

Firewall-and-NAT Access Ruledef Configuration Mode Commands

The Firewall-and-NAT Access Ruledef Configuration Mode is used to configure and manage Access rule definitions used by the Stateful Firewall (FW) and Network Address Translation (NAT) in-line services.

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

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

- bearer 3gpp apn, on page 2
- bearer 3gpp imsi, on page 3
- bearer username, on page 4
- create-log-record, on page 5
- end, on page 6
- exit, on page 6
- icmp any-match, on page 7
- icmp code, on page 8
- icmp type, on page 9
- icmpv6 any-match, on page 10
- icmpv6 code, on page 11
- icmpv6 type, on page 12
- ip any-match, on page 13
- ip downlink, on page 14
- ip dst-address, on page 15
- ip protocol, on page 16
- ip server-ip-address, on page 17
- ip server-ipv6-network-prefix, on page 18
- ip src-address, on page 19

- ip uplink, on page 21
- ip version, on page 22
- tcp any-match, on page 22
- tcp client-port, on page 23
- tcp dst-port, on page 25
- tcp either-port, on page 26
- tcp server-port, on page 28
- tcp src-port, on page 29
- udp any-match, on page 30
- udp client-port, on page 31
- udp dst-port, on page 33
- udp either-port, on page 34
- udp server-port, on page 35
- udp src-port, on page 37

bearer 3gpp apn

This command configures an access ruledef to analyze user traffic based on APN bearer.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs-fw-ruledef)#`

Syntax Description

`[ no ] bearer 3gpp apn [ case-sensitive ]` *`operator value`*

no

Removes previously configured bearer ruledef.

case-sensitive

This keyword makes the rule case sensitive.

By default, ruledefs are not case sensitive.

Default: Disabled

operator

Specifies how to logically match the APN name.

operator must be one of the following:

- **!=**: Does not equal

- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- =: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

value

The APN name to match in bearer flow.

value must be an alphanumeric string of 1 through 63 characters that can include punctuation characters.

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on APN name.

Example

The following command creates an access ruledef for analyzing user traffic for an APN named *apn12*:

```
bearer 3gpp apn = apn12
```

bearer 3gpp imsi

This command configures an access ruledef to analyze user traffic based on International Mobile Station Identification (IMSI) number in bearer flow.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

[no] bearer 3gpp imsi { *operator msid* | { !range | range } imsi-pool *imsi_pool* }

no

Removes previously configured bearer ruledef.

operator

Specifies how to logically match the MSID.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

msid

Specifies the Mobile Station Identifier.

{ !range | range } imsi-pool *imsi_pool*

{ !range | range }: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

imsi-pool *imsi_pool*: Specifies the IMSI pool name. *imsi_pool* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines Use this command to specify an access ruledef to analyze user traffic based on IMSI number of mobile station.

Example

The following command creates an access ruledef to analyze user traffic for the IMSI number *9198838330912*:

```
bearer 3gpp imsi = 9198838330912
```

bearer username

This command configures an access ruledef to analyze user traffic based on user name of the bearer flow.

Product PSF

NAT

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description **[no] bearer username [case-sensitive]** *operator value*

no

Removes previously configured bearer ruledef.

case-sensitive

This keyword makes the rule case sensitive.

By default, ruledefs are not case sensitive.

Default: Disabled

operator

Specifies how to logically match the MSID.

operator must be one of the following:

- **!=**: Does not equal
- **!contains**: Does not contain
- **!ends-with**: Does not end with
- **!starts-with**: Does not start with
- **=**: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

value

Specifies the user name.

value must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to specify a access ruledef to analyze user traffic based on user name of the bearer flow.

Example

The following command creates an access ruledef for analyzing user traffic for the user name *user12*:

```
bearer username = user12
```

create-log-record

This command enables/disables access ruledef logging.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs-fw-ruledef)#`

Syntax Description

`[ no ] create-log-record`

`no`

Disables access ruledef logging.

Usage Guidelines

Use this command to enable/disable access ruledef logging.

