Firewall-and-NAT Policy Configuration Mode Commands

Command Modes

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

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Important This configuration mode is only available in 8.1, 9.0, and later releases. This configuration mode must be used to configure Policy-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).

access-rule

This command creates and configures an access rule.

Product

PSF

NAT

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* > **fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

access-rule { no-ruledef-matches { downlink | uplink } action { deny [charging-action *charging_action* **] | permit [bypass-nat | nat-realm** *nat_realm* **[fw-and-nat-action** *name* **]] } | priority** *priority* **{ [dynamic-only | static-and-dynamic] access-ruledef** *ruledef_name* **{ deny [charging-action** *charging_action* **] | permit [[bypass-nat | nat-realm** *nat_realm* **[fw-and-nat-action** *name* **]] | trigger open-port { port_number | range** *start_port* **to** *end_port* **} direction { both | reverse | same }] } } }**
default access-rule no-ruledef-matches { downlink | uplink } action
no access-rule priority *priority*

default

Configures the default setting.

Default: Uplink direction: **permit**; Downlink direction: **deny**

no

Removes the access rule specified by the priority.

no-ruledef-matches

Configures action on packets with no ruledef match.

downlink

Specifies to act on downlink packets with no ruledef match.

uplink

Specifies to act on uplink packets with no ruledef match.

action

Specifies action to take on downlink/uplink packets with no ruledef match.

deny

Specifies to deny packets.

permit

Specifies to permit packets and allow the creation of data flows.

charging-action *charging_action*

Specifies the charging action. Optionally, a charging action can be configured for deny action. If a packet matches the deny rule, action is taken as configured in the charging action. If a charging action is specified, the content-ID and billing-action configured in the charging action are used. Also, the flow may be terminated (instead of just discarding the packet), if so configured in the specified charging action.

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

bypass-nat

Important In 9.0 and later releases, this keyword is NAT license dependent.

Specifies to bypass NAT.

nat-realm *nat_realm*

Important In 9.0 and later releases, this keyword is NAT license dependent.

Specifies the NAT realm to be used to perform NAT on subscriber packets matching the access ruledef. If the NAT realm is not specified, NAT will be bypassed. That is, NAT will not be performed on subscriber packets that are matching a ruledef with no NAT realm name configured in it.

nat_realm must be an alphanumeric string of 1 through 31 characters.

priority *priority*

Specifies priority of an access ruledef in the Firewall-and-NAT policy.

priority must be an integer from 1 through 65535 that is unique for each access ruledef in the Firewall-and-NAT policy.

[dynamic-only | static-and-dynamic] access-ruledef *ruledef_name*

Specifies the access ruledef name. Optionally, the ruledef type can also be specified.

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

trigger open-port { *port_number* | range *start_port* to *end_port* } direction { both | reverse | same }

Important In 9.0 and later releases, this keyword is Stateful Firewall license dependent.

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.

- *port_number*: Specifies the auxiliary port number to open for traffic, and must be an integer from 1 through 65535.
- **range** *start_port* **to** *end_port*: Specifies the range of port numbers to open for subscriber traffic.
  - *start_port* must be an integer from 1 through 65535.
  - *end_port* must be an integer from 1 through 65535, and must be greater than *start_port*.
- **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 access ruledefs to the Firewall-and-NAT policy and configure the priority and actions for rule matching.

The policy specifies the rules to be applied on calls. The ruledefs in the policy have priorities, based on which priority matching is done.

For Stateful Firewall, the port trigger configuration is optional, and can be configured only if a rule action is permit. When 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 that matches the rule. Multiple triggers can be defined for the same port number to permit multiple auxiliary ports for subscriber traffic.

When 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 Event Data Record (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, only the terminate-flow action is applicable if configured in the specified charging action.

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.
- Access ruledef matching is done. If a rule matches, the packet is allowed or dropped as per the **access-rule priority** configuration.
- If no access ruledef matches, the packet is allowed or dropped as per the **access-rule no-ruledef-matches** configuration.

For a packet dropped due to access ruledef match or no match (first packet of a flow), 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 in the ACS Rulebase Configuration Mode.

