SIP 着信認証

SBC は、着信 SIP 要求の認証確認のために、SIP 着信認証の 2 つのモード（ローカル モードとリモート モード）をサポートしています RADIUS サーバのサポート レベルに従って、SBC を設定するための認証モードを選択する必要があります。RADIUS サーバが draft-sterman-aaa-sip-00 to 01 だけに準拠している場合、ローカル モードを選択します。RADIUS サーバが RFC 4590 だけに準拠している場合、リモート認証モードを使用します。

（注） この機能は任意であり、着信要求の認証確認を行わないように SBC を設定できます。

SIP 着信認証機能の機能履歴

リリース	変更内容
リリース 3.5.1	この機能は、Cisco XR 12000 シリーズ ルータで導入されました。

内容

このモジュールの構成は次のとおりです。

SIP 着信認証の実装の前提条件

SIP 着信認証を実装するための前提条件を示します。

- 着信コールを認証するように SBC を設定する前に、目的の認証モードで SIP 隣接を設定します。
- RADIUS サーバを設定して、選択する着信認証のモードを指定します。

SIP 着信認証の実装に関する制約事項

次に、SIP 着信認証の実装に適用される制約事項および制約事項を示します。

- SBC は、隣接ごとに 1 つの着信認証レルムだけをサポートします。
- SBC は、RADIUS サーバが生成するナンスの有効性を確認しません。この確認を実行するように RADIUS サーバを設定する必要があります。
- SBC は、着信認証用に特定の RADIUS サーバ グループを隣接に指定しません。
- 着信認証、発信認証、および TLS 接続間でコールの信頼転移が発生しないため、着信認証が正常に完了しても、SBC がコールをセキュアなものとしてマーキングすることはなく、発信認証も実装されません。ただし、ユーザは同じ隣接に着信認証、発信認証、および TLS を個別に設定できます。

SIP 着信認証について

ローカル着信認証

ローカル着信認証を実行するように設定した場合、SBC はまずリモート ピアからの不正な要求の認証確認を行います。そのため、リモート ピアからの要求に対してチャレンジを行うには、隣接での認証レルムの設定が完了している必要があります。リモート ピアが要求を確認した後、要求は RADIUS サーバに転送され、コールを通過させるかどうかがここで決定されます。

リモート着信認証

リモートの着信認証を実行するように設定した場合、SBC は RADIUS サーバを利用して、リモート ピアからの正規の要求の認証確認を行います。SBC は、RADIUS サーバが生成した認証確認要求をリモート ピアに転送し、さらにリモート ピアの認証要求を RADIUS サーバに転送します。

発信認証との相互関係

隣接に着信認証が設定されている場合に、インバウンド要求が正常認証されると、その隣接のレルムと一致する許可（Authorization）ヘッダーが除去され、アウトバウンド信号に伝搬されません。ただし、他のレルムの許可ヘッダーはアウトバウンド要求にパススルーされます。

着信認証の障害モード

着信認証が設定されている場合、（標準の SIP 信号障害モードの他に）次の障害モードが発生することがあります。

受け入れ不能なパラメータ

エンドポイントまたは RADIUS サーバが **auth** または **auth-int** 以外の保護品質に関するパラメータを指定した場合、インバウンド要求は拒否され、403 応答が生成されます。また、MD5 および MD5-sess 以外のアルゴリズムが使用されている場合、SBC は 403 応答を生成します。

アクセス要求の拒否

RADIUS サーバが Access-Reject 応答で Access-Request 信号を拒否した場合、SBC は 403 応答をエンドポイントに送信します。

メモリ不足

SBC に着信認証要求を処理するのに十分なメモリが搭載されていない場合、要求は拒否され、503 応答が送信されます。

認証レルムの不一致

隣接の設定に含まれる認証レルムを指定する認証ヘッダーをピアが返さない場合、SBC は認証要求を拒否し、403 応答を送信します。

ナンスの不一致

ピアのナンスが SBC の生成するナンスに一致しない場合、SBC は認証要求を拒否し、403 応答を送信します。

ナンスのタイムアウト

ピアのナンスがタイムアウトした場合、SBC は 401 応答および新しいナンスを送信して、ナンスの認証確認を行います。

受け入れ可能な RADIUS サーバの不在

隣接に設定されたモードをサポートする RADIUS サーバがない場合、SBC は 501 応答で認証要求を拒否し、設定に一貫性がないことをユーザに警告するログを作成します。