Example

The following command enables access ruledef logging:

`create-log-record`

The following command disables access ruledef logging:

`no create-log-record`

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.

icmp any-match

This command configures an access ruledef to match any ICMPv4 traffic for the user.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-acs-fw-ruledef)#`

Syntax Description

`[ no ] icmp any-match` *`operator condition`*

no

Removes previously configured ICMPv4 any-match ruledef.

operator

Specifies how to logically match the analyzed state.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to be matched for the user traffic.

condition must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

Usage Guidelines

Use this command to specify an access ruledef to match any ICMPv4 traffic of the user.

Example

The following command creates an access ruledef to match any non-ICMPv4 traffic of the user:

```
icmp any-match = FALSE
```

icmp code

This command configures an access ruledef to analyze user traffic based on ICMPv4 code.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] icmp code` *operator code*

no

Removes previously configured ICMPv4 code ruledef.

operator

Specifies how to logically match the ICMPv4 code.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

code

Specifies the ICMPv4 code.

code must be an integer from 0 through 255.

Usage Guidelines

Use this command to define an access ruledef to analyze user traffic based on the ICMPv4 code.

Example

The following command creates an access ruledef for analyzing user traffic using the ICMPv4 code as *23*:

```
icmp code = 23
```

icmp type

This command configures an access ruledef to analyze user traffic based on ICMPv4 type.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] icmp type` *`operator type`*

no

Removes previously configured ICMPv4 type ruledef.

operator

Specifies how to logically match the ICMPv4 type.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

type

Specifies the ICMPv4 type.

type must be an integer from 0 through 255.

For example, 0 for ECHO Reply, 3 for Dest. Unreachable, and 5 for Redirect.

Usage Guidelines

Use this command to define an access ruledef to analyze user traffic based on the ICMPv4 type.

Example

The following command creates an access ruledef for analyzing user traffic using an ICMPv4 type as *123*:

```
icmp type = 123
```

icmpv6 any-match

This command configures an access ruledef to match any ICMPv6 traffic for the user.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-acs-fw-ruledef)#`

Syntax Description

`[ no ] icmpv6 any-match` *`operator condition`*

no

Removes previously configured ICMPv6 any-match ruledef.

operator

Specifies how to logically match the analyzed state.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to be matched for the user traffic.

condition must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

Usage Guidelines

Use this command to specify an access ruledef to match any ICMPv6 traffic of the user.

Example

The following command creates an access ruledef to match any non-ICMPv6 traffic of the user:

```
icmpv6 any-match = FALSE
```

icmpv6 code

This command configures an access ruledef to analyze user traffic based on ICMPv6 code.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] icmpv6 code` *`operator code`*

no

Removes previously configured ICMPv6 code ruledef.

operator

Specifies how to logically match the ICMPv6 code.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

code

Specifies the ICMPv6 code.

code must be an integer from 0 through 255.

Usage Guidelines

Use this command to define an access ruledef to analyze user traffic based on the ICMPv6 code.

Example

The following command creates an access ruledef for analyzing user traffic using the ICMPv6 code as *23*:

```
icmpv6 code = 23
```

icmpv6 type

This command configures an access ruledef to analyze user traffic based on ICMPv6 type.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] icmpv6 type` *operator type*

no

Removes previously configured ICMPv6 type ruledef.

operator

Specifies how to logically match the ICMPv6 type.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

type

Specifies the ICMPv6 type.

type must be an integer from 0 through 255.

For example, 0 for ECHO Reply, 3 for Dest. Unreachable, and 5 for Redirect.

Usage Guidelines

Use this command to define an access ruledef to analyze user traffic based on the ICMPv6 type.

Example

The following command creates an access ruledef for analyzing user traffic using an ICMPv6 type as *123*:

```
icmpv6 type = 123
```

ip any-match

This command configures an access ruledef to match any IP traffic for the user.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-acs-fw-ruledef)#`

Syntax Description

`[ no ] ip any-match` *`operator condition`*

no

Removes previously configured IP any-match ruledef.

operator

Specifies how to logically match the analyzed state.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to be matched for the user traffic.

condition must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

Usage Guidelines

Use this command to specify an access ruledef to match any IP traffic of the user.

