SIP Authentication

Cisco Unified Border Element (SP Edition) supports Session Initiation Protocol (SIP) authentication.

Note For Cisco IOS XE Release 2.4, this feature is supported in the unified model only.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, refer to the *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html.

For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or a Cisco IOS master commands list.

Feature History for SIP Authentication

Release	Modification
Cisco IOS XE Release 2.4	Support for SIP authentication was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	Support for interoperability for SIP authentication of INVITE requests was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 2.6	Support for interoperability for SIP authentication of outbound out-of-dialogue requests (using the same generation scheme as used by INVITE requests for the Call-ID, From and To dialog tags, and CSeq sequence numbers) was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Contents

This module contains the following sections:

SIP Outbound Authentication

When network entities communicate using SIP, one entity often needs to challenge another one to determine if it is authorized to transmit SIP signaling into the challenger's network. The SIP authentication model is based on the HTTP digest authentication, as described in the RFC 2617.

The use of basic authentication, where passwords are transmitted unencrypted, is not permitted in SIP.

This section contains the following subsections:

Prerequisites for Implementing SIP Outbound Authentication

The following prerequisites are required to implement SIP outbound authentication:

- Configure a SIP adjacency before you specify one or more authentication-realms.
- Configure the Cisco Unified Border Element (SP Edition) with a set of domains (realms) with which it can authenticate itself. Set the username and password to provide when challenged by each of these domains. This configuration is implemented per adjacency.

Note Multiple realms can be configured per adjacency and there is no limit on the number of these realms aside from memory availability. Different realms may be configured with the same username and password. Also, each realm may be configured with different username and password on different adjacencies. However, any realm can be configured a maximum of one time per adjacency.

Restrictions for Implementing SIP Outbound Authentication

The following restrictions apply to SIP outbound authentication:

- Cisco Unified Border Element (SP Edition) rejects any attempt to configure an authentication-realm with the same domain name as an existing authentication-realm. This restriction is valid per adjacency. Multiple adjacencies may have authentication-realms configured with the same domain.

Note The current command line interface (CLI) prohibits the user from configuring two authentication-realms with the same domain for the same adjacency. If this is attempted, the CLI interprets the second authentication-realm configuration as an attempt to reconfigure the first authentication-realm, and updates the user's credentials accordingly.

- Each authentication-realm can only be configured with a single username and password per adjacency.

Information About SIP Outbound Authentication

This section contains the following subsections:

Configuring Outbound Authentication in Cisco Unified Border Element (SP Edition)

When a SIP adjacency is configured, the user may specify one or more authentication-realms. Each authentication-realm represents a remote domain, from which Cisco Unified Border Element (SP Edition) receives authentication challenges on the adjacency. When an authentication-realm is configured, the user must specify the correct user name and password that Cisco Unified Border Element (SP Edition) uses to authenticate itself in that realm. Cisco Unified Border Element (SP Edition) stores all valid authentication-realms for each adjacency.

Authenticating the Cisco Unified Border Element (SP Edition) to Remote Devices

Upon receipt of a SIP 401 or 407 response that can be correlated to a request it sent, Cisco Unified Border Element (SP Edition) examines the attached authentication challenge. Cisco Unified Border Element (SP Edition) responds to any authentication challenge received on a given adjacency that matches one of the configured authentication-realms for that adjacency. Any authentication challenge that does not match the configured authentication-realm is passed through unchanged to the SBC's signaling peer for the adjacency, on which the original request was received.

To generate a response to an authentication challenge, Cisco Unified Border Element (SP Edition) does the following:

1. First, it looks up the realm parameter of the challenge in its list of configured authentication-realms for the outbound adjacency.
2. Second, it finds the password for that authentication-realm and generates an authentication response by combining the password with the nonce parameter from the challenge, and hashing the result.
3. If the challenger has requested **auth-int** quality of protection, Cisco Unified Border Element (SP Edition) also generates a hash of the entire message body and includes it in the response.
4. Cisco Unified Border Element (SP Edition) builds an Authorization (or Proxy-Authorization) header by including the following parameter values (following RFC 2617):

- Nonce from challenge.
- Realm from challenge.
- Digest-URI is set to the SIP URI of the challenged request.
- Message-QOP is set to **auth.**
- Response calculated as described previously.
- Username as specified for the relevant authentication-realm.
- If the challenge contained an **opaque** parameter, it is returned unchanged on the response.
- If the challenge contained the **qop-directive** parameter, then the **nonce-count** parameter is set to the number of the sent requests, using the response calculated from this nonce.

