CHAPTER 27

SIP 着信認証

Session Border Controller（SBC; セッション ボーダ コントローラ）は、着信 SIP 要求の認証確認のために、Session Initiation Protocol（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。Remote Authentication Dial-In User Service（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 および 01 だけに準拠している場合は、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は、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。

（注） ACE SBC Release 3.0.00 では、この機能は統合モデルに限りサポートされます。

SIP 着信認証機能の履歴

リリース	変更内容
ACE SBC Release 3.0.00	この機能は、SBC 統合モデルのサポートとともに Cisco 7600 シリーズ ルータに追加されました。

この章の構成

この章で説明する内容は、次のとおりです。

SIP 着信認証を実装するための前提条件

次に、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。

- どのモードの着信認証を選択するかを指定するように RADIUS サーバを設定します。

SIP 着信認証を実装するための制約事項

SIP 着信認証の実装には、次の制約および制限が適用されます。

- 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 Transport Layer Security（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、着信認証、発信認証、および TLS を同じ隣接に個別に設定できます。

SIP 着信認証について

ここの構成は、次のとおりです。

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。このため、リモート ピアからの要求の認証確認を行うには、隣接に認証レルムを設定しておく必要があります。リモート ピアが要求を検証すると、その要求は RADIUS サーバに転送され、そこでコールのパススルーを許可するか拒否するかが決定されます。

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。

発信認証とのやり取り

隣接は、着信認証用に設定されている場合、正常に着信要求を認証すると、その隣接のレルムと一致する認証ヘッダーを除去し、発信信号には伝送しません。ただし、他のレルムの認証ヘッダーは発信要求にパススルーされます。

着信認証の障害モード

着信認証を設定している場合、（標準の SIP 信号障害モード以外に）次の障害モードが発生することがあります。

許容できないパラメータ

エンドポイントまたは RADIUS サーバに **auth** や **auth-int** 以外の保護品質パラメータを指定している場合、着信要求は拒否され、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。

Access-Request 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 401 応答で要求の認証確認を再度行います。

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。

許容できる RADIUS サーバなし

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 着信認証を設定する方法

ここでは、RADIUS サーバに 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。

手順概要

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-realm inbound** *realm*
14. **authentication mode local**
15. **authentication nonce timeout** *time*
16. **exit**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `host1/Admin# 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：** `host1/Admin(config)# sbc mysbc`	SBC サービス モードを開始します。 • サービス名を定義するには、*service-name* 引数を使用します。
ステップ 3	**sbe** **例：** `host1/Admin(config-sbc)# sbe`	SBC の Signaling Border Element（SBE; シグナリング ボーダ エレメント）機能モードを開始します。
ステップ 4	**radius authentication** **例：** `host1/Admin(config-sbc-sbe)# radius authentication`	RADIUS クライアントを認証用に設定するため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 5	**activate** **例：** host1/Admin(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：** host1/Admin(config-sbc-sbe-auth)#server authserv	認証サーバを設定するためのモードを開始します。
ステップ 7	**address ipv4** *ipv4-address* **例：** host1/Admin(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：** host1/Admin(config-sbc-sbe-auth-ser)#mode local	ローカル着信認証用に RADIUS サーバを設定します。デフォルトでは、モードはリモート モードです。
ステップ 9	**key** *password* **例：** host1/Admin(config-sbc-sbe-auth-ser)# key authpass1	認証サーバ鍵を設定します。
ステップ 10	**exit** **例：** host1/Admin(config-sbc-sbe-auth-ser)# exit	認証サーバを設定するためのモードを終了します。
ステップ 11	**exit** **例：** host1/Admin(config-sbc-sbe-auth)# exit	RADIUS クライアントを設定するためのモードを終了し、SBE モードを開始します。
ステップ 12	**adjacency sip** *adjacency-name* **例：** host1/Admin(config-sbc-sbe)# adjacency sip test	SBE SIP 隣接モードを開始します。 • サービス名を定義するには、*adjacency-name* 引数を使用します。
ステップ 13	**authentication-realm inbound** *realm* **例：** host1/Admin(config-sbc-sbe)# authentication-realm inbound cisco.com	指定した SIP 隣接に指定のドメイン用の認証クレデンシャルを設定します。 **（注）** これは、ローカル モードでは必須のパラメータです。
ステップ 14	**authentication mode local** **例：** host1/Admin(config-sbc-sbe-adj-sip)# authentication mode local	ローカル着信認証用に SIP 隣接を設定します。リモート着信認証用に SIP 隣接を設定するには、値を **remote** に設定します。

	コマンドまたはアクション	目的
ステップ 15	**authentication nonce timeout** *time* **例：** host1/Admin(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。許容できる値の範囲は 0 ～ 65535 秒です。デフォルト値は 300 秒です。
ステップ 16	**exit** **例：** host1/Admin(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

```
host1/Admin# 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:   Local
Authenticated realm:  Cisco.com
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
```