The GGSN can dynamically activate or deactivate dynamic ruledefs for a subscriber based on the rule name received from a policy server. At rule match, if a rule in the policy 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

For Stateful Firewall, the following command assigns a priority of *10* to the access ruledef *test_rule*, adds it to the policy, and permits port trigger to be used for the rule to open ports in the range of *1000* to *2000* in either direction of the control connection:

```
access-rule priority 1 access-ruledef test_rule permit trigger open-port
 range 1000 to 2000 direction both
```

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.

firewall dos-protection

This command configures Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks.

Important In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] firewall dos-protection { all | flooding { icmp | tcp-syn | udp } | ftp-bounce | ip-sweep { icmp | tcp-syn | udp } | ip-unaligned-timestamp | ipv6-dst-options [invalid-options | unknown-options] | ipv6-extension-hdrs [limit *extension_limit* **] | ipv6-frag-hdr nested-fragmentation | ipv6-hop-by-hop [invalid-options | jumbo-payload | router-alert | unknown-options] | mime-flood | port-scan | source-router | tcp-window-containment | teardrop | winnuke }**
default firewall dos-protection

no

Disables Stateful Firewall protection for subscribers against the specified Denial of Service (DoS) attack(s).

default

Disables Stateful Firewall protection for subscribers against all DoS attacks.

all

Enables Stateful Firewall protection for subscribers against all DoS attacks supported by the Stateful Firewall service.

The IPv6 extension headers will be enabled only if the **firewall validate-ip-options** command is enabled in the Firewall-and-NAT policy configuration.

flooding { icmp | tcp-syn | udp }

Enables protection against the specified flooding attack:

- **icmp**: Enables protection against ICMP Flood attack.
- **tcp-syn**: Enables protection against TCP Syn Flood attack.
- **udp**: Enables protection against UDP Flood attack.

ftp-bounce

Enables protection against FTP Bounce attacks.

ip-sweep { icmp | tcp-syn | udp }

Enables protection against IP Sweep attacks in the downlink direction.

- **icmp**: Enables protection against ICMP IP Sweep attack.

- **tcp-syn**: Enables protection against TCP Syn IP Sweep attack.
- **udp**: Enables protection against UDP IP Sweep attack.

IP Sweep attacks are also detected in the uplink direction. The **firewall dos-protection ip-sweep** command must be configured in the ACS Configuration mode. The configuration values for packet limit and sampling interval are common for both uplink and downlink.

ip-unaligned-timestamp

Enables protection against IP Unaligned Timestamp attacks.

ipv6-dst-options [invalid-options | unknown-options]

Drops IPv6 packets containing the IPv6 destination options header.

The following options are specified in the Destination Options extension header:

- The Tunnel Encapsulation Limit (option type: 0x04) is a destination option defined in RFC 2473.
- The Home Address option (option type: 0xC9) is part of Mobile IP processing defined in RFC 3775. This option is only valid as a Destination Option.
- The NSAP Address option (option type: 0xC3) is assigned as a Destination Option by RFC 1888 and deprecated (reclassified as historic) by RFC 4048.
- **invalid-options**: Drops IPv6 packets containing invalid IPv6 destination options.

  The following values are invalid in a Destination Options extension header option type field. Packets with these options in a Destination Options header will be dropped.

  - Value 0xC2, Jumbo Payload
  - Value 0x05, Router Alert
  - Value 0x06, Quick start
  - Value 0x07, CALIPSO

- **unknown-options**: Drops IPv6 packets containing unknown IPv6 destination options.

ipv6-extension-hdrs [limit *extension_limit*]

Default: 8

Limits the number of IPv6 extension headers in an IPv6 packet. An IPv6 packet can contain zero or more extension headers.

Firewall will not fully parse packets with unknown extension headers as the extension header format is unspecified. Under such cases, the transport protocol will be considered as **unknown**. Packets with invalid length field in the extension headers and packets with next header 0x01 (ICMPv4) will be dropped. IPv6 uses ICMPv6 of type 0x3A.

extension_limit must be an integer from 0 through 4294967295.

ipv6-frag-hdr nested-fragmentation

Drops IPv6 packets containing nested fragmentation (reassembled packets containing a fragment header).

IPv6 fragmentation is done only by the source node. An IPv6 fragment packet must have only one fragment header. Firewall will drop packets with more than one fragment header. The Reassembled packet containing a fragment header will be dropped by Firewall. As per RFC 2460, the fragment length (except for last fragment) must be a multiple of 8 octets. If not, such fragments are dropped.

ipv6-hop-by-hop [invalid-options | jumbo-payload | router-alert | unknown-options]

Drops IPv6 packets containing the hop-by-hop extension header.