- Note that the domain parameter is not expected to be included on any challenges that Cisco Unified Border Element (SP Edition) must respond to. This parameter is not used on Proxy-Authenticate challenges, the type of challenge that Cisco Unified Border Element (SP Edition) most often receives. If the domain parameter is included, Cisco Unified Border Element (SP Edition) ignores it.

5. Finally, Cisco Unified Border Element (SP Edition) stores its calculated response and the received nonce with the other data for the authentication-realm. This allows Cisco Unified Border Element (SP Edition) to respond rapidly to the subsequent challenges from this realm with the same nonce. If Cisco Unified Border Element (SP Edition) lacks the resources to store its response, it carries on anyway. The next time an authorization challenge is received from this realm, Cisco Unified Border Element (SP Edition) has to recalculate its response. When Cisco Unified Border Element (SP Edition) re-uses a saved response, it updates the nonce count stored along with the nonce-response pair. This allows Cisco Unified Border Element (SP Edition) to correctly fill in the **nonce-count** field in Authorization responses.

How to Configure SIP Outbound Authentication

This section contains the steps for configuring SIP outbound authentication, allowing the user to add/remove one or more authentication-realms to/from an adjacency.

SUMMARY STEPS

1. **configure terminal**
2. **sbc** *service-name*
3. **sbe**
4. **adjacency sip** *adjacency-name*
5. **authentication-realm inbound** *domain* | **outbound** *domain username password*
6. **end**
7. **show sbc** ***sbc-name*** **sbe adjacency** ***adjacency-name*** **authentication-realms**
8. **show sbc** *service-name* **sbe all-authentication-realms**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enables global configuration mode.
Step 2	**sbc** *service-name* **Example:** `Router(config)# sbc mysbc`	Enters the mode of an SBC service. • Use the *service-name* argument to define the name of the service.
Step 3	**sbe** **Example:** `Router(config-sbc)# sbe`	Enters the mode of the signaling border element (SBE) function of the SBC.

	Command or Action	Purpose
Step 4	**adjacency sip** *adjacency-name* **Example:** `Router(config-sbc-sbe)# adjacency sip test`	Enters the mode of an SBE SIP adjacency. • Use the *adjacency-name* argument to define the name of the service.
Step 5	**authentication-realm** {**inbound** *domain*|**outbound** *domain username password}* **Example:** `Router(config-sbc-sbe-adj-sip)# authentication-realm outbound example.com usersbc passwrdsbc`	Configures a set of outbound authentication credentials for the specified domain on the specified adjacency. This command can be issued either before or after the adjacency has been attached. The **no** version of this command deconfigures the authentication-realm on the specified adjacency. • inbound—Specifies inbound authentication realm. • outbound—Specifies outbound authentication realm. • domain—Name of the domain for which the authentication credentials are valid. • username—User name that identifies the SBC in the specified domain. • password—Password to authenticate the username in the specified domain.
Step 6	**end** **Example:** `Router(config-sbc-sbe-adj-sip)# end`	Exits the adj-sip mode and returns to privileged EXEC mode
Step 7	**show sbc** *sbc-name* **sbe adjacency** *adjacency-name* **authentication-realms** **Example:** `Router# show sbc mySbc sbe adjacency SipToIsp42 authentication-realms`	Shows all currently configured authentication-realms for the specified SIP adjacency.
Step 8	**show sbc** *service-name* **sbe all-authentication-realms** **Example:** `Router# show sbc mySbc sbe all-authentication-realms`	Shows all currently configured authentication-realms for all SIP adjacencies.

Examples of Show Commands

```
Router# show sbc mySbc sbe adjacency SipToIsp42 authentication-realms

Configured authentication realms
--------------------------------
Domain       Username  Password
Example.com  usersbc   passwordsbc


Router# show sbc mySbc sbe all-authentication-realms
```

```
Configured authentication realms
--------------------------------
Adjacency: SipToIsp42
Domain       Username  Password     Example.com  usersbc   passwordsbc
Remote.com   usersbc   sbcpassword

Adjacency: SipToIsp50
Domain       Username  Password
Example.com  user2sbc  password2sbc
Other.com    sbcuser   sbcsbcsbc
```

SIP Inbound Authentication

Cisco Unified Border Element (SP Edition) supports two modes of Session Initiation Protocol (SIP) inbound authentication to challenge inbound SIP requests: local and remote. You must select the mode of authentication to configure Cisco Unified Border Element (SP Edition) according to the level of support present in the Remote Authentication Dial-In User Service (RADIUS) servers. If the RADIUS servers are compliant with only draft-sterman-aaa-sip-00 to 01, then select the local mode. If the RADIUS servers are compliant with only RFC 4590, then use the remote authentication mode.

