CHAPTER 38

Configuring SIP SDP Attribute Passthrough

Before ACE SBC release 3.1.00, the SBC handled SDP attribute passthrough by passing through all attribute lines (a=) on an Offer (sometimes changing or adding certain kinds of attribute lines).

For attribute lines on an Answer, the SBC passed through certain select lines (while ignoring the rest) and reflecting back the offerer's lines instead.

For ACE SBC release 3.1.00, the Session Border Controller (SBC) by default passes through all a= lines in SIP messages containing SDP offers and answers that it forwards. You can also configure the SBC to block certain a= lines, either by specifying a whitelist (a finite set of a=lines that are passed through, with all others blocked), or alternatively a blacklist (a finite set of a=lines that are blocked, with all others passed through).

Feature History for SIP Attribute Passthrough

Release	Modification
ACE SBC Release 3.1.00	SDP Attribute Passthrough was introduced on the Cisco7600 series router .

Restrictions for Configuring SIP SDP Attribute Passthrough

Review the following restrictions forSIP SDP Attribute Passthrough:

- The existing reflect behavior is not supported.
- Wildcard or prefix matching of attribute lines is not supported.
- Distinguishing media-level from session-level a-lines for the purposes of matching is not supported.
- Sophisticated matching conditions (for example, apply only to video streams or apply only to offers) are not supported.
- Attribute blocking in media bypass calls is not supported.
- Blocking function is restricted to unknown attributes.
- The following attributes are ignored by unknown attribute policy because this may interfere with the correct operation of the SBC.
  - a=rtpmap
  - a=fmtp
  - a=sendonly
  - a=recvonly

- a=inactive
- a=sendrecv
- a=ptime
- a=mid
- a=group
- a=curr
- a=des
- a=conf
- a=crypto.

At the point where the policy is applied, a (rate-limited) warning log is issued if the policy attempts to delete one of these lines.

Information about SIP SDP Attribute Passthrough

Additional per-call storage is needed to store the SDP policy that is being applied. This is expected to be ~160 bytes per call.

Configuring SIP SDP Attribute Passthrough

This section contains the steps for implementing SIP SDP attribute passthrough.

SUMMARY STEPS

1. **configure**
2. **sbc** *service-name*
3. **sbe**
4. **sdp-match-table** *table-name*
5. **action** *whitelist/blacklist*
6. **match-string** *name*
7. **match-string** *name*
8. **exit**
9. **sdp-match-table** *table-name*
10. **action** *whitelist/blacklist*
11. **match-string** *name*
12. **match-string** *name*
13. **exit**
14. **sdp-policy-table** *table-name*
15. **match-table** *table-name*
16. **exit**

17. **sdp-policy-table** *table-name*
18. **match-table** *table-name*
19. **exit**
20. **cac-policy-set** *number*
21. **first-cac-table** *table-name*
22. **first-cac-scope** *scope*
23. **cac-table** *table-name*
24. **match-type** *type*
25. **entry** *number*
26. **match-value** *value*
27. **action** *action-name*
28. **caller-inbound-policy** *policytab-name*
29. **caller-outbound-policy** *policytab-name*
30. **callee-inbound-policy** *policytab-name*
31. **callee-outbound-policy** *policytab-name*
32. **exit**
33. **exit**
34. **complete**
35. **exit**
36. **active-cac-policy-set** *number*
37. **show services sbc** *service-name* **sbe cac-policy-set** *number* **table** *number* **entry** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** `host1/Admin# configure`	Enables global configuration mode.
Step 2	**sbc** *service-name* **Example:** `host1/Admin(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:** `host1/Admin(config-sbc)# sbe`	Enters the mode of the signaling border element (SBE) function of the SBC.