The Hop-by-Hop Options extension header, if present, must be the first header to follow the IPv6 main header. This is indicated by a value of 0x00 in the next header field in the main header. The length must be expressed as a multiple of 8 octets (excluding the first 8 octets). If not, such packets will be dropped.

- **invalid-options**: Drops IPv6 packets containing invalid IPv6 hop-by-hop options.

  The following values are invalid in a Hop-by-Hop extension header option type field. Packets with these options in a hop-by-hop header will be dropped.

  - Value 0x04, Tunnel Encapsulation limit
  - Value 0xC9, Home Address Destination option
  - Value 0xC3, NSAP Address option

  The options are present in TLV (Type Length Value) format. If the length specified is invalid, then such packets will be dropped.

- **jumbo-payload**: Drops IPv6 packets with jumbo payload hop-by-hop options.

  The Jumbo Payload option (RFC 2675) has the option type value 0xC2 and is only valid as a Hop-by-Hop option. This option allows the creation of very large IP packets (packets larger than 65K bytes). If this option is allowed, the following validity checks will be done.

  - The IP payload length must be 0x00 when the Jumbo Payload option is present.
  - The Jumbo Payload option must be used only when the length is greater than 65,535; the two most significant bytes of the Jumbo length cannot be 0x00.
  - The Jumbo Payload option cannot be used in conjunction with a Fragmentation extension header.

  If any of the above checks fail, then the IPv6 packet will be dropped. The Option Type field must have 4n+2 alignment.

- **router-alert**: Drops IPv6 packets with router alert hop-by-hop options.

  The Router Alert (RFC 2711) option is used to signal the routers that a closer inspection of the packet is warranted. Denial of service (DoS) attacks can occur if an attacker sends large number of packets with this option. Only one option of this type must be present, regardless of value, per Hop-by-Hop header with 2n + 0 alignment.

- **unknown-options**: Drops IPv6 packets containing unknown IPv6 hop-by-hop options.

mime-flood

Enables protection against HTTP Multiple Internet Mail Extension (MIME) header flooding attacks.

port-scan

Enables protection against Port Scan attacks.

tcp-window-containment

Enables protection against TCP sequence number out-of-range attacks.

source-router

Enables protection against IPv4/IPv6 Source Route IP Option attacks.

This command can be used to filter IPv4/IPv6 packets containing Routing header of Type 0 (source routing). In this release, only type 0 filtering is supported.

teardrop

Enables protection against IPv4/IPv6 Teardrop attacks.

winnuke

Enables protection against WIN-NUKE attacks.

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 DoS attacks are detected only in the downlink direction.

Example

The following command enables protection from all supported DoS attacks:

```
firewall dos-protection all
```

firewall flooding

This command configures Stateful Firewall protection from Packet Flooding attacks.

Important In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

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 the default setting for the specified configuration.

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

The maximum sampling-interval configurable is 60 seconds.

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 than *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 IP addresses, 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 limit 1000
```

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

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

firewall icmp-checksum-error

This command configures Stateful Firewall action on packets with ICMP/ICMPv6 Checksum errors.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
firewall icmp-checksum-error { drop | permit }
default firewall icmp-checksum-error
```

default

Configures the default setting.

Default: **drop**

drop

Drops packets with ICMP/ICMPv6 Checksum errors.

permit

Permits packets with ICMP/ICMPv6 Checksum errors.

Usage Guidelines

Use this command to configure Stateful Firewall action on packets with ICMP/ICMPv6 Checksum errors. This command also applies to ICMP/ICMPv6 packets with Inner IP Checksum error.

For NAT-only calls, packets with ICMP/ICMPv6 errors are dropped, and other packets are allowed.

Example

The following command configures Stateful Firewall to drop packets with ICMP/ICMPv6 Checksum errors:

```
firewall icmp-checksum-error drop
```

firewall icmp-destination-unreachable-message-threshold

This command configures a threshold on the number of ICMP/ICMPv6 error messages sent by the subscriber for a particular data flow.

Important In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

Configures the default setting.

