Firewall Filter Match Conditions and Actions for EX-series Switches

Each term in a firewall filter consists of *match conditions* and an *action*. Match conditions are the values or fields that a packet must contain. You can define multiple, single, or no match conditions. If no match conditions are specified for the term, the packet is accepted by default. The action is the action that the switch takes if a packet matches the match conditions for the specific term. Allowed actions are accept a packet or discard a packet. In addition, you can specify action modifiers to count, mirror, rate limit, and classify packets.

For each firewall filter, you define the terms that specify the filtering criteria (match conditions) to apply to packets and the action for the switch to take if a match occurs.

Table 1 describes the match conditions you can specify when configuring a firewall filter. The string that defines a match condition is called a *match statement*. All match conditions are applicable to IPv4 traffic.

Table 1: Supported Match Conditions for Firewall Filters on EX-series Switches

Match Condition	Description	Direction/Interface
destination-address *ip-address*	IP destination address field, which is the address of the final destination node.	Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces.
destination-mac-address *mac-address*	Destination media access control (MAC) address of the packet.	Ingress ports, VLANs, and router interfaces. Egress VLANs. **NOTE:** Ingress and egress router interfaces are not supported on EX 8200 series.

Table 1: Supported Match Conditions for Firewall Filters on EX-series Switches *(continued)*

Match Condition	Description	Direction/Interface
destination-port *number*	TCP or User Datagram Protocol (UDP) destination port field. Typically, you specify this match in conjunction with the protocol match statement to determine which protocol is used on the port. In place of the numeric value, you can specify one of the following text synonyms (the port numbers are also listed): afs (1483), bgp (179), biff (512), bootpc (68), bootps (67), cmd (514), cvspserver (2401), dhcp (67), domain (53), eklogin (2105), ekshell (2106), exec (512), finger (79), ftp (21), ftp-data (20),	Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces.

Table 1: Supported Match Conditions for Firewall Filters on EX-series Switches *(continued)*

Match Condition	Description	Direction/Interface
	http (80), https (443), ident (113), imap (143), kerberos-sec (88), klogin (543), kpasswd (761), krb-prop (754), krbupdate (760), kshell (544), ldap (389), login (513), mobileip-agent (434), mobilip-mn (435), msdp (639), netbios-dgm (138), netbios-ns (137), netbios-ssn (139), nfsd (2049), nntp (119), ntalk (518), ntp (123), pop3 (110), pptp (1723), printer (515), radacct (1813),radius (1812), rip (520), rkinit (2108), smtp (25), snmp (161), snmptrap (162), snpp (444), socks (1080), ssh (22), sunrpc (111), syslog (514), tacacs-ds (65), talk (517), telnet (23), tftp (69), timed (525), who (513), xdmcp (177), zephyr-clt (2103), zephyr-hm (2104)	
destination-prefix-list *prefix-list*	IP destination prefix list field. You can define a list of IP address prefixes under a prefix-list alias for frequent use. You make this definition at the [edit policy-options] hierarchy level. **NOTE:** destination-prefix-list is not supported on EX 8200 series switches.	Ingress ports, VLANs, and router interfaces. Egress ports, VLANs and router interfaces.
dot1q-tag *number*	The tag field in the ethernet header. The tag values can be 1–4095.	Ingress ports and VLANs. Egress VLANs. **NOTE:** Egress VLANs are not supported on EX 8200 series.

Table 1: Supported Match Conditions for Firewall Filters on EX-series Switches *(continued)*

Match Condition	Description	Direction/Interface
dot1q-user-priority *number*	User-priority field of the tagged Ethernet packet. User-priority values can be 0–7. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): ■ background (1)—Background ■ best-effort (0)—Best effort ■ controlled-load (4)—Controlled load ■ excellent-load (3)—Excellent load ■ network-control (7)—Network control reserved traffic ■ standard (2)—Standard or Spare ■ video (5)—Video ■ voice (6)—Voice	Ingress ports and VLANs. Egress VLANs.
dscp *number*	Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant six bits of this byte form the DSCP. You can specify DSCP in hexadecimal, binary, or decimal form. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): ■ ef (46)—as defined in RFC 2598, *An Expedited Forwarding PHB*. ■ af11 (10), af12 (12), af13 (14); af21 (18), af22 (20), af23 (22); af31 (26), af32 (28), af33 (30); af41 (34), af42 (36), af43 (38) These four classes, with three drop precedences in each class, for a total of 12 code points, are defined in RFC 2597, *Assured Forwarding PHB*.	Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces.