	Command or Action	Purpose
Step 4	**sdp-match-table** *table-name* **Example:** `host1/Admin(config-sbc-sbe)# sdp-match-table 1`	Adds an existing sdp-match-table into policy.
Step 5	**action** *whitelist/blacklist* **Example:** `host1/Admin(config-sbc-sbe-sdp-match-tbl)# action blacklist`	Specifies an SDP policy table action.
Step 6	**match-string** *name* **Example:** `host1/Admin(config-sbc-sbe-sdp-match-tbl)# match-string attribute-name1`	Configures an SDP attribute matching string.
Step 7	**match-string** *name* **Example:** `host1/Admin(config-sbc-sbe-sdp-match-tbl)# match-string attribute-name2`	Configures an SDP attribute matching string.
Step 8	**exit** **Example:** `host1/Admin(config-sbc-sbe-sdp-match-tbl)# exit`	Returns to the previous submode.
Step 9	**sdp-match-table** *table-name* **Example:** `host1/Admin(config-sbc-sbe)# sdp-match-table-name 2`	Adds an existing sdp-match-table into policy.
Step 10	**action** *whitelist/blacklist* **Example:** `host1/Admin(config-sbc-sbe-sdp-match-tbl)# action blacklist`	Adds an action allowing a defined set of attributes and blocking the remaining attributes.
Step 11	**match-string** *name* **Example:** `host1/Admin(config-sbc-sbe-sdp-match-tbl)# match-string attribute-name1`	Configures an SDP attribute matching string.
Step 12	**match-string** *name* **Example:** `host1/Admin(config-sbc-sbe-sdp-match-tbl)# match-string attribute-name3`	Configures an SDP attribute matching string.

	Command or Action	Purpose
Step 13	**exit** **Example:** `host1/Admin(config-sbc-sbe-sdp-match-tbl)# exit`	Returns to the previous submode.
Step 14	**sdp-policy-table** *table-name* **Example:** `host1/Admin(config-sbc-sbe)# sdp-policy-table table-name1`	Configures an SDP policy table.
Step 15	**match-table** *table-name* **Example:** `host1/Admin(config-sbc-sbe-sdp-policy-tbl)# match-table table-name1`	Configure an SDP match table used in a policy.
Step 16	**exit** **Example:** `host1/Admin(config-sbc-sbe-sip-adj)# exit`	Returns to the previous submode.
Step 17	**sdp-policy-table** *table-name* **Example:** `host1/Admin(config-sbc-sbe)# sdp-policy-table table-name2`	Configures an SDP policy table.
Step 18	**match-table** *table-name* **Example:** `host1/Admin(config-sbc-sbe-sdp-policy-tbl)# match-table table-name2`	Configure an SDP match table used in a policy.
Step 19	**exit** **Example:** `host1/Admin(config-sbc-sbe-sip-adj)# exit`	Returns to the previous submode.
Step 20	**cac-policy-set** *number* **Example:** `host1/Admin(config-sbc-sbe)# cac-policy-set 1`	Enters the submode of CAC policy set configuration.
Step 21	**first-cac-table** *table-name* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy)# first-cac-table RootCacTable`	Configures the name of the first policy table to process when performing the admission control stage of policy.
Step 22	**first-cac-scope** *scope* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy)# first-cac-scope src-adjacency`	Configures the scope at which to begin defining limits when performing the admission control stage of policy.

	Command or Action	Purpose
Step 23	**cac-table** *table-name* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy)# cac-table RootCacTable`	Creates or configures an admission control table.
Step 24	**match-type** *type* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy-cactable)# match-type call-priority`	Configures a new CAC table type that enables the priority of the call to be used as a criterion in CAC policy.
Step 25	**entry** *number* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy-cactable)# entry 1`	Creates or modifies an entry in a table.
Step 26	**match-value** *value* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# match-value sipp1`	Configures the match type of an admission control table.
Step 27	**action** *action-name* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete`	Specifies the action to take if this entry is chosen.
Step 28	**caller-inbound-policy** *policytab-name* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# caller-inbound-policy foo`	Configures a caller inbound SDP policy table.
Step 29	**caller-outbound-policy** *policytab-name* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# caller-outbound-policy foo`	Configures a caller outbound SDP policy table.
Step 30	**callee-inbound-policy** *policytab-name* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# callee-inbound-policy foo2`	Configures a callee inbound SDP policy table.
Step 31	**callee-outbound-policy** *policytab-name* **Example:** `host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# callee-outbound-policy foo2`	Configures a callee outbound SDP policy table.

	Command or Action	Purpose
Step 32	**exit** **Example:** `host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# exit`	Returns to the previous submode.
Step 33	**exit** **Example:** `host1/Admin(config-sbc-sbe-cacpolicy-cactable)# exit`	Returns to the previous submode.
Step 34	**complete** **Example:** `host1/Admin(config-sbc-sbe-cacpolicy)# complete`	Performs a consistency check on the CAC policy set.
Step 35	**exit** **Example:** `host1/Admin(config-sbc-sbe-cacpolicy)# exit`	Returns to the previous submode.
Step 36	**active-cac-policy-set** *number* **Example:** `host1/Admin(config-sbc-sbe)# active-cac-policy-set 1`	Enters the active CAC policy set.
Step 37	**show services sbc** *service-name* **sbe cac-policy-set** *number* **table** *number* **entry** *number* **Example:** `host1/Admin(config-sbc-sbe)# show services sbc mysbc sbe cac-policy-set 1 table RootCacTable entry 1`	Displays detailed information for a given entry in a CAC policy table.

