P-CSCF Support

The Proxy-Call Session Control Function (P-CSCF) is the first contact point for the users of the IP Multimedia Subsystem (IMS). The P-CSCF functions as a proxy server for the user equipment; all Session Initiation Protocol (SIP) signaling traffic to and from the user equipment must go through the P-CSCF. The P-CSCF validates and then forwards requests from the user equipment and then processes and forwards the responses to the user equipment.

The P-CSCF can also function as a user agent in the context of the SIP operating procedures. If an abnormal condition arises in a session, the P-CSCF can unilaterally release the session for the user equipment. The user agent role can also be used to generate independent SIP messages required during the registration, such as sending the user's public and private identities. There may be more than one P-CSCF in the operator's network based on survivability, number of users, expected traffic, and network topology. The P-CSCF can be also referred to as the SIP server.

To implement the P-CSCF support on Cisco Unified Border Element (SP Edition), users must select an Inherit Profile for a SIP adjacency. The three available Inherit Profiles are:

- Standard Non-IMS Profile
- P-CSCF Access Profile
- P-CSCF Core Profile

Each of these profiles groups a set of IMS-related configuration fields that can be applied across multiple adjacencies.

If a valid profile is configured, this profile is applied to an adjacency that does not have a profile configured. If a profile is already selected for a SIP adjacency, that profile is used instead of the entity's profile.

In Cisco IOS XE Release 2.5 and later, Cisco Unified Border Element (SP Edition) supports Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) for SIP calls. This type of authentication is used for access authentication in mobile IMS deployments and typically may reside on a mobile subscriber's card inside a phone. No special configuration is needed. The only requirement is that a UNI SIP profile is configured on the access side of the network.

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.

Note For Cisco IOS XR Software Release and later, this feature is supported in the unified model only.

Feature History for P-CSCF Support

Release	Modification
Cisco IOS XR Software Release	This support was introduced on the Cisco IOS XR along with support for the unified model.
Cisco IOS XE Release 2.5	The HTTP Digest Authentication Using AKA feature was introduced on the Cisco ASR 1000 Series Routers.

Contents

This module contains the following sections:

Restrictions for Implementing P-CSCF Support

The following restrictions and limitations apply to implementing P-CSCF support:

- Since the Visited Network Identifier is not part of an Inherit Profile, you need to configure it independently on a per-adjacency basis.
- This feature does not offer support for securing access links through IPsec or Network Attachment Subsystem (NASS) bundled authentication.
- This feature does not support emergency calls.

Information About P-CSCF Support

This section contains the following subsections:

Standard Non-IMS Profile

This profile provides compatibility with existing Cisco Unified Border Element (SP Edition) functionality and is used for adjacencies that do not operate in an IMS network. When this profile is applied to an adjacency, Cisco Unified Border Element (SP Edition) exhibits the following properties:

- Contact headers are rewritten to ensure that the SBC remains on the signaling path.
- Unknown headers, methods, and options are, by default, not allowed to pass through.
- Cisco Unified Border Element (SP Edition) does not attach Path headers to outbound signals.
- Cisco Unified Border Element (SP Edition) does not attach Record-Route headers to outbound signals.
- The endpoints on this adjacency do not need to be registered to receive or send Non-REGISTER requests.
- The endpoints do not need to attach a Route header to outbound signals.
- The adjacencies do not generate P-Charging Vector headers for outbound signals.

P-CSCF Access Profile

This profile provides the configurations required to perform the functions of a P-CSCF Access adjacency. When this profile is applied to an adjacency, Cisco Unified Border Element (SP Edition) exhibits the following properties:

- Contact headers are not rewritten.
- The endpoints on this adjacency need to be registered to receive or send Non-REGISTER requests.
- The endpoints need to attach a Route header to outbound signals, which in turn, matches a Service-Route set from the Registrar.
- The SBC appends Record-Route headers to outbound signals for adjacencies with P-CSCF profiles.
- The SBC does not attach Path headers to outbound signals.
- The adjacencies do not generate P-Charging Vector headers for outbound signals.
- The SBC, by default, allows all inbound non-essential headers to pass through, except P-Asserted Identity, Security-Client, Security-Verify, P-Charging-Function Addresses, P-Charging-Vector, and P-Media-Authorization.
- The SBC, by default, allows all outbound non-essential headers, except P-Charging-Function-Addresses, P-Charging-Vector, and P-Media-Authorization.
- The SBC allows all inbound non-essential methods to pass through.
- The SBC allows all outbound non-essential methods to pass through; UEs are not permitted to act as Registrars.
- The Option tags in Supported, Require, or Proxy-Require headers are allowed to pass through in both directions.

P-CSCF Core Profile

This profile provides the configurations required to perform the functions of a P-CSCF Core adjacency. When this profile is applied to an adjacency, Cisco Unified Border Element (SP Edition) exhibits the following properties:

- Contact headers are not rewritten.
- The SBC, by default, allows all inbound unknown headers, except the P-Charging-Function-Addresses and P-Media-Authorization.
- The SBC appends Record-Route headers to outbound signals for adjacencies with P-CSCF profiles.
- The SBC attaches Path headers to outbound REGISTER signals from P-CSCF.
- The adjacencies generate P-Charging Vector headers for outbound signals.
- The endpoints on this adjacency do not need to be registered to receive or send Non-REGISTER requests.
- The SBC, by default, allows all outbound non-essential headers, except P-Charging-Function-Addresses and P-Media-Authorization.
- The SBC allows all unknown methods to pass through.
- The Option tags in Supported, Require, or Proxy-Require headers are allowed to pass through in both directions.

Effect of P-CSCF Inherit Profiles on Method Profiles, Header Profiles, and Option Profiles

Use of a P-CSCF inherit profile dynamically assigns the following sets of profiles (method profile, header profile, and option profile) to a call based on the P-CSCF inherit profile selected. Table 55-1 shows which P-CSCF inherit profile has an effect on which specific method profile, header profile, and option profile.

The effect is not visible in the adjacency configuration for header-profile, method-profile or option profiles, and can be overridden by explicit configuration of header, method, option profiles as needed.

Table 55-1 Effect of P-CSCF Inherit Profiles on Method, Header and Option Profiles

P-CSCF Inherit Profile	Method Profile	Header Profile	Option Profile
preset-p-cscf-access	preset-acc-in-mth Type: Blacklist Actions: No methods rejected preset-acc-out-mth Type: Blacklist Actions: Rejects REGISTER	preset-acc-in-hdr Type: Blacklist Actions: Removes Security-Client Removes Security-Verify Removes P-Charging-Vector Removes P-Asserted-Identity Removes P-Visited-Network-ID Removes P-Media-Authorization Removes P-Charging-Function-Address preset-acc-out-hdr Type: Blacklist Actions: Removes P-Charging-Vector Removes P-Media-Authorization	preset-acc-in-opt preset-acc-out-opt Type: Blacklist Actions: No options (Passes on all)
preset-p-cscf-core	preset-core-in-mth Type: Blacklist Actions: No methods removed preset-core-out-mth Type: Blacklist Actions: No methods rejected	preset-core-in-hdr preset-core-out-hdr Type: Blacklist Actions: Removes no headers (passes all)	preset-core-in-opt preset-core-out-opt Type: Blacklist Actions: No options (Passes on all)
preset-standard-non-ims	preset-std-in-mth preset-std-out-mth Type: Whitelist Actions: Passes INFO Passes UPDATE	preset-std-in-hdr preset-std-out-hdr Type: Whitelist Actions: Passes Server Passes Diversion Passes Resource-Priority	preset-std-in-opt preset-std-out-opt Type: Whitelist Actions: Passes Replaces (only)

Implementing P-CSCF Support

This section explains how to configure intrinsic profiles and profile inheritance.

