

ACS Rulebase Configuration Mode Commands

Command Modes

The ACS Rulebase Configuration Mode is used to configure Active Charging Service (ACS) rulebases.

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- action priority, on page 3
- active-charging rf, on page 6
- adc notify, on page 8
- app-notification, on page 9
- bandwidth default-policy, on page 10
- billing-records, on page 11
- cca diameter requested-service-unit, on page 12
- cca quota, on page 14
- cca quota time-duration algorithm, on page 15
- cca radius accounting interval, on page 17
- cca radius charging context, on page 18
- cca radius user-password, on page 19
- charging-action-override, on page 20
- charging-rule-optimization, on page 21
- check-point accounting, on page 22
- constituent-policies, on page 23
- content-filtering category policy-id, on page 25
- content-filtering flow-any-error, on page 26
- content-filtering mode, on page 27
- credit-control-group, on page 28
- description, on page 29
- dynamic-rule order, on page 30

- edr edr-dcca-fh, on page 31
- edr p2p, on page 32
- edr nemo-call, on page 33
- edr sn-charge-volume, on page 34
- edr suppress-zero-byte-records, on page 36
- edr transaction-complete, on page 36
- edr voip-call-end, on page 38
- egcdr inactivity-meter, on page 39
- egcdr cdr-encoding, on page 39
- egcdr tariff, on page 41
- egcdr threshold, on page 42
- egcdr time-duration algorithm, on page 43
- end, on page 45
- exit, on page 45
- extract-host-from-uri, on page 45
- firewall dos-protection, on page 46
- firewall flooding, on page 49
- firewall icmp-destination-unreachable-message-threshold, on page 50
- firewall max-ip-packet-size, on page 51
- firewall mime-flood, on page 52
- firewall no-ruledef-matches, on page 54
- firewall policy, on page 56
- firewall priority, on page 57
- firewall tcp-first-packet-non-syn, on page 60
- firewall tcp-idle-timeout-action, on page 61
- firewall tcp-reset-message-threshold, on page 62
- firewall tcp-syn-flood-intercept, on page 63
- flow any-error, on page 64
- flow control-handshaking, on page 66
- flow end-condition, on page 67
- flow limit-across-applications, on page 69
- flow rtsp-all-pkts, on page 71
- fw-and-nat default-policy, on page 72
- http header-parse-limit, on page 73
- ip readdress, on page 74
- ip reassembly-timeout, on page 75
- ip reset-tos, on page 76
- ip ttl, on page 76
- nat binding-record, on page 77
- nat policy, on page 78
- nat suppress-aaa-update call-termination, on page 80
- override-control, on page 80
- p2p dynamic-flow-detection, on page 83
- pcp service, on page 84
- post-processing dynamic, on page 85
- post-processing policy, on page 86

- post-processing priority, on page 87
- qos-renegotiate timeout, on page 89
- radius threshold, on page 90
- retransmissions-counted, on page 91
- ran bandwidth optimize, on page 91
- route priority, on page 92
- rtp dynamic-flow-detection, on page 96
- rtsp initial-bytes-limit, on page 97
- ruledef-parsing, on page 98
- tcp 2msl-timeout, on page 99
- tcp rst-robustness, on page 100
- tcp check-window-size, on page 100
- tcp mss, on page 101
- tcp out-of-order-timeout, on page 102
- tcp packets-out-of-order, on page 102
- tcp proxy-mode, on page 105
- tcp window-size, on page 107
- tethering-detection, on page 107
- tft-notify-ue-def-bearer, on page 109
- timestamp rounding, on page 110
- tpo default-policy, on page 111
- traffic-optimization, on page 111
- transactional-rule-matching, on page 112
- transport-layer-checksum, on page 113
- udr threshold, on page 114
- udr trigger, on page 115
- uidh-insertion, on page 117
- url-preprocessing, on page 118
- video optimization-preprocessing cae-readdressing, on page 119
- websocket flow-detection, on page 119
- wtp out-of-order-timeout, on page 120
- wtp packets-out-of-order, on page 120
- xheader-encryption, on page 121

action priority

This command allows you to configure the action priority for a ruledef / group-of-ruledefs in the current rulebase.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

action priority *action_priority* **{ [dynamic-only [adc [mute]] | static-and-dynamic | timedef** *timedef_name* **] { group-of-ruledefs** *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[monitoring-key** *monitoring_key* **] [description** *description* **] }**
no action priority *action_priority*

no

If previously configured, deletes the specified action priority configuration from the current rulebase.

priority *action_priority*

Specifies a priority for the specified ruledef / group-of-ruledefs in the current rulebase.

action_priority must be unique in the current rulebase, and must be an integer from 1 through 65535.

The priority controls the order in which this instance of the CLI command will be examined. Lower numbered priorities are examined first.

Up to 2048 instances may be configured, totaled among all rulebases in releases prior to 21.1. In 21.1 and later releases, up to 2500 instances can be configured.



Important If there are any changes to action priority and the Override Control/Inheritance feature is enabled, then execute the CLI command "**update active-charging override-control rulebase-config**". For more information on this command, see the *Command Line Interface Reference*.

dynamic-only

Enables matching of dynamic rules with static rules for this action priority on a flow.

Configuring the **dynamic-only** keyword causes the configuration to be defined, but not enabled. If enabled, the action associated with this option will not be matched against a flow until it is enabled from a dynamic charging interface like Gx. Gx can disable or enable this action entry in the rulebase using Gx messages.

Default: Disabled

adc

Specifies the ruledef to-be given as ADC rule. This keyword is optional and only visible when configured with the **dynamic-only** keyword.

Default: Disabled

mute

Disables application reporting to PCRF. This keyword is optional and visible only after configuring the **adc** keyword.

Default: Disabled

static-and-dynamic

The static-and-dynamic option causes the configuration to be defined and enabled, and allows a dynamic protocol (such as the Gx interface) to disable or re-enable the configuration.

Default: Enabled



Important When R7 Gx is enabled, "static-and-dynamic" rules behave exactly like "dynamic-only" rules. That is, they must be activated explicitly by the Policy and Charging Rules Function (PCRF). When Gx is not enabled, "static-and-dynamic" rules behave exactly like static rules.

timedef *timedef_name*



Important This keyword is only available in StarOS 8.1 and StarOS 9.0 and later releases.

Associates the specified time definition with the ruledef / group-of-ruledefs. Timedefs activate or deactivate ruledefs / groups-of-ruledefs, making them available for rule matching only when they are active.

timedef_name must be the name of a timedef, and must be an alphanumeric string of 1 through 63 characters.

A timedef can be used with several ruledefs / group-of-ruledefs. When a packet is received, and a ruledef / group-of-ruledefs is eligible for rule matching, if a timedef is associated with the ruledef / group-of-ruledefs, before rule matching the packet-arrival time is compared with the timeslots configured in the timedef. If the packet arrived in any of the timeslots configured in the associated timedef, rule matching is undertaken, else the next ruledef / group-of-ruledefs is considered.



Important The time considered for timedef matching is the system's local time.

ruledef *ruledef_name*

Adds the specified ruledef to the current rulebase.

ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

If the specified ruledef does not exist, there will be no ruledef triggers for this action priority within the current rulebase.



Important If the ruledef specified here is deleted or is not configured, the system accepts it without applying any ruledef under current rulebase for this action priority.

group-of-ruledefs *ruledefs_group_name*

Adds the specified group-of-ruledefs to the current rulebase.

ruledefs_group_name must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

When a group-of-ruledefs is specified, if any of the ruledefs within the group matches, the specified charging-action is applied, any more of the action instances are not processed.



Important If the group-of-ruledefs specified here is deleted or is not configured, the system accepts it without applying any ruledefs under current rulebase for this action priority.

charging-action *charging_action_name*

Specifies the charging action.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

If the specified charging action does not exist, there will be no charging action triggers for this action priority within the current rulebase.



Important If the charging action specified here is not configured or is later deleted, the system will not apply any charging action under current rulebase for this action priority.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

monitoring_key must be an integer from 1 through 4000000000.

description *description*

Adds specified text to the rule and action.

description must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure action priorities for ruledefs / group-of-ruledefs in a rulebase.

This CLI command can be entered multiple times to specify multiple ruledefs and charging actions. The ruledefs are examined in priority order, until a match is found and the corresponding charging action is applied.

Example

The following command assigns a rule and action with the action priority of *23*, a ruledef named *test*, and a charging action named *test1* to the current rulebase:

```
action priority 23 ruledef test charging-action test1
```

active-charging rf

This command allows you to enforce default rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting.

Important This command is customer specific. For more information contact your Cisco account representative.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

active-charging rf { rating-group-override *rating_group* **| service-id-override** *service_id* **}**
{ default | no } active-charging rf { rating-group-override | service-id-override }

default

Configures this command with its default setting.

Default: Override configuration is disabled; same as no.

no

Disables the override configuration.

no active-charging rf rating-group-override: Rating group override will not be enforced on the PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own rating group, it will continue to use that.

no active-charging rf service-id-override: Service ID override will not be enforced on the PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own service ID, it will continue to use that.

rating-group-override ***rating_group***

Enforces the specified rating group on all PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own rating group, it will be overridden by the specified rating group.

rating_group must be an integer from 1 through 65535.

service-id-override ***service_id***

Enforces the specified service ID on all PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own service ID, it will be overridden by the specified service ID.

service_id must be an integer from 1 through 65535.

Usage Guidelines

Use this command to enforce a specific rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting. As this CLI configuration is applied at the rulebase level, all the APNs that have the current rulebase defined will inherit the configuration.

Example

The following command configures the service ID *100*:

```
active-charging rf service-id-override 100
```

adc notify

This command allows you to configure a single "application start" or "application stop" notification for the ADC flow matching per rule is sent to the PCRF.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
[no] adc notify [once]
```

no

Disables the ADC notifications and ADC notifications are sent as per default behavior.

adc

Configures the ADC notifications.

notify

Configures the application notification. If this keyword is not configured, ADC notifications are sent as per default behavior.

once

Configures the application notification only once. PCRF takes the priority.

Usage Guidelines

Use this command to configure a single "application start" or "application stop" notification for the ADC flow matching per rule is sent to the PCRF. If this CLI is configured and the PCRF sends the custom mute notification, then the PCRF notification takes precedence over the standard behavior for reporting the notification.

Important If the CLI command **adc notify once** is configured at the rulebase, the converse **no adc notify** does not have any impact. To converse the CLI impact, do either of the following tasks:

- Switch the rulebase in which the CLI command **adc notify** once is not configured.
- Send the **custom unmute** for that particular dynamic rule.

Example

The following command configures a single "application start" or "application stop" notification for the ADC flow matching per rule is sent to the PCRF:

```
adc notify once
```

app-notification

This command enables APP_STOP buffering.

Note In 21.3.12 and later releases, the **notify** command is deprecated. The **notify** command has been replaced by the **app-notification** command.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
[ no ] adc app-notification { once-per-app [ once-per-ipflow ] | once
per-ipflow [ once-per-app ] }
```

no

Disables the ADC notifications and ADC notifications are sent as per default behavior.

adc

Configures the ADC notifications.

app-notification

This command enables APP_STOP buffering. A maximum of five APP_STOP messages is buffered per flow.

once-per-app

Notifies APP_START or APP_STOP notification once per App ID.

once-per-ipflow

Notifies APP_START or APP_STOP notifications per App ID per IP flow.

Usage Guidelines

Use this command to enable APP_STOP buffering. This command should be applied when the flow is being created. Changes to the configuration will be applied to the newly created flows.

The APP_STOP is buffered at a flow-level. Therefore, there is an increase in memory for every rule stored in the session manager.



Note This command does not affect the Custom-Mute feature as it is implemented at a flow-level.

bandwidth default-policy

This command allows you to configure the default bandwidth policy for the current rulebase.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

bandwidth default-policy *bandwidth_policy_name* **[fallback-enabled]**
no bandwidth default-policy

no

If previously configured, deletes the bandwidth default-policy configuration from the current rulebase.

bandwidth_policy_name

Specifies the default bandwidth policy for the current rulebase.

bandwidth_policy_name must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters.

fallback-enabled

Determines whether policy under rulebase can be applied as a fallback value. Fallback is disabled by default.

Usage Guidelines

Use this command to configure the default bandwidth policy for a rulebase.

For subscribers using the current rulebase, the default bandwidth policy will be used if in the APN/subscriber profile the **default active-charging bandwidth-policy fallback-enabled** command is configured, or no bandwidth policy is configured.

Example

The following command configures a bandwidth policy named *standard* for the rulebase:

```
bandwidth default-policy standard
```

billing-records

This command allows you to configure the type of billing to be performed for subscriber sessions.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
billing-records { egcdr | radius | rf | udr udr-format udr_format_name [
failure-handling-udr-format udr_format_name ] } +
no billing-records
```

no

If previously configured, deletes the billing-records configuration from the current rulebase.

egcdr

Generates an enhanced G-CDR (eG-CDR) for GGSN / P-GW-CDR for P-GW, and/or UDR with specified format on the occurrence of an interim trigger condition at the end of a subscriber session, or an SGSN-to-SGSN handoff.

radius

Generates postpaid RADIUS accounting records at the start and end of a subscriber session, and on the occurrence of an interim trigger condition. RADIUS accounting records are generated for each content ID.



Important In the GGSN, if in the APN configuration the "accounting-mode" is set to "none", the system continues to send ACS-generated RADIUS accounting messages. In the PDSN, if in the subscriber default configuration the "accounting-mode" is set to "none", the system does not send any RADIUS accounting messages (including ACS accounting messages).

rf

Enables Rf accounting.

Rf accounting is applicable only for dynamic and predefined rules that are marked for it. Dynamic rules have a field offline-enabled to indicate this. To mark a predefined rule as offline-enabled, use this keyword and the **billing-action** command in the ACS Charging Action Configuration Mode.

udr udr-format *udr_format_name*

Generates UDRs with specified the format on the occurrence of an interim trigger condition, at the end of a subscriber session, or a handoff.

udr_format_name must be the name of an UDR format, and must be an alphanumeric string of 1 through 63 characters.

+

Indicates that more than one of the keywords can be entered in a single command.

Usage Guidelines

Use this command to generate enhanced G-CDRs (eG-CDRs), P-GW-CDR for P-GW, RADIUS CDRs and/or UDRs for billing records. The format of eG-CDRs for the default GTPP group is controlled by the **inspector** command in the Context Configuration Mode.

If, in the APN configuration, the "accounting-mode" is set as default (GTPP), and in the rulebase configuration "billing-records egcdr" is configured, both G-CDRs and eG-CDRs are generated if configured. If, in the APN, the accounting-mode is set to "none" G-CDRs will not be generated.

Example

The following command sets the billing record to UDR with UDR format named *udr_format1*:

```
billing-records udr udr-format udr_format1
```

cca diameter requested-service-unit

This command allows you to specify the Diameter sub-AVPs to be included in the Diameter group AVP "Requested-Service-Unit" sent with DCCA Credit Control Requests (CCRs).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
cca diameter requested-service-unit sub-avp { time cc-time duration | units
 cc-service-specific-units charging_unit | volume { cc-input-octets bytes |
cc-output-octets bytes | cc-total-octets bytes } + }
no cca diameter requested-service-unit sub-avp
```

no

No sub-AVPs are included in the Requested-Service-Unit grouped AVP.

time cc-time *duration*

Specifies requested service unit for charging time duration in seconds in included sub-AVP.

duration specifies charging time in seconds, and must be an integer from 1 through 4000000000.

units cc-service-specific-units *charging_unit*

Specifies requested service unit by service specific units in bytes/packets in included sub-AVP.

charging_unit specifies service-specific charging unit and must be an integer from 1 through 4000000000.

volume { cc-input-octets *bytes* | cc-output-octets *bytes* | cc-total-octets *bytes* } +

Specifies requested service unit for charging octets by input, output, and total volume in included sub AVP.

- **cc-input-octets**: Specifies input charging octets.
- **cc-output-octets**: Specifies output charging octets.
- **cc-total-octets**: Specifies total charging octets.
- *bytes*: Specifies volume in bytes and must be an integer from 1 through 4000000000.

+: Indicates that more than one of the previous keywords can be entered within a single command.

Usage Guidelines

Use this command to include sub-AVPs based on time, volume, and service specific unit in the "Requested-Service-Unit" grouped AVP with CCRs through Gy interface.

Example

The following command sets the time based sub-AVP with charging duration of 45 seconds in "Requested-Service-Unit" group AVP on DCCA CCRs:

```
cca diameter requested-service-unit sub-avp time cc-time 45
```

cca quota

This command allows you to configure various time- and threshold-based quotas in the Prepaid Credit Control Service (Credit Control Application).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

cca quota { holding-time *holding_time* **content-id** *content_id* **| retry-time** *retry_time* **[max-retries** *retries* **] }**
{ default | no } cca quota { holding-time content-id *content_id* **| retry-time }**

holding-time *holding_time*

Specifies the value for the Quota Holding Time (QHT). QHT is used with both time-based and volume-based quotas. After *holding_time* seconds has passed without user traffic, the quota is reported back and the charging stops until new traffic starts.

holding_time must be an integer from 1 through 4000000000.

content-id *content_id*

Specifies the content ID (Rating group AVP) to use for the Quota holding time for the current rulebase.

content_id is the content ID specified for credit control service in ACS.

In 12.1 and earlier releases, *content_id* must be an integer from 1 through 65535.

In 12.2 and later releases, *content_id* must be an integer from 1 through 2147483647.

retry-time *retry_time* [max-retries *retries*]

Specifies the retry time for the quota request, in seconds.

retry_time must be an integer from 0 through 86400. To disable this assign 0.

Default: 60

This parameter defines the maximum frequency at which the Credit-Control Application (CCA) tries to obtain quota for a subscriber passing traffic for a category with no/exhausted quota.

For a subscriber not passing traffic, the CCA will not try to obtain quota (except once at session start time, if so configured). The quota request from the no quota state is sent in response to user packets only (never based on a timer).

When subscriber hits a charging action that is a flow redirect, the operator can optionally specify that this redirection shall clear the retry-time timer.

This allows the immediately following chargeable user traffic to trip a quota request, even if it would otherwise have been subject to the retry time limit. Such configuration allows quite a large value for retry-time in quota charging or a top-up scenario.

max-retries *retries* configures the maximum number of retries allowed for blockedlisted categories. This option has a default value of 65535 retries (the maximum value).

retries must be an integer from 1 through 65535. To disable the **max-retries** CLI command, use the **cca quota retry-time** *retry_time* CLI command.

To disable the **cca quota retry-time** command, use the **no** variant of the command, that is to say **no cca quota retry-time**.