Default: No limit

no

Removes the previous configuration.

messages

Specifies the threshold on the number of ICMP/ICMPv6 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/ICMPv6 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/ICMPv6 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/ICMPv6 error messages:

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

firewall icmp-echo-id-zero

This command configures Stateful Firewall action on echo packets with ICMP/ICMPv6 ID zero.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
firewall icmp-echo-id-zero { drop | permit }
default firewall icmp-echo-id-zero
```

default

Configures the default setting.

Default: **permit**

drop

Drops packets with ICMP/ICMPv6 ID zero.

permit

Permits packets with ICMP/ICMPv6 ID zero.

Usage Guidelines

Use this command to configure Stateful Firewall action on echo packets with ICMP/ICMPv6 ID zero.

Example

The following command configures Stateful Firewall to drop packets with ICMP/ICMPv6 ID zero:

```
firewall icmp-echo-id-zero drop
```

firewall icmp-fsm

This command enables/disables Stateful Firewall's ICMP/ICMPv6 Finite State Machine (FSM).

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] firewall icmp-fsm`

default

Configures the default setting.

Default: Enabled. Same as **firewall icmp-fsm**.

no

Disables Stateful Firewall ICMP/ICMPv6 FSM checks.

Usage Guidelines

Use this command to enable/disable Stateful Firewall ICMP/ICMPv6 FSM checks. When Stateful Firewall and ICMP/ICMPv6 FSM are enabled, ICMP/ICMPv6 reply messages for which there is no saved ICMP/ICMPv6 request message are discarded. ICMP/ICMPv6 error messages (i.e., messages containing an embedded message) for which there is no saved flow for the embedded message are discarded.

Example

The following command disables Stateful Firewall's ICMP/ICMPv6 FSM checks:

`no firewall icmp-fsm`

firewall ip-reassembly-failure

This command configures Stateful Firewall action on IPv4/IPv6 packets involved in IP Reassembly Failure scenarios.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
firewall ip-reassembly-failure { drop | permit }
default firewall ip-reassembly-failure
```

default

Configures the default setting.

Default: **permit**

drop

Drops IPv4/IPv6 packets involved in IP reassembly failure scenarios.

permit

Permits IPv4/IPv6 packets involved in IP reassembly failure scenarios.

Usage Guidelines

Use this command to configure Stateful Firewall action on IPv4/IPv6 packets involved in IP reassembly failure scenarios such as missing fragments, overlapping offset, etc.

For NAT-only calls, packets involved in IP reassembly failure scenarios are dropped.

Example

The following command specifies to drop IPv4/IPv6 packets involved in IP reassembly failure scenarios:

```
firewall ip-reassembly-failure drop
```

firewall malformed-packets

This command configures Stateful Firewall action on malformed packets. In release 12.0, this command supports ICMPv6 and IPv6 packets.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
firewall malformed-packets { drop | permit }
default firewall malformed-packets
```

default

Configures the default setting.

Default: **permit**

drop

Drops malformed packets.

permit

Permits malformed packets.

Usage Guidelines

Use this command to configure Stateful Firewall action on malformed packets.

For NAT-only calls, malformed packets are always permitted.

Example

The following command specifies Stateful Firewall to drop malformed packets:

```
firewall malformed-packets drop
```

firewall max-ip-packet-size

This command configures the maximum IPv4/IPv6 packet size (after IP reassembly) allowed over Stateful Firewall.

Important In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

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 setting.

Default: 65535 bytes (for both ICMP/ICMPv6 and non-ICMP/ICMPv6)

packet_size

Specifies the maximum packet size allowed by firewall. Any IPv6 packet with payload size greater than the configured value will be dropped.

packet_size must be an integer from 30000 through 65535.

protocol { icmp | non-icmp }

Specifies the transport protocol:

- **icmp**: Configuration for ICMP/ICMPv6 protocol.
- **non-icmp**: Configuration for protocols other than ICMP/ICMPv6.

Usage Guidelines

Use this command to configure the maximum IPv4/IPv6 packet size allowed for ICMP/ICMPv6 and non-ICMP/ICMPv6 packets to prevent packet flooding attacks to the host. Packets exceeding the configured size will be dropped for "Jolt" and "Ping-Of-Death" attacks.

Example

The following command allows a maximum packet size of *60000* for ICMP/ICMPv6 protocol:

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

firewall mime-flood

This command configures Stateful Firewall protection from MIME Flood attacks.

Important In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

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 the default setting for the specified parameter.

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.

This command is only effective if Stateful Firewall DoS protection for MIME flood attacks has been enabled using the **firewall dos-protection mime-flood** command, and the **route** command has been configured to send HTTP packets to the HTTP analyzer.

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 policy

This command enables/disables Stateful Firewall support in a Firewall-and-NAT policy.

Important

In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

In 11.0 and earlier releases:

```
firewall policy firewall-required
no firewall policy
```

In 12.0 and later releases:

```
firewall policy { ipv4-and-ipv6 | ipv4-only | ipv6-only }
{ default | no } firewall policy
```

default

Disables IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

no

Disables IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

firewall-required

Enables Stateful Firewall support in the Firewall-and-NAT policy.

Important This keyword is available only in 11.0 and earlier releases.

ipv4-and-ipv6

Enables both IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

ipv4-only

Enables IPv4 Stateful Firewall and disables IPv6 Stateful Firewall in the Firewall-and-NAT policy.

ipv6-only

Enables IPv6 Stateful Firewall and disables IPv4 Stateful Firewall support in the Firewall-and-NAT policy.

Usage Guidelines

Use this command to enable/disable IPv4 and/or IPv6 Stateful Firewall support for all subscribers using a Firewall-and-NAT policy.

Example

The following command enables IPv4 and IPv6 Stateful Firewall support in a Firewall-and-NAT policy:

```
firewall policy ipv4-and-ipv6
```

The following command disables Stateful Firewall support in a Firewall-and-NAT policy:

```
no firewall policy
```

firewall tcp-checksum-error

This command configures Stateful Firewall action on packets with TCP Checksum error.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
firewall tcp-checksum-error { drop | permit }
default firewall tcp-checksum-error
```

default

Configures the default setting.

Default: **drop**

drop

Drops packets with TCP Checksum errors.

permit

Permits packets with TCP Checksum errors.

Usage Guidelines

Use this command to configure Stateful Firewall action on packets with TCP Checksum error.

For NAT-only calls, packets with TCP Checksum errors are permitted.

Example

The following command specifies Stateful Firewall to drop packets with TCP Checksum errors:

```
firewall tcp-checksum-error drop
```

firewall tcp-first-packet-non-syn

This command configures Stateful Firewall action on TCP flows starting with a non-SYN packet.

Important In release 9.0, this command is deprecated. This configuration is available as the **firewall tcp-fsm [first-packet-non-syn { drop | permit | send-reset }]** command.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

Configures the default setting.

Default: **drop**

drop

Drops the non-SYN packet.

reset

Sends reset.

Usage Guidelines

Use this command to configure Stateful Firewall action on TCP flows starting with a non-SYN packet.

Example

For flows starting with a non-SYN packet, the following command specifies Stateful Firewall to drop the non-SYN packet:

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

firewall tcp-fsm

This command enables/disables Stateful Firewall's TCP Finite State Machine (FSM).

Product PSF

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **firewall tcp-fsm [first-packet-non-syn { drop | permit | send-reset }] { default | no } firewall tcp-fsm**

default

Configures the default setting.

Default: **drop**

no

Disables Stateful Firewall's TCP FSM.

first-packet-non-syn { drop | permit | send-reset }

Specifies Stateful Firewall action on TCP flows starting with a non-SYN packet:

- **drop**: Specifies to drop the packet.
- **permit**: Specifies to permit the packet.
- **send-reset**: Specifies to drop the packet and send TCP RST.

Default: **drop**

Usage Guidelines Use this command to enable/disable Stateful Firewall's TCP FSM checks. When Stateful Firewall and TCP FSM are enabled, state of the TCP session is checked to decide whether to forward TCP packets.

Example

The following command enables TCP FSM, and configures action to take on TCP flows starting with a non-SYN packet to drop the packet:

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

firewall tcp-idle-timeout-action

This command configures action on TCP idle timeout expiry.

Important In release 9.0 and later this command is also available to NAT.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`firewall tcp-idle-timeout-action { drop | reset }`
`{ default | no } firewall tcp-idle-timeout-action`

default

Configures the default setting.