Configuring Profile Inheritance

SUMMARY STEPS

1. **configure terminal**
2. **sbc** *service-name*
3. **sbe**
4. **sip inherit profile preset-p-cscf-access**
5. **adjacency sip** *adjacency-name*
6. **inherit profile preset-p-cscf-access**
7. **visited network identifier** *network-name*
8. **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 a SBE entity within an SBC service.
Step 4	**sip inherit profile preset-p-cscf-access** **Example:** `Router(config-sbc-sbe)# sip inherit profile preset-p-cscf-access`	Configures the P-CSCF Access Inherit Profile as the global profile. For a list of other configurable parameters, see the **sip inherit profile** command.
Step 5	**adjacency sip** *adjacency-name* **Example:** `Router(config-sbc-sbe)# adjacency sip sipadj`	Enters the mode of an SBE SIP adjacency. • Use the *adjacency-name* argument to define the name of the SIP adjacency.

	Command or Action	Purpose
Step 6	**inherit profile preset-p-cscf-access** **Example:** `Router(config-sbc-sbe-adj-sip)# inherit profile preset-p-cscf-access`	Configures the SIP adjacency to use the P-CSCF-Access profile.
Step 7	**visited network identifier** *network-name* **Example:** `Router(config-sbc-sbe-adj-sip)# visited network identifier mynetwork.com`	Configures the specified visited network identifier on the SIP adjacency.
Step 8	**exit** **Example:** `Router(config-sbc-sbe-adj-sip)# exit`	Exits the SIP adjacency mode to the SBE mode.

Information About HTTP Digest Authentication Using AKA

This section contains the following subsections:

Cisco Unified Border Element (SP Edition) supports Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) for SIP calls. This type of authentication is used for access authentication in mobile IMS deployments and typically resides on a mobile subscriber's card inside a phone. Cisco Unified Border Element (SP Edition) supports the HTTP Digest Authentication Using AKA feature with no special configuration needed, as long as a User-to-Network Interconnections (UNI) SIP profile is configured on the access side (that is, with a P-CSCF access side profile).

The AKA function carries out user authentication and session key distribution in Universal Mobile Telecommunications System (UMTS) networks. AKA is challenge- response based. The response to the challenge is computed by the application running on the mobile subscriber's card inside the phone.

HTTP Digest Authentication is common with IP-PBXs. The HTTP Digest Authentication procedure is used to ensure that only valid devices can register (at a SIP level) to a network. The SBC supports the typical registration call flow, that is, passing through authentication challenges and their responses. A typical call flow consists of a SIP REGISTER message from an endpoint that is routed by the SBC to the SIP registrar. The registrar replies with a 401 Unauthorized response and a "challenge."

The challenge contains a random number that the endpoint uses to compute a response, which is sent in another REGISTER message. Finally the registrar replies with a 200 OK message if the response was valid. In the case of HTTP Digest Authentication Using AKA, the response to the challenge is computed by the application running on the mobile subscriber's card inside the phone. The SBC supports this typical call flow by means of enabling a SIP profile that allows SIP registrations.

Another usage of HTTP Digest Authentication Using AKA concerns the ability of using the procedure to establish an IPsec connection (actually two IPsec connections) for ensuring signaling security. Cisco Unified Border Element (SP Edition) supports IPsec, however the ability to extract the port security association identifiers and key information from SIP messages is not supported in Cisco IOS XE Release 2.5.

Configuring HTTP Digest Authentication Using AKA

This task configures HTTP Digest Authentication Using AKA on two related adjacencies where preset-access and preset-core profiles must be configured.