Note This feature is optional and you can configure the Cisco Unified Border Element (SP Edition) not to challenge the inbound requests.

This section contains the following subsections:

Prerequisites for Implementing SIP Inbound Authentication

The following prerequisites are required to implement SIP inbound authentication:

- Configure a SIP adjacency with the intended mode of authentication before you configure Cisco Unified Border Element (SP Edition) to authenticate inbound calls.
- Configure the RADIUS server to specify which mode of inbound authentication is selected.

Restrictions for Implementing SIP Inbound Authentication

The following restrictions and limitations apply to implement SIP inbound authentication:

- Cisco Unified Border Element (SP Edition) supports only one inbound authentication realm per adjacency.
- Cisco Unified Border Element (SP Edition) does not check the validity of nonces generated by a RADIUS server; the RADIUS server must be configured to perform this check.

- Cisco Unified Border Element (SP Edition) does not designate a particular RADIUS server group on an adjacency for inbound authentication.
- Since trust-transference of calls does not occur between inbound authentication, outbound authentication, and Transport Layer Security (TLS) connections, a successful inbound authentication does not ensure that Cisco Unified Border Element (SP Edition) marks the call as secure or implement outbound authentication. Users can, however, configure inbound authentication, outbound authentication, and TLS independently on the same adjacency.

Information About SIP Inbound Authentication

This section contains the following subsections:

Local Inbound Authentication

When configured to perform local inbound authentication, Cisco Unified Border Element (SP Edition) is responsible for challenging an unauthorized request from the remote peer first. Therefore, to be able to challenge the request from the remote peer, the adjacency must already be configured with an authentication realm. After the remote peer has validated the request, it is forwarded to the RADIUS server, which then decides whether to permit the call to pass through or not.

Remote Inbound Authentication

When configured to perform remote inbound authentication, Cisco Unified Border Element (SP Edition) relies on the RADIUS server to challenge an authorized request from the remote peer. Cisco Unified Border Element (SP Edition) forwards the challenge request generated by the RADIUS server to the remote peer, and also forwards the remote peer's authentication request to the RADIUS server.

Interaction with Outbound Authentication

If an adjacency is configured for inbound authentication, then after it successfully authenticates an inbound request, the authorization headers matching the realm for that adjacency are stripped out and not propagated to the outbound signal. Authorization headers for other realms, however, are passed through to the outbound request.

Failure Modes for Inbound Authentication

When the inbound authentication is configured, the following failure modes may occur (in addition to the standard SIP signal failure modes):

Unacceptable Parameters

If the endpoint or RADIUS server specifies a quality of protection parameter other than **auth** or **auth-int**, then the inbound request is rejected and a 403 response is generated. Similarly, Cisco Unified Border Element (SP Edition) generates a 403 response when algorithms other than MD5 and MD5-sess are used.

Access-Request Rejection

If the RADIUS server rejects the Access-Request signal with an Access-Reject response, Cisco Unified Border Element (SP Edition) sends a 403 response to the endpoint.

Insufficient Memory

If Cisco Unified Border Element (SP Edition) does not have sufficient memory to process an inbound authentication request, it rejects the request and sends a 503 response.

No Match on Authentication Realm

If the peer does not return any authentication headers that specify the authentication realm contained in the adjacency's configuration, then Cisco Unified Border Element (SP Edition) rechallenges the request with 401 response.

No Match on Nonce

If the peer's nonce does not match the one generated by Cisco Unified Border Element (SP Edition), then Cisco Unified Border Element (SP Edition) rejects the authentication request and sends a 403 response.

Nonce Timed Out

If the peer's nonce has timed out, then Cisco Unified Border Element (SP Edition) challenges the nonce by sending a 401 response and a new nonce.

No Acceptable RADIUS Servers

If there is no RADIUS server to support a mode configured on the adjacency, then Cisco Unified Border Element (SP Edition) rejects the authentication request with a 501 response and creates a log to alert the user of the inconsistent configuration.

How to Configure SIP Inbound Authentication

This section contains the steps for configuring SIP local inbound authentication a RADIUS server.