Usage Guidelines

Use this command to set the prepaid credit control quotas.

cca quota retry time allows an operator to set the amount of time that the ACS waits before it retries the prepaid server for a content ID for which quota was exhausted earlier.

When the server sends the quota holding time (QHT) it has highest priority to use that QHT regardless of the value configured in the rulebase or Credit Control Application Configuration Mode. QHT configured here has the second priority for the content ID (rating group) configured here.

If the QHT is not available from the server or rulebase configuration mode, the QHT values configured via the Credit Control Application Configuration Mode are used.

Example

The following command configures the prepaid credit control request retry time to *30* seconds:

```
cca quota retry-time 30
```

The following command specifies the system to use the QHT value configured in the Credit Control Application Mode:

```
no cca quota holding-time content-id 1
```

The following command specifies the system to ignore the QHT value configured in the Credit Control Application Mode:

```
default cca quota holding-time content-id 1
```

The following command configures the prepaid credit control request retry time to *60* seconds and the maximum number of retries to *65535*:

```
default cca quota retry-time max-retries
```

cca quota time-duration algorithm

This command allows you to specify the algorithm to compute time duration for Prepaid Credit Control Application quotas in the current rulebase.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

cca quota time-duration algorithm { consumed-time *seconds* **[plus-idle] | continuous-time-periods** *seconds* **| parking-meter** *seconds* **} [content-id** *content_id* **]**
default cca quota time-duration algorithm
no cca quota time-duration algorithm { consumed-time | continuous-time-periods | parking-meter } [content-id *content_id* **]**

no

If previously configured, deletes the quota time-duration algorithm configuration from the current rulebase.

default

Configures this command with its default setting.

consumed-time *seconds*

Specifies the Quota Consumption Time (QCT) in seconds. QCT is used with active time-based quotas and to determine chargeable time envelopes for consuming time quota.

seconds must be an integer from 1 through 4294967295.

Default: 0 (disabled)

A time envelope is the basis for reporting active usage. For each time envelope, the quota consumption includes the last QCT (duration between first packet and last packet + QCT).

plus-idle

Specifies the idle time for QCT.

When used along with **consumed-time** it indicates the active usage + idle time, when no traffic flow occurs.

continuous-time-periods *seconds*

Specifies the charging quota continuous period, in seconds.

seconds must be an integer from 1 through 4294967295.

Default: 0 (disabled)

The Continuous Time Periods (CTP) mechanism constructs time-envelopes from consecutive base time intervals in which traffic has occurred up to and including a base time interval which contains no traffic. As with Quota-Consumption-Time envelopes, the end of an envelope can only be determined "retrospectively". Again, as with Quota-Consumption-Time, the envelope for CTP includes the last base time interval (the one which contained no traffic).

parking-meter *seconds*

Specifies the Parking Meter (PM) period, in seconds, for a particular rating group.

seconds must be an integer from 1 through 4294967295.

Default: 0 (disabled)

This mechanisms utilizes time quota, but instead of consuming linearly—once a decision to consume has been taken—the granted quota is consumed discretely in "chunks" of the base time interval at the start of each base time interval. Traffic is then allowed to flow for the period of the consumed quota.

The time interval seconds defines the length of the Parking Meter. A time-envelope corresponds to exactly one PM (and thus to one base time interval).

content-id *content_id*

Specifies the content ID (Rating group AVP) to use for the CCA Quota time duration algorithm selection in the current rulebase.

content_id is the content ID specified for credit control service in ACS.

In 12.1 and earlier releases, *content_id* must be an integer from 1 through 65535.

In 12.2 and later releases, *content_id* must be an integer from 1 through 2147483647.

Usage Guidelines

Use this command to set the various time charging algorithms/schemes for prepaid credit control charging.

If operator chooses **parking-meter** *seconds* style charging, then time is billed in *seconds* chunks.

Example

The following command configures the QCT to consumed-time duration of *400* seconds:

```
cca quota time-duration algorithm consumed-time 400
```

cca radius accounting interval

This command allows you to configure how often interim updates are generated by the RADIUS Credit Control Application to be sent to the prepaid server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

cca radius accounting interval *interval*
{ default | no } cca radius accounting interval

default

Configures the command with its default setting.

Default: Disabled; same as **no cca radius accounting interval**

no

Disables interim updates.

interval

Specifies the time interval, in seconds, between interim updates generated by the RADIUS Credit Control Application.

interval must be an integer from 1 through 3600.

Default: 1 (Disabled)

Usage Guidelines

Use this command to specify the RADIUS accounting interval between accounting of a prepaid subscriber. The same parameters are applicable for RADIUS server group.

Example

The following command defines RADIUS accounting interval of *20* seconds for RADIUS prepaid service in the rulebase:

```
cca radius accounting interval 20
```

cca radius charging context

This command allows you to specify the RADIUS servers used for the current rulebase when RADIUS credit control is enabled.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
cca radius charging context vpn_context [ group server_group_name ]
no cca radius charging context
```

no

RADIUS credit control will not be performed.

vpn_context

Specifies the charging context where RADIUS prepaid charging parameters are configured.

vpn_context must be an alphanumeric string of 1 through 79 characters.

group *server_group_name*

Specifies the RADIUS server group.

server_group_name must be the name of a RADIUS server group, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify the RADIUS charging context where RADIUS prepaid charging parameters are configured. The same parameters are applicable for RADIUS server group.

Example

The following command defines RADIUS charging context *prepaid_rad1* for RADIUS prepaid charging in the rulebase:

```
cca radius charging context prepaid_rad1
```

cca radius user-password

This command allows you to configure the value to use for the "User-Password" attribute in RADIUS messages sent to the prepaid server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
cca radius user-password [ encrypted ] password password
no cca radius user-password
```

no

If previously configured, deletes the RADIUS prepaid service user password configured in the current rulebase.

[encrypted] password *password*

Specifies the password for prepaid services within the current rulebase.

In 12.1 and earlier releases, *password* must be an alphanumeric string of 1 through 63 characters with or without encryption.

In 12.2 and later releases, *password* must be an alphanumeric string of 1 through 63 characters without encryption, and 1 through 132 characters with encryption enabled.

The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password**

keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

Usage Guidelines

Use this command to specify the RADIUS user password for prepaid services within the current rulebase.

Example

The following command configures the user password as *user_123* without encryption in the current rulebase:

```
cca radius user-password password user_123
```

charging-action-override

This command allows you to enable/disable overriding charging parameters of static rule with those of an ip-any rule or a specified dynamic rule.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
charging-action-override custom1 [ use-rule dynamic_rule_name ]
{ default | no } charging-action-override
```

default

Configures this command with its default setting.

Default: Disables overriding charging parameters of static rule with those of an ip-any or a specified dynamic rule.

no

Disables overriding charging parameters of static rule with those of an ip-any or a specified dynamic rule.

custom1

Specifies overriding Online/Offline, Service ID, Content ID, Flow Control, ARP, and QCI.

use-rule *dynamic_rule_name*

Optional: Specifies the dynamic rule to inherit charging parameters from. If a dynamic rule name is not specified, the charging properties will be inherited from any dynamic rule.

dynamic_rule_name specifies name of the dynamic rule, and must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage Guidelines

Use this command to enable/disable overriding charging parameters of static rule with those of a dynamic ip-any rule or a specified dynamic rule.

Example

The following command specifies to enable overriding charging parameters of static rule with those of a dynamic rule named *test*:

```
charging-action-override custom1 use-rule test
```

charging-rule-optimization

This command allows you to configure the internal optimization level to use, for improved performance, when evaluating each instance of the **action priority** command.



Important In StarOS 14.0 and later releases, this command is deprecated. In StarOS 14.0 and later releases, rule optimization is always enabled with the optimization level set to high.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
charging-rule-optimization { high | low | medium }
default charging-rule-optimization
```

default

Configures this command with its default setting.

Default: In 11.0 and later releases: **high** In 10.0 and earlier releases: **low**

high

Enables the highest level of optimization with high memory utilization.

low

Enables minimal level of optimization with minimal memory utilization.

medium



Important In 11.0 and later releases, the **medium** keyword is deprecated.

Enables medium level of optimization with moderate memory utilization.

Usage Guidelines Use this command to specify the level of internal optimization for improved performance when evaluating each instance of the **action priority** command.

Both the high and medium options cause re-organization of the entire memory structure whenever any change is made, such as on the addition of an **action priority** command.

Example

The following command specifies the highest optimization level for rule search and matching in the rulebase:

```
charging-rule-optimization high
```

check-point accounting

This command configures micro checkpoint syncup timer for ICSR and Session Recovery for Rf-Gy synchronization.

Product GGSN

P-GW

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
check-point accounting sync-timer { icsr | sr } timer_value [ sr | icsr ]
timer_value
no check-point accounting sync-timer { icsr | sr }
```

no

If the micro checkpoint syncup timer is already configured, then the **no** variant will delete the configuration.

sr *timer_value*

Configures micro check-pointing timer for Session Recovery (SR). By default, the session recovery check-pointing will be done on 8 seconds.

timer_value: Time configured will be in multiples of 2 seconds. Note that the timer value less than 4 seconds and greater than 60 seconds will not be accepted.

icsr *timer_value*

Configures micro check-pointing timer for ICSR. By default, the ICSR check-pointing will be done on 18 seconds.

timer_value: Time configured will be in multiples of 2 seconds. Note that the timer value less than 4 seconds and greater than 60 seconds will not be accepted.

Usage Guidelines

Use this command to configure micro checkpoint syncup timer for ICSR and Session Recovery. Micro Checkpoint Sync-up timer is an internal timer utilized by Rf and Gy modules to check point corresponding billing information.

Releases prior to 17.0, micro checkpoint sync-up timer was hardcoded with a value of 18 seconds for ICSR and 8 seconds for Session Recovery (SR). In 17.0 and later releases, the micro checkpoint sync-up timer is made configurable with an expectation that it be set at a value as low as 4 seconds. The timer value is reduced to ensure the accurate billing information during the ICSR or SR switchover event.

This CLI is available at both active charging service level and rulebase level. If the timer value is configured at both service and rulebase level, then the service level value will be overridden with rulebase level values.

This feature provides the operator with the flexibility to provision timer for accurate billing information in case of session recovery or ICSR switchover. However, this is a performance impacting feature and the impact of the micro checkpoint sync timer reduction needs to be carefully considered by the operator before provisioning a lower value.

Example

The following command configures the micro checkpoint syncup timer for Session Recovery as *8* seconds:

```
check-point accounting sync-timer sr 8
```

constituent-policies

This command allows you to configure the Bandwidth, Content Based Billing (CBB), and Firewall/Firewall-and-NAT constituent policies. The combination of the values of all three policies will uniquely identify the associated rulebase.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

constituent-policies { bandwidth-policy *bandwidth_policy_name* **| cbb-policy** *cbb_policy_name* **| firewall-policy** *fw_policy_name* **| fw-and-nat-policy** *fw_nat_policy_name* **} +**
no constituent-policies

no

If previously configured, deletes the constituent-policies configuration from the current rulebase.

bandwidth-policy *bandwidth_policy_name*

Specifies the Bandwidth policy.

bandwidth_policy_name must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters.

cbb-policy *cbb_policy_name*

Specifies the Content Based Billing (CBB) policy.

cbb_policy_name must be the name of a CBB policy, and must be an alphanumeric string of 1 through 63 characters.

firewall-policy *fw_policy_name*



Important This keyword is customer specific. For more information, please contact your Cisco account representative.

Specifies the Stateful Firewall policy.

fw_policy_name must be the name of a Stateful Firewall policy, and must be an alphanumeric string of 1 through 63 characters.

fw-and-nat-policy *fw_nat_policy_name*



Important This keyword is customer specific, and is only available in StarOS 8.1 and in StarOS 9.0 and later releases.

Specifies the Firewall-and-NAT policy.

fw_nat_policy_name must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the bandwidth, CBB, and Firewall/Firewall-and-NAT constituent policies that will identify the rulebase. The combination of the values of all three policies will uniquely identify the rulebase associated.

Example

The following command configures the constituent bandwidth policy named *test123*:

```
constituent-policies bandwidth-policy test123
```

content-filtering category policy-id

This command allows you to configure the Content Filtering Category Policy Identifier for Policy-based Content Filtering support in the current rulebase.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
content-filtering category policy-id cf_policy_id
no content-filtering category policy-id [ cf_policy_id ]
```

no

If previously configured, deletes the configuration from the current rulebase.

In StarOS 8.1 and later releases, optionally the policy ID can be specified. If the specified policy ID is invalid, or is not configured in the rulebase, an error message is displayed. If no policy ID is specified, whatever policy is configured, if any, is removed from the rulebase.

content-filtering category policy-id *cf_policy_id*

Configures the specified Content Filtering Category Policy in the current rulebase.

cf_policy_id must be the ID of an existing Content Filtering Category Policy, and must be an integer from 1 through 4294967295.

Important If the specified Content Filtering Category Policy does not exist, all packets will be passed regardless of the categories/actions determined for such packets.

Important The category policy ID that is configured using the **category policy-id** *cf_policy_id* command in the APN/Subscriber Configuration Mode prevails over this configuration.

Usage Guidelines

Use this command to configure the Content Filtering Category Policy ID for Policy-based Content Filtering support in the rulebase.

The Content Filtering Category Policy is created/deleted in the ACS Configuration Mode, and is configured in the Content Filtering Policy Configuration Mode.

Example

The following command configures the Content Filtering Category Policy ID *101* in the rulebase:

```
content-filtering category policy-id 101
```

content-filtering flow-any-error

This command allows you to specify action to take on Content Filtering packets in the case of ACS error scenarios.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
content-filtering flow-any-error { deny | permit }
default content-filtering flow-any-error
```

default

Configures this command with its default setting.

Default: **permit**

deny

Configures flow-any-error configuration as deny.

All the denied packets will be accounted for by the **discarded-flow-content-id** configuration in the Content Filtering Policy Configuration Mode. This content ID will be used to generate UDRs for packets denied via content filtering.

permit

Configures flow-any-error configuration as permit.

Usage Guidelines

Use this command to allow/discard content filtering packets in case of ACS error scenarios.

Example

The following command allows content filtering packets in case of an ACS error:

```
content-filtering flow-any-error permit
```

content-filtering mode

This command allows you to enable/disable the specified Category-based Content Filtering mode in the current rulebase.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
content-filtering mode { category { static-and-dynamic | static-only } |
 server-group cf_server_group }
no content-filtering mode
```

no

If previously configured, deletes the content-filtering mode configuration from the current rulebase. Content filtering will not to be performed for the current rulebase. This is the default setting.

category { static-and-dynamic | static-only }

Specifies the Category-based Content Filtering mode.

- **static-only**: Configures Category-based Content Filtering in static only mode, wherein all URLs are compared against an internal database to categorize the requested content.

  Using Category-based Content Filtering support requires configuration of the **require active-charging content-filtering category** command in the Global Configuration Mode.

- **static-and-dynamic**: Configures Category-based Content Filtering in Static-and-Dynamic mode, wherein a static rating of the URL is first performed, and only if the static rating fails to find a match, dynamic rating of the content that the server returns is then performed.



Important Before enabling static-and-dynamic rating in the rulebase, it must be enabled at the global level as the resources required for dynamic rating are allocated at the global level. To enable static-and-dynamic rating at the global level, in the Global Configuration Mode use the **require active-charging content-filtering category static-and-dynamic** command.

server-group *cf_server_group*

Enables and configures the Content Filtering Server Group (CFSG) mode within the rulebase to manage an external content filtering server with an Internet Content Adaptation Protocol (ICAP) client system.

cf_server_group must be the name of a CFSG, and must be unique, and must be an alphanumeric string of 1 through 63 characters.

If configured, ACS attempts to establish TCP connections to every server in the named group.

Usage Guidelines

Use this command to enable and apply the content filtering mode in the rulebase to manage a content filtering server with an ICAP client system.

Example

The following command enables the content filtering mode for external content filtering server group *CF_Server1* in the rulebase:

```
content-filtering mode server-group CF_Server1
```

The following command enables the category based static and dynamic content filtering mode for in the rulebase:

```
content-filtering mode category static-and-dynamic
```

credit-control-group

Configures the credit control group to be used for subscribers who use this rulebase.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

credit-control-group *cc_group_name*

no credit-control-group

no

Removes the credit-control group configuration from the current rulebase, if previously configured. This is the default setting.

cc_group_name

Specifies name of the credit-control group as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify the desired CC group whenever the rulebase is selected during the subscriber session setup. This is an optional CLI configuration, and used only when customized Assume Positive behavior is required for subscribers. This CLI configuration is applicable only during the session setup. Mid-session change in the CC group is not allowed.

The **credit-control-group cc-group-name** command is used to specify a credit-control group name association to the rulebase. The **no credit-control-group** CLI is to remove the association. The default setting is **no credit-control-group**.

If this CLI command is configured, the selection of the CC group is based on the following precedence order.

- PCRF provided CC group
- AAA provided CC group
- Rulebase configured CC group
- Subscriber Profile/APN selected CC group
- Default Credit-Control group

For example, if a CC group is configured in the rulebase then this CC group has higher precedence over the CC group value specified in the Subscriber/APN profile.

If the CC group configuration is not present in the rulebase, the default subscriber/APN profile configuration is applied.

Example

The following command configures the association of a credit-control group named *test* for the current rulebase:

```
credit-control-group test
```

description

Allows you to enter descriptive text for this configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
description text
no description
```

no

Clears the description for this configuration.

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines The description should provide useful information about this configuration.

dynamic-rule order

This command allows you to specify whether dynamic rules are matched before statically configured rules.

Product GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
dynamic-rule order { always-first | first-if-tied }
no dynamic-rule order
```

no

If previously configured, changes the dynamic-rule order configuration to its default behavior. By default, dynamic rules are matched against the flow prior to static or predefined rules.

always-first

Specifies to match all the dynamic rules against the flow prior to any static rule. This is the default value.

first-if-tied

Specifies to match rules against the flow based on their priority with the condition that dynamic rules match before a static rule of the same priority.

A rule is a combination of a ruledef, charging action, and precedence. Static rules are defined by the **action** CLI command in the ACS Rulebase Configuration Mode, and are applicable to all subscribers that are associated with the rulebase. Dynamic rules are obtained via a dynamic protocol, such as, the Gx-interface for a particular subscriber session.

Usage Guidelines Use this command to configure the order in which rules are selected for matching in between dynamic rules (per subscriber) and static rules (from rulebase).

Example

The following command matches all dynamic rules against the flow prior to any static rule:

```
dynamic-rule order always-first
```

edr edr-dcca-fh

This command configures generation of EDRs when the OCS is in unreachable state.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

edr edr-dcca-fh [charging-edr *charging_edr_format_name* **| edr-format** *edr_format_name* **| reporting-edr** *reporting_edr_format_name* **] +**
{ default | no } edr edr-dcca-fh

default

Configures this command with its default setting.

