



# Firewall-and-NAT Action Configuration Mode Commands

## Command Modes

The Firewall-and-NAT Action Configuration Mode enables configuring Stateful Firewall (FW) and Network Address Translation (NAT) actions.

Exec > ACS Configuration > Firewall-and-NAT Action Configuration

**active-charging service** *service\_name* > **fw-and-nat action** *action\_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-fw-and-nat-action) #
```



### Important

This configuration mode is only available in release 11.0 and later releases. This configuration mode must be used to configure Action-based Stateful Firewall and NAT features.



### Important

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

- [end, on page 1](#)
- [exit, on page 2](#)
- [flow check-point, on page 2](#)

## 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.

## flow check-point

This command checkpoints all the flows matching the Firewall-and NAT action.

---

**Product**

NAT

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Action Configuration

**active-charging service** *service\_name* > **fw-and-nat action** *action\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-action)#
```

---

**Syntax Description**

```
flow check-point [ data-usage data_usage [ and | or ] | time-duration duration
[ and | or ] ]
{ default | no } flow check-point
```

**default**

Configures the default Firewall action.

**no**

Deletes the Firewall action configuration.

**data-usage** *data\_usage*

Specifies the data usage in bytes.

*data\_usage* must be an integer from 1 through 4294967295.

The maximum limit for data-usage is 4 GB.

**time-duration** *duration*

Specifies the time duration in seconds.

*duration* must be an integer from 1 through 86400.

The maximum limit for time-duration is 24 hours.

#### **and | or**

This option allows to configure only **data-usage** or **time-duration**, or a combination of **data-usage** and **time-duration**.

---

#### **Usage Guidelines**

Use this command to enable/disable the check-pointing of NATed flows and control the type of flows that need to be check pointed based on specified criteria. Check pointing is done only for TCP and UDP flows.

#### **Example**

The following command checkpoints flows with data-usage set to 5000 bytes and time duration set to 300 seconds:

```
flow check-point data-usage 5000 and time-duration 300
```

flow check-point