SUMMARY STEPS

1. **configure terminal**
2. **sbc** *service-name*
3. **sbe**
4. **radius [accounting** *client-name* | **authentication]**
5. **server** *server-name*

6. **address**
7. **mode local**
8. **key** *password*
9. **exit**
10. **activate**
11. **exit**
12. **adjacency sip** *adjacency-name*
13. **authentication-realm inbound** *realm*
14. **authentication mode local**
15. **authentication nonce timeout** *time*
16. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enables global configuration mode.
Step 2	**sbc** *service-name* **Example:** `Router(config)# sbc mysbc`	Enters the mode of an SBC service. • Use the *service-name* argument to define the name of the service.
Step 3	**sbe** **Example:** `Router(config-sbc)# sbe`	Enters the mode of the signaling border element (SBE) function of the SBC.
Step 4	**radius [accounting** *client-name* | **authentication]** **Example:** `Router(config-sbc-sbe)# radius authentication`	Enters the mode for configuring a RADIUS client for authentication purposes.
Step 5	**server** *server-name* **Example:** `Router(config-sbc-sbe-auth)# server authserv`	Enters the mode for configuring the authentication server.
Step 6	**address ipv4** *ipv4-address* **Example:** `Router(config-sbc-sbe-auth-ser)# address ipv4 200.200.200.122`	Specifies the IPv4 address of the authentication server.

	Command or Action	Purpose
Step 7	**mode {local|remote}** or **server server-name mode {local|remote}** **Example:** `Router(config-sbc-sbe-auth-ser)# mode local`	Configures the RADIUS server for local inbound authentication. By default, the mode is remote.
Step 8	**key** *password* **Example:** `Router(config-sbc-sbe-auth-ser)# key authpass1`	Sets the authentication server key.
Step 9	**exit** **Example:** `Router(config-sbc-sbe-auth-ser)# exit`	Exits the mode for configuring the authentication server.
Step 10	**activate** **Example:** `Router(config-sbc-sbe-auth)# activate`	Activates the RADIUS client.
Step 11	**exit** **Example:** `Router(config-sbc-sbe-auth)# exit`	Exits the mode for configuring the RADIUS client and enters the SBE mode.
Step 12	**adjacency sip** *adjacency-name* **Example:** `Router(config-sbc-sbe)# adjacency sip test`	Enters the mode of an SBE SIP adjacency. • Use the *adjacency-name* argument to define the name of the service.
Step 13	**authentication-realm inbound** *realm* **Example:** `Router(config-sbc-sbe-adj-sip)# authentication-realm inbound cisco.com`	Configures a set of authentication credentials for a specified domain on the specified SIP adjacency. **Note** This is a mandatory parameter for local mode.
Step 14	**authentication mode local** **Example:** `Router(config-sbc-sbe-adj-sip)# authentication mode local`	Configures the SIP adjacency for local inbound authentication. To configure the SIP adjacency, for remote inbound authentication, set the value to **remote.**
Step 15	**authentication nonce timeout** *time* **Example:** `Router(config-sbc-sbe-adj-sip)# authentication nonce timeout 10000`	Configures the value of the authentication nonce timeout in seconds. The range of acceptable values is 0 to 65535 seconds. The default value is 300 seconds.
Step 16	**exit** **Example:** `Router(config-sbc-sbe-adj-sip)# exit`	Exits the adj-sip mode and returns to the SBE mode.

Examples of Show Commands

```
Router# show 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
```

Interoperability for SIP Authentication

Cisco Unified Border Element (SP Edition) supports interoperability between SIP devices and third-party soft switch equipments for SIP authentication of all SIP requests. The supported interoperability applies to dialog-creating INVITE requests and out-of-dialog REGISTER and SUBSCRIBE requests only.

Support for interoperability for SIP authentication of INVITE requests was introduced in Cisco IOS XE Release 2.5. Cisco Unified Border Element (SP Edition) uses a generation scheme that generates the Call-ID, From and To dialog tags, and CSeq sequence numbers on the outbound call leg using the inbound request message data which provides both uniqueness and retains the same values for subsequent requests resulting from any challenges.

Support for interoperability for SIP authentication of out-of-dialog requests was introduced in Cisco IOS XE Release 2.6. The same generation scheme used by INVITE requests (based on the inbound request message data) was implemented for out-of-dialog requests.

Cisco Unified Border Element (SP Edition) interoperates with third-party soft switch devices for processing SIP authentication of INVITE and out-of-dialog requests in the following way:

- The Call-ID of an authorized SIP request matches that of the initial request.
- The To and From headers of an authorized SIP request match those of the initial request, including the dialog tag (if any) in the From header.
- The CSeq sequence number of an authorized SIP request is one higher than the initial request.