Default: **reset**

no

Configures the TCP idle timeout expiry action to reset.

drop

Drops the session on TCP idle timeout expiry.

reset

Resends TCP RST on TCP idle timeout expiry. When configured to reset, the session is dropped, and the system can avoid packets arriving for the idle flow from getting dropped.

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-options-error

This command configures Stateful Firewall action on packets with TCP Option errors.

Product

PSF

Privileges

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

firewall tcp-options-error { drop | permit }
default firewall tcp-options-error

default

Configures the default setting.

Default: **permit**

drop

Drops packets with TCP Option errors.

permit

Permits packets with TCP Option errors.

Usage Guidelines

Use this command to configure Stateful Firewall action on packets with TCP Option errors.

Example

The following command configures Stateful Firewall to drop packets with TCP Option errors:

firewall tcp-options-error drop

firewall tcp-partial-connection-timeout

This command configures action on idle timeout for partially open TCP connections.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

firewall tcp-partial-connection-timeout *timeout*
{ default | no } firewall tcp-partial-connection-timeout

default

Configures the default setting.

no

Disables the idle timeout for partially open TCP connections.

timeout

Specifies the timeout in seconds.

timeout must be an integer from 0 through 86400.

Default: 30 seconds

Usage Guidelines Use this command to configure idle timeout for TCP connections that are yet to be established (partially open) in the case of Firewall enabled calls.

Example

The following command sets the idle timeout setting to *30* seconds:

```
firewall tcp-partial-connection-timeout 30
```

firewall tcp-reset-message-threshold

This command configures 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.

Product PSF

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

Configures the default setting.

Default: Disabled

no

Disables the configuration.

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 (TCP RST+ACK) 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 configures TCP SYN intercept parameters for protection against TCP SYN flooding attacks.

Important

In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

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

Configures the default settings for SYN Flood DoS protection.

mode { none | watch [aggressive] }

Specifies the TCP SYN flood intercept mode:

- **none**: Disables the TCP SYN Flood Intercept feature.
- **watch**: Configures TCP SYN flood intercept feature in watch mode. The Stateful Firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, the 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. This command enables and configures 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.

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 intercept watch timeout setting to *15* seconds:

```
firewall tcp-syn-flood-intercept watch-timeout 15
```

firewall tcp-syn-with-ecn-cwr

This command configures Stateful Firewall action on TCP SYN packets with either ECN or CWR flag set.

Product

PSF

Privileges

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
firewall tcp-syn-with-ecn-cwr { drop | permit }
default firewall tcp-syn-with-ecn-cwr
```

default

Configures the default setting.

Default: **permit**

drop

Drops TCP SYN packets with either ECN or CWR flag set.

permit

Permits TCP SYN packets with either ECN or CWR flag set.

Usage Guidelines

Use this command to configure Stateful Firewall action on receiving a TCP SYN packet with either ECN or CWR flag set.

Example

The following command configures Stateful Firewall to drop TCP SYN packets with ECN / CWR flag set:

```
firewall tcp-syn-with-ecn-cwr drop
```

firewall udp-checksum-error

This command configures Stateful Firewall action on packets with UDP Checksum error.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
firewall udp-checksum-error { drop | permit }
default firewall udp-checksum-error
```

default

Configures the default setting.

Default: **drop**

drop

Drops packets with UDP Checksum error.

permit

Permits packets with UDP Checksum error.

Usage Guidelines

Use this command to configure Stateful Firewall action on packets with UDP Checksum error.

For NAT-only calls, packets with UDP Checksum error are permitted.

Example

The following command specifies to drop packets with UDP Checksum error:

```
firewall udp-checksum-error drop
```

firewall validate-ip-options

This command enables / disables the Stateful Firewall validation of IP options for errors.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] firewall validate-ip-options
```

default

Configures the default setting.

Default: Disabled. Same as **no firewall validate-ip-options**

no

Disables validation of IP options.

Usage Guidelines

Use this command to enable / disable Stateful Firewall validation of IP options. When enabled, Stateful Firewall will drop packets with IP option errors.

For NAT calls, validation of IP Options is disabled.

Example

The following command enables validation of IP options:

```
firewall validate-ip-options
```

nat binding-record

This command configures the generation of NAT Binding Records.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
nat binding-record edr-format edr_format [ port-chunk-allocation ] [
port-chunk-release ]
{ default | no } nat binding-record
```

default

Configures the default setting.

