ACL Configuration Mode Commands

The Access Control List Configuration Mode is used to create and manage IP-based, user access privileges.

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

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

deny/permit (by source IP address masking)

Filters subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
{ deny | permit } [ log ] source_address source_wildcard
after { deny | permit } [ log ] source_address source_wildcard
before { deny | permit } [ log ] source_address source_wildcard
no { deny | permit } [ log ] source_address source_wildcard
```

after

Indicates that all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates that all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

Important The logging option is not supported for ACLs applied on SPIO or local contexts.

source_address

The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Usage Guidelines Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rules as it does not require a rule for each source and destination pair.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines two rules with the second logging filtered packets:

```
permit 1.2.3.0 0.0.0.31
deny log 1.2.4.0 0.0.0.15
```

The following sets the insertion point before the first rule defined above:

```
before permit 1.2.3.0 0.0.0.31
```

The following command sets the insertion point after the second rule defined above:

```
after deny log 1.2.4.0 0.0.0.15
```

The following deletes the first rule defined above:

```
no permit 1.2.3.0 0.0.0.31
```

deny/permit (any)

Filters subscriber sessions based on any packet received. This command is also sets the access control list insertion point.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
{ deny | permit } [ log ] any
after { deny | permit } [ log ] any
before { deny | permit } [ log ] any
no { deny | permit } [ log ] any
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: Packets are not logged.

Indicates all packets which match the filter are to be logged.

Important The logging option is not supported for ACLs applied on SPIO or local contexts.

any

Indicates all packets will match the filter regardless of source and/or destination.

Usage Guidelines

Define a catch all rule to place at the end of the list of rules.

Important

It is suggested that any rule which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security.

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following commands define two rules with the second logging filtered packets:

```
permit any
deny log any
```

The following sets the insertion point before the first rule defined above:

```
before permit any
```

The following command sets the insertion point after the second rule defined above:

```
after deny log any
```

The following deletes the first rule defined above:

```
no permit any
```

deny/permit (by host IP address)

Filters subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
{ deny | permit } [ log ] host source_host_address
after { deny | permit } [ log ] host source_host_address
before { deny | permit } [ log ] host source_host_address
no { deny | permit } [ log ] host source_host_address
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: Packets are not logged.

Indicates that all packets which match the filter are to be logged.

Important The logging option is not supported for ACLs applied on SPIO or local contexts.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

Usage Guidelines

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following commands define two rules with the second logging filtered packets:

```
permit host 10.2.3.4
deny log host 10.2.3.5
```

The following sets the insertion point before the first rule defined above:

```
before permit host 10.2.3.4
```

The following command sets the insertion point after the second rule defined above:

```
after deny log host 10.2.3.5
```

The following deletes the first rule defined above:

```
no permit host 10.2.3.4
```

deny/permit (by source ICMP packets)

Filters subscriber sessions based on the internet control message protocol (ICMP) packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

{ deny | permit } [log] icmp { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [*icmp_type* [*icmp_code*]]

after { deny | permit } [log] icmp { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [*icmp_type* [*icmp_code*]]

before { deny | permit } [log] icmp { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [*icmp_type* [*icmp_code*]]

no { deny | permit } [log] icmp { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [*icmp_type* [*icmp_code*]]

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

Important The logging option is not supported for ACLs applied on SPIO or local contexts.

source_address

The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

Usage Guidelines

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk.

The IP filtering allows flexible controls for pairs of individual hosts or groups by IP masking which allows the filtering of entire subnets if necessary.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following commands define two rules with the second logging filtered packets:

```
permit icmp host 10.2.3.4 any 168
deny log icmp 10.2.3.0 0.0.0.31 host 10.2.4.16 168 11
```

The following sets the insertion point before the first rule defined above:

```
before permit icmp host 10.2.3.4 any 168
```

The following command sets the insertion point after the second rule defined above:

```
after deny log icmp 10.2.3.0 0.0.0.31 host 10.2.4.16 168 11
```

The following deletes the first rule defined above:

```
no permit icmp host 10.2.3.4 any 168
```

deny/permit (by IP packets)

Filters subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

{ deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol *num*]
after { deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol *num*]
before { deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol *num*]
no { deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol *num*]

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: Packets are not logged.

Indicates all packets which match the filter are to be logged.

Important The logging option is not supported for ACLs applied on SPIO or local contexts.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

fragment

Indicates packet filtering is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.

num can be an integer ranging from 0 to 255.

Important This keyword is not applicable to a SPIO interface. Instead, you must specify the type of protocol packets for which you want to deny/permit processing on a SPIO. For example, **deny icmp**, **deny tcp**, or **deny udp**.

Usage Guidelines

Block IP packets when the source and destination are of interest.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following commands define two rules with the second logging filtered packets:

```
permit ip host 10.2.3.4 any fragment
deny log ip 10.2.3.0 0.0.0.31 host 10.2.4.16
```

The following sets the insertion point before the first rule defined above:

```
before permit ip host 10.2.3.4 any fragment
```

The following command sets the insertion point after the second rule defined above:

```
after deny log ip 10.2.3.0 0.0.0.31 host 10.2.4.16
```

The following deletes the first rule defined above:

```
no permit ip host 10.2.3.4 any fragment
```

deny/permit (by TCP/UDP packets)

Filters subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

{ deny | permit } [log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_port end_port*] }

after { deny | permit } [log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_port end_port*] }

before { deny | permit } [log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_port end_port*] }

no { deny | permit } [log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address*

} [eq *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **| range** *start_port end_port* **] }**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: Packets are not logged.

Indicates all packets which match the filter are to be logged.

Important The logging option is not supported for ACLs applied on SPIO or local contexts.

tcp | udp

Specifies the filter is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Filter applies to TPC packets.

- **udp**: Filter applies to UDP packets.

source_address

The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be an integer from 0 through 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be an integer from 0 through 65535.

range *start_port end_port*

Specifies a range of ports to be matched.

start_port must be an integer from 0 through 65535, and must be less than the *end_port* value.

end_port must be an integer from 0 through 65535, and must be greater than the *start_port* value.

Important This option is supported in PDIF Release 8.3.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following commands define four rules with the second and fourth rules logging filtered packets:

```
permit tcp host 10.2.3.4 any
deny log udp 10.2.3.0 0.0.0.31 host 10.2.4.16
permit tcp host 10.2.3.64 gt 1023 any
deny log udp 10.2.3.0 0.0.0.31 10.2.4.127 0.0.0.127
```

The following sets the insertion point before the first rule defined above:

```
before permit tcp host 10.2.3.4 any
```

The following command sets the insertion point after the second rule defined above:

```
after deny log udp 10.2.3.0 0.0.0.31 host 10.2.4.16
```

The following deletes the third rule defined above:

```
no permit tcp host 10.2.3.64 gt 1023 any
```

description

Allows you to enter descriptive text for this configuration.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
description text
no description
```

no

Clears the description for this configuration.

text

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

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

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

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.

readdress server

Alters the destination address and port number in TCP or UDP packet headers to redirect packets to a different server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

readdress server *redirect_address* **[port** *port_no* **] { tcp | udp } { { ***source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq]** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

after readdress server *redirect_address* **[port** *port_no* **] { tcp | udp } { { ***source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq]** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

before readdress server *redirect_address* **[port** *port_no* **] { tcp | udp } { { ***source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq]** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

no readdress server *redirect_address* **[port** *port_no* **] { tcp | udp } { { ***source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq]** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

redirect_address

The IP address to which the IP packets are redirected. TCP or UDP packet headers are rewritten to contain the new destination address. This must be an IPv4 address specified in dotted-decimal notation.

port *port_no*

The number of the port at the redirect address where the packets are sent. TCP or UDP packet headers are rewritten to contain the new destination port number.

tcp | udp

Specifies the redirect is to be applied to the IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be an integer from 0 through 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be an integer 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be an integer 0 through 65535.

