート ピアが暗号化を使用しようとすると、インバウンド接続およびアウトバウンド接続はすぐに閉じられます。
- 暗号化が必要なときにリモート ピアが暗号化を使用しない場合、インバウンド接続およびアウトバウンド接続はすぐに閉じられます。
- 該当する show コマンドを使用することにより、特定の SIP 隣接に対して設定されたセキュリティ サポートのレベルを表示できます。
- 信頼できない隣接で受信したコールは、安全に暗号化された発信隣接でルーティングされないことがあります。
- 暗号化によってセキュリティ保護された隣接は、デフォルトでは、ポート 5061 で受信します。このポートは、異なる値に設定される場合があります。
- リモート ピアにより提供される証明書内の Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）は、要求を送信したドメインと照らし合わせてチェックされます。この 2 つが一致しない場合、信号は廃棄されます。

SIP シグナリング暗号化の機能履歴

リリース	変更内容
リリース 3.4.1	この機能は、Cisco XR 12000 シリーズ ルータで導入されました。
リリース 3.5.0	変更なし。

内容

このモジュールの構成は次のとおりです。

- 「SIP シグナリング暗号化の実装の前提条件」（P.212）
- 「SIP シグナリング暗号化の実装の制約事項」（P.212）

- 「SIP シグナリング暗号化に関する情報」（P.213）
- 「SIP シグナリング暗号化の設定方法」（P.214）
- 「隣接に対して設定されているセキュリティ レベルを表示する show コマンドの例」（P.216）
- 「その他の関連資料」（P.216）

SIP シグナリング暗号化の実装の前提条件

次に、SIP シグナリング暗号化を実装するための前提条件を示します。

- SIP シグナリング暗号化機能には、セキュリティ パッケージが必要です。
- ストア認証は、CEPKI インフラストラクチャにより生成されます。

SIP シグナリング暗号化の実装の制約事項

SIP シグナリング暗号化には、次の制約事項が適用されます。

- 隣接が接続されている間は、SIP 隣接のセキュリティ ポリシーを変更することはできません。
- SBC で唯一必要な暗号化サポートは、Secure Sockets Layer（SSL）over Transport Layer Security（TLS）です。IPSec および SCTP 暗号化はサポートされません。
- SIP TLS コールの場合は、k9sec.pie をインストールしてからルータ証明書を設定し、その後で SBC を設定する必要があります。このプロセスに従わない場合、SBC は TLS コールを拒否します。
- 証明書を生成、保存、または維持するには、SBC は不要です。この機能は CEPKI インフラストラクチャにより行われます。
- 暗号化された隣接は、暗号化されていないトラフィックを受け入れません。
- 暗号化されていない隣接は、暗号化されたトラフィックを受け入れません。
- SBC は、3xx リダイレクションまたはターゲットリフレッシュの結果として、セキュアな要求をセキュアでないターゲットにリダイレクトしたり、その逆を行ったりすることはありません。たとえば、SIPS Uniform Resource Identifier（URI）宛てのコールを SIP URI にリダイレクトすることはできません。これが試行された場合は、コールを終了させるために、負の INVITE 応答が返されるか、BYE が両者に送信されます。
- エンドポイントは、SIPS 通信アドレスを提供しない限り、SIPS address-of-record の登録が許可されません。
- セキュリティ保護されていない隣接からセキュリティ保護されている隣接へのコールは許可されません。
- SBC には、信頼できるネットワーク エレメントによるコールのセキュリティ ダウングレードを禁止する機能はありません。発信コールがセキュアな隣接からプロキシに送信され、プロキシがこのコールをセキュアでないターゲットにリダイレクトしてからコールを SBC に返した場合は、SBC は、このコールを信頼できない隣接から新しいターゲットに転送することができます。SBC はプロキシとセキュアに接続しているため、プロキシのルーティングの決定を信頼します。この例の 2 つのコール レッグは、SBC から見ると別々のコールであるため、SBC は着信コール レッグがセキュリティ保護されていたことを認識しません。

SIP シグナリング暗号化に関する情報

コールをルーティングまたは拒否するときに使用される 2 つの主要なセキュリティ上のポイントは、次のとおりです。

- SIPS URI へのコールは、セキュアである必要があります。SIP URI へのコールは、セキュアである必要はありません。
- 信頼できる隣接で受信された信号は、セキュアであると見なされます。信頼できない隣接で受信された信号は、セキュアでないと見なされます。

隣接でのセキュリティ設定

次の 3 つのオプションを使用して、SIP 隣接でのクライアントおよびサーバのセキュリティ サポートを個別に設定できます。

- **Untrusted**：この隣接はいかなる手段によってもセキュリティ保護されていません。この隣接からはセキュアでないコール（SIPS URI 宛てではないコール）だけが発信できます。
- **Trusted-Encrypted**：この隣接では、セキュリティを保証するためにシグナリング暗号化が使用されます。暗号化には、ルータのデフォルトの証明書とキーが使用されます。この隣接からはセキュアなコール（SIPS URI へのコール）だけが発信できます。
- **Trusted-Unencrypted**：この隣接でのすべてのメッセージにセキュアなシグナリングを保証するために、SIP 以外のメカニズムが使用されます。このメカニズムの例としては、単一の信頼できる物理リンクがあります。この隣接からは、セキュアなコールもセキュアでないコールも発信されます。この設定により、暗号化をサポートしていないエンドポイントがセキュアな SIP コールに参加できます。

