

VSA Match Conditions and Actions for EX Series Switches

EX Series switches support the configuration of RADIUS server attributes specific to Juniper Networks. These attributes are known as vendor-specific attributes (VSAs). They are configured on RADIUS servers and work in combination with 802.1X authentication. Using VSAs, you can apply port firewall filter attributes as a subset of match conditions and actions sent from the RADIUS server to the switch as a result of 802.1X authentication success.

Each term in a VSA configured through the RADIUS server consists of *match conditions* and an *action*. Match conditions are the values or fields that the packet must contain. You can define single, multiple, 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.

The following guidelines apply when you specify match conditions and actions for VSAs:

- Both **match** and **action** statements are mandatory.
- Any or all options (separated by commas) may be included in each **match** and **action** statement.
- Fields separated by commas will be ANDed if they are of a different type. The same types cannot be repeated.
- For OR cases (for example, match 10.1.1.0/24 OR 11.1.1.0/24), apply multiple VSAs to the 802.1X supplicant.
- In order for the **forwarding-class** option to be applied, the forwarding class must be configured on the switch. If it is not configured on the switch, this option is ignored.

Table 1 describes the match conditions you can specify when configuring a VSA using the **match** command on the RADIUS server. The string that defines a match condition is called a *match statement*.

Table 1: Match Conditions

Option	Description
destination-mac <i>mac-address</i>	Destination media access control (MAC) address of the packet.
source-vlan <i>source-vlan</i>	Name of the source VLAN.
source-dot1q-tag <i>tag</i>	Tag value in the dot1q header, in the range 0 through 4095.
destination-ip <i>ip-address</i>	Address of the final destination node.

Table 1: Match Conditions *(continued)*

Option	Description
<code>ip-protocol protocol-id</code>	<p>IPv4 protocol value. In place of the numeric value, you can specify one of the following text synonyms:</p> <p>ah, egp (8), esp (50), gre (47), icmp (1), igmp (2), ipip (4), ipv6 (41), ospf (89), pim (103), rsvp (46), tcp (6), or udp (17)</p>
<code>source-port port</code>	<p>TCP or User Datagram Protocol (UDP) source port field. Normally, you specify this match statement in conjunction with the ip-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 options listed under destination-port.</p>
<code>destination-port port</code>	<p>TCP or UDP destination port field. Normally, you specify this match in conjunction with the ip-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 port numbers are also listed):</p> <p>afs (1483), bgp (179), biff (512), bootpc (68), bootps (67), cvspserver (2401), cmd (514), dhcp (67), domain (53), eklogin (2105), ekshell (2106), exec (512), finger (79), ftp (21), ftp-data (20), 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), telnet (23), tacacs-ds (65), talk (517), tftp (69), timed (525), who (513), xdmcp (177), zephyr-clt (2103), zephyr-hm (2104)</p>

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 VSAs

Option	Description
<code>(allow deny)</code>	Accept a packet or discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.
<code>forwarding-class class-of-service</code>	<p>(Optional) Classify the packet in one of the following forwarding classes:</p> <ul style="list-style-type: none"> ■ assured-forwarding ■ best-effort ■ expedited-forwarding ■ network-control
<code>loss-priority (low medium high)</code>	(Optional) Set the packet loss priority (PLP) to low , medium , or high . Specify both the forwarding class and loss priority.

Related Topics ■ Filtering 802.1X Supplicants Using RADIUS Server Attributes

- Understanding 802.1X and VSAs on EX Series Switches

Published: 2009-07-21