Example

The following command creates an access ruledef to match any non-IP traffic of the user:

`ip any-match = FALSE`

ip downlink

This command configures an access ruledef to analyze user traffic based on IP packet flow in downlink direction (to subscriber).

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] ip downlink` *`operator condition`*

no

Removes previously configured IP ruledef.

operator

Specifies how to logically match the packet flow direction.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.

condition must be one of the following:

- **TRUE**: Analyzed
- **FALSE**: Not analyzed

Usage Guidelines

Use this command to define an access ruledef to analyze user traffic based on the IP packet flow direction as downlink.

Example

The following command creates access ruledef for analyzing user traffic using an IP packet direction to downlink (to subscriber):

```
ip downlink = TRUE
```

ip dst-address

This command configures an access ruledef to analyze user traffic based on IP destination address.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] ip dst-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool }`

no

Removes previously configured IP destination address ruledef.

***operator* { *ipv4/ipv6_address* | *ipv4/ipv6_address/mask* }**

operator specifies how to logically match the IP destination address.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

ipv4/ipv6_address: Specifies the IP address of destination node for outgoing traffic. *ipv4/ipv6_address* must be the IP address entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

ipv4/ipv6_address/mask: Specifies the IP address of destination node for outgoing traffic. *ipv4/ipv6_address/mask* must be the IP address entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation. The mask bit is a numeric value which is the number of bits in the subnet mask.

{ !range | range } host-pool *host_pool* }

!range | range: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

host-pool *host_pool*: Specifies the host pool name. *host_pool* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on the IP destination address.

Example

The following command creates IP ruledef for analyzing user traffic using an IP destination address of *209.165.200.234*:

```
ip dst-address = 209.165.200.234
```

ip protocol

This command configures an access ruledef to analyze user traffic based on the protocol being transported by IP packets.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] ip protocol { { `*`operator`*** **` { `***`protocol`*** **` | `***`protocol_assignment`*** **` } } | { `***`operator protocol_assignment`*** **` } }`**

no

Removes previously configured IP protocol address ruledef.

***operator* { *protocol* | *protocol_assignment* }**

operator: Specifies how to logically match the IP protocol.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

protocol: Specifies the protocol by name.

protocol must be one of the following:

- ah
- esp

- gre
- icmp
- tcp
- udp

protocol_assignment: Specifies the protocol by assignment number. *protocol_assignment* must be an integer from 0 through 255 (for example, 1 for ICMP, 6 for TCP, and 17 for UDP).

operator protocol_assignment

operator: Specifies how to logically match the IP protocol.

operator must be one of the following:

- <=: Less than or equals
- >=: Greater than or equals

protocol_assignment: Specifies the protocol by assignment number.

protocol_assignment must be an integer from 0 through 255 (for example, 1 for ICMP, 6 for TCP, and 17 for UDP).

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on the IP protocol.

Example

The following command creates IP ruledef for analyzing user traffic using a protocol assignment of *1*:

```
ip protocol = 1
```

ip server-ip-address

This command configures an access ruledef to analyze user traffic based on IP server address.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] ip server-ip-address {` *`operator`* **`{`** *`ipv4/ipv6_address`* **`|`** *`ipv4/ipv6_address/mask`* **`} | { !range | range } host-pool`** *`host_pool_name`* **`}`**

no

Removes previously configured IP server address.

***operator*{ *ipv4/ipv6_address* | *ipv4/ipv6_address/mask*}**

operator: Specifies how to logically match the IP server address.

operator must be one of the following:

- **!=**: Does not equal
- <=: Less than or equals
- =: Equals
- >=: Greater than or equals

ipv4/ipv6_address: Specifies the server IP address. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. *ipv4/ipv6_address* must be an IP address in IPv4-dotted decimal notation or IPv6 colon-separated hexadecimal notation.

ipv4/ipv6_address/mask: Specifies the server IP address with subnet mask bit. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. *ipv4/ipv6_address/mask* must be an IP address in IPv4 dotted-decimal notation or IPv6 colon-separated hexadecimal notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

{ !range | range } host-pool *host_pool_name*

{ !range | range }: Specifies the range criteria.

