

Creating Firewall Exceptions for Stateless Firewalls

To create a firewall exception for a subscriber:

1. Access the subscriber's Firewall page.
2. In the Firewall page, click **Create Firewall Exception**.

The Create Exception dialog box appears. Figure 1 on page 2 shows the appearance of the dialog box when Enterprise Manager Portal is set to Advanced mode.

Figure 1: Create Exception Dialog Box for Stateless Firewalls

The screenshot shows a web browser window titled "Create Exception - Microsoft Internet Explorer". Inside the browser is a form titled "Create Exception". The form has the following fields and controls:

- Rule Name:** A text input field.
- IP Protocols:** A text input field.
- ToS Byte:** Three radio buttons: "DiffServ" (selected), "Precedence", and "Free Format (e.g. 110101xx)". There is a dropdown menu next to "DiffServ" and a text input field next to "Precedence".
- Source IP Addresses:** A list box with up/down arrows and a search button.
- Source Ports:** A text input field.
- Destination IP Addresses:** A list box with up/down arrows and a search button.
- Destination Ports:** A text input field.
- TCP Flags:** A text input field.
- Fragmentation Flags:** A text input field.
- Fragment Offset:** A text input field.
- Packet Length:** A text input field.
- ICMP Type:** A text input field.
- ICMP Code:** A text input field.
- Priority:** A text input field with the value "0".
- Direction:** A dropdown menu with "Incoming" selected.
- Action:** A dropdown menu with "Allow" selected.
- Enabled:** A checkbox that is currently unchecked.
- Buttons:** "Create", "Cancel", and "Reset" buttons at the bottom.

3. Enter field values to configure the values for the firewall exception.

See Fields for Exceptions to Stateless Firewalls in Enterprise Manager Portal.

Which protocols you select determines which associated protocol fields are available for editing.



NOTE: If a user changes the value for a protocol when the configuration level for the portal is set to Normal mode, values for the following fields may be deleted: TCP Flags, Fragmentation Flags, Fragmentation Offset, Packet Length, ICMP Type, and ICMP Code.

If the value of a protocol is changed to the original setting, the portal restores the associated field values that were previously removed.

4. Click **Create**.

The Firewall page shows the exception configured. Figure 2 on page 3 shows three exceptions configured for a brickwall firewall service. The exceptions appear in priority order.

Figure 2: Firewall Page with Firewall Service Applied and Exceptions Configured

The screenshot shows the 'Firewall Service' configuration page. At the top, there are tabs for 'Bandwidth & VPNs', 'Firewall', 'Addresses', 'NAT', 'Schedules', and 'Managers'. The 'Firewall' tab is selected. Below the tabs, there is a 'Firewall Service' section with a dropdown menu set to 'BrickWall' and an 'Apply' button. Below this, there is a table titled 'Exceptions to Firewall Service'. The table has columns: Name, Affected Traffic, Priority, Direction, Firewall Action, Schedule, Enabled, and a 'Delete' button. There are four exceptions listed: 'tcpProto1', 'tcpRule2', 'icmpRule', and 'tcpProtocol'. Each exception has a detailed view of its configuration, including IP Protocol, ToS Byte, Source Address, Destination Address, Destination Port, TCP Flags, Fragmentation Flags, Fragment Offset, and Packet Length. The 'tcpProto1' exception is enabled, while the others are not. At the bottom of the table, there is a 'Create Firewall Exception' button.