Default: Disabled

no

If previously configured, deletes the configuration from the current rulebase.

charging-edr *charging_edr_format_name*

Specifies to generate charging EDR during OCS unreachable period.

charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

edr-format *edr_format_name*

Specifies to generate EDR during OCS unreachable period.

edr_format_name must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr *reporting_edr_format_name*

Specifies to generate reporting EDR during OCS unreachable period.

reporting_edr_format_name must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the trigger to generate EDRs when the OCS is in unreachable state. This configuration provides the facility to track and report the actual quota usage through EDRs during Assume Positive scenarios for HA.

This feature has been enhanced to support reporting / recording the appropriate usage in volume and time during regular OCS sessions and during assume positive scenarios separately. In this release, EDRs will be generated with new closure reasons when OCS goes down for HA.

Example

The following command configures the generation of charging EDRs when OCS is unreachable:

```
edr edr-dcca-fh charging-edr edr1
```

edr p2p

This command configures generation of Event Detail Records (EDR) for P2P events. This command is associated with the Dynamic Software Upgrade process.

Product

ACS

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

edr p2p *p2p_event_list* **[charging-edr** *charging_edr_format_name* **| edr-format** *edr_format_name* **| reporting-edr** *reporting_edr_format_name* **] +**
{ default | no } edr p2p *p2p_event_list*

default

Configures this command with its default setting.

Default: Disabled

no

If previously configured, deletes the configuration from the current rulebase.

p2p_event_list

Specifies the name of the P2P EDR Event. The plugin supports only the "audio-end" and "video-end" events. This P2P event list can be any P2P event that is supported by the plugin.

p2p_event_list must be an alphanumeric string of 1 through 128 characters.

charging-edr *charging_edr_format_name*

Specifies to generate charging EDR for P2P events.

charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

edr-format *edr_format_name*

Specifies to generate EDR for P2P events.

edr_format_name must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr *reporting_edr_format_name*

Specifies to generate reporting EDR for P2P events.

reporting_edr_format_name must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the P2P events to generate EDRs. The list of P2P events will be populated from the currently loaded plugin.

A plugin is a functional software entity that provides incremental updates to a pre-existing StarOS software component. Plugins can be dynamically loaded at runtime and do not require a system restart. For more information on the Dynamic Software Upgrade feature, refer to *Application Detection and Control Administration Guide*.

Example

The following command configures the generation of EDRs for P2P *audio-end* event specifying to use the EDR format named *edr1*:

```
edr p2p audio-end edr-format edr1
```

edr nemo-call

This command enables/disables the NEMO feature for populating the EDRs with source IP, destination IP and VRF name of the NEMO Mobile Router (MR) host.

Product



Important This CLI command is available only with NEMO license. Contact your Cisco account representative for more information.

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

[default | no] edr nemo-call

default

Configures this command with its default setting.

Default: Disabled

no

If previously configured, deletes the configuration from the current rulebase.

nemo-call

This keyword controls the feature of populating the EDRs with source IP, destination IP and VRF name associated with UEs behind the NEMO MRs.

By default this keyword option will be disabled i.e. this CLI should be configured if the feature needs to be turned ON.

Usage Guidelines

Use this command to enable this feature of creating the EDRs with the source IP, destination IP and VRF name of the NEMO host.



Important This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Releases prior to 18.0, ECS did not see the inner user packet i.e. it sees only MIP packet containing user data in both uplink and downlink direction. For example, it sees [IP header1][GRE header] [IP header2] [payload].

In 18.0 and later releases, ECS will see and analyze the inner IP packets i.e. [IP header2] [payload], and determine the source IP, destination IP and VRF name of the NEMO hosts.

Example

The following command enables the generation of EDRs with source IP, destination IP and VRF name of the NEMO host:

edr nemo-call

edr sn-charge-volume

This command allows you to exclude/include packets/bytes that are dropped/retransmitted by the ACS in the total charge volume — "sn-charge-volume" EDR attribute.

Product



Important In release 17.0, this command has been deprecated. This configuration is available at rulebase level as **[local]host_name(config-rule-base)# [no] retransmissions-counted.**

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

[default | no] edr sn-charge-volume { count-dropped-units | count-retransmitted-units }

default

Configures this command with its default setting.

Default: Exclude, in the total charge volume, packets/bytes dropped/retransmitted by ACS.

no

Exclude, in the total charge volume, packets/bytes dropped/retransmitted by ACS.

count-dropped-units

Specifies to include dropped units in the total charge volume.

count-retransmitted-units

Specifies to include retransmitted units in the total charge volume.

Usage Guidelines

Use this command to exclude/include packets/bytes that are dropped/retransmitted by ACS in the total charge volume — "sn-charge-volume" EDR attribute.

This command applies only to the "sn-charge-volume" attribute and does not affect the "sn-volume-amt" counts in any way.

Example

The following specifies to include units retransmitted by ACS in the sn-charge-volume EDR attribute:

edr sn-charge-volume count-retransmitted-units

edr suppress-zero-byte-records

This command disables/enables the creation of EDRs when there is no data for the flows.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

[default | no] edr suppress-zero-byte-records

default

Configures this command with its default setting.

Default: Disabled; same as **no edr suppress-zero-byte-records**

no

Disables the suppression of zero-byte EDRs.

edr suppress-zero-byte-records

Suppresses zero-byte EDRs.

Usage Guidelines

Use this command to disable/enable the creation of EDRs that are empty. The situation where there is a zero-byte EDR would typically be possible when two successive EDRs are generated for a flow. This CLI command suppresses the second such EDR for the flow.

edr transaction-complete

This command enables/disables the generation of an EDR on the completion of a transaction.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
edr transaction-complete { dns | http } [ charging-edr charging_edr_format_name
 | edr-format edr_format_name | reporting-edr reporting_edr_format_name ]
{ default | no } edr transaction-complete
```

default

Configures this command with its default setting.

Default: Disabled; same as **no edr transaction-complete**

no

If previously configured, deletes the configuration from the current rulebase.

dns | http

- **dns**: DNS protocol related configuration
- **http**: HTTP protocol related configuration

edr-format *edr_format_name*

Specifies to generate EDR on transaction completion for DNS or HTTP protocol.

edr_format_name must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

charging-edr *charging_edr_format_name*

Specifies to generate charging EDR on transaction completion.

charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr *reporting_edr_format_name*

Specifies to generate reporting EDR on transaction completion.

reporting_edr_format_name must be the name of a reporting EDR, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the generation of an EDR when certain application transactions (for example, request/response pairs) complete. EDR generation is supported for DNS or HTTP protocol. Note that these EDRs are in addition to those that might be generated due to other conditions, for example, EDR configurations in a Charging Action.

Example

The following command configures the generation of charging EDRs on the completion of transactions for HTTP protocol specifying the EDR format as *test123*:

```
edr transaction-complete http charging-edr test123
```

edr voip-call-end

This command enables/disables generation of EDRs on the completion of Voice over IP (VoIP) calls. This command is no longer supported for ADC in 14.0 and later releases.

Product

ACS

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

In StarOS 12.2 and later releases:

edr voip-call-end { charging-edr *charging_edr_format_name* **| edr-format** *edr_format_name* **| reporting-edr** *reporting_edr_format_name* **} +**
{ default | no } edr voip-call-end

In StarOS 12.1 and earlier releases:

edr voip-call-end edr-format *edr_format_name*
{ default | no } edr voip-call-end

default

Configures this command with its default setting.

Default: Disabled; same as **no edr voip-call-end**

no

If previously configured, deletes the edr voip-call-end configuration from the current rulebase.

edr-format *edr_format_name*



Important This option is available only in 12.1 and earlier releases. In 12.2 and later releases, it has been deprecated and is replaced by the **charging-edr** option.

Specifies to generate an EDR when a VoIP call ends.

edr_format_name must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

charging-edr *charging_edr_format_name*

Important This option is available only in 12.2 and later releases.

Specifies to generate a charging EDR when a VoIP call ends.

charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr *reporting_edr_format_name*

Important This option is available only in 12.2 and later releases.

Specifies to generate a reporting EDR when a VoIP call ends.

reporting_edr_format_name must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to generate an EDR on the completion of voice calls. Note that these EDRs are in addition to those that might be generated due to other conditions, for example EDR configurations in a Charging Action. This command facilitates P2P voice duration reporting.

Example

In 12.1 and earlier releases, the following command specifies generating EDRs on completion of VoIP calls using the EDR format *test13*:

```
edr voip-call-end edr-format test13
```

In 12.2 and later releases, the following command specifies generating charging EDRs on completion of VoIP calls using the EDR format named *test23*:

```
edr voip-call-end charging-edr test23
```

egcdr inactivity-meter

Description This command has been deprecated. It is included in the CLI for backward compatibility with older configuration files. When executed performs no function. Use the **egcdr threshold interval** *interval* **[regardless-of-other-triggers]** command for this functionality.

egcdr cdr-encoding

This command allows you to configure the eG-CDR encoding type.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
egcdr cdr-encoding { ascii [ delimiter { colon | comma | pipe } ] | asn.1
 }
default egcdr cdr-encoding
```

default

Configures the default eG-CDR CDR-encoding format.

Default: **asn.1**

ascii [delimiter { colon | comma | pipe }]

Specifies to use ASCII encoding type to generate eG-CDR in ASCII format.

delimiter { colon | comma | pipe }: Specifies the delimiter character to use in eG-CDRs in ASCII format.

- **colon**: Specifies to use ":" (colon) as a delimiter in eG-CDR.
- **comma**: Specifies to use "," (comma), as a delimiter in eG-CDR.
- **pipe**: Specifies to use "|" (pipe) as a delimiter in eG-CDR.

Default: **pipe**

asn.1

Specifies to use ASN.1 encoding type to generate eG-CDR in ASN.1 format.

This is the default setting.

Usage Guidelines

Use this command to configure the eG-CDR encoding type.

For more information on using eG-CDR ASCII encoding type in your deployment, contact your Cisco account representative.

Example

The following command specifies to use ASCII encoding type to generate eG-CDR in ASCII format while specifying the delimiter character as comma:

```
egcdr cdr-encoding ascii delimiter comma
```

egcdr tariff

This command allows you to configure the eG-CDR tariff time to generate new eG-CDRs for GGSN and P-GW-CDRs for P-GW.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

`[ no ] egcdr tariff { minute` *`minute`* `hour` *`hour`* `} | replicate-ocs-tariff-time-change }`

no

If previously configured, deletes the configuration from the current rulebase.

minute *minute*

Specifies the minute for the time-of-day configuration.

minute must be an integer from 0 through 59.

hour *hour*

Specifies the hour for the time-of-day configuration.

hour must be an integer from 0 through 23.

replicate-ocs-tariff-time-change

Specifies that the Gz tariff time is automatically replicated from Gy, if the rules have both offline and online charging enabled.

Usage Guidelines

Use this command to configure the eG-CDR tariff time to generate new eG-CDRs for GGSN and P-GW-CDRs for P-GW. Up to four different time-of-day settings may be configured. When any configured tariff time is reached, the current eG-CDR/P-GW-CDR will be closed and a new eG-CDR/P-GW-CDR is opened.

Example

The following command defines an eG-CDR tariff for the 23rd minute of the 22nd hour of the day (10:23 PM):

`egcdr tariff minute 23 hour 22`

egcdr threshold

This command allows you to configure the thresholds for generating eG-CDRs for GGSN and P-GW-CDRs for P-GW.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

egcdr threshold { interval *interval* **[regardless-of-other-triggers] | volume { downlink | total | uplink }** *bytes* **}**
{ default | no } egcdr threshold { interval | volume }

no

If previously configured, deletes the eG-CDR threshold configuration from the current rulebase.

default

Configures this command with the default settings.

Default: Disabled; same as **no egcdr threshold interval** and **no egcdr threshold interval volume** commands.

interval *interval* [regardless-of-other-triggers]

Specifies the time interval, in seconds, for closing the eG-CDR/P-GW-CDR if the minimum time duration thresholds are satisfied.

interval must be an integer from 60 through 40000000.

regardless-of-other-triggers: This option enables eG-CDR/P-GW-CDR generation at the fixed time interval irrespective of any other eG-CDR/P-GW-CDR triggers that may have happened in between.

Default: Disabled.

volume { downlink | total | uplink } *bytes*

Specifies the uplink/downlink volume octet counts for the generation of the interim eG-CDRs/P-GW-CDRs.

- **downlink** *bytes*: Specifies the limit for the number of downlink (from network to subscriber) octets after which the eG-CDR/P-GW-CDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: 4000000000

- **total** *bytes*: Specifies the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-GW-CDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: Disabled

- **uplink** *bytes*: Specifies the limit for the number of uplink (from subscriber to network) octets after which the eG-CDR/P-GW-CDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: 4000000000

Usage Guidelines

Use this command to configure thresholds to generate eG-CDRs/P-GW-CDRs.

Thresholds can be specified for both time interval and for data volume, by entering the command twice (once with interval and once with volume). When either configured threshold is reached, the eG-CDR/P-GW-CDRs will be closed. The volume trigger can be specified for uplink or downlink or combined total (uplink + downlink) byte thresholds. The exact keyword forces the configured volume to exactly match the volume in the eG-CDR/P-GW-CDRs, so the triggering packet might have to be divided across two eG-CDRs/P-GW-CDRs.

When both interval and volume triggers are configured, we'll reset the interval time and accumulated volume amount whenever the eG-CDR/P-GW-CDRs is closed regardless of whether it was due to the interval time expiration or reaching the volume limit. Use the regardless-of-other-triggers optional keyword, if you want the eG-CDRs/P-GW-CDRs closed at the configured regular intervals, regardless of whether eG-CDRs/P-GW-CDRs are being closed due to reaching a volume limit.

When the PDP context is terminated, the eG-CDR/P-GW-CDRs will be closed regardless of whether the thresholds have been reached.

Example

The following command defines an eG-CDR threshold interval of *600* seconds:

```
egcdr threshold interval 600
```

egcdr time-duration algorithm

This command allows you to specify the algorithm to compute the duration of time utilization in an eG-CDR for the current rulebase.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

egcdr time-duration algorithm { consumed-time *consumed_time* **[plus-idle] | continuous-time-periods** *ctp_time* **| parking-meter** *seconds* **}**
{ default | no } egcdr time-duration algorithm

no

If previously configured, deletes the eG-CDR time-duration algorithm configuration from the current rulebase.

default

Configures this command with its default setting.

Default: Algorithm configured for CCA, or the CCA default if none is configured.

consumed-time *consumed_time* [plus-idle]

Specifies the actual consumption time in seconds. This is used to determine the actual used chargeable time envelopes for the purpose of consuming time quota.

consumed_time must be an integer from 1 through 4294967295.

Default: 0 (disabled)

Time envelope is the basis for reporting active usage. For each time envelope, the time consumption includes the time duration between arrival of last packet and first packet only.

plus-idle: Specifies the idle time between arrival of two packets to include in time usage record in eG-CDR.

When used along with **consumed-time** it indicates the active usage + idle time, when no traffic flow occurs.

continuous-time-periods *ctp_time*

Specifies the continuous time period to compute the usage record in eG-CDR.

ctp_time sets the audition, in seconds, to start a counter on arrival of the first packet and thereafter include only that period in charging in which one or more packets arrived. For the period where no packets arrived or no traffic was detected, usage will not be computed.

ctp_time must be an integer from 1 through 4294967295.

parking-meter *seconds*

Specifies the Parking Meter (PM) period, in seconds.

seconds must be an integer from 1 through 4294967295.

Parking meter is the method with which the usage time is set in the content-id containers in eG-CDRs. When a parking meter value is set, the user is charged for time in increments of the value set. For example, if the parking meter is set to 300 seconds (5 minutes) and the subscriber only uses one minute, the charge is for 5 minutes.

Usage Guidelines

Use this command to set the various time charging algorithms/schemes for time usage in eG-CDR.

For example, packets arrive at times T1, T2, T3 and T4. Then the typical time usage might be computed to be T4 – T1. However, if say there is an idle period between times T2 and T3, then system will compute the time usage to be (T2 – T1) + (T4 – T3).

consumed-time in above scenario calculates the time duration as (T2 – T1) + (T4 – T3) where **consumed-time** with **plus-idle** calculates the time duration as (T2-T1)+I + (T4 – T3)+I or (T4-T1).

Example

The following command sets consumed time duration to *400* seconds:

```
egcdr time-duration algorithm consumed-time 400
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **exit**

Usage Guidelines Use this command to return to the parent configuration mode.

extract-host-from-uri

This command allows you to configure whether to use the host name embedded in the URI as the host field, when the host field option in the HTTP or Wireless Session Protocol (WSP) header is absent.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
extract-host-from-uri { http | wsp ) +
{ default | no } extract-host-from-uri
```

default

Configures this command with its default setting.

Default: Disabled; same as **no extract-host-from-uri**

no

If previously configured, disables the extract-host-from-uri configuration, for both HTPP and WSP, from the current rulebase.

http | wsp

Specifies the protocol(s).

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage Guidelines

If the host field is not present in HTTP/WSP header, this command will extract host from the URI, and store it in the host field to enable "http host" and "wsp host" rule matches using the stored value.



Important Applying the **extract-host-from-uri** command a second time will overwrite the previous configuration. For example, if you apply the command **extract-host-from-uri http wsp http**, and then apply the command **extract-host-from-uri http wsp**, extraction of host from URI will happen only for WSP analyzer.

Example

The following command configures extraction of host from URI for both HTTP and WSP protocols:

```
extract-host-from-uri http wsp
```

firewall dos-protection

This command allows you to configure Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks.