- **!range**: Not in the range of
- **range**: In the range of

host-pool *host_pool_name*: Specifies name of the host pool. *host_pool_name* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on IPv4 or IPv6 server address. For uplink packets, this field matches the destination IP address in the IP header. For downlink packets, this field matches the source IP address in the IP header.

Example

The following command creates an IP ruledef for analyzing user traffic using IPv4 server address *209.165.200.234*:

```
ip server-ip-address = 209.165.200.234
```

ip server-ipv6-network-prefix

This command configures an access ruledef to analyze user traffic based on IPv6 server prefix.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

[no] ip server-ipv6-network-prefix *operator ipv6_prefix/prefix_length*

no

Removes previously configured IPv6 server prefix.

operator ipv6_prefix/prefix_length

operator: Specifies how to logically match the IPv6 server prefix.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

ipv6_prefix/prefix_length: Specifies the server's IPv6 address with subnet mask bit. *ipv6_prefix/prefix_length* must be in IPv6 colon-separated-hexadecimal notation with subnet mask bit. The *prefix_length* is the number of bits to match. The configurable prefix length values are 32, 40, 48, 56, 64 and 96.

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on IPv6 server prefix. When a first packet for a flow is received, it is matched against a set of rules configured in the Firewall-and-NAT policy. If the incoming IPv6 packet matches a ruledef and configured prefix, then it indicates that NAT64 needs to be applied on the packet. If the packet did not match the prefix configured, then NAT64 will not be applied on the packet. If there is no rule matching the packet or if there is no rule configured, then the incoming IPv6 packet is matched against the well-known prefix. If the well-known prefix matches, then NAT64 is applied on the packet.

Example

The following command creates an IP ruledef to analyze user traffic using the IPv6 server prefix *abcd:dcba* with *32* bits of the server IPv6 address:

```
ip server-ipv6-network-prefix = abcd:dcba::/32
```

ip src-address

This command configures an access ruledef to analyze user traffic based on IP source address.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

[no] ip src-address { *operator* { *ipv4/ipv6_address* | *ipv4/ipv6_address/mask* } | { !range | range } host-pool *host_pool* }

no

Removes previously configured IP destination address ruledef.

***operator* { *ipv4/ipv6_address* | *ipv4/ipv6_address/mask* }**

operator: Specifies how to logically match the IP source address.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

ipv4/ipv6_address: Specifies the IP address using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

ipv4/ipv6_address/mask: Specifies the IP address using IPV4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

{ !range | range } host-pool *host_pool*

!range | range: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

host-pool *host_pool*: Specifies the host pool name. *host_pool* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on the IP source address.

Example

The following command creates IP ruledef for analyzing user traffic using an IP source address of *209.165.200.234*:

```
ip src-address = 209.165.200.234
```

ip uplink

This command configures an access ruledef to analyze user traffic based on IP packet flow in the uplink direction (from subscriber).

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] ip uplink` *`operator condition`*

no

Removes previously configured IP uplink match ruledef.

operator

Specifies how to logically match the IP packet flow direction.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to match.

condition must be one of the following:

- **TRUE**: Not analyzed
- **FALSE**: Analyzed

Usage Guidelines

Use this command to define an access ruledef to analyze user traffic based on the IP packet flow direction as uplink.

Example

The following command creates access ruledef for analyzing user traffic using an IP packet direction to uplink (from subscriber):

```
ip uplink = TRUE
```

ip version

This command defines rule expressions to match version number in IP header.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

```
[ no ] ip version = { ipv4 | ipv6 }
```

no

Deletes the specified rule expression.

ipv4

Specifies the rule expression for IP version 4.

ipv6

Specifies the rule expression for IP version 6.

Usage Guidelines

Use this command to define rule expressions to match IPv4/IPv6 version number in IP header.

Example

The following command defines a rule expression to match user traffic for the IP version **ipv6**:

```
ip version = ipv6
```

tcp any-match

This command configures an access ruledef to match any TCP traffic for the user.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-acs-fw-ruledef)#`

Syntax Description

`[ no ] tcp any-match` *`operator condition`*

no

Removes previously configured TCP any-match ruledef.

operator

Specifies how to logically match the analyzed state.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

condition

Specifies the condition to be matched for the user traffic.

condition must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

Usage Guidelines

Use this command to specify an access ruledef to match any TCP traffic of the user.