SIP 着信認証の設定方法

ここでは、RADIUS サーバで SIP ローカル着信認証を設定する手順について説明します。

SIP 着信認証の設定

手順の概要

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **radius authentication**
5. **activate**
6. **server** *server-name*
7. **address**
8. **mode local**
9. **key** *password*
10. **exit**
11. **exit**
12. **adjacency sip** *adjacency-name*
13. **authentication mode local**
14. **authentication nonce timeout** *time*
15. **commit**
16. **exit**

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。

	コマンドまたはアクション	目的
ステップ 4	**radius authentication** **例：** `RP/0/0/CPU0:router(config-sbc-sbe)#radius authentication`	RADIUS クライアントで認証設定を行うモードを開始します。
ステップ 5	**activate** **例：** `RP/0/0/CPU0:router(config-sbc-sbe-auth)#activate`	RADIUS クライアントをアクティブ化します。
ステップ 6	**server** *server-name* **例：** `RP/0/0/CPU0:router(config-sbc-sbe-auth)#server authserv`	認証サーバを設定するモードを開始します。
ステップ 7	**address ipv4** *ipv4-address* **例：** `RP/0/0/CPU0:router(config-sbc-sbe-auth-ser)#address ipv4 200.200.200.122`	認証サーバの IPv4 アドレスを指定します。
ステップ 8	**mode local** **例：** `RP/0/0/CPU0:router(config-sbc-sbe-auth-ser)#mode local`	RADIUS サーバでローカル着信認証を設定します。デフォルトでは、モードはリモートです。
ステップ 9	**key** *password* **例：** `RP/0/0/CPU0:router(config-sbc-sbe-auth-ser)#key authpass1`	認証サーバ キーを設定します。
ステップ 10	**exit** **例：** `RP/0/0/CPU0:router(config-sbc-sbe-auth-ser)#exit`	認証サーバを設定するモードを終了します。
ステップ 11	**exit** **例：** `RP/0/0/CPU0:router(config-sbc-sbe-auth)#exit`	RADIUS クライアントを設定するモードを終了し、SBE モードを開始します。
ステップ 12	**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。

	コマンドまたはアクション	目的
ステップ 13	**authentication mode local** **例：** `RP/0/0/CPU0:router(config-sbc-sbe-adj-sip)# authentication mode local`	SIP 隣接でローカル着信認証を設定します。SIP 隣接でリモート着信認証を設定するには、この値を **remote** に設定します。
ステップ 14	**authentication nonce timeout** *time* **例：** `RP/0/0/CPU0:router(config-sbc-sbe-adj-sip)# authentication nonce timeout 10000`	認証ナンス タイムアウトの値を秒単位で設定します。有効な値の範囲は 0 ～ 65535 秒です。デフォルト値は 300 秒です。
ステップ 15	**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 16	**exit** **例：** `RP/0/0/CPU0:router(config-sbc-sbe-adj-sip)# exit`	adj-sip モードを終了し、SBE モードに戻ります。

show コマンドの例

```
# show services sbc mySbc sbe adjacencies SipToIsp42 detail
SBC server mySbc
Adjacency SipToIsp42
Status:  Attached
Signaling address: 10.2.0.122:5060
Signaling-peer:    200.200.200.179:8888
Force next hop:   No
Account:   core
Group:     None
In Header Profile:    Default
Out Header Profile:   Default
In method profile:    Default
Out method profile:   Default
In UA option profile: Default
Out UA option profile:   Default
In proxy option profile: Default
Priority set name:       Default
Local-id:             None
Rewrite REGISTER:     Off
Target address:       None
NAT Status:           Auto-Detect
Reg-min-expiry:       3000 seconds
Fast-register:        Enabled
Fast-register-int:    30 seconds
Authenticated mode:   None
Authenticated realm:  None
Authenticated nonce life time: 300 seconds
IMS visited NetID:    NOne
Inherit profile:      Default
Force next hop:       No
Home network ID:      None
UnEncrypt key data:   None
```

```
SIPIpassthrough:      No
Rewrite from domain:  Yes
Rewrite to header:    Yes
Media passthrough:    No
Preferred transport:  UDP
Hunting Triggers:     Global Triggers
Redirect mode:        Passthrough
Security:          Untrusted
```

その他の関連資料

ここでは、SBC での SIP 着信認証に関する関連資料について説明します。

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』*
RFC 2617	*『HTTP Authentication: Basic and Digest Access Authentication』*
RFC 4590	*『RADIUS Extension for Digest Authentication』*

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