Important In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
[ no ] firewall dos-protection { all | flooding { icmp | tcp-syn | udp }
 | ftp-bounce | ip-unaligned-timestamp | mime-flood | port-scan |
tcp-window-containment | source-router | teardrop | winnuke }
default firewall dos-protection
```

no

If previously enabled, disables Stateful Firewall protection for subscribers from all or specified DoS attack(s).

default

Configures this command with its default setting.

Default: Protection from all DOS attacks is disabled.

all

Enables protection against all DoS attacks supported by the Stateful Firewall in-line service.

flooding { icmp | tcp-syn | udp }

Enables protection against specified flooding attacks:

- **icmp**: Enables protection against ICMP Flood attacks
- **tcp-syn**: Enables protection against TCP SYN Flood attacks
- **udp**: Enables protection against UDP Flood attacks

ftp-bounce

Enables protection against FTP Bounce attacks.

In an FTP Bounce attack, an attacker is able to use the PORT command to request access to ports indirectly through a user system as an agent for the request. This technique is used to port scan hosts discreetly, and to access specific ports that the attacker cannot access through a direct connection.

ip-unaligned-timestamp

Enables protection against IP Unaligned Timestamp attacks.

In an IP Unaligned Timestamp attack, certain operating systems crash if they receive a frame with the IP timestamp option that is not aligned on a 32-bit boundary.

mime-flood

Enables protection against HTTP Multiple Internet Mail Extension (MIME) Header Flooding attacks.

In a MIME Flood attack an attacker sends huge amount of MIME headers which consumes a lot of memory and CPU usage.

port-scan

Enables protection against Port Scan attacks.

tcp-window-containment

Enables protection against TCP Sequence Number Out-of-Range attacks.

In a Sequence Number Out-of-Range attack the attacker sends packets with out-of-range sequence numbers forcing the system to wait for missing sequence packets.

source-router

Enables protection against IP Source Route IP Option attacks.

Source routing is an IP option mainly used by network administrators to check connectivity. When an IP packet leaves a system, its path through various networks to its destination is controlled by the routers and their current configuration. Source routing provides a means to override the control of the routers. Strict source routing specifies the path through all the routers to the destination. The same path in reverse is used to return responses. Loose source routing allows the attacker to spoof both an address and sets the loose source routing option to force the response to return to the attacker's network.

teardrop

Enables protection against Teardrop attacks.

In a Teardrop attack, overlapping IP fragments are exploited causing the TCP/IP fragmentation re-assembly to improperly handle overlapping IP fragments.

winnuke

Enables protection against WIN-NUKE attacks.

This is a type of Nuke denial-of-service attack against networks consisting of fragmented or otherwise invalid ICMP packets sent to the target, achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop.

The WinNuke exploits the vulnerability in the NetBIOS handler and a string of out-of-band data sent to TCP port 139 of the victim machine causing it to lock up and display a Blue Screen of Death.

Usage Guidelines

Use this command to enable Stateful Firewall protection from different types of DoS attacks. This command can be used multiple times for different DoS attacks.



Important The DoS attacks are detected only in the downlink direction.

Example

The following command enables Stateful Firewall protection from all supported DoS attacks:

```
firewall dos-protection all
```

firewall flooding

This command allows you to configure Stateful Firewall protection from Packet Flooding attacks.

Important In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-rule-base)#`

Syntax Description

`firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit` *`packets`* **`} | { sampling-interval`** *`interval`* **`} }`**
`default firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit } | { sampling-interval } }`

default

Configures this command the default setting for the specified keyword.

protocol { icmp | tcp-syn | udp }

Specifies the transport protocol:

- **icmp**: Configuration for ICMP protocol.
- **tcp-syn**: Configuration for TCP-SYN packet limit.
- **udp**: Configuration for UDP protocol.

packet limit *packets*

Specifies the maximum number of specified packets a subscriber can receive during a sampling interval.

packets must be an integer from 1 through 4294967295.

Default: 1000 packets per sampling interval for all protocols.

sampling-interval *interval*

Specifies the flooding sampling interval, in seconds.

interval must be an integer from 1 through 60.

Default: 1 second

Usage Guidelines

Use this command to configure the maximum number of ICMP, TCP-SYN, / UDP packets allowed to prevent the packet flooding attacks to the host.

Example

The following command ensures a subscriber will not receive more that 1000 ICMP packets per sampling interval:

```
firewall flooding protocol icmp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 UDP packets per sampling interval on different 5-tuples. That is, if an attacker is sending lot of UDP packets on different ports or using different spoofed IPs, those packets will be limited to 1000 packets per sampling interval. This way only "suspected" malicious packets are limited and not "legitimate" packets:

```
firewall flooding protocol udp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 TCP-SYN packets per sampling interval:

```
firewall flooding protocol tcp-syn packet limi 1000
```

The following command specifies a flooding sampling interval of 1 second:

```
firewall flooding sampling-interval 1
```

firewall icmp-destination-unreachable-message-threshold

This command allows you to configure a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow.



Important In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
firewall icmp-destination-unreachable-message-threshold messages
then-block-server
{ default | no } firewall icmp-destination-unreachable-message-threshold
```

default

Configures this command with its default setting.

Default: No limit

no

If previously configured, deletes the configuration from the current rulebase.

messages

Specifies the threshold on the number of ICMP error messages sent by the subscriber for a particular data flow.

messages must be an integer from 1 through 100.

Usage Guidelines

Use this command to configure a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow. After the threshold is reached, it is assumed that the server is not reacting properly to the error messages, and further downlink traffic to the subscriber on the unwanted flow is blocked.

Some servers that run QChat ignore the ICMP error messages (Destination Port Unreachable and Host Unreachable) from the mobiles. So the mobiles continue to receive unwanted UDP traffic from the QChat servers, and their batteries get exhausted quickly.

Example

The following command configures a threshold of 10 ICMP error messages:

```
firewall icmp-destination-unreachable-message-threshold 10
then-block-server
```

firewall max-ip-packet-size

This command allows you to configure the maximum IP packet size (after IP reassembly) allowed over Stateful Firewall.



Important In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

firewall max-ip-packet-size *packet_size* **protocol { icmp | non-icmp }**
default firewall max-ip-packet-size protocol { icmp | non-icmp }

default

Configures the default maximum IP packet size configuration.

Default: 65535 bytes (for both ICMP and non-ICMP)

packet_size

Specifies the maximum packet size.

packet_size must be an integer from 30000 through 65535.

protocol { icmp | non-icmp }

Specifies the transport protocol:

- **icmp**: Configuration for ICMP protocol.
- **non-icmp**: Configuration for protocols other than ICMP.

Usage Guidelines

Use this command to configure the maximum IP packet size allowed for ICMP and non-ICMP packets to prevent packet flooding attacks to the host. Packets exceeding the configured size will be dropped for "Jolt Attack" and "Ping-Of-Death Attack".

Example

The following command allows a maximum packet size of *60000* for ICMP protocol:

```
firewall max-ip-packet-size 60000 protocol icmp
```

firewall mime-flood

This command allows you to configure Stateful Firewall protection from Multipurpose Internet Mail Extensions (MIME) Flood attacks.



Important In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

firewall mime-flood { http-headers-limit *max_limit* **|**
max-http-header-field-size *max_size* **}**
default firewall mime-flood { http-headers-limit |
max-http-header-field-size }

default

Configures this command with its default setting.

http-headers-limit *max_limit*

Specifies the maximum number of headers allowed in an HTTP packet. If the number of HTTP headers in a page received is more than the specified limit, the request will be denied.

max_limit must be an integer from 1 through 256.

Default: 16

max-http-header-field-size *max_size*

Specifies the maximum header field size allowed in the HTTP header, in bytes. If the size of HTTP header in the received page is more than the specified number of bytes, the request will be denied.

max_size must be an integer from 1 through 8192.

Default: 4096 bytes

Usage Guidelines

Use this command to configure the maximum number of headers allowed in an HTTP packet, and the maximum header field size allowed in the HTTP header to prevent MIME flooding attacks.

Example

The following command sets the maximum number of headers allowed in an HTTP packet to *100*:

```
firewall mime-flood http-headers-limit 100
```

The following command sets the maximum header field size allowed in the HTTP header to *1000* bytes:

```
firewall mime-flood max-http-header-field-size 1000
```

firewall no-ruledef-matches

This command allows you to configure the default action for packets when no Stateful Firewall ruledef matches.

Important In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, use the **access-rule no-ruledef-matches** command available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

firewall no-ruledef-matches { downlink | uplink } action { deny [charging-action *charging_action_name* **] | permit [bypass-nat | nat-realm** *nat_realm_name* **] }**
default firewall no-ruledef-matches { downlink | uplink } action

default

Configures the default action for packets with no Stateful Firewall ruledef match.

downlink | uplink

Specifies the packet type:

- **downlink**: Downlink (from network to subscriber) packets with no Stateful Firewall ruledef match.

  Default: **deny**

- **uplink**: Uplink (from subscriber to network) packets with no Stateful Firewall ruledef match.

  Default: **permit**

action { deny [charging-action *charging_action_name*] | permit [bypass-nat | nat-realm *nat_realm_name*] }

Specifies the default action for packets with no Stateful Firewall ruledef match.

permit [bypass-nat | nat-realm *nat_realm_name* **]**: Permit packets.

Important The **bypass-nat** keyword is only available in StarOS 8.3 and later releases.

Optionally specify:

- **bypass-nat**: Specifies to bypass Network Address Translation (NAT).
- **nat-realm** *nat_realm_name*: Specifies a NAT realm to be used for performing NAT on subscriber packets.

  nat_realm_name must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

Important If neither **bypass-nat** or **nat-realm** are configured, NAT is performed if the **nat policy nat-required** CLI command is configured with the **default-nat-realm** option.

deny [charging-action *charging_action_name* **]**: Denies specified packets.

Optionally, a charging action can be specified.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the default action to be taken on packets with no Stateful Firewall ruledef matches.

If, for deny action, the optional charging action is configured, the action taken depends on what is configured in the charging action. For the Stateful Firewall rule, the "flow action", "billing action", and "content ID" of the charging action will be used to take action. If flow exists, flow statistics are updated.

Allowing/dropping of packets is determined in the following sequence:

- Check is done to see if the packet matches any pinholes. If yes, no rule matching is done and the packet is allowed.
- Stateful Firewall ruledef matching is done. If a rule matches, the packet is allowed or dropped as per the **firewall priority** configuration.
- If no Stateful Firewall ruledef matches, the packet is allowed or dropped as per the **no-ruledef-matches** configuration.

For a packet dropped due to Stateful Firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the **firewall priority** or the **firewall no-ruledef-matches** command respectively.

In StarOS 8.1, in the case of Policy-based Stateful Firewall, the charging action applied is the one configured in the **access-rule priority** or the **access-rule no-ruledef-matches** command respectively.

For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the **flow any-error charging-action** command.

Example

The following command configures Stateful Firewall to permit downlink packets with no ruledef matches:

```
firewall no-ruledef-matches downlink action permit
```

firewall policy

This command allows you to enable/disable Stateful Firewall support for all subscribers using the current rulebase.



Important In StarOS 8.0, this command is available in the APN/Subscriber Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
firewall policy firewall-required
{ default | no } firewall policy
```

default

Configures this command with its default setting.

Default: Stateful Firewall support is disabled for all subscribers using the current rulebase.

no

If previously enabled, disables Stateful Firewall support for all subscribers using the current rulebase.

firewall-required

Enables Stateful Firewall support for all subscribers using the current rulebase.

Usage Guidelines

Use this command to enable/disable Stateful Firewall support for all subscribers using the current rulebase.

Example

The following command enables Stateful Firewall support:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support:

```
no firewall policy
```

firewall priority

This command allows you to add and specify the priority and type of a Stateful Firewall ruledef in the current rulebase, and allows you to configure a single or range of ports to be allowed on the server for auxiliary/data connections.

Important In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, use the **access-rule priority** command available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

firewall priority *priority* **[dynamic-only | static-and-dynamic] firewall-ruledef** *firewall_ruledef_name* **{ { deny [charging-action** *charging_action_name* **] } | { permit [nat-realm** *nat_realm_name* **| [trigger open-port {** *aux_port_number* **| range** *start_port_number* **to** *end_port_number* **} direction { both | reverse | same }]] } }**
no firewall priority *priority*

no

If previously configured, deletes the specified Stateful Firewall ruledef priority configuration from the current rulebase.

priority

Specifies the Stateful Firewall ruledef's priority in the current rulebase.

priority must be a unique value in the current rulebase, and must be an integer from 1 through 65535.

[dynamic-only | static-and-dynamic] firewall-ruledef *firewall_ruledef_name*

Specifies the Stateful Firewall ruledef to add to the rulebase. Optionally, the Stateful Firewall ruledef type can be specified.

- **dynamic-only**: Firewall Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is disabled by default.
- **static-and-dynamic**: Firewall Static and Dynamic Ruledef—Predefined ruledef that can be disabled/enabled by the policy server, and is enabled by default.
- *firewall_ruledef_name* must be the name of a Stateful Firewall ruledef, and must be an alphanumeric string of 1 through 63 characters.

deny [charging-action *charging_action_name*]

Denies packets if the rule is matched. An optional charging action can be specified. If a packet matches the deny rule, action is taken as configured in the charging action. For Stateful Firewall ruledefs, only the terminate-flow action is applicable, if configured in the specified charging action.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

permit [nat-realm *nat_realm_name* | [bypass-nat] [trigger open-port { *aux_port_number* | range *start_port_number* to *end_port_number* }]]

Permits packets.

- **nat-realm** *nat_realm_name*: Specifies the NAT realm to be used for performing NAT on subscriber packets matching the Stateful Firewall ruledef.

  If the NAT realm is not specified, then NAT will be bypassed. That is, NAT will not be applied on subscriber packets that are matching a Stateful Firewall ruledef with no NAT realm name configured.

  nat_realm_name must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

- **bypass-nat**: Specifies that packets bypass NAT.



Important If the **nat-realm** is not configured, NAT is performed if the **nat policy nat-required** CLI command is configured with the **default-nat-realm** option.

- **trigger open-port {** *aux_port_number* **|** **range** *start_port_number* **to** *end_port_number* **}**: Permits packets if the rule is matched, and allows the creation of data flows for Stateful Firewall. Optionally a port trigger can be specified to be used for this rule to limit the range of auxiliary data connections (a single or range of port numbers) for protocols having control and data connections (like FTP). The trigger port will be the destination port of an association which matches a rule.
  - *aux_port_number*: Specifies the number of auxiliary ports to open for traffic, and must be an integer from 1 through 65535.
  - **range** *start_port_number* **to** *end_port_number*: Specifies the range of ports to open for subscriber traffic.

- *start_port_number* must be an integer from 1 through 65535. This is the start of the port range and must be less than *end_port_number*.
- *end_port_number* must be an integer from 1 through 65535. This is the end of the port range and must be greater than *start_port_number*.

direction { both | reverse | same }

Specifies the direction from which the auxiliary connection is initiated. This direction can be same as the direction of control connection, or the reverse of the control connection direction, or in both directions.

- **both**: Provides the trigger to open port for traffic in either direction of the control connection.
- **reverse**: Provides the trigger to open port for traffic in the reverse direction of the control connection (from where the connection is initiated).
- **same**: Provides the trigger to open port for traffic in the same direction of the control connection (from where the connection is initiated).

Usage Guidelines

Use this command to add Stateful Firewall ruledefs to the rulebase and configure the priority, type, and port triggers. Port trigger configuration is optional. Port trigger can be configured only if a rule action is permit.

The rulebase specifies the Stateful Firewall rules to be applied on the calls. The ruledefs within a rulebase have priorities, based on which priority matching is done. Once a rule is matched and the rule action is permit, if the trigger is configured, the appropriate check is made. The trigger port will be the destination port of an association which matches the rule.

Multiple triggers can be defined for the same port number to permit multiple auxiliary ports for subscriber traffic.

Once a rule is matched and if the rule action is deny, the action taken depends on what is configured in the specified charging action. If the flow exists, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as EDR enabled, an EDR is generated.
- If the content ID is configured, UDR information is updated.
- If the flow action is configured as "terminate-flow", the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.



Important For Stateful Firewall ruledefs, only the terminate-flow action is applicable if configured in the specified charging action.

For a packet dropped due to Stateful Firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the **firewall priority** or the **firewall no-ruledef-matches** command respectively.

In StarOS 8.1, in the case of Policy-based Firewall, the charging action applied is the one configured in the **access-rule priority** or the **access-rule no-ruledef-matches** command respectively.

For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the **flow any-error charging-action** command.

The GGSN can dynamically activate/deactivate dynamic Stateful Firewall ruledefs for a subscriber based on the rule name received from a policy server. At rule match, if a rule in the rulebase is a dynamic rule, and if the rule is enabled for the particular subscriber, rule matching is done for the rule. If the rule is disabled for the particular subscriber, rule matching is not done for the rule.

Example

The following command assigns a priority of *10* to the Stateful Firewall ruledef *fw_rule1*, adds it to the rulebase, and permits port trigger to be used for the rule to open ports in the range of *100* to *200* in either direction of the control connection:

```
firewall priority 10 firewall-ruledef fw_rule1 permit trigger open-port
range 100 to 200 direction both
```

The following command configures the Stateful Firewall ruledef *fw_rule2* as a dynamic ruledef:

```
firewall priority 7 dynamic-only firewall-ruledef fw_rule2 deny
```

firewall tcp-first-packet-non-syn

This command allows you to configure the action to take on TCP flows starting with a non-syn packet.



Important In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
firewall tcp-first-packet-non-syn { drop | reset }
default firewall tcp-first-packet-non-syn
```

default

Configures this command with its default setting.

Default: **drop**

drop

Specifies to drop the packet or session.

reset

Specifies to send reset.

Usage Guidelines

Use this command to configure action to take on TCP flow starting with a non-syn packet.

Example

The following command configures action to take on TCP flow starting with a non-syn packet to drop:

```
firewall tcp-first-packet-non-syn drop
```

firewall tcp-idle-timeout-action

This command allows you to configure the Stateful Firewall action to be taken on TCP idle timeout expiry.



Important In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
firewall tcp-idle-timeout-action { drop | reset }
default firewall tcp-idle-timeout-action
```

default

Configures this command with its default setting.

Default: **reset**

drop

Specifies to drop the packet or session on TCP timeout expiry.

reset

Specifies to send reset on TCP timeout expiry.

Usage Guidelines

Use this command to configure action to take on TCP idle timeout expiry.

Example

The following command configures action to take on TCP idle timeout expiry to drop:

```
firewall tcp-idle-timeout-action drop
```

firewall tcp-reset-message-threshold

This command allows you to configure a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After this threshold is reached, further downlink traffic to the subscriber on the unwanted flow is blocked.



Important This command is only available in StarOS 8.3 and later releases. In StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
firewall tcp-reset-message-threshold messages then-block-server
{ default | no } firewall tcp-reset-message-threshold
```

default

Configures this command with its default setting.

Default: **no firewall tcp-reset-message-threshold**

no

If previously configured, deletes the firewall tcp-reset-message-threshold configuration from the current rulebase.

messages

Specifies the threshold on the number of TCP reset messages sent by the subscriber for a particular data flow.

messages must be an integer from 1 through 100.

Usage Guidelines

Use this command to configure a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After the threshold is reached, assuming the server is not reacting properly to the reset messages further downlink traffic to the subscriber on the unwanted flow is blocked. This configuration enables QCHAT noise suppression for TCP.

Example

The following command sets the threshold on the number of TCP reset messages to *10*:

```
firewall tcp-reset-message-threshold 10 then-block-server
```

firewall tcp-syn-flood-intercept

This command allows you to configure the TCP intercept parameters to prevent TCP SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the **dos-protection** command.