Example of SIP SDP Attribute Passthrough

This section provides a sample configuration and output for SIP SDP Attribute Passthrough.

```
host1/Admin# config t
Enter configuration commands, one per line.  End with CNTL/Z.
host1/Admin(config)# sbc interwork
host1/Admin(config-sbc)# sbe
host1/Admin(config-sbc-sbe)# sdp-match-table matchtab1
host1/Admin(config-sbc-sbe-sdp-match-tbl)# action blacklist
host1/Admin(config-sbc-sbe-sdp-match-tbl)# match-string X-sqn
host1/Admin(config-sbc-sbe-sdp-match-tbl)# match-string X-cap
host1/Admin(config-sbc-sbe-sdp-match-tbl)# exit
host1/Admin(config-sbc-sbe)# sdp-match-table matchtab2
host1/Admin(config-sbc-sbe-sdp-match-tbl)# action blacklist
host1/Admin(config-sbc-sbe-sdp-match-tbl)# match-string X-sqn
host1/Admin(config-sbc-sbe-sdp-match-tbl)# match-string X-pc-csuites-rtp
host1/Admin(config-sbc-sbe-sdp-match-tbl)# exit
host1/Admin(config-sbc-sbe)# sdp-policy-table policytab1
```

```
host1/Admin(config-sbc-sbe-sdp-policy-tbl)# match-table matchtab1
host1/Admin(config-sbc-sbe-sdp-policy-tbl)# exit
host1/Admin(config-sbc-sbe)# sdp-policy-table policytab2
host1/Admin(config-sbc-sbe-sdp-policy-tbl)# match-table matchtab2
host1/Admin(config-sbc-sbe-sdp-policy-tbl)# exit
host1/Admin(config-sbc-sbe)# cac-policy-set 1
host1/Admin(config-sbc-sbe-cacpolicy)# first-cac-table 1
host1/Admin(config-sbc-sbe-cacpolicy)# first-cac-scope global
host1/Admin(config-sbc-sbe-cacpolicy)# cac-table 1
host1/Admin(config-sbc-sbe-cacpolicy-cactable)# match-type src-adjacency
host1/Admin(config-sbc-sbe-cacpolicy-cactable)# entry 1
host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# match-value sipp1
host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# action cac-complete
host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# caller-inbound-policy policytab1
host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# caller-outbound-policy policytab1
host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# callee-inbound-policy policytab2
host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# callee-outbound-policy policytab2
host1/Admin(config-sbc-sbe-cacpolicy-cactable-entry)# exit
host1/Admin(config-sbc-sbe-cacpolicy-cactable)# exit
host1/Admin(config-sbc-sbe-cacpolicy)# complete
host1/Admin(config-sbc-sbe-cacpolicy)# exit
host1/Admin(config-sbc-sbe)# active-cac-policy-set 1
```

This section provides a sample configuration and output for SIP SDP Attribute Passthrough.

```
host1/Admin(config-sbc-sbe)# do show services sbc interwork sbe cac-policy-set 1 table 1
entry 1
SBC Service "interwork"
Policy set 1 table 1 entry 1
  Match value               sipp1
  Action                    CAC policy complete
  Max calls                 Unlimited
  Max call rate             Unlimited
  Max in-call rate          Unlimited
  Max out-call rate         Unlimited
  Max registrations         Unlimited
  Max reg. rate             Unlimited
  Max bandwidth             Unlimited
  Max channels              Unlimited
  Transcoder                Allowed
  Caller privacy setting    Never hide
  Callee privacy setting    Never hide
  Early media               Allowed
  Early media direction     Both
  Early media timeout       0
  Restrict codecs to list   default
  Restrict caller codecs to list   default
  Restrict callee codecs to list   default
  Media bypass              Allowed
  SRTP Transport            Not Set
  Callee hold setting       Standard
  Caller hold setting       Standard
  Number of calls rejected by this entry    0
  Caller inbound SDP policy                 policytab1
  Caller outbound SDP policy                policytab1
  Callee inbound SDP policy                 policytab2
  Callee outbound SDP policy                policytab2
```