SUMMARY STEPS

1. **configure terminal**
2. **sbc** *sbc-name*
3. **sbe**
4. **adjacency** {**sip** | **h323**} *adjacency-name*
5. **inherit profile {preset-access | preset-core | preset-ibcf-ext-untrusted | preset-ibcf-external | preset-ibcf-internal | preset-p-cscf-access | preset-p-cscf-core | preset-peering | preset-standard-non-ims}**
6. **exit**
7. **adjacency** {**sip** | **h323**} *adjacency-name*
8. **inherit profile {preset-access | preset-core | preset-ibcf-ext-untrusted | preset-ibcf-external | preset-ibcf-internal | preset-p-cscf-access | preset-p-cscf-core | preset-peering | preset-standard-non-ims}**
9. **exit**
10. **end**
11. **show sbc** *sbc-name* **sbe adjacencies** ***adjacency-name*** **detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enables global configuration mode.
Step 2	**sbc** *sbc-name* **Example:** `Router(config)# sbc mySbc`	Creates the SBC service on the SBC and enters into SBC configuration mode.
Step 3	**sbe** **Example:** `Router(config-sbc)# sbe`	Enters the mode of the signaling border element (SBE) function of the SBC.
Step 4	**adjacency** {**sip**	**h323**} *adjacency-name* **Example:** `Router(config-sbc-sbe)# adjacency sip sipEndpoint`	Configures the SIP adjacency facing the endpoint, and enters into adjacency sip configuration mode.

	Command or Action	Purpose
Step 5	**inherit profile {preset-access | preset-core | preset-ibcf-ext-untrusted | preset-ibcf-external | preset-ibcf-internal | preset-p-cscf-access | preset-p-cscf-core | preset-peering | preset-standard-non-ims}** **Example:** `Router(config-sbc-sbe-adj-sip)# inherit profile preset-p-cscf-access`	Required. Configures a preset P-CSCF access profile for the SIP adjacency facing the endpoint. P-CSCF is Proxy-Call Session Control Function—part of its function is to authenticate the user and establish an IPsec security association with the IMS terminal.

Step 6	`exit`
	
	Example:
	`Router(config-sbc-sbe-adj-sip)# exit`
		Exits adjacency sip configuration mode and enters into sbe configuration mode.

Step 7	**adjacency** {**sip** | **h323**} *adjacency-name* **Example:** `Router(config-sbc-sbe)# adjacency sip SoftSwitch`	Configures the SIP adjacency facing the registrar/softswitch, and enters into adjacency sip configuration mode.
Step 8	**inherit profile {preset-access | preset-core | preset-ibcf-ext-untrusted | preset-ibcf-external | preset-ibcf-internal | preset-p-cscf-access | preset-p-cscf-core | preset-peering | preset-standard-non-ims}** **Example:** `Router(config-sbc-sbe-adj-sip)# inherit profile preset-p-cscf-core`	Required. Configures a preset P-CSCF core profile for the SIP adjacency facing the registrar/softswitch. An adjacency facing the registrar typically has a preset-core profile. The default is preset-core.

Step 9	`exit`
	
	Example:
	`Router(config-sbc-sbe-adj-sip)# exit`
		Exits adjacency sip configuration mode and enters into SBE configuration mode.

Step 10	`end`
	
	Example:
	`Router(config-sbc-sbe)# end`
		Exits SBE configuration mode and returns to EXEC mode.

Step 11	**show sbc** *sbc-name* **sbe adjacencies** ***adjacency-name*** **detail** **Example:** `Router# show sbc sbe mySBC sbe adjacencies SoftSwitch detail`	Displays all the detailed field output for the specified SIP adjacency.

Configuration Example—HTTP Digest Authentication Using AKA

The following is a configuration example used to verify HTTP Digest Authentication Using AKA:

```
sbc asr
 sbe
   adjacency sip UE
    inherit profile preset-p-cscf-access
    visited network identifier open-ims.test
    local-id host pcscf.open-ims.test
    signaling-address ipv4 10.190.5.129
    signaling-port 4060
    remote-address ipv4 10.0.0.0 255.255.0.0
    signaling-peer 10.0.120.19
    dbe-location-id 100
    fast-register disable
    attach

   adjacency sip OpenIMSCore
    inherit profile preset-p-cscf-core
    visited network identifier open-ims.test
    local-id host pcscf.open-ims.test
    signaling-address ipv4 10.190.5.129
    signaling-port 4060
    remote-address ipv4 10.0.48.236 255.255.255.255
    signaling-peer 10.0.48.236
    dbe-location-id 100
    registration rewrite-register
    registration target address open-ims.test
    attach
```