Name	Affected Traffic	Priority	Direction	Firewall Action	Schedule	Enabled	Delete
tcpProto1	IP Protocol: tcp ToS Byte: precedence: internet_control Source Address: 10.10.10.0/24 Destination Address: 10.11.12.0/24 Destination Port: 6789 TCP Flags: tcp-initial Fragmentation Flags: dont-fragment Fragment Offset: 100..170 Packet Length: 60..70	4	Incoming	Allow	No schedule	<input checked="" type="checkbox"/>	Delete
tcpRule2	All Traffic	7	Incoming	Allow	No schedule	<input type="checkbox"/>	Delete
icmpRule	IP Protocol: icmp Source Address: 1.1.1.0/24 Destination Address: 2.2.2.0/24 Fragmentation Flags: reserved Fragment Offset: 5000 Packet Length: 65535 ICMP Type: info-reply ICMP Code: 50..100	10	Outgoing	Discard	No schedule	<input type="checkbox"/>	Delete
tcpProtocol	IP Protocol: tcp ToS Byte: precedence: immediate Source Address: 10.10.10.0/24 Source Port: 23456 Destination Address: 10.11.12.0/24 Destination Port: 6789 TCP Flags: fin & lsyn & rst & lpush & ack & urgent Fragmentation Flags: dont-fragment Fragment Offset: 100..170 Packet Length: 60..70	45	Incoming	Allow	No schedule	<input checked="" type="checkbox"/>	Delete

Fields for Exceptions to Stateless Firewalls in Enterprise Manager Portal

Use the fields in this topic to configure rules for exceptions to stateless firewalls.

Rule Name

- Name of the subscription to the firewall service.
- Value—Alphanumeric string
- Guidelines—You must specify a name for the rule. Do not use spaces, dots, or punctuation characters in the name.
- Default—No value
- Example—WebAccess

IP Protocols

- IP protocol associated with this rule.
- Value—Type of IP protocols separated by commas, with the protocol specified by:
 - Number of IP protocol in the range 0–255
 - The following abbreviations:
 - ah—authentication header
 - egp—exterior gateway protocol
 - esp—Encapsulating Security Payload
 - gre—generic routing encapsulation
 - icmp—Internet Control Message Protocol
 - igmp—Internet Group Management Protocol
 - ipip—IP over IP
 - ospf—Open Shortest Path First
 - pim—Protocol Independent Multicast
 - rsvp—Resource Reservation Protocol
 - sctp—Stream Control Transmission Protocol
 - tcp—Transmission Control Protocol
 - udp—User Datagram Protocol
 - Blank—Any IP protocol
- Default—No value
- Example—tcp

ToS Byte

- ToS byte in the header of the IP datagram associated with traffic affected by this rule.
- Value
 - DiffServ—DiffServ is used to classify packets by the selected value.
 - Precedence—Value for the drop precedence.
 - Free Format—ToS byte in binary format.

Use an x to indicate a bit to be ignored.

- Guidelines—You can configure the ToS byte only if the configuration level is set to Advanced.

Specify the ToS byte in this field if you want to specify a specific type of service. If you want to specify all types of service, leave this field empty.

- Default—No value
- Example—Free Format 000010xx

Source IP Addresses

- IP addresses (as contained in the IP packets) of traffic to which the rule applies.
- Value—[not] <networkAddress> / <networkMask>
 - not—All addresses except the listed addresses
 - <networkAddress> —IP address of the network
 - <networkMask> —Subnet mask
- Guidelines—To specify traffic with a particular source IP address, enter an IP address. To specify all traffic except that with a particular source IP address, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty. To specify multiple source IP addresses, enter multiple addresses on different lines. You can specify multiple source IP addresses only if the configuration level is set to Advanced.
- Default—No value
- Example—192.0.2.0/24

Source Ports

- Source TCP/UDP port(s) (contained in the IP packets) of traffic affected by this rule.
- Values
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)

- Ranges of port numbers separated by two dots (..)
- Guidelines— To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

Destination IP Addresses

- Destination IP addresse(s) (contained in the IP packets) of traffic affected by this rule.
- Value—[not] < networkAddress > / < networkMask >
 - not—Address, or set of IP addresses as expressed by the netmask, for which the firewall service is not available
 - < networkAddress > —IP address of the network
 - < networkMask > —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify a netmask for a destination IP address or a set of IP addresses that should not be included, precede the IP address with the keyword **not**. The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—192.0.2.0/24

Destination Ports

- Destination TCP/UDP port(s) (contained in the IP packets) of traffic affected by this rule.
- Value
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)

- Ranges of port numbers separated by two dots (..)
- Guidelines—To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

TCP Flags

- Conditions in the TCP flags in the TCP message header. This field is enabled when the TCP protocol is selected.
- Value—Expression or text synonym that identifies the TCP flags
- Guidelines—You can enter a value for TCP flags only if you select TCP as the IP protocol.