Usage Guidelines

Use this command to define a rule that redirects packets to a different destination address. The TCP and UDP packet headers are modified with the new destination address and destination port.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Prior to Release 8.3, for packets received from the packet data network destined for a subscriber's UE, the system applied logic to reset the source address of a packet to the original destination address of the input packet before applying the outbound access control list (ACL). In Release 8.3 and higher, the system reverses the order and applies the outbound ACL before resetting the source address. This change impacts all current readdress server rules in inbound IPv4 ACLs.

Important After Release 8.3, for every readdress server rule in an inbound IPv4 ACL, you must add a permit rule to an outbound ACL that explicitly permits packets from the readdress rule's redirect address and port number. If the permit rule is omitted, the system will reject all packets destined for the subscriber's UE from the readdress rule's redirect address and port number.

Example

The following command defines a rule that redirects packets to the server at 192.168.10.4, UDP packets coming from any host with a destination of any host are matched:

```
readdress server 192.168.10.4 udp any any
```

The following sets the insertion point before the rule defined above:

```
before readdress server 192.168.10.4 udp any any
```

The following command sets the insertion point after the first rule defined above:

```
after readdress server 192.168.10.4 udp any any
```

The following deletes the rule defined above:

```
no readdress server 192.168.10.4 udp any any
```

redirect context (by IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
redirect context context_id [ log ] source_address source_wildcard
after redirect context context_id [ log ] source_address source_wildcard
before redirect context context_id [ log ] source_address source_wildcard
no redirect context context_id [ log ] source_address source_wildcard
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Usage Guidelines Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of 23 and the source IP and wildcard of 192.168.22.0 and 0.0.0.31:

```
redirect context 23 198.162.22.0 0.0.0.31
```

The following sets the insertion point before the rule defined above:

```
before redirect context 23 198.162.22.0 0.0.0.31
```

The following command sets the insertion point after the first rule defined above:

```
after redirect context 23 198.162.22.0 0.0.0.31
```

The following deletes the first rule defined above:

```
no redirect context 23 198.162.22.0 0.0.0.31
```

redirect context (any)

Redirects subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
redirect context context_id [ log ] any
after redirect context context_id [ log ] any
before redirect context context_id [ log ] any
no redirect context context_id [ log ] any
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage Guidelines

Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important Any rule which is added as a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of 23 and any source IP:

```
redirect context 23 any
```

The following sets the insertion point before the rule defined above:

```
before redirect context 23 any
```

The following command sets the insertion point after the first rule defined above:

```
after redirect context 23 any
```

The following deletes the first rule defined above:

```
no redirect context 23 any
```

redirect context (by host IP address)

Redirects subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect context *context_id* **[log] host** *source_ipv4_address*
after redirect context *context_id* **[log] host** *source_ipv4_address*

before redirect context *context_id* **[log] host** *source_ipv4_address*
no redirect context *context_id* **[log] host** *source_ipv4_address*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_ipv4_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

Usage Guidelines

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of 23 and a host IP address of 192.168.200.11:

```
redirect context 23 host 192.168.200.11
```

The following sets the insertion point before the rule defined above:

```
before redirect context 23 host 192.168.200.11
```

The following command sets the insertion point after first the rule defined above:

```
after redirect context 23 host 192.168.200.11
```

The following deletes the first rule defined above:

```
no redirect context 23 host 192.168.200.11
```

redirect context (by source ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**
after redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**
before redirect context *context_id* **[log] icmp {** *source_address source_wildcard*

```
 | any | host source_host_address } { dest_address dest_wildcard | any | host
dest_host_address } [ icmp_type [ icmp_code ] ]
no redirect context context_id [ log ] icmp { source_address source_wildcard |
any | host source_host_address } { dest_address dest_wildcard | any | host
dest_host_address } [ icmp_type [ icmp_code ] ]
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

Usage Guidelines

Define a rule to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of 23, and ICMP packets coming from the host with the IP address 198.162.100.25:

```
redirect context 23 icmp host 192.168.100.25
```

The following sets the insertion point before the rule defined above:

```
before redirect context 23 icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule defined above:

```
after redirect context 23 icmp host 192.168.100.25
```

The following deletes the first rule defined above:

```
no redirect context 23 icmp host 192.168.100.25
```

redirect context (by IP packets)

Redirects subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect context *context_id* **[log] ip {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**
after redirect context *context_id* **[log] ip {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**
before redirect context *context_id* **[log] ip {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**
no redirect context *context_id* **[log] ip {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.

num can be an integer ranging from 0 to 255.

Usage Guidelines

Block IP packets when the source and destination are of interest.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of 23, and IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched:

```
redirect context 23 ip host 198.162.100.25 any fragment
```

The following sets the insertion point before the rule defined above:

```
before redirect context 23 ip host 198.162.100.25 any fragment
```

The following command sets the insertion point after the first rule defined above:

```
after redirect context 23 ip host 198.162.100.25 any fragment
```

The following deletes the first rule defined above:

```
no redirect context 23 ip host 198.162.100.25 any fragment
```

redirect context (by TCP/UDP packets)

Redirects subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect context *context_id* **[log] { tcp | udp } { { ***source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

after redirect context *context_id* **[log] { tcp | udp } { { ***source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

before redirect context *context_id* **[log] { tcp | udp } { { ***source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **] }**

no redirect context *context_id* **[log] { tcp | udp } { { ***source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port*

| lt *source_port* **| neq** *source_port* **] } { {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **]**
}

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be an integer from 0 through 65535.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of 23, and UDP packets coming from any host are matched:

```
redirect context 23 udp any
```

The following sets the insertion point before the rule defined above:

```
before redirect context 23 udp any
```

The following command sets the insertion point after the first rule defined above:

```
after redirect context 23 udp any
```

The following deletes the rule defined above:

```
no redirect context 23 udp any
```

redirect css delivery-sequence

This is a restricted command. In 9.0 and later releases, this command is obsoleted.

redirect css service (any)

Redirects subscriber sessions based on any packet received (Content Service Steering). This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
redirect css service service_name [ log ] any
after redirect css service service_name [ log ] any
before redirect css service service_name [ log ] any
no redirect css service service_name [ log ] any
```

after

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definitions which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage Guidelines

Define a catch all rule definitions to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important Any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1* and any source IP:

```
redirect css service chgsvc1 any
```

The following sets the insertion point before the rule definition above:

```
before redirect service chgsvc1 any
```

The following command sets the insertion point after the first rule definitions above:

```
after redirect service chgsvc1 any
```

The following deletes the first rule definition above:

```
no redirect service chgsvc1 any
```

redirect css service (by host IP address)

Redirecst subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
redirect css service service_name [ log ] host source_host_address
after redirect css service service_name [ log ] host source_host_address
before redirect css service service_name [ log ] host source_host_address
no redirect css service service_name [ log ] host source_host_address
```

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

Usage Guidelines

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1* and a host IP address of *192.168.200.11*:

```
redirect css service chgsvc1 host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 host 192.168.200.11
```

redirect css service (by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] icmp { any | host** *source_host_address* **| *source_address source_wildcard* } { any | host** *dest_host_address* **| *dest_address dest_wildcard* } [** *icmp_type* **[** *icmp_code* **]**
before redirect css service *service_name* **[log] icmp { any | host**

source_host_address **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**
after redirect css service *service_name* **[log] icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**
no redirect css service *service_name* **[log] icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

Usage Guidelines

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and ICMP packets coming from the host with the IP address *198.162.100.25*:

```
redirect css service chgsvc1 icmp host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 icmp host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 icmp host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 icmp host 192.168.200.11
```

redirect css service (by IP packets)