This section contains the following subsections:

- Information About SIP Outbound Authentication, page 48-3
- Information About Interoperability for SIP Authentication, page 48-13

Restrictions for Interoperability for SIP Authentication

The following restrictions apply to support for Interoperability for SIP Authentication on the Cisco Unified Border Element (SP Edition):

- Cisco Unified Border Element (SP Edition) meets the following interoperability requirements only when the received signaling from the upstream call leg also meets the same:
  - The Call-ID of an authorized SIP request matches that of the initial request.
  - The To and From headers of an authorized SIP request match those of the initial request, including the dialog tag (if any) in the From header.
  - The CSeq sequence number of an authorized SIP request is one higher than the initial request.
- Cisco Unified Border Element (SP Edition) depends on the randomness of the values in the received signaling. For example, if a calling endpoint generates insufficiently random values, then the values sent by the SBC on the outbound call leg will also be insufficiently random. However, the SBC uses any and all randomness from the Call-IDs and From tags generated by the caller, and in addition takes steps to avoid Call-ID and tag collisions between the upstream and downstream signaling.
- If the input from certain configuration fields to Call-ID and To/From header generation is changed between forwarding an initial SIP request and the subsequent authorized SIP request to that adjacency, then the headers of the two requests do not match. This can lead to call setup failure, depending on the downstream signaling entities. In particular, note the following:
  - The local-id or signaling-address configuration under adjacency affects Call-ID and From-tag generation.
  - Header rewriting configuration can apply to From and To headers. To meet the interoperability requirements, this rewriting must produce identical results on successive requests.
  - Cisco Unified Border Element (SP Edition) does not issue warnings to the user before accepting such configuration changes.
- Interoperability for SIP authentication affects dialog-creating INVITE requests and out-of-dialogue requests. Requests with other methods are not affected.
- To meet the interoperability requirements, the initial and authorized requests should not be routed out of different adjacencies.

Information About Interoperability for SIP Authentication

This section provides information about interoperability for SIP authentication.

SIP Requests

SIP requests refer to the messages within the scope of a single challenge or response sequence. There can be several sequences before a request is accepted, but the first sequence of any pair of consecutive requests is referred to as the initial request and the second one is referred to as the authorized request.

SIP requests are both dialog-creating INVITE requests and out-of-dialog requests.

The following SIP request terms are used in this chapter:

Initial request—A SIP request with insufficient authentication credentials, which is challenged with a "401–Unauthorized" or a "407–Proxy Authentication Required" response.

Authorized request—The corresponding subsequent request, sent on receipt of the 401/407 challenge response. This request contains an extra Authorization or Proxy-Authorization header.

Call-ID Generation

Cisco Unified Border Element (SP Edition) generates Call-ID values for outbound dialog-creating INVITE requests and out-of-dialogue requests (such as REGISTERS and SUBSCRIBES), based on the Call-ID of the inbound request and on configuration.

The generated Call-ID values are composed of a 32-character hexadecimal MD5 hash of the received Call-ID, an '@' character, and a local-id string representing the SBC itself.

Example:

```
Call-ID: 4264330abc5106c8ab70ed3fd222b7b2@sbc.home.net
```

Note The local-id string is the configuration from the outbound adjacency. If this configuration is absent, the canonical text representation of the signaling-address from the outbound adjacency is used.

From Tag Generation

Cisco Unified Border Element (SP Edition) generates From header dialog tag values for outbound dialog-creating INVITE requests and out-of-dialogue requests (such as REGISTERS and SUBSCRIBES), based on the From tag of the inbound request and on configuration.

The generated From tag values are composed of a local-id string representing the SBC itself, two eight-character hexadecimal MD5 hashes of the received From tag, and a numerical index identifying the internal component responsible for the dialog.

Example:

```
From: "Fred" <sip:2222222@sbc.home.net>;tag=sbc.home.net+1+a27d9765+b7f0f7e1
```

The local-id string is generated from configuration in the same way as for Call-IDs.

CSeq Sequence Number Generation

Cisco Unified Border Element (SP Edition) chooses the sequence number for use in the CSeq header of an outbound dialog-creating INVITE request and out-of-dialogue requests (such as REGISTERS and SUBSCRIBES) to be the same as the sequence number on the received inbound request.

Cisco Unified Border Element (SP Edition) continues to choose sequence numbers for subsequent outbound requests on the same dialog by storing the dialog's current sequence number, and incrementing it each time a new transaction is created.

Example:

```
CSeq: 949005087 INVITE
```

Pass-Through Authentication

SBC supports passing through authentication challenges and their responses. No configuration is required for this.

- 407 responses are passed through by SBC.
- On challenge responses, a quality of protection (qop) of "auth-int" is stripped out, as SBC necessarily modifies the message, which negates the integrity of the authentication. If this is the only qop offered, the challenge is converted into a 403 Forbidden return code.