Important In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
firewall tcp-syn-flood-intercept { mode { none | watch [ aggressive ] }
| watch-timeout intercept_watch_timeout }
default firewall tcp-syn-flood-intercept { mode | watch-timeout }
```

default

Sets the default values of TCP intercept parameters for SYN Flood DoS protection.

mode { none | watch [aggressive] }

Specifies the TCP SYN flood intercept mode:

- **none**: Disables TCP SYN flood intercept feature.
- **watch**: Configures TCP SYN flood intercept feature in watch mode. Stateful Firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, Stateful Firewall clears the half-open connections by sending RST to TCP client and server. The default watch-timeout for connection establishment is 30 seconds.
- **aggressive**: Configures TCP SYN flood Intercept or Watch feature for aggressive behavior. Each new connection request causes the oldest incomplete connection to be deleted. When operating in watch mode, the watch timeout is reduced by half. If the watch-timeout is 30 seconds, under aggressive conditions it becomes 15 seconds. When operating in intercept mode, the retransmit timeout is reduced by half (i.e. if the timeout is 60 seconds, it is reduced to 30 seconds). Thus the amount of time waiting for connections to be established is reduced by half (i.e. it is reduced to 150 seconds from 300 seconds under aggressive conditions).

Default: **none**

watch-timeout *intercept_watch_timeout*

Specifies the TCP intercept watch timeout, in seconds.

intercept_watch_timeout must be an integer from 5 through 30.

Default: 30

Usage Guidelines

This TCP intercept functionality provides protection against TCP SYN Flooding attacks.

The system captures TCP SYN requests and responds with TCP SYN-ACKs. If a connection initiator completes the handshake with a TCP ACK, the TCP connection request is considered as valid by system and system forwards the initial TCP SYN to the valid target which triggers the target to send a TCP SYN-ACK. Now system intercepts with TCP SYN-ACK and sends the TCP ACK to complete the TCP handshake. Any TCP packet received before the handshake completion will be discarded.

Example

The following command sets the TCP intercept watch timeout setting to *5* seconds:

```
firewall tcp-syn-flood-intercept watch-timeout 5
```

flow any-error

This command allows you to specify the charging action to be used for packets dropped by Stateful Firewall due to any error conditions.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

flow any-error charging-action *charging_action_name*
default flow any-error

default

Configures the default action for packets dropped by Stateful Firewall due to any errors.

Default: Update the flow statistics if flow is available

charging_action_name

Specifies the charging action based on which accounting action is taken on packets dropped by Stateful Firewall due to any errors.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

Important The charging action specified here should preferably not be used for action on packets dropped due to Stateful Firewall ruledef match or no-match (in the **firewall priority** and **firewall no-ruledef-matches** commands) and the content ID within the charging action must be unique so that dropped counts will not interfere with other content IDs.

Usage Guidelines

Use this command to configure the charging action for packets dropped by Stateful Firewall due to any error conditions, such as, a packet being inappropriate based on the state of the protocol of the packet's session, or DoS protection causing the packet to be discarded, and so on.

For a packet dropped due to Stateful Firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the **firewall priority** or the **firewall no-ruledef-matches** command respectively.

In StarOS 8.1, in the case of Policy-based Firewall, the charging action applied is the one configured in the **access-rule priority** or the **access-rule no-ruledef-matches** command respectively.

For a packet dropped due to any error condition after data session is created, the charging action used is the one configured in the **flow any-error charging-action** command.

If the charging action applied on a packet is the one specified in the **flow any-error charging-action** command, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as EDR enabled, an Event Data Record (EDR) is generated.
- If the content ID is configured, Usage Data Record (UDR) information is updated.
- If the flow action is configured as "terminate-flow", the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.

Example

The following command specifies the charging action *test2* for accounting action on packets dropped/discarded by Stateful Firewall due to any error:

```
flow any-error charging-action test2
```

flow control-handshaking

This command allows you to specify how to charge for the control traffic associated with an application.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
flow control-handshaking { charge-to-application { [ all-packets ] [
initial-packets ] [ mid-session-packets ] [ tear-down-packets ] } |
charge-separate-from-application }
default flow control-handshaking
no flow control-handshaking [ charge-to-application ]
```

default flow control-handshaking

Configures this command with its default setting.

Default: Same as **no flow control-handshaking**

no flow control-handshaking [charge-to-application]

If previously configured, deletes the flow control-handshaking configuration from the current rulebase. The control packets will use whatever content-id is determined by the normal use of the **action** commands.

In this command, the optional keyword **charge-to-application** is deprecated and has no effect.

charge-to-application { [all-packets] [initial-packets] [mid-session-packets] [tear-down-packets] }

Configures the charging action to include the flow control packets either during initial handshaking only or specified control packets during session for charging.

- **all-packets**: Specifies that the initial setup packets will wait until the application has been determined before assigning the content-id, and all mid-session ACK packets as well as the final tear-down packets will use that content-id.
- **initial-packets**: Specifies that only the initial setup packets will wait for content-id assignment.

- **mid-session-packets**: Specifies that the ACK packets after the initial setup will use the application's or content-id assignment.
- **tear-down-packets**: Specifies that the final tear-down packets (TCP or WAP) will use the application's or content-id assignment.

charge-separate-from-application

Configures the charging action to separate the charging of the initial control packets or all subsequent control packets from regular charging.

Usage Guidelines

Use this command to configure how to charge for the control traffic associated with an application ruledef. Applications like HTTP use TCP to set up and tear down connections before the HTTP application starts. This command controls whether the packets that set up and tear down the connections should use the same content ID as the application's flow.

In normal mode 3-way handshake TCP packets (SYN, SYN-ACK, and ACK) and closing or intermittent packets (FIN, RST, etc.) directed and charged based on configured matched rules. This command makes the system to wait for the start and stop of layer 7 packet flow and content ID and charge the initial, intermittent, and closing TCP packets as configured to the same matching rules and content ID as of the flow.

This command also affects applications that do not use TCP but use other methods for control packets, for example WAP, where WTP/UDP may be used to set up and tear down connection-oriented WSP.

Example

Following command enables the charging for initial TCP handshaking control packets and wait for content-id of data traffic flow:

```
flow control-handshaking charge-to-application initial-packets
```

The following command enables charging all mid-session ACKs as well as tear-down packets to application:

```
flow control-handshaking charge-to-application mid-session-packets
tear-down-packets
```

flow end-condition

This command allows you to configure the end condition of the session flows related to a user session and triggers EDR generation.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

flow end-condition { hagr | handoff | normal-end-signaling | session-end | tethering-signature-change | interim *interim_timer_value* **| timeout } [flow-overflow] + { charging-edr** *charging_edr_format_name* **| reporting-edr** *reporting_edr_format_name* **}**
no flow end-condition

no

If previously configured, deletes the flow end-condition configuration from the current rulebase.

hagr

Creates an EDR with the specified EDR format whenever a flow is terminated due to Inter-chassis Session Recovery action.

handoff

Creates an EDR with the specified EDR format whenever a flow ends due to hand-off. Whenever a handoff occurs, ACS closes the EDRs for all current flows using the specified EDR format, and begins new statistics collection for the flows for the EDRs that will be generated when the flows actually end.

normal-end-signaling

Creates an EDR with the specified EDR format whenever flow end is signaled normally, for example like detecting FIN and ACK for a TCP flow, or a WSP-DISCONNECT terminating a connection-oriented WSP flow over UDP) and create an EDR for the flow using the specified EDR format.

session-end

Creates an EDR with the specified EDR format whenever a subscriber session ends. By this option ACS creates an EDR with the specified format name for every flow that has had any activity since last EDR was created for the flow on session end.

tethering-signature-change

Creates an EDR with specified EDR format for tethering signature change of a flow because of mid flow SYN packets.

Whenever a tethering signature change occurs, ACS closes the EDR with the specified closure reason and begins new statistics collection for the flow. If enabled, flow statistics may get split across multiple EDRs of the flow if tethering signature change occurs.

The maximum limit for tethering signature change detection depends on the **tethering-detection max-syn-packet-in-flow** CLI command. EDR/REDR generation for tethering signature change is also dependent on this CLI configuration.

interim *interim_timer_value*

This condition specifies the interim threshold condition of the flow where an EDR is generated based on the configured timer value. The *interim_timer_value* is configured in minutes with a configurable range from 15 to 1440 minutes.

The interim keyword is applicable only for new flows that are created and not on existing flows.

timeout

Creates an EDR with the specified EDR format whenever a flow ends due to a timeout condition.

flow-overflow



Important This keyword is applicable only when used with the **hagr**, **handoff**, **tethering-signature-change**, and **session-end** keywords.

Creates an EDR with the specified EDR format whenever there is a flow-overflow condition. If any of the specified end-conditions that affect subscriber information stored at ACS (such as call line) is configured, the "flow-overflow" EDR is generated.

+

Indicates that more than one of the keywords can be entered within a single command.

charging-edr *charging_edr_format_name*

Specifies the charging EDR format.

charging_edr_format_name must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr *reporting_edr_format_name*

Specifies the reporting EDR format.

reporting_edr_format_name must be the name of a reporting EDR format, and must be a unique alphanumeric string of 1 through 63 characters.

Usage Guidelines Use this command to enable or disable the capturing of EDRs based on flow end condition.

Example

The following command configures the flow end condition as handoff and creates a charging EDR with format named *EDR_format1*:

```
flow end-condition handoff charging-edr EDR_format1
```

flow limit-across-applications

This command allows you to limit the total number of simultaneous flows per Subscriber/APN sent to a rulebase regardless of the flow type, or limit flows based on the protocol type under the Session Control feature.

Product ACS

Privilege Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
flow limit-across-applications { limit | non-tcp limit | tcp limit }
no flow limit-across-applications [ non-tcp | tcp ]
```

no

If previously configured, deletes the flow limit-across-applications configuration from the current rulebase.

flow limit-across-applications *limit*

Specifies the maximum number of flows across all applications for the rulebase.

limit must be an integer from 1 through 4000000000.

Default: No limits

non-tcp *limit*

Specifies the maximum limit of non-TCP type flows.

limit must be an integer from 1 through 4000000000.

Default: No limits

tcp *limit*

Specifies the maximum limit of TCP flows.

limit must be an integer from 1 through 4000000000.

Default: No limits

Usage Guidelines

Use this command to limit the total number of flows allowed per subscriber for a rulebase regardless of flow type, or limit flows based on the protocol—non-TCP (connection-less) or TCP (connection-oriented).

If a subscriber attempts to exceed these limits system discards the packets of new flow. This limit processing of this command has following aspects for UDP, TCP, ICMP and some of the exempted flows:

- UDP/ICMP: System waits for the flow timeout before updating the counter and removing it from the count of number of flows.
- TCP: After a TCP flow ends, system waits for a short period of time to accommodate the retransmission of any missed packet from one end. TCP flows those are ended, but are still in wait period for timeout are exempted for this limit processing.
- Exempted flows: System exempts all the other flows specified with the **flow limit-for-flow-type** command in the ACS Charging Action Configuration Mode set to **no**.

Example

The following command defines the maximum number of *200000* flows for the rulebase:

```
flow limit-across-applications 200000
```

flow rtsp-all-pkts

This command allows you to delay charge packets in an RTSP flow.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
[ no | default ] flow rtsp-all-pkts charge-to-application
```

no

If previously configured, deletes the flow rtsp-all-pkts configuration from the current rulebase.

default

Configures this command with its default setting.

Default: Same as **no flow rtsp-all-pkts charge-to-application**.

flow rtsp-all-pkts charge-to-application

Configures delay charging for RTSP traffic. When this configuration is enabled, all packets (TCP control packets and RTSP packets) prior to the RTSP SETUP will be charged to application as per the application ruledef. In other words, they will be charged to the content-id established by the first SETUP of the RTSP flow.

Usage Guidelines

Use this command to delay charge packets in a RTSP flow. All initial packets (TCP control packets (all packets including initial, mid-session, end-session) and RTSP packets prior to the first SETUP) can be delay charged. Apart from the initial packets, all intermittent TCP control packets are also charged to the last matched Ruledef for the given RTSP flow. This command is used in conjunction with the **rtsp initial-bytes-limit** *RTSP_bytes* command.

The following command enables the RTSP flow's delay charging:

```
flow rtsp-all-pkts charge-to-application
```

fw-and-nat default-policy

This command allows you to configure the default Firewall-and-NAT policy for the current rulebase. This command must be used to configure the Policy-based Firewall-and-NAT feature.



Important This command is only available in StarOS 8.1 and StarOS 9.0 and later releases.

Product

PSF

NAT

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

fw-and-nat default-policy *fw_nat_policy_name*
no fw-and-nat default-policy

no

If previously configured, deletes the Firewall-and-NAT default policy configuration from the current rulebase.

fw_nat_policy_name

Specifies the default Firewall-and-NAT policy for the current rulebase.

fw_nat_policy_name must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the default Firewall-and-NAT policy for a rulebase.

For subscribers using the current rulebase, the default Firewall-and-NAT policy will be used if in the APN/subscriber profile the **default fw-and-nat policy** command is configured, and a policy to use is not received from the AAA/OCS.

For more information, see the *Personal Stateful Firewall Administration Guide*.

Example

The following command configures a Firewall-and-NAT policy named *standard* to the rulebase:

fw-and-nat default-policy standard

http header-parse-limit

This command allows you to configure the HTTP header parse limit, on exceeding which the flow is marked as permanent failure and is matched and charged against **http error = TRUE** ruledef.



Important This command is customer specific. For more information contact your Cisco account representative.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

http header-parse-limit *parse_limit_bytes*
{ default | no } http header-parse-limit

default

Configures the default setting for this command.

Default: 12000 bytes

no

If enabled, disables the header-parse-limit configuration in the current rulebase.



Important Disabling header parse limit may lead to uncharged bytes (due to no rule-matching until header is complete) if header is not correctly terminated.

parse_limit_bytes

Specifies the header-parse-limit, number of bytes.

parse_limit_bytes must be an integer from 1 through 256000.

Usage Guidelines

If a user sends HTTP LF terminated traffic instead of the usual HTTP CRLF terminated traffic, and similarly the server is responding with LF terminated traffic, the traffic does not result in any rule match, and rule match happens only at flow idle or at call clear when the quota for the same is not requested/updated. This results in a revenue hole for prepaid subscribers.

For operators who have Stateful Firewall in-line service enabled, and are okay if packets are dropped, a workaround is to configure the **firewall mime-flood** command in the ACS Configuration Mode, which enables to configure the maximum number of headers allowed in an HTTP packet and the maximum header field size

allowed in the HTTP header (in bytes). However, a limitation of this workaround is that Stateful Firewall supports MIME flood detection only in the downlink direction.

The support for LF termination has been added in StarOS 14.0 and later releases. For this release, with the help of configurable maximum header length support, HTTP analyzer would be allowing such LF terminated HTTP request/responses to pass through without rule matching only until the configured maximum header length is reached. When this threshold is reached, immediately the analyzer marks such HTTP session as failure and rule match would occur for **http error = TRUE** for the current packet as well as for all the previous packets that passed through unmatched. At this point, the quota for all such packets will be requested and reported.

Example

The following command sets the HTTP header parse limit to *10000* bytes:

```
http header-parse-limit 10000
```

ip readdress

This command allows you to configure the LBO restriction on Downlink and Uplink data volume transfer.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
ip readdress failure-action terminate
{ default | no } ip readdress failure-action
```

default

Configures the default setting for this command.

no

If previously configured, disables the LBO restriction on Downlink and Uplink data volume transfer.

ip readdress

Configures the IP Readdress options.

failure-action

Configures the failure action for IP Readdress.

terminate

Terminates the flow.

Usage Guidelines

After the subscriber quota is exhausted, all the ongoing download of files must be terminated and the UE must be allowed access to only user-defined servers (Self-Care Portal). Use this CLI command to achieve the functionality of Local Break Out (LBO) restriction on Downlink and Uplink data volume transfer.

ip reassembly-timeout

This command allows you to configure how long to hold onto IP fragments for reassembly, while waiting for the complete packet to arrive.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

ip reassembly-timeout *timeout_duration*
default ip reassembly-timeout

default

Configures the default setting for this command.

Default: 5000 milliseconds

timeout_duration

Specifies the timeout duration, in milliseconds, to hold fragmented packets before reassembly.

timeout_duration must be an integer from 100 through 30000.

Usage Guidelines

Use this command to configure duration for timeout timer to hold IP fragmented packets before reassembly is needed.

IP fragmented packet are retained, until either all fragmented packets have been received or the configured timeout has expired for the oldest fragment. If all fragments have been received, a temporary complete packet is reconstructed for analysis. Then all fragments are forwarded in order from first to last. If all fragments are not received, the fragments will be forwarded without being passed through the protocol analyzers, except for the IP analyzer.

Example

The following command sets the timeout timer to *15000* milliseconds:

```
ip reassembly-timeout 15000
```

ip reset-tos

This command allows you to reset the IP Type of Service (ToS) value of incoming packets to the default QCI value, before proceeding with the rest of ACS processing.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

[default | no] ip reset-tos

default

Configures this command with its default setting.

Default: Disabled

no

If previously configured, deletes the IP reset-tos configuration from the current rulebase.

Usage Guidelines

Use this command to reset the ToS field of any packet after it reaches ACS, or to broaden the range of values that are used in the ToS field in the IP header of any packet.

ip ttl

This command allows you to rewrite the TTL/Hop-limit value in the IP header downlink packets.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

ip ttl *ttl_value* **downlink**
{ no } ip ttl

no

If previously configured, disables the rewriting of TTL/Hop-limit value in the IP header downlink packets.

ip

Specifies the IP related to a user session.

ttl *ttl_value*

Rewrites the TTL value for the IP packet. The *ttl_value* specifies the value to be configured.

downlink

Modifies the IP header TTL on downlink packets.

Usage Guidelines

When the TTL/Hop-limit value is configured under the rulebase, all the subscribers under this rulebase are enabled for this feature, and TTL is rewritten as per the configured CLI value in all the downlink packets. The TTL is rewritten in all the downlink packets under that rulebase irrespective of service and access technology. The feature supports Flow Aware Packet Acceleration (FAPA), fragmentation, and buffering.

nat binding-record

This command allows you to configure NAT Binding Record (NBR) generation.



Important This command is only available in StarOS 8.3. In StarOS 9.0 and later releases this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
nat binding-record edr-format edr_format_name [ port-chunk-allocation ] [
port-chunk-release ] +
{ default | no } nat binding-record
```

default

Configures this command with its default setting.

Default: **port-chunk-release**

no

If previously configured, deletes the configuration from the current rulebase.

edr-format *edr_format_name*

Specifies the EDR format.

edr_format_name must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

port-chunk-allocation

Specifies generating NBR when a port chunk is allocated.

port-chunk-release

Specifies generating NBR when a port chunk is released.