Redirects subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
after redirect css service *service_name* **[log] ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
before redirect css service *service_name* **[log] ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
no redirect css service *service_name* **[log] ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition that exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage Guidelines

Block IP packets when the source and destination are of interest.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and IP packets coming from the host with the IP address *198.162.100.25*, and fragmented packets for any destination are matched:

redirect css service chgsvc1 ip host 192.168.100.25 any fragment

The following sets the insertion point before the rule definition above:

before redirect css service chgsvc1 ip host 192.168.100.25 any fragment

The following command sets the insertion point after the first rule definition above:

after redirect css service chgsvc1 ip host 192.168.100.25 any fragment

The following deletes the first rule definition above:

no redirect css service chgsvc1 ip host 192.168.100.25 any fragment

redirect css service (by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source to the mobile node or the network (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-acl)#`

Syntax Description

redirect css service *service_name* **[log]** *source_address source_wildcard*
after redirect css service *service_name* **[log]** *source_address source_wildcard*
before redirect css service *service_name* **[log]** *source_address source_wildcard*
no redirect css service *service_name* **[log]** *source_address source_wildcard*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Usage Guidelines

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines a rule definition to redirect packets to a charging service named *chgsvc1*:

```
redirect css service chgsvc1 10.2.3.0 0.0.0.31
```

redirect css service (by TCP/UDP packets)

Redirects subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port* | range *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_dest_port end_dest_port*] }**
after redirect css service *service_name* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port* | range *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_dest_port end_dest_port*] }**
before redirect css service *service_name* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port* | range *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_dest_port end_dest_port*] }**
no redirect css service *service_name* **[log] { tcp | udp } { { *source_address source_wildcard* | any | host *source_host_address* } [eq *source_port* | gt *source_port* | lt *source_port* | neq *source_port* | range *start_source_port end_source_port*] } { { *dest_address dest_wildcard* | any | host *dest_host_address* } [eq *dest_port* | gt *dest_port* | lt *dest_port* | neq *dest_port* | range *start_dest_port end_dest_port*] }**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.

start_source_port is the initial port in the range and *end_source_port* is the final port in the range.

Both *start_source_port* and *end_source_port* can be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.

start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.

Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and UDP packets coming from any host are matched:

```
redirect css service chgsvc1 udp any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 udp any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 udp any
```

The following command deletes the rule definition above:

```
no redirect css service chgsvc1 udp any
```

redirect css service (for downlink, any)

Redirects subscriber sessions based on any packet received in the downlink (from the Mobile Node) direction (Content Service Steering). This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
redirect css service service_name [ log ] downlink any
after redirect css service service_name [ log ] downlink any
before redirect css service service_name [ log ] downlink any
no redirect css service service_name [ log ] downlink any
```

after

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage Guidelines

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important Any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1* and any source IP:

```
redirect css service chgsvc1 downlink any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink any
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 downlink any
```

redirect css service (for downlink, by host IP address)

Redirects subscriber sessions based on the targeted host IP address in the downlink (from the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] downlink host** *source_host_address*
before redirect css service *service_name* **[log] downlink host** *source_host_address*
after redirect css service *service_name* **[log] downlink host** *source_host_address*
no redirect css service *service_name* **[log] downlink host** *source_host_address*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

Usage Guidelines

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1and* a host IP address of *192.168.200.11*:

```
redirect css service chgsvc1 downlink host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 downlink host 192.168.200.11
```

redirect css service (for downlink, by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] downlink icmp { any | host** *source_host_address* **| *source_address source_wildcard* } { any | host** *dest_host_address* **| *dest_address dest_wildcard* } [*icmp_type* [*icmp_code*]**

after redirect css service *service_name* **[log] downlink icmp { any | host** *source_host_address* **| *source_address source_wildcard* } { any | host** *dest_host_address* **| *dest_address dest_wildcard* } [*icmp_type* [*icmp_code*]**

before redirect css service *service_name* **[log] downlink icmp { any | host** *source_host_address* **| *source_address source_wildcard* } { any | host** *dest_host_address* **| *dest_address dest_wildcard* } [*icmp_type* [*icmp_code*]**

no redirect css service *service_name* **[log] downlink icmp { any | host** *source_host_address* **| *source_address source_wildcard* } { any | host** *dest_host_address* **| *dest_address dest_wildcard* } [*icmp_type* [*icmp_code*]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

Usage Guidelines

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and ICMP packets coming in the downlink (from the Mobile Node) direction from the host with the IP address 192.168.100.25:

redirect css service chgsvc1 downlink icmp host 192.168.100.25

The following sets the insertion point before the rule definition above:

before redirect css service chgsvc1 downlink icmp host 192.168.100.25

The following command sets the insertion point after the first rule definition above:

after redirect css service chgsvc1 downlink icmp host 192.168.100.25

The following deletes the first rule definition above:

no redirect css service chgsvc1 downlink icmp host 192.168.100.25

redirect css service (for downlink, by IP packets)

Redirects subscriber sessions based on the internet protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-acl)#`

Syntax Description

redirect css service *service_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
after redirect css service *service_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
before redirect css service *service_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
no redirect css service *service_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage Guidelines

Block IP packets when the source and destination are of interest.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and downlink IP packets coming from the host with the IP address *198.162.100.25*, and fragmented packets for any destination are matched:

```
redirect css service chgsvc1 downlink ip host 198.162.100.25 any fragment
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink ip host 198.162.100.25 any
fragment
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink ip host 198.162.100.25 any
fragment
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 downlink ip host 198.162.100.25 any
fragment
```

redirect css service (for downlink, by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source in the downlink (from the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] downlink** *source_address source_wildcard*
after redirect css service *service_name* **[log] downlink** *source_address source_wildcard*
before redirect css service *service_name* **[log] downlink** *source_address source_wildcard*
no redirect css service *service_name* **[log] downlink** *source_address source_wildcard*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Usage Guidelines Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines a rule definition to redirect packets to a charging service named *chgsvc1*:

```
redirect css service chgsvc1 downlink 10.2.3.0 0.0.0.31
```

redirect css service (for downlink, by TCP/UDP packets)

Redirects subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

Product All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] downlink { tcp | udp } { {** *source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **| range** *start_source_port end_source_port* **] } { {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **| range** *start_dest_port end_dest_port* **] }**

after redirect css service *service_name* **[log] downlink { tcp | udp } { {** *source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **| range** *start_source_port end_source_port* **] } { {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **| range** *start_dest_port end_dest_port* **] }**

before redirect css service *service_name* **[log] downlink { tcp | udp } { {** *source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **| range** *start_source_port end_source_port* **] } { {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **| range** *start_dest_port end_dest_port* **] }**

no redirect css service *service_name* **[log] downlink { tcp | udp } { {** *source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **| range** *start_source_port end_source_port* **] } { {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **| range** *start_dest_port end_dest_port* **] }**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.

start_source_port is the initial port in the range and *end_source_port* is the final port in the range.

Both *start_source_port* and *end_source_port* can be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.

start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.

Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and UDP packets coming from any host are matched:

```
redirect css service chgsvc1 downlink udp any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink udp any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink udp any
```

The following deletes the rule definition above:

```
no redirect css service chgsvc1 downlink udp any
```

redirect css service (for uplink, any)

Redirects subscriber sessions based on any packet received in the uplink (to the Mobile Node) direction (Content Service Steering). This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
redirect css service service_name [ log ] uplink any
after redirect css service service_name [ log ] uplink any
before redirect css service service_name [ log ] uplink any
no redirect css service service_name [ log ] uplink any
```