Default: **port-chunk-release**

no

Disables generating NAT Binding Records.

edr-format *edr_format*

Specifies the Event Data Record (EDR) format name.

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

port-chunk-allocation

Specifies generating NAT Binding Records when a port-chunk is allocated.

port-chunk-release

Specifies generating NAT Binding Record when a port-chunk is released.

Usage Guidelines Use this command to configure the generation of NAT Binding Records.

Example

The following command configures an EDR format named *test123* and specifies generating NAT Binding Records when a port chunk is allocated:

```
nat binding-record edr-format test123 port-chunk-allocation
```

nat check-point-info

This command enables or disables the checkpointing of basic NAT, H323 and SIP ALG recovery. ICSR recovery can also be enabled or disabled for basic NAT and SIP flows.

Product

PSF

NAT

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] nat check-point-info { basic [icsr-also | limit-flows *limit* **] | h323-alg | sip-alg [icsr-also] }**

default

Configures this command with its default setting.

Default: Disabled

no

Disables the basic NAT recovery and stand-alone H323 ALG and SIP ALG recovery. Also disables ICSR recovery for SIP ALG.

basic [icsr-also | limit-flows *limit*]

Configures the basic flow checkpointing information.

- **icsr-also**: Enables checkpointing for ICSR.
- **limit-flows**: Limits the specified flows for basic NAT checkpointing. *limit* must be an integer from 1 through 100.

  Default: 100

h323-alg

Enables checkpointing of H323 ALG.

sip-alg [icsr-also]

Enables checkpointing of SIP ALG.

- **icsr-also**: Enables checkpointing for ICSR.

Usage Guidelines Use this command to enable or disable the checkpointing of basic NAT, standalone H323 and SIP ALG recovery. ICSR recovery can also be enabled or disabled for basic NAT and SIP flows. The maximum basic flows that can be checkpointed is also configured. By default, 100 flows can be recovered in a standalone chassis and ICSR setup.

Example

The following command enables basic NAT recovery and ICSR recovery with flows limited to *10*:

```
nat check-point info basic limit-flows 10 icsr-also
```

nat icsr-flow-recovery

This command enables/disables the NAT ICSR Flow checkpointing support for subscribers in a Firewall-and-NAT policy. This command is deprecated in StarOS 14.0 and later releases, and is replaced by the **nat check-point-info** command.

Product NAT

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **`[ default | no ] nat icsr-flow-recovery`**

default

Configures the default setting.

Default: Disabled. Same as **no icsr-flow-recovery**.

no

Disables the NAT ICSR Flow checkpointing.

Usage Guidelines Use this command to enable/disable all NAT ICSR Flow checkpointing for subscribers using this policy.

Example

The following command enables NAT ICSR Flow checkpointing:

```
nat icsr-flow-recovery
```

nat max-chunk-per-realm

This command enables or disables the allocation of multiple NAT IP addresses for the same N:1 NAT realm for a subscriber.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

nat max-chunk-per-realm { multiple-ip | single-ip }
{ default | no } nat max-chunk-per-realm

default

Configures the default setting.

Default: **nat max-chunk-per-realm single-ip**

no

Disables the allocation of multiple NAT IP addresses for the same NAT realm for a subscriber.

multiple-ip

Enables the feature, that is, allows allocation of multiple IP addresses per NAT realm.

single-ip

Allows allocation of only one IP address per NAT realm. If the port chunks get exhausted, packets will be dropped. This is the default behavior.

Usage Guidelines

Use this command to enable or disable the allocation of multiple NAT IP addresses for the same N:1 NAT realm for a subscriber. This enhancement is applicable only for N:1 NAT realms and not for 1:1 NAT realms.

nat pkts-drop

This command is used to configure the EDR format in which records for dropped NAT packets will be saved and the time interval for EDR generation.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

nat pkts-drop { edr-format *edr_format_name* **| timeout** *timeout_value* **}**
{ default | no } nat pkts-drop { edr-format | timeout }

default

Configures the default setting.

Default: Disables the configuration. Same as **no nat pkts-drop { edr-format | timeout }** command.

no

Disables the configured EDR format in which records for dropped NAT packets will be saved and the time interval for EDR generation.

edr-format *edr_format_name*

Specifies the Event Data Record (EDR) format name.