ユーザ エージェント サーバ（UAS）側の処理

インバウンド要求は、2 つの点に基づいてマーキングされます。発信側が信頼できるかどうか、およびコールのターゲットがセキュアかどうかです。

発信側の信頼性は、次のように決定されます。

- 信頼できる隣接から着信した SIP 要求は、信頼できる要求としてマーキングされます。
- 信頼できない隣接から着信した SIP 要求は、信頼できない要求としてマーキングされます。

望ましいターゲットのセキュリティは、次のように決定されます。

- SIPS URI への要求は、アウトバウンド セキュリティを必要とする要求としてマーキングされます。
- SIP URI への要求は、アウトバウンド セキュリティを必要としない要求としてマーキングされます。

発信側が信頼できず、ターゲットがセキュリティを必要とする場合、インバウンド要求は拒否されます。その他の組み合わせは、いずれもルーティング処理に転送されます。

ルーティング処理

ルーティング ポリシー システム（RPS）ポリシーによって、要求の次のルーティング先が決定します。デフォルトの動作は次のとおりです。

- コールがアウトバウンド セキュリティを必要とする場合、RPS は信頼できる（trusted）発信隣接だけを考慮します。
- コールがアウトバウンド セキュリティを必要としない場合、RPS は信頼できない（untrusted）発信隣接、または信頼できる暗号化されていない（trusted-unencrypted）発信隣接だけを考慮します。

RPS がコールに適切な発信隣接を見つけることができない場合、コールは拒否されます。

ユーザ エージェント クライアント（UAC）側の処理

発信隣接では、当初の要求の URI スキームを保存し、コールの当初のターゲットが SIPS URI であった場合、コールが SIPS URI に送信されるように保証します。また、コールの当初のターゲットが SIP URI であった場合、コールは SIP URI に送信されます。

3xx クラスの応答およびターゲットリフレッシュの指示を受信すると、通信設定が検査されます。信頼できない隣接では、コールのターゲットは、SIPS ターゲットに再ルーティングできません。同様に、信頼できる隣接では、コールのターゲットは、SIP ターゲットに再ルーティングできません。リモートピアがこれを試みた場合、コールは拒否されます。

SIP シグナリング暗号化の設定方法

ここでは、SIP シグナリング暗号化の設定手順を示します。

SIP シグナリング暗号化の設定

手順の概要

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **adjacency sip** *adjacency-name*
5. **security** *type*
6. **commit**
7. **exit**
8. **show services sbc** *service-name* **sbe adjacencies**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/0/CPU0:router# configure`	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	**sbc** *service-name* **例：** `RP/0/0/CPU0:router(config)# sbc mysbc`	SBC サービスのモードを開始します。 • *service-name* 引数を使用して、サービスの名前を定義します。
ステップ 3	**sbe** **例：** `RP/0/0/CPU0:router(config-sbc)# sbe`	SBC の Signaling Border Element（SBE）機能のモードを開始します。
ステップ 4	**adjacency sip** *adjacency-name* **例：** `RP/0/0/CPU0:router(config-sbc-sbe)# adjacency sip test`	SBE SIP 隣接のモードを開始します。 • *adjacency-name* 引数を使用して、サービスの名前を定義します。
ステップ 5	**security** *type* **例：** `RP/0/0/CPU:router(config-sbc-sbe-adj-sip)# security trusted-encrypted`	この隣接でトランスポート レベルのセキュリティをどのように実装するかを詳細に設定します。このコマンドの no 形式を使用すると、この隣接がセキュリティ保護されなくなります。このフィールドは、隣接が接続されていない場合にのみ変更できます。 *type* に指定できる値は、次のとおりです。 • untrusted：隣接はセキュリティ保護されません。 • trusted-encrypted：隣接は暗号化によりセキュリティ保護されます。 • trusted-unencrypted：隣接は、他の方法（たとえば、単一専用物理リンク）によりセキュリティ保護されていると見なされます。
ステップ 6	**commit** **例：** `RP/0/0/CPU0:router(config-sbc-sbe-adj-sip)# commit`	設定変更を保存します。実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。
ステップ 7	**exit** **例：** `RP/0/0/CPU0:router(config-sbc-sbe-adj-sip)# exit`	SIP モードを終了して SBE モードに戻ります。**exit** コマンドを繰り返し入力して各モードを終了します。
ステップ 8	**show services sbc** *service-name* **sbe adjacencies** **例：** `RP/0/0/CPU0:router# show services sbc mysbc sbe adjacencies`	すべての隣接で設定されているセキュリティ サポートのレベルを表示します。

隣接に対して設定されているセキュリティレベルを表示する show コマンドの例

```
# show services sbc sbe adjacencies
SBC Service "TestSBC"
  Adjacency SipA (SIP)
    Status:               Attached
    Signaling address:    10.1.0.2:5060
    Signaling-peer:       1.2.3.4
    Account:              ISP123
    Security:             Trusted-Encrypted
```

その他の関連資料

次の各項では、SBC での SIP シグナリング暗号化に関連する参考資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS XR マスター コマンド リファレンス	*『Cisco IOS XR Master Commands List』*
Cisco IOS XR SBC インターフェイス コンフィギュレーション コマンド	*『Cisco IOS XR Session Border Controller Command Reference』*
Cisco IOS XR ソフトウェアを使用するルータを初回に起動し設定するための情報	*『Cisco IOS XR Getting Started Guide』*
Cisco IOS XR コマンド モード	*『Cisco IOS XR Command Mode Reference』*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB の場所を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用して、[Cisco Access Products] メニューからプラットフォームを選択します。 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

RFC	タイトル
RFC 3261	*『SIP: Session Initiation Protocol』*
RFC 2543	*『Session Initiation Protocol』*

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html