Example

The following command creates an access ruledef to match any non-TCP traffic of the user:

```
tcp any-match = FALSE
```

tcp client-port

This command configures an access ruledef to analyze user traffic based on client TCP port.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] tcp client-port {` *`operator port_number`* **`| { !range | range } {`** *`start_range`* **`to`** *`end_range`* **`| port-map`** *`port_map`* **`} }`**

no

Removes the previously configured client TCP port ruledef.

operator

Specifies how to logically match the port number.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.

port_number must be an integer from 1 through 65535.

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

start_range* to *end_range

Specifies the starting and ending port numbers for the range of destination TCP ports.

start_range must be an integer from 1 through 65535.

end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.

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

Usage Guidelines Use this command to specify an access ruledef to analyze user traffic based on client TCP port.

Example

The following command creates an access ruledef for analyzing user traffic matching client port for TCP as *50*:

```
tcp client-port = 50
```

tcp dst-port

This command configures an access ruledef to analyze user traffic based on destination TCP port.

Product PSF

NAT

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description **`[ no ] tcp dst-port {`** *`operator port_number`* **`| { !range | range } {`** *`start_range`* **`to`** *`end_range`* **`| port-map`** *`port_map`* **`} }`**

no

Removes the previously configured destination TCP port ruledef.

operator

Specifies how to logically match the port number.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.

port_number must be an integer from 1 through 65535.

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

start_range* to *end_range

Specifies the starting and ending port numbers for the range of destination TCP ports.

start_range must be an integer from 1 through 65535.

end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.

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

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on destination TCP port.

Example

The following command creates an access ruledef for analyzing user traffic matching destination port for TCP as *10*:

```
tcp dst-port = 10
```

tcp either-port

This command configures an access ruledef to analyze user traffic based on either (destination or source) TCP ports.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] tcp either-port {` *`operator port_number`* **`| { !range | range } {`** *`start_range`* **`to`** *`end_range`* **`| port-map`** *`port_map`* **`} }`**

no

Removes previously configured TCP either-port (destination or source) ruledef.

operator

Specifies how to logically match the port number.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.

port_number must be an integer from 1 through 65535.

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

start_range* to *end_range

Specifies the starting and ending port numbers for the port range.

start_range must be an integer from 1 through 65535.

end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.

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

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on either TCP port.

Example

The following command creates an access ruledef for analyzing user traffic matching destination or source port for TCP as *10*:

```
tcp either-port = 10
```

tcp server-port

This command configures an access ruledef to analyze user traffic based on server TCP port.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

[no] tcp server-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

no

Removes the previously configured server TCP port ruledef.

operator

Specifies how to logically match the port number.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.

port_number must be an integer from 1 through 65535.

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

start_range* to *end_range

Specifies the starting and ending port numbers for the range of destination TCP ports.

start_range must be an integer from 1 through 65535.

end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.

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

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on server TCP port.

Example

The following command creates an access ruledef for analyzing user traffic matching server port for TCP as *100*:

```
tcp server-port = 100
```

tcp src-port

This command configures an access ruledef to analyze user traffic based on source TCP port.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] tcp src-port {` *operator port_number* **`| { !range | range } {`** *start_range* **`to`** *end_range* **`| port-map`** *port_map* **`} }`**

no

Removes previously configured source TCP port ruledef.

operator

Specifies how to logically match the port number.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.

port_number must be an integer from 1 to 65535.

range | !range

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

start_range* to *end_range

Specifies the starting and ending port numbers for the port range.

start_range must be an integer from 1 through 65535.

end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.

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

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on source TCP port.

Example

The following command creates an access ruledef for analyzing user traffic matching source port for TCP as *10*:

```
tcp src-port = 10
```

udp any-match

This command configures an access ruledef to match any UDP traffic for the user.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] udp any-match` *`operator condition`*

no

Removes previously configured UDP any-match ruledef.

operator

Specifies how to logically match the analyzed state.

operator must be one of the following:

- **!=**: does not equal
- **=**: equals

condition

Specifies the condition to be matched for the user traffic.

condition must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

Usage Guidelines

Use this command to specify an access ruledef to match any UDP traffic of the user.