Table 1: Supported Match Conditions for Firewall Filters on EX-series Switches *(continued)*

Match Condition	Description	Direction/Interface
ether-type [ipv4 | arp | mpls | dot1q | *value*]	Ethernet type field of a packet. The *EtherType value* specifies what protocol is being transported in the Ethernet frame. In place of the numeric value, you can specify one of the following text synonyms: ■ aarp—EtherType value AARP (0x80F3) ■ appletalk—EtherType value AppleTalk (0x809B) ■ arp—EtherType value ARP (0x0806) ■ ipv4—EtherType value IPv4 (0x0800) ■ mpls multicast—EtherType value MPLS multicast (0x8848) ■ mpls unicast—EtherType value MPLS unicast (0x8847) ■ oam—EtherType value OAM (0x88A8) ■ ppp—EtherType value PPP ■ pppoe-discovery—EtherType value PPPoE Discovery Stage (0x8863) ■ pppoe-session—EtherType value PPPoE Session Stage (0x8864) ■ sna—EtherType value SNA (0x80D5)	Ingress ports and VLANs. Egress VLANs. **NOTE:** Egress ports, VLANs, and router interfaces are not supported on EX 8200 series.
fragment-flags [is-fragment | more-fragment | dont-fragment]	IP fragmentation flags.	fragment-flags [is-fragment] supported for: Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces. fragment-flags [more-fragment | dont-fragment] supported for: Ingress ports, VLANs, and router interfaces.

Table 1: Supported Match Conditions for Firewall Filters on EX-series Switches *(continued)*

Match Condition	Description	Direction/Interface
icmp-code *number*	ICMP code field. This value or keyword provides more specific information than icmp-type. Because the value's meaning depends upon the associated icmp-type, you must specify icmp-type along with icmp-code. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed). The keywords are grouped by the ICMP type with which they are associated: ■ parameter-problem—ip-header-bad (0), required-option-missing (1) ■ redirect—redirect-for-host (1), redirect-for-network (0), redirect-for-tos-and-host (3), redirect-for-tos-and-net (2) ■ time-exceeded—ttl-eq-zero-during-reassembly (1), ttl-eq-zero-during-transit (0) ■ unreachable—communication-prohibited-by-filtering (13), destination-host-prohibited (10), destination-host-unknown (7), destination-network-prohibited (9), destination-network-unknown (6), fragmentation-needed (4), host-precedence-violation (14), host-unreachable (1), host-unreachable-for-TOS (12), network-unreachable (0), network-unreachable-for-TOS (11), port-unreachable (3), precedence-cutoff-in-effect (15), protocol-unreachable (2), source-host-isolated (8), source-route-failed (5)	Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces.

Table 1: Supported Match Conditions for Firewall Filters on EX-series Switches *(continued)*

Match Condition	Description	Direction/Interface
icmp-type *number*	ICMP packet type field. Typically, you specify this match in conjunction with the protocol match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): echo-reply (0), echo-request (8), info-reply (16), info-request (15), mask-request (17), mask-reply (18), parameter-problem (12), redirect (5), router-advertisement (9), router-solicit (10), source-quench (4), time-exceeded (11), timestamp (13), timestamp-reply (14), unreachable (3)	Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces.
interface *interface-name*	Interface on which the packet is received. You can specify the wildcard character (*) as part of an interface name. **NOTE:** An interface from which a packet is sent cannot be used as a match condition.	Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces.
ip-options	Presence of the options field in the IP header. **NOTE:** ip-options is not supported on EX 8200 series switches.	Ingress ports, VLANs, and router interfaces.
precedence *precedence*	IP precedence. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): ■ critical-ecp (5) ■ flash (3) ■ flash-override (4) ■ immediate (2) ■ internet-control (6) ■ net-control (7) ■ priority (1) ■ routine (0)	Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces.

Table 1: Supported Match Conditions for Firewall Filters on EX-series Switches *(continued)*

Match Condition	Description	Direction/Interface
protocol *list of protocols*	IPv4 protocol value. In place of the numeric value, you can specify one of the following text synonyms: egp (8), esp (50), gre (47), icmp (1), igmp (2), ipip (4), ospf (89), pim (103), rsvp (46), tcp (6), udp (17)	Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces.
source-address *ip-address*	IP source address field, which is the address of the source node sending the packet.	Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces.
source-mac-address *mac-address*	Source MAC address.	Ingress ports and VLANs. Egress VLANs.
source-port *number*	TCP or UDP source-port field. Typically, you specify this match in conjunction with the protocol match statement to determine which protocol is being used on the port. In place of the numeric field, you can specify one of the text synonyms listed under destination-port.	Ingress ports, VLANs, and router interfaces. Egress VLANs and router interfaces.
source-prefix-list *prefix-list*	IP source prefix list field. You can define a list of IP address prefixes under a prefix-list alias for frequent use. You make this definition at the [edit policy-options] hierarchy level. **NOTE:** source-prefix-list is not supported on EX 8200 series switches	Ingress ports, VLANs, and router interfaces. Egress ports, VLANs and router interfaces.
tcp-established	TCP packets of an established TCP connection. This condition matches packets other than the first packet of a connection. tcp-established is a synonym for the bit names ""(ack | rst)". tcp-established does not implicitly check that the protocol is TCP. To do so, specify the protocol tcp match condition. **NOTE:** tcp-established is not supported on EX 8200 series switches.	Ingress ports, VLANs, and router interfaces.

