

Configuring IPsec Conditions (SRC CLI)

You can configure IPsec conditions for JUNOS policy rules. Use the following configuration statements to add IPsec conditions to a classify-traffic condition:

```

policies group name list name rule name traffic-condition name ipsec-condition
{
  spi spi ;
  ip-flags ip-flags ;
  ip-flags-mask ip-flags-mask ;
  fragment-offset fragment-offset ;
  packet-length packet-length ;
  protocol protocol ;
  protocol-operation protocol-operation;
}

```

To add IPsec conditions to a classify-traffic condition:

1. From configuration mode, enter the IPsec configuration. For example:

```

user@host# edit policies group vpn list input rule pr traffic-condition ctc
ipsec-condition

```

2. (Optional) Specify the authentication header (AH) or the encapsulating security payload (ESP) security parameter index (SPI).

```

[edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
user@host# set spi spi

```

3. (Optional) Configure the value of the IP flags field in the IP header.

```

[edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
user@host# set ip-flags ip-flags

```

4. (Optional) Configure the mask that is associated with the IP flag.

```

[edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
user@host# set ip-flags-mask ip-flags-mask

```

5. (Optional) Configure the value of the fragment offset field.

```

[edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
user@host# set fragment-offset fragment-offset

```

6. (Optional) Configure the packet length on which to match. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead.

```

[edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
user@host# set packet-length packet-length

```

7. Configure the protocol matched by this classify-traffic condition.

```
[edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
user@host# set protocol protocol
```

8. (Optional) Verify the IPSec condition configuration.

```
[edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
user@host# show
spi 2;
ip-flags 0;
ip-flags-mask 0;
fragment-offset 0;
packet-length packetLength;
protocol ah;
protocol-operation 1;
```

- Related Topics**
- Before You Configure Classify-Traffic Conditions
 - Configuring Classify-Traffic Conditions
 - Configuring IPSec Conditions (C-Web Interface)

Published: 2009-09-22