+

Indicates that more than one of the previous keywords can be entered within a single command.

Usage Guidelines

Use this command to configure NBR generation.

Example

The following command configures an EDR format named *test123* and specifies generating NBR when a port chunk is allocated, and when a port chunk is released:

```
nat binding-record edr-format test123 port-chunk-allocation
port-chunk-release
```

nat policy

This command allows you to enable/disable Network Address Translation (NAT) processing for all subscribers using the current rulebase.

Important In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Important Before enabling NAT processing for a subscriber, Stateful Firewall must be enabled for the subscriber. See the firewall policy CLI command.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

nat policy nat-required [default-nat-realm *nat_realm_name* **]**
{ default | no } nat policy

default

Configures this command with its default setting.

Default: NAT processing is disabled for all subscribers using the current rulebase.

no

If previously enabled, disables NAT processing for all subscribers using the current rulebase.

nat policy nat-required

Enables NAT processing for all subscribers using the current rulebase.

default-nat-realm *nat_realm_name*

Important This keyword is only available in StarOS 8.3 and later releases.

Specifies the default NAT realm to be used if one is not already configured.

nat_realm_name must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

Important Including the default NAT realm, a maximum of three NAT realms are supported.

Usage Guidelines

Use this command to enable/disable NAT processing for all subscribers using the current rulebase.

After NAT is enabled for a subscriber, the NAT IP address to be used is chosen from the NAT realms defined in the rule priority lines within the rulebase. See the firewall priority CLI command.

NAT enable/disable status in the rulebase can be changed any time, however the changed NAT status will not be applied for active calls using the rulebase. The new NAT status is only applied to new calls.

Example

The following command enables NAT processing:

```
nat policy nat-required
```

The following command disables NAT processing:

```
no nat policy
```

nat suppress-aaa-update call-termination

This command allows you to suppress sending NAT Bind Updates (NBU) to the AAA server when a call gets terminated.

Important This command is customer-specific. For more information please contact your Cisco account representative. In release 9.0, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
nat suppress-aaa-update call-termination
default nat suppress-aaa-update
```

default

Configures this command with its default setting.

Default: Disabled. No suppression of AAA updates.

Usage Guidelines

Use this command to suppress the sending of NAT Bind Updates (NBU) to the AAA server when the call gets terminated, as these NBUs would be cleared at the AAA after receiving the accounting-stop. This enables to minimize the number of messages between the chassis and AAA server. When not configured, NBUs are sent to the AAA server whenever a port chunk is allocated, de-allocated, or the call is cleared (PPP disconnect).

Example

The following command suppresses the sending of NBU to the AAA server when PPP disconnect happens:

```
nat suppress-aaa-update call-termination
```

override-control

This command enables or disables Override Control (OC) feature. The Diameter capability exchange message should indicate support for OC feature when this CLI command is enabled.

Product



Important Override Control is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-rule-base)#`

Syntax Description

`[ default | no ] override-control[ align-with-gor | with-oc-name [ align-with-gor ]]`

default

Configures this command with its default setting.

Default: Disabled

In 20 and later releases: If **with-oc-name** option is not configured in rulebase, OC will be identified using the Rule/CA and exclude rule as keys. This is the default behavior.

no

If previously enabled, disables Override control in the current rulebase.

align-with-gor

Resolves ambiguity when same ruledefs are defined in multiple Group of Ruledefs.

with-oc-name

This optional keyword specifies to use OC-name as the unique key to identify an OC for a subscriber session.

Default: Disabled

In releases prior to 20, PCRF uses a combination of the following key parameters for identification of OC.

- Rule names
- Charging-action names
- Exclude-rule names

There is no unique OC name or ID to identify the OC for a particular subscriber session. In release 20, a new Diameter AVP "Override-Control-Name" is defined in the Override-Control grouped AVP. This OC name is used as the unique key to identify OC for any further updates like OC modification or deletion.

This keyword "**with-oc-name**" is added to the **override-control** CLI command to support Override-Control-Name AVP in the Override-Control AVP. If the **override-control with-oc-name** CLI is configured in rulebase, only OCs with Override-Control-Name AVP are supported and the OCs without name AVP are rejected.

If Override-Control-Name AVP is received when the **override-control** CLI command is configured, i.e. OC install is supported without OC name, appropriate error is reported in error logs. Then OC is dropped and OC failure statistics is incremented. Similarly if **override-control with-oc-name** CLI is configured and OC is received without the name AVP, appropriate error is reported, OC is dropped and OC failure statistics is incremented. On receiving an OC without name, installed OC list (without name) is searched for secondary identification criteria. If no OC with same rule/charging-action/exclude rule list is found, it is installed as a different OC.

Also, for OCs with the name AVP, operator can add rule/charging-action/exclude rule to the existing OC in the same category. That means, the rules can be added to a rule level OC, CA names can be added to a CA level OC, and exclude rules can be added to a wildcard or CA level OC.

OCs received with Override-Control-Name AVP are uniquely identified by the OC name. When the Override-Control-Name AVP is not present in Override-Control AVP, the OCs are identified based on the secondary identification criteria, i.e., the list of rule names, charging-action names, and exclude-rule names as these were the criteria before this feature change.

During rulebase change, the feature to support OC name will be controlled based on the configuration of new rulebase. After rulebase change OC will be accepted as per the CLI configured in new rulebase. This is the only scenario where for a single call session, OC can be installed with both OC name and without OC name.

When software upgrade is done on a standby setup where same rulebase is configured with the CLI **override-control with-oc-name**, then no calls are dropped and OC installation status will remain the same as before upgrade. Any new call which is established after upgrade and OC is installed with-oc-name then this will be accepted and applied on new call. Any calls which were established pre-upgrade will accept OC without name and will be identified uniquely by rule/charging-action/exclude rule.

During the downgrade, OC-name will be dropped and OCs will be recreated assuming Rule/CA/Exclude rule name list as the primary key for unique identification.

Usage Guidelines

Use this command to enable or disable Override Control feature and also specify to use Rule/CA list as unique key to identify OC for a session. This feature is available at the rulebase level and is license controlled. The Diameter capability exchange message should indicate support for Override control feature when this CLI command is enabled.

Inheritance feature does not support overwriting parameters at Rule level and charging action level and supports exclusion of only one rule. In order to provide this flexibility and also have a generic capability on chassis, Override Control feature is introduced. This feature will define a set of custom AVPs that will enable the PCRF to override charging and policy parameters for all rules (wildcard) or a specified set of rules or charging actions.

The override values should be sent by PCRF over Gx using the custom AVPs. Override Control provides this capability while addressing the limitations with Inheritance feature like rule level control, charging action level control, exclusion of more than one rule, different override values to be specified for a subscriber, etc. So, the Override Control feature will replace the Inheritance feature.



Important In this release, both Inheritance and the Override Control features will be supported. Note that both these two features should not be enabled simultaneously. If by mistake, both these features are enabled, only Override Control is applied.

The Gx interface is updated to include custom AVPs for the PCRF to send override values to P-GW. These override values may be sent for all rules (wildcard) or for specific rule(s) or for charging action(s). In case the override values are sent for a charging action, a rule or some of the rules may be excluded from using the override values by sending the rules names in the Gx message. The override values will be check pointed and recovered in case of either standalone recovery or ICSR.

This Override Control feature is expected to maintain existing active calls using inheritance post upgrade. Inheritance feature and Override control should not be enabled simultaneously. It is necessary that Inheritance feature be turned off once Override Control feature is enabled. Override Control once enabled will apply only to new calls and does not effect existing calls.

Override Control feature allows the customer to dynamically modify the parameters of static or predefined rules with parameters sent by PCRF over the Gx interface.

When multiple overrides are received from PCRF, the following is the priority in which they are applied:

- Rule level override control
- Charging action level override control
- Wildcard level override control

When installing a predef rule, if override control is received for that predef rule and QCI/ARP is overridden, then the new overridden QCI/ARP values are used for bearer binding of the predef rule. If the QCI/ARP is not overridden, then the values configured in charging action is used. The override charging and policy parameters received from PCRF will continue to apply for the entire duration of the call. These values may be modified by PCRF by sending the modified values with the same override control criteria (Rule name(s), Charging Action Name(s) and Exclude Rule(s)). Any change in the Override Control criteria will be interrupted as a new OC. There can only be one wildcard OC installed for a subscriber.

p2p dynamic-flow-detection

This command allows you to enable/disable the P2P analyzer to detect peer-to-peer (P2P) applications.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

`[ default | no ] p2p dynamic-flow-detection`

default

Configures this command with its default setting.

Default: Disabled

no

If previously enabled, disables P2P dynamic flow detection in the current rulebase.

p2p dynamic-flow-detection

Enables dynamic P2P flow detection.

Usage Guidelines Use this command to enable dynamic-flow detection. This allows the P2P analyzer to detect the P2P applications configured for the ACS.

pcp service

This command allows you to configure the PCP service for the current rulebase.



Important This command is customer specific. Contact your Cisco account representative for more information.

Product NAT

PSF

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
pcp service pcp_service_name
no pcp service
```

no

If previously configured, deletes the PCP service configuration from the current rulebase. This service is disabled by default.

pcp_service_name

Specifies the PCP service name for the current rulebase.

pcp_service_name must be the name of a PCP service, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines Use this command to configure the PCP service for the current rulebase.

Example

The following command configures a PCP service named *pcp1* for the rulebase:

```
pcp service pcp1
```

post-processing dynamic

This command allows you to specify ruledefs/group-of-ruledefs as dynamic post-processing ruledefs/group-of-ruledefs. This allows the system to differentiate normal post-processing rules from preconfigured ones. By default, this configuration is disabled.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

post-processing dynamic { group-of-ruledefs *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[description** *description* **]**
no post-processing dynamic { group-of-ruledefs *ruledefs_group_name* **| ruledef** *ruledef_name* **}**

no

If previously configured, deletes the specified configuration from the current rulebase.

group-of-ruledefs *ruledefs_group_name*

Adds the specified group-of-ruledefs to the current rulebase.

ruledefs_group_name must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

ruledef *ruledef_name*

Adds the specified ruledef to the current rulebase.

ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

charging-action *charging_action_name*

Specifies the charging action.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

description *description*

Specifies an optional description for this configuration.

description must be an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to configure specific ruledefs/group-of-ruledefs as dynamic post-processing ruledefs/group-of-ruledefs. This allows the system to differentiate normal post-processing rules from the

preconfigured ones. This makes possible enabling/disabling ruledefs/groups-of-ruledefs entry from an external server.

Example

The following command specifies the ruledef named *test_rule* as a dynamic post-processing ruledef configured with the charging action *ca13* and a description of *testing*:

```
post-processing dynamic ruledef test_rule charging-action ca13 description
 testing
```

post-processing policy

This command allows you to specify the post-processing policy to be applied on Limit-Reached packets.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
post-processing policy { always | not-for-dynamic-discard }
default post-processing policy
```

default

Configures this command with its default setting.

Default: **not-for-dynamic-discard**

always

Specifies to apply post-processing even if the Credit Control Application (CCA) decides to discard packets due to limit-reached condition. If there are post-processing priority-based rules, CCA will check for any redirection rules. Otherwise, by default, CCA will discard the packets. No other post-processing actions like forward, next-hop, or xheader-insertion will be applied on the limit-reached packets.

not-for-dynamic-discard

Specifies to apply post-processing only if CCA decides not to discard packet. Will directly discard the limit-reached context and will not apply post-processing priority based rules.

Usage Guidelines

This command allows to enable post-processing priority based rules for content in blockedlisted state. Whenever RADIUS/Diameter prepay server blockedlists content the packets are generally discarded. To enable redirection of such content, post-processing should be enabled on the blockedlisted content. With this command, RADIUS/Diameter Credit-Control application will decide whether to allow post-processing to be enabled or not for the blockedlisted content.

The following is a sample configuration:

```
configure
 active-charging service service1
  ruledef http_low
   http any-match = TRUE
   cca quota-state = limit-reached
   rule-application post-processing
  #exit
  ruledef httpany
   http any-match = TRUE
  #exit
  charging-action standard1
   content-id 1
   cca charging credit
  #exit
  charging-action redirect
   flow action redirect-url http://aoc.com
  #exit
  rulebase base1
   action priority 30 ruledef httpany charging-action standard1
   post-processing policy always
   post-processing priority 1 ruledef http_low charging-action redirect
  #exit
end
```

Example

The following command will enable post processing on Limit-Reached packets:

post-processing policy always

post-processing priority

This command allows you to configure the post-processing priority and action to be taken on specific ruledef in the current rulebase.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

post-processing priority *priority* **{ group-of-ruledefs** *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[description**

```
description ]
no post-processing priority priority
```

no

If previously configured, deletes the specified post-processing priority configuration from the current rulebase.

priority *priority*

Specifies priority for the ruledef/group-of-ruledefs in the current rulebase.

priority must be a unique value in the current rulebase, and must be an integer from 1 through 65535.

group-of-ruledefs *ruledefs_group_name*

Important Post-processing with group-of-ruledefs is not supported in this release.

Specifies the group-of-ruledefs.

ruledefs_group_name must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

Important The group-of-ruledefs specified must be configured for post-processing. See the **group-of-ruledefs-application** command in the ACS Group-of-Ruledefs Configuration mode.

ruledef *ruledef_name*

Specifies the ruledef.

ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

Important The ruledef specified must be configured for post-processing. See the **rule-application** command in the *ACS Ruledef Configuration Mode Commands* chapter.

charging-action *charging_action_name*

Specifies the charging action.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

description *description*

Specifies an optional description for this configuration.

description must be an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to configure the post-processing priority and action to be taken on a ruledef in the rulebase.

Example

The following command configures the ruledef named *test_ruledef* with a priority of *10*, and the charging action named *test_ca* for post processing:

```
post-processing priority 10 ruledef test_ruledef charging-action test_ca
```

qos-renegotiate timeout

This command allows you to configure the timeout setting for the Quality of Service (QoS) Renegotiation feature.

Important This command is license dependent. For more information contact your Cisco account representative.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
qos-renegotiate timeout timeout
no qos-renegotiate timeout
```

no

If previously configured, deletes the qos-renegotiate timeout configuration from the current rulebase.

timeout

Specifies the timeout period for the QoS Renegotiation feature in the current rulebase.

timeout is the timeout period in seconds, and must be an integer from 0 through 4294967295. If set to 0, timeout is disabled.

Usage Guidelines

Use this command to configure timeout setting for the QoS Renegotiation feature.

Example

The following command sets the QoS renegotiate timeout period to 1000 seconds:

```
qos-renegotiate timeout 1000
```

radius threshold

This command allows you to configure the interval and volume thresholds to generate interim RADIUS Charging Data Records (CDRs) and write them to CDR file for ACS postpaid billing.

Product

HA

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

radius threshold { interval *interval* **| volume total** *volume* **}**
{ default | no } radius threshold { interval | volume total }

no

If previously configured, deletes the RADIUS threshold configuration from the current rulebase.

default

Configures this command with the default settings.

Default: Disabled

interval *interval*

Specifies the time interval, in seconds, for generating RADIUS interim accounting requests.

interval must be an integer from 60 through 40000000.

Default: Disabled

volume total *volume*

Specifies the limit for the total number of octets (uplink+downlink) after which a stop-start pair will be sent to RADIUS.

volume must be an integer from 100000 through 4000000000.

Default: Disabled

Usage Guidelines

Use this command to specify a time interval threshold to generate interim RADIUS CDRs and write it to RADIUS CDR file for postpaid billing.

Example

The following command configures a time threshold interval of *600* seconds for RADIUS CDRs:

```
radius threshold interval 600
```

retransmissions-counted

This command allows to count retransmissions in all charging modules.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-rule-base)#`

Syntax Description

`[ no ] retransmissions-counted`

no

Retransmissions will be counted for all the charging modules. This command will override the CLI at the charging action as well as the CLI pertaining to the retransmissions at the rulebase.

Usage Guidelines

Use this command to count retransmissions for all the charging modules.

Example

With the following command, retransmissions will not be counted for any of the charging modules:

`no retransmissions-counted`

ran bandwidth optimize

This command is used to enable optimized calculation of [MBR, GBR] when a subscriber (voice) call is put on hold in case of VoLTE.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-rule-base)#`

Syntax Description

`[ default | no ] ran-bandwidth optimize`

no

If previously configured, disables the optimization feature for calculating [MBR, GBR] values based on Flow-Status AVP value.

Usage Guidelines

Use this command to enable optimized calculation of [MBR, GBR] values when a subscriber (voice) call is put on hold in case of VoLTE.

When the rule is installed and active, the system uses the GBR/MBR assigned in the rule for calculating the GBR / MBR values towards the bearers created. When more than one rule is installed, P-GW adds the GBR / MBR values from all the active and installed rules even if the flow of a certain rule is marked as disabled. This current behavior is in accordance with 3GPP TS standard specification 29.212, and this might result in RAN bandwidth wastage. To avoid this wastage, some optimization is done while calculating MBR and GBR for GBR bearer.

This optimization feature provides the ability to configure a list of APNs, for which the optimized calculation of MBR, GBR can be enabled. By default, this optimized calculation should be enabled only for the IMS APN.

This feature further helps optimize the logic of aggregating MBR and GBR values, based on "Flow-Status" AVP value received in the rule definition through RAR.

During session setup, when a CCA-I is received, and if **ran bandwidth optimize** is configured for the associated rulebase, the system will aggregate [MBR, GBR] of only the rules which have flow-status='ENABLED'. This information will subsequently be sent to UE.



Important The last used [MBR, GBR] for GBR bearer needs to be recovered in the event of a session manager or chassis switchover. Failure to do so can result in miscalculation of [MBR, GBR] after recovery.

By default, this CLI will be disabled. Any change in this configuration will not affect existing calls on the system. Optimized bandwidth calculation will be done only for the new calls established after enabling this CLI command.

route priority

This command allows you to configure the routing of packets to protocol analyzers.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

route priority *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http | sip [advanced |**

```
 basic-and-advanced ] | smtp | tftp | wsp-connection-less |
wsp-connection-oriented } [ description description ]
no route priority route_priority
```

no

If previously configured, deletes the specified route priority configuration from the current rulebase.

route priority *route_priority*

Specifies the route priority for the specified ruledef in the current rulebase.

route_priority must be an integer from 1 through 65535.

Lower numbered priorities are examined first. Up to 1024 instances can be configured across all rulebases.

ruledef *ruledef_name*

Specifies the ruledef to evaluate packets to determine analyzer.

ruledef_name specifies the name of the ruledef configured for the route application using the **rule-application** command in the ACS Ruledef Configuration Mode.

ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

analyzer

Specifies the analyzer for the ruledef, and must be one of the following:

- **dns**: Route to DNS protocol analyzer.
- **file-transfer**: Route to file analyzer.
- **ftp-control**: Route to FTP control protocol analyzer.
- **ftp-data**: Route to FTP data protocol analyzer.
- **h323**: Route to H323 protocol analyzer.
- **http**: Route to HTTP protocol analyzer.
- **imap**: Route to IMAP protocol analyzer.
- **mipv6**: Route to MIPv6 protocol analyzer.
- **mms**: Route to MMS protocol analyzer.
- **pop3**: Route to POP3 protocol analyzer.
- **pptp**: Route to PPTP protocol analyzer.
- **radius**: Route to RADIUS protocol analyzer.
- **rtcp**: Route to RTCP protocol analyzer.
- **rtp**: Route to RTP protocol analyzer.
- **rtsp**: Route to RTSP protocol analyzer.
- **sdp**: Route to SDP protocol analyzer.

- **secure-http**: Route to secure HTTP protocol analyzer.
- **sip [advanced | basic-and-advanced]**: Route to SIP protocol analyzer.
  - **advanced**: For SIP calls to work with NAT/Stateful Firewall, a SIP Application-Level Gateway (ALG) is required to do payload translation of SIP packets and pin-hole (dynamic flow) creation for media packets. A SIP routing rule must to be configured for routing the packets to the SIP ALG for processing. If the keyword **advanced** is configured, the packets matching the routing rule will be routed to SIP ALG for processing and not to ACS SIP analyzer. If not configured, then packets will not be routed to SIP ALG and will be routed to ACS SIP analyzer for processing.

    Also, see **firewall nat-alg** CLI command in the ACS Configuration Mode.
  - **basic-and-advanced**: For SIP ALG to co-exist with SIP Analyzer, the packets are routed through ACS SIP Analyzer and SIP ALG. The SIP packets can pass through ACS functionality (by ACS SIP Analyzer processing) and at the same time payload translation/pinhole-creation can happen successfully (by SIP ALG processing). If **basic-and-advanced** is configured, then the packets matching the routing rule will be routed through the SIP Analyzer and then through SIP ALG for processing.
- **tftp**: Route to TFTP protocol analyzer.
- **smtp**: Route to SMTP protocol analyzer.
- **wsp-connection-less**: Route to WSP connection-less protocol analyzer.
- **wsp-connection-oriented**: Route to WSP connection-oriented protocol analyzer.

Important To route packets to the P2P analyzer, the ruledef should have rules to match all IP packets. Otherwise, the analyzer may not detect all P2P traffic.

Important Use the **show active-charging analyzer statistics** command in the Exec Mode to see the list of supported analyzers.

description *description*

Enables to add a description to the rule and action for later reference in saved configuration file.

description must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Instances of this CLI command control which packets are routed to which protocol analyzers. Packets sent to ACS are always passed through the IP protocol analyzer. This CLI command controls which higher layer analyzers are also invoked.

Analyzer	Common ways to route to the analyzer
dns	UDP destination port or source port is DNS (53).
file-transfer	FTP and the command name is **retr** or **stor**; or, HTTP and the request method is **get** or **post**.

Analyzer	Common ways to route to the analyzer
ftp	TCP destination port or source port is FTP control (21) or FTP data (20); or, ftp analyzer (for FTP control packets) dynamically detected an FTP data flow over TCP (tcp dynamic-flow = ftp-data).
http	TCP destination port or source port is HTTP (80).
icmp	All IPv4 packets with IP protocol = ICMP (1) are automatically routed here.
imap	TCP destination port or source port is IMAP (143).
ip	All IPv4 packets are automatically routed here.
mipv6	MIPv6 analyser can be routed in one of the following ways: • All IPv4 UDP packets with destination port = 5846 • All IPv4 UDP packets with destination port = 5846, and destination IP present in LMA server host-pool • All IPv6 packets with destination IP present in LMA server host-pool
mms	WSP content type is application/vnd.wap.**mms**-message; or, WSP uri contains "**mms**"; or, HTTP content type is application/vnd.wap.mms-message; or, HTTP uri contains "**mms**".
p2p	Use the **p2p dynamic-flow-detection** CLI command to enable detection of the different P2P applications specified by the **p2p application** CLI command; that will cause every TCP or UDP packet to be automatically routed here
pop3	TCP destination port or source port is POP3 (110).
radius	UDP source or destination port 1812 to be used.
rtp and **rtcp**	RTSP has embedded RTP/RTCP payloads (you need to enable RTP dynamic flow detection to catch those flows); or, RTSP or SDP (for SDP within SIP) creates an RTP/RTCP flow over UDP (in addition to enabling the aforementioned dynamic flow detection, you must make sure that UDP packets are routed to the UDP analyzer) or, RTP/RTCP uses predefined UDP port numbers (e.g. default UDP port numbers of 5004/5005).
rtsp	TCP destination port or source port is RTSP (554).
sdp	RTSP or SIP content type is application/sdp
secure-http	TCP destination port or source port is HTTPS (443). Note that HTTP may use the CONNECT method (see RFC 2817), in which case, the subscriber will be upgraded with transport layer security, but the traffic to/from the chassis will still be HTTP and be passed through the http rather than the secure-http analyzer (assuming that routing to the http analyzer has been configured).
sip	UDP destination port or source port is SIP (5060).
smtp	TCP destination port or source port is SMTP (25).
tcp	All IPv4 packets with IP protocol = TCP (6) are automatically routed here.

Analyzer	Common ways to route to the analyzer
udp	All IPv4 packets with IP protocol = UDP (17) are automatically routed here.
wap2	TCP destination port or source port of the carrier-specific port number for WAP-2 (e.g. one carrier uses 8799); or, send all HTTP traffic to the **wap2** analyzer if the carrier does not use a special port number.
wsp	UDP destination port or source port is connection-less WSP (9200) or connection-oriented WSP (9201).
wtp	Packets are automatically routed here, if you specified "wsp-connection-oriented" as described above.

Example

The following command assigns a route and rule action with the route priority of 23, a ruledef named *test*, and an analyzer *test_analyzer* with description as *route_test1* to the current rulebase:

```
route priority 23 ruledef test analyzer test_analyzer description
route_test1
```

rtp dynamic-flow-detection

This command allows you to enable/disable the Real Time Streaming Protocol (RTSP) and Session Description Protocol (SDP) analyzers to detect the start/stop of RTP and RTCP flows.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

[default | no] rtp dynamic-flow-detection

default

Configures this command with its default setting.

Default: Disabled; same as **no rtp dynamic-flow-detection**.

no

If previously configured, deletes this configuration from the current rulebase.

Usage Guidelines Use this command to enable the RTSP and SDP analyzer to detect the start/stop of RTP and RTCP flows. This command is used in conjunction with the **route priority** command.

Example

The following command enables RTP dynamic flow detection:

```
rtp dynamic-flow-detection
```

rtsp initial-bytes-limit

This command allows to set the maximum number of uplink and downlink bytes, added together to accumulate, while rule matching and charging is being delayed for RTSP flows. The limit is per RTSP flow.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
rtsp initial-bytes-limit rtsp_bytes
default rtsp initial-bytes-limit
```

default

Configures the RTSP initial packets limit to 6000 bytes.

RTSP_bytes

Specifies the maximum number of uplink and downlink bytes limit.

rtsp_bytes must be an integer from 1 through 256000.

Usage Guidelines Use this command to configure the maximum number of uplink and downlink bytes per RTSP flow that can be accumulated before the first SETUP request. The accumulated bytes include both TCP-control packets as well as RTSP packets. Once this limit is reached, rule matching occurs and charging is enforced on the flow. This command is used in conjunction with the **flow rtsp-all-pkts charge-to-application** command.

Example

The following command sets the RTSP initial bytes limit to 9000 bytes:

```
rtsp initial-bytes-limit 9000
```

ruledef-parsing

This command allows you to configure whether to consider or ignore the port number embedded in the application header (for example, the ":80" in www.star.com:80) when comparing the ruledef expressions to the packet contents.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
[ no ] ruledef-parsing ignore-port-numbers-embedded-in-application-headers
 analyzers { http rtsp sip wsp }
default ruledef-parsing
```

no

If previously configured, deletes the ruledef-parsing configuration from the current rulebase.

default

Configures this command with its default setting.

Default: Same as **no ruledef-parsing ignore-port-numbers-embedded-in-application-headers analyzers { http rstp sip wsp }**— not ignoring port numbers that are embedded in application headers.

ignore-port-numbers-embedded-in-application-headers analyzers { http rtsp sip wsp }

Ignore the port numbers present in application header.

Specifies analyzers for which the port number must be ignored.

Usage Guidelines

Use this command to make the HTTP, RTSP, SIP, and WSP analyzer ignore port numbers embedded in application headers.

Example

The following command makes the HTTP analyzer in the current rulebase ignore port numbers embedded in application headers:

```
ruledef-parsing ignore-port-numbers-embedded-in-application-headers
analyzers http
```

tcp 2msl-timeout

This command allows you to configure how long to retain the TCP flow after the FIN has been acknowledged.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

tcp 2msl-timeout *2msl_timeout* **[port-reuse]**
{ default | no } tcp 2msl-timeout

default

Configures this command with its default setting.

Default: 2 seconds

no

Disables the timeout and sets the system to delete the flow immediately upon seeing the FIN acknowledged.

tcp 2msl-timeout *2msl_timeout*

Specifies the duration to keep the TCP flow.

2msl_timeout specifies the timeout duration, in seconds, and must be an integer from 1 through 20.

port-reuse

Allows the source port reuse to reopen the TCP flow in 2msl timeout.

Usage Guidelines

Use this command to configures how long to retain the TCP flow after the FIN has been acknowledged.

Acknowledgment to the FIN is not guaranteed to be received by the destination, then the FIN could be resent and re-acknowledged. In this scenario, it is desirable to still have the flow, so that the re-sends do not create a new flow.

Example

The following command sets the timeout to *4* seconds:

tcp 2msl-timeout 4 port-reuse

tcp rst-robustness

This command allows you to configure the TCP RST robustness.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-rule-base)#`

Syntax Description

`tcp rst-robustness`
`{ default | no } tcp rst-robustness`

default

Configures this command with its default setting.

no

Disables the TCP RST robustness feature.

tcp rst-robustness

Enables or disables TCP RST robustness as per RFC 5961 in the ACS Rulebase Configuration Mode.

Usage Guidelines

Use this command to enable the TCP robustness RFC 5961. The feature is disabled by default.

Example

The following command enables the TCP RST robustness in the ACS Rulebase Configuration Mode:

`tcp rst-robustness`

tcp check-window-size

This command allows you to enable/disable TCP window-size checking.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
[ default | no ] tcp check-window-size
```

default

Configures this command with its default setting.

Default: Enabled (packets after the erroneous packet (with size greater than the receiver's window size) will hit tcp-error ruledef).

Default: Disabled. The TCP window-size check has been disabled, only the L7 parsing is continued. The operator can configure the TCP window-size check, if required.

no

Disables the window-size check and continues with normal L7 parsing.

tcp check-window-size

Enables the window-size check and continues with normal L7 parsing.

Usage Guidelines

Use this command to enable/disable TCP window-size check for packets out of TCP window.

Example

The following command enables TCP window-size check:

```
tcp check-window-size
```

tcp mss

This command allows you to configure the TCP Maximum Segment Size (MSS) in TCP SYN packets.



Important This command is only available in StarOS 8.1 and later releases.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

tcp mss *tcp_mss* **{ add-if-not-present | limit-if-present } +**
{ default | no } tcp mss

default

Configures this command with its default setting.

Default: Disabled

no

If previously configured, deletes the TCP MSS configuration from the current rulebase.

tcp mss *tcp_mss*

Specifies the TCP MSS.

tcp_mss must be an integer from 496 through 65535.

add-if-not-present

Specifies to add the TCP MSS if not present in the packet.

limit-if-present

Specifies to limit the TCP MSS if present in the packet.

Usage Guidelines

Using this command, TCP MSS can be limited if already present in the TCP SYN packets. If there are no errors detected in IP header/TCP mandatory header and there are no memory allocation failures, TCP optional header is parsed. If TCP MSS is present in the optional header and its value is greater than the configured MSS value, the value present in the TCP packet is replaced with the configured one.

If the TCP optional header is not present in the SYN packet and there are no errors in already present TCP header, the TCP MSS value configured will be inserted while sending the current packet out.

Example

The following command limits the TCP maximum segment size to *3000*, and if not present adds it to the packets:

```
tcp mss 3000 limit-if-present add-if-not-present
```

tcp out-of-order-timeout

Description This command has been deprecated, and is replaced by the **tcp packets-out-of-order** command.

tcp packets-out-of-order

This command allows you to configure processing of TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

tcp packets-out-of-order { timeout *timeout_duration* **| transmit [after-reordering | immediately] }**
default tcp packets-out-of-order { timeout | transmit }

default

Configures this command with its default setting.

- **timeout**: 5000 milliseconds
- **transmit**: **immediately**

timeout *timeout_duration*

Specifies the timeout duration for re-assembly of TCP out-of-order packets.

timeout_duration is the timeout duration, in milliseconds, and must be an integer from 100 through 30000.

Default: 5000 milliseconds

transmit [after-reordering | immediately]

Configures the TCP out-of-order segment behavior after buffering a copy.

- **after-reordering:** Delivers the TCP out-of-order segments in-sequence to the ECS analyzer after all packets are received and successfully reordered. The 'after-reordering' feature is doing this by buffering out-of-order packets, and only releasing them after the missing out-of-order packets are received (or after OOO timeout).

  When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is done, and then the last packet is forwarded (as the latest). If reordering is not successful within the specified OOO timeout, all the subsequent received packets in that TCP flow are forwarded without being passed through the analysers (except the L3/L4 analyzer). As a consequence only L3/L4 rule matching will take place. If memory allocation fails or the received packet is partial retransmitted data, the packet will also be forwarded immediately without being passed through the protocol analyzers, except for the L3/L4 analyzers.

Important On the outgoing interface, no in-sequence delivery is guaranteed. This feature is intended to: -deliver the TCP segments in-order to the ECS analysers -buffer the original packets during OOO conditions, such that application-based flow actions (ex: Header insertion) can still take place on the actual data packets Its not intended to put the packets in-sequence on the outgoing interface (although some improvement can be seen there as well) -the cost of this feature is additional delay for OOO packets (up to a maximum of the OOO timeout).

- **Immediately:** Delivers the TCP out-of-order segments in-sequence to the ECS analyzer after all packets are received and successfully reordered. The 'immediately' feature is accomplishing this by making a copy of out-of-order packets, and buffering those, while transmitting the original data packets through the outgoing interface immediately. When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is done, and then the last packet is forwarded.

  If reordering of the buffered packets is not successful within the specified OOO timeout, all the subsequent received packets in that TCP flow are forwarded without being passed through the analysers (except the L3/L4 analyzer). As a consequence only L3/L4 rule matching will take place.

  If memory allocation fails or the received packet is partial retransmitted data, the packet will also be forwarded immediately without being passed through the protocol analyzers, except for the L3/L4 analysers.

Important This feature is not changing anything on the sequencing of the packets -This feature has the consequence that during OOO conditions, certain application-based flow actions (ex: Header insertion) could not take place as the original packets are already sent out by the time the ECS analyser receives the (copies of) in-sequence packets.

Default: **immediately**

Usage Guidelines

Use this command to configure how to process TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

Important When TCP OOO processing has been configured in the rulebase, a session manager crash might be observed due to overlapping TCP segments and/or reordering packet arriving within TCP OOO configured timeout value or default value (5 sec). This issue can be resolved by changing the rulebase configuration for TCP OOO packets from **transmit after-reordering** to **transmit immediately**.

Example

The following command sets the timeout timer to *10000* milliseconds:

```
tcp packets-out-of-order timeout 10000
```

tcp proxy-mode

This command allows you to enable/disable TCP Proxy mode for all subscribers using the current rulebase.



Important In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

ACS

CF

MVG

TPO

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
tcp proxy-mode { dynamic { all | content-filtering | dcca | ip-readdressing
 | nexthop-readdressing | xheader-insert } + | static [ port [ port_number
 [ to port_number ] ] ] }
default tcp proxy-mode
no tcp proxy-mode [ dynamic { content-filtering | dcca | ip-readdressing
 | nexthop-readdressing | xheader-insert } + | static [ port [ port_number
 [ to port_number ] ] ] ]
```

default

Configures this command with its default setting.

Default: Disabled

no

If previously enabled, disables TCP Proxy mode.

Optionally, TCP Proxy can be disabled for specific options that were previously enabled.

dynamic { all | content-filtering | dcca | ip-readdressing | nexthop-readdressing | xheader-insert } +

Enables TCP proxy for subscriber-initiated TCP flows under the specified condition(s).

- **all**: Specifies that subscriber-initiated TCP flows be proxied if all/any of the following conditions are satisfied.

- **content-filtering**: Specifies that subscriber-initiated TCP flows be proxied if a URL is requested, and that URL is checked because Category-based Content Filtering is enabled in the rulebase.
- **dcca**: Specifies that subscriber-initiated TCP flows be proxied if DCCA is enabled in the charging action.
- **ip-readdressing**: Specifies that subscriber-initiated TCP flows be proxied if IP Readdressing feature is enabled in the charging action.
- **nexthop-readdressing**: Specifies that subscriber-initiated TCP flows be proxied if Nexthop Readdressing feature is enabled in the charging action.
- **xheader-insert**: Specifies that subscriber-initiated TCP flows be proxied if x-Header Insertion feature is enabled in the charging action.

static [port [*port_number* [to *port_number*]]]

Enables static TCP proxy for every subscriber-initiated TCP flow, unless specific ports are specified.

port [*port_number* **[to** *port_number* **]]]**

Specifies port numbers and/or range of port numbers.

port_number must be an integer from 1 through 65535.



Important Up to 32 port numbers and eight port ranges can be specified.

Usage Guidelines



Important In release 11.0, TCP Proxy functions only in Static mode. Dynamic TCP Proxy mode is supported only in 12.0 and later releases.

Use this command to enable/disable TCP Proxy mode for all subscribers using this ACS rulebase. Optionally, TCP Proxy can be enabled/disabled for specific ACS features. Note that enabling/disabling the TCP Proxy feature for any of the optional ACS features, does not affect that feature.

Note that the last command overwrites any previous configuration. For example, when the following commands are applied in sequence:

tcp proxy-mode dynamic nexthop-readdressing

tcp proxy-mode dynamic xheader-insert

The nexthop configuration is overwritten by the x-header configuration.