You can enter a logical expression that contains the symbols for the six TCP flags: urgent, ack, push, rst, syn, and fin. You can use the following logical operators in the list of flags:

- &—And. Separates flag settings in the list.
- !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.

You can use the following expression instead of the entire expression:

- tcp-initial—syn & !ack

The interface displays text synonyms for expressions if stored data matches the expression.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—No value
- Example
 - syn
 - tcp-initial

Fragmentation Flags

- Logical expression using the dont-fragment, more-fragments, and reserved IP fragmentation flags.
- Value—Flags expression
- Guidelines—The expression can also contain the following logical operators:
 - &—And. Separates flag settings in the list.
 - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.
- Default—No value
- Example
 - more-fragments
 - ! dont-fragment

Fragment Offset

- IP fragment offset—a value that defines the order in which to assemble fragments for an IP datagram.
- Value—One of the following:
 - Number in the range 0–8191
 - Range of numbers separated by two dots (..) within the range 0–8191
- Default—No value
- Example
 - 50
 - 50 .. 76

Packet Length

- Length of packets.
- Value—One of the following:
 - Number in the range 0–65536
 - Range of numbers separated by two dots (..) within the range 0–65536
- Default—No value
- Example
 - 15000
 - 15000 .. 30000

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message in the following formats:
 - Number of the ICMP message type in the range 0–255
 - Symbolic name for an ICMP message type
 - Comma-separated list of ICMP types and ranges of ICMP types
 - Ranges of ICMP types separated by two dots (..) within the range 0–255
 - Blank—Any ICMP type
- Guidelines—You can enter a value for this field only if you select the icmp protocol (protocol number 1).

The following list shows the symbolic name and associated numbers for ICMP types. The ICMP types are the same as those on JUNOS routing platforms with the addition of traceroute.

- 0—echo-reply
- 8—echo-request
- 16—info-reply
- 15—info-request
- 18—mask-reply
- 17—mask-request
- 12—parameter-problem
- 5—redirect
- 9—router-advertisement
- 10—router-solicit
- 4—source-quench
- 11—time-exceeded
- 13—timestamp
- 14—timestamp-reply
- 30—traceroute
- 3—unreachable

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—10 .. 25, 27

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code in the following formats:
 - Number of ICMP code in the range 0–255
 - Comma-separated list of code numbers and ranges of code numbers
 - Ranges of code numbers separated by two dots (..) within the range 0–255
 - Blank—Any ICMP code
- Guidelines—You can enter a value for this field only if you select particular protocols.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—75

Priority

- Numeric value that indicates which firewall exception takes precedence if a subscriber has multiple exceptions for a firewall service.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the firewall exception. A lower number indicates a higher priority. Use a unique priority for each firewall exception that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Direction

- Direction, with respect to the enterprise, of the traffic.
- Value
 - Incoming—Applies to traffic that starts outside the enterprise
 - Outgoing—Applies to traffic that starts inside the enterprise

- Both—Applies to traffic flows that start inside or outside the enterprise
- Guidelines—If you select a custom firewall rule, you cannot specify a direction. Custom firewall rules should have names that reflect what the rule does.
- Default—Incoming
- Example—Both

Action

- Way in which the firewall should handle the incoming or outgoing traffic.
- Value
 - Allow—Let the traffic through the firewall.
 - Reject—Send an ICMP reply that explains why the firewall blocked the traffic.
 - Discard—Drop the traffic without sending any reply.
 - A custom value configured by the service provider.
- Guidelines—Other actions may be available—one for each custom firewall rule.
- Default—Allow
- Example—Discard

Enabled

- Status of the rule.
- Value
 - Gray box—Rule is inherited from a parent subscriber or the rule is scheduled
 - White box—Rule is configured for this subscriber
 - Box with check mark—Rule is enabled
 - Empty box—Rule is disabled
- Guidelines—Click box to enable or disable a rule.
- Default—Rule is disabled