Example

The following command creates an access ruledef to match any UDP traffic of the user:

```
udp any-match = TRUE
```

udp client-port

This command configures an access ruledef to analyze user traffic based on client UDP port.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] udp client-port {` *`operator port_number`* **`| { !range | range } {`** *`start_range`* **`to`** *`end_range`* **`| port-map`** *`port_map`* **`} }`**

no

Removes previously configured client UDP port ruledef.

operator

Specifies how to logically match the port number.

operator must be one of the following:

- **!=**: Does not equal
- <=: Less than or equals
- =: Equals
- >=: Greater than or equals

port_number

Specifies the port number to match.

port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

start_range* to *end_range

Specifies the starting and ending port numbers for the port range.

start_range must be an integer from 1 through 65535.

end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.

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

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on client UDP port.

Example

The following command creates an access ruledef for analyzing user traffic matching client port for UDP as *10*:

```
udp client-port = 10
```

udp dst-port

This command configures an access ruledef to analyze user traffic based on destination UDP port.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

[no] udp dst-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

no

Removes previously configured destination UDP ports ruledef.

operator

Specifies how to logically match the port number.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.

port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

start_range* to *end_range

Specifies the starting and ending port numbers for the port range.

start_range must be an integer from 1 through 65535.

end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.

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

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on destination UDP port.

Example

The following command creates an access ruledef for analyzing user traffic matching destination port for UDP as *10*:

```
udp dst-port = 10
```

udp either-port

This command configures an access ruledef to analyze user traffic based on either (destination or source) UDP port.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] udp either-port {` *`operator port_number`* **`| { !range | range } {`** *`start_range`* **`to`** *`end_range`* **`| port-map`** *`port_map`* **`} }`**

no

Removes previously configured either-port (destination or source) UDP ruledef.

operator

Specifies how to logically match the port number.

operator must be one of the following:

- **!=**: Does not equal
- <=: Less than or equals

- =: Equals
- >=: Greater than or equals

port_number

Specifies the port number to match.

port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

start_range* to *end_range

Specifies the starting and ending port numbers for the port range.

start_range must be an integer from 1 through 65535.

end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.

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

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on either UDP port.

Example

The following command creates an access ruledef for analyzing user traffic matching destination or source port for UDP as *10*:

```
udp either-port = 10
```

udp server-port

This command configures an access ruledef to analyze user traffic based on server UDP port.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* > **access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

[no] udp server-port { *operator port_number* **| { !range | range } {** *start_range* **to** *end_range* **| port-map** *port_map* **} }**

no

Removes previously configured server UDP port ruledef.

operator

Specifies how to logically match the port number.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.

port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

start_range to *end_range*

Specifies the starting and ending port numbers for the port range.

start_range must be an integer from 1 through 65535.

end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.

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

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on server UDP port.

Example

The following command creates an access ruledef for analyzing user traffic matching server port for UDP as *100*:

```
udp server-port = 100
```

udp src-port

This command configures an access ruledef to analyze user traffic based on source UDP port.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service *service_name* **> access-ruledef** *access_ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

Syntax Description

`[ no ] udp src-port {` *`operator port_number`* **`| { !range | range } {`** *`start_range`* **`to`** *`end_range`* **`| port-map`** *`port_map`* **`} }`**

no

Removes previously configured source UDP port ruledef.

operator

Specifies how to logically match the port number.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

port_number

Specifies the port number to match.

port_number must be an integer from 1 through 65535.

!range | range

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

start_range* to *end_range

Specifies the starting and ending port numbers for the port range.

start_range must be an integer from 1 through 65535.

end_range must be an integer from 1 through 65535 that is greater than *start_range*.

port-map *port_map*

Specifies name of the port-map for the port range.

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

Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on source UDP port.

Example

The following command creates an access ruledef for analyzing user traffic matching source port for UDP as *10*:

```
udp src-port = 10
```