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

timeout *timeout_value*

Specifies the NAT packet drop EDR timeout in seconds.

timeout_value must be an integer from 1 through 86400.

Usage Guidelines

Use this command to configure the EDR format in which records for dropped NAT packets will be saved and the time interval for EDR generation.

Example

The following command configures an EDR format named *test1* and specifies a packet drop timeout of *200* seconds:

```
nat pkts-drop edr-format test1 timeout 200
```

nat policy

This command enables/disables Network Address Translation (NAT) support in a Firewall-and-NAT policy.

Important In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* > **fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

In 12.1 and earlier releases:

nat policy nat-required [default-nat-realm *nat_realm_name* **[fw-and-nat-action** *action_name* **]]**
no nat policy

In 12.2 and later releases:

nat policy [ipv4-and-ipv6 | ipv4-only | ipv6-only] [default-nat-realm *nat_realm_name* **[fw-and-nat-action** *action_name* **]]**
no nat policy

no

Disables both NAT44 and NAT64 support in the Firewall-and-NAT policy.

nat-required

Enables NAT support in the Firewall-and-NAT policy.

Important This keyword is available only in 12.1 and earlier releases, and is supported in release 12.2 for backward compatibility. The **nat policy nat-required** command enables only NAT44.

ipv4-and-ipv6

Enables NAT processing for both IPv4 and IPv6 in the Firewall-and-NAT policy.

ipv4-only

Enables NAT processing for IPv4 in the Firewall-and-NAT policy.

ipv6-only

Enables NAT processing for IPv6 in the Firewall-and-NAT policy.

default-nat-realm *nat_realm_name*

Specifies the default NAT realm for the Firewall-and-NAT policy.

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

fw-and-nat-action *action_name*

Specifies the Firewall-and-NAT action name.

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

Usage Guidelines

Use this command to enable/disable IPv4 and/or IPv6 NAT support for all subscribers using a Firewall-and-NAT policy.

In release 8.1, to enable NAT support for a subscriber, Stateful Firewall must also be enabled for that subscriber. See the **firewall policy** CLI command.

Once NAT is enabled for a subscriber, the NAT IP address to be used is chosen from the NAT realms specified in the rules. See the **access-rule** CLI command.

You can enable/disable NAT at any time, however the changed NAT status will not be applied to active calls. The new NAT status will only be applied to new calls.

Example

The following command enables NAT support in a Firewall-and-NAT policy:

```
nat policy nat-required
```

The following command disables NAT support in a Firewall-and-NAT policy:

```
no nat policy
```

The following command enables IPv4 and IPv6 NAT support in a Firewall-and-NAT policy:

```
nat policy ipv4-and-ipv6
```

nat private-ip-flow-timeout

This command configures the Private IP NPU flow timeout setting.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

nat private-ip-flow-timeout *timeout*
{ default | no } nat private-ip-flow-timeout

default

Configures the default setting.

Default: 180 seconds

no

Disables the Private IP NPU flow timeout configuration.

When disabled, the flow is installed at call setup and will be removed only when the subscriber disconnects.

timeout

Specifies the Private IP NPU flow timeout period in seconds.

timeout must be an integer from 180 through 86400.

Usage Guidelines

Use this command to configure the Private IP NPU flow timeout setting.

For NAT-enabled calls, by default, the downlink private IP NPU flow will not be installed at call setup for a subscriber session. The flow will only be installed on demand. When there is no traffic on the private flow, the private IP flow will be removed after the configurable timeout period.

Example

The following command configures the Private IP NPU flow timeout setting to *36000* seconds:

nat private-ip-flow-timeout 36000

nat suppress-aaa-update

This command suppresses sending NAT Bind Update (NBU) to the AAA server when PPP disconnect happens.

Important This command is customer-specific. For more information please contact your local service representative.

Product

NAT

Privilege

Security Administrator, Administrator

Command Modes

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

active-charging service *service_name* **> fw-and-nat policy** *policy_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
nat suppress-aaa-update call-termination
default nat suppress-aaa-update
```

default

Configures the default setting.

Default: No suppression of AAA updates.

Usage Guidelines

Use this command to suppress sending of NBU to the AAA server when PPP disconnect happens, 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, NBU 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:

```
nat suppress-aaa-update call-termination
```