Example

The following command enables TCP proxy for subscriber-initiated TCP flows whenever next-hop-forwarding-address is configured in the charging action:

```
tcp proxy-mode dynamic nexthop-readdressing
```

tcp window-size

This command allows the operator to configure the maximum window size of a TCP packet.

Product

P-GW

SAE-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-rule-base)#`

Syntax Description

`[ no ] tcp window-size downlink` *`tcp_window_size`*
`[ no ] tcp window-size`

no

Disables the TCP window size configuration.

tcp window-size

Configures the maximum window size of the TCP packet. The window size value is an integer ranging from 16384 to 1073725440.

downlink

This keyword applies the window size configuration only for the downlink packets.

Usage Guidelines

Use this command to configure the maximum window size of a TCP packet. The operator can restrict the effective window size of all downlink TCP packets.

Example

The following command configures a window-size value 17890 :

```
tcp window-size downlink 17890
```

tethering-detection

This command allows you to enable/disable the Tethering Detection feature for the current rulebase, and specifies the database to use.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

tethering-detection [application | dns-based | ip-ttl value *ttl_value* **| max-syn-packet-in-flow** *max_syn_packets* **| os-db-only | os-ua-db | ua-db-only]**
{ default | no } tethering-detection

default

Configures this command with its default setting.

Default: By default, the Tethering Detection feature is disabled. When enabled, unless a specific database is specified to be used, by default tethering detection will make use of both the databases.

no

If previously configured, deletes the tethering detection configuration from the current rulebase.

application

Specifies to perform tethering detection based on App-based method.

With release 21.1.3, the App-based Tethering Detection is introduced only for Netflix and YouTube.

dns-based

Specifies to perform tethering detection based on DNS-based method.

ip-ttl value *ttl_value*

Specifies to perform tethering detection using IP-TTL configuration. *ttl_value* must be an integer from 1 through 255 to configure TTL values for tethered flows.

max-syn-packet-in-flow *max_syn_packets*

Specifies the number of SYN packets applicable for tethering detection in a flow. *max_syn_packets* must be an integer from 1 through 3.

Default number of SYN packets is 1. This means that only the first SYN packet in flow will be analyzed for IP-TTL/OS signature generation and tethering detection. All other mid-flow SYN packets will be ignored for IP-TTL/OS signature generation and tethering detection.

os-db-only

In 17 and earlier releases: Specifies to perform tethering detection using only the OS signature database.

In 18 and later releases: Specifies to perform tethering detection using IPv4 and IPv6 OS signature databases.

os-ua-db

In 17 and earlier releases: Specifies to perform tethering detection using only OS and UA signature databases.

In 18 and later releases: Specifies to perform tethering detection using IPv4 OS, IPv6 OS, and UA signature databases.

ua-db-only

Specifies to perform tethering detection using only the UA signature database.

Usage Guidelines

Use this command to enable/disable the Tethering Detection feature for a rulebase, and configures the database to use. Tethering Detection can be done for IPv4, IPv6, TCP and UDP flows.

Changing the configuration does not affect existing flows of the subscriber. If Tethering Detection was disabled and is turned enabled, it will be applied only to new flows of subscribers using the rulebase.



Important IPv6 Tethering Detection is supported only with TTL and UA signatures, and not supported for OS signatures.

Also, see the **tethering-database** command in the *ACS Configuration Mode Commands* chapter.

Example

The following command enables the Tethering Detection feature in the rulebase, and specifies to use only the OS database:

```
tethering-detection os-db-only
```

tft-notify-ue-def-bearer

This command allows you to control whether TFT updates are sent to UE or not for default bearer for the specified rulebase.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
{ default | no } tft-notify-ue-def-bearer
```

default

The default behavior is to send the TFT updates of default bearer for the specified APN to UE.

no

This keyword controls the TFT updates of default bearer for the APN attached to the chassis, from being sent to the UE.

Usage Guidelines

Use this command at the rulebase level to control whether TFT updates are sent to UE or not for default bearer for the specified rulebase.

This feature provides the operator the flexibility to configure this per Rulebase and also configure to suppress TFT updates only. The CLI command allows sending other QoS updates to the UE and controls only the TFT related updates. This CLI is supported only for default bearer.

In releases prior to 15.0, the "**no policy-control update-default-bearer**" CLI command is used to suppress all the TFT updates to the UE on the default bearer including the initial TFTs sent in the Create Session Response. Also, this configuration is available for the entire system and not per rulebase. Additionally, this CLI command suppresses all the QoS related updates (including change in bit rate) to the UE.

timestamp rounding

This command allows you to enable/disable timestamp rounding in EDRs or eG-CDRs.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

timestamp rounding { edr | egcdr } { ceiling | floor | round-off } { default | no } timestamp rounding { edr | egcdr }

default

Configures this command with its default setting.

Default: **round-off**

no

Disables timestamp rounding.

edr

Enables timestamp rounding for EDRs.

egcdr

Enables timestamp rounding for eG-CDRs.

ceiling

If the fractional part of the seconds is greater than 0, adds 1 to the number of seconds and discards the fraction.

floor

Discards the fractional part of the second.

round-off

Sets the fractional part of the seconds to nearest integer value. If the fractional value is greater than or equal to 0.5, it adds 1 to the number of seconds and discards the fractional part of second.

Usage Guidelines

Use this command to configure the timestamp rounding setting.

The specified rounding will be performed before system attempts any calculation. For example using round-off, if the start time is 1.4, and the end time is 1.6, then the calculated duration will be 1 (for example, 2 – 1 = 1).

This command may be repeated for each type of EDR or eG-CDR.

Example

The following command sets the EDR timestamp to nearest integer value second; for example, 34:12.23 to 34:12.00:

```
timestamp rounding edr round-off
```

tpo default-policy

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

traffic-optimization

This command allows you to turn ON/OFF the traffic optimization for UDP traffic.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
[ no ] traffic-optimization udp
```

no

If previously configured, turns OFF the traffic optimization for UDP traffic.

By default, traffic optimization for UDP traffic is disabled.

udp

Specifies traffic optimization for UDP traffic.

Usage Guidelines Use this command to turn ON/OFF the traffic optimization for UDP traffic.

Important Enabling/Disabling traffic optimization is controlled by service-scheme framework.

transactional-rule-matching

This command allows you to enable or disable transactional rule matching (TRM) which allows the Enhanced Charging Service (ECS) to bypass per-packet rule matching on a transaction once the transaction is fully classified.

Important The TRM feature is supported in SSI platform; earlier it was restricted only to ASR5500.

Product

ACS

ADC

Privilege Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
[ default | no ] transactional-rule-matching
```

default

Configures this command with its default setting.

Default: Disabled.

no

If already configured, disables transactional rule matching.

Usage Guidelines

Use this command to enable or disable transactional rule matching. This allows the Enhanced Charging Service (ECS) to bypass per-packet rule matching on a transaction once the transaction is fully classified.

A transaction for TRM can be defined as the entire UDP flow, the ACK of the 3-way handshake to the FIN/RST of a TCP flow, or the HTTP request to the next HTTP request, or HTTP request to the FIN/RST for the final request of the flow. Rule matching can be performed on IP L4 rules (UDP, TCP), HTTP, and HTTPS.

In 16.0 and later releases, ADC and TRM/FP can be enabled together. ADC flows will be considered for TRM optimization. Most VoIP applications that require all packets of the flow do not support TRM. When TRM/FP is enabled with ADC, such protocols will not take TRM/FP.



Important From 16.0 release, **Transactional Rule Matching** and **Fastpath** functionalities have been merged, and will be governed by only the **transactional-rule-matching** keyword alone. The keyword **fastpath** independently can no longer be used to turn on or turn off this functionality.

Example

The following command enables transactional rule matching:

```
transactional-rule-matching
```

transport-layer-checksum

This command allows you to enable/disable checksum verification for TCP and UDP packets.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
[ no ] transport-layer-checksum verify-during-packet-inspection [ tcp |
udp ]
default transport-layer-checksum
```

no

Disables the checksum calculation for the specified packet type.

default

Configures this command with its default setting.

Default: Same as **transport-layer-checksum verify-during-packet-inspection**—to perform the checksum verification calculation on all TCP and UDP packets.

[tcp | udp]

Specifies that either TCP or UDP packets should be verified/not verified.

If neither of these keywords is specified the command applies to both TCP and UDP packets.

Usage Guidelines

Use this command to disable or enable performing checksum verification calculations on TCP or UDP packets.

If the checksum is not verified, the packets will go through the TCP/UDP analyzers (and deeper analyzers, if so configured via the **route** command) regardless of the value of the TCP/UDP checksum.

If the checksum is verified, only packets with good checksums will go through the TCP/UDP analyzers (and deeper analyzers, if so configured).

Example

The following command disables checksum verification calculations on all TCP and UDP packets:

```
no transport-layer-checksum verify-during-packet-inspection
```

udr threshold

This command allows you to configure the threshold limit to generate Usage Data Records (UDRs) that provide Comma Separated Value (CSV) records written periodically in a fixed schema designed to reflect a total billable quantity.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
udr threshold { interval interval | volume { downlink bytes [ uplink bytes ]
 | total bytes | downlink bytes [ uplink bytes ] } }
default udr threshold { interval | volume }
no udr threshold { interval | volume { downlink [ uplink ] | total |
uplink [ downlink ] } }
```

no

If previously configured, deletes the UDR threshold configuration from the current rulebase.

default

Configures this command with its default setting.

Default: Disabled; same as **no udr threshold interval** and **no udr threshold volume**.

interval *interval*

Specifies the time interval, in seconds, for closing the UDR if the minimum time duration thresholds are satisfied. By default, this option is disabled.

interval must be an integer from 60 through 40000000.

Default: 0 (Disabled)

volume

Specifies uplink/downlink volume octet counts for the generation of interim UDRs.

- **downlink** *bytes*: Specifies the limit for the number of downlink octets after which the UDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: 4000000000

- **total** *bytes*: Specifies the limit for the total number of octets (uplink+downlink) after which the UDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: Disabled

- **uplink** *bytes*: Specifies the limit for the number of uplink octets after which the UDR is closed.

  bytes must be an integer from 100000 through 4000000000.

  Default: 4000000000

UDR records are generated whenever either threshold is reached.

Usage Guidelines Use this command to enable thresholds for generation of UDRs.

Example

The following command specifies that UDR records should be generated every 10 minutes (*600* seconds):

```
udr threshold interval 600
```

udr trigger

This command allows you to configure additional triggers for generating UDRs.



Important This command is only available in StarOS 8.3 and later releases.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
udr trigger { first-hit-content-id | tariff-time minute minutes hour hours
| nemo-prefix-update }
no udr trigger { first-hit-content-id | tariff-time | nemo-prefix-update
 }
default udr trigger [ nemo-prefix-update ]
```

no

Disables first-hit-content-id UDR trigger.

default

Configures this command with its default setting.

Default: Disabled; no additional triggers.

first-hit-content-id

Specifies to generate interim UDR on first packet hit per rating group/content ID.

tariff-time minute *minutes* hour *hours*

This keyword allows to configure tariff time trigger to close ongoing UDR buckets and save all data traffic up to tariff time in a single UDR file. By default, this CLI keyword is disabled.

Configuring this keyword enables the PDSN/PCEF to generate content base UDR record for each concurrent online subscriber in each of day cross and place them in a single UDR file. The charging records include content based service (by duration and by volume).

Tariff time is stored at rulebase level. Therefore if the tariff time is updated while there are ongoing calls in the network, the old tariff time will be ignored and the new tariff time will be applied to the existing as well as upcoming calls.

At the end of the "Tariff Time" period, the UDR files are created and the next set of records are stored in a new UDR file.

nemo-prefix-update



Important This keyword is available only with NEMO license.

On configuring this keyword/trigger, UDRs will be generated in case a NEMO update event is received. If this trigger is not configured UDRs will not be generated even if a NEMO update event is received from session manager. If the "**no**" or "**default**" option is used, it will disable the UDR trigger for nemo-prefix-update.

Usage Guidelines

This command enables to assign first packet trigger to interim UDRs—for generating UDR for first packet hit per rating group/content ID. The first-hit-content-id trigger when configured causes an UDR to be generated as soon as a packet hits a Charging Action with a content ID. UDR generation will be triggered when this command is configured and present in the rulebase.

Example

The following command assigns first packet trigger to interim UDRs, for generating UDR for first packet hit per rating group/content ID:

udr trigger first-hit-content-id

uidh-insertion

This command allows you to enable insertion of UIDH Hash values in HTTP requests that require UIDH service.

Product

ACS

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-rule-base)#`

Syntax Description

uidh-insertion server-name *server_name* **[bypass wl-lookup]**
no uidh-insertion

no

If previously configured, deletes the UIDH insertion configuration from the current rulebase.

server-name

Specifies the UIDH server name The server_name is a string ranging in size from 1 to 63 characters.

bypass wl-lookup

This command if configured bypasses the URL Host look-up. By default, URL Host whitelist is enabled, that is, bypass is not applied. However, Bypass with permitlist look-up can be applied during run-time.



Note From StarOS 21.26 and later releases, the term “whitelist” is replaced with “permitlist” in the help string.

Usage Guidelines

Use this command to enable insertion of UIDH Hash values in HTTP requests that require UIDH service.

The UIDH value is inserted in the HTTP header of the traffic flows for permitlisted destination URLs and whitelisted subscribers MDNs.

Note The term “whitelist” is replaced with “permitlist” in the CLI from StarOS 21.26 and later releases.

When a session is attached to P-GW, the P-GW queries the UIDH server. If there is no response from the UIDH server, the UIDH service is not enabled for this session.

url-preprocessing

This command allows you to enable/disable a group-of-prefixed-urls for preprocessing of embedded URLs.

Important This command is customer specific. For more information, please contact your Cisco account representative.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* **> rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

[no] url-preprocessing bypass group-of-prefixed-urls *prefixed_urls_group_name*

no

If previously configured, deletes the URL-preprocessing bypass configuration from the current rulebase.

group-of-prefixed-urls *prefixed_urls_group_name*

Specifies the group-of-prefixed-urls.

prefixed_urls_group_name must be the name of a group-of-prefixed-urls, and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to enable/disable a group-of-prefixed-urls for preprocessing of embedded URLs. This command can be issued multiple times to enable multiple groups. If an embedded URL begins with the string specified within any of the groups, that prefix text will be removed from the URL.

Example

The following command enables looking for prefixed URLs of the group-of-prefixed-urls named *test5*:

```
url-preprocessing bypass group-of-prefixed-urls test5
```

video optimization-preprocessing cae-readdressing

This command allows you to enable/disable CAE readdressing at the rulebase level.

Important In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

ACS

MVG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

```
video optimization-preprocessing cae-readdressing
[ default | no ] video optimization-preprocessing
```

default

Configures this command with its default setting.

no

If already configured, disables CAE readdressing.

Usage Guidelines

Use this command to configure ACS to readdress the flows to CAE.

websocket flow-detection

This command allows you to enable or disable websocket flow detection at rulebase level.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description `[ no ] websocket flow-detection [ protocol1 | protocol2 | protocol3 | ...]`

no

Disables the websocket flow detection.

[protocol 1 | protocol2 | protocol3 | ...]

Specifies protocol for detection.

If both protocol1 and protocol2 are specified, then specifies protocol detection of both protocols.

Usage Guidelines Use this command to disable or enable websocket flow detection identification of protocols.

Important Currently, websocket is only using HTTP protocol as a transport layer, so the CLI will have only http as option.

Example

The following command disables websocket flow detection identification of protocols:

```
no websocket flow-detection [proto1 | proto2 | proto3 ]
```

wtp out-of-order-timeout

Description This command has been deprecated, and is replaced by the command.

wtp packets-out-of-order

This command allows you to configure how to process Wireless Transaction Protocol (WTP) packets that are out of order, while waiting for the earlier packet(s) to arrive.

Product ACS

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description `wtp packets-out-of-order { out-of-order-timeout timeout | transmit [ after-reordering | immediately ] }`
`default wtp packets-out-of-order { out-of-order-timeout | transmit }`

default

Configures this command with its default setting.

- **out-of-order-timeout**: 5000 milliseconds
- **transmit**: **immediately**

out-of-order-timeout *timeout*

Specifies the maximum duration for which WTP out-of-order packets are retained, before reassembly is needed.

timeout is the timeout duration, in milliseconds, and must be an integer from 100 through 30000.

Default: 5000 milliseconds

transmit [after-reordering | immediately]

Specifies the WTP out-of-order segment behavior after buffering a copy:

- **after-reordering**: Sends WTP out-of-order segment after it becomes ordered
- **immediately**: Sends WTP out-of-order segment immediately after buffering a copy

Default: **immediately**

Usage Guidelines

Use this command to configure TCP out-of-order segment options.

If out-of-order-timeout is specified, out-of-order packets are retained, until either all packets have been received or the configured timeout has expired for the oldest packet. If all packets have been received, a temporary complete packet is reconstructed for analysis. Then all packets are forwarded in order from first to last. If all packets are not received, the packets will be forwarded without being passed through the protocol analyzers, except for the IP analyzer.

If **after-reordering** transmitting is specified, the packets are held onto and reordered. After successfully reordering the packets, they are processed in the proper order. If reordering is not successful due to timeout (wtp out-of-order-timeout), the received packets are forwarded without being passed through the protocol analyzers.

If **immediately** is specified, the packets are transmitted as they are received without any in-line services or Charging Action processing, however a copy of each packet is retained. When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is undertaken, and then the last packet is forward (unless otherwise configured by the in-line services or Charging Action).

Example

The following command sets the timeout timer to *10000* milliseconds:

```
wtp packets-out-of-order out-of-order-timeout 10000
```

xheader-encryption

This command allows you to configure X-Header Encryption feature's parameters.

Product



Important This command is license dependent. For more information please contact your Cisco account representative.

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Rulebase Configuration

active-charging service *service_name* > **rulebase** *rulebase_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax Description

xheader-encryption { certificate-name *certificate_name* **| re-encryption period** *period* **}**
default xheader-encryption re-encryption period
no xheader-encryption { certificate-name | re-encryption }

default

Configures this command with its default setting.

Default: Disabled

no

If previously configured, deletes the configuration from the current rulebase.

certificate-name *certificate_name*

Specifies the encryption certificate to use for the X-Header Encryption feature.

certificate_name must be the name of an encryption certificate, and must be an alphanumeric string of 1 through 63 characters.

Default: Disabled; no encryption certificate

re-encryption period *period*

Specifies how often to re-generate the encryption keys.

period specifies the re-encryption time period in minutes, and must be an integer from 1 through 10000.

Default: Disabled; no re-encryption

Usage Guidelines

Use this command to configure the X-Header Encryption feature's certificate and re-encryption parameters.

Example

The following command configures the X-Header Encryption feature to use the certificate named *testcert*:

```
xheader-encryption certificate-name testcert
```