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage Guidelines

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important It is suggested that any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1* and any source IP:

```
redirect css service chgsvc1 uplink any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink any
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink any
```

redirect css service (for uplink, by host IP address)

Redirects subscriber sessions based on the targeted host IP address in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] uplink host** *source_host_address*
after redirect css service *service_name* **[log] uplink host** *source_host_address*
before redirect css service *service_name* **[log] uplink host** *source_host_address*
no redirect css service *service_name* **[log] uplink host** *source_host_address*

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

after

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

Usage Guidelines

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *chgsvc1* and a host IP address of *192.168.200.11*:

```
redirect css service chgsvc1 uplink host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink host 192.168.200.11
```

redirect css service (for uplink, by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] uplink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**
after redirect css service *service_name* **[log] uplink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**
before redirect css service *service_name* **[log] uplink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**
no redirect css service *service_name* **[log] uplink icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

Usage Guidelines

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and ICMP packets in the uplink (to the Mobile Node) direction from the host with the IP address *198.162.100.25*:

```
redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink icmp host 192.168.100.25
```

redirect css service (for uplink, by IP packets)

Redirects subscriber sessions based on the internet protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] uplink ip { any | host** *source_host_address* **| *source_address source_wildcard* } { any | host** *dest_host_address* **| *dest_address dest_wildcard* } [fragment]**
after redirect css service *service_name* **[log] uplink ip { any | host** *source_host_address* **| *source_address source_wildcard* } { any | host** *dest_host_address* **| *dest_address dest_wildcard* } [fragment]**
before redirect css service *service_name* **[log] uplink ip { any | host** *source_host_address* **| *source_address source_wildcard* } { any | host** *dest_host_address* **| *dest_address dest_wildcard* } [fragment]**
no redirect css service *service_name* **[log] uplink ip { any | host** *source_host_address* **| *source_address source_wildcard* } { any | host** *dest_host_address* **| *dest_address dest_wildcard* } [fragment]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage Guidelines

Block IP packets when the source and destination are of interest.

Important

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and uplink IP packets going to the host with the IP address *198.162.100.25*, and fragmented packets for any destination are matched:

```
redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink ip host 198.162.100.25 any
fragment
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink ip host 198.162.100.25 any
fragment
```

The following command deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

redirect css service (for uplink, by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect css service *service_name* **[log] uplink** *source_address source_wildcard*
after redirect css service *service_name* **[log] uplink** *source_address source_wildcard*
before redirect css service *service_name* **[log] uplink** *source_address source_wildcard*
no redirect css service *service_name* **[log] uplink** *source_address source_wildcard*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Usage Guidelines

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Important

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines a rule definition to redirect packets to a charging service named *chgsvc1*:

```
redirect css service chgsvc1 uplink 10.2.3.0 0.0.0.31
```

redirect css service (for uplink, by TCP/UDP packets)

Redirects subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
redirect css service service_name [ log ] uplink { tcp | udp } { {
source_address source_wildcard | any | source_host_address } [ eq source_port | gt
source_port | lt source_port | neq source_port | range start_source_port end_source_port
 ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port
 | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port
 ] }
after redirect css service service_name [ log ] uplink { tcp | udp } { {
source_address source_wildcard | any | source_host_address } [ eq source_port | gt
source_port | lt source_port | neq source_port | range start_source_port end_source_port
 ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port
 | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port
 ] }
before redirect css service service_name [ log ] uplink { tcp | udp } { {
source_address source_wildcard | any | source_host_address } [ eq source_port | gt
source_port | lt source_port | neq source_port | range start_source_port end_source_port
 ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port
 | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port
 ] }
```

no redirect css service *service_name* **[log] uplink { tcp | udp } { {** *source_address source_wildcard* **| any |** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **| range** *start_source_port end_source_port* **] } { {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **| range** *start_dest_port end_dest_port* **] }**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

no

Removes the rule definition which exactly matches the options specified.

css service *service_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

service_name must be an alphanumeric string from 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.

start_source_port is the initial port in the range and *end_source_port* is the final port in the range.

Both *start_source_port* and *end_source_port* can be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.

start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.

Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and UDP packets coming from any host are matched:

```
redirect css service chgsvc1 uplink udp any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink udp any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink udp any
```

The following deletes the rule definition above:

```
no redirect css service chgsvc1 uplink udp any
```

redirect nexthop (by IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

```
redirect nexthop nexthop_addr { context context_id | interface interface_name }
[ log ] source_address source_wildcard
after redirect nexthop nexthop_addr { context context_id | interface interface_name
 } [ log ] source_address source_wildcard
before redirect nexthop nexthop_addr { context context_id | interface
interface_name } [ log ] source_address source_wildcard
no redirect nexthop nexthop_addr { context context_id | interface interface_name
 } [ log ] source_address source_wildcard
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 to 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Usage Guidelines

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and the source IP and wildcard of 192.168.22.0 and 0.0.0.31:

```
redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

redirect nexthop (any)

Redirects subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**
after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**
before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**
no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 to 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage Guidelines

Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important Any rule which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and any source IP:

```
redirect nexthop 192.168.10.4 context 23 any
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 any
```

The following command sets the insertion point after the first rule defined above:

after redirect nexthop 192.168.10.4 context 23 any

The following deletes the first rule defined above:

no redirect nexthop 192.168.10.4 context 23 any

redirect nexthop (by host IP address)

Redirects subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax Description

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] host** *source_ipv4_address*
after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] host** *source_ipv4_address*
before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] host** *source_ipv4_address*
no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] host** *source_ipv4_address*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 to 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_ipv4_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

Usage Guidelines

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and a host IP address of 192.168.200.11:

```
redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

redirect nexthop (by source ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 through 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

Usage Guidelines

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and ICMP packets coming from the host with the IP address 198.162.100.25:

```
redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

redirect nexthop (by IP packets)

Redirects subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] ip { source_address source_wildcard | any | host** *source_host_address* **} { dest_address dest_wildcard | any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**
after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] ip { source_address source_wildcard | any | host** *source_host_address* **} { dest_address dest_wildcard | any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**
before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] ip { source_address source_wildcard | any | host** *source_host_address* **} { dest_address dest_wildcard | any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**
no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] ip { source_address source_wildcard | any | host** *source_host_address* **} { dest_address dest_wildcard | any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 through 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.

num can be an integer ranging from 0 to 255.

Usage Guidelines

Block IP packets when the source and destination are of interest.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched:

```
redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any
fragment
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25
any fragment
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any
 fragment
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any
fragment
```

redirect nexthop (by TCP/UDP packets)

Redirects subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context *context_name* **> ip access-list** *acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

Syntax Description

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] { tcp | udp } { {** *source_address source_wildcard* **| any | host**

source_host_address } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port*] }
after redirect nexthop *nexthop_addr* { **context** *context_id* | **interface** *interface_name* } [**log**] { **tcp** | **udp** } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port*] }
before redirect nexthop *nexthop_addr* { **context** *context_id* | **interface** *interface_name* } [**log**] { **tcp** | **udp** } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port*] }
no redirect nexthop *nexthop_addr* { **context** *context_id* | **interface** *interface_name* } [**log**] { **tcp** | **udp** } { { *source_address source_wildcard* | **any** | **host** *source_host_address* } [**eq** *source_port* | **gt** *source_port* | **lt** *source_port* | **neq** *source_port*] } { { *dest_address dest_wildcard* | **any** | **host** *dest_host_address* } [**eq** *dest_port* | **gt** *dest_port* | **lt** *dest_port* | **neq** *dest_port*] }

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 through 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) from which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be an integer from 0 through 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be an integer from 0 through 65535.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Important Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and UDP packets coming from any host are matched:

```
redirect nexthop 192.168.10.4 context 23 udp any
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 udp any
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 udp any
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 udp any
```