Table 1: Supported Match Conditions for Firewall Filters on EX-series Switches *(continued)*

Match Condition	Description	Direction/Interface
tcp-flags [*flags* tcp-initial]	One or more TCP flags: ■ bit-name—fin, syn, rst, push, ack, urgent ■ logical operators—& (logical AND), ! (negation) ■ numerical value— 0x01 through 0x20 ■ text synonym—tcp-initial To specify multiple flags, use logical operators. **NOTE:** tcp-flags is not supported on egress firewall filters.	Ingress ports, VLANs, and router interfaces.
tcp-initial	Matches the first TCP packet of a connection. tcp-initial is a synonym for the bit names ""(syn & !ack)". tcp-initial does not implicitly check that the protocol is TCP. To do so, specify the protocol tcp match condition.	Ingress ports, VLANs, and router interfaces.
ttl *value*	TTL type to match. The value range is 1 through 255.	Ingress router interfaces.
vlan [*vlan-name* | *vlan-id*]	The VLAN that is associated with the packet.	Ingress ports and VLANs. Egress VLANs.

Some of the numeric range and bit-field match conditions allow you to specify a text synonym. For a list of all the synonyms for a match condition, do any of the following:

- If you are using the J-Web Configuration page, select the synonym from the appropriate list.
- If you are using the CLI, type a question mark (?) after the from statement.

To specify the bit-field value to match, you must enclose the values in quotation marks (" "). For example, a match occurs if the RST bit in the TCP flags field is set:

```
tcp-flags "rst";
```

For information about logical operators and how to use bit-field logical operations to create expressions that are evaluated for matches, see Understanding Firewall Filter Match Conditions.

When you define one or more terms that specify the filtering criteria, you also define the action to take if the packet matches all criteria. Table 2 shows the actions that you can specify in a term.

Table 2: Actions for Firewall Filters

Action	Description
accept	Accept a packet.
discard	Discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.
reject *message-type*	Discard a packet, and send an ICMPv4 message (type 3) "destination unreachable". You can log the rejected packets if you configure the syslog action modifier. You can specify one of the following message codes: administratively-prohibited (default), bad-host-tos, bad-network-tos, host-prohibited, host-unknown, host-unreachable, network-prohibited, network-unknown, network-unreachable, port-unreachable, precedence-cutoff, precedence-violation, protocol-unreachable, source-host-isolated, source-route-failed, or tcp-reset. If you specify tcp-reset, a TCP reset is returned if the packet is a TCP packet. Otherwise nothing is returned. If you do not specify a message-type, the ICMP notification "destination unreachable" is sent with the default message "communication administratively filtered". **NOTE:** reject is supported on ingress interface only. **NOTE:** reject is not supported on EX 8200 series switches.
routing-instance	Forwards matched packets to a virtual routing instance. **NOTE:** routing-instance is not supported on EX 8200 series switches.

In addition to the actions, you can specify action modifiers. Table 3 shows the action modifers that you can specify in a term.

Table 3: Action Modifiers for Firewall Filters

Action Modifier	Description
analyzer *analyzer-name*	Mirror port traffic to a specified destination port or VLAN that is connected to a protocol analyzer application. Mirroring copies all packets seen on one switch port to a network monitoring connection on another switch port. The analyzer name must be configured under [edit ethernet-switching-options analyzer]. You can specify mirroring for ingress port, VLAN and router firewall filters only.
count *counter-name*	Count the number of packets that pass this filter, term, or policer. **NOTE:** count is not supported on EX 8200 series switches.

Table 3: Action Modifiers for Firewall Filters *(continued)*

Action Modifier	Description
forwarding-class *class*	Classify the packet in one of the following forwarding classes: ■ assured-forwarding ■ best-effort ■ expedited-forwarding ■ network-control
log	Log the packet's header information in the Routing Engine. To view this information, issue the show firewall log command in the CLI. **NOTE:** log is supported on ingress interface only. **NOTE:** log is not supported on EX 8200 series switches.
loss-priority [*low* | *high*]	Set the Packet Loss Priority (PLP).
policer *policer-name*	Apply rate limits to the traffic. You can specify a policer for ingress port, VLAN, and router firewall filters only.
syslog	Log an alert for this packet. You can specify that the log be sent to a server for storage and analysis. **NOTE:** syslog is supported on ingress interface only. **NOTE:** syslog is not supported on EX 8200 series switches.

Related Topics

- Firewall Filter Configuration Statements Supported by JUNOS Software for EX-series Switches
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX-series Switches
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX-series Switches
- Understanding Firewall Filter Match Conditions
- Understanding How Firewall Filters Are Evaluated
- Understanding How Firewall Filters Test a Packet's Protocol
- Understanding the Use of Policers in Firewall Filters
- Understanding Filter-Based Forwarding for EX-series Switches